Advanced Master

Secure Information Management

tech universidade tecnológica

tech universidade tecnológica

Advanced Master
Secure Information Management

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

Acesso ao site: www.techtitute.com/br/informatica/advanced-master/advanced-master-secure-information-management

Índice

01

Apresentação do programa

Na era digital de hoje, as atividades em vários campos são gerenciadas de forma integrada pela Internet. O entretenimento, o trabalho e a comunicação com amigos e familiares dependem cada vez mais de ferramentas e recursos online. Enormes quantidades de informações são transferidas diariamente, desde dados simples em conversas de mídia social e aplicativos de mensagens até informações pessoais e profissionais confidenciais hospedadas em plataformas bancárias ou comerciais. Esse cenário exige especialistas capazes de lidar e proteger informações em vários contextos, priorizando sua segurança. É por isso que a TECH criou este programa em Engenharia de Software, focado na formação de profissionais com as habilidades necessárias para gerenciar e proteger informações de forma eficaz, abordando os desafios digitais atuais e contribuindo para criar ambientes tecnológicos mais seguros e confiáveis.

A proteção dos dados é fundamental diante das ameaças constantes. Você pode ser o responsável por guardar essas informações valiosas"

A cada segundo, milhares de dados são gerados, compartilhados e armazenados no ambiente digital. Desde a realização de pagamentos online e o acesso a serviços educacionais até a coordenação de atividades comerciais ou a proteção de identidades digitais, a tecnologia tornou-se um pilar essencial que transforma continuamente a maneira como vivemos e trabalhamos. Essas interações geram e transferem grandes quantidades de dados a cada instante, desde informações pessoais até arquivos confidenciais relacionados a empresas e instituições. Esse fluxo constante de dados destaca a necessidade de um tratamento adequado para garantir sua segurança e privacidade.

Gerenciar e proteger esses dados não é uma tarefa simples, pois exige uma combinação de conhecimentos altamente especializados em áreas como cibersegurança e gerenciamento de informações. Essas disciplinas, embora distintas, devem ser integradas para enfrentar os complexos desafios do ambiente digital atual. Nesse contexto, o Advanced Master em Secure Information Management representa uma oportunidade única para engenheiros e profissionais de TI interessados em adquirir uma visão abrangente que lhes permitirá dominar as duas áreas e se posicionar como líderes em um setor em constante crescimento.

Muitas empresas e instituições se deparam com a necessidade de proteger dados críticos e altamente confidenciais, mas não possuem o conhecimento necessário para garantir o gerenciamento, a preservação e a vigilância eficazes de suas informações digitais. Para atender a essa demanda, a TECH elaborou um programa que combina os melhores conteúdos com uma equipe de professores com reconhecida experiência profissional. Essa abordagem garante que os alunos adquiram as ferramentas e os conhecimentos necessários para se destacar no mercado de trabalho e acessar posições estratégicas em organizações que buscam fortalecer sua segurança da informação.

Este **Advanced Master em Secure Information Management** conta com o programa educacional mais completo e atualizado do mercado. Suas principais características são:

- O desenvolvimento de casos práticos apresentados por especialistas em Secure Information Management
- 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 no gerenciamento do Secure Information Management
- 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

Adquira as habilidades necessárias para proteger e gerenciar dados de forma eficaz em um ambiente digital competitivo"

Descubra a metodologia educacional mais inovadora projetada pela TECH para garantir um aprendizado imersivo e contextualizado.

Consolide seus conhecimentos teóricos com os inúmeros recursos práticos incluídos neste Advanced Master em Secure Information Management”

Acesse um programa 100% online que permite que você estude no seu próprio ritmo, a qualquer momento e de qualquer lugar do mundo.

Seu corpo docente inclui profissionais da área de finanças, que trazem sua experiência profissional para este programa, além de especialistas reconhecidos de empresas líderes e universidades de prestígio.

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.

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

Os materiais didáticos que compõem esse Advanced Master em Secure Information Management foram desenvolvidos por uma equipe de especialistas em cibersegurança e gerenciamento de dados. Dessa forma, o programa de estudos se aprofunda nas principais ameaças digitais e nas metodologias mais avançadas para a proteção e o gerenciamento de informações. Isso permitirá que os alunos identifiquem riscos específicos e desenvolvam soluções eficazes para garantir a segurança dos dados em vários ambientes profissionais. A agenda também aborda as ferramentas mais inovadoras do setor, impulsionando estratégias para proteger os ativos digitais das organizações.

Você contribuirá para a proteção de dados confidenciais e para a criação de sistemas seguros que garantam a continuidade operacional de empresas e instituições”

Módulo 1. Análise de dados na organização empresarial

1.1. Análise de Negócios
- 1.1.1. Análise de Negócios
- 1.1.2. Estrutura de dados
- 1.1.3. Fases e elementos

1.2. Análise de dados nas empresas
- 1.2.1. Paineis de controle e kpi' s por departamentos
- 1.2.2. Relatórios operacionais, táticos e estratégicos
- 1.2.3. Análise de dados aplicada a cada departamento
  - 1.2.3.1. Marketing e comunicação
  - 1.2.3.2. Comercial
  - 1.2.3.3. Atendimento ao cliente
  - 1.2.3.4. Compras
  - 1.2.3.5. Administração
  - 1.2.3.6. RH
  - 1.2.3.7. Produção
  - 1.2.3.8. TI

1.3. Marketing e comunicação
- 1.3.1. Kpi' s à medida, aplicações e benefícios
- 1.3.2. Sistemas de marketing e *data warehouse*
- 1.3.3. Implementação de uma estrutura analítica de dados em Marketing
- 1.3.4. Plano de marketing e comunicação
- 1.3.5. Estratégias, previsões e gestão de campanhas

1.4. Comercial e vendas
- 1.4.1. Contribuições de análise de dados na área comercial
- 1.4.2. Necessidades do Departamento de Vendas
- 1.4.3. Pesquisa de mercado

1.5. Atendimento ao cliente
- 1.5.1. Fidelização
- 1.5.2. Qualidade pessoal e inteligência emocional
- 1.5.3. Satisfação do cliente

1.6. Compras
- 1.6.1. Análise de dados para pesquisa de mercado
- 1.6.2. Análise de dados para estudos de concorrência
- 1.6.3. Outras aplicações

1.7. Administração
- 1.7.1. Necessidades do Departamento de Administração
- 1.7.2. *Data Warehouse* e análise de risco financeiro
- 1.7.3. *Data Warehouse* e análise de risco de crédito

1.8. Recursos humanos
- 1.8.1. RH e os benefícios da análise de dados
- 1.8.2. Ferramentas analíticas de dados no departamento de RH
- 1.8.3. Aplicações analíticas de dados no departamento de RH

1.9. Produção
- 1.9.1. Análise de dados em um departamento de produção
- 1.9.2. Aplicações
- 1.9.3. Benefícios

1.10. TI
- 1.10.1. Departamento de TI
- 1.10.2. Análise de dados e transformação digital
- 1.10.3. Inovação e produtividade

Módulo 2. Gestão, manipulação de dados e informações para a ciência dos dados

2.1. Estatísticas Variáveis, índices e ratios
- 2.1.1. Estatísticas
- 2.1.2. Dimensões estatísticas
- 2.1.3. Variáveis, índices e ratios

2.2. Tipologia de dados
- 2.2.1. Qualitativos
- 2.2.2. Quantitativos
- 2.2.3. Caracterização e categorias

2.3. Conhecimento de dados resultantes de medições
- 2.3.1. Medidas de centralização
- 2.3.2. Medidas de dispersão
- 2.3.3. Correlação

2.4. Conhecimento de dados provenientes de gráficos
- 2.4.1. Visualização de acordo com o tipo de dados
- 2.4.2. Interpretação de informações gráficas
- 2.4.3. Customização de gráficos com R

2.5. Probabilidade
- 2.5.1. Probabilidade
- 2.5.2. Função de probabilidade
- 2.5.3. Distribuição

2.6. Coleta de dados
- 2.6.1. Metodologia de coleta
- 2.6.2. Ferramentas de coleta
- 2.6.3. Canais de coleta

2.7. Limpeza de dados
- 2.7.1. Fases da limpeza de dados
- 2.7.2. Qualidade dos dados
- 2.7.3. Manipulação de dados (com R)

2.8. Análise de dados, interpretação e avaliação dos resultados
- 2.8.1. Medidas estatísticas
- 2.8.2. Índices de relação
- 2.8.3. Mineração de dados

2.9. Armazém de dados (*datawarehouse*)
- 2.9.1. Elementos
- 2.9.2. Desenho

2.10. Disponibilidade de dados
- 2.10.1. Acesso
- 2.10.2. Utilidade
- 2.10.3. Segurança

Módulo 3. Dispositivos e plataformas IoT como base para a ciência dos dados

3.1. *Internet of Things*
- 3.1.1. Internet do futuro, *Internet of Things*
- 3.1.2. O consórcio da internet industrial

3.2. Arquitetura de referência
- 3.2.1. A Arquitetura de referência
- 3.2.2. Camadas
- 3.2.3. Componentes

3.3. Sensores e dispositivos IoT
- 3.3.1. Principais componentes
- 3.3.2. Sensores e atuadores

3.4. Comunicações e protocolos
- 3.4.1. Protocolos. Modelo OSI
- 3.4.2. Tecnologias de comunicação

3.5. Plataformas *cloud* para IoT e IIoT
- 3.5.1. Plataformas de propósito geral
- 3.5.2. Plataformas Industriais
- 3.5.3. Plataformas de código aberto

3.6. Gestão de dados em plataformas IoT
- 3.6.1. Mecanismos de gestão de dados Dados abertos
- 3.6.2. Intercâmbio e visualização de dados

3.7. Segurança de IoT
- 3.7.1. Requisitos e áreas de segurança
- 3.7.2. Estratégias de segurança IIoT

3.8. Aplicações de IoT
- 3.8.1. Cidades inteligentes
- 3.8.2. Saúde e condicionamento físico
- 3.8.3. Lar inteligente (Smart Home)
- 3.8.4. Outras aplicações

3.9. Aplicações IIoT
- 3.9.1. Fabricação
- 3.9.2. Transporte
- 3.9.3. Energia
- 3.9.4. Agricultura e pecuária
- 3.9.5. Outros setores

3.10. Indústria 4.0.
- 3.10.1. IoRT *(Internet of Robotics Things)*
- 3.10.2. Fabricação aditiva 3D
- 3.10.3. *Big Data Analytics*

Módulo 4. Representação gráfica para análise de dados

4.1. Análise exploratória
- 4.1.1. Representação para análise de informações
- 4.1.2. O valor da representação gráfica
- 4.1.3. Novos paradigmas da representação gráfica

4.2. Otimização para a ciência de dados
- 4.2.1. Gama cromática e desenho
- 4.2.2. Gestalt na representação gráfica
- 4.2.3. Erros a serem evitados e recomendações

4.3. Fontes de dados básicos
- 4.3.1. Para representação de qualidade
- 4.3.2. Para representação de Quantidade
- 4.3.3. Para representação de tempo

4.4. Fontes de dados complexos
- 4.4.1. Arquivos, listas e BBDD
- 4.4.2. Dados abertos
- 4.4.3. Dados de geração contínua

4.5. Tipos de gráficos
- 4.5.1. Representações básicas
- 4.5.2. Representação em bloco
- 4.5.3. Representação para análise de dispersão
- 4.5.4. Representações circulares
- 4.5.5. Representações de bolhas
- 4.5.6. Representações geográficas

4.6. Tipos de visualização
- 4.6.1. Comparativo e relacional
- 4.6.2. Distribuição
- 4.6.3. Hierárquica

4.7. Desenho de relatório com representação gráfica
- 4.7.1. Aplicação de gráficos em relatórios de marketing
- 4.7.2. Aplicação de gráficos em paineis de Avaliação e kpi' s
- 4.7.3. Aplicação de gráficos em planos estratégicos
- 4.7.4. Outros usos: ciência, saúde, negócios

4.8. Narrativa gráfica
- 4.8.1. Narrativa gráfica
- 4.8.2. Evolução
- 4.8.3. Utilidade

4.9. Ferramentas orientadas à visualização
- 4.9.1. Ferramentas avançadas
- 4.9.2. Software online
- 4.9.3. *Open Source*

4.10. Novas tecnologias na visualização de dados
- 4.10.1. Sistemas para virtualização da realidade
- 4.10.2. Sistemas para o aumento e melhoria da realidade
- 4.10.3. Sistemas inteligentes

Módulo 5. Ferramentas da ciência de dados

5.1. Ciência de dados
- 5.1.1. Ciência de dados
- 5.1.2. Ferramentas avançadas para o cientista de dados

5.2. Dados, informações e conhecimentos
- 5.2.1. Dados, informações e conhecimentos
- 5.2.2. Tipos de dados
- 5.2.3. Fontes de dados

5.3. De dados a informações
- 5.3.1. Análise de dados
- 5.3.2. Tipos de análise
- 5.3.3. Extração de informações de um *Dataset*

5.4. Extração de informações através da visualização
- 5.4.1. A visualização como ferramenta de análise
- 5.4.2. Métodos de visualização
- 5.4.3. Visualização de um conjunto de dados

5.5. Qualidade dos dados
- 5.5.1. Dados de qualidade
- 5.5.2. Limpeza de dados
- 5.5.3. Pré-processamento básico de dados

5.6. *Dataset*
- 5.6.1. Enriquecimento do *dataset*
- 5.6.2. A maldição da dimensionalidade
- 5.6.3. Modificação de nosso conjunto de dados

5.7. Desequilíbrio
- 5.7.1. Desequilíbrio de classes
- 5.7.2. Técnicas de mitigação do desequilíbrio
- 5.7.3. Equilíbrio de um *dataset*

5.8. Modelos não supervisionados
- 5.8.1. Modelo não supervisionado
- 5.8.2. Métodos
- 5.8.3. Classificação com modelos não supervisionados

5.9. Modelos supervisionados
- 5.9.1. Modelo supervisionado
- 5.9.2. Métodos
- 5.9.3. Classificação com modelos supervisionados

5.10. Ferramentas e práticas recomendadas
- 5.9.1. Práticas recomendadas para um cientista de dados
- 5.10.2. O melhor modelo
- 5.10.3. Ferramentas úteis

Módulo 6. Mineração de dados - seleção, pré-processamento e transformação

6.1. Inferência estatística
- 6.1.1. Estatística descritiva vs. Inferência estatística
- 6.1.2. Procedimentos paramétricos
- 6.1.3. Procedimentos paramétricos

6.2. Análise exploratória
- 6.2.1. Análise descritiva
- 6.2.2. Visualização
- 6.2.3. Preparação dos dados

6.3. Preparação dos dados
- 6.3.1. Integração e limpeza de dados
- 6.3.2. Normalização de dados
- 6.3.3. Transformando atributos

6.4. Os Valores Perdidos
- 6.4.1. Tratamento de valores perdidos
- 6.4.2. Métodos de imputação de máxima verosimilhança
- 6.4.3. Imputação de valores perdidos utilizando a aprendizado de máquinas

6.5. O ruído nos dados
- 6.5.1. Classes de ruído e seus atributos
- 6.5.2. Filtragem de ruídos
- 6.5.3. O efeito do ruído

6.6. A maldição da dimensionalidade
- 6.6.1. *Oversampling*
- 6.6.2. *Undersampling*
- 6.6.3. Redução de dados multidimensionais

6.7. De atributos contínuos a discretos
- 6.7.1. Dados contínuos versus discretos
- 6.7.2. Processo de discretização

6.8. Os dados
- 6.8.1. Seleção de dados
- 6.8.2. Perspectivas e critérios de seleção
- 6.8.3. Métodos de seleção

6.9. Seleção de Instâncias
- 6.9.1. Métodos para seleção de instâncias
- 6.9.2. Seleção de protótipos
- 6.9.3. Métodos avançados para seleção de instâncias

6.10. Pré-processamento de dados em ambientes *Big Data*
- 6.10.1. *Big Data*
- 6.10.2. Pré-processamento "clássico" versus massivo
- 6.10.3. *Smart Data*

Módulo 7. Previsibilidade e análise de fenômenos estocásticos

7.1. Séries cronológicas
- 7.1.1. Séries cronológicas
- 7.1.2. Utilidade e aplicabilidade
- 7.1.3. Casuística relacionada

7.2. A Série temporal
- 7.2.1. Tendência Sazonalidade da ST
- 7.2.2. Variações típicas
- 7.2.3. Análise de resíduos

7.3. Tipologia
- 7.3.1. Estacionárias
- 7.3.2. Não estacionárias
- 7.3.3. Transformações e ajustes

7.4. Esquemas para séries cronológicas
- 7.4.1. Esquema (modelo) aditivo
- 7.4.2. Esquema (modelo) multiplicativo
- 7.4.3. Procedimentos para determinar o tipo de modelo

7.5. Métodos básicos de *forecast*
- 7.5.1. Mídia
- 7.5.2. *Naïve*
- 7.5.3. *Naïve* sazonal
- 7.5.4. Comparação de métodos

7.6. Análise de resíduos
- 7.6.1. Autocorrelação
- 7.6.2. ACF de resíduos
- 7.6.3. Teste de correlação

7.7. Regressão no contexto das séries cronológicas
- 7.7.1. ANOVA
- 7.7.2. Fundamentos
- 7.7.3. Aplicações práticas

7.8. Modelos preditivos de séries cronológicas
- 7.8.1. ARIMA
- 7.8.2. Suavização exponencial

7.9. Manipulação e Análise de Séries Temporais com R
- 7.9.1. Preparação dos dados
- 7.9.2. Identificação de padrões
- 7.9.3. Análise do modelo
- 7.9.4. Predição

7.10. Análise gráfica combinada com R
- 7.10.1. Situações típicas
- 7.10.2. Aplicação prática para a solução de problemas simples
- 7.10.3. Aplicação prática para a solução de problemas avançados

Módulo 8. Desenho e desenvolvimento de sistemas inteligentes

8.1. Pré-processamento de dados
- 8.1.1. Pré-processamento de dados
- 8.1.2. Transformação de dados
- 8.1.3. Mineração de dados

8.2. Aprendizado de máquina
- 8.2.1. Aprendizagem supervisionada e não supervisionada
- 8.2.2. Aprendizagem de reforço
- 8.2.3. Outros paradigmas de aprendizagem

8.3. Algoritmos de classificação
- 8.3.1. Aprendizado de Máquina Indutivo
- 8.3.2. SVM e KNN
- 8.3.3. Métricas e pontuações para classificação

8.4. Algoritmos de Regressão
- 8.4.1. Regressão linear, regressão logística e modelos não lineares
- 8.4.2. Séries cronológicas
- 8.4.3. Métricas e pontuações para regressão

8.5. Algoritmos de agrupamento
- 8.5.1. Técnicas de agrupamento hierárquico
- 8.5.2. Técnicas de agrupamento particional
- 8.5.3. Métricas e pontuações para *clustering*

8.6. Técnicas de regras de associação
- 8.6.1. Métodos para extração de regras
- 8.6.2. Métricas e pontuações para algoritmos de regras de associação

8.7. Técnicas avançadas de classificação Múltiplos Classificadores
- 8.7.1. Algoritmos de *Bagging*
- 8.7.2. Classificador *Random Forests*
- 8.7.3. *Boosting* para árvores de decisão

8.8. Modelos gráficos probabilísticos
- 8.8.1. Modelos probabilísticos
- 8.8.2. Redes bayesianas. Propriedades, representação e parametrização
- 8.8.3. Outros modelos gráficos probabilísticos

8.9. Redes Neuronais
- 8.9.1. Aprendizado de máquinas com redes neurais artificiais
- 8.9.2. Redes *feedforward*

8.10. Aprendizado profundo
- 8.10.1. Redes *feedforward* profundas
- 8.10.2. Redes neurais convolucionais e modelos de sequência
- 8.10.3. Ferramentas para implementação de redes neurais profundas

Módulo 9. Arquiteturas e sistemas para uso intensivo de dados

9.1. Requisitos não funcionais Pilares de aplicações de dados massivos
- 9.1.1. Confiabilidade
- 9.1.2. Adaptabilidade
- 9.1.3. Capacidade de manutenção

9.2. Modelos de dados
- 9.2.1. Modelo relacional
- 9.2.2. Modelo documental
- 9.2.3. Modelo de dados tipo grafo

9.3. Bases de dados. Gestão de armazenamento e recuperação de dados
- 9.3.1. Índices has
- 9.3.2. Armazenamento estruturado em logs
- 9.3.3. Árvores B

9.4. Formatos de codificação de dados
- 9.4.1. Formatos específicos de linguagem
- 9.4.2. Formatos padronizados
- 9.4.3. Formatos de codificação binária
- 9.4.4. Fluxo de dados entre processos

9.5. Replicação
- 9.5.1. Objetivos da Replicação
- 9.5.2. Modelos de replicação
- 9.5.3. Problemas com a Replicação

9.6. Transações distribuídas
- 9.6.1. Transação
- 9.6.2. Protocolos para transações distribuídas
- 9.6.3. Transações serializáveis

9.7. Particionamento
- 9.7.1. Formas de particionamento
- 9.7.2. Interação do índice secundário e de particionamento
- 9.7.3. Reequilíbrio do particionamento

9.8. Processamento de dados *offline*
- 9.8.1. Processamento por lotes
- 9.8.2. Sistemas de arquivos distribuídos
- 9.8.3. *MapReduce*

9.9. Processamento de dados em tempo real
- 9.9.1. Tipos de *broker* de mensagens
- 9.9.2. Representação de bancos de dados como fluxos de dados
- 9.9.3. Processamento do fluxo de dados

9.10. Aplicações práticas no mundo dos negócios
- 9.10.1. Consistência nas leituras
- 9.10.2. Abordagem holística dos dados
- 9.10.3. Escalonamento de um serviço distribuído

Módulo 10. Aplicação prática da ciência de dados em setores empresariais

10.1. Setor sanitário
- 10.1.1. Implicações da IA e da análise de dados no setor sanitário
- 10.1.2. Oportunidades e desafios

10.2. Riscos e tendências no setor sanitário
- 10.2.1. Uso no setor sanitário
- 10.2.2. Riscos potenciais relacionados ao uso de IA

10.3. Serviços financeiros
- 10.3.1. Implicações da IA e da análise de dados para o setor de serviços financeiros
- 10.3.2. Uso em serviços financeiros
- 10.3.3. Riscos potenciais relacionados ao uso de IA

10.4. Retail
- 10.4.1. Implicações da IA e da análise de dados no setor de retail
- 10.4.2. Uso no retail
- 10.4.3. Riscos potenciais relacionados ao uso de IA

10.5. Indústria 4.0.
- 10.5.1. Implicações da IA e da análise de dados na Indústria 4.0.
- 10.5.2. Uso na Indústria 4.0.

10.6. Riscos e tendências na Indústria 4.0.
- 10.6.1. Riscos potenciais relacionados ao uso de IA

10.7. Administração pública
- 10.7.1. Implicações da IA e da análise de dados na administração pública
- 10.7.2. Uso na administração pública
- 10.7.3. Riscos potenciais relacionados ao uso de IA

10.8. Educação
- 10.8.1. Implicações da IA e da análise de dados na educação
- 10.8.2. Riscos potenciais relacionados ao uso de IA

10.9. Silvicultura e agricultura
- 10.9.1. Implicações da IA e da análise de dados na Silvicultura e agricultura
- 10.9.2. Uso em silvicultura e agricultura
- 10.9.3. Riscos potenciais relacionados ao uso de IA

10.10. Recursos humanos
- 10.10.1. Implicações da IA e da análise de dados na gestão de recursos humanos
- 10.10.2. Aplicações práticas no mundo empresarial
- 10.10.3. Riscos potenciais relacionados ao uso de IA

Módulo 11. Ciberespionagem e cibersegurança

11.1. Ciberinteligência
- 11.1.1. Ciberinteligência
  - 11.1.1.1. Inteligência
    - 11.1.1.1.1. Ciclo de inteligência
  - 11.1.1.2. Ciberinteligência
  - 11.1.1.3. Ciberespionagem e cibersegurança
- 11.1.2. Analista de Inteligência
  - 11.1.2.1. O papel do analista de inteligência
  - 11.1.2.2. Vias do analista de inteligência em atividade avaliativa

11.2. Segurança Cibernética
- 11.2.1. Camadas de segurança
- 11.2.2. Identificação de ameaças cibernéticas
  - 11.2.2.1. Ameaças externas
  - 11.2.2.2. Ameaças internas
- 11.2.3. Ações adversas
  - 11.2.3.1. Engenharia social
  - 11.2.3.2. Métodos comumente utilizados

11.3. Técnicas e ferramentas de inteligência
- 11.3.1. OSINT
- 11.3.2. SOCMINT
- 11.3.3. HUMIT
- 11.3.4. Distribuições e ferramentas Linux
- 11.3.5. OWISAM
- 11.3.6. OWISAP
- 11.3.7. PTES
- 11.3.8. OSSTM

11.4. Metodologias de avaliação
- 11.4.1. Análise de inteligência
- 11.4.2. Técnicas para organizar as informações adquiridas
- 11.4.3. Confiabilidade e credibilidade das fontes de informação
- 11.4.4. Metodologias de análise
- 11.4.5. Apresentação dos resultados da inteligência

11.5. Auditorias e documentação
- 11.5.1. Auditoria na segurança da informática
- 11.5.2. Documentação e licenças para auditoria
- 11.5.3. Tipos de auditoria
- 11.5.4. Entregáveis
  - 11.5.4.1. Relatório técnico
  - 11.5.4.2. Relatório Executivo

11.6. Anonimato na rede
- 11.6.1. Uso do anonimato
- 11.6.2. Técnicas de anonimización (Proxy, VPN)
- 11.6.3. Redes TOR, Freenet e IP2

11.7. Ameaças e tipos de segurança
- 11.7.1. Tipos de ameaças
- 11.7.2. Segurança física
- 11.7.3. Segurança de rede
- 11.7.4. Segurança lógica
- 11.7.5. Segurança de Aplicações Web
- 11.7.6. Segurança da dispositivos móveis

11.8. Regulamentos e *compliance*
- 11.8.1. RGPD
- 11.8.2. A estratégia nacional de cibersegurança de 2019
- 11.8.3. Família ISO 27000
- 11.8.4. Estrutura de Segurança Cibernética da NIST
- 11.8.5. PIC
- 11.8.6. ISO 27032
- 11.8.7. Normativas *cloud*
- 11.8.8. SOX
- 11.8.9. PCI

11.9. Análise de risco e métricas
- 11.9.1. Escopo dos riscos
- 11.9.2. O patrimônio
- 11.9.3. Ameaças
- 11.9.4. Vulnerabilidades
- 11.9.5. Avaliação de risco
- 11.9.6. Tratamento de risco

11.10. Importantes órgãos de segurança cibernética
- 11.10.1. NIST
- 11.10.2. ENISA
- 11.10.3. INCIBE
- 11.10.4. OEA
- 11.10.5. UNASUR - PROSUR

Módulo 12. Segurança do host

12.1. Cópias de segurança
- 12.1.1. Estratégias para backups
- 12.1.2. Ferramentas para Windows
- 12.1.3. Ferramentas para Linux
- 12.1.4. Ferramentas para MacOS

12.2. Anti-vírus do usuário
- 12.2.1. Tipos de antivírus
- 12.2.2. Antivírus para Windows
- 12.2.3. Antivírus para Linux
- 12.2.4. Antivírus para MacOS
- 12.2.5. Antivírus para smartphones

12.3. Detectores de intrusão - HIDS
- 12.3.1. Métodos de detecção de intrusão
- 12.3.2. *Sagan*
- 12.3.3. *Aide*
- 12.3.4. *Rkhunter*

12.4. *Firewall* local
- 12.4.1. *Firewalls* para Windows
- 12.4.2. *Firewalls* para Linux
- 12.4.3. *Firewalls* para MacOS

12.5. Gestores de senhas
- 12.5.1. *Password*
- 12.5.2. *LastPass*
- 12.5.3. *KeePass*
- 12.5.4. *StickyPassword*
- 12.5.5. *RoboForm*

12.6. Detectores de *phishing*
- 12.6.1. Detecção manual de *phishing*
- 12.6.2. Ferramentas *antiphishing*

12.7. *Spyware*
- 12.7.1. Mecanismos de prevenção
- 12.7.2. Ferramentas *antispyware*

12.8. Rastreadores
- 12.8.1. Medidas para proteger o sistema
- 12.8.2. Ferramentas antirrastreamento

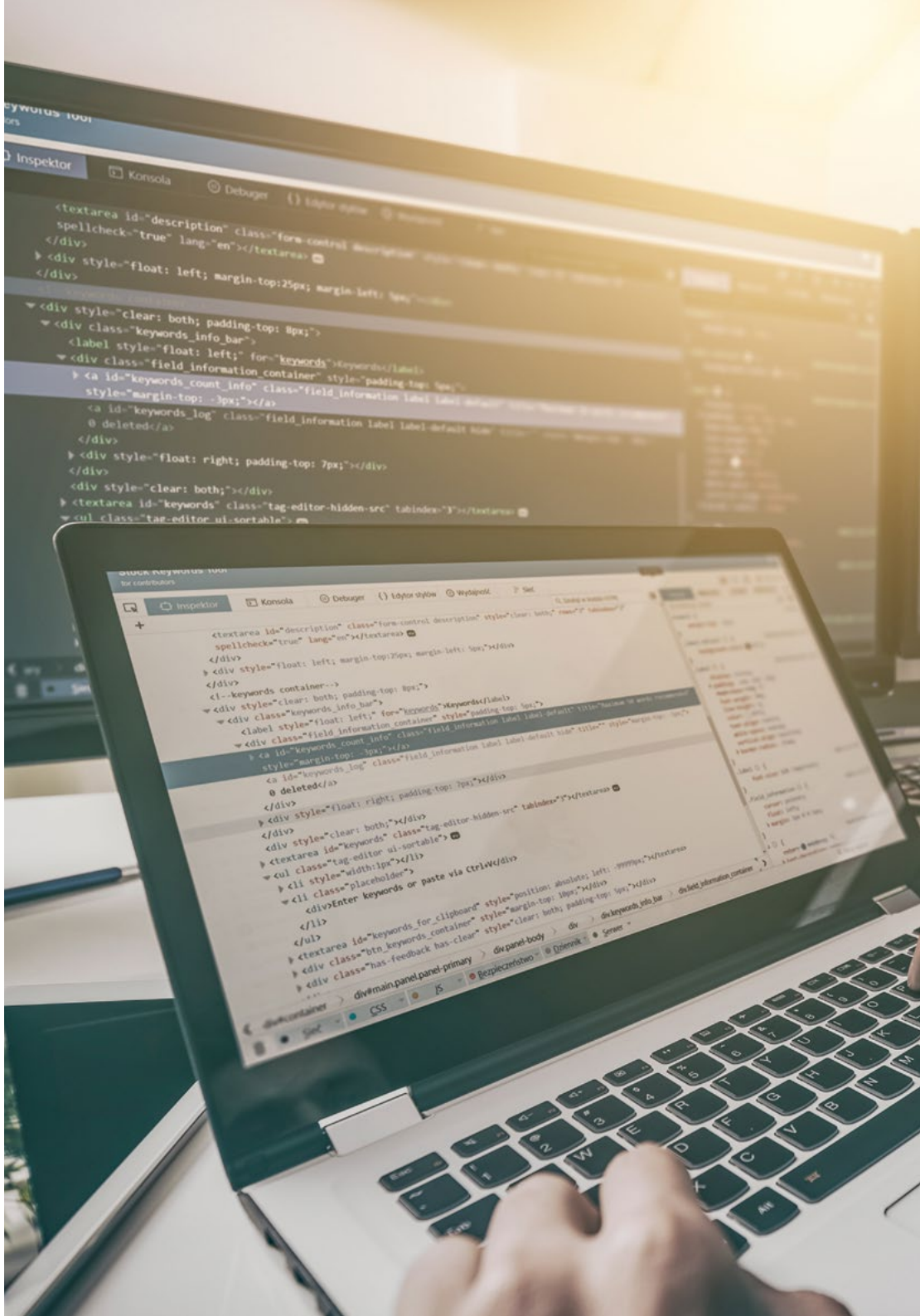
12.9. EDR- *End Point Detection and Response*
- 12.9.1. Comportamento do sistema EDR
- 12.9.2. Diferenças entre EDR e antivírus
- 12.9.3. O futuro dos sistemas EDR

12.10. Controle sobre a instalação de software
- 12.10.1. Repositórios e lojas de software
- 12.10.2. Listas de software permitido ou proibido
- 12.10.3. Critérios de atualização
- 12.10.4. Privilégios para instalar software

Módulo 13. Segurança de rede (Perímetro)

13.1. Sistemas de detecção e prevenção de ameaças
- 13.1.1. Estrutura geral para incidentes de segurança
- 13.1.2. Sistemas de defesa atuais: *Defense in Depth* e SOC
- 13.1.3. Arquiteturas de redes atuais
- 13.1.4. Tipos de ferramentas de detecção e prevenção de incidentes
  - 13.1.4.1. Sistemas baseados em rede
  - 13.1.4.2. Sistemas baseados em host
  - 13.1.4.3. Sistemas centralizados
- 13.1.5. Comunicação e detecção de instâncias/*hosts*, contenedores e *serverless*

13.2. *Firewall*
- 13.2.1. Tipos de *firewalls*
- 13.2.2. Ataques e atenuações
- 13.2.3. *Firewalls* comuns em kernel Linux
  - 13.2.3.1. UFW
  - 13.2.3.2. Nftables e iptables
  - 13.2.3.3. *Firewalld*
- 13.2.4. Sistemas de detecção baseados em logs do sistema
  - 13.2.4.1. TCP *Wrappers*
  - 13.2.4.2. *BlockHosts* e *DenyHosts*
  - 13.2.4.3. Fai2ban



13.3. Sistemas de Detecção e Prevenção de Intrusão (IDS/IPS)
- 13.3.1. Ataques ao IDS/IPS
- 13.3.2. Sistemas IDS/IPS
  - 13.3.2.1. *Snort*
  - 13.3.2.2. Suricata

13.4. *Firewalls* de próxima geração (NGFWs)
- 13.4.1. Diferenças entre NGFW e Firewall tradicional
- 13.4.2. Principais capacidades
- 13.4.3. Soluções comerciais
- 13.4.4. Firewalls para serviços de *Cloud*
  - 13.4.4.1. Arquitetura *Cloud* VPC
  - 13.4.4.2. *Cloud* ACLs
  - 13.4.4.3. *Security Group*

13.5. Proxy
- 13.5.1. Tipos de Proxy
- 13.5.2. Uso de Proxy Vantagens e Desvantagens

13.6. Motores antivírus
- 13.6.1. Contexto geral de *Malware* e IOCs
- 13.6.2. Problemas no motor do antivírus

13.7. Sistemas de proteção de correio
- 13.7.1. Antispam
  - 13.7.1.1. Listas negras e brancas
  - 13.7.1.2. Filtros bayesianos
- 13.7.2. *Mail Gateway* (MGW)

13.8. SIEM
- 13.8.1. Componentes e arquitetura
- 13.8.2. Regras de correlação e casos de uso
- 13.8.3. Desafios atuais dos sistemas SIEM

13.9. SOAR
- 13.9.1. SOAR e SIEM: inimigos ou aliados?
- 13.9.2. O futuro dos sistemas SOAR

13.10. Outros sistemas baseados em rede
- 13.10.1. WAF
- 13.10.2. NAC
- 13.10.3. HoneyPots e HoneyNets
- 13.10.4. CASB

Módulo 14. Segurança para Smartphones

14.1. O mundo do dispositivo móvel
- 14.1.1. Tipos de plataformas móveis
- 14.1.2. Dispositivos iOS
- 14.1.3. Dispositivos Android

14.2. Gestão de Segurança Móvel
- 14.2.1. Projeto de Segurança Móvel OWASP
  - 14.2.1.1. Top 10 Vulnerabilidades
- 14.2.2. Comunicações, redes e modos de conexão

14.3. O dispositivo móvel no ambiente empresarial
- 14.3.1. Riscos
- 14.3.2. Políticas de segurança
- 14.3.3. Monitoramento de dispositivos
- 14.3.4. Gerenciamento de dispositivos móveis (MDM)

14.4. Privacidade do usuário e segurança dos dados
- 14.4.1. Estados de informação
- 14.4.2. Proteção e confidencialidade dos dados
  - 14.4.2.1. Permissões
  - 14.4.2.2. Criptografia
- 14.4.3. Armazenamento seguro de dados
  - 14.4.3.1. Armazenamento seguro no iOS
  - 14.4.3.2. Armazenamento seguro em Android
- 14.4.4. Boas práticas no desenvolvimento de aplicações

14.5. Vulnerabilidades e vetores de ataque
- 14.5.1. Vulnerabilidades
- 14.5.2. Vetores de ataque
  - 14.5.2.1. *Malware*
  - 14.5.2.2. Exfiltração de dados
  - 14.5.2.3. Manipulação de dados

14.6. Principais ameaças
- 14.6.1. Usuário não forçado
- 14.6.2. *Malware*
  - 14.6.2.1. Tipos de *Malware*
- 14.6.3. Engenharia social
- 14.6.4. Vazamento de dados
- 14.6.5. Roubo de informações
- 14.6.6. Redes *Wi-Fi* inseguras
- 14.6.7. Software desatualizado
- 14.6.8. Aplicações maliciosas
- 14.6.9. Senhas inseguras
- 14.6.10. Configurações de segurança fracas ou inexistentes
- 14.6.11. Acesso físico
- 14.6.12. Perda ou roubo do dispositivo
- 14.6.13. Personificação (Integridade)
- 14.6.14. Criptografia fraca ou quebrada
- 14.6.15. Negação de Serviço (DoS)

14.7. Principais ataques
- 14.7.1. Ataques de *phishing*
- 14.7.2. Ataques relacionados aos modos de comunicação
- 14.7.3. Ataques de *Smishing*
- 14.7.4. Ataques de *Criptojacking*
- 14.7.5. *Man in The Middle*

14.8. *Hacking*
- 14.8.1. *Rooting e Jailbreaking*
- 14.8.2. Anatomia de um ataque móvel
  - 14.8.2.1. Propagação da ameaça
  - 14.8.2.2. Instalação de *malware* no dispositivo
  - 14.8.2.3. Persistência
  - 14.8.2.4. Execução de *Payload* e extração de informações
- 14.8.3. *Hacking* sobre dispositivos iOS: mecanismos e ferramentas
- 14.8.4. *Hacking* em dispositivos Android: mecanismos e ferramentas

14.9. Testes de penetração
- 14.9.1. *iOS pentesting*
- 14.9.2. *Android PenTesting*
- 14.9.3. Ferramentas

14.10. Segurança e proteção
- 14.10.1. Configurações de segurança
  - 14.10.1.1. Nos dispositivos iOS
  - 14.10.1.2. Nos dispositivos Android
- 14.10.2. Medidas de segurança
- 14.10.3. Ferramentas de proteção

Módulo 15. Segurança de IoT

15.1. Dispositivos.
- 15.1.1. Tipos de dispositivos
- 15.1.2. Arquiteturas padronizadas
  - 15.1.2.1. ONEM2M
  - 15.1.2.2. IoTWF
- 15.1.3. Protocolos de implementação
- 15.1.4. Tecnologias de conectividade

15.2. Dispositivos IoT Áreas de aplicação
- 15.2.1. *SmartHome*
- 15.2.2. *SmartCity*
- 15.2.3. Transportes
- 15.2.4. *Wearables*
- 15.2.5. Setor de saúde
- 15.2.6. IioT

15.3. Protocolos de comunicação
- 15.3.1. MQTT
- 15.3.2. LWM2M
- 15.3.3. OMA-DM
- 15.3.4. TR-069

15.4. *SmartHome*
- 15.4.1. Automação doméstica
- 15.4.2. Redes
- 15.4.3. Eletrodomésticos
- 15.4.4. Vigilância e segurança

15.5. *SmartCity*
- 15.5.1. Iluminação
- 15.5.2. Meteorologia
- 15.5.3. Segurança

15.6. Transportes
- 15.6.1. Localização
- 15.6.2. Fazendo pagamentos e obtendo serviços
- 15.6.3. Conectividade

15.7. *Wearables*
- 15.7.1. Roupas inteligentes
- 15.7.2. Joias inteligentes
- 15.7.3. Relógios Inteligentes

15.8. Setor de saúde
- 15.8.1. Monitoramento da taxa de exercício/coração
- 15.8.2. Monitoramento de pacientes e pessoas idosas
- 15.8.3. Implantável
- 15.8.4. Robôs cirúrgicos

15.9. Conectividade
- 15.9.1. *Wi-Fi/Gateway*
- 15.9.2. *Bluetooth*
- 15.9.3. Conectividade embutida

15.10. Securitização
- 15.10.1. Redes dedicadas
- 15.10.2. Gerenciador de senhas
- 15.10.3. Uso de protocolos criptografados
- 15.10.4. Dicas de uso

Módulo 16. *Hacking* ético

16.1. Ambiente de trabalho
- 16.1.1. Distribuições Linux
  - 16.1.1.1. Kali Linux - Offensive Security
  - 16.1.1.2. Parrot OS
  - 16.1.1.3. Ubuntu
- 16.1.2. Sistemas de virtualização
- 16.1.3. *Sandbox*
- 16.1.4. Implantação de laboratórios

16.2. Metodologias
- 16.2.1. OSSTM
- 16.2.2. OWASP
- 16.2.3. NIST
- 16.2.4. PTES
- 16.2.5. ISSAF

16.3. *Footprinting*
- 16.3.1. Inteligência de código aberto (OSINT)
- 16.3.2. Busca de violações e vulnerabilidades de dados
- 16.3.3. Uso de ferramentas passivas

16.4. Escaneamento em rede
- 16.4.1. Ferramentas de escaneamento
  - 16.4.1.1. Nmap
  - 16.4.1.2. Hping3
  - 16.4.1.3. Outras ferramentas de Escaneamento
- 16.4.2. Técnicas de digitalização
- 16.4.3. Técnicas de evasão de *Firewall* e IDS
- 16.4.4. *Banner Grabbing*
- 16.4.5. Diagramas de rede

16.5. Enumeração
- 16.5.1. Enumeração SMTP
- 16.5.2. Enumeração DNS
- 16.5.3. Enumeração NetBIOS e Samba
- 16.5.4. Enumeração LDAP
- 16.5.5. Enumeração SNMP
- 16.5.6. Outras técnicas de enumeração

16.6. Análise de vulnerabilidades
- 16.6.1. Soluções de análise de vulnerabilidades
  - 16.6.1.1. Qualys
  - 16.6.1.2. Nessus
  - 16.6.1.3. CFI LanGuard
- 16.6.2. Sistemas de Pontuação de Vulnerabilidade
  - 16.6.2.1. CVSS
  - 16.6.2.2. CVE
  - 16.6.2.3. NVD

16.7. Ataques a redes *wireless*
- 16.7.1. Metodologia de *hacking* em redes sem fio
  - 16.7.1.1. Wi-Fi/Gateway
  - 16.7.1.2. Análise de tráfego
  - 16.7.1.3. Ataques de *aircrack*
    - 16.7.1.3.1. Ataques WEP
    - 16.7.1.3.2. Ataques WPA/WPA2
  - 16.7.1.4. Ataques de *Evil Twin*
  - 16.7.1.5. Ataques a WPS
  - 16.7.1.6. *Jamming*
- 16.7.2. Ferramentas para a segurança sem fio

16.8. Hacking de servidores web
- 16.8.1. *Cross site Scripting*
- 16.8.2. CSRF
- 16.8.3. *Sessão Hijacking*
- 16.8.4. *SQLinjection*

16.9. Exploração de vulnerabilidades
- 16.9.1. Uso de *exploits* conhecidos
- 16.9.2. Uso de *metasploit*
- 16.9.3. Uso de *malware*
  - 16.9.3.1. Definição e escopo
  - 16.9.3.2. Geração de *malware*
  - 16.9.3.3. Bypass de soluções anti-vírus

16.10. Persistência
- 16.10.1. Instalação de rootkits
- 16.10.2. Uso de ncat
- 16.10.3. Uso de tarefas programadas para backdoors
- 16.10.4. Criação de usuários
- 16.10.5. Detecção de HIDS

Módulo 17. Engenharia inversa

17.1. Compiladores
- 17.1.1. Tipos de códigos
- 17.1.2. Fases de um Compilador
- 17.1.3. Tabela de símbolos
- 17.1.4. Tratamento de erros
- 17.1.5. Compilador GCC

17.2. Tipos de análise em compiladores
- 17.2.1. Análise lexical
  - 17.2.1.1. Terminologia
  - 17.2.1.2. Componentes léxicos
  - 17.2.1.3. Analisador Lexical LEX
- 17.2.2. Análise sintática
  - 17.2.2.1. Gramáticas sem contexto
  - 17.2.2.2. Tipos de análise sintática
    - 17.2.2.2.1. Análise top-down
    - 17.2.2.2.2. Análise bottom-up
  - 17.2.2.3. Árvores sintáticas e derivações
  - 17.2.2.4. Tipos de analisadores sintáticos
    - 17.2.2.4.1. Analisadores LR (*Left To Right*)
    - 17.2.2.4.2. Analizadores LALR
- 17.2.3. Análise semântica
  - 17.2.3.1. Gramáticas de Atributos
  - 17.2.3.2. S-Atribuídas
  - 17.2.3.3. L-Atribuídas

17.3. Estruturas de dados de montagem
- 17.3.1. Variáveis
- 17.3.2. Arrays
- 17.3.3. Apontadores
- 17.3.4. Estruturas
- 17.3.5. Objetos

17.4. Estruturas de Códigos de montagem
- 17.4.1. Estruturas de seleção
  - 17.4.1.1. If, else if, Else
  - 17.4.1.2. Switch
- 17.4.2. Estruturas de Iteração
  - 17.4.2.1. For
  - 17.4.2.2. While
  - 17.4.2.3. Uso do break
- 17.4.3. Funções

17.5. Arquitetura de Hardware x86
- 17.5.1. Arquitetura de do processador x86
- 17.5.2. Estruturas de dados de x86
- 17.5.3. Estruturas de Códigos de x86

17.6. Arquitetura de Hardware ARM
- 17.6.1. Arquitetura do processador ARM
- 17.6.2. Estruturas de dados de ARM
- 17.6.3. Estruturas de Códigos de ARM

17.7. Análise de código estático
- 17.7.1. Desmontadores
- 17.7.2. IDA
- 17.7.3. Reconstrutores de código

17.8. Análise de código Dinâmica
- 17.8.1. Análise comportamental
  - 17.8.1.1. Comunicações
  - 17.8.1.2. Monitoração
- 17.8.2. Depuradores de código Linux
- 17.8.3. Depuradores de código no Windows

17.9. *Sandbox*
- 17.9.1. Arquitetura de *Sandbox*
- 17.9.2. Evasão de *Sandbox*
- 17.9.3. Técnicas de detecção
- 17.9.4. Técnicas de prevenção
- 17.9.5. Contra-medidas
- 17.9.6. *Sandbox* em Linux
- 17.9.7. *Sandbox* em Windows
- 17.9.8. *Sandbox* em MacOS
- 17.9.9. *Sandbox* em Android

17.10. Análise de malware
- 17.10.1. Métodos de análise de *malware*
- 17.10.2. Técnicas de ofuscação de *malware*
  - 17.10.2.1. Ofuscação executável
  - 17.10.2.2. Restrição de ambientes de execução
- 17.10.3. Ferramentas de análise de *malware*

Módulo 18. Desenvolvimento seguro

18.1. Desenvolvimento seguro
- 18.1.1. Qualidade, funcionalidade e segurança
- 18.1.2. Confidencialidade, integridade e disponibilidade
- 18.1.3. Ciclo de vida do desenvolvimento de software

18.2. Fase de requisitos
- 18.2.1. Controle de autenticação
- 18.2.2. Controle de papéis e privilégios
- 18.2.3. Requisitos orientados ao risco
- 18.2.4. Aprovação de privilégios

18.3. Fases de análise e projeto
- 18.3.1. Acesso aos componentes e administração do sistema
- 18.3.2. Pistas de auditoria
- 18.3.3. Gestão da sessão
- 18.3.4. Dados históricos
- 18.3.5. Tratamento adequado de erros
- 18.3.6. Separação de funções

18.4. Fase de implementação e codificação
- 18.4.1. Assegurando o ambiente de desenvolvimento
- 18.4.2. Preparação da documentação técnica
- 18.4.3. Codificação segura
- 18.4.4. Segurança das comunicações

18.5. Boas práticas de codificação seguras
- 18.5.1. Validação dos dados de entrada
- 18.5.2. Codificação dos dados de
- 18.5.3. Estilo de programação
- 18.5.4. Gerenciamento de registro de mudanças
- 18.5.5. Práticas criptográficas
- 18.5.6. Gerenciamento de erros e logs
- 18.5.7. Gerenciamento de arquivos
- 18.5.8. Gerenciamento de memória
- 18.5.9. Padronização e reutilização das funções de segurança

18.6. Preparação do servidor e *Hardening*
- 18.6.1. Gerenciamento de usuários, grupos e funções no servidor
- 18.6.2. Instalação de software
- 18.6.3. *Hardening* do servidor
- 18.6.4. Configuração robusta do ambiente de aplicação

18.7. Preparação da BBDD e *Hardening*
- 18.7.1. Otimização do motor da BD
- 18.7.2. Criação de seu próprio usuário para a aplicação
- 18.7.3. Atribuição dos privilégios necessários ao usuário
- 18.7.4. *Hardening* da BD

18.8. Fase de testes
- 18.8.1. Controle de qualidade nos controles de segurança
- 18.8.2. Inspeção por fases de código
- 18.8.3. Verificação da gestão das configurações
- 18.8.4. Teste da caixa preta

18.9. Preparando a transição para a produção
- 18.9.1. Realizar o controle de mudanças
- 18.9.2. Realizar o procedimento de mudança de produção
- 18.9.3. Realizar o procedimento de *rollback*
- 18.9.4. Testes de pré-produção

18.10. Fase de manutenção
- 18.10.1. Garantia baseada em risco
- 18.10.2. Teste de manutenção de segurança da caixa branca
- 18.10.3. Teste de manutenção de segurança da caixa preta

Módulo 19. Análise Forense

19.1. Aquisição e replicação de dados
- 19.1.1. Aquisição volátil de dados
  - 19.1.1.1. Informações do sistema
  - 19.1.1.2. Informação da rede
  - 19.1.1.3. Ordem de volatilidade
- 19.1.2. Aquisição estática de dados
  - 19.1.2.1. Criação de uma imagem duplicada
  - 19.1.2.2. Preparação de um documento de cadeia de custódia
- 19.1.3. Métodos de validação dos dados adquiridos
  - 19.1.3.1. Métodos para Linux
  - 19.1.3.2. Métodos para Windows

19.2. Avaliação e derrota das técnicas anti-forenses
- 19.2.1. Objetivos das técnicas forenses
- 19.2.2. Eliminação de dados
  - 19.2.2.1. Eliminação de dados e arquivos
  - 19.2.2.2. Recuperação de arquivos
  - 19.2.2.3. Recuperação de partições apagadas
- 19.2.3. Proteção por senha
- 19.2.4. Esteganografia
- 19.2.5. Limpeza segura do dispositivo
- 19.2.6. Criptografia

19.3. Análise Forense do sistema operacional
- 19.3.1. Windows Forensics
- 19.3.2. Forense Linux
- 19.3.3. Mac forensics

19.4. Análise Forense de Rede
- 19.4.1. Análise de logs
- 19.4.2. Correlação dos dados
- 19.4.3. Pesquisa de rede
- 19.4.4. Passos a seguir na análise forense da rede

19.5. Forense da Web
- 19.5.1. Investigação de ataques na web
- 19.5.2. Detecção de ataques
- 19.5.3. Localização de endereços IP

19.6. Análise forense de bancos de dados
- 19.6.1. Forense da MSSQL
- 19.6.2. Forense da MySQL
- 19.6.3. Forense da Web
- 19.6.4. Forense da MSSQL

19.7. Análise forense em *cloud*
- 19.7.1. Tipos de crimes em *cloud*
  - 19.7.1.1. *Cloud* como sujeito
  - 19.7.1.2. *Cloud* como objeto
  - 19.7.1.3. *Cloud* como ferramenta
- 19.7.2. Desafios da análise forense em *cloud*
- 19.7.3. Investigação dos serviços de armazenamento em *cloud*
- 19.7.4. Ferramentas de análise forense para *cloud*

19.8. Investigação de crimes por e-mail
- 19.8.1. Sistemas de e-mail
  - 19.8.1.1. Clientes de e-mail
  - 19.8.1.2. Servidor de e-mail
  - 19.8.1.3. Servidor SMTP
  - 19.8.1.4. Servidor POP3
  - 19.8.1.5. Servidor IMAP4
- 19.8.2. Crimes por e-mail
- 19.8.3. Mensagem de e-mail
  - 19.8.3.1. Cabeçalhos padrão
  - 19.8.3.2. Cabeçalhos estendidos
- 19.8.4. Passos para a investigação destes crimes
- 19.8.5. Ferramentas forenses por e-mail

19.9. Forense móvel
- 19.9.1. Redes celulares
  - 19.9.1.1. Tipos de redes
  - 19.9.1.2. Conteúdo do CdR
- 19.9.2. *Subscriber Identity Module* (SIM)
- 19.9.3. Aquisição lógica
- 19.9.4. Aquisição física
- 19.9.5. Aquisição do sistema de arquivo

19.10. Redação e apresentação de relatórios forenses
- 19.10.1. Aspectos importantes de um relatório forense
- 19.10.2. Classificação e tipos de Relatórios
- 19.10.3. Guia para escrever um relatório
- 19.10.4. Apresentação do relatório
  - 19.10.4.1. Preparação prévia para o depoimento
  - 19.10.4.2. Deposição
  - 19.10.4.3. Lidando com a mídia

Módulo 20. Desafios atuais e futuros da segurança cibernética

20.1. Tecnologia *blockchain*
- 20.1.1. Área de aplicação
- 20.1.2. Garantia de confidencialidade
- 20.1.3. Garantia de não repudiação

20.2. Dinheiro digital
- 20.2.1. Bitcoins
- 20.2.2. Critpomonedas
- 20.2.3. Mineração de moedas criptográficas
- 20.2.4. Esquemas piramidais
- 20.2.5. Outros crimes e problemas potenciais

20.3. *Deepfake*
- 20.3.1. Impacto na mídia
- 20.3.2. Perigos para a sociedade
- 20.3.3. Mecanismos de detecção

20.4. O futuro da inteligência artificial
- 20.4.1. Inteligência artificial e computação cognitiva
- 20.4.2. Usos para simplificar o atendimento ao cliente

20.5. Privacidade digital
- 20.5.1. Valor dos dados na rede
- 20.5.2. Uso dos dados na rede
- 20.5.3. Gerenciamento de privacidade e identidade digital

20.6. Ciberconflitos, cibercriminosos e ciberataques
- 20.6.1. O impacto da cibersegurança nos conflitos internacionais
- 20.6.2. Consequências dos ciberataques sobre a população em geral
- 20.6.3. Tipos de cibercriminosos Medidas de proteção

20.7. Trabalho à distância
- 20.7.1. Revolução do trabalho à distância durante e após a Covid19
- 20.7.2. Engarrafamentos de acesso
- 20.7.3. Variação da superfície de ataque
- 20.7.4. As necessidades dos trabalhadores

20.8. Tecnologias *wireless* emergentes
- 20.8.1. WPA3
- 20.8.2. 5G
- 20.8.3. Ondas milimétricas
- 20.8.4. Tendência em *Get Smart* ao invés de *Get more*

20.9. Endereçamento futuro em redes
- 20.9.1. Problemas atuais com o endereçamento IP
- 20.9.2. IPv6
- 20.9.3. IPv4+
- 20.9.4. Vantagens do IPv4+ em relação ao IPv4
- 20.9.5. Vantagens do IPv6 sobre o IPv4

20.10. O desafio de aumentar a conscientização da educação precoce e contínua da população
- 20.10.1. Estratégias atuais do governo
- 20.10.2. Resistência da população ao aprendizado
- 20.10.3. Planos de capacitação a serem adotados pelas empresas

Você aprenderá por meio de casos reais criados em ambientes de aprendizado simulados que refletem os desafios atuais de gerenciamento de dados e segurança cibernética"

04

Objetivos de ensino

O principal objetivo do Advanced Master em Secure Information Management é proporcionar aos alunos um excelente conhecimento em duas áreas fundamentais e complementares da ciência e engenharia da computação: gerenciamento de dados em ambientes digitais e segurança cibernética. Esse programa combina as duas disciplinas para capacitar profissionais na implementação de soluções avançadas, permitindo que eles enfrentem os desafios do trabalho com as ferramentas necessárias para gerenciar e proteger informações confidenciais em suas organizações.

Transforme sua carreira com este inovador Advanced Master, projetado para marcar um ponto de virada em sua especialização em gestão de dados e segurança cibernética"

Objetivos gerais

- Desenvolver habilidades avançadas em análise de dados e segurança cibernética para otimizar os processos de negócios com ferramentas e técnicas inovadoras
- Implementar estratégias de segurança eficazes para evitar ameaças digitais a sistemas, redes e dispositivos móveis em sistemas, redes e dispositivos móveis
- Resolver desafios de segurança cibernética por meio de auditoria, engenharia reversa e análise forense baseada em evidências
- Antecipar tendências tecnológicas aplicando soluções inovadoras que protegem ativos digitais e sistemas avançados

Liderar a gestão de dados e a segurança cibernética no ambiente digital com este programa de especialização"

Objetivos específicos

Módulo 1. Análise de dados na organização empresarial

- Desenvolver habilidades no uso de técnicas de análise de dados
- Gerar informações valiosas que orientam a tomada de decisões estratégicas em organizações comerciais, melhorando a eficiência e a competitividade

Módulo 2. Gestão, Manipulação de Dados e Informações para a Ciência de Dados

- Capacitar em gestão e manipulação eficientes de grandes volumes de dados
- Aplicar metodologias e ferramentas para estruturar, limpar e transformar dados em informações úteis para projetos de ciência de dados

Módulo 3. Dispositivos e plataformas IoT como base para a Ciência de Dados

- Fornecer o conhecimento necessário sobre as plataformas e os dispositivos da Internet das Coisas e sua integração na ciência de dados
- Aprofundar-se na captura, no processamento e na análise de dados em tempo real

Módulo 4. Representação gráfica para análise de dados

- Representar dados graficamente usando ferramentas e técnicas avançadas de visualização
- Facilitar a compreensão de padrões, tendências e relacionamentos em grandes conjuntos de dados

Módulo 5. Ferramentas da ciência de dados

- Capacitar-se no uso de ferramentas e softwares específicos de ciência de dados, como Python
- Aprofundar seu conhecimento sobre coleta, análise e apresentação de dados em diversos contextos profissionais

Módulo 6. Mineração de dados. Seleção, pré-processamento e transformação

- Fornecer o conhecimento e as habilidades necessárias para aplicar técnicas de mineração de dados
- Analisar a seleção, o pré-processamento e a transformação de dados para extrair padrões e tendências significativos

Módulo 7. Previsibilidade e análise de fenômenos estocásticos

- Desenvolver habilidades na modelagem e análise de fenômenos estocásticos
- Usar métodos estatísticos avançados para prever o comportamento e as tendências em ambientes incertos e dinâmicos

Módulo 8. Design e desenvolvimento de sistemas inteligentes

- Capacitar no projeto e desenvolvimento de sistemas inteligentes, integrando técnicas de aprendizado de máquina e inteligência artificial
- Criar soluções automatizadas que resolvam problemas complexos com eficiência

Módulo 9. Arquiteturas e sistemas para uso intensivo de dados

- Fornecer conhecimento sobre a criação de arquiteturas de sistemas capazes de processar com eficiência grandes volumes de dados
- Usar tecnologias avançadas, como bancos de dados distribuídos e processamento paralelo

Módulo 10. Aplicação prática da ciência de dados em setores empresariais

- Desenvolver a capacidade de aplicar práticas de ciência de dados em vários setores de negócios
- Integrar o conhecimento adquirido para melhorar a tomada de decisões, a otimização de processos e a inovação na empresa

Módulo 11. Ciberespionagem e cibersegurança
- Fornecer o conhecimento e as habilidades necessárias para aplicar técnicas de inteligência cibernética e de segurança cibernética
- Proteger sistemas e redes empresariais contra ameaças cibernéticas e garantir a integridade dos dados

Módulo 12. Segurança do Host
- Capacitar na implementação de medidas de segurança em sistemas host
- Garantir a proteção de servidores e aplicativos essenciais por meio do uso de ferramentas e boas práticas de segurança de TI

Módulo 13. Segurança de rede (perímetro)
- Fornecer conhecimento sobre a proteção de redes e sistemas de computador no nível do perímetro
- Gerenciar firewalls, VPNs e outras ferramentas para garantir a segurança na infraestrutura de rede da empresa

Módulo 14. Segurança para Smartphones
- Desenvolver competências para garantir a segurança em dispositivos móveis
- Compreensão das vulnerabilidades comuns e implementação de medidas preventivas para proteger informações e aplicativos em smartphones

Módulo 15. Segurança de IoT
- Fornecer o conhecimento necessário para implementar soluções de segurança para dispositivos de IoT
- Proteger redes e sistemas que interconectam dispositivos e garantem a confidencialidade e a integridade dos dados gerados

Módulo 16. Hacking ético
- Capacitar nas práticas de hacking ético, ensinando como realizar testes de penetração controlados
- Identificar vulnerabilidades nos sistemas de TI para melhorar a segurança antes que elas possam ser exploradas por invasores

Módulo 17. Engenharia inversa
- Fornecer conhecimento de técnicas de engenharia reversa, permitindo a análise e a compreensão de software e hardware
- Detectar falhas de segurança ou melhorar a funcionalidade dos sistemas existentes

Módulo 18. Desenvolvimento seguro
- Capacitar em desenvolvimento seguro de software, ensinando boas práticas de codificação e segurança durante o ciclo de vida do software
- Ser capaz de evitar vulnerabilidades e proteger os sistemas de TI contra ataques

Módulo 19. Análise Forense
- Desenvolver as habilidades necessárias para conduzir investigações forenses digitais
- Usar ferramentas e técnicas avançadas para recuperar, analisar e preservar evidências eletrônicas em incidentes de segurança de computadores

Módulo 20. Desafios atuais e futuros da segurança cibernética
- Explorar os desafios atuais e futuros no campo da segurança de TI, analisando as ameaças emergentes e as novas tecnologias de proteção
- Aprofundar as estratégias para mitigar os riscos em um ambiente tecnológico em constante mudança

05

Oportunidades profissionais

Após a conclusão do Advanced Master em Secure Information Management, os profissionais terão adquirido uma sólida compreensão das estratégias mais avançadas em segurança cibernética e gerenciamento de dados digitais. Os alunos estarão preparados para projetar e implementar soluções que garantam a proteção de informações confidenciais e otimizem os processos de análise e tomada de decisões em ambientes de negócios. Dessa forma, eles melhorarão suas perspectivas de carreira e assumirão funções especializadas, como analistas de segurança cibernética, consultores de inteligência ou gerentes de dados críticos.

Você garantirá a segurança dos ativos digitais e desempenhará um papel fundamental na transformação digital das organizações"

Perfil do aluno

Os alunos do Advanced Master em Secure Information Management serão altamente qualificados para gerenciar e proteger informações em ambientes digitais. Você terá conhecimentos avançados em áreas como segurança cibernética, inteligência digital e análise de dados, além de habilidades práticas no projeto e na implementação de estratégias de defesa contra ameaças. Seu perfil combina um profundo conhecimento técnico com competências estratégicas que lhe permitirão liderar projetos em setores-chave de negócios.

> *Você se tornará um líder em proteção de dados e segurança cibernética, trabalhando com empresas para enfrentar os desafios do ambiente digital.*

- **Gestão da Segurança:** Desenvolver a capacidade de identificar riscos, implementar estratégias de defesa em várias camadas e garantir a confidencialidade, a integridade e a disponibilidade dos dados.
- **Análise crítico e resolução de problemas:** Você aplicará técnicas avançadas para avaliar sistemas, detectar vulnerabilidades e projetar soluções adaptadas a diferentes ambientes tecnológicos.
- **Competência técnica e digital:** Você lidará com ferramentas avançadas para análise de dados, segurança cibernética e sistemas de inteligência, permitindo que você lidere projetos de inovação tecnológica
- **Pensamento estratégico:** Projetar políticas de segurança e estratégias de negócios que atendam às demandas atuais e futuras do ambiente digital.
- **Colaboração interdisciplinar:** Você trabalhará com equipes multidisciplinares para enfrentar desafios complexos e garantir a segurança em redes, plataformas de IoT e dispositivos móveis

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

1. **Diretor de cibersegurança:** Líder responsável pela coordenação de equipes e pela elaboração de estratégias para proteger ativos digitais em grandes organizações
2. **Analista de Dados:** Desenvolver sistemas de análise preditiva e de visualização para otimizar a tomada de decisões
3. **Consultor de inteligência digital:** Consultor especializado em fornecer soluções avançadas baseadas em inteligência e análise de risco
4. **Especialista em IoT e segurança:** Designer de medidas de proteção para dispositivos conectados e ambientes industriais
5. **Hacker Ético:** Avaliar vulnerabilidades corrigir falhas em sistemas corporativos para evitar ataques cibernéticos
6. **Auditoria de Segurança:** Inspetor conduzindo auditorias e análises forenses para garantir a conformidade regulamentar
7. **Gerenciador de dados corporativos:** Administrador responsável por projetar e gerenciar sistemas de armazenamento e análise para melhorar a eficiência operacional.

Conclua este programa e se destaque como um especialista nas áreas mais procuradas do ambiente digital"

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.

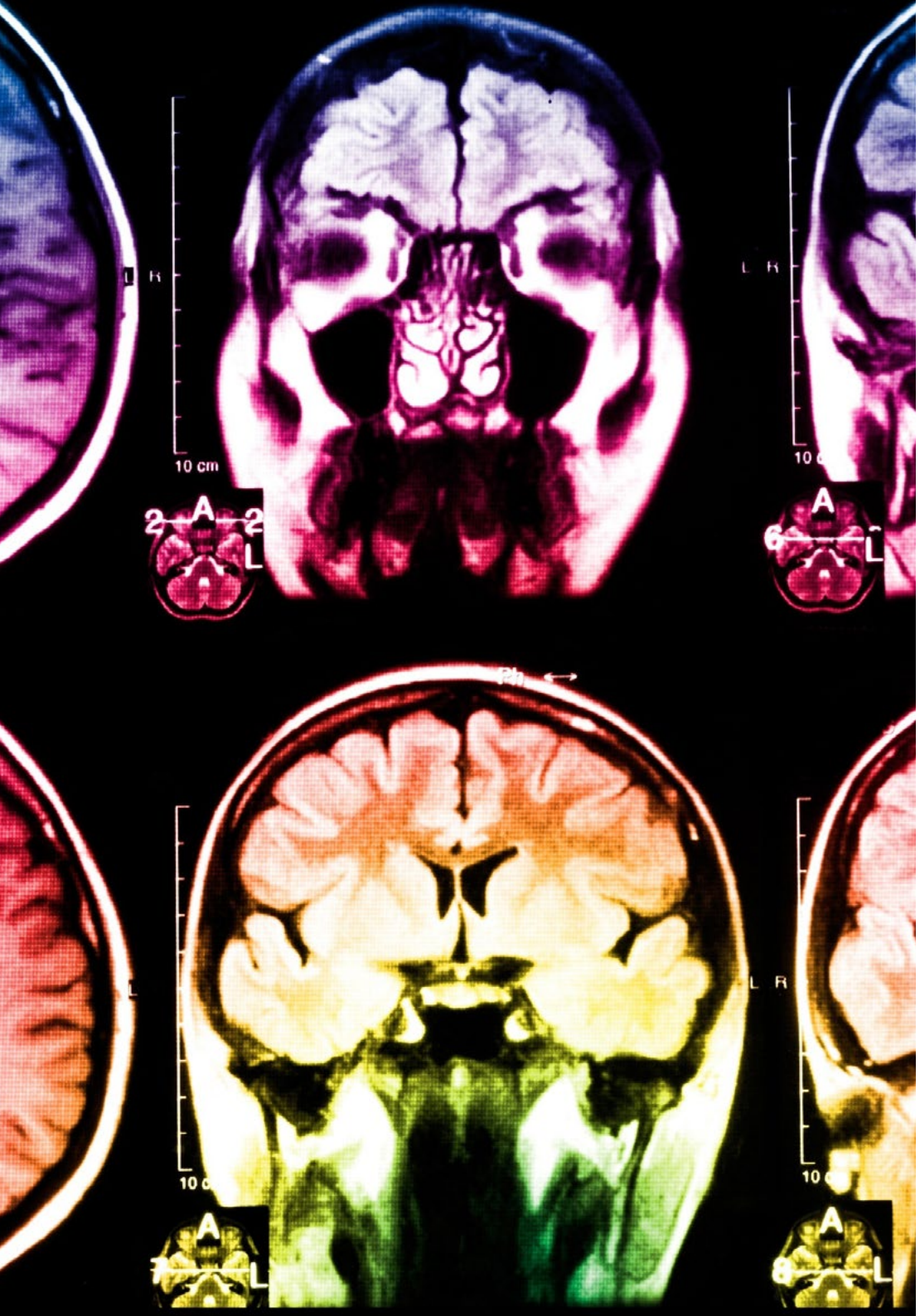
Por outro lado, também para favorecer ao máximo o contato entre mentor e mentorado, é oferecida uma ampla variedade de possibilidades de comunicação, tanto em tempo real quanto em diferido (mensagens internas, fóruns de discussão, serviço telefônico, contato por e-mail com a secretaria técnica, bate-papo,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

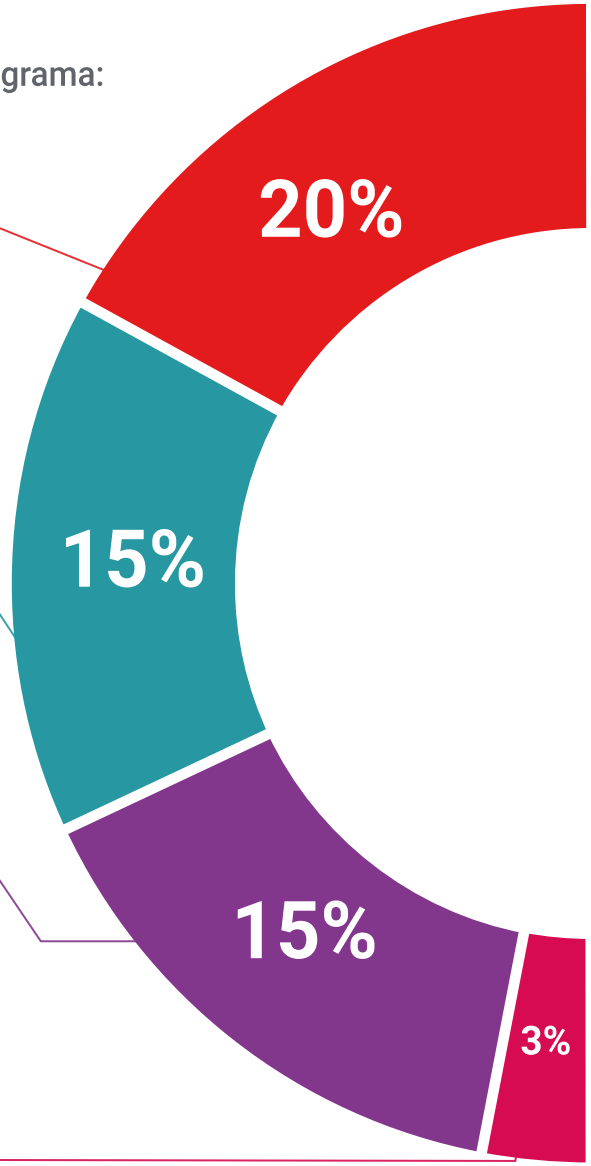
Resumos interativos

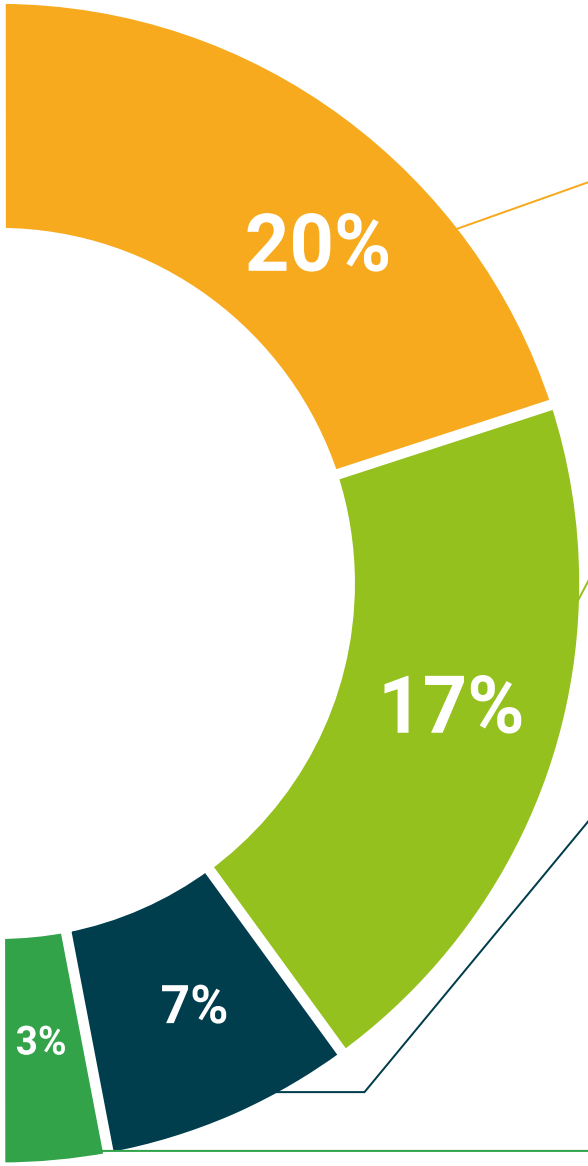
Apresentamos os conteúdos de forma atraente e dinâmica em pílulas multimídia que incluem áudio, vídeos, imagens, diagramas e mapas conceituais com o objetivo de reforçar o conhecimento.

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 curso é ministrado por profissionais líderes em segurança cibernética e gerenciamento de dados digitais. Sua experiência garante que os alunos recebam conteúdo abrangente e atualizado que seja diretamente aplicável às suas carreiras. Assim, os professores desse Advanced Master em Secure Information Management compartilham seus conhecimentos, formando especialistas altamente qualificados que são procurados por grandes empresas internacionais.

Tenha sucesso com os melhores e adquira o conhecimento e as competências essenciais para liderar o gerenciamento de dados e a segurança cibernética no ambiente digital”

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

Dr. Arturo Peralta Martín-Palomino

- CEO e CTO em Prometeus Global Solutions
- CTO em Korporate Technologies
- CTO em AI Shephers GmbH
- Consultor e Assessor Estratégico de Negócios da Alliance Medical
- Diretor de Design e Desenvolvimento da DocPath
- Doutorado em Engenharia da Computação pela Universidade de Castilla - La Mancha
- Doutorado em Economia, Negócios e Finanças pela Universidade Camilo José Cela
- Doutorado em Psicologia pela Universidade de Castilla - La Mancha
- Mestrado em Executive MBA pela Universidade Isabel I
- Mestrado em Gestão Comercial e de Marketing pela Universidade Isabel I
- Mestrado Especialista em Big Data por Formação Hadoop
- Mestrado em Tecnologia da Informação Avançada pela Universidade de Castilla-La Mancha
- Membro de grupo de pesquisa SMILE

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

Professores

Sr. Andrés Montoro Montarroso

- Pesquisador no grupo SMILe da Universidade de Castilla-La Mancha
- Pesquisador da Universidade de Granada
- Cientista de Dados na Prometeus Global Solutions
- Vice-presidente e desenvolvedor de software da CireBits
- Doutorado em Tecnologia da Informação Avançada pela Universidade de Castilla-La Mancha
- Graduado em Engenharia da Computação pela Universidade de Castilla - La Mancha
- Mestrado em Ciência de Dados e Engenharia da Computação pela Universidade de Granada
- Professor convidado na disciplina de Sistemas Baseados em Conhecimento na Escuela Superior de Informática de Ciudad Real, ministrando a palestra: *Técnicas Avançadas de Inteligência Artificial: Busca e análise de potenciais radicais nas mídias sociais"*.
- Professor convidado na disciplina de Mineração de dados, Escuela Superior de Informática de Ciudad Real, ministrando a conferência: *Aplicações de Processamento de Linguagem Natural: Lógica Difusa para a análise de mensagens em redes sociais*
- Palestrante no Seminário sobre Prevenção da Corrupção nas Administrações Públicas e Inteligência Artificial na Faculdade de Ciências Jurídicas e Sociais de Toledo, ministrando a palestra: *Técnicas de Inteligência Artificial*
- Palestrante no primeiro Seminário Internacional de Direito Administrativo e Inteligência Artificial (DAIA) Organizada pelo Centro de Estudos Europeus Luis Ortega Álvarez e pelo Instituto de Pesquisa TransJus. Conferência intitulada *Análise de Sentimentos para a prevenção do discurso de ódio nas mídias sociais*

Sr. Luis Javier Peris Morillo

- Senior Technical Lead e Delivery Lead Support na HCL Technologies
- Editor técnico na Baeldung
- Agile Coach e Diretor de Operações na Mirai Advisory
- Desenvolvedor, Team Lead, Scrum Master, Agile Coach e Product Manager na DocPath
- Tecnólogo na ARCO
- Formado em Engenharia Superior de Computação pela Universidade de Castilla-La Mancha
- Pós-graduado em Gestão de Projeto pela CEOE

Sra. Galina Fernández Meléndez

- Especialista em Big Data
- Analista de dados na Aresi Gestión de Fincas
- Analista de Dados na ADN Mobile Solution
- Formada em Administração de Empresas pela Universidad Bicentenaria de Aragua. Caracas, Venezuela
- Formada em Planejamento e Finanças Públicas pela Escola Venezuelana de Planejamento
- Mestrado em Análise de Dados e Inteligência de Negócios pela Universidade de Oviedo
- MBA em Administração e Direção de Empresas pela Escola de Negócios Europeia de Barcelona
- Mestrado em Big Data e Business Intelligence (Escola de Negócios Europeia de Barcelona

Sra. María Elena Pedrajas Parabás

- New Technologies and Digital Transformation Consultant em Management Solutions
- Pesquisadora no Departamento de Informática e Análise Numérica na Universidade de Córdoba
- Pesquisadora no Centro Singular de Pesquisa em Tecnologias Inteligentes em Santiago de Compostela
- Formada em Engenharia da Computação pela Universidade de Córdoba
- Mestrado em Ciência de Dados e Engenharia da Computação pela Universidade de Granada
- Mestrado em Consultoria Empresarial pela Universidade Pontifícia Comillas

Sra. Yésica Martínez Cerrato

- Responsável pela formação técnica na Securitas Seguridad España
- Especialista em Educação, Negócios e Marketing
- *Product Manager* de Segurança Eletrônica na Securitas Seguridad Espanha
- Analista de Inteligência Empresarial na Ricopia Technologies
- Técnico de TI e responsável pelas salas de aula de informática da OTEC na Universidade de Alcalá de Henares
- Colaboradora da Associação ASALUMA
- Grau em Engenharia Eletrônica de Comunicações pela Escola Politécnica Superior da Universidade de Henares

Sr. Rubén Fondón Alcalde

- Analista EMEA de Amazon Web Services
- Analista de Negócios de Gestão de Valor do Cliente na Vodafone Espanha
- Chefe de Integração de Serviços na Entelgy para a Telefónica Global Solutions
- Gerente de Contas Online para Servidores Clone na EDM Electronics
- Gerente de implementação de serviços internacionais na Vodafone Empresa global
- Consultor de soluções para a Espanha e Portugal, Telvent Global Services
- Analista de Negócios para o Sul da Europa na Vodafone Global Enterprise
- Engenheiro de Telecomunicações da Universidade Europeia de Madri
- Mestrado em Grandes Dados e Analítica pela Universidade Internacional de Valência

Sr. Tobias Díaz Díaz-Chirón

- Pesquisador no laboratório ArCO da Universidade de Castilla-La Mancha
- Consultor na Blue Telecom
- Freelance dedicado principalmente ao setor de telecomunicações, especializado em redes 4G/5G
- OpenStack: deploy and administration
- Engenheiro Superior em Informática pela Universidade de Castilla-La Mancha
- Especialização em Arquitetura e Redes de Computadores
- Professor associado da Universidade de Castilla-La Mancha
- Palestrante no curso Sepecam sobre administração de redes

Sr. Tato Sánchez, Rafael

- Diretor Técnico da Indra Sistemas SA
- Engenheiro de Sistemas na ENA Tráfico SAU
- Mestrado em Indústria 4.0 pela Universidade em Internet
- Mestrado em Engenharia Industrial pela Universidade Europeia
- Formado em Engenharia Eletrônica Industrial e de Automatização pela Universidad Europeia
- Engenheiro Técnico Industrial pela Universidade Politécnica de Madri

Sra. Marcos Sbarbaro, Victoria Alicia

- 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. 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. Rafael Armero Fernández

- Business Intelligence Consultant na SDG Group
- Digital Engineer na MI-GSO
- Logistic Engineer na Torrecid SA
- Quality Intern na INDRA
- Graduado em Engenharia Aeroespacial pela Universidade Politécnica de Valencia
- Mestrado em Professional Development 4.0 pela Universidade de Alcalá

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. 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. 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

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

08

Certificação

O Advanced Master em Secure Information Management garante, além da capacitação mais rigorosa e atualizada, o acesso a um certificado emitido pela TECH Global University

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

Este **Advanced Master em Secure Information Management** conta com o conteúdo científico 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 Secure Information Management**

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

Secure Information Management

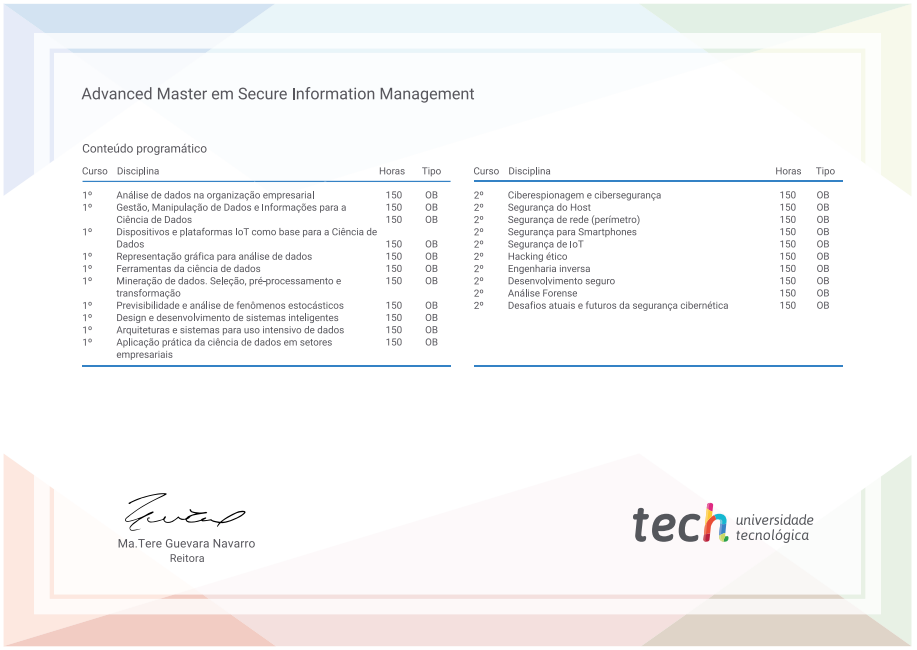
Este é um curso próprio desta Universidade, com duração de 3.000 horas, com data de início dd/mm/aaaa e data final dd/mm/aaaaa.

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 Secure Information Management

Conteúdo programático

Curso	Disciplina	Horas	Tipo
1º	Análise de dados na organização empresarial	150	OB
1º	Gestão, Manipulação de Dados e Informações para a Ciência de Dados	150	OB
1º	Dispositivos e plataformas IoT como base para a Ciência de Dados	150	OB
1º	Representação gráfica para análise de dados	150	OB
1º	Ferramentas da ciência de dados	150	OB
1º	Mineração de dados. Seleção, pré-processamento e transformação	150	OB
1º	Previsibilidade e análise de fenômenos estocásticos	150	OB
1º	Design e desenvolvimento de sistemas inteligentes	150	OB
1º	Arquiteturas e sistemas para uso intensivo de dados	150	OB
1º	Aplicação prática da ciência de dados em setores empresariais	150	OB

Curso	Disciplina	Horas	Tipo
2º	Ciberespionagem e cibersegurança	150	OB
2º	Segurança do Host	150	OB
2º	Segurança de rede (perímetro)	150	OB
2º	Segurança para Smartphones	150	OB
2º	Segurança de IoT	150	OB
2º	Hacking ético	150	OB
2º	Engenharia inversa	150	OB
2º	Desenvolvimento seguro	150	OB
2º	Análise Forense	150	OB
2º	Desafios atuais e futuros da segurança cibernética	150	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
Secure Information Management

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

Advanced Master

Secure Information Management

tech universidade tecnológica