Weiterbildender Masterstudiengang
Management der Informationssicherheit

tech technologische universität

tech technologische universität

Weiterbildender Masterstudiengang
Management der Informationssicherheit

- Modalität: **online**
- Dauer: **2 Jahre**
- Qualifizierung: **TECH Technologische Universität**
- Aufwand: **16 Std./Woche**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

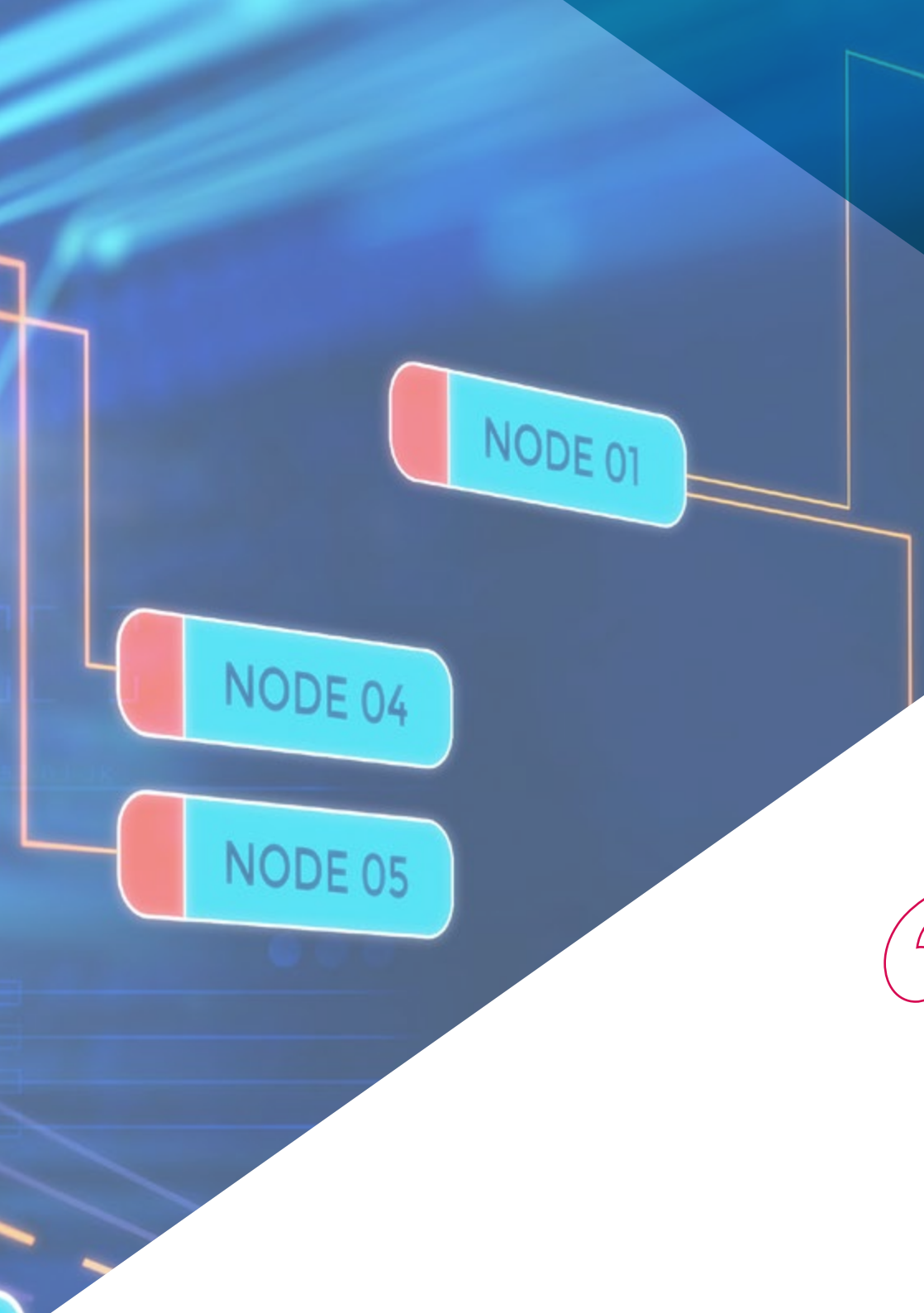
Internetzugang: www.techtitute.com/de/informatik/weiterbildender-masterstudiengang/weiterbildender-masterstudiengang-management-informationssicherheit

Index

01

Präsentation

Die Welt von heute wird von der digitalen Umgebung beherrscht. In ihr wird ein breites Spektrum an Aktivitäten in verschiedenen Bereichen verwaltet. Freizeit, Arbeit oder der Kontakt mit Freunden und Familie sind ohne das Internet und all die vorhandenen Online-Tools nicht mehr denkbar. Aus diesem Grund werden täglich riesige Mengen an Informationen übertragen, von harmlosen Daten in Gesprächen über soziale Netzwerke und Messaging-Anwendungen bis hin zu hochsensiblen persönlichen und beruflichen Informationen, die auf Bank- oder Unternehmenswebsites gehostet werden. In diesem komplexen Kontext werden Spezialisten benötigt, die alle Arten von Informationen aus diesen Bereichen verwalten können, ohne dabei die Sicherheit aus den Augen zu verlieren. Zahlreiche Unternehmen suchen nach Personen mit diesem Profil, um ihre Informationen zu schützen.



Jeden Tag versuchen böswillige Menschen, die Sicherheit von Unternehmen und Institutionen, die wertvolle Daten verwalten, zu gefährden: Sie könnten der große Beschützer dieser Informationen sein"

Jeden Tag führen Millionen von Menschen alle möglichen Aktivitäten im Internet durch. Sie lesen die Nachrichten, chatten mit Freunden und Familie, tauschen Meinungen in sozialen Netzwerken aus, erledigen Verwaltungsaufgaben in verschiedenen Unternehmen und Institutionen, tauschen alle Arten von Dateien aus oder erledigen arbeitsbezogene Aufgaben. So werden in jedem Moment unzählige Datenmengen auf der ganzen Welt erstellt und übertragen.

Sie mit angemessener Sicherheit zu verwalten, ist keine leichte Aufgabe, da es eine Reihe von spezifischen Fachkenntnissen aus verschiedenen Bereichen erfordert, die normalerweise nicht miteinander in Berührung kommen würden. Aus diesem Grund ist dieser Weiterbildende Masterstudiengang in Management der Informationssicherheit eine hervorragende Gelegenheit für all jene Ingenieure und IT-Fachleute, die Informationsmanagement und Cybersicherheit integrieren wollen, um führende Spezialisten in beiden Bereichen zu werden.

Viele Unternehmen und Institutionen verwenden hochsensible und wertvolle Daten, die ordnungsgemäß verwaltet, aufbewahrt und überwacht werden müssen. Es gibt noch nicht viele Experten in beiden Disziplinen, die damit richtig umgehen können. Studenten, die diesen Studiengang abschließen, werden also in der besten Position sein, um führende Positionen in Unternehmen zu erreichen, die ihre digitalen Informationen schützen wollen.

Zu diesem Zweck hat TECH die besten Inhalte entwickelt und die besten Lehrkräfte mit umfassender Berufserfahrung in diesen Bereichen zusammengebracht, damit die Studenten einen möglichst umfassenden Unterricht erhalten und am Arbeitsplatz vorankommen können.

Dieser **Weiterbildender Masterstudiengang in Management der Informationssicherheit** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- Die Entwicklung von Fallstudien, die von Experten der Informatik präsentiert werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt soll wissenschaftliche und praktische Informationen zu den für die berufliche Praxis wesentlichen Disziplinen vermitteln
- Er enthält praktische Übungen in denen der Selbstbewertungsprozess durchgeführt werden kann um das Lernen zu verbessern
- Sein besonderer Schwerpunkt liegt auf innovativen Methoden der digitalen Datenverwaltung und -sicherheit
- Theoretische Vorträge, Fragen an den Experten, Diskussionsforen zu kontroversen Themen und individuelle Reflexionsarbeit
- Die Verfügbarkeit des Zugriffs auf die Inhalte von jedem, festen oder tragbaren Gerät, mit Internetanschluss

Alles, was wir in der digitalen Sphäre tun, wird aufgezeichnet. Machen Sie das Internet zu einem sichereren Ort mit diesem weiterbildenden Masterstudiengang"

Die besten Unternehmen des Landes werden Ihnen die Verwaltung und Sicherheit ihrer Daten anvertrauen, wenn Sie dieses Programm abschließen"

Dieser weiterbildende Masterstudiengang kombiniert zwei wesentliche Disziplinen für die Zukunft Ihrer Karriere. Schreiben Sie sich ein und erreichen Sie alle Ihre Ziele.

Lernen Sie alles über Datenverwaltung und -sicherheit und erleben Sie, wie Sie in kürzester Zeit beruflich vorankommen.

Das Lehrteam besteht aus Fachleuten aus dem Bereich der Informatik, die ihre Berufserfahrung in dieses Programm einbringen, sowie aus anerkannten Spezialisten aus führenden Unternehmen und renommierten Universitäten.

Die multimedialen Inhalte, die mit den neuesten Bildungstechnologien entwickelt wurden, ermöglichen den Fachleuten ein situiertes und kontextbezogenes Lernen, d.h. eine simulierte Umgebung, die ein immersives Studium ermöglicht, das auf die Fortbildung in realen Situationen ausgerichtet ist.

Das Konzept dieses Studiengangs konzentriert sich auf problemorientiertes Lernen, bei dem der Student versuchen muss, die verschiedenen Situationen der beruflichen Praxis zu lösen, die im Laufe des Programms auftreten. Dabei wird die Fachkraft durch ein innovatives interaktives Videosystem unterstützt, das von anerkannten Experten entwickelt wurde.

02

Ziele

Das Hauptziel dieses Weiterbildenden Masterstudiengangs in Management der Informationssicherheit ist es, den Studenten die besten Kenntnisse in zwei verschiedenen, aber miteinander verbundenen Bereichen der Informatik und des Ingenieurwesens zu vermitteln: Datenverwaltung im digitalen Umfeld und Cybersicherheit. Durch die Kombination dieser beiden Bereiche werden Informatiker und Fachleute mit diesem Programm in der Lage sein, die besten Lösungen für jede Situation, die sich in ihrer Karriere ergibt, anzuwenden und ihren Unternehmen die am besten geeigneten Werkzeuge für die Verwaltung und den Schutz aller Arten von sensiblen Informationen anzubieten.

Ihr Ziel ist es, der beste Spezialist in Ihrem Unternehmen zu sein, und TECH bietet Ihnen die Mittel, um dieses Ziel zu erreichen"

Allgemeine Ziele

- Analyse der Vorteile der Anwendung von Datenanalysetechniken in jeder Abteilung des Unternehmens
- Die Grundlage für das Verständnis der Bedürfnisse und Anwendungen der einzelnen Abteilungen entwickeln
- Fachwissen generieren, um das richtige Werkzeug auszuwählen
- Techniken und Ziele vorschlagen, um je nach Abteilung so produktiv wie möglich zu sein
- Die Rolle des Cybersecurity-Analysten untersuchen
- Social Engineering und seine Methoden erforschen
- Untersuchung von OSINT, HUMINT, OWASP, PTEC, OSSTM und OWISAM-Methoden
- Durchführung einer Risikoanalyse und Verstehen der Risikokennzahlen
- Bestimmung des angemessenen Einsatzes von Anonymität und der Nutzung von Netzwerken wie TOR, I2P und Freenet
- Zusammenstellung der bestehenden Cybersicherheitsvorschriften
- Fachwissen für die Durchführung eines Sicherheitsaudits generieren
- Ausarbeitung angemessener Nutzungsrichtlinien
- Erkennungs- und Präventionssysteme für die wichtigsten Bedrohungen untersuchen
- Bewertung neuer Systeme zur Erkennung von Bedrohungen und deren Weiterentwicklung gegenüber herkömmlichen Lösungen
- Analyse der derzeit wichtigsten mobilen Plattformen, ihrer Eigenschaften und Nutzung
- Identifizierung, Analyse und Bewertung der Sicherheitsrisiken von IoT-Projektteilen

- Auswertung der erhaltenen Informationen und Entwicklung von Präventions- und *Hacking*-Mechanismen
- Anwendung von Reverse Engineering auf die Cybersicherheitsumgebung
- Festlegung der Tests, die mit der entwickelten Software durchgeführt werden sollen
- Alle vorhandenen Beweise und Daten sammeln, um einen forensischen Bericht zu erstellen
- Korrekte Präsentation des forensischen Berichts
- Analyse des aktuellen und zukünftigen Stands der IT-Sicherheit
- Untersuchung der Risiken neu aufkommender Technologien
- Die verschiedenen Technologien in Bezug auf die Computersicherheit zusammenstellen

Cybersicherheit und Datenverwaltung sind schnelllebige Disziplinen. Absolvieren Sie diesen weiterbildenden Masterstudiengang und erhalten Sie das aktuellste Wissen"

Spezifische Ziele

Modul 1. Datenanalytik in der Unternehmensorganisation

- Entwicklung analytischer Fähigkeiten, um hochwertige Entscheidungen zu treffen
- Untersuchung von effektiven Marketing- und Kommunikationskampagnen
- Die Erstellung von abteilungsspezifischen Dashboards und KPIs bestimmen
- Fachwissen generieren, um prädiktive Analysen zu entwickeln
- Vorschlagen von Geschäfts- und Loyalitätsplänen auf der Grundlage von Marktstudien
- Die Fähigkeit entwickeln, dem Kunden zuzuhören
- Statistisches, quantitatives und technisches Wissen in realen Situationen anwenden

Modul 2. Datenverwaltung, Datenbearbeitung und Informationen für die Datenwissenschaft

- Durchführen einer Datenanalyse
- Verschiedene Daten vereinheitlichen: Konsistenz der Informationen erreichen
- Bereitstellung relevanter, effektiver Informationen für die Entscheidungsfindung
- Bestimmung der besten Praktiken für die Datenverwaltung je nach Typologie und Verwendungszweck
- Festlegung von Richtlinien für den Datenzugriff und die Wiederverwendung
- Gewährleistung von Sicherheit und Verfügbarkeit: Verfügbarkeit, Integrität und Vertraulichkeit von Informationen
- Untersuchung von Tools zur Datenverwaltung mit Hilfe von Programmiersprachen

Modul 3. IoT-Geräte und -Plattformen als Grundlage für die Datenwissenschaft

- Identifizierung, was IoT (Internet of Things) und IIoT (Industrial Internet of Things) ist
- Untersuchung des Industrial Internet Consortium
- Analyse der IoT-Referenzarchitektur
- Besprechung von IoT-Sensoren und -Geräten und deren Klassifizierung
- Identifizierung der im IoT verwendeten Kommunikationsprotokolle und Technologien
- Untersuchung der verschiedenen Cloud-Plattformen im IoT: Allgemeiner Zweck, Industrie, Open Source
- Entwicklung von Mechanismen zum Datenaustausch
- Festlegung von Sicherheitsanforderungen und -strategien
- Einführung in die verschiedenen IoT- und IIoT-Anwendungsbereiche

Modul 4. Grafische Darstellung für die Datenanalyse

- Fachwissen über Datendarstellung und -analyse aufbauen
- Die verschiedenen Arten von gruppierten Daten untersuchen
- Ermittlung der am häufigsten verwendeten grafischen Darstellungen in verschiedenen Bereichen
- Bestimmung der Gestaltungsprinzipien bei der Datenvisualisierung
- Einführung in die grafische Erzählung als Werkzeug
- Analyse der verschiedenen Softwaretools für die grafische Darstellung und explorative Datenanalyse

Modul 5. Tools der Datenwissenschaft

- Entwicklung von Fähigkeiten zur Umwandlung von Daten in Informationen, aus denen Wissen gewonnen werden kann
- Bestimmung der Hauptmerkmale eines Dataset, seiner Struktur, seiner Komponenten und der Auswirkungen seiner Verteilung auf die Modellierung
- Unterstützung der Entscheidungsfindung durch eine vollständige vorherige Analyse der Daten
- Entwicklung von Fähigkeiten zur Lösung von Fallstudien mit Hilfe von Techniken der Datenwissenschaft
- Festlegung der am besten geeigneten allgemeinen Tools und Methoden für die Modellierung jedes Datasets auf der Grundlage der durchgeführten Vorverarbeitungen
- Ergebnisse analytisch auswerten und die Auswirkungen der gewählten Strategie auf die verschiedenen Metriken verstehen
- Demonstration der Kritikfähigkeit an den Ergebnissen, die nach Anwendung von Vorverarbeitungs- oder Modellierungsmethoden erzielt wurden

Modul 6. Data Mining - Auswahl, Vorverarbeitung und Transformation

- Fachwissen über die vorherige Statistik für die Datenanalyse und -auswertung generieren
- Die notwendigen Fähigkeiten zur Identifizierung, Vorbereitung und Umwandlung von Daten entwickeln
- Die verschiedenen vorgestellten Methoden bewerten und Vor- und Nachteile identifizieren
- Untersuchung von Problemen in hochdimensionalen Datenumgebungen
- Entwicklung der Implementierung der Algorithmen für die Datenvorverarbeitung
- Demonstration der Fähigkeit, Datenvisualisierungen für die deskriptive Analyse zu interpretieren
- Entwicklung fortgeschrittener Kenntnisse über die verschiedenen vorhandenen Datenaufbereitungstechniken zur Datenbereinigung, Normalisierung und Datentransformation

Modul 7. Vorhersagbarkeit und Analyse von stochastischen Phänomenen

- Zeitreihen analysieren
- Entwicklung der Formulierung und der grundlegenden Eigenschaften von univariaten Zeitreihenmodellen
- Untersuchung der Methodik der Modellierung und Vorhersage von Echtzeitreihen
- Bestimmung von univariaten Modellen einschließlich Ausreißern
- Anwendung dynamischer Regressionsmodelle und der Methodik zur Erstellung solcher Modelle aus beobachteten Reihen
- Spektralanalyse von univariaten Zeitreihen sowie die Grundlagen der periodogrammbasierten Inferenz und deren Interpretation
- Schätzung der Wahrscheinlichkeit und des Trends einer Zeitreihe für einen bestimmten Zeithorizont

Modul 8. Design und Entwicklung von intelligenten Systemen

- Den Übergang von Informationen zu Wissen analysieren
- Entwicklung der verschiedenen Arten von Techniken des maschinellen Lernens
- Untersuchung von Metriken und Scores zur Quantifizierung der Qualität von Modellen
- Implementierung der verschiedenen Algorithmen für maschinelles Lernen
- Probabilistische Argumentationsmodelle identifizieren
- Die Grundlagen des Deep Learning legen
- Demonstration der erworbenen Fähigkeiten, um die verschiedenen Algorithmen des maschinellen Lernens zu verstehen

Modul 9. Datenintensive Architekturen und Systeme

- Anforderungen für datenintensive Systeme festlegen
- Untersuchung verschiedener Datenmodelle und Analyse von Datenbanken
- Analyse der wichtigsten Funktionen für verteilte Systeme und ihrer Bedeutung in verschiedenen Systemtypen
- Bewertung, welche weit verbreiteten Anwendungen die Grundlagen verteilter Systeme nutzen, um ihre Systeme zu gestalten
- Analyse, wie Datenbanken Informationen speichern und abrufen
- Die verschiedenen Replikationsmodelle und die damit verbundenen Probleme identifizieren
- Entwicklung von Möglichkeiten der Partitionierung und verteilten Transaktionen
- Identifizierung von Batch-Systemen und (nahezu) Echtzeit-Systemen

Modul 10. Praktische Anwendung der Datenwissenschaft in Geschäftsbereichen

- Analyse des Stands der Technik bei Künstlicher Intelligenz (KI) und Datenanalyse
- Entwicklung von Fachwissen über die am häufigsten verwendeten Technologien
- Ein besseres Verständnis der Technologie durch Anwendungsfälle schaffen
- Analyse der gewählten Strategien zur Auswahl der besten Technologien für die Implementierung
- Anwendungsbereiche festlegen
- Untersuchung der tatsächlichen und potenziellen Risiken der angewandten Technologie
- Vorschläge zu den Vorteilen, die sich aus der Nutzung ergeben
- Identifizierung von Zukunftstrends in bestimmten Sektoren

Modul 11. Cyberintelligenz und Cybersicherheit

- Entwicklung der in der Cybersicherheit verwendeten Methoden
- Untersuchung des Intelligence-Zyklus und dessen Anwendung auf Cyberintelligenz
- Die Rolle des Informationsanalysten und die Hindernisse für die Evakuierungsaktivitäten bestimmen
- Analyse von OSINT, OWISAM, OSSTM, PTES, OWASP-Methoden
- Die gebräuchlichsten Tools für die Produktion von Informationen einrichten
- Eine Risikoanalyse durchführen und die verwendeten Metriken verstehen
- Die Optionen für Anonymität und die Nutzung von Netzwerken wie TOR, I2P, FreeNet festlegen
- Detaillierte Angaben zu den aktuellen Cybersicherheitsvorschriften

Modul 12. Host-Sicherheit

- Festlegung der Backup-Richtlinienfür persönliche und berufliche Daten
- Bewertung der verschiedenen Tools, um Lösungen für bestimmte Sicherheitsprobleme zu finden
- Einrichtung von Mechanismen, um das System auf dem neuesten Stand zu halten
- Analyse der Ausrüstung zur Erkennung von Eindringlingen
- Festlegung der Regeln für den Zugriff auf das System
- Prüfung und Klassifizierung von Mails, um Betrug zu vermeiden
- Listen mit erlaubter Software erstellen

Modul 13. Netzwerksicherheit (Perimeter)

- Analyse aktueller Netzwerkarchitekturen zur Identifizierung des zu schützenden Perimeters
- Entwicklung spezifischer Firewall- und Linux-Konfigurationen, um die häufigsten Angriffe zu entschärfen
- Kompilierung der gebräuchlichsten Lösungen wie Snort und Suricata, sowie deren Konfiguration
- Untersuchung der verschiedenen zusätzlichen Schichten, die von Firewalls der neuen Generation und Netzwerkfunktionen in Cloud-Umgebungen bereitgestellt werden
- Bestimmung der Tools für den Netzwerkschutz und Nachweis, warum sie für eine mehrschichtige Verteidigung von grundlegender Bedeutung sind

Modul 14. Smartphone-Sicherheit

- Untersuchung der verschiedenen Angriffsvektoren, um zu vermeiden, ein leichtes Ziel zu werden
- Bestimmung der wichtigsten Angriffe und Arten von Malware, denen Benutzer mobiler Geräte ausgesetzt sind
- Analyse der aktuellsten Geräte, um eine sicherere Konfiguration zu erstellen
- Angabe der wichtigsten Schritte zur Durchführung eines Penetrationstests auf iOS- und Android-Plattformen
- Entwicklung von Fachwissen über die verschiedenen Schutz- und Sicherheitstools
- Einführung von Best Practices in der mobilitätsorientierten Programmierung

Modul 15. IoT-Sicherheit

- Analyse der wichtigsten IoT-Architekturen
- Untersuchung von Konnektivitätstechnologien
- Entwicklung der wichtigsten Anwendungsprotokolle
- Die verschiedenen Typen der vorhandenen Geräte identifizieren
- Bewertung des Risikoniveaus und bekannter Schwachstellen
- Entwicklung sicherer Nutzungsrichtlinien
- Festlegung angemessener Bedingungen für die Verwendung dieser Geräte

Modul 16. Ethisches *Hacking*

- Prüfung der IOSINT-Methoden
- Sammeln von öffentlich zugänglichen Informationen
- Scannen von Netzwerken nach Informationen im aktiven Modus
- Entwicklung von Testlabors
- Analysetools für *Pentesting*-Leistungen
- Katalogisierung und Bewertung der verschiedenen Schwachstellen der Systeme
- Die verschiedenen *Hacking*-Methoden konkretisieren

Modul 17. Reverse Engineering

- Die Phasen eines Compilers analysieren
- Untersuchen Sie die x86-Prozessorarchitektur und die ARM-Prozessorarchitektur
- Die verschiedenen Arten der Analyse bestimmen
- Anwendung von Sandboxing in verschiedenen Umgebungen
- Entwicklung verschiedener Techniken zur Analyse von Malware
- Entwicklung von Tools für die Malware-Analyse

Modul 18. Sichere Entwicklung

- Die Anforderungen festlegen, die für den korrekten und sicheren Betrieb einer Applikation erforderlich sind
- Überprüfen der Logdateien, um Fehlermeldungen zu verstehen
- Analyse verschiedener Ereignisse und Entscheidung darüber, was dem Benutzer angezeigt und was in den Logs gespeichert werden soll
- Generieren von bereinigtem, leicht überprüfbarem, qualitativ hochwertigem Code
- Bewertung der geeigneten Dokumentation für jede Phase der Entwicklung
- Das Verhalten des Servers konkretisieren, um das System zu optimieren
- Entwicklung von modularem, wiederverwendbarem und wartbarem Code

Modul 19. Forensische Analyse

- Die verschiedenen Elemente identifizieren, die ein Verbrechen offenbaren
- Generierung von Spezialwissen, um Daten von verschiedenen Medien zu erhalten, bevor sie verloren gehen
- Wiederherstellung von absichtlich gelöschten Daten
- Analyse von Systemlogs und Aufzeichnungen
- Festlegung, wie die Daten dupliziert werden, um die Originale nicht zu verändern
- Nachweise belegen, dass sie konsistent sind
- Erstellung eines robusten und nahtlosen Berichts
- Präsentation der Ergebnisse auf konsistente Weise
- Festlegung, wie Sie den Bericht gegenüber der zuständigen Behörde verteidigen
- Strategien für sichere Telearbeit konkretisieren

Modul 20. Aktuelle und zukünftige Herausforderungen in der IT-Sicherheit

- Untersuchung der Verwendung von Kryptowährungen, der Auswirkungen auf die Wirtschaft und der Sicherheit
- Analyse der Situation der Nutzer und des Grades des digitalen Analphabetismus
- Bestimmung des Anwendungsbereichs von *Blockchain*
- Präsentation von Alternativen zu IPv4 bei der Netzwerkadressierung
- Entwicklung von Strategien zur Aufklärung der Bevölkerung über die richtige Nutzung von Technologien
- Erstellen von Fachwissen, um neue Sicherheitsherausforderungen zu bewältigen und Identitätsdiebstahl zu verhindern
- Strategien für sichere Telearbeit konkretisieren

03

Kompetenzen

Studenten, die diesen Weiterbildenden Masterstudiengang in Management der Informationssicherheit absolvieren, werden in der Lage sein, eine Vielzahl von hochspezialisierten Aufgaben in den Bereichen der Datenverwaltung und Cybersicherheit auszuführen. Dieser Studiengang kombiniert also beide Fachrichtungen, um komplementäres Wissen anzubieten, das in verschiedenen beruflichen Situationen und Umgebungen eingesetzt werden kann. Auf diese Weise werden die Studenten einen umfassenden Lernprozess durchlaufen, der sie zu echten Spezialisten auf diesem Gebiet macht.

Ihre neuen Fähigkeiten werden Sie zum größten Spezialisten in Ihrem Umfeld machen"

Allgemeine Kompetenzen

- Entwicklung einer technischen und geschäftlichen Perspektive der Datenanalyse
- Die neuesten Algorithmen, Plattformen und Tools zur Erkundung, Visualisierung, Manipulation, Verarbeitung und Analyse von Daten verstehen
- Implementierung einer für die Wertschöpfung notwendigen Geschäftsvision als Schlüsselelement für die Entscheidungsfindung
- In der Lage sein, spezifische Probleme der Datenanalyse zu lösen
- Kenntnis der in der Cybersicherheit verwendeten Methoden
- Bewertung jeder Art von Bedrohung, um eine optimale Lösung für jeden Fall zu finden
- Erstellung von intelligenten Komplettlösungen zur Automatisierung des Verhaltens bei Zwischenfällen
- Wissen, wie man die Risiken im Zusammenhang mit Schwachstellen innerhalb und außerhalb des Unternehmens einschätzen kann
- Die Entwicklung und die Auswirkungen des IoT im Laufe der Zeit verstehen
- Nachweisen, dass ein System verwundbar ist, es zu Präventionszwecken angreifen und solche Probleme lösen können
- Anwendung von *Sandboxing* in verschiedenen Umgebungen
- Kenntnis der Richtlinien, die ein guter Entwickler befolgen sollte, um die erforderliche Sicherheit zu gewährleisten

Spezifische Kompetenzen

- Spezialisierung auf *Data Science* aus technischer und geschäftlicher Sicht
- Visualisierung von Daten auf die am besten geeignete Weise, um die gemeinsame Nutzung und das Verständnis durch verschiedene Profile zu unterstützen
- Die wichtigsten Funktionsbereiche des Unternehmens, in denen Datenwissenschaft den größten Nutzen bringen kann, ansprechen
- Entwicklung des Datenlebenszyklus, seiner Typologie und der für seine Verwaltung erforderlichen Technologien und Phasen
- Verarbeitung und Manipulation von Daten mit speziellen Sprachen und Bibliotheken
- Entwicklung fortgeschrittener Kenntnisse in den grundlegenden Data-Mining-Techniken für Datenauswahl, Vorverarbeitung und Datentransformation
- Spezialisierung auf die wichtigsten Algorithmen des *Machine Learning* zur Extraktion von verborgenem Wissen in Daten
- Fachwissen über die Software-Architekturen und -Systeme, die für die datenintensive Nutzung von Daten erforderlich sind, generieren
- Bestimmung, wie das IoT eine Quelle für die Erzeugung von Daten und Schlüsselinformationen sein kann, auf die Datenwissenschaft zur Wissensextraktion angewendet werden kann
- Analyse der verschiedenen Möglichkeiten der Anwendung von Datenwissenschaft in verschiedenen Sektoren oder Branchen anhand von Beispielen aus der Praxis
- Durchführung von defensiven Sicherheitsmaßnahmen
- Gründliche und spezialisierte Kenntnisse der IT-Sicherheit
- Spezialkenntnisse auf dem Gebiet der Cybersicherheit und Cyber Intelligence
- Fundierte Kenntnisse grundlegender Aspekte wie des Intelligence-Zyklus, der Intelligence-Quellen, des Social Engineering, der OSINT-Methodik, des HUMINT, der Anonymisierung und der Risikoanalyse, der bestehenden Methoden (OWASP, OWISAM, OSSTM, PTES) und der aktuellen Cybersicherheitsvorschriften
- Verständnis der Bedeutung einer mehrschichtigen Verteidigung, auch bekannt als *Defense in Depth*, die alle Aspekte eines Unternehmensnetzwerks abdeckt, wobei einige der besprochenen Konzepte und Systeme auch gestärkt und Umgebung genutzt und angewendet werden können
- Wissen, wie man Sicherheitsverfahren für Smartphones und tragbare Geräte anwendet
- Kenntnis der Mittel des sogenannten ethischen *Hackings* und Schutz eines Unternehmens vor einer Cyber-Attacke
- Untersuchung eines Cybersicherheitsvorfalls
- Kenntnis der verschiedenen vorhandenen Angriffs- und Verteidigungstechniken
- Analyse der Rolle des Cybersicherheitsanalysten und Kenntnis der Funktionsweise von Social Engineering und seiner Methoden

Möchten Sie sich von anderen Spezialisten abheben, wissen aber nicht, wie? Dieser weiterbildende Masterstudiengang ist genau das, wonach Sie suchen"

04

Kursleitung

Dieser Studiengang wird von den besten Professoren auf dem Gebiet der Cybersicherheit und der digitalen Datenverwaltung unterrichtet. Ihre Erfahrung garantiert, dass die Studenten die vollständigsten und aktuellsten Inhalte erhalten, damit sie diese direkt auf ihre berufliche Laufbahn anwenden können. Auf diese Weise geben die Dozenten dieses Weiterbildenden Masterstudiengangs in Management der Informationssicherheit ihr gesamtes Wissen an die Studenten weiter und sorgen dafür, dass diese zu hochqualifizierten Spezialisten werden, die von großen Unternehmen in ihren Ländern nachgefragt werden.

Die besten Spezialisten zeigen Ihnen, wie Sie eine führende Rolle in der Branche einnehmen können"

Internationale Gastdirektorin

Dr. Frederic Lemieux ist international als innovativer Experte und inspirierende Führungspersönlichkeit in den Bereichen der **Intelligenz, der nationalen Sicherheit, der inneren Sicherheit, der Cybersicherheit** und der **disruptiven Technologien** anerkannt. Sein ständiges Engagement und seine wichtigen Beiträge zu Forschung und Bildung machen ihn zu einer zentralen Figur bei der Förderung der Sicherheit und des Verständnisses der heutigen neuen Technologien. Während seiner beruflichen Laufbahn hat er an mehreren renommierten Institutionen wie der **Universität von Montreal,** der **George Washington Universität** und der Universität von Georgetown zukunftsweisende akademische Programme konzipiert und geleitet.

Im Laufe seiner umfangreichen Erfahrung hat er mehrere Bücher von großer Bedeutung veröffentlicht, die sich alle mit **kriminalistischer Aufklärung, Polizeiarbeit, Cyber-Bedrohungen und internationaler Sicherheit** befassen. Er hat auch einen wichtigen Beitrag zum Bereich der Cybersicherheit geleistet, indem er zahlreiche Artikel in akademischen Zeitschriften veröffentlicht hat, die sich mit der Verbrechensbekämpfung bei großen Katastrophen, der Terrorismusbekämpfung, den Nachrichtendiensten und der polizeilichen Zusammenarbeit beschäftigen. Darüber hinaus war er Podiumsteilnehmer und Hauptredner bei verschiedenen nationalen und internationalen Konferenzen und hat sich als führender Wissenschaftler und Praktiker etabliert.

Dr. Lemieux hatte redaktionelle und bewertende Funktionen in verschiedenen akademischen, privaten und staatlichen Organisationen inne, was seinen Einfluss und sein Engagement für Spitzenleistungen in seinem Fachgebiet widerspiegelt. Im Rahmen seiner angesehenen akademischen Laufbahn war er Professor für Praxis und Fakultätsleiter der MPS-Programme für **Angewandte Intelligenz, Risikomanagement für Cybersicherheit, Technologiemanagement und Informationstechnologiemanagement** an der **Universität von Georgetown.**

Dr. Lemieux, Frederic

- Forscher im Bereich Intelligenz, Cybersicherheit und Disruptive Technologien an der Universität von Georgetown
- Direktor des Masterstudiengangs in Information Technology Management an der Universität von Georgetown
- Direktor des Masterstudiengangs in Technology Management an der Universität von Georgetown
- Direktor des Masterstudiengangs in Cybersecurity Risk Management an der Universität von Georgetown
- Direktor des Masterstudiengangs in Applied Intelligence an der Universität von Georgetown
- Professor für Praktika an der Universität von Georgetown
- Promotion in Kriminologie an der School of Criminology der Universität von Montreal
- Hochschulabschluss in Soziologie, Nebenfach Psychologie, Universität von Laval
- Mitglied von:
- New Program Roundtable Committee, Universität von Georgetown

Dank TECH werden Sie mit den besten Fachleuten der Welt lernen können"

Leitung

Dr. Peralta Martín-Palomino, Arturo

- CEO und CTO bei Prometeus Global Solutions
- CTO bei Korporate Technologies
- CTO bei AI Shephers GmbH
- Promotion in technischer Informatik an der Universität von Castilla La Mancha
- Promotion in Wirtschaftswissenschaften, Unternehmen und Finanzen an der Universität Camilo José Cela Außerordentlicher Promotionspreis
- Doktor der Psychologie an der Universität von Castilla La Mancha
- Masterstudiengang in fortgeschrittenen Informationstechnologien von der Universität von Castilla La Mancha
- Masterstudiengang MBA+E (Master in Business Administration and Organisational Engineering) an der Universität von Castilla La Mancha
- Außerordentlicher Professor, der an der Universität von Castilla La Mancha Bachelor- und Masterstudiengänge in Computertechnik unterrichtet
- Professor für den Masterstudiengang in Big Data und Data Science an der Internationalen Universität von Valencia
- Professor für den Masterstudiengang in Industrie 4.0 und den Masterstudiengang in Industriedesign und Produktentwicklung
- Mitglied der SMILe-Forschungsgruppe der Universität von Castilla La Mancha

Fr. Fernández Sapena, Sonia

- Ausbilderin für Computersicherheit und Ethical *Hacking* Nationales Referenzzentrum für IT und Telekommunikation in Getafe Madrid
- Zertifizierte E-Council-Ausbilderin Madrid
- Kursleitung der folgenden Zertifizierungen: EXIN Ethical *Hacking* Foundation und EXIN Cyber & IT Security Foundation Madrid
- Von der CAM akkreditierte Fachausbilderin für die folgenden Berufszertifikate: IT-Sicherheit (IFCT0190), Verwaltung von Sprach- und Datennetzen (IFCM0310), Verwaltung von Abteilungsnetzen (IFCT0410), Alarmmanagement in Telekommunikationsnetzen (IFCM0410), Betreiber von Sprach- und Datennetzen (IFCM0110) und Verwaltung von Internetdiensten (IFCT0509)
- Externe Mitarbeit CSO/SSA (*Chief Security Officer/Senior Security Architect*) Universität der Balearischen Inseln
- Informatik-Ingenieurin. Universität von Alcalá de Henares. Madrid
- Masterstudiengang in DevOps: Docker und Kubernetes. Cas-Training. Madrid
- Microsoft Azure Security Techonologies E-Council. Madrid

Professoren

Hr. Armero Fernández, Rafael

- Business Intelligence Consultant bei SDG Group
- Digital Engineer bei Mi-GSO
- Logistic Engineer bei Torrecid S.A
- Quality Intern bei INDRA
- Hochschulabschluss in Luft- und Raumfahrttechnik an der Polytechnischen Universität von Valencia
- Masterstudiengang in Professional Development 4.0 von der Universität von Alcalá de Henares

Hr. Peris Morillo, Luis Javier

- Technical Lead bei Capitole Consulting
- Senior Technical Lead und Delivery Lead Support bei HCL
- Agile Coach und COO bei Mirai Advisory
- Entwickler, Team Lead, Scrum Masterstudiengang, Agile Coach, Produkt Manager bei DocPath
- Höhere Ingenieurausbildung in Informatik an der ESI von Ciudad Real (UCLM)
- Nachdiplomstudium in Projektmanagement von CEOE (Spanischer Verband der Unternehmensorganisationen)
- 50+ MOOCs, die von renommierten Universitäten wie der Stanford University, der Michigan University, der Yonsei University, der Polytechnischen Universität von Madrid, usw. angeboten werden

Hr. Montoro Montarroso, Andrés

- Forscher in der SMILe-Gruppe an der Universität von Castilla La Mancha
- Datenwissenschaftler bei Prometeus Global Solutions
- Hochschulabschluss in Informatik an der Universität von Castilla La Mancha, mit Spezialisierung auf Computerwissenschaften
- Masterstudiengang in Datenwissenschaft und Computertechnik an der Universität von Granada

Fr. Fernández Meléndez, Galina

- Datenanalystin bei ADN Mobile Solution
- ETL-Prozesse, Data Mining, Datenanalyse und -visualisierung, Erstellung von KPIs, Entwurf und Implementierung von Dashboards, Managementkontrolle R-Entwicklung, SQL-Verwaltung und andere
- Musterbestimmung, prädiktive Modellierung, maschinelles Lernen
- Hochschulabschluss in Betriebswirtschaftslehre. Universität Bicentenaria von Aragua-Caracas
- Diplom in Planung und öffentlichen Finanzen. Venezolanische Schule für Planung - Schule für Finanzen
- Masterstudiengang in Datenanalyse und Business Intelligence. Universität von Oviedo
- MBA en Administración y Dirección De Empresas (Europäische Wirtschaftshochschule Barcelona)
- Masterstudiengang in Big Data und Business Intelligence (Europäische Wirtschaftshochschule Barcelona)

Fr. Pedrajas Parabás, Elena

- Business Analyst bei Management Solutions in Madrid
- Forscher in der Abteilung für Informatik und numerische Analyse an der Universität von Cordoba
- Forscherin am Singular Centre for Research in Intelligent Technologies in Santiago de Compostela
- Hochschulabschluss in Computertechnik Masterstudiengang in Datenwissenschaft und Computertechnik Lehrerfahrung

Fr. Martínez Cerrato, Yésica

- Technikerin für elektronische Sicherheitsprodukte bei Securitas Security Spanien
- Business Intelligence Analyst bei Ricopia Technologies (Alcalá de Henares) Abschluss in elektronischer Kommunikationstechnik an der Polytechnischen Hochschule, Universität von Alcalá
- Verantwortlich für die Schulung neuer Mitarbeiter in Vertriebsmanagement-Software (CRM, ERP, INTRANET), Produkte und Verfahren bei Ricopia Technologies (Alcalá de Henares)
- Verantwortlich für die Schulung neuer Stipendiaten, die in die Computer-Klassenzimmer integriert werden an der Universität von Alcalá
- Projektmanagerin im Bereich Großkundenintegration bei Correos y Telégrafos (Madrid)
- Computertechnikerin - Verantwortlich für die Computer-Klassenzimmer OTEC, Universität von Alcalá (Alcalá de Henares)
- Lehrerin für Computerkurse bei der Vereinigung ASALUMA (Alcalá de Henares)
- Stipendium für die Ausbildung zum Computertechniker in OTEC, Universität von Alcala (Alcalá de Henares)

Hr. Fondón Alcalde, Rubén

- Business Analyst für Kundenwertmanagement bei Vodafone Spanien
- Leiter der Abteilung Service Integration bei Entelgy für Telefónica Global Solutions
- Clone Server Online-Kundenbetreuer bei EDM Electronics
- Business Analyst für Südeuropa bei Vodafone Global Enterprise
- Ingenieur für Telekommunikation an der Europäischen Universität Madrid
- Masterstudiengang in Big Data und Analytics an der Internationalen Universität von Valencia

Hr. Díaz Díaz-Chirón, Tobías

- Forscher im ArCO-Labor der Universität von Castilla La Mancha, einer Gruppe, die sich mit Projekten im Zusammenhang mit Computerarchitekturen und -netzen befasst
- Berater bei Blue Telecom, einem Unternehmen, das sich auf den Telekommunikationssektor spezialisiert hat
- Hochschulabschluss in Senior IT-Techniker an der Universität von Castilla La Mancha

Hr. Tato Sánchez, Rafael

- Projektmanagement bei INDRA SISTEMAS S.A. Verwaltung des Wartungsvertrags für die Installationen intelligenter Verkehrssysteme, die von der Verkehrssteuerungs- und -managementzentrale der Generaldirektion für Verkehr in Madrid abhängen
- Technischer Direktor bei INDRA SISTEMAS S.A., Leitung des Zentrums für Verkehrskontrolle und -management der Generaldirektion für Verkehr in Madrid
- Systemingenieur. ENA TRÁFICO S.A.
- Technischer Ingenieur für Elektrizität von der Polytechnischen Universität von Madrid
- Hochschulabschluss in Industrieelektronik und Automatisierungstechnik an der Europäischen Universität von Madrid
- Berufliche Zertifizierung. SSCE0110: Lehrtätigkeit in der beruflichen Bildung für die Erwerbstätigkeit
- Masterstudiengang in Industrie 4.0 von der Internationalen Universität von La Rioja (UNIR)

Hr. Catalá Barba, José Francisco

- Mittleres Management im MINISDEF Verschiedene Aufgaben und Verantwortlichkeiten innerhalb der GOE III, wie z.B. die Verwaltung und das Management von Vorfällen im internen Netzwerk, die Entwicklung von maßgeschneiderten Programmen für verschiedene Bereiche, Schulungskurse für Netzwerkbenutzer und Konzernpersonal im Allgemeinen
- Elektroniker in der Ford-Fabrik in Almusafes, Valencia, Programmierung von Robotern, PLCs, Reparatur und Wartung
- Elektronik-Techniker
- Entwickler von Apps für mobile Geräte

Hr. Jiménez Ramos, Álvaro

- Senior Sicherheitsanalyst bei The Workshop
- L1 Cybersecurity Analyst bei Axians
- L2 Cybersecurity Analyst bei Axians
- Cybersecurity-Analyst bei SACYR S.A.
- Hochschulabschluss in Telematik-Ingenieurwesen an der Polytechnischen Universität von Madrid
- Masterstudiengang in Cybersicherheit und ethisches *Hacking* von CICE
- Fortgeschrittenenkurs in Cybersicherheit von Deusto Formación

Fr. Marcos Sbarbaro, Victoria Alicia

- Native Android Mobile Applikationsentwicklung bei B60 UK
- Analytikerin-Programmiererin für die Verwaltung, Koordination und Dokumentation einer virtualisierten Sicherheitsalarmumgebung bei einem Kunden
- Analytikerin-Programmiererin von Java-Anwendungen in Geldautomaten für Kunden
- Software Development Expertin für die Validierung von Unterschriften und die Anwendung zur Dokumentenverwaltung beim Kunden
- Systemtechnikerin für die Migration von Geräten und für die Verwaltung, Wartung und Schulung von PDA-Mobilgeräten beim Kunden vor Ort
- Technische Ingenieurwissenschaften für Computersysteme Universität Oberta de Catalunya (UOC)
- Masterstudiengang in Computersicherheit und Ethical *Hacking* Offizieller EC-Council und CompTIA von der Fachhochschule für neue Technologien CICE

Hr. Peralta Alonso, Jon

- Rechtsanwalt / DSB Altia Consultores S.A.
- Dozent im Masterstudiengang für Datenschutz, Cybersicherheit und IKT-Recht Öffentliche Universität des Baskenlandes (UPV-EHU)
- Rechtsanwalt / Rechtsbeistand Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Rechtsberater / Praktikant Professionelles Büro: Oscar Padura
- Hochschulabschluss in Jura Öffentliche Universität des Baskenlandes
- Masterstudiengang in Datenschutzbeauftragter. EIS Innovative School
- Masterstudiengang in Rechtswissenschaften. Öffentliche Universität des Baskenlandes
- Masterstudiengang in Zivilprozessrecht. Internationale Universität Isabel I de Castilla

Hr. Redondo, Jesús Serrano

- Junior FrontEnd Entwickler und Junior Cybersecurity Techniker
- FrontEnd-Entwickler bei Telefónica, Madrid
- FrontEnd-Entwickler. Best Pro Consulting SL, Madrid
- Installateur von Telekommunikationsgeräten und -dienstleistungen. Zener Group, Castillo und León
- Installateur von Telekommunikationsgeräten und -dienstleistungen. Lican Comunicaciones SL, Castilla und León
- Zertifikat in Computersicherheit. CFTIC Getafe, Madrid
- Höherer Techniker: Telekommunikation und Computersysteme. IES Trinidad Arroyo, Palencia
- Höherer Techniker: Elektrotechnische MV- und LV-Installationen. IES Trinidad Arroyo, Palencia
- Ausbildung in Reverse Engineering, Stenographie, Verschlüsselung. Incibe Hacker Academy (Incibe Talents)

Die führenden Fachleute auf diesem Gebiet haben sich zusammengetan, um Ihnen das umfassendste Wissen auf diesem Gebiet zu bieten, damit Sie sich mit absoluter Erfolgsgarantie weiterentwickeln können"

05

Struktur und Inhalt

Die Inhalte dieses Weiterbildenden Masterstudiengangs in Management der Informationssicherheit wurden unter Berücksichtigung des aktuellen Stands des Berufs entwickelt, so dass die Studenten das bestmögliche Wissen erhalten und es in ihrem Arbeitsbereich anwenden können. In den 20 Modulen, aus denen sich dieser Studiengang zusammensetzt, werden die Studenten alles über digitales Daten- und Informationsmanagement und Sicherheit lernen und zu echten Spezialisten auf diesem Gebiet werden.

Es gibt kein besseres Programm. Dieser Großmeister bietet Ihnen alles, was Sie brauchen, um der führende Experte in diesen Bereichen zu sein"

Modul 1. Datenanalytik in der Unternehmensorganisation

1.1. Business-Analyse
- 1.1.1. Business-Analyse
- 1.1.2. Datenstruktur
- 1.1.3. Phasen und Elemente

1.2. Datenanalytik im Unternehmen
- 1.2.1. Dashboards und KPI's nach Abteilungen
- 1.2.2. Operative, taktische und strategische Berichterstattung
- 1.2.3. Datenanalytik für jede Abteilung
  - 1.2.3.1. Marketing und Kommunikation
  - 1.2.3.2. Verkauf
  - 1.2.3.3. Kundendienst
  - 1.2.3.4. Einkauf
  - 1.2.3.5. Verwaltung
  - 1.2.3.6. HR
  - 1.2.3.7. Produktion
  - 1.2.3.8. IT

1.3. Marketing und Kommunikation
- 1.3.1. Zu messende KPI's, Anwendungen und Vorteile
- 1.3.2. Marketing-Systeme und *Data Warehouse*
- 1.3.3. Implementierung einer Struktur zur Datenanalyse im Marketing
- 1.3.4. Marketing- und Kommunikationsplan
- 1.3.5. Strategien, Prognosen und Kampagnenmanagement

1.4. Kommerziell und Verkauf
- 1.4.1. Beiträge der Datenanalytik im kommerziellen Bereich
- 1.4.2. Bedürfnisse der Verkaufsabteilung
- 1.4.3. Marktstudien

1.5. Kundendienst
- 1.5.1. Loyalität
- 1.5.2. Persönliche Qualität und emotionale Intelligenz
- 1.5.3. Kundenzufriedenheit

1.6. Einkauf
- 1.6.1. Datenanalytik für die Marktforschung
- 1.6.2. Datenanalytik für die Wettbewerbsforschung
- 1.6.3. Andere Anwendungen

1.7. Verwaltung
- 1.7.1. Bedürfnisse der Verwaltungssabteilung
- 1.7.2. *Data Warehouse* und finanzielle Risikoanalyse
- 1.7.3. *Data Warehouse* und finanzielle Risikoanalyse

1.8. Personalwesen
- 1.8.1. Personalwesen und Vorteile der Datenanalyse
- 1.8.2. Datenanalysetools im Personalwesen
- 1.8.3. Anwendung von Datenanalysen im Personalwesen

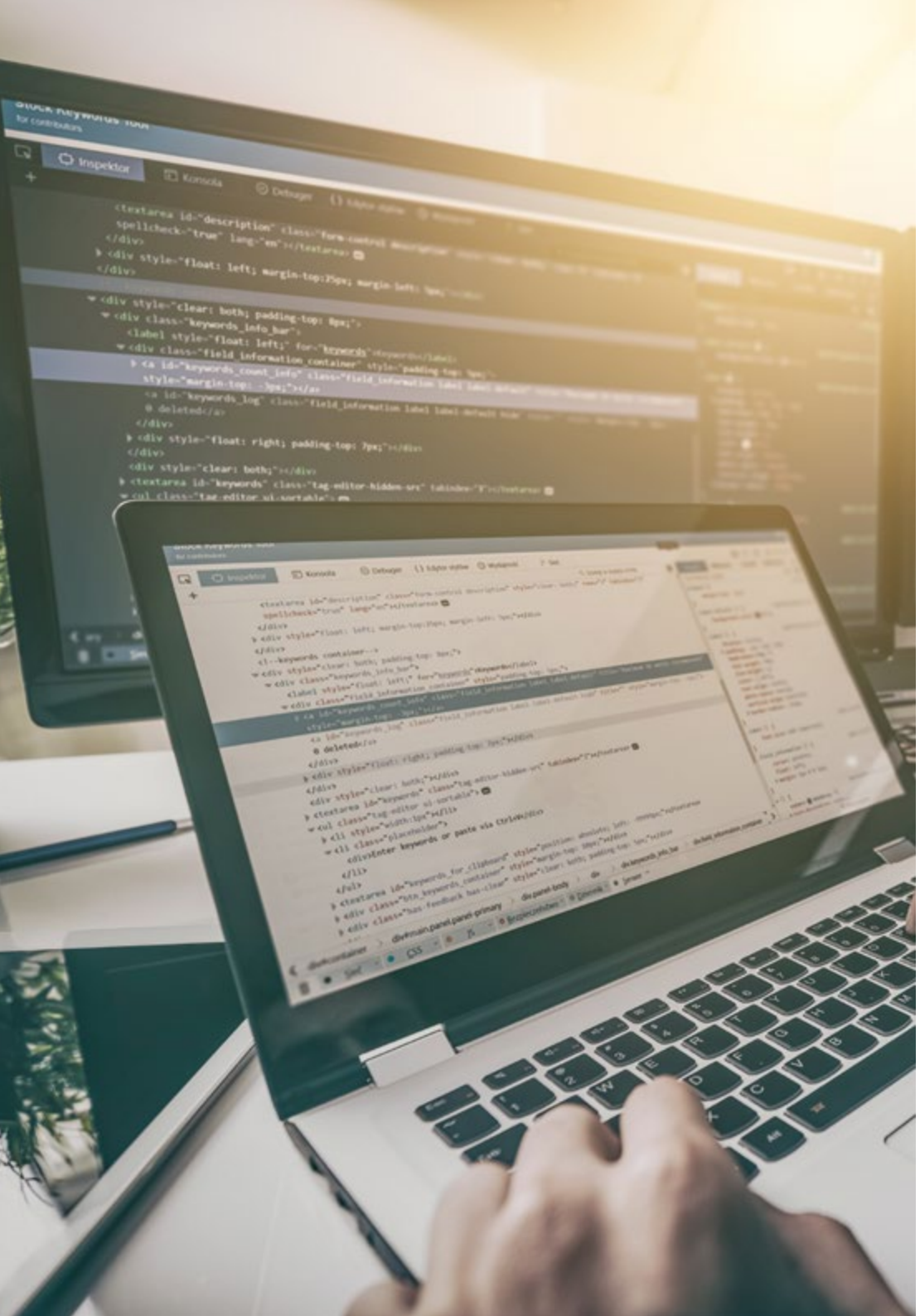
1.9. Produktion
- 1.9.1. Datenanalyse in einer Produktionsabteilung
- 1.9.2. Anwendungen
- 1.9.3. Vorteile

1.10. IT
- 1.10.1. IT-Abteilung
- 1.10.2. Datenanalytik und digitale Transformation
- 1.10.3. Innovation und Produktivität

Modul 2. Datenverwaltung, Datenbearbeitung und Informationen für die Datenwissenschaft

2.1. Statistik Variablen, Indizes und Kennziffern
- 2.1.1. Die Statistik
- 2.1.2. Statistische Dimensionen
- 2.1.3. Variablen, Indizes und Kennziffern

2.2. Daten-Typologie
- 2.2.1. Qualitative
- 2.2.2. Quantitative
- 2.2.3. Charakterisierung und Kategorien



2.3. Wissen über Daten aus Messungen
- 2.3.1. Maßnahmen der Zentralisierung
- 2.3.2. Maße der Streuung
- 2.3.3. Korrelation

2.4. Wissen über Daten aus Diagrammen
- 2.4.1. Visualisierung nach Datentyp
- 2.4.2. Interpretation von grafischen Informationen
- 2.4.3. Anpassung von Grafiken mit R

2.5. Wahrscheinlichkeit
- 2.5.1. Wahrscheinlichkeit
- 2.5.2. Wahrscheinlichkeitsfunktion
- 2.5.3. Verteilungen

2.6. Datenerhebung
- 2.6.1. Methodik der Erhebung
- 2.6.2. Erhebungsinstrumente
- 2.6.3. Kanäle für die Erhebung

2.7. Datenbereinigung
- 2.7.1. Phasen der Datenbereinigung
- 2.7.2. Qualität der Daten
- 2.7.3. Datenmanipulation (mit R)

2.8. Datenanalyse, Interpretation und Bewertung der Ergebnisse
- 2.8.1. Statistische Maßnahmen
- 2.8.2. Beziehungsindizes
- 2.8.3. Data Mining

2.9. Datenlager (*Data Warehouse*)
- 2.9.1. Elemente
- 2.9.2. Entwurf

2.10. Verfügbarkeit von Daten
- 2.10.1. Zugang
- 2.10.2. Nützlichkeit
- 2.10.3. Sicherheit

Modul 3. IoT-Geräte und -Plattformen als Grundlage für die Datenwissenschaft

3.1. *Internet of Things*
- 3.1.1. Internet der Zukunft, *Internet of Things*
- 3.1.2. Das Konsortium Industrielles Internet

3.2. Referenzarchitektur
- 3.2.1. Die Referenzarchitektur
- 3.2.2. Schichten
- 3.2.3. Komponenten

3.3. Sensoren und IoT-Geräte
- 3.3.1. Hauptkomponenten
- 3.3.2. Sensoren und Aktoren

3.4. Kommunikation und Protokolle
- 3.4.1. Protokolle. OSI-Modell
- 3.4.2. Kommunikationstechnologien

3.5. *Cloud*-Plattformen für IoT und IIoT
- 3.5.1. Allzweck-Plattformen
- 3.5.2. Industrielle Plattformen
- 3.5.3. Open-Source-Plattformen

3.6. Datenmanagement in IoT-Plattformen
- 3.6.1. Mechanismen zur Datenverwaltung. Offene Daten
- 3.6.2. Datenaustausch und Visualisierung

3.7. IoT-Sicherheit
- 3.7.1. Sicherheitsanforderungen und -bereiche
- 3.7.2. IIoT-Sicherheitsstrategien

3.8. IoT-Anwendungen
- 3.8.1. Intelligente Städte
- 3.8.2. Gesundheit und Fitness
- 3.8.3. Intelligentes Zuhause
- 3.8.4. Andere Anwendungen

3.9. IIoT-Anwendungen
- 3.9.1. Herstellung
- 3.9.2. Transport
- 3.9.3. Energie
- 3.9.4. Landwirtschaft und Viehzucht
- 3.9.5. Andere Sektoren

3.10. Industrie 4.0
- 3.10.1. IoRT *(Internet of Robotics Things)*
- 3.10.2. 3D Additive Fertigung
- 3.10.3. *Big Data Analytics*

Modul 4. Grafische Darstellung für die Datenanalyse

4.1. Explorative Analyse
- 4.1.1. Repräsentation für die Informationsanalyse
- 4.1.2. Der Wert der grafischen Darstellung
- 4.1.3. Neue Paradigmen der grafischen Darstellung

4.2. Optimierung für Datenwissenschaft
- 4.2.1. Farbpalette und Design
- 4.2.2. Gestalt in der grafischen Darstellung
- 4.2.3. Zu vermeidende Fehler und Tipps

4.3. Grundlegende Datenquellen
- 4.3.1. Für die Qualitätsdarstellung
- 4.3.2. Für die Mengendarstellung
- 4.3.3. Für die Zeitdarstellung

4.4. Komplexe Datenquellen
- 4.4.1. Dateien, Listen und DB
- 4.4.2. Offene Daten
- 4.4.3. Kontinuierlich generierte Daten

4.5. Arten von Grafiken
- 4.5.1. Grundlegende Darstellungen
- 4.5.2. Blockdarstellung
- 4.5.3. Darstellung für die Ausbreitungsanalyse
- 4.5.4. Zirkuläre Darstellungen
- 4.5.5. Blasen-Darstellungen
- 4.5.6. Geografische Darstellung

4.6. Arten der Visualisierung
- 4.6.1. Vergleichend und relational
- 4.6.2. Verteilung
- 4.6.3. Hierarchisch

4.7. Berichtsentwurf mit grafischer Darstellung
- 4.7.1. Anwendung von Diagrammen in Marketingberichten
- 4.7.2. Anwendung von Diagrammen in Dashboards und KPI's
- 4.7.3. Anwendung von Grafiken in strategischen Plänen
- 4.7.4. Andere Verwendungen: Wissenschaft, Gesundheit, Wirtschaft

4.8. Grafisches Geschichtenerzählen
- 4.8.1. Grafisches Geschichtenerzählen
- 4.8.2. Entwicklung
- 4.8.3. Nützlichkeit

4.9. Visualisierungsorientierte Tools
- 4.9.1. Erweiterte Tools
- 4.9.2. Online-Software
- 4.9.3. *Open Source*

4.10. Neue Technologien zur Datenvisualisierung
- 4.10.1. Systeme zur Virtualisierung der Realität
- 4.10.2. Systeme für Realitätserweiterung und -verbesserung
- 4.10.3. Intelligente Systeme

Modul 5. Tools der Datenwissenschaft

5.1. Datenwissenschaft
- 5.1.1. Datenwissenschaft
- 5.1.2. Fortgeschrittene Tools für den Data Scientist

5.2. Daten, Informationen und Wissen
- 5.2.1. Daten, Informationen und Wissen
- 5.2.2. Datentypen
- 5.2.3. Datenquellen

5.3. Von Daten zu Informationen
- 5.3.1. Analyse der Daten
- 5.3.2. Arten der Analyse
- 5.3.3. Extraktion von Informationen aus einem *Dataset*

5.4. Extraktion von Informationen durch Visualisierung
- 5.4.1. Visualisierung als Analyseinstrument
- 5.4.2. Methoden der Visualisierung
- 5.4.3. Visualisierung eines Datensatzes

5.5. Qualität der Daten
- 5.5.1. Datenqualität
- 5.5.2. Datenbereinigung
- 5.5.3. Grundlegende Datenvorverarbeitung

5.6. *Dataset*
- 5.6.1. *Dataset*-Anreicherung
- 5.6.2. Der Fluch der Dimensionalität
- 5.6.3. Ändern unseres Datensatzes

5.7. Ungleichgewicht
- 5.7.1. Ungleichgewicht der Klassen
- 5.7.2. Techniken zur Begrenzung von Ungleichgewichten
- 5.7.3. *Dataset*-Abgleich

5.8. Unüberwachte Modelle
- 5.8.1. Unüberwachtes Modell
- 5.8.2. Methoden
- 5.8.3. Klassifizierung mit unüberwachten Modellen

5.9. Überwachte Modelle
- 5.9.1. Überwachtes Modell
- 5.9.2. Methoden
- 5.9.3. Klassifizierung mit überwachten Modellen

5.10. Tools und bewährte Verfahren
- 5.10.1. Bewährte Praktiken für einen Data Scientist
- 5.10.2. Das beste Modell
- 5.10.3. Nützliche Tools

Modul 6. Data Mining - Auswahl, Vorverarbeitung und Transformation

6.1. Statistische Inferenz
- 6.1.1. Deskriptive Statistik vs. Statistische Inferenz
- 6.1.2. Parametrische Verfahren
- 6.1.3. Nicht-parametrische Verfahren

6.2. Explorative Analyse
- 6.2.1. Deskriptive Analyse
- 6.2.2. Visualisierung
- 6.2.3. Vorbereitung der Daten

6.3. Vorbereitung der Daten
- 6.3.1. Datenintegration und -bereinigung
- 6.3.2. Normalisierung der Daten
- 6.3.3. Attribute umwandeln

6.4. Verlorene Werte
- 6.4.1. Umgang mit verlorenen Werten
- 6.4.2. Maximum-Likelihood-Imputationsmethoden
- 6.4.3. Imputation verlorener Werte durch maschinelles Lernen

6.5. Datenrauschen
- 6.5.1. Lärmklassen und Attribute
- 6.5.2. Rauschfilterung
- 6.5.3. Rauscheffekt

6.6. Der Fluch der Dimensionalität
- 6.6.1. *Oversampling*
- 6.6.2. *Undersampling*
- 6.6.3. Multidimensionale Datenreduktion

6.7. Kontinuierliche zu diskreten Attributen
- 6.7.1. Kontinuierliche versus diskrete Daten
- 6.7.2. Prozess der Diskretisierung

6.8. Daten
- 6.8.1. Datenauswahl
- 6.8.2. Perspektiven und Auswahlkriterien
- 6.8.3. Methoden der Auswahl

6.9. Auswahl der Instanzen
- 6.9.1. Methoden für die Instanzauswahl
- 6.9.2. Auswahl der Prototypen
- 6.9.3. Erweiterte Methoden für die Instanzauswahl

6.10. Vorverarbeitung von Daten in *Big Data*-Umgebungen
- 6.10.1. *Big Data*
- 6.10.2. "Klassische" versus massive Vorbearbeitung
- 6.10.3. *Smart Data*

Modul 7. Vorhersagbarkeit und Analyse von stochastischen Phänomenen

7.1. Zeitreihen
- 7.1.1. Zeitreihen
- 7.1.2. Nützlichkeit und Anwendbarkeit
- 7.1.3. Verwandte Kasuistik

7.2. Die Zeitreihen
- 7.2.1. Saisonaler Trend von ZR
- 7.2.2. Typische Variationen
- 7.2.3. Residuale Analyse

7.3. Typologien
- 7.3.1. Stationär
- 7.3.2. Nicht stationär
- 7.3.3. Transformationen und Anpassungen

7.4. Schemata für Zeitreihen
- 7.4.1. Additives (Modell) Schema
- 7.4.2. Multiplikatives (Modell) Schema
- 7.4.3. Verfahren zur Bestimmung der Art des Modells

7.5. Grundlegende Methoden des *Forecast*
- 7.5.1. Durchschnitt
- 7.5.2. *Naiv*
- 7.5.3. Saisonale *Naïve*
- 7.5.4. Vergleich der Methoden

7.6. Residuale Analyse
- 7.6.1. Autokorrelation
- 7.6.2. ACF der Residuen
- 7.6.3. Korrelationstest

7.7. Regression im Kontext von Zeitreihen
- 7.7.1. ANOVA
- 7.7.2. Grundlagen
- 7.7.3. Praktische Anwendung

7.8. Prädiktive Zeitreihenmodelle
- 7.8.1. ARIMA
- 7.8.2. Exponentiale Glättung

7.9. Zeitreihenmanipulation und -analyse mit R
- 7.9.1. Vorbereitung der Daten
- 7.9.2. Muster-Identifizierung
- 7.9.3. Modell-Analyse
- 7.9.4. Vorhersage

7.10. Grafische Analyse kombiniert mit R
- 7.10.1. Typische Situationen
- 7.10.2. Praktische Anwendung zum Lösen einfacher Probleme
- 7.10.3. Praktische Anwendung für fortgeschrittene Problemlösungen

Modul 8. Design und Entwicklung von intelligenten Systemen

8.1. Vorverarbeitung der Daten
- 8.1.1. Vorverarbeitung der Daten
- 8.1.2. Datenumwandlung
- 8.1.3. Data Mining

8.2. Automatisches Lernen
- 8.2.1. Überwachtes und unüberwachtes Lernen
- 8.2.2. Lernen durch Verstärkung
- 8.2.3. Andere Lern-Paradigma

8.3. Klassifizierungsalgorithmen
- 8.3.1. Induktives automatisches Lernen
- 8.3.2. SVM und KNN
- 8.3.3. Metriken und Punktzahlen für die Rangliste

8.4. Regressionsalgorithmen
- 8.4.1. Lineare Regression, logistische Regression und nicht-lineare Modelle
- 8.4.2. Zeitreihen
- 8.4.3. Regressionsmetriken und -werte

8.5. Clustering-Algorithmen
- 8.5.1. Hierarchische Clustering-Techniken
- 8.5.2. Partitionelle Clustering-Techniken
- 8.5.3. *Clustering*-Metriken und -Bewertungen

8.6. Assoziationsregel-Techniken
- 8.6.1. Methoden zur Extraktion von Regeln
- 8.6.2. Metriken und Punktzahlen für Assoziationsregel-Algorithmen

8.7. Erweiterte Klassifizierungstechniken. Multiklassifizierer
- 8.7.1. *Bagging*-Algorithmen
- 8.7.2. "*Random Forests*" Sortierer
- 8.7.3. "*Boosting*" für Entscheidungsbäume

8.8. Probabilistische grafische Modelle
- 8.8.1. Probabilistische Modelle
- 8.8.2. Bayes'sche Netzwerke. Eigenschaften, Darstellung und Parametrisierung
- 8.8.3. Andere probabilistische grafische Modelle

8.9. Neuronale Netze
- 8.9.1. Maschinelles Lernen mit künstlichen neuronalen Netzen
- 8.9.2. *Feedforward*-Netzwerke

8.10. Tiefes Lernen
- 8.10.1. Tiefe *Feedforward*-Netzwerke
- 8.10.2. Faltungsneuronale Netze und Sequenzmodelle
- 8.10.3. Tools für die Implementierung tiefer neuronaler Netze

Modul 9. Datenintensive Architekturen und Systeme

9.1. Nicht-funktionale Anforderungen. Säulen der Big Data-Anwendungen
- 9.1.1. Verlässlichkeit
- 9.1.2. Anpassungsfähigkeit
- 9.1.3. Instandhaltbarkeit

9.2. Datenmodelle
- 9.2.1. Relationales Modell
- 9.2.2. Dokumentarisches Modell
- 9.2.3. Graph-Datenmodell

9.3. Datenbanken. Verwaltung der Speicherung und des Abrufs von Daten
- 9.3.1. Hash-Indizes
- 9.3.2. Strukturierte Speicherung von Logs
- 9.3.3. B-Bäume

9.4. Datenverschlüsselungsformate
- 9.4.1. Sprachspezifische Formate
- 9.4.2. Standardisierte Formate
- 9.4.3. Binäre Kodierungsformate
- 9.4.4. Prozessübergreifender Datenfluss

9.5. Replikation
- 9.5.1. Ziele der Replikation
- 9.5.2. Replikationsmodelle
- 9.5.3. Probleme mit der Replikation

9.6. Verteilte Transaktionen
- 9.6.1. Transaktion
- 9.6.2. Protokolle für verteilte Transaktionen
- 9.6.3. Serialisierbare Transaktionen

9.7. Aufteilung
- 9.7.1. Formulare unterteilen
- 9.7.2. Interaktion von Sekundärindex und Partitionierung
- 9.7.3. Partitionierung neu ausbalancieren

9.8. *Offline*-Datenverarbeitung
- 9.8.1. Stapelverarbeitung
- 9.8.2. Verteilte Dateisysteme
- 9.8.3. *MapReduce*

9.9. Datenverarbeitung in Echtzeit
- 9.9.1. Message *Broker*-Typen
- 9.9.2. Darstellung von Datenbanken als Datenströme
- 9.9.3. Verarbeitung von Datenströmen

9.10. Praktische Anwendungen im Unternehmen
- 9.10.1. Konsistenz bei der Lektüre
- 9.10.2. Ganzheitlicher Ansatz für Daten
- 9.10.3. Skalierung eines verteilten Dienstes

Modul 10. Praktische Anwendung der Datenwissenschaft in Geschäftsbereichen

10.1. Gesundheitssektor
- 10.1.1. Auswirkungen von KI und Datenanalyse im Gesundheitssektor
- 10.1.2. Chancen und Herausforderungen

10.2. Risiken und Trends in der Gesundheitsbranche
- 10.2.1. Verwendung im Gesundheitssektor
- 10.2.2. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

10.3. Finanzdienstleistungen
- 10.3.1. Auswirkungen von KI und Datenanalyse auf den Finanzdienstleistungssektor
- 10.3.2. Verwendung bei Finanzdienstleistungen
- 10.3.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

10.4. Retail
- 10.4.1. Auswirkungen von KI und Datenanalyse auf den Retail-Sektor
- 10.4.2. Verwendung im Retail
- 10.4.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

10.5. Industrie 4.0
- 10.5.1. Auswirkungen von KI und Datenanalyse in der Industrie 4.0
- 10.5.2. Einsatz in der Industrie 4.0

10.6. Risiken und Trends in der Industrie 4.0
- 10.6.1. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

10.7. Öffentliche Verwaltung
- 10.7.1. Auswirkungen von KI und Datenanalyse in der öffentlichen Verwaltung
- 10.7.2. Verwendung in der öffentlichen Verwaltung
- 10.7.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

10.8. Bildung
- 10.8.1. Auswirkungen von KI und Datenanalyse im Bildungswesen
- 10.8.2. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

10.9. Forst- und Landwirtschaft
- 10.9.1. Auswirkungen von KI und Datenanalyse auf Forst- und Landwirtschaft
- 10.9.2. Verwendung in Forst- und Landwirtschaft
- 10.9.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

10.10. Personalwesen
- 10.10.1. Auswirkungen von KI und Datenanalyse auf das Personalmanagement
- 10.10.2. Praktische Anwendungen in der Geschäftswelt
- 10.10.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

Modul 11. Cyberintelligenz und Cybersicherheit

11.1. Cyberintelligenz
- 11.1.1. Cyberintelligenz
  - 11.1.1.2. Die Intelligenz
    - 11.1.1.2.1. Intelligenz-Zyklus
  - 11.1.1.3. Cyberintelligenz
  - 11.1.1.4. Cyberintelligenz und Cybersicherheit
- 11.1.2. Der Informationsanalyst
  - 11.1.2.1. Die Rolle des Informationsanalysten
  - 11.1.2.2. Voreingenommenheit des Informationsanalysten bei der Bewertung von Aktivitäten

11.2. Cybersicherheit
- 11.2.1. Schichten der Sicherheit
- 11.2.2. Identifizierung von Cyber-Bedrohungen
  - 11.2.2.1. Externe Bedrohungen
  - 11.2.2.2. Interne Bedrohungen
- 11.2.3. Nachteilige Maßnahmen
  - 11.2.3.1. Social Engineering
  - 11.2.3.2. Häufig verwendete Methoden

11.3. Intelligente Tools und Techniken
- 11.3.1. OSINT
- 11.3.2. SOCMINT
- 11.3.3. HUMIT
- 11.3.4. Linux-Distributionen und -Tools
- 11.3.5. OWISAM
- 11.3.6. OWISAP
- 11.3.7. PTES
- 11.3.8. OSSTM

11.4. Methoden der Bewertung
- 11.4.1. Informationsanalyse
- 11.4.2. Techniken zur Organisation der erworbenen Informationen
- 11.4.3. Verlässlichkeit und Glaubwürdigkeit von Informationsquellen
- 11.4.4. Methodologien der Analyse
- 11.4.5. Präsentation der Geheimdienstergebnisse

11.5. Audits und Dokumentation
- 11.5.1. Das IT-Sicherheitsaudit
- 11.5.2. Dokumentation und Berechtigungen für Audits
- 11.5.3. Arten von Audits
- 11.5.4. Liefergegenstände
  - 11.5.4.1. Technischer Bericht
  - 11.5.4.2. Bericht der Geschäftsführung

11.6. Anonymität im Netz
- 11.6.1. Nutzung der Anonymität
- 11.6.2. Anonymisierungstechniken (Proxy, VPN)
- 11.6.3. TOR, Freenet und IP2-Netzwerke

11.7. Bedrohungen und Arten von Sicherheit
- 11.7.1. Arten von Bedrohungen
- 11.7.2. Physische Sicherheit
- 11.7.3. Netzwerksicherheit
- 11.7.4. Logische Sicherheit
- 11.7.5. Sicherheit von Webanwendungen
- 11.7.6. Sicherheit für mobile Geräte

11.8. Regulierung und *Compliance*
- 11.8.1. Datenschutz-Grundverordnung
- 11.8.2. Nationale Strategie für Cybersicherheit von 2011
- 11.8.3. ISO 27000- Familie
- 11.8.4. NIST Cybersecurity Framework
- 11.8.5. PIC
- 11.8.6. ISO 27032
- 11.8.7. *Cloud*-Standards
- 11.8.8. SOX
- 11.8.9. ICP

11.9. Risikoanalyse und Metriken
- 11.9.1. Umfang der Risiken
- 11.9.2. Vermögenswerte
- 11.9.3. Bedrohungen
- 11.9.4. Schwachstellen
- 11.9.5. Risikobewertung
- 11.9.6. Risikobehandlung

11.10. Einschlägige Stellen für Cybersicherheit
- 11.10.1. NIST
- 11.10.2. ENISA
- 11.10.3. INCIBE
- 11.10.4. OEA
- 11.10.5. UNASUR - PROSUR

Modul 12. Host-Sicherheit

12.1. Sicherungskopien
- 12.1.1. Strategien zur Datensicherung
- 12.1.2. Tools für Windows
- 12.1.3. Tools für Linux
- 12.1.4. Werkzeuge für MacOS

12.2. Benutzer Antivirus
- 12.2.1. Arten von Antivirenprogrammen
- 12.2.2. Antivirus für Windows
- 12.2.3. Antivirus für Linux
- 12.2.4. Antivirus für MacOS
- 12.2.5. Antivirus für Smartphones

12.3. HIDS Eindringlingsdetektoren
- 12.3.1. Methoden zur Erkennung von Eindringlingen
- 12.3.2. *Sagan*
- 12.3.3. *Aide*
- 12.3.4. *Rkhunter*

12.4. Lokale *Firewall*
- 12.4.1. *Firewalls* für Windows
- 12.4.2. *Firewalls* für Linux
- 12.4.3. *Firewalls* für MacOS

12.5. Passwort-Manager
- 12.5.1. *Password*
- 12.5.2. *LastPass*
- 12.5.3. *KeePass*
- 12.5.4. *Sticky Password*
- 12.5.5. *RoboForm*

12.6. *Phishing*-Detektoren
- 12.6.1. Manuelle *Phishing*-Erkennung
- 12.6.2. *Anti-Phishing*-Tools

12.7. *Spyware*
- 12.7.1. Vermeidungsmechanismen
- 12.7.2. *Anti-Spyware*-Tools

12.8. Tracker
- 12.8.1. Maßnahmen zum Schutz des Systems
- 12.8.2. Anti-Tracker-Tools

12.9. EDR - *Endpunkt-Erkennung und Reaktion*
- 12.9.1. Verhalten des EDR-Systems
- 12.9.2. Unterschiede zwischen EDR und Anti-Virus
- 12.9.3. Die Zukunft der EDR-Systeme

12.10. Kontrolle über die Software-Installation
- 12.10.1. Repositories und Software-Speicher
- 12.10.2. Listen mit erlaubter oder verbotener Software
- 12.10.3. Update-Kriterien
- 12.10.4. Berechtigungen für die Software-Installation

Modul 13. Netzwerksicherheit (Perimeter)

13.1. Systeme zur Erkennung und Abwehr von Bedrohungen
- 13.1.1. Allgemeiner Rahmen für Sicherheitsvorfälle
- 13.1.2. Aktuelle Verteidigungssysteme*: Defense in Depth* und SOC
- 13.1.3. Aktuelle Netzwerkarchitekturen
- 13.1.4. Arten von Tools zur Erkennung und Verhinderung von Vorfällen
  - 13.1.4.1. Netzwerkbasierte Systeme
  - 13.1.4.2. Host-basierte Systeme
  - 13.1.4.3. Zentralisierte Systeme
- 13.1.5. Kommunikation und Erkennung von Instanzen/*Hosts*, Containern und *Serverless*

13.2. *Firewall*
- 13.2.1. Arten von *Firewalls*
- 13.2.2. Angriffe und Schadensbegrenzung
- 13.2.3. Gängige *Firewalls* in Kernel Linux
  - 13.2.3.1. UFW
  - 13.2.3.2. Nftables und iptables
  - 13.2.3.3. *Firewall*
- 13.2.4. Erkennungssysteme auf der Grundlage von Systemlogs
  - 13.2.4.1. TCP *Wrappers*
  - 13.2.4.2. *BlockHosts* und *DenyHosts*
  - 13.2.4.3. Fai2ban

13.3. Systeme zur Erkennung und Verhinderung von Eindringlingen (IDS/IPS)
- 13.3.1. Angriffe auf IDS/IPS
- 13.3.2. IDS/IPS-Systeme
  - 13.3.2.1. *Snort*
  - 13.3.2.2. Suricata

13.4. *Firewalls* der nächsten Generation (NGFW)
- 13.4.1. Unterschiede zwischen NGFW und traditionellen Firewalls
- 13.4.2. Kernkapazitäten
- 13.4.3. Business Lösungen
- 13.4.4. Firewalls für *Cloud*-Dienste
  - 13.4.4.1. *Cloud* VPC Architektur
  - 13.4.4.2. *Cloud* ACLs
  - 13.4.4.3. *Security Group*

13.5. Proxy
- 13.5.1. Arten von Proxys
- 13.5.2. Proxy-Nutzung. Vorteile und Nachteile

13.6. Antivirus-Engines
- 13.6.1. Allgemeiner Kontext von *Malware* und IOCs
- 13.6.2. Probleme mit Anti-Viren-Programmen

13.7. Mailschutzsysteme
- 13.7.1. Antispam
  - 13.7.1.1. Whitelisting und Blacklisting
  - 13.7.1.2. Bayes'sche Filter
- 13.7.2. *Mail Gateway* (MGW)

13.8. SIEM
- 13.8.1. Komponenten und Architektur
- 13.8.2. Korrelationsregeln und Anwendungsfälle
- 13.8.3. Aktuelle Herausforderungen von SIEM-Systemen

13.9. SOAR
- 13.9.1. SOAR und SIEM: Feinde oder Verbündete?
- 13.9.2. Die Zukunft der SOAR-Systeme

13.10. Andere netzwerkbasierte Systeme
- 13.10.1. WAF
- 13.10.2. NAC
- 13.10.3. HoneyPots und HoneyNets
- 13.10.4. CASB

Modul 14. Smartphone-Sicherheit

14.1. Die Welt der mobilen Geräte
- 14.1.1. Arten von mobilen Plattformen
- 14.1.2. IOS-Geräte
- 14.1.3. Android-Geräte

14.2. Verwaltung der mobilen Sicherheit
- 14.2.1. OWASP Projekt für mobile Sicherheit
  - 14.2.1.1. Top 10 Schwachstellen
- 14.2.2. Kommunikation, Netzwerke und Verbindungsarten

14.3. Das mobile Gerät in der Unternehmensumgebung
- 14.3.1. Risiken
- 14.3.2. Sicherheitsrichtlinien
- 14.3.3. Geräteüberwachung
- 14.3.4. Verwaltung mobiler Geräte (MDM)

14.4. Datenschutz und Datensicherheit
- 14.4.1. Informationen Staaten
- 14.4.2. Datenschutz und Vertraulichkeit
  - 14.4.2.1. Zugriffsrechte
  - 14.4.2.2. Verschlüsselung
- 14.4.3. Sichere Speicherung von Daten
  - 14.4.3.1. Sicherer Speicher auf iOS
  - 14.4.3.2. Sicherer Speicher auf Android
- 14.4.4. Bewährte Praktiken bei der Applikationsentwicklung

14.5. Schwachstellen und Angriffsvektoren
- 14.5.1. Schwachstellen
- 14.5.2. Angriffsvektoren
  - 14.5.2.1. *Malware*
  - 14.5.2.2. Exfiltration von Daten
  - 14.5.2.3. Datenmanipulation

14.6. Wichtigste Bedrohungen
- 14.6.1. Ungezwungener Benutzer
- 14.6.2. *Malware*
  - 14.6.2.1. Arten von *Malware*
- 14.6.3. Social Engineering
- 14.6.4. Datenleck
- 14.6.5. Datendiebstahl
- 14.6.6. Ungesicherte *WLAN*-Netzwerke
- 14.6.7. Veraltete Software
- 14.6.8. Bösartige Anwendungen
- 14.6.9. Unsichere Passwörter
- 14.6.10. Schwache oder nicht vorhandene Sicherheitseinstellungen
- 14.6.11. Physischer Zugang

14.6.12. Verlust oder Diebstahl des Geräts
14.6.13. Impersonation (Integrität)
14.6.14. Schwache oder defekte Kryptographie
14.6.15. Denial of Service (DoS)
14.7. Große Angriffe
14.7.1. *Phishing*-Angriffe
14.7.2. Angriffe im Zusammenhang mit Kommunikationsmodi
14.7.3. *Smishing*-Angriffe
14.7.4. *Criptojacking*-Angriffe
14.7.5. *Man in The Middle*
14.8. *Hacking*
14.8.1. *Rooting und Jailbreaking*
14.8.2. Anatomie eines mobilen Angriffs
14.8.2.1. Ausbreitung der Bedrohung
14.8.2.2. Installation von *Malware* auf dem Gerät
14.8.2.3. Persistenz
14.8.2.4. Ausführung der *Payload* und Extraktion von Informationen
14.8.3. *Hacking* auf iOS-Geräten: Mechanismen und Tools
14.8.4. *Hacking* auf Android-Geräten: Mechanismen und Tools
14.9. Penetrationstests
14.9.1. *iOS PenTesting*
14.9.2. *Android PenTesting*
14.9.3. Instrumente
14.10. Schutz und Sicherheit
14.10.1. Sicherheitseinstellungen
14.10.1.1. Auf iOS-Geräten
14.10.1.2. Auf Android-Geräten
14.10.2. Sicherheitsmaßnahmen
14.10.3. Schutz-Tools

Modul 15. IoT-Sicherheit

15.1. Geräte
15.1.1. Arten von Geräten
15.1.2. Standardisierte Architekturen
15.1.2.1. ONEM2M
15.1.2.2. IoTWF
15.1.3. Anwendungsprotokolle
15.1.4. Konnektivitätstechnologien
15.2. IoT-Geräte. Anwendungsbereiche
15.2.1. *SmartHome*
15.2.2. *SmartCity*
15.2.3. Transport
15.2.4. *Wearables*
15.2.5. Gesundheitssektor
15.2.6. IIoT
15.3. Kommunikationsprotokolle
15.3.1. MQTT
15.3.2. LWM2M
15.3.3. OMA-DM
15.3.4. TR-069
15.4. *SmartHome*
15.4.1. Hausautomatisierung
15.4.2. Netzwerke
15.4.3. Haushaltsgeräte
15.4.4. Überwachung und Sicherheit
15.5. *SmartCity*
15.5.1. Beleuchtung
15.5.2. Meteorologie
15.5.3. Sicherheit
15.6. Transport
15.6.1. Lokalisation
15.6.2. Zahlungen leisten und Dienstleistungen in Anspruch nehmen
15.6.3. Konnektivität

15.7. *Wearables*
- 15.7.1. Intelligente Kleidung
- 15.7.2. Intelligenter Schmuck
- 15.7.3. Intelligente Uhren

15.8. Gesundheitssektor
- 15.8.1. Training/Herzfrequenzüberwachung
- 15.8.2. Überwachung von Patienten und älteren Menschen
- 15.8.3. Implantierbare Geräte
- 15.8.4. Chirurgische Roboter

15.9. Konnektivität
- 15.9.1. *WLAN/Gateway*
- 15.9.2. *Bluetooth*
- 15.9.3. Eingebettete Konnektivität

15.10. Verbriefung
- 15.10.1. Dedizierte Netzwerke
- 15.10.2. Passwort Manager
- 15.10.3. Verwendung von verschlüsselten Protokollen
- 15.10.4. Tipps für die Verwendung

Modul 16. Ethisches *Hacking*

16.1. Arbeitsumgebung
- 16.1.1. Linux-Distributionen
  - 16.1.1.1. Kali Linux - Offensive Security
  - 16.1.1.2. Parrot OS
  - 16.1.1.3. Ubuntu
- 16.1.2. Virtualisierungssysteme
- 16.1.3. *Sandbox*
- 16.1.4. Einsatz von Labors

16.2. Methoden
- 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. Open Source Intelligence (OSINT)
- 16.3.2. Suche nach Datenschutzverletzungen und Schwachstellen
- 16.3.3. Verwendung von passiven Tools

16.4. Netzwerk-Scans
- 16.4.1. Tools zum Scannen
  - 16.4.1.1. Nmap
  - 16.4.1.2. Hping3
  - 16.4.1.3. Andere Scan-Tools
- 16.4.2. Scanning-Techniken
- 16.4.3. Techniken zur Umgehung von *Firewalls* und IDS
- 16.4.4. *Banner Grabbing*
- 16.4.5. Netzwerk-Diagramme

16.5. Aufzählung
- 16.5.1. SMTP Aufzählung
- 16.5.2. DNS Aufzählung
- 16.5.3. NetBIOS und Samba Aufzählung
- 16.5.4. LDAP Aufzählung
- 16.5.5. SNMP Aufzählung
- 16.5.6. Andere Aufzählungstechniken

16.6. Scannen auf Schwachstellen
- 16.6.1. Lösungen zum Scannen auf Schwachstellen
  - 16.6.1.1. Qualys
  - 16.6.1.2. Nessus
  - 16.6.1.3. CFI LanGuard
- 16.6.2. Systeme zur Bewertung von Schwachstellen
  - 16.6.2.1. CVSS
  - 16.6.2.2. CVE
  - 16.6.2.3. NVD

16.7. Angriffe auf *drahtlose* Netzwerke
- 16.7.1. Methodik zum *Hacking* drahtloser Netzwerke
  - 16.7.1.1. WLAN Discovery
  - 16.7.1.2. Verkehrsanalyse
  - 16.7.1.3. *Aircrack*-Angriffe
    - 16.7.1.3.1. WEP-Angriffe
    - 16.7.1.3.2. WPA/WPA2-Angriffe
  - 16.7.1.4. *Evil Twin*-Angriffe
  - 16.7.1.5. WPS-Angriffe
  - 16.7.1.6. *Jamming*
- 16.7.2. Tools für drahtlose Sicherheit

16.8. Hacking von Webservern
- 16.8.1. *Cross site Scripting*
- 16.8.2. CSRF
- 16.8.3. *Session Hijacking*
- 16.8.4. *SQLinjection*

16.9. Ausnutzung von Schwachstellen
- 16.9.1. Verwendung von bekannten *Exploits*
- 16.9.2. Verwendung von *Metasploit*
- 16.9.3. Verwendung von *Malware*
  - 16.9.3.1. Definition und Umfang
  - 16.9.3.2. Generierung von *Malware*
  - 16.9.3.3. Umgehung von Anti-Viren-Lösungen

16.10. Persistenz
- 16.10.1. Installation von Rootkits
- 16.10.2. Verwendung von Ncat
- 16.10.3. Verwendung von geplanten Aufgaben für Backdoors
- 16.10.4. Benutzer erstellen
- 16.10.5. HIDS aufspüren

Modul 17. Reverse Engineering

17.1. Compiler
- 17.1.1. Arten von Code
- 17.1.2. Compiler-Phasen
- 17.1.3. Symboltabelle
- 17.1.4. Fehler-Handler
- 17.1.5. GCC Compiler

17.2. Arten der Compiler-Analyse
- 17.2.1. Lexikalische Analyse
  - 17.2.1.1. Terminologie
  - 17.2.1.2. Lexikalische Komponenten
  - 17.2.1.3. LEX Lexikalischer Analysator
- 17.2.2. Syntaktische Analyse
  - 17.2.2.1. Kontextfreie Grammatiken
  - 17.2.2.2. Arten des Parsing
    - 17.2.2.2.1. Top-down-Parsing
    - 17.2.2.2.2. Bottom-up-Parsing
  - 17.2.2.3. Syntaktische Bäume und Ableitungen
  - 17.2.2.4. Arten von Parsern
    - 17.2.2.4.1. LR-Parser (*Left to Right*)
    - 17.2.2.4.2. LALR-Parser
- 17.2.3. Semantische Analyse
  - 17.2.3.1. Attribut-Grammatiken
  - 17.2.3.2. S-Attribute
  - 17.2.3.3. L-Attribute

17.3. Montage Datenstrukturen
- 17.3.1. Variablen
- 17.3.2. Arrays
- 17.3.3. Zeiger
- 17.3.4. Strukturen
- 17.3.5. Objekte

17.4. Assembly Code-Strukturen
- 17.4.1. Auswahl-Strukturen
  - 17.4.1.1. If, else if, Else
  - 17.4.1.2. Switch
- 17.4.2. Iterations-Strukturen
  - 17.4.2.1. For
  - 17.4.2.2. While
  - 17.4.2.3. Verwendung des Break
- 17.4.3. Funktionen

17.5. x86-Hardware-Architektur
- 17.5.1. x86-Prozessorarchitektur
- 17.5.2. x86 Datenstrukturen
- 17.5.3. x86 Code-Strukturen

17.6. ARM Hardware-Architektur
- 17.6.1. ARM-Prozessorarchitektur
- 17.6.2. ARM-Daten-Strukturen
- 17.6.3. ARM-Code-Strukturen

17.7. Statische Code-Analyse
- 17.7.1. Disassembler
- 17.7.2. IDA
- 17.7.3. Code-Rekonstrukteure

17.8. Dynamische Code-Analyse
- 17.8.1. Verhaltensanalyse
  - 17.8.1.1. Kommunikation
  - 17.8.1.2. Überwachung
- 17.8.2. Linux Code-Debugger
- 17.8.3. Windows-Code-Debugger

17.9. *Sandbox*
- 17.9.1. *Sandbox*-Architektur
- 17.9.2. *Sandbox*-Umgehung
- 17.9.3. Erkennungstechniken
- 17.9.4. Ausweichtechniken
- 17.9.5. Gegenmaßnahmen
- 17.9.6. *Sandbox* in Linux
- 17.9.7. *Sandbox* in Windows
- 17.9.8. *Sandox* in MacOS
- 17.9.9. *Sandbox* in Android

17.10. Malware-Analyse
- 17.10.1. Methoden zur *Malware*-Analyse
- 17.10.2. Techniken zur Verschleierung von *Malware*
  - 17.10.2.1. Ausführbare Verschleierung
  - 17.10.2.2. Einschränkung der Ausführungsumgebungen
- 17.10.3. Tools zur Analyse des *Malware*

Modul 18. Sichere Entwicklung

18.1. Sichere Entwicklung
- 18.1.1. Qualität, Funktionalität und Sicherheit
- 18.1.2. Vertraulichkeit, Integrität und Verfügbarkeit
- 18.1.3. Lebenszyklus der Softwareentwicklung

18.2. Phase der Anforderungen
- 18.2.1. Kontrolle der Authentifizierung
- 18.2.2. Kontrolle von Rollen und Privilegien
- 18.2.3. Risikoorientierte Anforderungen
- 18.2.4. Genehmigung von Privilegien

18.3. Analyse- und Entwurfsphasen
- 18.3.1. Komponentenzugriff und Systemverwaltung
- 18.3.2. Prüfpfade
- 18.3.3. Sitzungsmanagement
- 18.3.4. Historische Daten
- 18.3.5. Angemessene Fehlerbehandlung
- 18.3.6. Trennung der Funktionen

18.4. Phase der Implementierung und Kodierung
- 18.4.1. Absicherung der Entwicklungsumgebung
- 18.4.2. Ausarbeitung der technischen Dokumentation
- 18.4.3. Sichere Kodierung
- 18.4.4. Sicherheit der Kommunikation

18.5. Gute sichere Kodierungspraktiken
- 18.5.1. Validierung von Eingabedaten
- 18.5.2. Verschlüsselung der Ausgabedaten
- 18.5.3. Programmierstil
- 18.5.4. Handhabung des Änderungsprotokolls
- 18.5.5. Kryptographische Praktiken
- 18.5.6. Fehler- und Protokollverwaltung
- 18.5.7. Dateiverwaltung
- 18.5.8. Speicherverwaltung
- 18.5.9. Standardisierung und Wiederverwendung von Sicherheitsfunktionen

18.6. Vorbereitung von Servern und *Hardening*
- 18.6.1. Verwaltung von Benutzern, Gruppen und Rollen auf dem Server
- 18.6.2. Software-Installation
- 18.6.3. *Hardening* des Servers
- 18.6.4. Robuste Konfiguration der Anwendungsumgebung

18.7. DB-Vorbereitung und *Hardening*
- 18.7.1. Optimierung der DB-Engine
- 18.7.2. Erstellung eines eigenen Benutzers für die Anwendung
- 18.7.3. Zuweisung der erforderlichen Berechtigungen an den Benutzer
- 18.7.4. *Härtung* der DB

18.8. Testphase
- 18.8.1. Qualitätskontrolle bei Sicherheitskontrollen
- 18.8.2. Stufenweise Code Inspektion
- 18.8.3. Überprüfung der Konfigurationsverwaltung
- 18.8.4. Blackbox-Tests

18.9. Vorbereitungen für den Übergang zur Produktion
- 18.9.1. Änderungskontrolle durchführen
- 18.9.2. Führen Sie die Produktionsumstellung durch
- 18.9.3. *Rollback*-Prozedur durchführen
- 18.9.4. Tests in der Vorproduktionsphase

18.10. Erhaltungsphase
- 18.10.1. Risikobasierte Versicherung
- 18.10.2. White-Box-Tests zur Wartung der Sicherheit
- 18.10.3. Black Box Sicherheits-Wartungstests

Modul 19. Forensische Analyse

19.1. Datenerfassung und Replikation
- 19.1.1. Volatile Datenerfassung
  - 19.1.1.1. System-Informationen
  - 19.1.1.2. Netzwerk-Informationen
  - 19.1.1.3. Volatilität bestellen
- 19.1.2. Statische Datenerfassung
  - 19.1.2.1. Erstellung eines doppelten Bildes
  - 19.1.2.2. Erstellung eines Dokuments für die Überwachungskette
- 19.1.3. Methoden zur Validierung der erfassten Daten
  - 19.1.3.1. Methoden für Linux
  - 19.1.3.2. Methoden für Windows

19.2. Bewertung und Beseitigung von Anti-Forensik-Techniken
- 19.2.1. Ziele der forensischen Techniken
- 19.2.2. Löschung von Daten
  - 19.2.2.1. Löschung von Daten und Dateien
  - 19.2.2.2. Dateiwiederherstellung
  - 19.2.2.3. Wiederherstellung von gelöschten Partitionen
- 19.2.3. Passwortschutz
- 19.2.4. Steganographie
- 19.2.5. Sicheres Löschen von Geräten
- 19.2.6. Verschlüsselung

19.3. Betriebssystem-Forensik
- 19.3.1. Windows-Forensik
- 19.3.2. Linux-Forensik
- 19.3.3. Mac-Forensik

19.4. Netzwerk-Forensik
- 19.4.1. Log-Analyse
- 19.4.2. Korrelation der Daten
- 19.4.3. Netzwerk-Untersuchung
- 19.4.4. Schritte der forensischen Netzwerkanalyse

19.5. Web-Forensik
- 19.5.1. Untersuchung von Webangriffen
- 19.5.2. Angriffserkennung
- 19.5.3. Standort der IP-Adresse

19.6. Datenbank-Forensik
- 19.6.1. MSSQL-Forensik
- 19.6.2. MySQL-Forensik
- 19.6.3. PostgreSQL-Forensik
- 19.6.4. MongoDB-Forensik

19.7. *Cloud*-Forensik
- 19.7.1. Arten von *Cloud*-Verbrechen
  - 19.7.1.1. *Cloud* als Thema
  - 19.7.1.2. *Die Wolke* als Objekt
  - 19.7.1.3. Die *Cloud* als Werkzeug
- 19.7.2. Herausforderungen der *Cloud*-Forensik
- 19.7.3. Untersuchung von *Cloud*-Speicherdiensten
- 19.7.4. Forensische Analyse-Tools für die *Cloud*

19.8. Untersuchung von E-Mail-Verbrechen
- 19.8.1. Mail-Systeme
  - 19.8.1.1. Mail Clients
  - 19.8.1.2. Mail-Server
  - 19.8.1.3. SMTP-Server
  - 19.8.1.4. POP3-Server
  - 19.8.1.5. IMAP4-Server
- 19.8.2. Mail Verbrechen
- 19.8.3. Mail-Nachricht
  - 19.8.3.1. Standard-Kopfzeilen
  - 19.8.3.2. Erweiterte Kopfzeilen
- 19.8.4. Schritte bei der Untersuchung dieser Verbrechen
- 19.8.5. Tools für die E-Mail-Forensik

19.9. Mobile forensische Analyse
- 19.9.1. Zellulare Netzwerke
  - 19.9.1.1. Arten von Netzwerken
  - 19.9.1.2. CDR Inhalt
- 19.9.2. *Subscriber Identity Module* (SIM)
- 19.9.3. Logische Akquisition
- 19.9.4. Physische Akquisition
- 19.9.5. Dateisystem-Erfassung

19.10. Forensische Berichte schreiben und einreichen
- 19.10.1. Wichtige Aspekte eines forensischen Berichts
- 19.10.2. Klassifizierung und Arten von Berichten
- 19.10.3. Leitfaden zum Schreiben eines Berichts
- 19.10.4. Präsentation des Berichts
  - 19.10.4.1. Vorbereitung auf die Zeugenaussage
  - 19.10.4.2. Hinterlegung
  - 19.10.4.3. Der Umgang mit den Medien

Modul 20. Aktuelle und zukünftige Herausforderungen in der IT-Sicherheit

20.1. *Blockchain*-Technologie
- 20.1.2. Anwendungsbereiche
- 20.1.3. Garantie der Vertraulichkeit
- 20.1.4. Garantie der Nicht-Abstreitbarkeit

20.2. Digitales Geld
- 20.2.1. Bitcoins
- 20.2.2. Kryptowährungen
- 20.2.3. Schürfen von Kryptowährungen
- 20.2.4. Schneeballsysteme
- 20.2.5. Andere mögliche Verbrechen und Probleme

20.3. *Deepfake*
- 20.3.2. Auswirkungen auf die Medien
- 20.3.3. Gefahren für die Gesellschaft
- 20.3.4. Erkennungsmechanismen

20.4. Die Zukunft der künstlichen Intelligenz
- 20.4.1. Künstliche Intelligenz und kognitives Computing
- 20.4.2. Anwendungen zur Vereinfachung des Kundendienstes

20.5. Digitale Privatsphäre
- 20.5.1. Wert der Daten im Netzwerk
- 20.5.2. Verwendung von Daten im Netzwerk
- 20.5.3. Datenschutz und Verwaltung digitaler Identitäten

20.6. Cyber-Konflikte, Cyber-Kriminelle und Cyber-Angriffe
- 20.6.1. Auswirkungen der Cybersicherheit auf internationale Konflikte
- 20.6.2. Folgen von Cyberangriffen auf die allgemeine Bevölkerung
- 20.6.3. Arten von Cyber-Kriminellen. Schutzmaßnahmen

20.7. Telearbeit
- 20.7.1. Revolution der Telearbeit während und nach Covid19
- 20.7.2. Engpässe beim Zugang
- 20.7.3. Variation der Angriffsfläche
- 20.7.4. Bedürfnisse der Arbeiter

20.8. Aufkommende *Wireless*-Technologien
- 20.8.1. WPA3
- 20.8.2. 5G
- 20.8.3. Millimeter-Wellen
- 20.8.4. Trend zu *"Get Smart"* anstelle von *"Get more"*

20.9. Künftige Adressierung in Netzwerken
- 20.9.1. Aktuelle Probleme mit der IP-Adressierung
- 20.9.2. IPv6
- 20.9.2. IPv4+
- 20.9.3. Vorteile von IPv4+ gegenüber IPv4
- 20.9.4. Vorteile von IPv6 gegenüber IPv4

20.10. Die Herausforderung, das Bewusstsein für eine frühzeitige und kontinuierliche Schulung der Bevölkerung zu schärfen
- 20.10.1. Aktuelle Strategien der Regierung
- 20.10.2. Der Widerstand der Menschen gegen das Lernen
- 20.10.3. Ausbildungspläne, die von den Unternehmen angenommen werden müssen

06

Methodik

Dieses Fortbildungsprogramm bietet eine andere Art des Lernens. Unsere Methodik wird durch eine zyklische Lernmethode entwickelt: ***das Relearning***.

Dieses Lehrsystem wird z. B. an den renommiertesten medizinischen Fakultäten der Welt angewandt und wird von wichtigen Publikationen wie dem ***New England Journal of Medicine*** als eines der effektivsten angesehen.

Entdecken Sie Relearning, ein System, das das herkömmliche lineare Lernen aufgibt und Sie durch zyklische Lehrsysteme führt: eine Art des Lernens, die sich als äußerst effektiv erwiesen hat, insbesondere in Fächern, die Auswendiglernen erfordern"

Fallstudie zur Kontextualisierung aller Inhalte

Unser Programm bietet eine revolutionäre Methode zur Entwicklung von Fähigkeiten und Kenntnissen. Unser Ziel ist es, Kompetenzen in einem sich wandelnden, wettbewerbsorientierten und sehr anspruchsvollen Umfeld zu stärken.

Mit TECH werden Sie eine Art des Lernens erleben, die die Grundlagen der traditionellen Universitäten in der ganzen Welt verschiebt"

Eine innovative und andersartige Lernmethode

Dieses TECH-Programm ist ein von Grund auf neu entwickeltes, intensives Lehrprogramm, das die anspruchsvollsten Herausforderungen und Entscheidungen in diesem Bereich sowohl auf nationaler als auch auf internationaler Ebene vorsieht. Dank dieser Methodik wird das persönliche und berufliche Wachstum gefördert und ein entscheidender Schritt in Richtung Erfolg gemacht. Die Fallmethode, die Technik, die diesem Inhalt zugrunde liegt, gewährleistet, dass die aktuellste wirtschaftliche, soziale und berufliche Realität berücksichtigt wird.

> *Unser Programm bereitet Sie darauf vor, sich neuen Herausforderungen in einem unsicheren Umfeld zu stellen und in Ihrer Karriere erfolgreich zu sein"*

Die Fallmethode ist das am weitesten verbreitete Lernsystem an den besten Informatikschulen der Welt, seit es sie gibt. Die Fallmethode wurde 1912 entwickelt, damit die Jurastudenten das Recht nicht nur anhand theoretischer Inhalte erlernen, sondern ihnen reale, komplexe Situationen vorlegen, damit sie fundierte Entscheidungen treffen und Werturteile darüber fällen können, wie diese zu lösen sind. Sie wurde 1924 als Standardlehrmethode in Harvard eingeführt.

Was sollte eine Fachkraft in einer bestimmten Situation tun? Mit dieser Frage konfrontieren wir Sie in der Fallmethode, einer handlungsorientierten Lernmethode. Während des gesamten Kurses werden die Studierenden mit mehreren realen Fällen konfrontiert. Sie müssen Ihr gesamtes Wissen integrieren, recherchieren, argumentieren und Ihre Ideen und Entscheidungen verteidigen.

Relearning Methodik

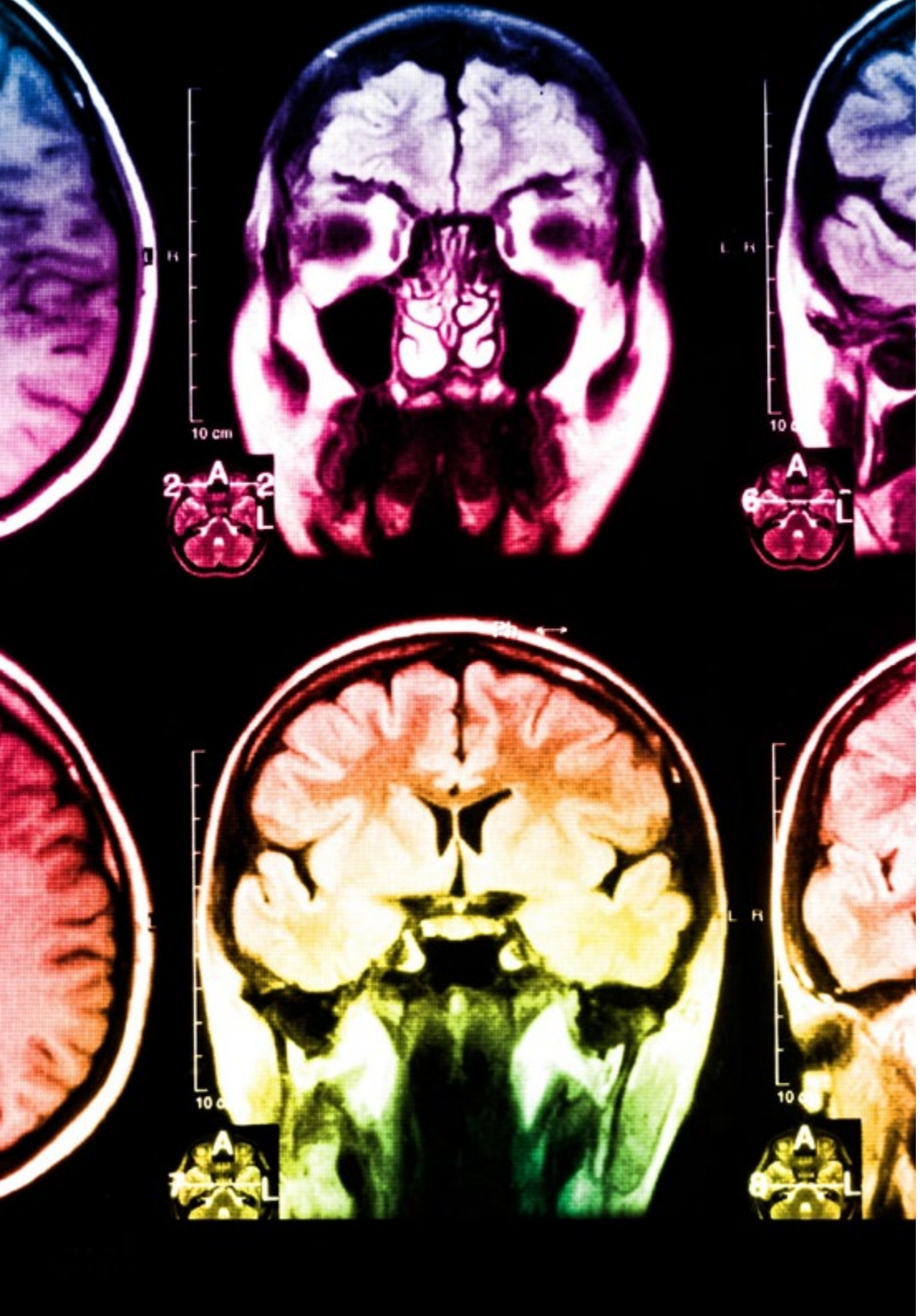
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

Wir ergänzen die Fallstudie mit der besten 100%igen Online-Lehrmethode: Relearning.

Im Jahr 2019 erzielten wir die besten Lernergebnisse aller spanischsprachigen Online-Universitäten der Welt.

Bei TECH lernen Sie mit einer hochmodernen Methodik, die darauf ausgerichtet ist, die Führungskräfte der Zukunft auszubilden. Diese Methode, die an der Spitze der weltweiten Pädagogik steht, wird Relearning genannt.

Unsere Universität ist die einzige in der spanischsprachigen Welt, die für die Anwendung dieser erfolgreichen Methode zugelassen ist. Im Jahr 2019 ist es uns gelungen, die Gesamtzufriedenheit unserer Studenten (Qualität der Lehre, Qualität der Materialien, Kursstruktur, Ziele...) in Bezug auf die Indikatoren der besten Online-Universität in Spanisch zu verbessern.



In unserem Programm ist das Lernen kein linearer Prozess, sondern erfolgt in einer Spirale (lernen, verlernen, vergessen und neu lernen). Daher wird jedes dieser Elemente konzentrisch kombiniert. Mit dieser Methode wurden mehr als 650.000 Hochschulabsolventen mit beispiellosem Erfolg in so unterschiedlichen Bereichen wie Biochemie, Genetik, Chirurgie, internationales Recht, Managementfähigkeiten, Sportwissenschaft, Philosophie, Recht, Ingenieurwesen, Journalismus, Geschichte, Finanzmärkte und -Instrumente ausgebildet. Dies alles in einem sehr anspruchsvollen Umfeld mit einer Studentenschaft mit hohem sozioökonomischem Profil und einem Durchschnittsalter von 43,5 Jahren.

Das Relearning ermöglicht es Ihnen, mit weniger Aufwand und mehr Leistung zu lernen, sich mehr auf Ihr Fachgebiet einzulassen, einen kritischen Geist zu entwickeln, Argumente zu verteidigen und Meinungen zu kontrastieren: eine direkte Gleichung zum Erfolg.

Nach den neuesten wissenschaftlichen Erkenntnissen der Neurowissenschaften wissen wir nicht nur, wie wir Informationen, Ideen, Bilder und Erinnerungen organisieren, sondern auch, dass der Ort und der Kontext, in dem wir etwas gelernt haben, von grundlegender Bedeutung dafür sind, dass wir uns daran erinnern und es im Hippocampus speichern können, um es in unserem Langzeitgedächtnis zu behalten.

Auf diese Weise sind die verschiedenen Elemente unseres Programms im Rahmen des so genannten neurokognitiven kontextabhängigen E-Learnings mit dem Kontext verbunden, in dem der Teilnehmer seine berufliche Praxis entwickelt.

Dieses Programm bietet die besten Lehrmaterialien, die sorgfältig für Fachleute aufbereitet sind:

Studienmaterial

Alle didaktischen Inhalte werden von den Fachleuten, die den Kurs unterrichten werden, speziell für den Kurs erstellt, so dass die didaktische Entwicklung wirklich spezifisch und konkret ist.

Diese Inhalte werden dann auf das audiovisuelle Format angewendet, um die TECH-Online-Arbeitsmethode zu schaffen. Und das alles mit den neuesten Techniken, die dem Studenten qualitativ hochwertige Stücke aus jedem einzelnen Material zur Verfügung stellen.

Meisterklassen

Die Nützlichkeit der Expertenbeobachtung ist wissenschaftlich belegt.

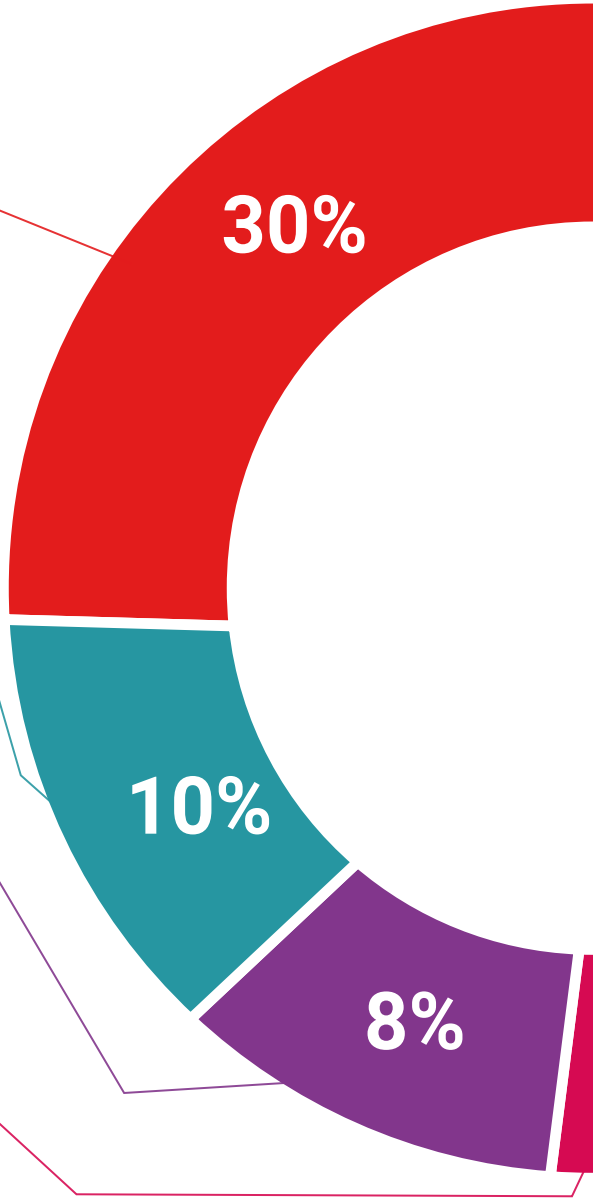
Das sogenannte Learning from an Expert baut Wissen und Gedächtnis auf und schafft Vertrauen für zukünftige schwierige Entscheidungen.

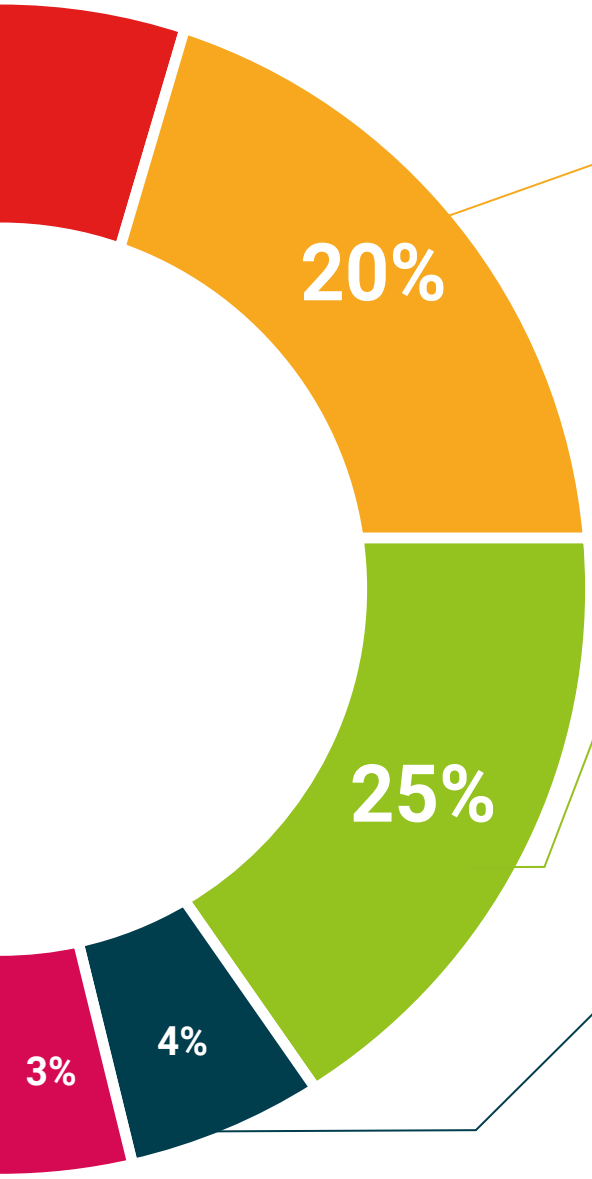
Fertigkeiten und Kompetenzen Praktiken

Sie werden Aktivitäten durchführen, um spezifische Kompetenzen und Fertigkeiten in jedem Fachbereich zu entwickeln. Praktiken und Dynamiken zum Erwerb und zur Entwicklung der Fähigkeiten und Fertigkeiten, die ein Spezialist im Rahmen der Globalisierung, in der wir leben, entwickeln muss.

Weitere Lektüren

Aktuelle Artikel, Konsensdokumente und internationale Leitfäden, u.a. In der virtuellen Bibliothek von TECH haben die Studenten Zugang zu allem, was sie für ihre Ausbildung benötigen.





Fallstudien

Sie werden eine Auswahl der besten Fallstudien vervollständigen, die speziell für diese Qualifizierung ausgewählt wurden. Die Fälle werden von den besten Spezialisten der internationalen Szene präsentiert, analysiert und betreut.

Interaktive Zusammenfassungen

Das TECH-Team präsentiert die Inhalte auf attraktive und dynamische Weise in multimedialen Pillen, die Audios, Videos, Bilder, Diagramme und konzeptionelle Karten enthalten, um das Wissen zu vertiefen.

Dieses einzigartige Bildungssystem für die Präsentation multimedialer Inhalte wurde von Microsoft als "europäische Erfolgsgeschichte" ausgezeichnet.

Prüfung und Nachprüfung

Die Kenntnisse der Studenten werden während des gesamten Programms regelmäßig durch Bewertungs- und Selbsteinschätzungsaktivitäten und -übungen beurteilt und neu bewertet, so dass die Studenten überprüfen können, wie sie ihre Ziele erreichen.

07

Qualifizierung

Der Weiterbildender Masterstudiengang in Management der Informationssicherheit garantiert neben der strengsten und aktuellsten Ausbildung auch den Zugang zu einem von der TECH Technologischen Universität ausgestellten Diplom.

Schließen Sie dieses Programm erfolgreich ab und erhalten Sie Ihren Universitätsabschluss ohne lästige Reisen oder Formalitäten"

Dieser **Weiterbildender Masterstudiengang in Management der Informationssicherheit** enthält das vollständigste und aktuellste Programm auf dem Markt.

Sobald der Student die Prüfungen bestanden hat, erhält er/sie per Post* mit Empfangsbestätigung das entsprechende Diplom, ausgestellt von der **TECH Technologischen Universität**.

Das von **TECH Technologische Universität** ausgestellte Diplom drückt die erworbene Qualifikation aus und entspricht den Anforderungen, die in der Regel von Stellenbörsen, Auswahlprüfungen und Berufsbildungsausschüssen verlangt werden.

Titel: **Weiterbildender Masterstudiengang in Management der Informationssicherheit**

Anzahl der offiziellen Arbeitsstunden: **3.000 Std.**

tech technologische universität

Verleiht dieses

DIPLOM

an

Herr/Frau _____, mit Ausweis-Nr. _____

Für den erfolgreichen Abschluss und die Akkreditierung des Programms

WEITERBILDENDER MASTERSTUDIENGANG

in

Management der Informationssicherheit

Es handelt sich um einen von dieser Universität verliehenen Abschluss, mit einer Dauer von 3.000 Stunden, mit Anfangsdatum tt/mm/jjjj und Enddatum tt/mm/jjjj.

TECH ist eine private Hochschuleinrichtung, die seit dem 28. Juni 2018 vom Ministerium für öffentliche Bildung anerkannt ist.

Zum 17. Juni 2020

Tere Guevara Navarro
Rektorin

einzigartiger Code TECH: AFWOR23S techtitute.com/titel

Weiterbildender Masterstudiengang in Management der Informationssicherheit

Allgemeiner Aufbau des Lehrplans

Kurs	Modul	Stunden	Kategorie
1°	Datenanalytik in der Unternehmensorganisation	150	OB
1°	Datenverwaltung, Datenbearbeitung und Informationen für die Datenwissenschaft	150	OB
1°	IoT-Geräte und -Plattformen als Grundlage für die Datenwissenschaft	150	OB
1°	Grafische Darstellung für die Datenanalyse	150	OB
1°	Tools der Datenwissenschaft	150	OB
1°	Data Mining - Auswahl, Vorverarbeitung und Transformation	150	OB
1°	Vorhersagbarkeit und Analyse von stochastischen Phänomenen	150	OB
1°	Design und Entwicklung von intelligenten Systemen	150	OB
1°	Datenintensive Architekturen und Systeme	150	OB
1°	Praktische Anwendung der Datenwissenschaft in Geschäftsbereichen	150	OB
2°	Cyberintelligenz und Cybersicherheit	150	OB
2°	Host-Sicherheit	150	OB
2°	Netzwerksicherheit (Perimeter)	150	OB
2°	Smartphone-Sicherheit	150	OB
2°	IoT-Sicherheit	150	OB
2°	Ethisches *Hacking*	150	OB
2°	Reverse Engineering	150	OB
2°	Sichere Entwicklung	150	OB
2°	Forensische Analyse	150	OB
2°	Aktuelle und zukünftige Herausforderungen in der IT-Sicherheit	150	OB

Tere Guevara Navarro
Rektorin

tech technologische universität

*Haager Apostille. Für den Fall, dass der Student die Haager Apostille für sein Papierdiplom beantragt, wird TECH EDUCATION die notwendigen Vorkehrungen treffen, um diese gegen eine zusätzliche Gebühr zu beschaffen.

tech technologische universität

Weiterbildender Masterstudiengang

Management der Informationssicherheit

- Modalität: **online**
- Dauer: **2 Jahre**
- Qualifizierung: **TECH Technologische Universität**
- Aufwand: **16 Std./Woche**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Weiterbildender Masterstudiengang
Management der Informationssicherheit

tech technologische universität