Advanced Master

Alta Gestão de Cibersegurança (CISO, Chief Information Security Officer)

tech universidade tecnológica

tech universidade tecnológica

Advanced Master
Alta Gestão de Cibersegurança (CISO, Chief Information Security Officer)

- Modalidade: **online**
- Duração: **2 anos**
- Certificado: **TECH Universidade Tecnológica**
- Horário: **no seu próprio ritmo**
- Provas: **online**

Acesso ao site: www.techtitute.com/br/informatica/advanced-master/advanced-master-alta-gestao-ciberseguranca-ciso-chief-information-security-officer

Índice

01

Apresentação do programa

Atualmente, a cibersegurança tornou-se um pilar fundamental na proteção de indivíduos e empresas contra o crescente número de ameaças digitais. Essa disciplina se concentra não apenas em proteger os sistemas de tecnologia e as informações críticas das organizações, mas também em liderar o planejamento, a implementação e o monitoramento das estratégias de segurança. Assim, seu principal objetivo é mitigar os riscos e responder com eficácia a ataques e incidentes cibernéticos. As principais responsabilidades de um diretor de segurança cibernética incluem a elaboração de políticas de segurança, o gerenciamento de riscos tecnológicos e a liderança de equipes especializadas. Diante dos desafios decorrentes do progresso tecnológico e da digitalização, este programa foi projetado especificamente para abordar essas questões. A TECH não se concentra apenas em garantir a eficiência na proteção das informações, mas também em identificar e gerenciar novas vulnerabilidades. Isso posiciona o CISO como o elemento mais importante para a resiliência de qualquer organização.

Com a TECH, especialize-se e torne-se um líder em uma das áreas mais importantes de TI”

O Alta Gestão de Cibersegurança tem sido fundamental para garantir a estabilidade e a continuidade das organizações em um mundo digitalizado e altamente interconectado. Por meio da implementação de estratégias de segurança robustas e da adoção de tecnologias avançadas, os riscos foram atenuados e ataques catastróficos foram evitados. Em setores críticos, como o bancário, o de saúde e o de infraestrutura pública, a segurança foi reforçada por meio de governança e conformidade, impulsionada por líderes especializados nessa área.

Essa disciplina permitiu que as organizações estabelecessem ambientes de trabalho digitais mais seguros, fortalecendo assim a confiança de clientes, parceiros e usuários. Os resultados bem-sucedidos geraram economias significativas de milhões de dólares em possíveis perdas econômicas, além de promover uma cultura organizacional na qual a segurança é uma prioridade compartilhada. Além disso, provou ser essencial para proteger a inovação, a reputação e a sustentabilidade das organizações em um cenário em constante evolução.

Esse Advanced Master da TECH foi criado para especializar profissionais na liderança de estratégias de segurança eficazes. Ao longo do programa, os alunos aprenderão em seu próprio ritmo, concentrando-se no desenvolvimento de habilidades gerenciais e em uma visão estratégica de negócios. Além disso, você terá acesso a uma especialização de ponta que o preparará para se destacar em uma carreira que está em alta demanda no mercado global. Graças ao seu formato 100% online, os alunos poderão combinar seus estudos com suas responsabilidades profissionais, o que lhes permitirá progredir sem comprometer sua atividade profissional.

Este **Advanced Master em Alta Gestão de Cibersegurança (CISO, Chief Information Security Officer)** conta com o conteúdo mais completo e atualizado do mercado Suas principais características são:

- Desenvolvimento de casos práticos apresentados por especialistas na área de informática
- O conteúdo gráfico, esquemático e extremamente útil, fornece informações científicas e práticas sobre as disciplinas essenciais para o exercício da profissão
- Exercícios práticos em que o processo de autoavaliação é realizado para melhorar a aprendizagem
- Sua ênfase especial em metodologias inovadoras na alta gerência de cibersegurança (CISO, Chief Information Security Officer)
- Aulas teóricas, perguntas a especialistas, fóruns de discussão sobre temas controversos e trabalhos de reflexão individual
- Disponibilidade de acesso a todo o conteúdo a partir de qualquer dispositivo, fixo ou portátil, com conexão à Internet

Esse Advanced Master coloca você na vanguarda do setor e abre inúmeras oportunidades de carreira"

Desenvolva as habilidades necessárias para enfrentar os desafios do futuro sem deixar de lado suas atividades atuais”

Torne-se o protetor de infraestruturas tecnológicas com o método Relearning que se adapta ao seu ritmo de aprendizado.

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

O corpo docente deste programa abarca profissionais da área de jornalismo, que transferem a experiência do seu trabalho para esta capacitação, além de especialistas reconhecidos de sociedades científicas de referência e universidades de prestigio.

O conteúdo multimídia desenvolvido com a mais recente tecnologia educacional, oferece ao profissional uma aprendizagem situada e contextual, ou seja, um ambiente simulado que proporcionará um estudo imersivo e programado para capacitar em situações reais.

Este programa se fundamenta na Aprendizagem Baseada em Problemas, através da qual o aluno deverá resolver as diferentes situações de prática profissional que surgirem ao longo do programa. Para isso, o profissional contará com a ajuda de um inovador sistema de vídeo interativo, realizado por especialistas reconhecidos nesta área.

02

Por que 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 idiomas, a TECH se posiciona como líder em empregabilidade, com uma taxa de inserção profissional de 99%. Além disso, conta com um vasto corpo docente formado por mais de 6.000 professores de prestígio internacional.

Estude na maior universidade digital do mundo e garanta seu sucesso profissional. O futuro começa na TECH”

A melhor universidade online do mundo de acordo com a FORBES

A conceituada revista Forbes, especializada em negócios e finanças, destacou a TECH como «a melhor universidade online do mundo». Foi o que afirmou recentemente em um artigo de sua edição digital, no qual faz referência à história de sucesso dessa instituição, «graças à oferta acadêmica que oferece, à seleção de seu corpo docente e a um método de aprendizagem inovador destinado a formar os profissionais do futuro».

A melhor equipe de professores top internacional

A equipe de professores da TECH é composta por mais de 6.000 profissionais de renome internacional. Professores, pesquisadores e executivos seniores de multinacionais, incluindo Isaiah Covington, técnico de desempenho do Boston Celtics; Magda Romanska, pesquisadora principal do Harvard MetaLAB; Ignacio Wistumba, presidente do departamento de patologia molecular translacional do MD Anderson Cancer Center; e D.W. Pine, diretor de criação da revista TIME, entre outros.

A maior universidade digital do mundo

A TECH é a maior universidade digital do mundo. A TECH é a maior universidade digital do mundo. Somos a maior instituição educacional, com o melhor e mais amplo catálogo educacional digital, 100% online, abrangendo a grande maioria das áreas do conhecimento. Oferecemos o maior número de cursos próprios, pós-graduações e graduações oficiais do mundo. No total, são mais de 14.000 programas universitários em onze idiomas diferentes, o que nos torna a maior instituição de ensino do mundo.

Forbes
Mejor universidad online del mundo

Plan
de estudios más completo

Profesorado
TOP
Internacional

La metodología más eficaz

nº1
Mundial
Mayor universidad online del mundo

Os planos de estudos mais completos do panorama universitário

A TECH oferece os planos de estudos mais completos do cenário universitário, com programas que abrangem conceitos fundamentais e, ao mesmo tempo, os principais avanços científicos em suas áreas específicas. Além disso, esses programas são continuamente atualizados para garantir aos alunos a vanguarda acadêmica e as habilidades profissionais mais procuradas. Dessa forma, os programas da universidade proporcionam aos seus alunos uma vantagem significativa para impulsionar suas carreiras rumo ao sucesso.

Um método de aprendizado único

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

A universidade online oficial da NBA

A TECH é a Universidade Online Oficial da NBA. Por meio de um acordo com a maior liga de basquete do mundo, oferece aos seus alunos programas universitários exclusivos, além de uma grande variedade de recursos educacionais voltados para o negócio da liga e outras áreas da indústria esportiva. Cada programa tem um plano de estudos único e conta com palestrantes convidados excepcionais: profissionais com trajetórias esportivas destacadas que compartilham suas experiências sobre os temas mais relevantes.

Líderes em empregabilidade

A TECH se consolidou como a universidade líder em empregabilidade. 99% dos seus alunos conseguem um emprego na área que estudaram em até um ano após a conclusão de qualquer programa da universidade. Um número semelhante obtém uma melhoria imediata em sua carreira. Isso é possível graças a uma metodologia de ensino baseada na aquisição de competências práticas, essenciais para o desenvolvimento profissional.

Google Partner Premier

A gigante da tecnologia Google concedeu à TECH o selo Google Partner Premier. Esse reconhecimento, disponível apenas para 3% das empresas no mundo, destaca a experiência eficaz, flexível e adaptada que a universidade oferece aos seus alunos. O reconhecimento não apenas credencia o máximo rigor, desempenho e investimento nas infraestruturas digitais da TECH, mas também coloca essa universidade como uma das empresas de tecnologia mais avançadas do mundo.

A Universidade mais bem avaliada por seus alunos

O site de avaliação Global score posicionou a TECH como a universidade mais bem avaliada do mundo por seus alunos. Esse portal de avaliações, o mais confiável e prestigiado, pois verifica e valida a autenticidade de cada opinião publicada, concedeu à TECH a sua classificação mais alta, 4,9 de 5, com base em mais de 1000 avaliações recebidas. Esses números colocam a TECH como referência absoluta de universidade internacional.

03

Plano de estudos

O Advanced Master em Cibersegurança (CISO) foi criado para especializar líderes estratégicos capazes de gerenciar a segurança da informação em organizações globais. Por meio de uma abordagem abrangente e atualizada, o programa abrange áreas importantes, como governança de cibersegurança e gerenciamento de riscos. Dessa forma, os alunos desenvolverão habilidades gerenciais para liderar equipes de alto desempenho e implementar políticas de segurança. Além disso, ao mesmo tempo em que adquirem conhecimento das 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 você para ser o estrategista que previne, detecta e mitiga as ameaças cibernéticas em todo o ambiente de negócios global”

Módulo 1. Ciberespionagem e cibersegurança

1.1. Ciberinteligência
- 1.1.1. Ciberinteligência
  - 1.1.1.1. Inteligência
    - 1.1.1.1.1. Ciclo de inteligência
  - 1.1.1.2. Ciberinteligência
  - 1.1.1.3. Ciberespionagem e cibersegurança
- 1.1.2. O analista de inteligência
  - 1.1.2.1. O papel do analista de inteligência
  - 1.1.2.2. Vias do analista de inteligência em atividade avaliativa

1.2. Segurança Cibernética
- 1.2.1. Camadas de segurança
- 1.2.2. Identificação de ameaças cibernéticas
  - 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 comumente utilizados

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

1.4. Metodologias de avaliação
- 1.4.1. Análise de inteligência
- 1.4.2. Técnicas para organizar as informações adquiridas
- 1.4.3. Confiabilidade e credibilidade das fontes de informação
- 1.4.4. Metodologias de análise
- 1.4.5. Apresentação dos resultados da inteligência

1.5. Auditorias e documentação
- 1.5.1. Auditoria na segurança da informática
- 1.5.2. Documentação e licenças para auditoria
- 1.5.3. Tipos de auditoria
- 1.5.4. Entregáveis
  - 1.5.4.1. Relatório técnico
  - 1.5.4.2. Relatório Executivo

1.6. Anonimato na rede
- 1.6.1. Uso do anonimato
- 1.6.2. Técnicas de anonimización (Proxy, VPN)
- 1.6.3. Redes TOR, Freenet e IP2

1.7. Ameaças e tipos de segurança
- 1.7.1. Tipos de ameaças
- 1.7.2. Segurança física
- 1.7.3. Segurança de rede
- 1.7.4. Segurança lógica
- 1.7.5. Segurança de Aplicações Web
- 1.7.6. Segurança da dispositivos móveis

1.8. Regulamentos e *compliance*
- 1.8.1. RGPD
- 1.8.2. A estratégia nacional de cibersegurança de 2019
- 1.8.3. Família ISO 27000
- 1.8.4. Estrutura de Segurança Cibernética da NIST
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. Normativas *cloud*
- 1.8.8. SOX
- 1.8.9. PCI

1.9. Análise de risco e métricas
- 1.9.1. Escopo dos riscos
- 1.9.2. O patrimônio
- 1.9.3. Ameaças

1.9.4. vulnerabilidades
1.9.5. Avaliação de risco
1.9.6. Tratamento de risco
1.10. Importantes órgãos de segurança cibernética
1.10.1. NIST
1.10.2. ENISA
1.10.3. INCIBE
1.10.4. OEA
1.10.5. UNASUR - PROSUR

Módulo 2. Segurança do Host

2.1. Cópias de segurança
2.1.1. Estratégias para backups
2.1.2. Ferramentas para Windows
2.1.3. Ferramentas para Linux
2.1.4. Ferramentas para MacOS
2.2. Anti-vírus do usuário
2.2.1. Tipos de antivírus
2.2.2. Antivírus para Windows
2.2.3. Antivírus para Linux
2.2.4. Antivírus para MacOS
2.2.5. Antivírus para smartphones
2.3. Detectores de intrusão - HIDS
2.3.1. Métodos de detecção de intrusão
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 senhas
2.5.1. Password
2.5.2. LastPass
2.5.3. KeePass
2.5.4. StickyPassword
2.5.5. RoboForm
2.6. Detectores de *phishing*
2.6.1. Detecção manual de *phishing*
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-tracking
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. Controle 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 atualização
2.10.4. Privilégios para instalar software

Módulo 3. Segurança de rede (perímetro)

3.1. Sistemas de detecção e prevenção de ameaças
3.1.1. Estrutura geral para incidentes de segurança
3.1.2. Sistemas de defesa atuais: *Defense in Depth* e SOC
3.1.3. Arquiteturas de redes atuais

3.1.4. Tipos de ferramentas de detecção 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 detecção de instâncias/hosts, containers e serverless
3.2. Firewall
3.2.1. Tipos de firewalls
3.2.2. Ataques e atenuações
3.2.3. Firewalls comuns em *kernel* Linux
3.2.3.1. UFW
3.2.3.2. *Nftables e iptables*
3.2.3.3. Firewalld
3.2.4. Sistemas de detecção baseados em logs do sistema
3.2.4.1. TCP Wrappers
3.2.4.2. BlockHosts e DenyHosts
3.2.4.3. Fai2ban
3.3. Sistemas de Detecção e Prevenção de Intrusão (IDS/IPS)
3.3.1. Ataques ao IDS/IPS
3.3.2. Sistemas IDS/IPS
3.3.2.1. Snort
3.3.2.2. Suricata
3.4. Firewalls de próxima geração (NGFW)
3.4.1. Diferenças entre NGFW e Firewall tradicional
3.4.2. Principais capacidades
3.4.3. Soluções comerciais
3.4.4. Firewalls para serviços de Cloud
3.4.4.1. Arquitetura Cloud VPC
3.4.4.2. Cloud ACLs
3.4.4.3. Security Group
3.5. *Proxy*
3.5.1. Tipos de *proxy*
3.5.2. Uso de *Proxy* Vantagens e Desvantagens
3.6. Motores antivírus
3.6.1. Contexto geral de *Malware* e IOCs
3.6.2. Problemas no motor do antivírus
3.7. Sistemas de proteção de correio
3.7.1. Antispam
3.7.1.1. Listas negras e brancas
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 uso
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 e HoneyNets
3.10.4. CASB

Módulo 4. Segurança para 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. As 10 principais vulnerabilidades
4.2.2. Comunicações, redes e modos de conexão

4.3. O dispositivo móvel no ambiente empresarial
- 4.3.1. Riscos
- 4.3.2. Políticas de segurança
- 4.3.3. Monitoramento de dispositivos
- 4.3.4. Gerenciamento de dispositivos móveis (MDM)

4.4. Privacidade do usuário e segurança dos dados
- 4.4.1. Estados de informação
- 4.4.2. Proteção e confidencialidade dos dados
  - 4.4.2.1. Permissões
  - 4.4.2.2. Criptografia
- 4.4.3. Armazenamento seguro de dados
  - 4.4.3.1. Armazenamento seguro no 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 de dados

4.6. Principais ameaças
- 4.6.1. Usuário não forçado
- 4.6.2. *Malware*
  - 4.6.2.1. Tipos de malware
- 4.6.3. Engenharia social
- 4.6.4. Vazamento de dados
- 4.6.5. Roubo de informações
- 4.6.6. Redes Wi-Fi inseguras
- 4.6.7. Software desatualizado
- 4.6.8. Aplicações maliciosas
- 4.6.9. Senhas 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. Fraude por personificação (Integridade)
- 4.6.14. Criptografia fraca ou quebrada
- 4.6.15. Negação de Serviço (DoS)

4.7. Principais ataques
- 4.7.1. Ataques de *phishing*
- 4.7.2. Ataques relacionados aos modos de comunicação
- 4.7.3. Ataques de *Phishing*
- 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 de *Payload* e extração de informações
- 4.8.3. Hacking sobre *dispositivos* iOS: mecanismos e ferramentas
- 4.8.4. Hacking em *dispositivos* Android: mecanismos e ferramentas

4.9. Testes de penetração
- 4.9.1. iOS *pentesting*
- 4.9.2. Android *PenTesting*
- 4.9.3. Ferramentas

4.10. Segurança e proteção
- 4.10.1. Configurações de segurança
  - 4.10.1.1. Nos dispositivos iOS
  - 4.10.1.2. Dispositivos Android
- 4.10.2. Medidas de segurança
- 4.10.3. Ferramentas de proteção

Módulo 5. Segurança de IoT

5.1. Dispositivos.
- 5.1.1. Tipos de dispositivos
- 5.1.2. Arquiteturas padronizadas
  - 5.1.2.1. ONEM2M
  - 5.1.2.2. IoTWF
- 5.1.3. Protocolos de implementação
- 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 de 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. Automação doméstica
- 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. Fazendo pagamentos e obtendo serviços
- 5.6.3. Conectividade

5.7. *Wearables*
- 5.7.1. Roupas inteligentes
- 5.7.2. Joias inteligentes
- 5.7.3. Relógios Inteligentes

5.8. Setor de saúde
- 5.8.1. Exercício/monitoramento da frequência cardíaca
- 5.8.2. Monitoramento de pacientes e pessoas idosas
- 5.8.3. Dispositivos implantáveis
- 5.8.4. Robôs cirúrgicos

5.9. Conectividade
- 5.9.1. Wi-Fi/Gateway
- 5.9.2. Bluetooth
- 5.9.3. Conectividade embutida

5.10. Securitização
- 5.10.1. Redes dedicadas
- 5.10.2. Gerenciador de senhas
- 5.10.3. Uso de protocolos criptografados
- 5.10.4. Dicas de uso

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. Implantação 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 código aberto (OSINT)
- 6.3.2. Busca de violações e vulnerabilidades de dados
- 6.3.3. Uso de ferramentas passivas

6.4. Escaneamento em rede
- 6.4.1. Ferramentas de escaneamento
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. Outras ferramentas de Escaneamento
- 6.4.2. Técnicas de digitalização
- 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 NetBIOS e Samba
- 6.5.4. Enumeração LDAP
- 6.5.5. Enumeração 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 Vulnerabilidade
  - 6.6.2.1. CVSS
  - 6.6.2.2. CVE
  - 6.6.2.3. NVD

6.7. Ataques a redes sem fio
- 6.7.1. Metodologia de hacking em redes wireless
  - 6.7.1.1. Wi-Fi *Discovery*
  - 6.7.1.2. Análise de tráfego
  - 6.7.1.3. Ataques de *aircrack*
    - 6.7.1.3.1. Ataques WEP
    - 6.7.1.3.2. Ataques WPA/WPA2
  - 6.7.1.4. Ataques de *Evil Twin*
  - 6.7.1.5. Ataques a WPS
  - 6.7.1.6. *Jamming*
- 6.7.2. Ferramentas para a segurança sem fio

6.8. Hacking de servidores web
- 6.8.1. *Cross Site Scripting*
- 6.8.2. CSRF
- 6.8.3. *Sessão Hijacking*
- 6.8.4. *SQLinjection*

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

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

Módulo 7. Engenharia inversa

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. Tratamento de erros
- 7.1.5. Compilador GCC

7.2. Tipos de análise em compiladores
- 7.2.1. Análise lexical
  - 7.2.1.1. Terminologia
  - 7.2.1.2. Componentes léxicos
  - 7.2.1.3. Analisador Lexical LEX
- 7.2.2. Análise sintática
  - 7.2.2.1. Gramáticas sem contexto
  - 7.2.2.2. Tipos de análise sintática
    - 7.2.2.2.1. Análise top-down
    - 7.2.2.2.2. Análise bottom-up
  - 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. Analizadores 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 Códigos 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. Uso do *break*
- 7.4.3. Funções

7.5. Arquitetura de Hardware x86
- 7.5.1. Arquitetura de do processador x86
- 7.5.2. Estruturas de dados de x86
- 7.5.3. Estruturas de Códigos de x86
- 7.5.3. Estruturas de Códigos de x86

7.6. Arquitetura de Hardware ARM
- 7.6.1. Arquitetura do processador ARM
- 7.6.2. Estruturas de dados de ARM
- 7.6.3. Estruturas de Códigos de ARM

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

7.8. Análise de código Dinâmica
- 7.8.1. Análise comportamental
  - 7.8.1.1. Comunicações
  - 7.8.1.2. Monitoração
- 7.8.2. Depuradores de código Linux
- 7.8.3. Depuradores de código no Windows

7.9. Sandbox
- 7.9.1. Arquitetura de *Sandbox*
- 7.9.2. Evasão de *Sandbox*
- 7.9.3. Técnicas de detecção
- 7.9.4. Técnicas de prevenção

7.9.5. Contra-medidas
7.9.6. Sandbox e Linux
7.9.7. Sandbox e Windows
7.9.8. Sandbox em MacOS
7.9.9. Sandbox em Android
7.10. Análises de *malware*
7.10.1. Métodos de análise de *malware*
7.10.2. Técnicas de ofuscação de *malware*
7.10.2.1. Ofuscação executável
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. Controle de autenticação
8.2.2. Controle de papéis e privilégios
8.2.3. Requisitos orientados ao risco
8.2.4. Aprovação de privilégios
8.3. Fases de análise e projeto
8.3.1. Acesso aos componentes e administração do sistema
8.3.2. Pistas de auditoria
8.3.3. Gestão da sessão
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. Assegurando o ambiente de desenvolvimento
8.4.2. Preparação da documentação técnica
8.4.3. Codificação segura
8.4.4. Segurança das comunicações
8.5. Boas práticas de codificação seguras
8.5.1. Validação dos dados de entrada
8.5.2. Codificação dos dados de
8.5.3. Estilo de programação
8.5.4. Gerenciamento de registro de mudanças
8.5.5. Práticas criptográficas
8.5.6. Gerenciamento de erros e logs
8.5.7. Gerenciamento de arquivos
8.5.8. Gestão de Memória
8.5.9. Padronização e reutilização das funções de segurança
8.6. Preparação do servidor *hardening*
8.6.1. Gerenciamento de usuários, grupos e funções no servidor
8.6.2. Instalação de software
8.6.3. *Hardening* do servidor
8.6.4. Configuração robusta do ambiente de aplicação
8.7. Preparação da BD *hardening*
8.7.1. Otimização do motor da BD
8.7.2. Criação de seu próprio usuário para a aplicação
8.7.3. Atribuição dos privilégios necessários ao usuário
8.7.4. *Hardening* da BD
8.8. Fase de testes
8.8.1. Controle de qualidade nos controles de segurança
8.8.2. Inspeção por fases de código
8.8.3. Verificação da gestão das configurações
8.8.4. Teste da caixa preta
8.9. Preparando a transição para a produção
8.9.1. Realizar o controle de mudanças
8.9.2. Realizar o procedimento de mudança de produção
8.9.3. Realizar o procedimento de *rollback*
8.9.4. Testes de pré-produção

8.10. Fase de manutenção
- 8.10.1. Garantia baseada em risco
- 8.10.2. Teste de manutenção de segurança da caixa branca
- 8.10.3. Teste de manutenção de segurança da caixa preta

Módulo 9. Implementação Prática de Políticas de Segurança em Software e Hardware

9.1. Implementação Prática de Políticas de Segurança em Software e Hardware
- 9.1.1. Implementação da 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 "Defesa Confidencial"
- 9.2.4. O RFID ativo

9.3. Políticas de segurança no acesso a software e sistemas
- 9.3.1. Implementação de políticas de controle de acesso
- 9.3.2. Implementação de políticas de acesso às comunicações
- 9.3.3. Tipos de ferramentas de segurança para controle de acesso

9.4. Gestão de acesso de usuários
- 9.4.1. Gestão dos direitos de acesso
- 9.4.2. Segregação de papéis e funções de acesso
- 9.4.3. Implementação de direitos de acesso em sistemas

9.5. Controle de acesso a sistemas e aplicações
- 9.5.1. Regras de acesso mínimo
- 9.5.2. Tecnologias de login seguro
- 9.5.3. Políticas de segurança de senhas

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 hardening de sistemas
- 9.7.1. Controles CIS básicos
- 9.7.2. Controles CIS fundamentais
- 9.7.3. Controles CIS organizacionais

9.8. Segurança operacional
- 9.8.1. Proteção contra códigos maliciosos
- 9.8.2. Cópias de segurança
- 9.8.3. Registro de atividade e supervisão

9.9. Gestão das vulnerabilidades técnicas
- 9.9.1. Vulnerabilidades técnicas
- 9.9.2. Gestão das vulnerabilidades técnicas
- 9.9.3. Restrições na instalação de software

9.10. Implementação de práticas de política de segurança
- 9.10.1. Vulnerabilidades lógicas
- 9.10.2. Implementação de políticas de defesa

Módulo 10. Análise Forense

10.1. Aquisição e replicação de dados
- 10.1.1. Aquisição volátil de dados
  - 10.1.1.1. Informações do sistema
  - 10.1.1.2. Informação da rede
  - 10.1.1.3. Ordem de volatilidade
- 10.1.2. Aquisição estática de dados
  - 10.1.2.1. Criação de uma imagem duplicada
  - 10.1.2.2. Preparação de um documento de 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 das técnicas anti-forenses
- 10.2.1. Objetivos das técnicas forenses
- 10.2.2. Eliminação de dados
  - 10.2.2.1. Eliminação de dados e arquivos
  - 10.2.2.2. Recuperação de arquivos
  - 10.2.2.3. Recuperação de partições apagadas
- 10.2.3. Proteção por senha
- 10.2.4. Esteganografia
- 10.2.5. Limpeza segura do dispositivo
- 10.2.6. Criptografia

10.3. Sistema operacional forense
- 10.3.1. Windows Forensics
- 10.3.2. Forense Linux
- 10.3.3. Mac forensics

10.4. Análise forense de rede
- 10.4.1. Análise de logs
- 10.4.2. Correlação dos dados
- 10.4.3. Pesquisa de rede
- 10.4.4. Passos a seguir na análise forense da rede

10.5. Análise forense de site
- 10.5.1. Investigação de ataques na web
- 10.5.2. Detecção de ataques
- 10.5.3. Localização de endereços IP

10.6. Base de dados Forense
- 10.6.1. Forense da MSSQL
- 10.6.2. Forense da MySQL
- 10.6.3. Forense da Web
- 10.6.4. Forense da MSSQL

10.7. Análise forense em Cloud
- 10.7.1. Tipos de crimes em Cloud
  - 10.7.1.1. Cloud como tema
  - 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 dos serviços de armazenamento em Cloud
- 10.7.4. Ferramentas de análise forense em Cloud

10.8. Investigação de crimes por e-mail
- 10.8.1. Sistemas de e-mail
  - 10.8.1.1. Clientes de e-mail
  - 10.8.1.2. Servidor de e-mail
  - 10.8.1.3. Servidor SMTP
  - 10.8.1.4. Servidor POP3
  - 10.8.1.5. Servidor IMAP4
- 10.8.2. Crimes por e-mail
- 10.8.3. Mensagem de e-mail
  - 10.8.3.1. Cabeçalhos padrão
  - 10.8.3.2. Cabeçalhos estendidos
- 10.8.4. Passos para a investigação destes crimes
- 10.8.5. Ferramentas forenses por e-mail

10.9. Forense móvel
- 10.9.1. Redes celulares
  - 10.9.1.1. Tipos de redes
  - 10.9.1.2. Conteúdo 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 arquivo

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. Lidando com a mídia

Módulo 11. Segurança no projeto e desenvolvimento de sistemas

11.1. Sistemas de informação
- 11.1.1. Domínios de 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 de sistemas de informação
  - 11.2.1.1. Empresarial
  - 11.2.1.2. Estratégico
  - 11.2.1.3. De acordo com o escopo de aplicação
  - 11.2.1.4. Específico
- 11.2.2. Sistemas de informação. Exemplos reais
- 11.2.3. Evolução dos sistemas de informação: Fases
- 11.2.4. Metodologias dos sistemas de Informação

11.3. Segurança dos sistemas de Informação Implicações legais
- 11.3.1. Acesso a dados
- 11.3.2. Ameaças à segurança: Vulnerabilidades
- 11.3.3. Implicações legais Delitos
- 11.3.4. Procedimentos de manutenção de um sistema de informação

11.4. Segurança dos sistemas de Informação Protocolo de segurança
- 11.4.1. Segurança de um sistema de Informação
  - 11.4.1.1. Integridade
  - 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 em sistemas de Informação Medidas e sistemas de controle de acesso
- 11.5.1. Medidas de segurança
- 11.5.2. Tipo de medidas de segurança
  - 11.5.2.1. Prevenção
  - 11.5.2.2. Detecção
  - 11.5.2.3. Correção
- 11.5.3. Sistemas de controle 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. Criminalidade informática
- 11.7.1. Crime Digital
- 11.7.2. Crimes Digitais Tipologia
- 11.7.3. Crime Digital Ataques Tipologia
- 11.7.4. O caso da Realidade Virtual
- 11.7.5. Perfis dos infratores e das vítimas. Tipificação do crime
- 11.7.6. Crimes Digitais Exemplos e casos reais

11.8. Plano de segurança em um sistema de informação
- 11.8.1. Plano de segurança Objetivos
- 11.8.2. Plano de segurança Planejamento
- 11.8.3. Plano de riscos Análise
- 11.8.4. Política de segurança Implementação na organização
- 11.8.5. Plano de segurança Implementação na organização
- 11.8.6. Procedimentos de segurança Tipos
- 11.8.7. Planos de segurança Exemplos

11.9. Plano de Contingência
- 11.9.1. Plano de Contingência Funções
- 11.9.2. Plano de emergência: Elementos e objetos
- 11.9.3. Plano de contingência na organização Implementação
- 11.9.4. Planos de Contingência Exemplos

11.10. Governança de segurança dos sistemas de informação
- 11.10.1. Regulamentações legais
- 11.10.2. Padrões
- 11.10.3. Certificações
- 11.10.4. Tecnologias

Módulo 12. Arquitetura e modelos de segurança da informação

12.1. Arquitetura de segurança da informação
- 12.1.1. SGSI/PDS
- 12.1.2. Alinhamento estratégico
- 12.1.3. Gestão do risco
- 12.1.4. Avaliação do desempenho

12.2. Modelos de segurança da informação
- 12.2.1. Baseado em políticas de segurança
- 12.2.2. Baseado em ferramentas de proteção
- 12.2.3. Baseado em equipes de trabalho

12.3. Modelo de segurança Componentes-chave
- 12.3.1. Identificação de riscos
- 12.3.2. Definição de controles
- 12.3.3. Avaliação contínua de níveis de risco
- 12.3.4. Plano de conscientização para funcionários, fornecedores, parceiros, etc.

12.4. Processo de gestão de riscos
- 12.4.1. Identificação de ativos
- 12.4.2. Identificação de ameaças
- 12.4.3. Avaliação de risco
- 12.4.4. Priorização de controles
- 12.4.5. Reavaliação e risco residual

12.5. Processos de negócio e segurança da informação
- 12.5.1. Processos de negócio
- 12.5.2. Avaliação de risco baseada em parâmetros de negócio
- 12.5.3. Análise de impacto nos negócios
- 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. Planejar
  - 12.6.1.2. Realizar
  - 12.6.1.3. Verificar
  - 12.6.1.4. Atuar

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 da infraestrutura de rede
- 12.7.5. Tecnologias e soluções de criptografia
- 12.7.6. Segurança de terminais (EDR)

12.8. O marco regulatório
- 12.8.1. Normativas setoriais
- 12.8.2. Certificações
- 12.8.3. Legislações

12.9. Norma ISO 27001
- 12.9.1. Implementação
- 12.9.2. Certificado
- 12.9.3. Auditorias e testes de intrusão
- 12.9.4. Gestão contínua de risco
- 12.9.5. Classificação da informação

12.10. Legislação de privacidade RGPD (GDPR)
- 12.10.1. Escopo do Regulamento Geral de Proteção de Dados (RGPD)
- 12.10.2. Dados pessoais
- 12.10.3. Funções no processamento de dados pessoais
- 12.10.4. Direitos ARCO
- 12.10.5. O DPO Funções

Módulo 13. Sistemas de Gestão de Segurança da Informação(SGSI)

13.1. Segurança da informação. Aspectos fundamentais
- 13.1.1. Segurança da informação
  - 13.1.1.1. Confidencialidade
  - 13.1.1.2. Integridade
  - 13.1.1.3. Disponibilidade
  - 13.1.1.4. Medidas de Segurança da Informação

13.2. Sistemas de gestão de segurança da informação
- 13.2.1. Modelos de gestão de segurança da informação
- 13.2.2. Documentos para implantar 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 gestão de segurança da informação
- 13.3.4. Outros padrões de referência

13.4. Normas ISO/IEC 27.000
- 13.4.1. Objeto e área de aplicação
- 13.4.2. Estrutura da norma
- 13.4.3. Certificado
- 13.4.4. Fases de acreditação
- 13.4.5. Benefícios das normas ISO/IEC 27.000

13.5. Design e implantação de um sistema geral de segurança da informação
- 13.5.1. Fases de implantação de um sistema geral de segurança da informação
- 13.5.2. Plano 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 conformidade com os padrões/normas

13.7. Fase II: preparação
- 13.7.1. Contexto organizacional
- 13.7.2. Análise de regulamentos de segurança aplicáveis
- 13.7.3. Escopo do sistema geral de segurança da informação
- 13.7.4. Políticas do sistema geral de segurança da informação
- 13.7.5. Objetivos do sistema geral de segurança da informação

13.8. Fase III: planejamento
- 13.8.1. Classificação de ativos
- 13.8.2. Avaliação de riscos
- 13.8.3. Identificação de ameaças e riscos

13.9. Fase IV: implantação e acompanhamento
- 13.9.1. Análise de resultados
- 13.9.2. Atribuição de responsabilidades
- 13.9.3. Calendário 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 TI

14.1. Gestão da Segurança
- 14.1.1. Operações de segurança
- 14.1.2. Aspecto legal e regulatório
- 14.1.3. Viabilidade do negócio
- 14.1.4. Gestão de riscos
- 14.1.5. Gestão de identidades e acessos

14.2. Estrutura da área de segurança A sede do CISO
- 14.2.1. Estrutura organizacional Posição do CISO na estrutura
- 14.2.2. As linhas de defesa
- 14.2.3. Organograma do escritório do CISO
- 14.2.4. Gestão de orçamento

14.3. Governança de segurança
- 14.3.1. Comitê de Segurança
- 14.3.2. Comitê de Monitoramento de Riscos
- 14.3.3. Comitê de Auditoria
- 14.3.4. Comitê de crises

14.4. Governança de segurança. Funções
- 14.4.1. Políticas e normas
- 14.4.2. Plano diretor de segurança
- 14.4.3. Paineis de controle
- 14.4.4. Conscientização e capacitação
- 14.4.5. Segurança na cadeia de suprimentos

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. Marco de trabalho em cibersegurança NIST CSF
- 14.6.1. Metodologia NIST
  - 14.6.1.1. Identificar
  - 14.6.1.2. Proteger
  - 14.6.1.3. Detectar
  - 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. Auditorias de segurança
- 14.8.1. Teste de intrusão
- 14.8.2. Exercícios de *Red Team*
- 14.8.3. Auditorias de código fonte. Desenvolvimento seguro
- 14.8.4. Segurança dos 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. Atividade 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 incidentes cibernéticos

14.10. Gestão de vulnerabilidades
- 14.10.1. Análise de vulnerabilidades
- 14.10.2. Avaliação vulnerabilidade
- 14.10.3. Bastion Host do sistema
- 14.10.4. Vulnerabilidades do 0° dia. 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 incidências
- 15.1.2. Responsabilidades e procedimentos
- 15.1.3. Notificação de eventos

15.2. Sistemas de Detecção e Prevenção de Intrusão (IDS/IPS)
- 15.2.1. Dados operacionais do sistema
- 15.2.2. Tipos de sistemas de detecção de intrusão
- 15.2.3. Critérios para a localização do IDS/IPS

15.3. Resposta a incidentes de segurança
- 15.3.1. Procedimento de coleta 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 coleta de evidências eletrônicas
  - 15.5.2.1. Análise de evidências eletrônicas
  - 15.5.2.2. Coleta de evidências eletrônicas

15.6. Ferramentas de Sistemas de Detecção e Prevenção de Intrusão (IDS/IPS)
- 15.6.1. Snort
- 15.6.2. Suricata
- 15.6.3. Solar-Winds

15.7. Ferramentas de centralização 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 incidentes cibernéticos
- 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. Manejo de um incidente
- 15.9.3. Coordenação e compartilhamento de informações

15.10. Norma ISO 27035
- 15.10.1. Norma ISO 27035. Princípios da gestão de incidentes
- 15.10.2. Diretrizes para a elaboração de um plano de gestão de incidentes
- 15.10.3. Diretrizes de operações de resposta a incidentes

Módulo 16. Análise de riscos e ambiente de segurança TI

16.1. Análise do ambiente
- 16.1.1. Análise da situação atual
  - 16.1.1.1. Ambiente 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. Ambiente 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. Econômico
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. Fortalezas
16.2. Risco e incerteza
16.2.1. Riscos
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. Objetivo
16.3.2. Princípios
16.3.3. Marco de referência
16.3.4. Processo
16.4. Metodologia de análise e gestão dos riscos do sistema 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 (PILAR)
16.5. Transferência de risco cibernético
16.5.1. Transferência de riscos
16.5.2. Riscos cibernéticos Tipologia
16.5.3. Seguro contra riscos cibernéticos
16.6. Metodologias ágeis para a gestão de riscos
16.6.1. Metodologias Ágeis
16.6.2. Scrum para gestão de risco
16.6.3. *Agile Risk Management*
16.7. Tecnologias para gestão de risco
16.7.1. Inteligência artificial aplicada à gestão de riscos
16.7.2. *Blockchain* e criptografia Métodos de preservação de valor
16.7.3. Computação quântica Oportunidade ou ameaça
16.8. Mapeamento de riscos de TI baseados em metodologias ágeis
16.8.1. Representação de probabilidade e impacto em ambientes ágeis
16.8.2. O risco como uma ameaça ao valor
16.8.3. Revolução 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 orientado para o risco
16.10. Inovação e transformação digital na gestão de riscos de TI
16.10.1. Inovação e transformação digital na gestão de riscos de TI
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 de riscos
17.1.2. O risco na segurança
17.1.3. Metodologias na gestão de ameaças
17.1.4. Implantação 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 proteção

17.3. Sistemas de auditoria para localização de ameaças
- 17.3.1. Classificação e fluxo de informações
- 17.3.2. Análise de processos vulneráveis

17.4. Classificação de riscos
- 17.4.1. Tipos de riscos
- 17.4.2. Cálculo da probabilidade de ameaças
- 17.4.3. Risco residual

17.5. Tratamento de risco
- 17.5.1. Implementação de medidas de salvaguarda
- 17.5.2. Transferir ou assumir

17.6. Controle de riscos
- 17.6.1. Processo contínuo da gestão de riscos
- 17.6.2. Implementação de métricas de segurança
- 17.6.3. Modelo estratégico de métricas de segurança da informação

17.7. Metodologias práticas para análise e controle de ameaças
- 17.7.1. Catálogo de ameaças
- 17.7.2. Catálogo de medidas de controle
- 17.7.3. Catálogo de salvaguardas

17.8. Norma ISO 27005
- 17.8.1. Identificação de riscos
- 17.8.2. Análise de risco
- 17.8.3. Avaliação de 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 prejuízo

17.10. Design de fases e processos na análise de ameaças
- 17.10.1. Identificação de elementos críticos da organização
- 17.10.2. Determinação de ameaças e impactos
- 17.10.3. Análise de impacto e riscos
- 17.10.4. Metodologias

Módulo 18. Implementação Prática de Políticas de Segurança contra Ataques

18.1. *System Hacking*
- 18.1.1. Riscos e vulnerabilidades
- 18.1.2. Contra-medidas

18.2. DoS em serviços
- 18.2.1. Riscos e vulnerabilidades
- 18.2.2. Contra-medidas

18.3. *Sessão Hijacking*
- 18.3.1. O processo de *Hijacking*
- 18.3.2. Contramedidas para *Hijacking*

18.4. Evasão do IDS, *Firewalls and Honeypots*
- 18.4.1. Técnicas de prevenção
- 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 wifi
- 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 que causam ransomware
- 18.9.2. Implementação de contramedidas

18.10. Engenharia social
- 18.10.1. Tipos de engenharia social
- 18.10.2. Contramedidas à engenharia social

Módulo 19. Criptografia em TI

19.1. Criptografia
- 19.1.1. Criptografia
- 19.1.2. Fundamentos matemáticos

19.2. Criptologia
- 19.2.1. Criptologia
- 19.2.2. Criptanálise
- 19.2.3. Esteganografia e estegoanálise

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. Comprimento da chave
- 19.4.2. Gestão da chaves
- 19.4.3. Tipos de algoritmos
- 19.4.4. Funções Hash *Hash*
- 19.4.5. Geradores de números pseudo-aleatórios
- 19.4.6. Uso de algoritmos

19.5. Criptografia simétrica
- 19.5.1. Cifrados 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 cifrados 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 y 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 em relação à computação quântica
- 19.10.3. Distribuição de chaves quânticas

Módulo 20. Gestão de identidades e acessos em Segurança TI

20.1. Gestão de identidades e acessos(IAM)
- 20.1.1. Identidade digital
- 20.1.2. Gestão de identidades
- 20.1.3. Federação de identidades

20.2. Controle de acesso físico
- 20.2.1. Sistemas de proteção
- 20.2.2. Segurança das áreas
- 20.2.3. Instalações de recuperação

20.3. Controle de acesso lógico
- 20.1.1. Autenticação Tipologia
- 20.1.2. Protocolos de autenticação
- 20.1.3. Ataques de autenticação

20.4. Controle de acesso lógico Autenticação MFA
- 20.4.1. Controle de acesso lógico Autenticação MFA
- 20.4.2. Senhas Importância
- 20.4.3. Ataques de autenticação

20.5. Controle de acesso lógico Autenticação biométrica
- 20.5.1. Controle de acesso lógico Autenticação biométrica
  - 20.5.1.1. Autenticação biométrica Requisitos
- 20.5.2. Funcionamento
- 20.5.3. Modelos 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 controle de acesso
- 20.8.1. FW - Parede de Fogo
- 20.8.2. VPN - Redes Privadas Virtuais
- 20.8.3. IDS - Sistema de Detecção de Intrusão

20.9. Sistemas de controle de acesso a rede
- 20.9.1. NAC
- 20.9.2. Arquitetura e elementos
- 20.9.3. Operação e padronização

20.10. Acesso a redes sem fio
- 20.10.1. Tipos de redes sem fio
- 20.10.2. Segurança em redes sem fio
- 20.10.3. Ataques em redes sem fio

Módulo 21. Segurança nas comunicações e operação de software

21.1. Segurança informática em comunicações e operação software
- 21.1.1. Segurança informática
- 21.1.2. Segurança Cibernética
- 21.1.3. Segurança na nuvem

21.2. Segurança informática em comunicações e operação de 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 de software
- 21.1.1. Desenvolvimento seguro Protocolo HTTP
- 21.1.2. Desenvolvimento seguro Ciclo de vida
- 21.1.3. Desenvolvimento seguro Segurança PHP
- 21.1.4. Desenvolvimento seguro Segurança NET
- 21.1.5. Desenvolvimento seguro Melhores práticas

21.6. Sistemas de gestão de segurança da informação em comunicações e operação de 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. Operações SOC
- 21.7.3. SIEM *vendors*

21.8. A função da segurança nas organizações
- 21.8.1. Funções nas organizações
- 21.8.2. Funções dos especialistas em IoT nas companhias
- 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 implementação

21.10. A Cibersegurança atualmente
- 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 na segurança
- 22.1.3. Segurança em ambientes *Cloud Computing.* Aspectos principais 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 compartilhada
- 22.3.1. Elementos de segurança gestionados pelo fornecedor
- 22.3.2. Elementos gestionados pelo cliente
- 22.3.3. Definição da estratégia de 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 de sistemas de banco de dados
- 22.5.3. Securitização de dados em trânsito

22.6. Proteção de infraestrutura
- 22.6.1. Projeto e implementação de rede segura
- 22.6.2. Segurança em recursos computacionais
- 22.6.3. Ferramentas e recursos para a proteção da infraestrutura

22.7. Detecção de ameaças e ataques
- 22.7.1. Sistemas de auditoria, *Logging* e monitoramento
- 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. Plano da continuidade de negócio
- 22.8.3. Análise forense e remediação de incidentes da mesma natureza

22.9. Segurança em *Clouds* públicos
- 22.9.1. AWS (Amazon Web Services)
- 22.9.2. Microsoft Azure
- 22.9.3. Google GCP
- 22.9.4. Oracle Cloud

22.10. Regulamentos e conformidade
- 22.10.1. Cumprimento das normas de segurança
- 22.10.2. Gestão de riscos
- 22.10.3. Pessoas e processos nas organizações

Módulo 23. Ferramentas de Monitoramento em Políticas de Segurança de Sistemas de Informação

23.1. Políticas de monitoramento de sistemas da informação
- 23.1.1. Monitoramento de sistemas
- 23.1.2. Métricas
- 23.1.3. Tipos de métricas

23.2. Auditoria e registro em sistemas
- 23.2.1. Auditoria e registro em Windows
- 23.2.2. Auditoria e registro 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. Monitoramento de redes
- 23.4.1. O monitoramento de redes em sistemas de controle
- 23.4.2. Ferramentas de monitoramento para sistemas de controle

23.5. Nagios. Sistema de monitoramento de redes
- 23.5.1. Nagios
- 23.5.2. Funcionamento do Nagios
- 23.5.3. Instalação do Nagios

23.6. Zabbix. Sistema de monitoramento de redes
- 23.6.1. Zabbix
- 23.6.2. Funcionamento do Zabbix
- 23.6.3. Instalação do Zabbix

23.7. Cacti. Sistema de monitoramento de redes
- 23.7.1. Cacti
- 23.7.2. Funcionamento de Cacti
- 23.7.3. Instalação de Cacti

23.8. Pandora. Sistema de monitoramento de redes
- 23.8.1. Pandora
- 23.8.2. Funcionamento de Pandora
- 23.8.3. Instalação de Pandora

23.9. SolarWinds. Sistema de monitoramento de redes
- 23.9.1. SolarWinds
- 23.9.2. Funcionamento do SolarWinds
- 23.9.3. Instalação de SolarWinds

23.10. Regulamento sobre monitoramento
- 23.10.1. Controles CIS sobre auditoria e registro
- 23.10.2. NIST 800-123 (EUA)

Módulo 24. Segurança em comunicações de dispositivos Iot

24.1. Da telemetria ao IoT
- 24.1.1. Telemetria
- 24.1.2. Conectividade 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. Vulnerabilidades de segurança do IoT
- 24.3.1. Dispositivos IoT
- 24.3.2. Dispositivos IoT Casos de uso
- 24.3.3. Dispositivos IoT Vulnerabilidades

24.4. Conectividade IoT
- 24.4.1. Redes PAN, LAN, WAN
- 24.4.2. Tecnologias sem fio não IoT
- 24.4.3. Tecnologias sem fio LPWAN

24.5. Tecnologias LPWAN
- 24.5.1. O triângulo de ferro das redes LPWAN
- 24.5.2. Bandas de frequência livres vs. Bandas licenciadas
- 24.5.3. Opções de tecnologia LPWAN

24.6. Tecnologia LoRaWAN
- 24.6.1. Tecnologia LoRaWAN
- 24.6.2. Casos de uso LoRaWAN Ecossistema
- 24.6.3. Segurança em LoRaWAN

24.7. Tecnologia Sigfox
- 24.7.1. Tecnologia Sigfox
- 24.7.2. Casos de uso Sigfox Ecossistema
- 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 uso celular IoT Ecossistema
- 24.8.3. Segurança em celular IoT

24.9. Tecnologia WiSUN
- 24.9.1. Tecnologia WiSUN
- 24.9.2. Casos de uso WiSUN Ecossistema
- 24.9.3. Segurança em WiSUN

24.10. Outras tecnologias IoT
- 24.10.1. Outras tecnologias IoT
- 24.10.2. Casos de uso e ecossistema de outras tecnologias IoT
- 24.10.3. Segurança em outras tecnologias IoT

Módulo 25. Plano de continuidade de negócio associado à segurança

25.1. Plano continuidade de negócio
- 25.1.1. Os planos de continuidade de negócio (PCN)
- 25.1.2. Plano de continuidade de negócio(PCN) Aspectos fundamentais
- 25.1.3. Plano de Continuidade de Negócio (PCN) para a avaliação da empresa

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

25.4. Gestão de riscos associado ao PCN
- 25.4.1. Análise de impacto nos negócios
- 25.4.2. Benefícios da implantação 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 terapia Contingência
- 25.5.4. Fase 4: Testes, 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. Entregáveis Criação de um plano

25.7. Fase de determinação da estratégia de continuidade em um PCN
- 25.7.1. Funções na fase de determinação da estratégia
- 25.7.2. Tarefas na fase de determinação da estratégia
- 25.7.3. Entregáveis

25.8. Fase de resposta a contingências em um PCN
- 25.8.1. Funções na fase resposta
- 25.8.2. Tarefas nesta fase
- 25.8.3. Entregáveis

25.9. Fase de teste, manutenção e revisão de um PCN
- 25.9.1. Funções na fase de teste, manutenção e revisão
- 25.9.2. Tarefas na fase de teste, manutenção e revisão
- 25.9.3. Entregáveis

25.10. Normas ISO associadas ao planejamento de continuidade do negócio (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 Prática de Recuperação de Desastres de Segurança

26.1. DRP. Plano de recuperação em caso 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. Design da estratégia de recuperação
- 26.2.3. Atribuição de funções 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. Estabelecendo os tipos específicos de DRP necessários
- 26.2.7. Realização de um plano de capacitação, conscientização 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. Design de uma Estratégia de DRP (Recuperação de Desastres)
- 26.4.1. Estratégia de recuperação em caso de desastres
- 26.4.2. Orçamentos
- 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 da informação
- 26.5.1. Planejamento da continuidade
- 26.5.2. Implantação da continuidade
- 26.5.3. Verificação da avaliação da continuidade

26.6. Escopo de um BCP (Plano de Continuidade Empresarial)
- 26.6.1. Determinação dos processos mais críticos
- 26.6.2. Abordagem por ativo
- 26.6.3. Abordagem por processo

26.7. Implementação de processos comerciais seguros
- 26.7.1. Atividades Prioritárias
- 26.7.2. Tempos ideais de recuperação
- 26.7.3. Estratégias de sobrevivência

26.8. Análise da organização
- 26.8.1. Obtenção da informação
- 26.8.2. Análise de impacto nos negócios (BIA)
- 26.8.3. Análise de riscos na organização

26.9. Resposta à terapia Contingência
- 26.9.1. Plano de crises
- 26.9.2. Planos operacionais de recuperação do ambiente
- 26.9.3. Procedimentos técnicos de trabalho ou incidentes

26.10. Norma Internacional ISO 27031 BCP
- 26.10.1. Objetivos
- 26.10.2. Termos e definições
- 26.10.3. Operação

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, repartições e recursos

27.2. Controles físicos de entrada
- 27.2.1. Políticas de controle de acesso físico
- 27.2.2. Sistemas de controle de entrada física

27.3. Vulnerabilidades de acesso físico
- 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 da íris e da retina
- 27.4.4. Outros sistemas biométricos fisiológicos

27.5. Sistemas biométricos de comportamento
- 27.5.1. Reconhecimento de assinaturas
- 27.5.2. Reconhecimento do escritor
- 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 suprimentos e segurança de cabeamento
- 27.7.2. Localização dos equipamentos
- 27.7.3. Saída dos equipamentos fora das instalações
- 27.7.4. Equipamentos de informática desacompanhados e uma política transparente de banca

27.8. Proteção ambiental
- 27.8.1. Sistemas de proteção contra incêndios
- 27.8.2. Sistemas de proteção sísmica
- 27.8.3. Sistemas de proteção contra terremotos

27.9. Segurança no centro de processamento de dados
- 27.9.1. Portas de segurança
- 27.9.2. Sistemas de videovigilância (CCTV)
- 27.9.3. Controle de segurança

27.10. Regulamento Internacional de 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 Comunicação Segura na Empresa

28.1. Gestão de segurança nas redes
- 28.1.1. Controle e monitoramento 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 registro
- 28.3.4. Diferenças com TLS 1,2

28.4. Algoritmos criptográficos
- 28.4.1. Algoritmos criptográficos utilizados nas 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 túneis e transporte
- 28.7.1. Comunicações em túneis
- 28.7.2. Comunicações em transporte
- 28.7.3. Implementação de túneis criptografados

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. Teste de integração
- 28.9.2. Teste de sistema criptográfico

28.10. Sistemas criptográficos
- 28.10.1. Vulnerabilidades de sistemas criptográficos
- 28.10.2. Salvaguardas na criptografia

Módulo 29. Aspectos Organizacionais de Política de Segurança da Informação

29.1. Organização interna
- 29.1.1. Atribuição de responsabilidades
- 29.1.2. Segregação de tarefas
- 29.1.3. Contatos 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. Gestão de mídias de armazenamento

29.3. Políticas de segurança nos processos comerciais
- 29.3.1. Análise de processos comerciais vulneráveis
- 29.3.2. Análise de impacto nos negócios
- 29.3.3. Processos de classificação em relação ao impacto nos negócios

29.4. Políticas de segurança ligadas a Recursos Humanos
- 29.4.1. Antes da contratação
- 29.4.2. Durante a contratação
- 29.4.3. Rescisão ou mudança de cargo

29.5. Políticas de segurança na direção
- 29.5.1. Diretrizes da gestão em segurança da informação
- 29.5.2. BIA- Analisando o impacto
- 29.5.3. Plano de recuperação como uma política de segurança

29.6. Aquisição e manutenção de sistemas de informação
- 29.6.1. Requisitos de segurança dos sistemas de Informação
- 29.6.2. Segurança dos dados de desenvolvimento e suporte
- 29.6.3. Dados de prova

29.7. Segurança com fornecedores
- 29.7.1. Segurança informática com fornecedores
- 29.7.2. Gestão da prestação de serviços com garantia
- 29.7.3. Segurança na cadeia de suprimentos

29.8. Segurança operacional
- 29.8.1. Responsabilidade na operação
- 29.8.2. Proteção contra códigos maliciosos
- 29.8.3. Cópias de segurança
- 29.8.4. Registros de atividades e supervisão

29.9. Gestão de segurança e regulamentação
- 29.9.1. Cumprimento dos requisitos legais
- 29.9.2. Revisões na segurança da informação

29.10. Segurança na gestão para a continuidade do negócio
- 29.10.1. Continuidade de segurança da informação
- 29.10.2. Redundâncias

Um plano de estudos completo da TECH lhe ensinará como ser um líder visionário que garante a proteção da organização a longo prazo"

04

Objetivos de ensino

O Advanced Master em Alta Gestão de Cibersegurança (CISO) tem como objetivo capacitar líderes estratégicos capazes de gerenciar a segurança da informação em qualquer tipo de organização. Ao longo do programa, os alunos desenvolverão competências para identificar, avaliar e atenuar os riscos cibernéticos e implementar políticas de segurança eficazes. Além disso, terão uma compreensão aprofundada das tecnologias emergentes e das práticas recomendadas em arquitetura de segurança, garantindo a proteção dos dados e a continuidade dos negócios. O programa também promove uma visão comercial integrada da segurança cibernética, alinhando as iniciativas aos objetivos corporativos e garantindo a conformidade com os padrões internacionais. Os alunos estarão preparados para serem agentes de mudança e promoverem uma cultura organizacional voltada para a proteção digital.

Nessa especialização 100% online, você encontrará o material didático e a pesquisa mais atualizados do cenário universitário"

Objetivos gerais

- Desenvolver líderes estratégicos de segurança cibernética que possam gerenciar a proteção de ativos digitais e infraestruturas de tecnologia de organizações globais
- Integrar a cibersegurança à estratégia de negócios, alinhando as iniciativas de proteção digital com os objetivos gerais da organização
- Capacitar-se na implementação de políticas de segurança cibernética e estruturas regulatórias que garantem a conformidade regulatória e a proteção de informações em ambientes digitais
- Promover a liderança e o gerenciamento de equipes de segurança cibernética, melhorando a capacidade de tomar decisões estratégicas em situações de crise e gerenciar projetos de segurança no nível organizacional

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

Objetivos específicos

Módulo 1. Ciberespionagem e cibersegurança
- Desenvolver as habilidades necessárias para implementar estratégias de inteligência cibernética e segurança cibernética
- Proteger os sistemas de TI contra ameaças cibernéticas por meio da coleta, análise e uso de inteligência digital

Módulo 2. Segurança do Host
- Capacitar na implementação de medidas de segurança em sistemas host
- Garantir a proteção de servidores e dispositivos contra vulnerabilidades,*malware* e acesso não autorizado

Módulo 3. Segurança de rede (perímetro)
- Fornecer o conhecimento necessário para proteger as redes de computadores no nível do perímetro
- Gerenciar ferramentas e técnicas de segurança, como firewalls, VPNs e sistemas de detecção de intrusão

Módulo 4. Segurança para *Smartphones*
- Fornecer uma compreensão abrangente da segurança de dispositivos móveis
- Aprofundar-se na proteção contra ameaças como *malware*, perda de dados e ataques por meio de aplicativos móveis

Módulo 5. Segurança de IoT
- Capacitar-se na implementação de políticas de segurança para dispositivos IoT
- Proteger a infraestrutura e os dados gerados por dispositivos conectados por meio de redes e plataformas de IoT

Módulo 6. Hacking ético
- Desenvolver as habilidades necessárias para realizar testes de penetração e auditorias de segurança usando técnicas de hacking ético
- Ser capaz de identificar vulnerabilidades e evitar ataques

Módulo 7. Engenharia inversa
- Dominar de técnicas de engenharia reversa, permitindo a análise e a compreensão de software e *hardware*
- Identificar possíveis vulnerabilidades e soluções de segurança

Módulo 8. Desenvolvimento seguro
- Ensinar as práticas recomendadas de desenvolvimento seguro de software
- Aplicar princípios de segurança em todo o ciclo de vida do desenvolvimento para minimizar os riscos e as vulnerabilidades dos aplicativos

Módulo 9. Implementação prática de políticas de segurança em software e *hardware*
- Fornecer as habilidades necessárias para projetar e implementar uma segurança robusta de software e hardware
- Garantir a proteção contra ameaças internas e externas

Módulo 10. Análise Forense
- Desenvolver habilidades em análise forense digital
- Analisar a coleta, a preservação e a análise de evidências digitais em casos de incidentes de segurança de computadores

Módulo 11. Segurança no projeto e desenvolvimento de sistemas
- Abordar a integração de medidas de segurança desde as fases de projeto e desenvolvimento dos sistemas de TI
- Garantir a proteção contra possíveis vulnerabilidades desde o início do projeto

Módulo 12. Arquitetura e modelos de segurança da informação
- Fornecer o conhecimento necessário sobre arquiteturas e modelos de segurança da informação
- Projetar e implementar sistemas robustos que protejam os dados e os recursos da organização

Módulo 13. Sistemas de Gestão de Segurança da Informação(SGSI)
- Implementar um sistema de gerenciamento de segurança da informação
- Proteger as informações comerciais de forma eficaz, garantindo a conformidade com os regulamentos e as boas práticas recomendadas

Módulo 14. Gestão da Segurança TI
- Fornecer o conhecimento necessário para gerenciar com eficácia a segurança nas infraestruturas tecnológicas da empresa
- Minimizar os riscos e garantir a continuidade dos negócios

Módulo 15. Políticas de Gestão de Incidentes de Segurança
- Capacitar-se na criação e implementação de políticas eficazes para o gerenciamento de incidentes
- Estabelecer protocolos claros para detecção, análise e resposta a violações de segurança

Módulo 16. Análise de riscos e ambiente de segurança TI
- Fornecer o conhecimento necessário para realizar uma análise de risco do ambiente de TI, identificando ameaças e vulnerabilidades
- Implementar estratégias de atenuação para proteger a infraestrutura tecnológica

Módulo 17. Políticas de Segurança para Análise de Ameaças em Sistemas Informáticos
- Capacitar-se no desenvolvimento de políticas de segurança para identificar, analisar e atenuar as ameaças aos sistemas de computador
- Usar ferramentas e métodos adequados para proteger os ativos digitais da organização

Módulo 18. Implementação Prática de Políticas de Segurança contra Ataques
- Implementar políticas de segurança eficazes contra possíveis ataques
- Garantir a proteção dos sistemas e informações essenciais da organização

Módulo 19. Criptografia em TI
- Ensinar os fundamentos e as aplicações da criptografia no campo da tecnologia da informação
- Implementar algoritmos de criptografia e segurança na transmissão de dados

Módulo 20. Gestão de identidades e acessos em Segurança TI
- Desenvolver as habilidades necessárias para gerenciar a identidade e o acesso nos sistemas de TI
- Estabelecer políticas de autenticação e controle de acesso para proteger os recursos e os dados da organização

Módulo 21. Segurança nas comunicações e operação de software
- Capacitar-se na proteção de comunicações digitais e na implementação de medidas de segurança na operação de software
- Garantir a confidencialidade, a integridade e a disponibilidade das informações

Módulo 22. Segurança em ambientes Cloud
- Implementar políticas de segurança em ambientes de computação em nuvem
- Garantir que os dados e os aplicativos estejam protegidos contra acesso não autorizado e ataques

Módulo 23. Ferramentas de Monitoramento em Políticas de Segurança de Sistemas de Informação
- Capacitar no uso de ferramentas de monitoramento para avaliar a eficácia das políticas de segurança em sistemas de informação
- Aprofundar a detecção precoce de vulnerabilidades e ataques

Módulo 24. Segurança em comunicações de dispositivos Iot
- Desenvolver habilidades na implementação de medidas de segurança para proteger as comunicações entre dispositivos IoT
- Minimizar os riscos associados à troca de dados entre dispositivos conectados

Módulo 25. Plano de continuidade de negócio associado à segurança
- Desenvolver um plano de continuidade de negócios que garanta a proteção e a rápida recuperação dos sistemas
- Estabelecer protocolos para a proteção de dados críticos em caso de incidentes de segurança

Módulo 26. Política Prática de Recuperação de Desastres de Segurança
- Criar políticas de recuperação de desastres
- Garantir 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-se na implementação de políticas de segurança física e ambiental para proteger os recursos físicos da organização
- Garantir o ambiente adequado para a operação segura dos sistemas de tecnologia

Módulo 28. Políticas de Comunicação Segura na Empresa
- Fornecer o conhecimento necessário para desenvolver políticas de comunicações seguras na organização
- Proteger redes e canais de comunicação contra espionagem e vazamento de informações

Módulo 29. Aspectos Organizacionais de Política de Segurança da Informação
- Fornecer as ferramentas necessárias para implementar políticas organizacionais para o gerenciamento da segurança da informação
- Estabelecer funções, responsabilidades e processos adequados para proteger os ativos de informação

05

Oportunidades profissionais

Após a conclusão do Advanced Master em Alta Gestão de Cibersegurança (CISO), os alunos estarão totalmente qualificados para assumir funções importantes na proteção e no gerenciamento da segurança da informação em várias organizações. Além disso, conseguirão liderar estratégias de segurança em empresas multinacionais, gerenciando e atenuando os riscos cibernéticos. Além disso, eles estarão preparados para cargos que exigem habilidades para liderar iniciativas de segurança cibernética e garantir a proteção de ativos digitais em qualquer setor.

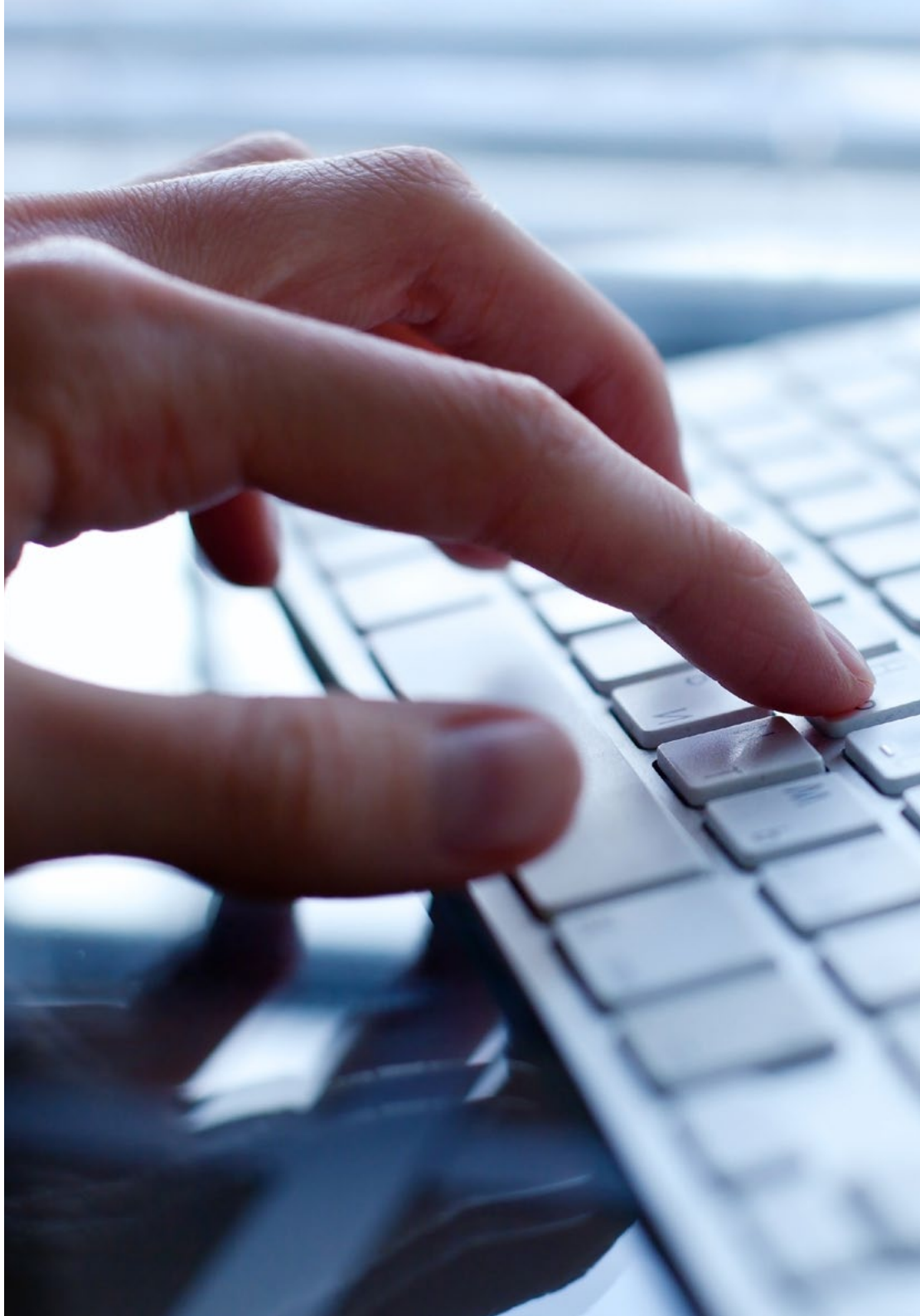
Com esse Advanced Master, você se especializará como um gerente capaz de antecipar riscos e proteger informações críticas"

Perfil do aluno

O aluno do Advanced Master em Alta Gestão de Cibersegurança (CISO) será um líder estratégico com profundo conhecimento de segurança da informação no contexto de organizações globais. Você será capaz de projetar e implementar políticas de segurança avançadas e liderar equipes multidisciplinares. Além disso, você terá sólidas habilidades de gerenciamento e governança, o que lhe permitirá enfrentar os desafios de segurança cibernética em vários setores, garantindo a proteção dos ativos digitais. Essa oportunidade fornecerá as ferramentas necessárias para que você fique por dentro das últimas tendências tecnológicas e se adapte ao cenário digital em rápida mudança.

Prepare-se para ser um dos melhores profissionais, minimizando o impacto dos ataques cibernéticos e voltando ao normal rapidamente.

- **Liderança estratégica e adaptabilidade:** Capacidade de liderar equipes multidisciplinares e gerenciar políticas de segurança, adaptando-se às rápidas mudanças tecnológicas e emergentes na segurança cibernética
- **Gerenciamento de riscos e tomada de decisões informadas:** Capacidade de identificar, avaliar e mitigar riscos cibernéticos, tomando decisões com base em dados e análises detalhados
- **Análise crítica e gerenciamento de incidentes:** Capacidade de identificar vulnerabilidades, gerenciar incidentes de segurança e coordenar a resposta a crises, garantindo a continuidade dos negócios
- **Comunicação eficaz e pensamento estratégico:** Capacidade de comunicar riscos e soluções de forma clara para as diferentes partes interessadas, adotando uma abordagem abrangente e estratégica para a proteção de ativos digitais



Após concluir o Advanced Master, você poderá usar seus conhecimentos e habilidades nos seguintes cargos:

1. **Chief Information Security Officer (CISO):** Líder estratégico responsável pela proteção de informações e segurança cibernética em toda a organização, desenvolvendo políticas e supervisionando a infraestrutura de segurança digital.
2. **Diretor de cibersegurança:** Responsável pelo gerenciamento e supervisão das equipes de segurança de TI, desenvolvendo e implementando estratégias para proteger a infraestrutura tecnológica da empresa
3. **Gerente de segurança de TI:** Responsável por gerenciar e coordenar políticas de segurança digital, supervisionando a proteção de dados e sistemas de TI contra possíveis ameaças
4. **Consultor de cibersegurança:** Especialista em assessorar empresas sobre a melhor forma de implementar e gerenciar políticas de segurança cibernética, ajudando a reduzir os riscos e a cumprir as regulamentações internacionais.
5. **Gerente de Gestão de Riscos de TI:** Responsável por identificar, avaliar e mitigar os riscos cibernéticos que possam afetar a segurança dos sistemas de informação e tecnologia da organização
6. **Chefe de Segurança da Informação:** Líder encarregado de supervisionar e coordenar todas as iniciativas relacionadas à proteção de dados e sistemas de TI na organização.

Você está a um passo de melhorar sua vida profissional com esse Advanced Master que só a TECH pode oferecer”

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

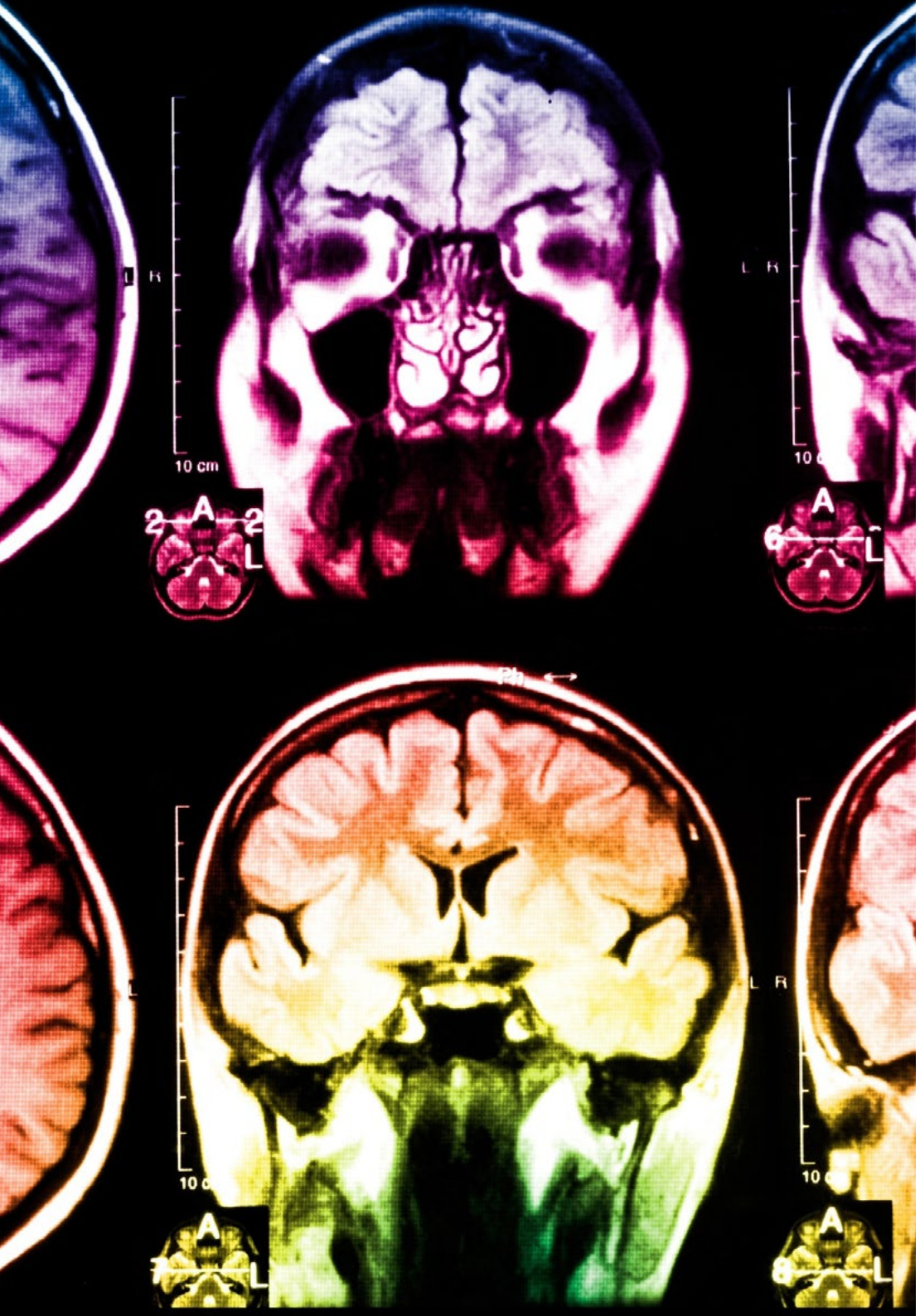
Por outro lado, também para favorecer ao máximo o contato entre mentor e mentorado, é oferecida uma ampla variedade de possibilidades de comunicação, tanto em tempo real quanto em diferido (mensagens internas, fóruns de discussão, serviço telefônico, contato por e-mail com a secretaria técnica, bate-papo,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

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

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

A eficácia do método é justificada por quatro conquistas fundamentais:

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



A metodologia universitária mais bem avaliada por seus alunos

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

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

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

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

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

Material de estudo

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

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

Práticas de aptidões e competências

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

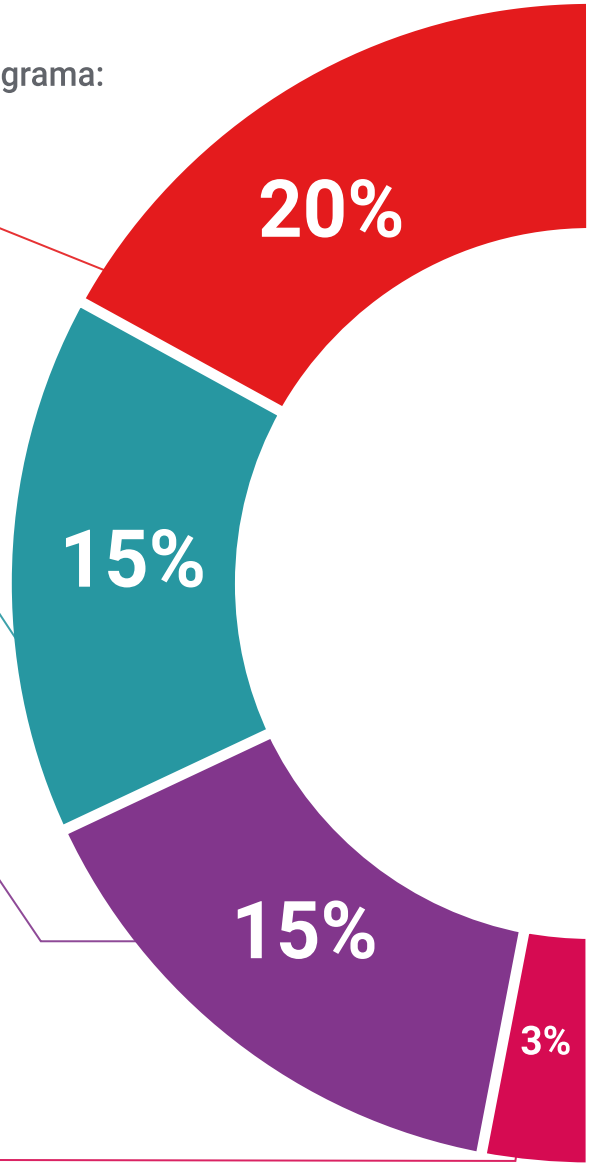
Resumos interativos

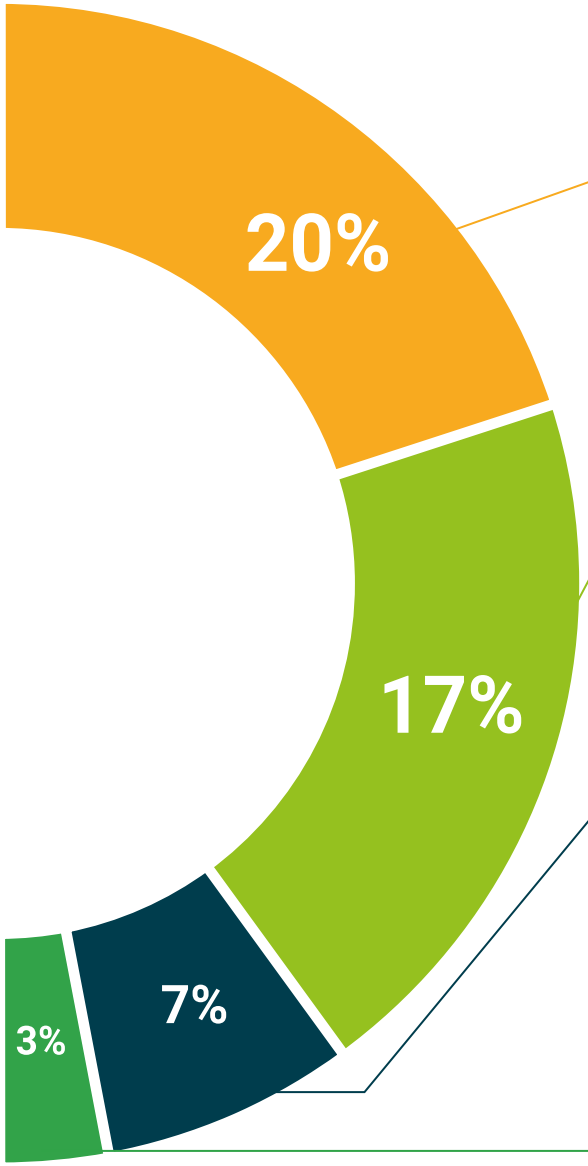
Apresentamos os conteúdos de forma atraente e dinâmica em pílulas multimídia que incluem áudio, vídeos, imagens, diagramas e mapas conceituais com o objetivo de reforçar o conhecimento.

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

Leituras complementares

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





Case Studies

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

Testing & Retesting

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

Masterclasses

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

O *Learning from an expert* fortalece o conhecimento e a memória, e aumenta nossa confiança para tomar decisões difíceis no futuro.

Guias rápidos de ação

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

07

Equipe de professores

Esse Advanced Master em Alta Gestão de Cibersegurança (CISO, Chief Information Security Officer) tem um corpo docente formado por profissionais ativos que conhecem perfeitamente o estado atual dessa área e que, portanto, transferirão ao aluno todas as chaves da cibersegurança atual. Dessa forma, o aluno desse programa tem a garantia de obter os últimos avanços nesse campo, podendo acessá-los graças à prestigiada equipe de professores que a TECH selecionou.

A TECH lhe oferece os diretores e professores mais especializados para que sua abordagem e aprendizado sejam os melhores”

Diretor Internacional Convidado

O Dr. Frederic Lemieux é reconhecido internacionalmente como um especialista inovador e líder inspirador nas áreas de **Inteligência**, **Segurança Nacional, Segurança Interna, Cibersegurança** e **Tecnologias Disruptivas.** Sua dedicação constante e contribuições relevantes em pesquisa e educação o posicionam como uma figura-chave na promoção da segurança e da compreensão das tecnologias emergentes atuais Durante sua carreira profissional, ele conceituou e dirigiu programas acadêmicos de ponta em várias instituições renomadas, incluindo a **Universidade de Montreal**, a **Universidade George Washington** e a **Universidade de Georgetown**.

Ao longo de sua extensa trajetória, publicou vários livros de grande relevância, todos relacionados à **inteligência criminal, ao policiamento, ameaças cibernéticas e segurança internacional.** Além disso, ele contribuiu significativamente para o campo da segurança cibernética, publicando vários artigos em revistas acadêmicas, que examinam o controle do crime durante grandes desastres, combate ao terrorismo, agências de inteligência e cooperação policial. Foi palestrante em várias conferências nacionais e internacionais, estabelecendo-se como uma referência na esfera acadêmica e profissional.

O Dr. Lemieux ocupou cargos editoriais e de avaliação em várias organizações acadêmicas, privadas e governamentais, o que reflete sua influência e compromisso com a excelência em sua área de especialização. Dessa forma, sua prestigiada carreira acadêmica o levou a atuar como Professor de Prática e Diretor do Corpo Docente dos programas MPS em **Inteligência Aplicada, Gerenciamento de Risco de Segurança Cibernética, Gerenciamento de Tecnologia e Gerenciamento de TI**, na **Universidade de Georgetown.**

Dr. Frederic Lemieux

- Diretor do Mestrado em Gestão de Riscos de Segurança Cibernética em Georgetown, Washington, EUA
- Diretor do Mestrado em Gestão de Tecnologia da Universidade de Georgetown
- Diretor do Mestrado em Inteligência Aplicada da Universidade de Georgetown
- Professor de Estágio na Universidade de Georgetown
- Doutor em Criminologia pela Escola de Criminologia da Universidade de Montreal
- Formado em Sociologia com especialização em Psicologia pela Universidade de Laval
- Membro: New Program Roundtable Committee, Universidade de Georgetown

Graças à TECH você será capaz de aprender com os melhores profissionais do mundo"

Direção

Sra. Sonia Fernández Sapena

- Formadora em Segurança Informática e Hacking Ético no Centro de Referência Nacional de Getafe, em Informática e Telecomunicações de Madrid
- Instrutora certificada E-Council
- Instrutora nas seguintes certificações: EXIN Ethical Hacking Foundation e EXIN Cyber & IT Security Foundation. Madri
- Instrutor especializada credenciada pela CAM para os seguintes certificados de profissionalismo: Segurança Informática (IFCT0190), Gerenciamento de Redes de Voz e Dados (IFCM0310), Administração de Redes Departamentais (IFCT0410), Gerenciamento 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
- Formada em Engenharia da Computação pela Universidade de Alcalá de Henares de Madrid
- Mestrado em DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

Sr. Martín Olalla Bonal

- Gerente Sênior de Prática de *Blockchain* no EY
- Especialista técnico cliente *Blockchain* para IBM
- Diretor de Arquitetura da Blocknitive
- Coordenador de equipe em bancos de dados distribuídos não relacionais para a WedoIT, uma subsidiária da IBM
- Arquiteto de infraestruturas na Bankia
- Responsável pelo Departamento de Maquetação da T-Systems
- Coordenador de Departamento para Bing Data España SL.

Professores

Sra. Victoria Alicia Marcos Sbarbaro

- Desenvolvedora de aplicativos móveis Android nativo na B60. UK
- Analista Programadora para a gestão, coordenação e documentação de um ambiente de alarme de segurança virtualizado
- Analista programadora de aplicações Java para ATMs
- Profissional de Desenvolvimento de *Software* para validação de assinatura e aplicação de gerenciamento de documentos no local do cliente
- Técnico de Sistemas para a migração de equipamentos e para o gerenciamento, manutenção e treinamento de PDAs móveis e treinamento de dispositivos móveis PDA no cliente
- Engenheiro Técnico de Informática de Sistemas pela Universidade Oberta de Catalunha
- Mestrado em Segurança Informática e Hacking Ético Oficial EC- Conselho e CompTIA pela Escola Profissional de Novas Tecnologias CICE

Sr. Alejandro Entrenas

- Chefe de projetos na Cibersegurança. Entelgy Innotec Security
- Consultor de cibersegurança. Entelgy
- Analista de segurança da informação. Innovery Espanha
- Analista em segurança da informação. Atos
- Formado em Engenharia Técnica em Sistemas de Computação pela Universidade de Córdoba
- Mestrado em Gestão de Segurança da Informação na Universidade Politécnica de Madrid
- Certificado ITIL v4 Foundation em Gerenciamento de Serviços de TI. ITIL Certified
- IBM Security QRadar SIEM 7.1 Advanced. Avnet
- IBM Security QRadar SIEM 7.1 Foundations. Avnet

Sr. José Francisco Catalá Barba

- Técnico eletrônico. Especialista em segurança cibernética
- Desenvolvedor de aplicativos móveis
- Técnico eletrônico em Comando Intermediário no Ministério da Defesa da Espanha.
- Técnico em eletrônica na fábrica da Ford Sita em Valência

Sr. Jon Peralta Alonso

- Consultor Sênior de Proteção de Dados e Cibersegurança Altia
- Advogado / Assessor jurídico da Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- Consultor jurídico/estagiário em uma empresa profissional: Oscar Padura
- Formado em Direito pela Universidade Pública do País Basco
- Mestrado em Proteção de Dados Delegado pela EIS Innovative School
- Mestrado em Direito pela Universidade Pública do País Basco
- Mestrado em Prática de Litígio Civil pela Universidad Internacional Isabel I de Castela
- Professor do Mestrado em Proteção de Dados Pessoais, Segurança Cibernética e Direito de TIC

Sr. Félix Gonzalo Alonso

- CEO e fundador da Smart REM Solutions
- Diretor de Engenharia de Risco e Inovação da Dynargy
- Diretor administrativo e sócio fundador da consultoria de tecnologia Risknova
- Mestrado em Gestão de Seguros pelo Instituto de Colaboração entre Empresas de Seguros
- Graduação em Engenharia Industrial Técnica, com especialização em Eletrônica Industrial pela Universidade Pontifícia de Comillas

Sr. Álvaro Jiménez Ramos
- Analista de segurança cibernética
- Analista Sênior de Segurança no The Workshop
- Analista de Cibersegurança L1 na Axians
- Analista de Cibersegurança L2 na Axians
- Analista de Cibersegurança na SACYR S.A.
- Formada em Engenharia Telemática pela Universidade Politécnica de Madri
- Mestrado em Segurança Cibernética e Hacking Ético pela CICE
- Curso Avançado em Segurança Cibernética pela Deusto Formación

Sr. Jesús Serrano Redondo
- Desenvolvedor da Web e técnico de segurança cibernética
- Desenvolvedor Web em Roams, Palencia
- Desenvolvedor FrontEnd na Telefónica, Madri
- Desenvolvedor FrontEnd na Best Pro Consulting SL, Madri
- Instalador de equipamentos e serviços de telecomunicações no Grupo Zener, Castilla y León
- Instalador de equipamentos e serviços de telecomunicações na Lican Comunicaciones SL, Castilla y León
- Certificado em Segurança de Computadores pelo CFTIC Getafe, Madri
- Técnico Superior em Telecomunicações e Sistemas de Computação pelo IES Trinidad Arroyo, Palencia
- Técnico Superior em Instalações Eletrotécnicas de Média e Baixa Tensão pelo IES Trinidad Arroyo, Palencia
- Formação em engenharia reversa, estenografia e criptografia pela Incibe Hacker Academy

Sr. Javier Nogales Ávila
- Enterprise Cloud e Sourcing Senior Consultant em Quint
- Cloud e Technology Consultant na Indra
- Associate Technology Consultant na Accenture
- Formado em Engenharia de Organização Industrial pela Universidade de Jaén
- MBA em Administração e Gerenciamento de Negócios pela ThePower Business School

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

Sr. Juan Manuel Rodrigo Estébanez
- Cofundador da Ismet Tech
- Gerente de segurança da informação no Ecix Group
- *Operational Security Officer* em Atos IT Solutions and Services A/S
- Professor de Gestão de Cibersegurança em estudos universitários
- Formado em Engenharia pela Universidade de Valladolid
- Mestrado em Sistemas de Gestão Integrada pela Universidade CEU San Pablo

Sr. Jorge del Valle Arias

- Engenheiro de telecomunicações com experiência em desenvolvimento de negócios
- Smart City Solutions & Software Business Development Manager Espanha. Itron, Inc
- Consultor IoT
- Diretor interino de negócios de IoT. TCOMET
- Responsável pela unidade de negócios de IoT e Indústria 4.0. Diode Espanha
- Gerente de Vendas de Área para IoT e Telecomunicações. Soluções Aicox
- Diretor Técnico (CTO) e Gerente de Desenvolvimento de Negócios. Consultoria TELYC
- Fundador e CEO da Sensor Intelligence
- Chefe de Operações e Projetos. Codio
- Diretor de Operações da Codium Networks
- Engenheiro-chefe de design de hardware e firmware. AITEMIN
- Chefe regional de planejamento e otimização de RF - Rede LMDS de 3,5 GHz. Clearwire
- Engenheiro de Telecomunicações da Universidade Politécnica de Madrid
- Executive MBA pela Escola Internacional Graduate School of La Salle, em Madrid
- Mestrado em Energias Renováveis. CEPYME

Sr. Juan Luis Gozalo Fernández

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

Sra. Lorena Jurado Jabonero

- Responsável pela Segurança da Informação (CISO) no Grupo Pascual
- Cybersecurity Manager na KPMG. Espanha
- Consultora de controle e gerenciamento de projetos de infraestrutura e processos de TI no Bankia
- Engenheira de ferramentas operacionais na Dalkia
- Desenvolvedora no Grupo Banco Popular
- Desenvolvedora de aplicativos da Universidade Politécnica de Madri.
- Formada em Engenharia da Computação pela Universidade Alfonso X el Sabio.
- Engenheira Técnico em Gestão de Informática pela Universidade Politécnica de Madrid
- Certified Data Privacy Solutions Engineer (CDPSE) pela ISACA

Sr. Octavio Ortega Esteban

- Especialista em marketing e desenvolvimento web
- Programador de aplicativos de computador e desenvolvedor Web *Freelance*
- *Chief Operating Officer* na Smallsquid SL
- Administrador de e-commerce da Ortega y Serrano
- Professor em cursos de Certificado de Profissionalismo em Computação e Comunicações
- Professor de cursos de segurança de computadores
- Formado em Psicologia pela Universidade Aberta da Catalunha
- Técnico Superior Universitário em Análise, Design e Soluções de *Software*
- Técnico Superior Universitário em Programação Avançada

Sr. Mario Embid Ruiz

- Advogado especialista em TIC e proteção de dados na Martínez-Echevarría Abogados
- Responsável legal pela Branddocs SL
- Analista de Risco do Segmento PME do BBVA
- Professor em estudos universitários de pós-graduação relacionados ao Direito
- Formado em Direito pela Universidad Rey Juan Carlos
- Formado em Administração e Gerenciamento de Negócios pela Universidad Rey Juan Carlos
- Mestrado em Novas Tecnologias, Internet e Direito Audiovisual pelo Centro de Estudos Universitários Villanueva

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

08

Certificação

O Advanced Master em Alta Gestão de Cibersegurança (CISO, Chief Information Security Officer) garante, além da capacitação mais rigorosa e atualizada, o acesso a um título de Advanced Master emitido pela TECH Universidade Tecnológica.

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

Este **Advanced Master em Alta Gestão de Cibersegurança (CISO, Chief Information Security Officer)** conta com o conteúdo mais completo e atualizado do mercado.

Uma vez aprovadas as avaliações, o aluno receberá por correio o certificado* correspondente ao título de **Advanced Master** emitido pela **TECH Universidade Tecnológica.**

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

Título: **Advanced Master em Alta Gestão de Cibersegurança (CISO, Chief Information Security Officer)**

Modalidade: **online**

Duração: **2 anos**


tech universidade tecnológica

Outorga o presente

CERTIFICADO

a

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

por ter concluído e aprovado com sucesso o programa de

ADVANCED MASTER

em

Alta Gestão de Cibersegurança (CISO, Chief Information Security Officer)

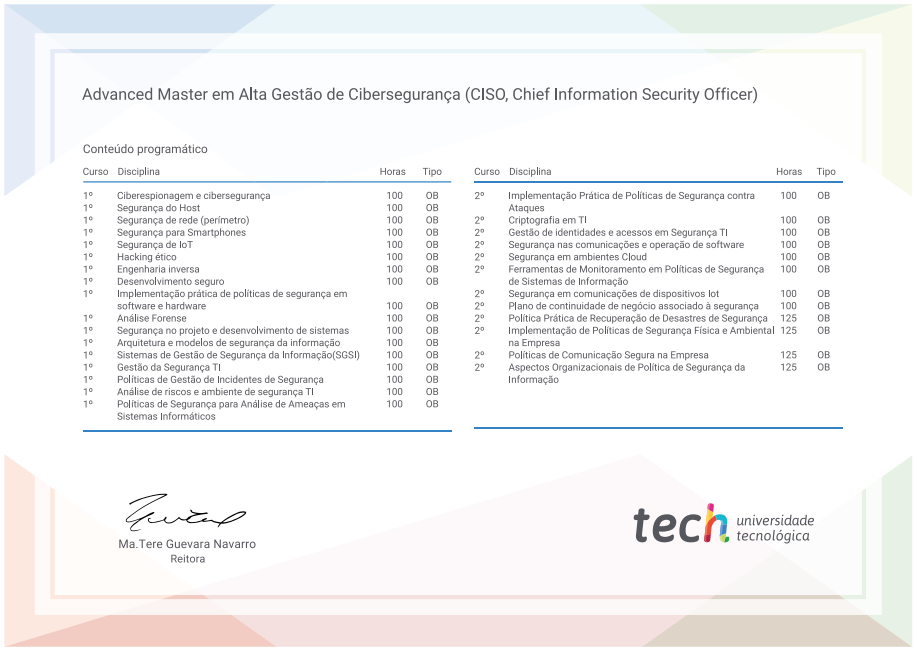
Este é um curso próprio desta Universidade, com duração de 3.000 horas, com data de início dd/mm/aaaa e data final dd/mm/aaaaa.

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

Em 17 de junho de 2020

Ma.Tere Guevara Navarro
Reitora

código único TECH: AFWOR23S techtitute.com/titulos


Advanced Master em Alta Gestão de Cibersegurança (CISO, Chief Information Security Officer)

Conteúdo programático

Curso	Disciplina	Horas	Tipo
1º	Ciberespionagem e cibersegurança	100	OB
1º	Segurança do Host	100	OB
1º	Segurança de rede (perímetro)	100	OB
1º	Segurança para Smartphones	100	OB
1º	Segurança de IoT	100	OB
1º	Hacking ético	100	OB
1º	Engenharia inversa	100	OB
1º	Desenvolvimento seguro	100	OB
1º	Implementação prática de políticas de segurança em software e hardware	100	OB
1º	Análise Forense	100	OB
1º	Segurança no projeto e desenvolvimento de sistemas	100	OB
1º	Arquitetura e modelos de segurança da informação	100	OB
1º	Sistemas de Gestão de Segurança da Informação(SGSI)	100	OB
1º	Gestão da Segurança TI	100	OB
1º	Políticas de Gestão de Incidentes de Segurança	100	OB
1º	Análise de riscos e ambiente de segurança TI	100	OB
1º	Políticas de Segurança para Análise de Ameaças em Sistemas Informáticos	100	OB

Curso	Disciplina	Horas	Tipo
2º	Implementação Prática de Políticas de Segurança contra Ataques	100	OB
2º	Criptografia em TI	100	OB
2º	Gestão de identidades e acessos em Segurança TI	100	OB
2º	Segurança nas comunicações e operação de software	100	OB
2º	Segurança em ambientes Cloud	100	OB
2º	Ferramentas de Monitoramento em Políticas de Segurança de Sistemas de Informação	100	OB
2º	Segurança em comunicações de dispositivos Iot	100	OB
2º	Plano de continuidade de negócio associado à segurança	100	OB
2º	Política Prática de Recuperação de Desastres de Segurança	125	OB
2º	Implementação de Políticas de Segurança Física e Ambiental na Empresa	125	OB
2º	Políticas de Comunicação Segura na Empresa	125	OB
2º	Aspectos Organizacionais de Política de Segurança da Informação	125	OB

Ma.Tere Guevara Navarro
Reitora

tech universidade tecnológica

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

tech universidade tecnológica

Advanced Master
Alta Gestão de Cibersegurança (CISO, Chief Information Security Officer)

- Modalidade: **online**
- Duração: **2 anos**
- Certificado: **TECH Universidade Tecnológica**
- Horário: **no seu próprio ritmo**
- Provas: **online**

Advanced Master

Alta Gestão de Cibersegurança (CISO, Chief Information Security Officer)

tech universidade tecnológica