Advanced Master

Secure Information Management

tech global university

tech global university

Advanced Master
Secure Information Management

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

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

Índice

01 Apresentação do programa — pág. 4

02 Porquê estudar na TECH? — pág. 8

03 Plano de estudos — pág. 12

04 Objetivos de ensino — pág. 32

05 Oportunidades de carreira — pág. 38

06 Metodología de estudo — pág. 42

07 Corpo docente — pág. 52

08 Certificação — pág. 62

01

Apresentação do programa

Na era digital atual, as atividades de diferentes áreas são geridas de forma integrada através da internet. O entretenimento, o trabalho e a comunicação com amigos e familiares dependem, cada vez mais, de ferramentas e recursos online. Diariamente, são transferidas enormes quantidades de informações, desde dados simples em conversas nas redes sociais e aplicações de mensagens até informações sensíveis de carácter pessoal e profissional armazenadas em plataformas bancárias ou empresariais. Este panorama exige especialistas capazes de gerir e proteger informações em diversos contextos, priorizando a sua segurança. Por isso, a TECH concebeu este programa em Engenharia de Software, focado na formação de profissionais com as competências necessárias para gerir e proteger a informação de forma eficaz, enfrentando os desafios digitais atuais e contribuindo para criar ambientes tecnológicos mais seguros e confiáveis.

Proteger dados é crucial face a ameaças constantes. Pode ser o guardião dessa valiosa informação"

A cada segundo, milhares de dados são gerados, partilhados e armazenados no ambiente digital. Desde realizar pagamentos online e aceder a serviços educativos até coordenar atividades empresariais ou proteger identidades digitais, a tecnologia tornou-se um pilar essencial que transforma continuamente a forma como vivemos e trabalhamos. Estas interações geram e transferem quantidades massivas de dados a todo instante, desde informações pessoais até arquivos sensíveis relacionados com empresas e instituições. Este fluxo constante de dados destaca a necessidade de uma gestão adequada para garantir a sua segurança e privacidade.

Gerir e proteger estes dados não é uma tarefa simples, pois requer a combinação de conhecimentos altamente especializados em áreas como a cibersegurança e a gestão de informação. Estas disciplinas, embora distintas, devem ser integradas para enfrentar os complexos desafios do ambiente digital atual. Neste contexto, o Advanced Master em Secure Information Management representa uma oportunidade única para engenheiros e profissionais de informática interessados em adquirir uma visão integral que permita-lhes dominar ambas as áreas e se posicionar como líderes num setor em constante crescimento.

Numerosas empresas e instituições enfrentam a necessidade de proteger dados críticos e altamente sensíveis, mas carecem de especialistas que possam garantir uma administração, conservação e vigilância eficazes das suas informações digitais. Para responder a essa demanda, a TECH desenvolveu um programa que combina os melhores conteúdos com uma equipa docente de reconhecida trajetória profissional. Esta abordagem assegura que os alunos adquiram as ferramentas e os conhecimentos necessários para destacar-se no mercado de trabalho e aceder a cargos estratégicos em organizações que buscam reforçar a segurança da sua informação.

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

- O desenvolvimento de casos práticos apresentados por especialistas em Secure Information Management
- Os conteúdos gráficos, esquemáticos e eminentemente práticos, concebidos para oferecer uma informação científica e prática sobre as disciplinas indispensáveis para o exercício profissional
- Os exercícios práticos onde o processo de autoavaliação pode ser efetuado a fim de melhorar a aprendizagem
- O seu foco especial em metodologias inovadoras em Gestão Secure Informaction Management
- As lições teóricas, perguntas aos especialistas, fóruns de discussão sobre temas controversos e trabalhos de reflexão individual
- A disponibilidade de acesso aos conteúdos a partir de qualquer dispositivo fixo ou portátil com conexão à Internet

Adquira as competências necessárias para garantir a segurança e gerir eficazmente os dados em um ambiente digital competitivo”

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

Descubra a metodologia educativa mais inovadora desenvolvida pela TECH para garantir um aprendizado imersivo e contextualizado.

Aceda a um programa 100% online que lhe permite estudar no seu ritmo, a qualquer momento e de qualquer lugar do mundo.

Inclui em seu corpo docente profissionais provenientes da área das Finanças, que trazem para este programa a experiência adquirida em seu trabalho, além de reconhecidos especialistas de empresas de referência e universidades prestigiadas.

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

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

02

Porquê estudar na TECH?

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

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

A melhor universidade online do mundo segundo a FORBES

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

O melhor corpo docente top internacional

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

A maior universidade digital do mundo

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

Os planos de estudos mais completos do panorama universitário

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

Um método de aprendizagem único

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

A universidade online oficial da NBA

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

Líderes em empregabilidade

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

Google Partner Premier

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

A universidade mais bem classificada pelos seus alunos

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

03

Plano de estudos

Os materiais didáticos que compõem este Advanced Master em Secure Information Management foram elaborados por uma equipa de especialistas em cibersegurança e gestão de dados. Dessa forma, o plano de estudos aprofunda-se nas principais ameaças digitais e nas metodologias mais avançadas para a proteção e administração de informação. Isso permitirá aos egressos identificar riscos específicos e desenvolver soluções eficazes para garantir a segurança dos dados em diversos ambientes profissionais. Ademais, o conteúdo aborda as ferramentas mais inovadoras do setor, impulsionando estratégias destinadas a proteger os ativos digitais das organizações.

Contribuirá para a proteção de dados sensíveis 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 negócio
- 1.1.1. Análise de negócio
- 1.1.2. Estrutura do dado
- 1.1.3. Fases e elementos

1.2. Análise de dados na empresa
- 1.2.1. Painel de controlo 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. Serviço 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. IT

1.3. Marketing e comunicação
- 1.3.1. Kpi' s a medir, 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. Estratégia, previsão e gestão de campanhas

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

1.5. Serviço 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 estudos de mercado
- 1.6.2. Análise de dados para estudos de competência
- 1.6.3. Outras aplicações

1.7. Administração
- 1.7.1. Necessidades no 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. Aplicação analíticas de dados no departamento de RH

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

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

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

2.1. Estatística Variáveis, índices e rácios
- 2.1.1. A Estatística
- 2.1.2. Dimensões e estatísticas
- 2.1.3. Variáveis, índices e rácios

2.2. Tipologia do dado
- 2.2.1. Qualitativos
- 2.2.2. Quantitativo
- 2.2.3. Caraterização e categorias

2.3. Conhecimento dos dados a partir de medidas
- 2.3.1. Medidas de centralização
- 2.3.2. Medidas de dispersão
- 2.3.3. Correlação

2.4. Conhecimento dos dados a partir de gráficos
- 2.4.1. Visualização de acordo com o tipo de dados
- 2.4.2. Interpretação de informação gráfica
- 2.4.3. Customização de gráficos com R

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

2.6. Recolha de dados
- 2.6.1. Metodologia de recolha
- 2.6.2. Ferramentas de recolha
- 2.6.3. Canais de recolha

2.7. Limpeza de dados
- 2.7.1. Fases de 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. Indicadores de relação
- 2.8.3. Extração de dados

2.9. Armazém de dados (*Datawarehouse*)
- 2.9.1. Elementos
- 2.9.2. Design

2.10. Disponibilidade dos 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 de 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. Componentes principais
- 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 de dados e visualização

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

3.8. Aplicações de IoT
- 3.8.1. Cidades inteligentes
- 3.8.2. Saúde e condição física
- 3.8.3. Casa inteligente
- 3.8.4. Outras aplicações

3.9. Aplicações de 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. Fabrico aditivo 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 informação
- 4.1.2. O valor da representação gráfica
- 4.1.3. Novos paradigmas da representação gráfica

4.2. Otimização para a ciência dos dados
- 4.2.1. A Gama cromática e o design
- 4.2.2. A Gestalt na representação gráfica
- 4.2.3. Erros a evitar e conselhos

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. Ficheiros, listas e bases de dados
- 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 de blocos
- 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. Comparativas e relacional
- 4.6.2. Distribuição
- 4.6.3. Hierarquia

4.7. Conceção de relatórios com representação gráfica
- 4.7.1. Aplicação de gráficos em relatórios de Marketing
- 4.7.2. Aplicação de gráficos em paineis de controlo e Kpi' s
- 4.7.3. Aplicação de gráficos em planos estratégicos
- 4.7.4. Outros usos: ciência, saúde, negócios

4.8. Narração gráfica
- 4.8.1. A narração gráfica
- 4.8.2. Evolução
- 4.8.3. Utilidade

4.9. Ferramentas orientadas para a 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 a virtualização da realidade
- 4.10.2. Sistemas para aumento e melhoria da realidade
- 4.10.3. Sistemas inteligentes

Módulo 5. Ferramentas de ciência de dados

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

5.2. Dados, informação e conhecimento
- 5.2.1. Dados, informação e conhecimento
- 5.2.2. Tipos de dados
- 5.2.3. Fontes de dados

5.3. Dos dados à informação
- 5.3.1. Análise de dados
- 5.3.2. Tipos de análise
- 5.3.3. Extração de informação de um *Dataset*

5.4. Extração de informação 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 do 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 boas práticas
- 5.10.1. Boas práticas para um cientista de dados
- 5.10.2. O melhor modelo
- 5.10.3. Ferramentas úteis

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

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

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

6.3. Preparação de 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 aprendizagem automática

6.5. O ruído dos dados
- 6.5.1. Classes de ruído e atributos
- 6.5.2. Filtragem de ruído
- 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 dados discretos
- 6.7.2. Processo de discretização

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

6.9. Seleção de instâncias
- 6.9.1. Métodos para a seleção de instâncias
- 6.9.2. Seleção de protótipos
- 6.9.3. Métodos avançados para a 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 fenómenos estocásticos

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

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

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

7.4. Esquemas para séries temporais
- 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. Media
- 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 temporais
- 7.7.1. ANOVA
- 7.7.2. Fundamentos
- 7.7.3. Aplicação prática

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

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

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

Módulo 8. Conceção 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. Extração de dados

8.2. Aprendizagem automática
- 8.2.1. Aprendizagem supervisionada e não supervisionada
- 8.2.2. Aprendizagem por reforço
- 8.2.3. Outros paradigmas de aprendizagem

8.3. Algoritmos de classificação
- 8.3.1. Aprendizagem Automática Indutiva
- 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 temporais
- 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 parcial
- 8.5.3. Métricas e pontuações para *clustering*

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

8.7. Técnicas de classificação avançadas. Multiclassificadores
- 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. Aprendizagem automática com redes neuronais artificiais
- 8.9.2. Redes *feedforward*

8.10. Aprendizagem profunda
- 8.10.1. Redes *feedforward* profundas
- 8.10.2. Redes neuronais convolucionais e modelos sequenciais
- 8.10.3. Ferramentas para implementação de redes neuronais profundas

Módulo 9. Arquiteturas e sistemas para uso intensivo de dados

9.1. Requisitos não funcionais. Pilares das aplicações de dados massivos
- 9.1.1. Fiabilidade
- 9.1.2. Adaptabilidade
- 9.1.3. Mantenibilidade

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

9.3. Bases de dados. Gestão do armazenamento e recuperação de dados
  9.3.1. Índices hash
  9.3.2. Armazenamento estruturado em log
  9.3.3. Árvores B
9.4. Formatos de codificação de dados
  9.4.1. Formatos específicos da linguagem
  9.4.2. Formatos estandardizados
  9.4.3. Formatos de codificação binários
  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 de índice secundário e particionado
  9.7.3. Reequilíbrio de partições
9.8. Processamento de dados *offline*
  9.8.1. Processamento por lotes
  9.8.2. Sistemas de ficheiros 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 bases de dados como fluxos de dados
  9.9.3. Processamento de fluxos de dados
9.10. Aplicações práticas na empresa
  9.10.1. Consistência nas leituras
  9.10.2. Abordagem holística dos dados
  9.10.3. Dimensionamento de um serviço distribuído

Módulo 10. Aplicação prática da ciência dos dados nos setores de atividade empresarial

10.1. Setor da saúde
  10.1.1. Implicações da IA e da análise de dados no setor da saúde
  10.1.2. Oportunidades e desafios
10.2. Riscos e tendências no setor da saúde
  10.2.1. Uso no setor da saúde
  10.2.2. Potenciais riscos relacionados com a utilização de IA
10.3. Serviços financeiros
  10.3.1. Implicações da IA e da análise de dados no setor dos serviços financeiros
  10.3.2. Uso nos serviços financeiros
  10.3.3. Potenciais riscos relacionados com a utilização de IA
10.4. Retail
  10.4.1. Implicações da IA e da análise de dados no setor do Retail
  10.4.2. Uso no retail
  10.4.3. Potenciais riscos relacionados com a utilização 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. Potenciais riscos relacionados com a utilização 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. Potenciais riscos relacionados com a utilização de IA
10.8. Educação
  10.8.1. Implicações da IA e da análise de dados na Educação
  10.8.2. Potenciais riscos relacionados com a utilização 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 na silvicultura e agricultura
  10.9.3. Potenciais riscos relacionados com a utilização 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. Potenciais riscos relacionados com a utilização de IA

Módulo 11. Ciberinteligência e cibersegurança

11.1. Ciberinteligência
- 11.1.1. Ciberinteligência
  - 11.1.1.1. A inteligência
    - 11.1.1.1.1. Ciclo de inteligência
  - 11.1.1.2. Ciberinteligência
  - 11.1.1.3. Ciberinteligência e cibersegurança
- 11.1.2. O Analista de Inteligência
  - 11.1.2.1. O papel do analista de inteligência
  - 11.1.2.2. Os enviesamentos do analista de inteligência na atividade avaliativa

11.2. Cibersegurança
- 11.2.1. As camadas de segurança
- 11.2.2. Identificação das ciberameaças
  - 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 mais utilizados

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

11.4. Metodologias de avaliação
- 11.4.1. A análise de inteligência
- 11.4.2. Técnicas de organização da informação adquirida
- 11.4.3. Fiabilidade 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. A auditoria na segurança informática
- 11.5.2. Documentação e autorizações para auditoria
- 11.5.3. Tipos de auditoria
- 11.5.4. Resultados
  - 11.5.4.1. Relatório técnico
  - 11.5.4.2. Relatório executivo

11.6. Anonimato na rede
- 11.6.1. Utilização do anonimato
- 11.6.2. Técnicas de anonimato (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 nas redes
- 11.7.4. Segurança lógica
- 11.7.5. Segurança em aplicações web
- 11.7.6. Segurança em dispositivos móveis

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

11.9. Análise de riscos e métricas
- 11.9.1. Alcance de riscos
- 11.9.2. Os ativos
- 11.9.3. As ameaças
- 11.9.4. As vulnerabilidades
- 11.9.5. Avaliação do risco
- 11.9.6. Tratamento do risco

11.10. Organismos importantes em matéria de cibersegurança
- 11.10.1. NIST
- 11.10.2. ENISA
- 11.10.3. INCIBE
- 11.10.4. OEA
- 11.10.5. UNASUR - PROSUR

Módulo 12. Segurança em host

12.1. Cópias de segurança
- 12.1.1. Estratégia para as cópias de segurança
- 12.1.2. Ferramentas para Windows
- 12.1.3. Ferramentas para Linux
- 12.1.4. Ferramentas para MacOS

12.2. Antivírus do utilizador
- 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. Detetores de intrusos - HIDS
- 12.3.1. Métodos de deteção de intrusos
- 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 palavras-passe
- 12.5.1. *Password*
- 12.5.2. *LastPass*
- 12.5.3. *KeePass*
- 12.5.4. *StickyPassword*
- 12.5.5. *RoboForm*

12.6. Detetores de *phishing*
- 12.6.1. Deteção de *phishing* de forma manual
- 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 anti-rastreamento

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. Controlo 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 atualizações
- 12.10.4. Privilégios para instalar software

Módulo 13. Segurança na rede (Perimetral)

13.1. Sistemas de deteção e prevenção de ameaças
- 13.1.1. Quadro geral dos incidentes de segurança
- 13.1.2. Sistemas de defesa atuais*: Defense in Depth* e SOC
- 13.1.3. Arquiteturas de rede atuais
- 13.1.4. Tipos de ferramentas para a deteção 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*, contentores e *serverless*

13.2. *Firewall*
- 13.2.1. Tipos de *firewalls*
- 13.2.2. Ataques e mitigação
- 13.2.3. *Firewalls* comuns em kernel Linux
  - 13.2.3.1. UFW
  - 13.2.3.2. Nftables e iptables
  - 13.2.3.3. *Firewalls*

13.2.4. Sistemas de deteção 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 deteção e prevenção de intrusões (IDS/IPS)
13.3.1. Ataques sobre IDS/IPS
13.3.2. Sistemas de IDS/IPS
13.3.2.1. *Snort*
13.3.2.2. Suricata
13.4. *Firewalls* da próxima geração (NGFW)
13.4.1. Diferenças entre NGFW e firewalls tradicionais
13.4.2. Capacidades principais
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 de antivírus
13.6.1. Contexto geral do *Malware* e IOCs
13.6.2. Problemas dos motores de antivírus
13.7. Sistemas de proteção de correio eletrónico
13.7.1. Antispam
13.7.1.1. Listas brancas e negras
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 utilização
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 y HoneyNets
- 13.10.4. CASB

Módulo 14. Segurança em 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 da 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 meio empresarial
- 14.3.1. Riscos
- 14.3.2. Políticas de segurança
- 14.3.3. Monitorização de dispositivos
- 14.3.4. Gestão de dispositivos móveis (MDM)

14.4. Privacidade do utilizador e segurança de dados
- 14.4.1. Estados da informação
- 14.4.2. Proteção e confidencialidade dos dados
  - 14.4.2.1. Autorizações
  - 14.4.2.2. Encriptação
- 14.4.3. Armazenamento seguro dos dados
  - 14.4.3.1. Armazenamento seguro em 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 dos dados

14.6. Principais ameaças
- 14.6.1. Utilizador não forçado
- 14.6.2. *Malware*
  - 14.6.2.1. Tipos de *Malware*
- 14.6.3. Engenharia social
- 14.6.4. Fuga de dados
- 14.6.5. Roubo de informação
- 14.6.6. Redes *Wi-Fi* não seguras
- 14.6.7. Software desatualizado
- 14.6.8. Aplicações maliciosas
- 14.6.9. Palavras-passe 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. Suplantação de identidade (Integridade)
- 14.6.14. Criptografia fraca ou danificada
- 14.6.15. Denegação de Serviços (DoS)

14.7. Principais ataques
- 14.7.1. Ataques de *phishing*
- 14.7.2. Ataques relacionados com os 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 do *Payload* e extração da informação
- 14.8.3. *Hacking* em dispositivos iOS: mecanismos e ferramentas
- 14.8.4. *Hacking* em dispositivos Android: mecanismos e ferramentas

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

14.10. Proteção e segurança
- 14.10.1. Configuração de segurança
  - 14.10.1.1. Em dispositivos iOS
  - 14.10.1.2. Em dispositivos Android
- 14.10.2. Medidas de segurança
- 14.10.3. Ferramentas de proteção

Módulo 15. Segurança em IoT

15.1. Dispositivos
- 15.1.1. Tipos de dispositivos
- 15.1.2. Arquiteturas standardizadas
  - 15.1.2.1. ONEM2M
  - 15.1.2.2. IoTWF
- 15.1.3. Protocolos de aplicação
- 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 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. Domótica
- 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. Realização de pagamentos e obtenção de serviços
- 15.6.3. Conectividade

15.7. *Wearables*
- 15.7.1. Roupa inteligente
- 15.7.2. Jóias inteligentes
- 15.7.3. Relógios inteligentes

15.8. Setor Saúde
- 15.8.1. Monitorização de exercício/ritmo cardíaco
- 15.8.2. Acompanhamento de doentes e pessoas idosas
- 15.8.3. Implantáveis
- 15.8.4. Robôs cirúrgicos

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

15.10. Securitização
- 15.10.1. Redes dedicadas
- 15.10.2. Gestor de palavras-passe
- 15.10.3. Utilização de protocolos encriptados
- 15.10.4. Conselhos de utilização

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. Implementação 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 fontes abertas (OSINT)
- 16.3.2. Pesquisa de falhas e vulnerabilidades de dados
- 16.3.3. Utilização de ferramentas passivas

16.4. Verificação de redes
- 16.4.1. Ferramentas de verificação
  - 16.4.1.1. Nmap
  - 16.4.1.2. Hping3
  - 16.4.1.3. Outras ferramentas de verificação
- 16.4.2. Técnicas de verificação
- 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 de NetBIOS e Samba
- 16.5.4. Enumeração de LDAP
- 16.5.5. Enumeração de 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 vulnerabilidades
  - 16.6.2.1. CVSS
  - 16.6.2.2. CVE
  - 16.6.2.3. NVD

16.7. Ataques a redes *inalámbricas*
- 16.7.1. Metodologia de *hacking* em redes inalámbricas
  - 16.7.1.1. Wi-Fi Discovery
  - 16.7.1.2. Análise de tráfico
  - 16.7.1.3. Ataques do *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 segurança sem fios

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

16.9. Exploração de vulnerabilidades
- 16.9.1. Utilização de *exploits* conhecidos
- 16.9.2. Utilização de *metasploit*
- 16.9.3. Utilização de *malware*
  - 16.9.3.1. Definição e alcance
  - 16.9.3.2. Geração de *malware*
  - 16.9.3.3. Bypass de soluções antivírus

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

Módulo 17. Engenharia reversa

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. Gestor de erros
- 17.1.5. Compilador GCC

17.2. Tipos de análise em compiladores
- 17.2.1. Análise léxica
  - 17.2.1.1. Terminologia
  - 17.2.1.2. Componentes léxicos
  - 17.2.1.3. Analisador léxico LEX
- 17.2.2. Análise sintático
  - 17.2.2.1. Gramáticas livres de contexto
  - 17.2.2.2. Tipos de análise sintáticos
    - 17.2.2.2.1. Análise descendente
    - 17.2.2.2.2. Análise ascendente
  - 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. Analisadores 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 código 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. Utilização do break
- 17.4.3. Funções

17.5. Arquitetura Hardware x86
- 17.5.1. Arquitetura de processadores x86
- 17.5.2. Estruturas de dados em x86
- 17.5.3. Estruturas de código em x86

17.6. Arquitetura Hardware ARM
- 17.6.1. Arquitetura de processadores ARM
- 17.6.2. Estruturas de dados em ARM
- 17.6.3. Estruturas de código em 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 dinâmico
- 17.8.1. Análise de comportamento
  - 17.8.1.1. Comunicações
  - 17.8.1.2. Monitorização
- 17.8.2. Depuradores de código em Linux
- 17.8.3. Depuradores de código em Windows

17.9. *Sandbox*
- 17.9.1. Arquitetura de um *Sandbox*
- 17.9.2. Evasão de um *Sandbox*
- 17.9.3. Técnicas de deteção
- 17.9.4. Técnicas de evasão
- 17.9.5. Contramedidas
- 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 de executáveis
  - 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 da programação de software

18.2. Fase de Requisitos
- 18.2.1. Controlo da autenticação
- 18.2.2. Controlo de papéis e privilégios
- 18.2.3. Requisitos orientados para o risco
- 18.2.4. Aprovação de privilégios

18.3. Fases de análise e design
- 18.3.1. Acesso a componentes e administração do sistema
- 18.3.2. Pistas de auditoria
- 18.3.3. Gestão de sessões
- 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. Garantia do ambiente de desenvolvimento
- 18.4.2. Elaboração da documentação técnica
- 18.4.3. Codificação segura
- 18.4.4. Segurança nas comunicações

18.5. Boas práticas de codificação segura
- 18.5.1. Validação de dados de entrada
- 18.5.2. Codificação dos dados de saída
- 18.5.3. Estilo de programação
- 18.5.4. Gestão do registo de alterações
- 18.5.5. Práticas criptográficas
- 18.5.6. Gestão de erros e logs
- 18.5.7. Gestão de ficheiros
- 18.5.8. Gestão de memória
- 18.5.9. Padronização e reutilização das funções de segurança

18.6. Preparação do servidor e *Hardening*
- 18.6.1. Gestão de utilizadores, grupos e papéis no servidor
- 18.6.2. Instalação de software
- 18.6.3. *Hardening* do servidor
- 18.6.4. Configuração robusta do ambiente da aplicação

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

18.8. Fase de testes
- 18.8.1. Controlo de qualidade nos controlos de segurança
- 18.8.2. Inspeção do código por fases
- 18.8.3. Comprovação da gestão das configurações
- 18.8.4. Testes de caixa negra

18.9. Preparação da transição à produção
- 18.9.1. Realizar o controlo de alterações
- 18.9.2. Realizar o procedimento de passagem à produção
- 18.9.3. Realizar procedimento de *rollback*
- 18.9.4. Testes em fase de pré-produção

18.10. Fase de manutenção
- 18.10.1. Garantia baseada no risco
- 18.10.2. Testes de manutenção de segurança da caixa branca
- 18.10.3. Testes de manutenção de segurança da caixa negra

Módulo 19. Análise forense

19.1. Aquisição de dados e duplicação
- 19.1.1. Aquisição de dados voláteis
  - 19.1.1.1. Informação do sistema
  - 19.1.1.2. Informação da rede
  - 19.1.1.3. Ordem de volatilidade
- 19.1.2. Aquisição de dados estáticos
  - 19.1.2.1. Criação de uma imagem duplicada
  - 19.1.2.2. Preparação de um documento para a 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 de técnicas antiforenses
- 19.2.1. Objetivos das técnicas antiforenses
- 19.2.2. Eliminação de dados
  - 19.2.2.1. Eliminação de dados e ficheiros
  - 19.2.2.2. Recuperação de ficheiros
  - 19.2.2.3. Recuperação de partições apagadas
- 19.2.3. Proteção com palavra-passe
- 19.2.4. Esteganografia
- 19.2.5. Limpeza segura de dispositivos
- 19.2.6. Encriptação

19.3. Análise forense do sistema operativo
- 19.3.1. Análise forense de Windows
- 19.3.2. Análise forense de Linux
- 19.3.3. Análise forense de Mac

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

19.5. Análise forense Web
- 19.5.1. Investigação de ataques na web
- 19.5.2. Deteção de ataques
- 19.5.3. Localização de direções IPs

19.6. Análise forense de bases de dados
- 19.6.1. Análise forense em MSSQL
- 19.6.2. Análise forense em MySQL
- 19.6.3. Análise forense em PostgreSQL
- 19.6.4. Análise forense em MongoDB

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 sobre os serviços de armazenamento na *cloud*
- 19.7.4. Ferramentas de análise forense para *cloud*

19.8. Investigação de crimes por correio eletrónico
- 19.8.1. Sistemas de correio eletrónico
  - 19.8.1.1. Clientes de correio eletrónico
  - 19.8.1.2. Servidor de correio eletrónico
  - 19.8.1.3. Servidor SMTP
  - 19.8.1.4. Servidor POP3
  - 19.8.1.5. Servidor IMAP4
- 19.8.2. Crimes de correio eletrónico
- 19.8.3. Mensagem de correio eletrónico
  - 19.8.3.1. Cabeçalhos standard
  - 19.8.3.2. Cabeçalhos extendidos
- 19.8.4. Passos na investigação destes crimes
- 19.8.5. Ferramentas forenses para correio eletrónico

19.9. Análise forense de telemóveis
- 19.9.1. Redes celulares
  - 19.9.1.1. Tipos de redes
  - 19.9.1.2. Conteúdos 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 ficheiros

19.10. Redação e apresentação de relatórios forenses
- 19.10.1. Aspetos 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. Lidar com os meios de comunicação social

Módulo 20. Desafios atuais e futuros em segurança informática

20.1. Tecnologia *blockchain*
- 20.1.1. Domínios de aplicação
- 20.1.2. Garantia de confidencialidade
- 20.1.3. Garantia de não repúdio

20.2. Dinheiro digital
- 20.2.1. Bitcoins
- 20.2.2. Criptomoedas
- 20.2.3. Exploração de criptomoedas
- 20.2.4. Esquemas em pirâmide
- 20.2.5. Outros potenciais delitos e problemas

20.3. *Deepfake*
- 20.3.1. Impacto nos meios de comunicação social
- 20.3.2. Perigos para a sociedade
- 20.3.3. Mecanismos de deteção

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

20.5. Privacidade digital
- 20.5.1. Valor dos dados na rede
- 20.5.2. Utilização dos dados na rede
- 20.5.3. Gestão da privacidade e da identidade digital

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

20.7. Teletrabalho
- 20.7.1. Revolução do teletrabalho durante e após a Covid19
- 20.7.2. Obstáculos no acesso
- 20.7.3. Variação da superfície de ataque
- 20.7.4. 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* em vez 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 em relação ao IPv4

20.10. O desafio da sensibilização para a formação precoce e contínua da população
- 20.10.1. Estratégias governamentais atuais
- 20.10.2. Resistência da população à aprendizagem
- 20.10.3. Planos de formação a serem adotados pelas empresas

Aprenderá através de casos reais concebidos em ambientes de aprendizagem simulados que refletem os desafios atuais da gestão de dados e da cibersegurança”

04

Objetivos de ensino

O objetivo principal do Advanced Master em Secure Information Management é proporcionar aos alunos conhecimentos de excelência em duas áreas fundamentais e complementares da informática e das engenharias: a gestão de dados em ambientes digitais e a cibersegurança. Este programa combina ambas disciplinas para capacitar profissionais na implementação de soluções avançadas, permitindo-lhes enfrentar desafios profissionais com as ferramentas necessárias para administrar e proteger informações sensíveis nas suas organizações.

Transforme a sua carreira profissional com este Advanced Master inovador, desenhado para marcar uma mudança significativa na sua especialização em gestão de dados e cibersegurança"

Objetivos gerais

- Desenvolver conhecimentos avançados em análise de dados e cibersegurança para otimizar processos empresariais com ferramentas e técnicas inovadoras
- Implementar estratégias de segurança eficazes para prevenir ameaças digitais em sistemas, redes e dispositivos móveis
- Resolver desafios em cibersegurança através de auditorias, engenharia reversa e análise forense baseada em provas
- Antecipar tendências tecnológicas aplicando soluções inovadoras que protejam ativos digitais e sistemas avançados

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

Objetivos específicos

Módulo 1. Análise de dados na organização empresarial

- Desenvolver competências na utilização de técnicas de análise de dados
- Gerar informações valiosas que impulsionem a tomada de decisões estratégicas nas organizações empresariais, melhorando a eficiência e a competitividade

Módulo 2. Gestão, manipulação de dados e informação para a Ciência de Dados

- Capacitar na gestão e manipulação eficiente 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 dos Dados

- Fornecer os conhecimentos necessários sobre as plataformas e dispositivos da Internet das Coisas e a sua integração na ciência de dados
- Aprofundar na captura, processamento e análise de dados em tempo real

Módulo 4. Representação gráfica para análise de dados

- Representar graficamente os dados através de ferramentas e técnicas avançadas de visualização
- Facilitar a compreensão de padrões, tendências e relações dentro de grandes conjuntos de dados

Módulo 5. Ferramentas de ciência de dados

- Capacitar no uso de ferramentas e software específicos de ciência de dados, como Python
- Aprofundar na coleta, análise e apresentação de dados em diversos contextos profissionais

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

- Fornecer os conhecimentos e habilidades necessários para aplicar técnicas de extração de dados
- Analisar a seleção, o pré-processamento e a transformação de dados para extrair padrões e tendências significativas

Módulo 7. Previsibilidade e análise de fenómenos estocásticos

- Desenvolver competências na modelagem e análise de fenômenos estocásticos
- Utilizar métodos estatísticos avançados para prever comportamentos e tendências em ambientes incertos e dinâmicos

Módulo 8. Design e desenvolvimento de sistemas inteligentes

- Capacitar no design e desenvolvimento de sistemas inteligentes, integrando técnicas de aprendizado de máquina e inteligência artificial
- Criar soluções automáticas que resolvam problemas complexos de maneira eficiente

Módulo 9. Arquiteturas e sistemas para uso intensivo de dados

- Fornecer conhecimentos sobre a criação de arquiteturas de sistemas capazes de processar grandes volumes de dados de maneira eficiente
- Utilizar tecnologias avançadas, como bases de dados distribuídas e processamento paralelo

Módulo 10. Aplicação prática da ciência dos dados nos setores de atividade empresarial

- Desenvolver a capacidade de aplicar práticas de ciência de dados em diversos setores empresariais
- Integrar os conhecimentos adquiridos para melhorar a tomada de decisões, a otimização de processos e a inovação na empresa

Módulo 11. Ciberinteligência e cibersegurança
- Fornecer os conhecimentos e habilidades necessários para aplicar técnicas de ciberinteligência e cibersegurança
- Proteger os sistemas e redes empresariais contra ameaças cibernéticas e garantir a integridade dos dados

Módulo 12. Segurança em Host
- Capacitar na Implementação de medidas de segurança em sistemas host
- Assegurar a proteção de servidores e aplicações críticas através do uso de ferramentas e boas práticas de segurança informática

Módulo 13. Segurança na rede (perimetral)
- Proporcionar conhecimentos sobre a proteção de redes e sistemas informáticos a nível perimetral
- Gerir cortafogos, VPNs e outras ferramentas para garantir a segurança na infraestrutura de rede da empresa

Módulo 14. Segurança em Smartphones
- Desenvolver competências para assegurar a segurança em dispositivos móveis
- Compreender as vulnerabilidades comuns e aplicar medidas preventivas para proteger a informação e as aplicações em smartphones

Módulo 15. Segurança em IoT
- Proporcionar os conhecimentos necessários para implementar soluções de segurança em dispositivos IoT
- Proteger redes e sistemas que interconectam dispositivos, garantindo a confidencialidade e integridade dos dados gerados

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

Módulo 17. Engenharia reversa
- Proporcionar conhecimentos sobre técnicas de engenharia reversa, permitindo analisar e compreender o funcionamento de software e hardware
- Detetar falhas de segurança ou melhorar a funcionalidade dos sistemas existentes

Módulo 18. Desenvolvimento seguro
- Capacitar no desenvolvimento de software seguro, ensinando boas práticas de codificação e segurança durante o ciclo de vida do software
- Ser capaz de prevenir vulnerabilidades e proteger os sistemas informáticos contra ataques

Módulo 19. Análise forense
- Desenvolver as competências necessárias para realizar investigações forenses digitais
- Utilizar ferramentas e técnicas avançadas para recuperar, analisar e preservar provas eletrónicas em incidentes de segurança informática

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

05

Oportunidades de carreira

Após concluir este Advanced Master em Secure Information Management, os profissionais terão adquirido uma compreensão sólida das estratégias mais avançadas em cibersegurança e gestão de dados digitais. Os alunos estarão preparados para desenhar e implementar soluções que garantam a proteção da informação sensível e otimizem os processos de análise e tomada de decisões em ambientes empresariais. Dessa forma, melhorarão as suas perspetivas profissionais e assumir-se-ão em papéis especializados como analistas de cibersegurança, consultores de inteligência ou gestores de dados críticos.

Garantirá a segurança dos ativos digitais e será uma peça chave na transformação digital das organizações"

Perfil dos nossos alunos

O aluno do Advanced Master em Secure Information Management será um profissional altamente capacitado para gerir e proteger informações em ambientes digitais. Possuirá um conhecimento avançado em áreas como cibersegurança, inteligência digital e análise de dados, além de competências práticas no desenho e implementação de estratégias de defesa contra ameaças. O seu perfil combina um entendimento técnico profundo com competências estratégicas que lhe permitirão liderar projetos em setores empresariais chave.

Tornar-se-á um líder na proteção de dados e cibersegurança, colaborando com empresas para enfrentar os desafios do ambiente digital.

- **Gestão da segurança:** Desenvolverá a capacidade de identificar riscos, implementar estratégias de defesa multicamada e garantir a confidencialidade, integridade e disponibilidade dos dados.
- **Análise crítica e resolução de problemas:** Aplicará técnicas avançadas para avaliar sistemas, detetar vulnerabilidades e desenhar soluções adaptadas a diferentes ambientes tecnológicos.
- **Competência técnica e digital:** Gerirá ferramentas avançadas de análise de dados, cibersegurança e sistemas de inteligência, permitindo-lhe liderar projetos de inovação tecnológica.
- **Pensamento estratégico:** Desenhará políticas de segurança e estratégias empresariais que respondam às exigências atuais e futuras do ambiente digital.
- **Colaboração interdisciplinar:** Trabalhará com equipas multidisciplinares para abordar desafios complexos e garantir a segurança em redes, plataformas IoT e dispositivos móveis.

Depois de concluir o Advanced Master, poderá aplicar os seus conhecimentos e competências nos seguintes cargos:

1. **Diretor de Cibersegurança:** Líder responsável por coordenar equipas e desenhar estratégias para proteger ativos digitais em grandes organizações
2. **Analista de Dados:** Designer de análises preditivas e sistemas de visualização para otimizar a tomada de decisões
3. **Consultor em Inteligência Digital:** Consultor especializado em oferecer soluções avançadas baseadas em inteligência e análise de riscos
4. **Especialista em IoT e Segurança:** Designer de medidas de proteção para dispositivos conectados e ambientes industriais.
5. **Hacker Ético:** Avaliador de vulnerabilidades que corrige falhas em sistemas empresariais para prevenir ciberataques.
6. **Auditor de Segurança:** Inspetor que realiza auditorias e análises forenses para garantir o cumprimento das normas.
7. **Gestor de Dados Empresariais:** Administrador responsável por desenhar e gerir sistemas de armazenamento e análise para melhorar a eficiência operacional.

Complete este programa e destaque-se como 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.

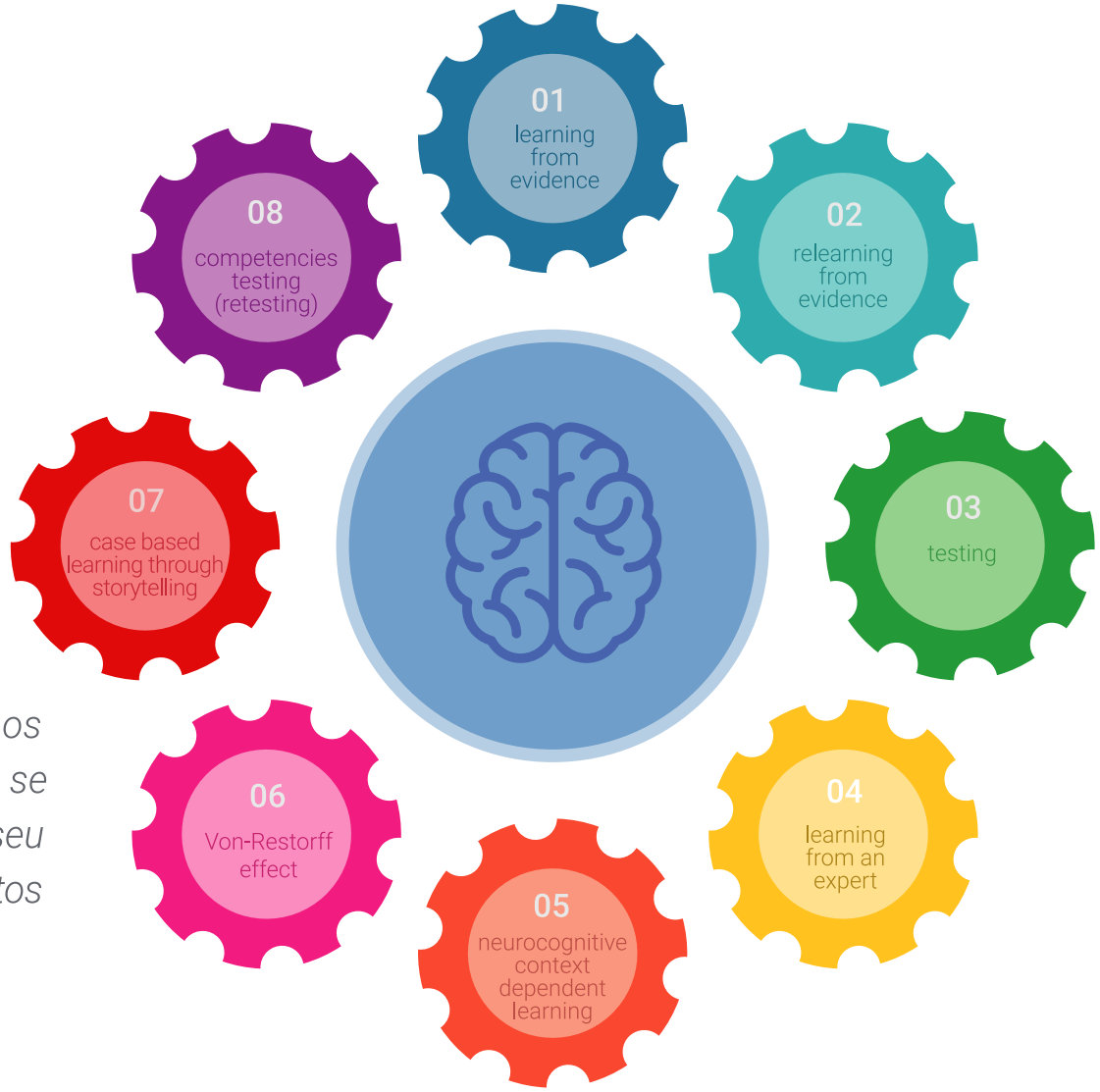
Esse método orientado para a ação será aplicado em toda a trajetória acadêmica do aluno com a TECH. Dessa forma, o aluno será confrontado com várias situações da vida real e terá de integrar conhecimentos, pesquisar, argumentar e defender suas ideias e decisões. A premissa era responder à pergunta sobre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

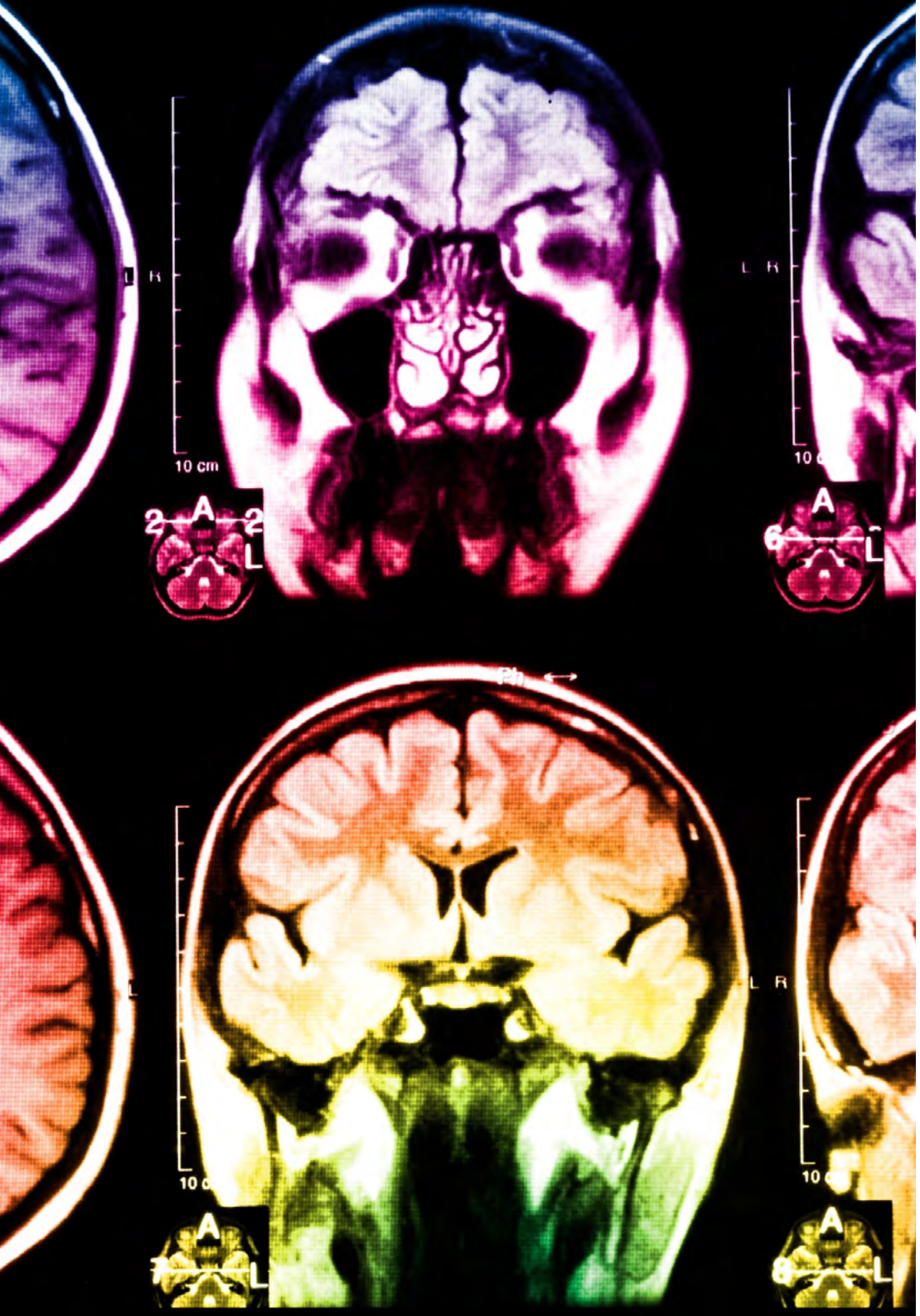
Por outro lado, também para favorecer ao máximo o contato entre mentor e mentorado, é oferecida uma ampla variedade de possibilidades de comunicação, tanto em tempo real quanto em diferido (mensagens internas, fóruns de discussão, serviço telefônico, contato por e-mail com a secretaria técnica, bate-papo,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

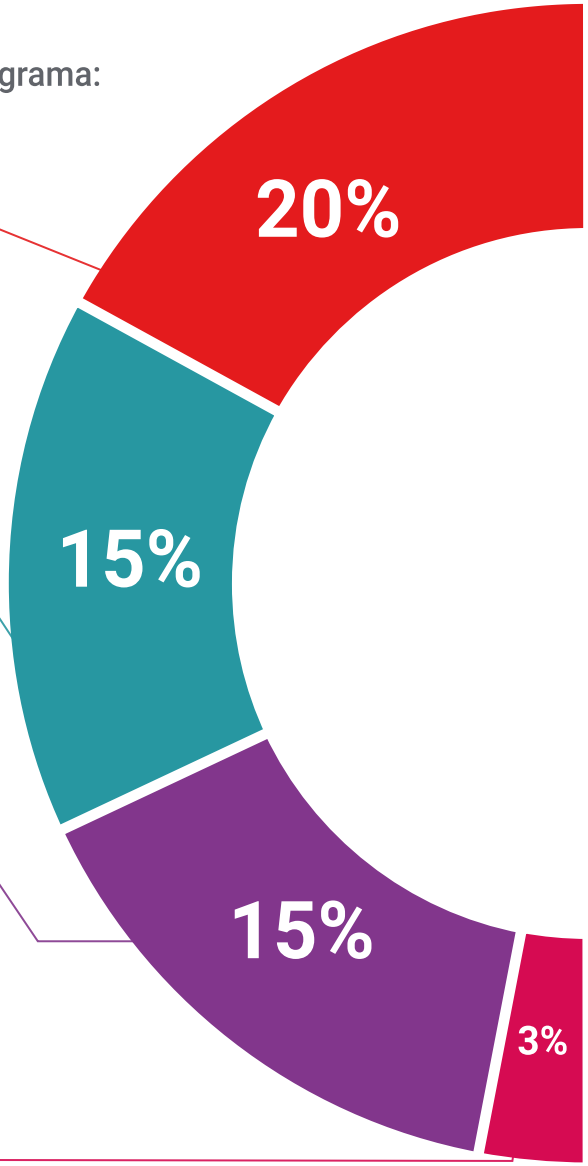
Resumos interativos

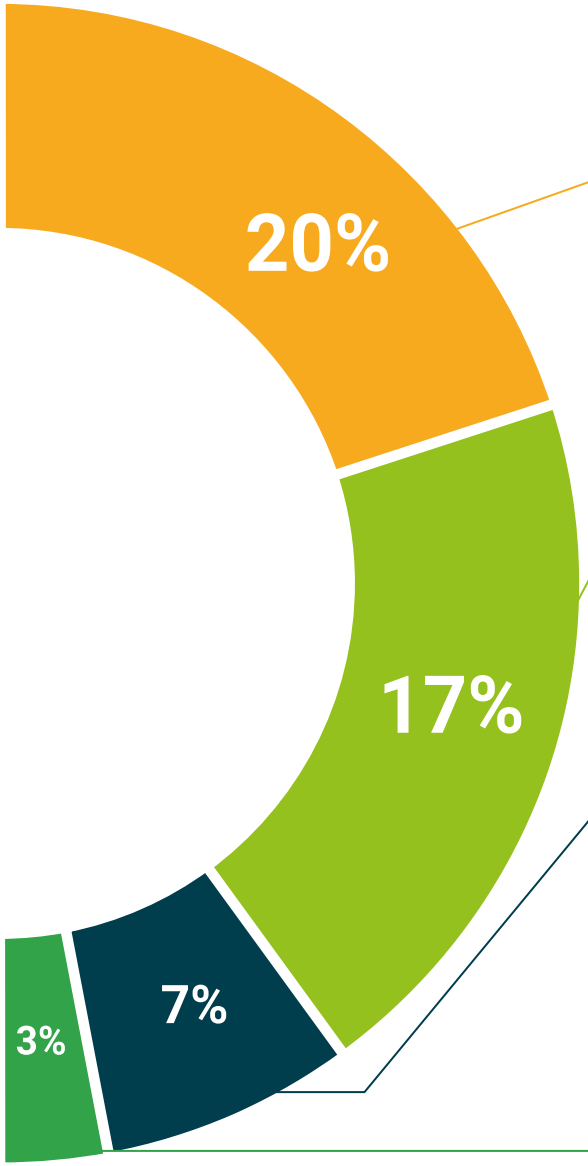
Apresentamos os conteúdos de forma atraente e dinâmica em pílulas multimídia que incluem áudio, vídeos, imagens, diagramas e mapas conceituais com o objetivo de reforçar o conhecimento.

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

Corpo docente

Esta qualificação é ministrada por destacados profissionais em cibersegurança e gestão digital de dados. A sua experiência garante que os alunos recebam conteúdos completos e atualizados, diretamente aplicáveis nas suas carreiras. Dessa forma, os docentes deste Advanced Master em Secure Information Management partilham os seus conhecimentos, formando especialistas altamente qualificados e procurados por grandes empresas a nível internacional.

Triunfe ao lado dos melhores e adquira os conhecimentos e competências chave para liderar na gestão de dados e cibersegurança no ambiente digital"

Diretor Internacional Convidado

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

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

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

Sr. Lemieux, Frederic

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

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

Direção

Dr. Peralta Martín-Palomino, Arturo

- CEO e CTO, Prometeus Global Solutions
- CTO em Korporate Technologies
- CTO em AI Shepherds GmbH
- Consultor e Assessor Empresarial Estratégico na Alliance Medical
- Diretor de Design e Desenvolvimento na DocPath
- Doutoramento em Engenharia Informática pela Universidade de Castilla-La Mancha
- Doutoramento em Economia, Empresas e Finanças pela Universidade Camilo José Cela
- Doutoramento 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 pela Formação Hadoop
- Mestrado em Tecnologias Avançadas de Informação da Universidade de Castilla-La Mancha
- Miembro do Grupo de Investigação SMILE

Sra. Fernández Sapena, Sonia

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

Professores

Sr. Montoro Montarroso, Andrés

- Investigador no grupo SMILe, Universidade de Castilla-La Mancha
- Investigador na Universidade de Granada
- Cientista de Dados na Prometeus Global Solutions
- Vice-presidente e Software Developer na CireBits
- Doutoramento em Tecnologias Informáticas Avançadas pela Universidade de Castilla-La Mancha
- Licenciatura em Engenharia Informática pela Universidade de Castilla-La Mancha
- Mestrado em Ciência de Dados e Engenharia de Computadores pela Universidade de Granada
- Professor convidado na disciplina de Sistemas Baseados em Conhecimento da Escola Superior de Informática de Ciudad Real, ministrando a conferência: *Técnicas Avançadas de Inteligência Artificial: Pesquisa e análise de potenciais radicais em Mídias Sociais*
- Professor convidado na disciplina de Mineração de Dados da Escola Superior de Informática de Ciudad Real, ministrando a conferência: *Aplicações do Processamento de Linguagem Natural: Lógica fuzzy na análise de mensagens em redes sociais*
- Palestrante no Seminário sobre Prevenção da Corrupção nas Administrações Públicas e Inteligência Artificial da Faculdade de Ciências Jurídicas e Sociais de Toledo, ministrando a conferência: *Técnicas de Inteligência Artificial*
- Palestrante no primeiro Seminário Internacional de Direito Administrativo e Inteligência Artificial (DAIA). Organizado pelo Centro de Estudos Europeus Luis Ortega Álvarez e pelo Institut de Recerca TransJus. Conferência intitulada *Análise de Sentimentos para a prevenção de mensagens de ódio nas redes sociais*

Sr. Peris Morillo, Luis Javier

- Senior Technical Lead e Delivery Lead Support na HCL Technologies
- Redator 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 em ARCO
- Licenciatura em Engenharia Superior em Informática pela Universidade de Castilla-La Mancha
- Pós-graduado em Gestão de Projetos pela CEOE

Sra. Fernández Meléndez, Galina

- Especialista em Big Data
- Analista de Dados na Aresi Gestão de Fincas
- Analista de Dados na ADN Mobile Solution
- Licenciatura em Administração de Empresas pela Universidade Bicentenária de Aragua. Caracas, Venezuela
- Curso 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 pela Escola de Negócios Europeia de Barcelona

Sra. Pedrajas Perabá, María Elena

- New Technologies and Digital Transformation Consultant en Management Solutions
- Investigadora no Departamento de Informática e Análise Numérica na Universidade de Córdoba
- Investigadora no Centro Singular de Investigação em Tecnologias Inteligentes em Santiago de Compostela
- Licenciatura em Engenharia Informática pela Universidade de Córdoba
- Mestrado em Ciência de Dados e Engenharia de Computadores pela Universidade de Granada
- Mestrado em Consultoria de Negócios pela Universidade Pontifícia Comillas

Sra. Yésica Martínez Cerrato

- Responsável de Formações Técnicas na Securitas Seguridad Espanha
- Especialista em Educação, Negócios e Marketing
- *Product Manager* de Segurança Eletrónica na Securitas Seguridad Espanha
- Analista de inteligência Empresarial na Ricopia Technologies
- Técnica de Informática e Responsável pelas Aulas de informática OTEC na Universidade de Alcalá de Henares
- Colaboradora na Associação ASALUMA
- Licenciatura em Engenharia Electrónica de Comunicações na Escola Politécnica Superior na Universidade de Alcalá de Henares

Sr. Fondón Alcalde, Rubén

- Analista EMEA de Amazon Web Services
- Analista de Negócio em Gestão de Valor do Cliente na Vodafone Espanha
- Chefe de Integração de Serviços na Entelgy para a Telefónica Global Solutions
- Administrador de Contas online de Servidores clónicos na EDM Electronics
- Diretor de Implementação de Serviços Internacionais na Vodafone Global Enterprise
- Consultor de soluções para Espanha e Portugal na Telvent Global Services
- Analista de Negócios para o Sul da Europa na Vodafone Global Enterprise
- Engenheiro de Telecomunicações pela Universidade Europeia de Madrid
- Mestrado em Big Data e Analytics pela Universidade Internacional de Valência

Sr. Díaz Díaz-Chirón, Tobías

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

Sr. Tato Sánchez, Rafael

- Diretor Técnico na 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
- Licenciatura em Engenharia Eletrónica Industrial e Automática pela Universidade Europeia
- Engenheiro Técnica Industrial pela Universidade Politécnica de Madrid

Sra. Marcos Sbarbaro, Victoria Alicia

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

Sr. Catalá Barba, José Francisco

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

Sr. Armero Fernández, Rafael

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

Sr. Peralta Alonso, Jon

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

Sr. Redondo, Jesús Serrano

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

Sr. Jiménez Ramos, Álvaro

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

08

Certificação

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

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

Este programa permitirá a obtenção do certificado próprio de **Advanced Master em Secure Information Management** reconhecido pela TECH Global University, a maior universidade digital do mundo.

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

Título: **Advanced Master em Secure Information Management**

Modalidade: **online**

Duração: **2 anos**

Acreditação: **120 ECTS**

tech global university

Sr./Sra. _____, com o documento de identidade nº _____, foi aprovado satisfatoriamente e obteve o certificado de:

Advanced Master em Secure Information Management

Trata-se de um título próprio com duração de 3600 horas, o equivalente a 120 ECTS, com data de início dd/mm/aaaa e data final dd/mm/aaaa.

A TECH Global University é uma universidade oficialmente reconhecida pelo Governo de Andorra em 31 de janeiro de 2024, que pertence ao Espaço Europeu de Educação Superior (EEES).

Andorra la Vella, 28 de fevereiro de 2024

Dr. Pedro Navarro Illana
Reitor

código único TECH: BBADCEADBECB99D techtitute.com/titulos

Advanced Master em Secure Information Management

Distribuição geral do programa

Curso	Disciplina	ECTS	Carácter
1º	Análise de dados na organização empresarial	6	OB
1º	Gestão, manipulação de dados e informação para a ciência de dados	6	OB
1º	Dispositivos e plataformas IoT como base para a ciência dos dados	6	OB
1º	Representação gráfica para análise de dados	6	OB
1º	Ferramentas de ciência de dados	6	OB
1º	Exploração de dados. seleção, pré-processamento e transformação	6	OB
1º	Previsibilidade e análise de fenómenos estocásticos	6	OB
1º	Conceção e desenvolvimento de sistemas inteligentes	6	OB
1º	Arquiteturas e sistemas para uso intensivo de dados	6	OB
2º	Aplicação prática da ciência dos dados nos setores de atividade empresarial	6	OB
2º	Ciberinteligência e cibersegurança	6	OB
2º	Segurança em host	6	OB
2º	Segurança na rede (Perimetral)	6	OB
2º	Segurança em Smartphones	6	OB
2º	Segurança em IoT	6	OB
2º	*Hacking* ético	6	OB
2º	Engenharia reversa	6	OB
2º	Desenvolvimento seguro	6	OB
2º	Análise forense	6	OB
2º	Desafios atuais e futuros em segurança informática	6	OB

Dr. Pedro Navarro Illana
Reitor

tech global university

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

tech global university

Advanced Master
Secure Information Management

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

Advanced Master

Secure Information Management

tech global university