Privater Masterstudiengang

MBA in Fortgeschrittenes Cybersecurity Management (CISO)

tech technologische universität

tech technologische universität

Privater Masterstudiengang
MBA in Fortgeschrittenes Cybersecurity Management (CISO)

- Modalität: **online**
- Dauer: **12 Monate**
- Qualifizierung: **TECH Technologische Universität**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Internetzugang: www.techtitute.com/de/informatik/masterstudiengang/masterstudiengang-mba-fortgeschrittenes-cybersecurity-management-ciso

Index

01

Präsentation

Die Welt von heute bewegt sich auf eine vollständige Digitalisierung zu. Immer mehr grundlegende Prozesse, Vorgänge und Aufgaben aller Art werden über ein elektronisches Gerät abgewickelt. Aber dieser Fortschritt birgt auch gewisse Risiken, da Computer, *Smartphones*, *Tablets* und alle Arten von digitalen Anwendungen anfällig für Cyberangriffe sein können. Aus diesem Grund sind viele Unternehmen auf der Suche nach Experten, die die Cybersicherheit ihrer Dienste effektiv steuern und verwalten können. Dieses neue Berufsprofil ist sehr gefragt. Daher wurde dieses Programm entwickelt, um den Informatikern die neuesten Kenntnisse und Techniken zu vermitteln und sie darauf vorzubereiten, in jedem Unternehmen, das dies benötigt, als Direktor für Cybersicherheit zu arbeiten.

Dieses Programm bereitet Sie intensiv darauf vor, sich auf das Management von Cybersicherheit zu spezialisieren, dem derzeit gefragtesten Berufsprofil im IT-Bereich“

In den letzten Jahren hat sich der Prozess der Digitalisierung beschleunigt, angetrieben durch die kontinuierlichen Fortschritte in der Informationstechnologie. Es ist also nicht nur die Technologie, die sich stark verbessert hat, sondern auch die digitalen Werkzeuge selbst, mit denen viele Aufgaben heute erledigt werden. Diese Fortschritte haben es zum Beispiel ermöglicht, dass viele Bankgeschäfte über eine mobile Anwendung abgewickelt werden können. Auch im Gesundheitssektor hat sich einiges getan, sei es bei den Terminsystemen oder beim Zugang zu medizinischen Unterlagen. Außerdem ist es dank dieser Technologien möglich, Rechnungen einzusehen oder Dienstleistungen von Unternehmen in Bereichen wie der Telefonie anzufordern.

Aber diese Fortschritte haben auch zu einer Zunahme von Computerschwachstellen geführt. So haben sich zwar die Möglichkeiten zur Durchführung verschiedener Aktivitäten und Aufgaben erweitert, aber die Angriffe auf die Sicherheit von Geräten, Anwendungen und Websites haben proportional zugenommen. Aus diesem Grund suchen immer mehr Unternehmen nach Fachleuten, die auf Cybersicherheit spezialisiert sind und ihnen einen angemessenen Schutz gegen alle Arten von Computerangriffen bieten können.

Daher ist das Profil des Cybersecurity Direktors eines der gefragtesten bei Unternehmen, die im Internet tätig sind oder Dienstleistungen im digitalen Umfeld anbieten. Und um dieser Nachfrage gerecht zu werden, hat TECH diesen MBA in Fortgeschrittenes Cybersecurity Management (CISO) entwickelt, der den Informatikern alle notwendigen Werkzeuge an die Hand gibt, um diese Position effektiv und unter Berücksichtigung der neuesten Entwicklungen in Bezug auf Schutz und Schwachstellen in diesem technologischen Bereich auszuüben.

In diesem Programm können sie sich mit Aspekten wie der Sicherheit bei der Entwicklung und dem Design von Systemen, den besten kryptographischen Techniken und der Sicherheit in *Cloud-Computing*-Umgebungen befassen. Sie werden dabei eine 100%ige Online-Methode anwenden, die es ihnen ermöglicht, ihre berufliche Tätigkeit mit ihrem Studium zu verbinden, ohne starre Zeitpläne oder unbequeme Fahrten zu einem akademischen Zentrum. Darüber hinaus stehen ihnen zahlreiche multimediale Studienmittel zur Verfügung, die von den renommiertesten und spezialisiertesten Dozenten auf dem Gebiet der Cybersicherheit unterrichtet werden.

Dieser **MBA in Fortgeschrittenes Cybersecurity Management (CISO)** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- Die Entwicklung praktischer Fälle, die von Experten für Informatik und Cybersicherheit vorgestellt werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt vermittelt alle für die berufliche Praxis unverzichtbaren wissenschaftlichen und praktischen Informationen
- Die praktischen Übungen, bei denen der Selbstbewertungsprozess zur Verbesserung des Lernens durchgeführt werden kann
- Sein besonderer Schwerpunkt liegt auf innovativen Methoden
- Theoretische Lektionen, 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

Erfahren Sie aus erster Hand mehr über die besten Sicherheitstechniken für Cloud-Computing-Umgebungen oder die Blockchain-Technologie“

Sie kommen in den Genuss zahlreicher multimedialer Inhalte, um Ihren Studienprozess zu beschleunigen, und werden dabei von einem hoch angesehenen Dozententeam auf dem Gebiet der Cybersicherheit unterstützt“

Die Online-Methode von TECH ermöglicht es Ihnen, Zeit und Ort des Studiums selbst zu bestimmen, ohne Ihre berufliche Tätigkeit zu beeinträchtigen.

Sie können der Cybersecurity-Direktor der besten Unternehmen in Ihrer Region werden.

Das Dozententeam des Programms besteht aus Fachkräften aus der Branche, die ihre Erfahrungen aus ihrer Arbeit in diese Fortbildung einbringen, sowie aus anerkannten Spezialisten von führenden Gesellschaften und renommierten Universitäten.

Die multimedialen Inhalte, die mit der neuesten Bildungstechnologie entwickelt wurden, werden der Fachkraft ein situiertes und kontextbezogenes Lernen ermöglichen, d. h. eine simulierte Umgebung, die eine immersive Fortbildung bietet, die auf die Ausführung von realen Situationen ausgerichtet ist.

Das Konzept dieses Programms konzentriert sich auf problemorientiertes Lernen, bei dem die Fachkraft versuchen muss, die verschiedenen Situationen aus der beruflichen Praxis zu lösen, die während des gesamten Studiengangs gestellt werden. Zu diesem Zweck wird sie von einem innovativen interaktiven Videosystem unterstützt, das von renommierten Experten entwickelt wurde.

02

Ziele

Die rasante Entwicklung der Computertechnologien hat große Fortschritte mit sich gebracht und der gesamten Bevölkerung zahlreiche Dienste angeboten. Aber auch die Zahl der Schwachstellen und Cyberangriffe hat zugenommen. Deshalb besteht das Hauptziel dieses Programms darin, aus dem Informatiker einen echten Spezialisten für das Management der Cybersicherheit zu machen, was einen enormen und sofortigen beruflichen Fortschritt garantiert. Mit seinen neuen Kenntnissen wird er also die Möglichkeit haben, Zugang zu großen Unternehmen zu erhalten, die in verschiedenen Sektoren digital arbeiten.

Das Ziel dieses Programms ist es, Sie zu einer Fachkraft zu machen, die darauf vorbereitet ist, die Cybersicherheitsabteilung eines großen Unternehmens zu leiten“

Allgemeine Ziele

- Erwerben von Fachwissen über ein Informationssystem, Typen und zu berücksichtigende Sicherheitsaspekte
- Identifizieren der Schwachstellen eines Informationssystems
- Entwickeln der gesetzlichen Bestimmungen und Typisierung von Verbrechen, die ein Informationssystem angreifen
- Bewerten der verschiedenen Sicherheitsarchitekturmodelle, um das für das Unternehmen am besten geeignete Modell zu ermitteln
- Identifizieren der regulatorischen Rahmenbedingungen für die Anwendung und deren Rechtsgrundlagen
- Analysieren der organisatorischen und funktionalen Struktur eines Informationssicherheitsbereichs (das Büro des CISO)
- Analysieren und Entwickeln des Konzepts des Risikos und der Ungewissheit in der Umwelt, in der wir leben
- Prüfen des Risikomanagementmodells auf der Grundlage von ISO 31.000
- Untersuchen der Wissenschaft der Kryptologie und der Beziehung zu ihren Zweigen: Kryptographie, Kryptoanalyse, Steganographie und Stegoanalyse
- Analysieren der Arten von Kryptographie nach der Art des Algorithmus und nach ihrer Verwendung
- Prüfen der digitalen Zertifikate
- Prüfen der *Public Key Infrastructure* (PKI)
- Entwickeln des Konzepts des Identitätsmanagements
- Identifizieren von Authentifizierungsmethoden
- Erwerben von Fachwissen über das Ökosystem der IT-Sicherheit
- Bewerten der Kenntnisse in Bezug auf Cybersicherheit
- Identifizieren der Sicherheitsbereiche in der *Cloud*
- Analysieren der Dienste und Tools in jedem der Sicherheitsbereiche
- Entwickeln der Sicherheitsspezifikationen für jede LPWAN-Technologie
- Vergleichendes Analysieren der Sicherheit von LPWAN-Technologien

Mit diesem privaten Masterstudiengang, der die fortschrittlichsten Kenntnisse im Bereich der Cybersicherheit bietet, werden Ihre beruflichen Ziele in greifbare Nähe rücken“

Spezifische Ziele

Modul 1. Sicherheit in Design und Entwicklung von Systemen

- Bewerten der Sicherheit eines Informationssystems in all seinen Komponenten und Schichten
- Identifizieren aktueller Arten von Sicherheitsbedrohungen und Trends
- Festlegen von Sicherheitsrichtlinien durch Definition von Sicherheits- und Notfallrichtlinien und -plänen
- Analysieren von Strategien und Tools zur Gewährleistung der Integrität und Sicherheit von Informationssystemen
- Anwenden spezifischer Techniken und Tools für jede Art von Angriff oder Sicherheitsschwachstelle
- Schützen der im Informationssystem gespeicherten vertraulichen Informationen
- Kennen des rechtlichen Rahmens und der Typisierung des Verbrechens, um die Vision mit der Typisierung des Täters und seines Opfers zu vervollständigen

Modul 2. Architekturen und Modelle für die Informationssicherheit

- Abstimmen des Sicherheitsmasterplans auf die strategischen Ziele des Unternehmens
- Einrichten eines kontinuierlichen Risikomanagement-Rahmens als integraler Bestandteil des *Master Security Plans*
- Festlegen geeigneter Indikatoren für die Überwachung der Umsetzung des ISMS
- Einrichten einer richtlinienbasierten Sicherheitsstrategie
- Analysieren der Ziele und Verfahren im Zusammenhang mit dem Plan zur Sensibilisierung von Mitarbeitern, Lieferanten und Partnern
- Identifizieren der in jeder Organisation geltenden Vorschriften, Zertifizierungen und Gesetze innerhalb des gesetzlichen Rahmens
- Entwickeln der Schlüsselelemente, die in der Norm ISO 27001:2013 gefordert werden
- Implementieren eines Modells zur Verwaltung des Datenschutzes in Übereinstimmung mit der europäischen GDPR/RGPD-Verordnung

Modul 3. IT-Sicherheitsmanagement

- Identifizieren der verschiedenen Strukturen, die ein Bereich der Informationssicherheit haben kann
- Entwickeln eines Sicherheitsmodells, das auf drei Verteidigungslinien basiert
- Vorstellen der verschiedenen periodischen und außerordentlichen Ausschüsse, in denen der Bereich Cybersicherheit vertreten ist
- Angeben der technologischen Hilfsmittel, die die Hauptfunktionen des *Security Operations Teams* (SOT) unterstützen
- Bewerten der für jedes Szenario geeigneten Maßnahmen zur Kontrolle der Schwachstellen
- Entwickeln des Rahmenwerks für Sicherheitsoperationen auf der Grundlage des NIST CSF
- Festlegen des Umfangs der verschiedenen Arten von Audits (*Red Team*, *Pentesting*, *Bug Bounty* usw.)
- Vorschlagen von Aktivitäten nach einem Sicherheitsvorfall
- Einrichten einer Kommandozentrale für Informationssicherheit, die alle relevanten Akteure (Behörden, Kunden, Lieferanten usw.) einbezieht

Modul 4. Risikoanalyse und IT-Sicherheitsumgebung

- Untersuchen des Umfelds, in dem wir tätig sind, mit einem ganzheitlichen Blick
- Identifizieren der wichtigsten Risiken und Potenziale, die das Erreichen unserer Ziele beeinträchtigen können
- Analysieren der Risiken auf der Grundlage der besten uns zur Verfügung stehenden Methoden
- Bewerten der potenziellen Auswirkungen dieser Risiken und Chancen
- Entwickeln von Techniken, um die Risiken und Potenziale so anzugehen, dass der Mehrwert maximiert wird
- Vertiefen der verschiedenen Techniken zur Übertragung von Risiko und Wert
- Erzielen von Mehrwert durch die Entwicklung eigener Modelle für ein agiles Risikomanagement
- Prüfen der Ergebnisse, um kontinuierliche Verbesserungen im Projekt- und Prozessmanagement auf der Grundlage risikoorientierter oder *Risk-Driven*-Managementmodelle vorzuschlagen
- Innovieren und Umwandeln allgemeiner Daten in relevante Informationen für eine risikobasierte Entscheidungsfindung

Modul 5. Kryptographie in der IT

- Zusammenstellen der grundlegenden Operationen (XOR, große Zahlen, Substitution und Transposition) und der verschiedenen Komponenten (One-Way-Funktionen, Hash, Zufallszahlengeneratoren)
- Analysieren kryptographischer Techniken
- Entwickeln verschiedener kryptographische Algorithmen
- Demonstrieren der Verwendung digitaler Signaturen und ihrer Anwendung in digitalen Zertifikaten
- Bewerten von Schlüsselverwaltungssystemen und der Bedeutung von kryptographischen Schlüssellängen
- Untersuchen von Algorithmen zur Schlüsselableitung
- Analysieren des Lebenszyklus von Schlüsseln
- Auswerten von Blockchiffre- und Stromchiffre-Modi
- Bestimmen der Pseudo-Zufallszahlengeneratoren
- Entwickeln realer Kryptographie-Anwendungen, wie Kerberos, PGP oder Smart Cards
- Prüfen verwandter Verbände und Gremien, wie ISO, NIST oder NCSC
- Bestimmen der Herausforderungen in der Kryptographie des Quantencomputings

Modul 6. Identitäts- und Zugriffsmanagement in der IT-Sicherheit

- Entwickeln des Konzepts der digitalen Identität
- Bewerten der physischen Zugangskontrolle zu Informationen
- Untersuchen der Grundlagen der biometrischen Authentifizierung und MFA-Authentifizierung
- Bewerten von Angriffen auf die Vertraulichkeit von Informationen
- Analysieren des Identitätsverbundes
- Einrichten der Netzwerkzugangskontrolle

Modul 7. Sicherheit bei Kommunikation und Softwarebetrieb
- Entwickeln von Fachwissen über physische und logische Sicherheit
- Demonstrieren von Kenntnissen über Kommunikation und Netzwerke
- Identifizieren größerer bösartiger Angriffe
- Einrichten eines sicheren Entwicklungsrahmen
- Nachweisen von Kenntnissen über die wichtigsten Vorschriften zum Management von Informationssicherheitssystemen
- Begründen des Betriebs eines operativen Zentrums für Cybersicherheit
- Demonstrieren der Bedeutung von Cybersicherheitspraktiken für organisatorische Katastrophen

Modul 8. Sicherheit in *Cloud*-Umgebungen
- Identifizieren der Risiken bei der Bereitstellung einer öffentlichen *Cloud*-Infrastruktur
- Definieren der Sicherheitsanforderungen
- Entwicklung eines Sicherheitsplans für eine *Cloud*-Bereitstellung
- Identifizieren der *Cloud*-Dienste, die für die Ausführung eines Sicherheitsplans eingesetzt werden sollen
- Bestimmen der operativen Anforderungen für Präventionsmechanismen
- Festlegen von Richtlinien für ein Protokollierungs- und Überwachungssystem
- Vorschlagen von Maßnahmen zur Reaktion auf Vorfälle

Modul 9. Sicherheit der Kommunikation von IoT-Geräten
- Einführen in die vereinfachte IoT-Architektur
- Erklären der Unterschiede zwischen allgemeinen Konnektivitätstechnologien und Konnektivitätstechnologien für das IoT
- Etablieren des Konzepts des Eisernen Dreiecks der IoT-Konnektivität
- Analysieren der Sicherheitsspezifikationen der LoRaWAN-Technologie, NB-IoT-Technologie und WiSUN-Technologie
- Begründen der Wahl der richtigen IoT-Technologie für jedes Projekt

Modul 10. *Business Continuity Plan* in Verbindung mit Sicherheit
- Vorstellen der wichtigsten Elemente jeder Phase und die Merkmale des *Business Continuity Plans* (BCP) analysieren
- Begründen der Notwendigkeit eines *Business Continuity Plans*
- Bestimmen der Erfolgs- und Risikokarten für jede Phase des *Business Continuity Plans*
- Festlegen eines Aktionsplans für die Umsetzung
- Bewerten der Vollständigkeit eines *Business Continuity Plans* (BCP)
- Entwickeln des Plans für die erfolgreiche Implementierung eines *Business Continuity Plans*

Modul 11. Führung, Ethik und soziale Verantwortung der Unternehmen
- Analysieren der Auswirkungen der Globalisierung auf die Unternehmensführung und Corporate Governance
- Beurteilen der Bedeutung einer effektiven Führung für das Management und den Erfolg von Unternehmen
- Definieren von interkulturellen Managementstrategien und deren Bedeutung in unterschiedlichen Geschäftsumgebungen
- Entwickeln von Führungsqualitäten und Verstehen der aktuellen Herausforderungen für Führungskräfte
- Bestimmen der Prinzipien und Praktiken der Unternehmensethik und deren Anwendung bei der Entscheidungsfindung in Unternehmen
- Strukturieren von Strategien zur Umsetzung und Verbesserung von Nachhaltigkeit und sozialer Verantwortung in Unternehmen

Modul 12. Personal- und Talentmanagement
- Bestimmen der Beziehung zwischen strategischer Ausrichtung und Personalmanagement
- Vertiefen der Kompetenzen, die für ein effektives kompetenzbasiertes Personalmanagement erforderlich sind
- Vertiefen der Methoden für Leistungsbeurteilung und Leistungsmanagement
- Integrieren von Innovationen im Talentmanagement und deren Auswirkungen auf die Bindung und Loyalität des Personals
- Entwickeln von Strategien zur Motivation und Entwicklung von Hochleistungsteams
- Vorschlagen effektiver Lösungen für das Veränderungsmanagement und die Konfliktlösung in Organisationen

Modul 13. Wirtschaftlich-finanzielle Verwaltung

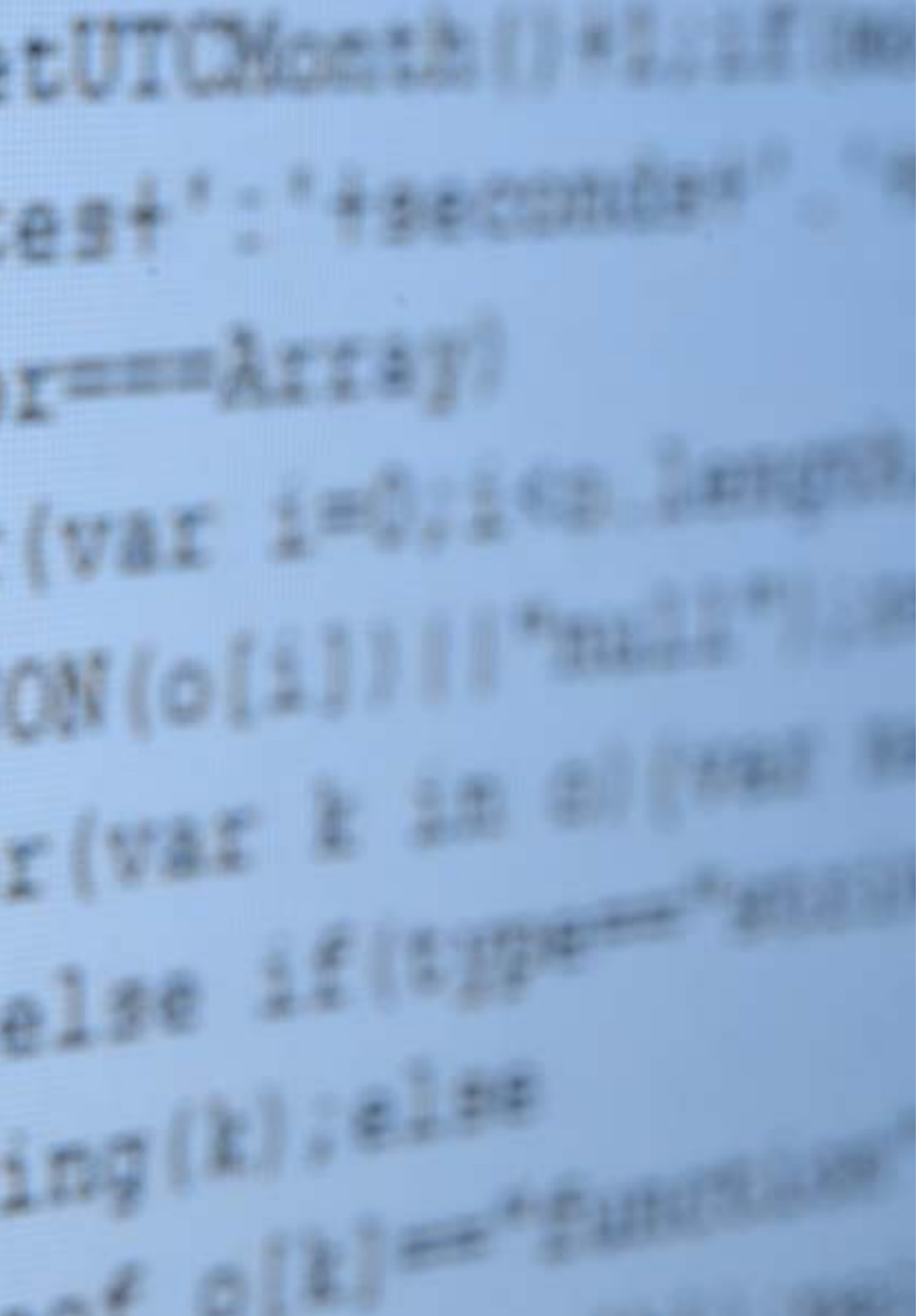
- Analysieren der makroökonomischen Rahmenbedingungen und deren Einfluss auf das nationale und internationale Finanzsystem
- Definieren von Informationssystemen und Business Intelligence für die finanzielle Entscheidungsfindung
- Unterscheiden wichtiger finanzieller Entscheidungen und Risikomanagement im Finanzmanagement
- Bewerten von Strategien für die Finanzplanung und die Beschaffung von Unternehmensfinanzierung

Modul 14. Kaufmännisches Management und strategisches Marketing

- Strukturieren des konzeptionellen Rahmens und der Bedeutung des Marketingmanagements in Unternehmen
- Vertiefen der Schlüsselelemente und Aktivitäten des Marketings und ihrer Auswirkungen auf die Organisation
- Bestimmen der Phasen des Prozesses der strategischen Marketingplanung
- Bewerten von Strategien zur Verbesserung der Unternehmenskommunikation und des digitalen Rufs des Unternehmens

Modul 15. Geschäftsleitung

- Definieren des Konzepts des General Management und seiner Bedeutung für die Unternehmensführung
- Bewerten der Aufgaben und Verantwortlichkeiten des Managements in der Organisationskultur
- Analysieren der Bedeutung von Betriebsmanagement und Qualitätsmanagement in der Wertschöpfungskette
- Entwickeln von Fähigkeiten zur zwischenmenschlichen Kommunikation und zum Sprechen in der Öffentlichkeit für die Ausbildung von Pressesprechern



Mit diesem privaten Masterstudiengang, der die fortschrittlichsten Kenntnisse im Bereich der Cybersicherheit bietet, werden Ihre beruflichen Ziele in greifbare Nähe rücken“

03

Kompetenzen

Dank dieses privaten Masterstudiengangs wird die Fachkraft zahlreiche neue Fähigkeiten auf dem Gebiet der Cybersicherheit erwerben. Das Aufkommen von Technologien wie *Blockchain*, *Cloud Computing* und künstlicher Intelligenz in den letzten Jahren hat zur Entwicklung neuer Bereiche der Cybersicherheit geführt. Aus diesem Grund wurde dieses Programm speziell entwickelt, um Fachleuten alle notwendigen Fähigkeiten zu vermitteln, um sich an diese boomenden Technologien anzupassen.

Die Fähigkeiten, die Ihnen dieses Programm vermittelt, werden es Ihnen ermöglichen, sich auf den neuesten Stand zu bringen und sich an die neue IT-Umgebung anzupassen, in der Technologien wie Blockchain oder künstliche Intelligenz auf den Plan gerückt sind“

Allgemeine Kompetenzen

- Anwenden der am besten geeigneten Sicherheitsmaßnahmen in Abhängigkeit von den Bedrohungen
- Festlegen der Sicherheitspolitik und des Sicherheitsplans eines Unternehmens für Informationssysteme und Vervollständigung des Entwurfs und der Umsetzung des Notfallplans
- Erstellen eines Audit-Programms, das den Selbstbewertungsbedarf der Organisation in Bezug auf die Cybersicherheit abdeckt
- Entwickeln eines Programms zum Scannen und Überwachen von Schwachstellen und eines Plans zur Reaktion auf Cyber-Sicherheitsvorfälle
- Maximieren der sich bietenden Chancen und Eliminierung aller potenziellen Risiken durch Design
- Zusammenstellen der Schlüsselverwaltungssysteme
- Bewerten der Informationssicherheit eines Unternehmens
- Analysieren der Systeme für den Informationszugang
- Entwickeln von *Best Practices* für die sichere Entwicklung
- Darstellen der Risiken, die Unternehmen eingehen, wenn sie nicht über eine sichere Informationssicherheitsumgebung verfügen

Spezifische Kompetenzen

- Entwickeln eines Informationssicherheits-Managementsystems (ISMS)
- Identifizieren der Schlüsselelemente, aus denen ein ISMS besteht
- Anwenden der MAGERIT-Methodik, um das Modell weiterzuentwickeln und einen Schritt weiter zu gehen
- Entwickeln neuer Risikomanagement-Methoden auf der Grundlage des Konzepts des *agile Risk Management*
- Identifizieren, Analysieren, Bewerten und Behandeln der Risiken, mit denen die Fachleute konfrontiert sind, aus einer neuen Geschäftsperspektive auf der Grundlage eines *Risk-Driven* oder risikoorientierten Modells, das es nicht nur ermöglicht, in seinem eigenen Umfeld zu überleben, sondern auch seinen eigenen Wertbeitrag zu steigern
- Untersuchen des Prozesses der Entwicklung einer Sicherheitsstrategie bei der Bereitstellung von *Cloud*-Diensten für Unternehmen
- Bewerten der Unterschiede in den spezifischen Implementierungen der verschiedenen Public *Cloud*-Anbieter
- Bewerten der IoT-Konnektivitätsoptionen für ein Projekt, mit Schwerpunkt auf LPWAN-Technologien
- Einführen in die grundlegenden Spezifikationen der wichtigsten LPWAN-Technologien für das IoT

04

Kursleitung

Die enorme Komplexität der heutigen Cybersicherheit erfordert einen umfassenden und detaillierten Weiterbildungsprozess. Aus diesem Grund hat TECH die besten auf diesen Bereich spezialisierten Dozenten zusammengebracht. So wird die Fachkraft von einem Dozententeam begleitet und beaufsichtigt, das über die neuesten Fortschritte in diesem Bereich auf dem Laufenden ist, so dass sie in der Lage ist, die besten Techniken der Cybersicherheit in ihre tägliche Arbeit einzubeziehen und gleichzeitig die notwendigen Managementfähigkeiten in diesem Bereich zu erwerben.

Ihnen stehen echte Cybersicherheitsspezialisten zur Verfügung. Das ist die Gelegenheit, auf die Sie gewartet haben“

Internationaler Gastdirektor

Mit über 20 Jahren Erfahrung in der Gestaltung und Leitung globaler **Talentakquisitionsteams** ist Jennifer Dove eine Expertin für **Personalbeschaffung** und **Strategie im Technologiebereich**. Im Laufe ihrer Karriere hatte sie leitende Positionen in verschiedenen Technologieorganisationen von Fortune-50-Unternehmen inne, darunter NBC Universal und Comcast. Ihre Erfolgsbilanz hat es ihr ermöglicht, sich in wettbewerbsintensiven, wachstumsstarken Umgebungen auszuzeichnen.

Als **Vizepräsidentin für Talentakquise** bei **Mastercard** ist sie für die Überwachung der Strategie und Durchführung des Talent Onboarding verantwortlich und arbeitet mit Geschäftsführern und **Personalleitern** zusammen, um operative und strategische Einstellungsziele zu erreichen. Ihr Ziel ist es insbesondere, **vielfältige**, **integrative** und **leistungsstarke Teams** aufzubauen, die die Innovation und das Wachstum der Produkte und Dienstleistungen des Unternehmens vorantreiben. Darüber hinaus ist sie Expertin für den Einsatz von Instrumenten zur Gewinnung und Bindung der besten Mitarbeiter aus aller Welt. Zudem ist sie für die **Stärkung** der **Arbeitgebermarke** und des Wertversprechens von Mastercard durch Publikationen, Veranstaltungen und soziale Medien verantwortlich.

Jennifer Dove hat ihr Engagement für eine kontinuierliche berufliche Weiterentwicklung unter Beweis gestellt, indem sie sich aktiv an Netzwerken von Personalfachleuten beteiligt und zur Eingliederung zahlreicher Mitarbeiter in verschiedenen Unternehmen beigetragen hat. Nach ihrem Hochschulabschluss in **Organisationskommunikation** an der Universität von Miami hatte sie leitende Positionen im Recruiting bei Unternehmen in verschiedenen Bereichen inne.

Darüber hinaus wurde sie für ihre Fähigkeit anerkannt, organisatorische Umgestaltungen zu leiten, **Technologien** in **Einstellungsprozesse zu integrieren** und Führungsprogramme zu entwickeln, die Einrichtungen auf künftige Herausforderungen vorbereiten. Außerdem hat sie erfolgreich **Wellness**-Programme eingeführt, die die Zufriedenheit und Bindung der Mitarbeiter deutlich erhöht haben.

Fr. Dove, Jennifer

- Vizepräsidentin für Talentakquise bei Mastercard, New York, USA
- Direktorin für Talentakquise bei NBC Universal, New York, USA
- Leiterin der Personalbeschaffung bei Comcast
- Leiterin der Personalbeschaffung bei Rite Hire Advisory
- Geschäftsführende Vizepräsidentin, Verkaufsabteilung bei Ardor NY Real Estate
- Direktorin für Personalbeschaffung bei Valerie August & Associates
- Kundenbetreuerin bei BNC
- Kundenbetreuerin bei Vault
- Hochschulabschluss in Organisationskommunikation an der Universität von Miami

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

Internationaler Gastdirektor

Rick Gauthier ist eine Führungspersönlichkeit im Technologiebereich mit jahrzehntelanger Erfahrung in **führenden multinationalen Technologieunternehmen**. Er hat sich auf dem Gebiet der **Cloud**-Services und der Verbesserung von End-to-End-Prozessen profiliert. Er gilt als äußerst effektiver Teamleiter und Manager, der ein natürliches Talent dafür hat, ein hohes Maß an Engagement bei seinen Mitarbeitern sicherzustellen.

Er ist ein Naturtalent in Sachen Strategie und Innovation in der Geschäftsführung, entwickelt neue Ideen und untermauert seinen Erfolg mit hochwertigen Daten. Seine Erfahrung bei **Amazon** hat es ihm ermöglicht, die IT-Dienste des Unternehmens in den USA zu verwalten und zu integrieren. Bei **Microsoft** leitete er ein Team von 104 Mitarbeitern, das für die Bereitstellung der unternehmensweiten IT-Infrastruktur und die Unterstützung der Produktentwicklungsabteilungen im gesamten Unternehmen verantwortlich war.

Diese Erfahrung hat ihn zu einem herausragenden Manager mit bemerkenswerten Fähigkeiten zur Steigerung der Effizienz, Produktivität und allgemeinen Kundenzufriedenheit gemacht.

Hr. Gauthier, Rick

- Regionaler IT-Manager - Amazon, Seattle, Vereinigte Staaten
- Senior Programm-Manager bei Amazon
- Vizepräsident bei Wimmer Solutions
- Senior Manager für technische Produktivitätsdienste bei Microsoft
- Hochschulabschluss in Cybersicherheit von der Western Governors University
- Technisches Zertifikat in *Commercial Diving* von Divers Institute of Technology
- Hochschulabschluss in Umweltstudien vom The Evergreen State College

Nutzen Sie die Gelegenheit, sich über die neuesten Fortschritte auf diesem Gebiet zu informieren und diese in Ihrer täglichen Praxis anzuwenden“

Internationaler Gastdirektor

Romi Arman ist ein renommierter internationaler Experte mit mehr als zwei Jahrzehnten Erfahrung in den Bereichen **digitale Transformation**, **Marketing, Strategie** und **Beratung**. Im Laufe seiner langen Karriere hat er viele Risiken auf sich genommen und ist ein ständiger **Verfechter** von **Innovation** und **Wandel** im Geschäftsumfeld. Mit dieser Expertise hat er mit CEOs und Unternehmensorganisationen auf der ganzen Welt zusammengearbeitet und sie dazu gebracht, sich von traditionellen Geschäftsmodellen zu lösen. Auf diese Weise hat er Unternehmen wie Shell Energy geholfen, **echte Marktführer** zu werden, die sich auf ihre **Kunden** und die **digitale Welt** konzentrieren.

Die von Arman entwickelten Strategien haben eine latente Wirkung, denn sie haben es mehreren Unternehmen ermöglicht, die **Erfahrungen von Verbrauchern**, **Mitarbeitern** und **Aktionären gleichermaßen zu verbessern**. Der Erfolg dieses Experten ist durch greifbare Kennzahlen wie **CSAT**, **Mitarbeiterengagement** in den Institutionen, für die er tätig war, und das Wachstum des **Finanzindikators EBITDA** in jeder von ihnen messbar.

Außerdem hat er in seiner beruflichen Laufbahn **Hochleistungsteams aufgebaut und geleitet**, die sogar für ihr **Transformationspotenzial** ausgezeichnet wurden. Speziell bei Shell hat er sich stets bemüht, drei Herausforderungen zu meistern: die komplexen **Anforderungen** der Kunden an die **Dekarbonisierung** zu erfüllen, eine **„kosteneffiziente Dekarbonisierung" zu unterstützen** und eine fragmentierte **Daten-**, **Digital- und Technologielandschaft zu überarbeiten**. So haben seine Bemühungen gezeigt, dass es für einen nachhaltigen Erfolg unerlässlich ist, von den Bedürfnissen der Verbraucher auszugehen und die Grundlagen für die Transformation von Prozessen, Daten, Technologie und Kultur zu schaffen.

Andererseits zeichnet sich der Manager durch seine Beherrschung der **geschäftlichen Anwendungen** von **Künstlicher Intelligenz** aus, ein Fach, in dem er einen Aufbaustudiengang an der London Business School absolviert hat. Gleichzeitig hat er Erfahrungen im Bereich **IoT** und **Salesforce** gesammelt.

Hr. Arman, Romi

- Direktor für digitale Transformation (CDO) bei der Shell Energy Corporation, London, UK
- Globaler Leiter für eCommerce und Kundenservice bei der Shell Energy Corporation, London, UK
- Nationaler Key Account Manager (Automobilhersteller und Einzelhandel) bei Shell in Kuala Lumpur, Malaysia
- Senior Management Consultant (Finanzdienstleistungssektor) für Accenture mit Sitz in Singapur
- Hochschulabschluss an der Universität von Leeds
- Aufbaustudiengang in Geschäftsanwendungen der KI für leitende Angestellte an der London Business School
- Zertifizierung zum CCXP Customer Experience Professional
- Kurs in Digitale Transformation für Führungskräfte von IMD

Möchten Sie Ihr Wissen mit höchster pädagogischer Qualität aktualisieren? TECH bietet Ihnen die aktuellsten Inhalte auf dem akademischen Markt, die von authentischen Experten von internationalem Prestige entwickelt wurden"

Internationaler Gastdirektor

Manuel Arens ist ein **erfahrener Experte** für Datenmanagement und Leiter eines hochqualifizierten Teams. Arens ist **globaler Einkaufsleiter** in der Abteilung für technische Infrastruktur und Rechenzentren von Google, wo er den größten Teil seiner Karriere verbracht hat. Von Mountain View, Kalifornien, aus hat er Lösungen für die operativen Herausforderungen des Tech-Giganten erarbeitet, wie beispielsweise die **Integrität von Stammdaten,** die **Aktualisierung von Lieferantendaten** und die **Priorisierung** von Lieferanten. Er hat die Planung der Lieferkette von Rechenzentren und die Risikobewertung von Lieferanten geleitet und dabei Prozessverbesserungen und ein Workflow-Management geschaffen, die zu erheblichen Kosteneinsparungen geführt haben.

Mit mehr als einem Jahrzehnt Erfahrung in der Bereitstellung digitaler Lösungen und der Führung von Unternehmen in verschiedenen Branchen verfügt er über umfassende Erfahrung in allen Aspekten der Bereitstellung strategischer Lösungen, einschließlich **Marketing, Medienanalyse, Messung** und **Attribution**. Für seine Arbeit hat er mehrere Auszeichnungen erhalten, darunter den **BIM Leadership Preis**, den **Search Leadership Preis**, den **Preis für das Programm zur Leadgenerierung im Export** und den **Preis für das beste Vertriebsmodell von EMEA.**

Arens war auch als **Vertriebsleiter** in Dublin, Irland, tätig. In dieser Funktion baute er innerhalb von drei Jahren ein Team von 4 auf 14 Mitarbeiter auf und führte das Vertriebsteam so, dass es Ergebnisse erzielte und gut miteinander und mit funktionsübergreifenden Teams zusammenarbeitete. Außerdem war er als **Senior Industrieanalyst** in Hamburg tätig und erstellte Storylines für über 150 Kunden, wobei er interne und externe Tools zur Unterstützung der Analyse einsetzte. Er entwickelte und verfasste ausführliche Berichte, in denen er sein Fachwissen unter Beweis stellte, einschließlich des Verständnisses der **makroökonomischen und politischen/ regulatorischen Faktoren**, die die Einführung und Verbreitung von Technologien beeinflussen.

Er hat auch Teams bei Unternehmen wie **Eaton, Airbus und Siemens** geleitet, wo er wertvolle Erfahrungen im Kunden- und Lieferkettenmanagement sammeln konnte. Er zeichnet sich besonders dadurch aus, dass er die Erwartungen immer wieder übertrifft, indem er wertvolle Kundenbeziehungen aufbaut und **nahtlos mit Menschen auf allen Ebenen eines Unternehmens** zusammenarbeitet, einschließlich Stakeholdern, Management, Teammitgliedern und Kunden. Sein datengesteuerter Ansatz und seine Fähigkeit, innovative und skalierbare Lösungen für die Herausforderungen der Branche zu entwickeln, haben ihn zu einer führenden Persönlichkeit in seinem Bereich gemacht.

Hr. Arens, Manuel

- Globaler Einkaufsleiter bei Google, Mountain View, USA
- Senior B2B Analytics and Technology Manager bei Google, USA
- Vertriebsleiter bei Google, Irland
- Senior Industrial Analyst bei Google, Deutschland
- Kundenbetreuer bei Google, Irland
- Accounts Payable bei Eaton, UK
- Lieferkettenmanager bei Airbus, Deutschland

Setzen Sie auf TECH! Sie werden Zugang zu den besten didaktischen Materialien haben, die auf dem neuesten Stand der Technik und der Bildung sind und von international anerkannten Spezialisten auf diesem Gebiet umgesetzt werden“

Internationaler Gastdirektor

Andrea La Sala ist ein **erfahrener Marketingmanager**, dessen Projekte einen **bedeutenden Einfluss** auf die **Modewelt** hatten. Im Laufe seiner erfolgreichen Karriere hat er verschiedene Aufgaben in den Bereichen **Produkt**, **Merchandising** und **Kommunikation** übernommen. All dies in Verbindung mit renommierten Marken wie **Giorgio Armani**, **Dolce & Gabbana**, **Calvin Klein** und anderen.

Die Ergebnisse dieser **hochkarätigen internationalen Führungskraft** sind auf seine nachgewiesene Fähigkeit zurückzuführen, **Informationen in klaren Rahmen zu synthetisieren** und **konkrete**, auf **spezifische Geschäftsziele ausgerichtete Maßnahmen** durchzuführen. Darüber hinaus ist er für seine **Proaktivität** und seine **Anpassung an einen raschen Arbeitsrhythmus** bekannt. Außerdem verfügt er über ein **ausgeprägtes kommerzielles Bewusstsein**, eine **Marktvision** und eine **echte Leidenschaft** für die **Produkte**.

Als **Globaler Direktor für Marke und Merchandising** bei **Giorgio Armani** hat er eine Vielzahl von **Marketingstrategien** für **Bekleidung** und **Accessoires** überwacht. Seine Taktiken konzentrierten sich auch auf den **Einzelhandel** und die **Bedürfnisse** und das **Verhalten der Verbraucher**. In dieser Funktion war La Sala auch für die Gestaltung des Produktmarketings in verschiedenen Märkten verantwortlich und fungierte als **Teamleiter** in den **Abteilungen Design**, **Kommunikation** und **Verkauf**.

Andererseits hat er in Unternehmen wie **Calvin Klein** oder der **Gruppe Coin** Projekte zur Förderung der **Struktur**, **Entwicklung** und **Vermarktung verschiedener Kollektionen** durchgeführt. Er war auch für die Erstellung von **effektiven Kalendern** für **Einkaufs- und Verkaufskampagnen** verantwortlich. Zudem hat er die **Bedingungen**, **Kosten**, **Prozesse** und **Lieferfristen** der verschiedenen Operationen verwaltet.

Diese Erfahrungen haben Andrea La Sala zu einem der besten und qualifiziertesten **Unternehmensführer** in der **Mode-** und **Luxusbranche** gemacht. Er verfügt über eine hohe Managementkapazität, mit der es ihm gelungen ist, die **positive Positionierung verschiedener Marken** und die Neudefinition ihrer Key Performance Indicators (KPI) effektiv umzusetzen.

Hr. La Sala, Andrea

- Globaler Direktor für Marke und Merchandising bei Giorgio Armani, Mailand, Italien
- Direktor für Merchandising bei Calvin Klein
- Markenleiter bei der Gruppe Coin
- Brand Manager bei Dolce & Gabbana
- Brand Manager bei Sergio Tacchini S.p.A.
- Marktanalyst bei Fastweb
- Hochschulabschluss in Betriebs- und Volkswirtschaft an der Università degli Studi del Piemonte Orientale

Bei TECH erwarten Sie die qualifiziertesten und erfahrensten internationalen Fachleute, die Ihnen einen erstklassigen Unterricht bieten, der auf dem neuesten Stand der Wissenschaft ist und auf den neuesten Erkenntnissen beruht. Worauf warten Sie, um sich einzuschreiben?"

Internationaler Gastdirektor

Mick Gram ist international ein Synonym für Innovation und Exzellenz im Bereich der **Business Intelligence**. Seine erfolgreiche Karriere ist mit Führungspositionen in multinationalen Unternehmen wie **Walmart** und **Red Bull** verbunden. Er ist auch bekannt für seine Vision, **aufkommende Technologien zu identifizieren**, die langfristig einen nachhaltigen Einfluss auf das Unternehmensumfeld haben.

Andererseits gilt er als **Pionier** bei der **Verwendung von Datenvisualisierungstechniken**, die komplexe Datensätze vereinfachen, sie zugänglich machen und die Entscheidungsfindung erleichtern. Diese Fähigkeit wurde zur Säule seines beruflichen Profils und machte ihn zu einem begehrten Aktivposten für viele Organisationen, die auf das **Sammeln von Informationen und darauf basierende konkrete Maßnahmen** setzen.

Eines seiner herausragendsten Projekte der letzten Jahre war die **Plattform Walmart Data Cafe**, die größte ihrer Art weltweit, die in der Cloud für ***Big Data-Analysen*** verankert ist. Darüber hinaus war er als **Direktor** für **Business Intelligence** bei **Red Bull** tätig, wo er Bereiche wie **Verkauf, Vertrieb, Marketing und Lieferkettenoperationen** abdeckte. Sein Team wurde kürzlich für seine ständige Innovation bei der Nutzung der neuen API von Walmart Luminate für Shopper- und Channel-Insights ausgezeichnet.

Was die Ausbildung betrifft, so verfügt die Führungskraft über mehrere Master- und Aufbaustudiengänge an renommierten Zentren wie der **Universität von Berkeley** in den Vereinigten Staaten und der **Universität von Kopenhagen** in Dänemark. Durch diese ständige Weiterbildung hat der Experte modernste Kompetenzen erlangt. So gilt er als **geborener Anführer** der **neuen globalen Wirtschaft**, in deren Mittelpunkt das Streben nach Daten und ihren unendlichen Möglichkeiten steht.

Hr. Gram, Mick

- Direktor für *Business Intelligence* und Analytik bei Red Bull, Los Angeles, USA
- Architekt für *Business Intelligence*-Lösungen für Walmart Data Café
- Unabhängiger Berater für *Business Intelligence* und *Data Science*
- Direktor für *Business Intelligence* bei Capgemini
- Chefanalyst bei Nordea
- Senior Berater für *Business Intelligence* bei SAS
- Executive Education in KI und Machine Learning am UC Berkeley College of Engineering
- Executive MBA in E-Commerce an der Universität von Kopenhagen
- Hochschulabschluss und Masterstudiengang in Mathematik und Statistik an der Universität von Kopenhagen

Studieren Sie an der laut Forbes besten Online-Universität der Welt! In diesem MBA haben Sie Zugang zu einer umfangreichen Bibliothek mit Multimedia-Ressourcen, die von international renommierten Professoren entwickelt wurden"

Internationaler Gastdirektor

Scott Stevenson ist ein angesehener Experte für **digitales Marketing**, der seit über 19 Jahren für eines der mächtigsten Unternehmen der Unterhaltungsindustrie, **Warner Bros. Discovery**, tätig ist. In dieser Funktion war er maßgeblich an der **Überwachung der Logistik** und der **kreativen Arbeitsabläufe** auf mehreren digitalen Plattformen beteiligt, darunter soziale Medien, Suche, Display und lineare Medien.

Seine Führungsqualitäten haben entscheidend dazu beigetragen, die **Produktionsstrategien** für **bezahlte Medien** voranzutreiben, was zu einer deutlichen **Verbesserung** der **Konversionsraten** seines Unternehmens führte. Gleichzeitig hat er während seiner früheren Tätigkeit im Management desselben multinationalen Unternehmens andere Aufgaben übernommen, wie z. B. die des Marketingdirektors und des Verkehrsleiters.

Stevenson war auch am weltweiten Vertrieb von Videospielen und **digitalen Eigentumskampagnen** beteiligt. Außerdem war er für die Einführung operativer Strategien im Zusammenhang mit der Fortbildung, Fertigstellung und Lieferung von Ton- und Bildinhalten für ***Fernsehwerbung und Trailer*** verantwortlich.

Darüber hinaus hat er einen Hochschulabschluss in Telekommunikation von der Universität von Florida und einen Masterstudiengang in Kreativem Schreiben von der Universität von Kalifornien absolviert, was seine Fähigkeiten in den Bereichen **Kommunikation** und **Storytelling** unter Beweis stellt. Außerdem hat er an der Fakultät für Berufliche Entwicklung der Universität Harvard an bahnbrechenden Programmen über den Einsatz von **Künstlicher Intelligenz** in der **Wirtschaft** teilgenommen. Sein berufliches Profil ist somit eines der wichtigsten im Bereich **Marketing** und **digitale Medien**.

Hr. Stevenson, Scott

- Direktor für Marketingdienste bei Warner Bros. Discovery, Burbank, USA
- Verkehrsleiter bei Warner Bros. Entertainment
- Masterstudiengang in Kreatives Schreiben von der Universität von Kalifornien
- Hochschulabschluss in Telekommunikation von der Universität von Florida

Erreichen Sie Ihre akademischen und beruflichen Ziele mit den am besten qualifizierten Experten der Welt! Die Dozenten dieses MBA werden Sie durch den gesamten Lernprozess begleiten"

Internationaler Gastdirektor

Dr. Eric Nyquist ist ein führender **internationaler Sportexperte**, der auf eine beeindruckende Karriere zurückblicken kann. Er ist bekannt für seine **strategischen Führungsqualitäten** und seine Fähigkeit, Veränderungen und **Innovationen** in **hochrangigen Sportorganisationen** voranzutreiben.

Er hatte unter anderem leitende Positionen als **Direktor für Kommunikation und Einfluss** bei **NASCAR** in **Florida, USA**, inne. Mit seiner langjährigen Erfahrung bei NASCAR hat Dr. Nyquist auch eine Reihe von Führungspositionen innegehabt, darunter **Senior-Vizepräsident für strategische Entwicklung** und **Leitender Direktor für Geschäftsangelegenheiten**, wobei er mehr als ein Dutzend Disziplinen von der **strategischen Entwicklung** bis zum **Unterhaltungsmarketing** leitete.

Nyquist hat auch Chicagos Top-**Sportfranchises** einen bedeutenden Stempel aufgedrückt. Als **Geschäftsführender Vizepräsident** der **Chicago Bulls** und der **Chicago White Sox** hat er seine Fähigkeit unter Beweis gestellt, **geschäftliche** und **strategische Erfolge** in der Welt des **Profisports** zu erzielen.

Schließlich begann er seine Karriere im **Sport**, als er in **New York** als **leitender strategischer Analyst** für **Roger Goodell** in der **National Football League (NFL)** arbeitete und davor als **Rechtspraktikant** beim **Amerikanischen Fußballverband**.

Hr. Nyquist, Eric

- Direktor für Kommunikation und Einfluss, NASCAR, Florida, USA
- Senior-Vizepräsident für strategische Entwicklung, NASCAR, USA
- Vizepräsident für strategische Planung bei NASCAR
- Leitender Direktor für Geschäftsangelegenheiten bei NASCAR
- Geschäftsführender Vizepräsident, Chicago White Sox
- Geschäftsführender Vizepräsident, Chicago Bulls
- Manager für Geschäftsplanung bei der National Football League (NFL)
- Praktikant für Geschäftsangelegenheiten/Recht beim amerikanischen Fußballverband
- Promotion in Rechtswissenschaften an der Universität von Chicago
- Masterstudiengang in Betriebswirtschaft (MBA) an der Booth School of Business der Universität von Chicago
- Hochschulabschluss in Internationaler Wirtschaft am Carleton College

Dank dieses 100%igen Online-Universitätsabschlusses können Sie Ihr Studium mit Hilfe der führenden internationalen Experten auf dem Gebiet, das Sie interessiert, mit Ihren täglichen Verpflichtungen verbinden. Schreiben Sie sich jetzt ein!"

Leitung

Hr. Olalla Bonal, Martín

- Senior Manager der Blockchain-Praxis bei EY
- Technischer Spezialist für Blockchain-Kunden bei IBM
- Direktor für Architektur bei Blocknitive
- Teamkoordinator für nicht relationale verteilte Datenbanken bei wedoIT, Tochtergesellschaft von IBM
- Infrastruktur-Architekt bei Bankia
- Leiter der Layout-Abteilung bei T-Systems
- Abteilungskoordinator für Bing Data España SL

Professoren

Dr. Nogales Ávila, Javier

- Enterprise Cloud and sourcing senior consultant, Quint
- Cloud and Technology Consultant, Indra
- Associate Technology Consultant, Accenture
- Hochschulabschluss an der Universität von Jaén und der University of Technology and Economics of Budapest (BME)
- Hochschulabschluss in Ingenieurwesen für industrielle Organisation

Hr. Rodrigo Estébanez, Juan Manuel

- Mitgründer von Ismet Tech
- Manager für Informationssicherheit bei der Ecix-Gruppe
- *Operational Security Officer* bei Atos IT Solutions and Services A/S
- Cybersicherheitsmanagement im Rahmen von Universitätsstudien
- Hochschulabschluss in Ingenieurwesen an der Universität von Valladolid
- Masterstudiengang in Integrierten Managementsystemen an der Universität CEU San Pablo

Professoren

Dr. Gómez Rodríguez, Antonio

- Leitender Ingenieur für Cloud-Lösungen bei Oracle
- Mitorganisator des Malaga Developer Meetup
- Beratungsspezialist für die Sopra Group und Everis
- Teamleiter bei System Dynamics
- Software-Entwickler bei SGO Software
- Masterstudiengang in E-Business an der La Salle Wirtschaftsschule
- Aufbaustudiengang in Informationstechnologien und -systemen vom Katalanischen Institut für Technologie
- Hochschulabschluss in Telekommunikationstechnik an der Polytechnischen Universität von Katalonien

Dr. del Valle Arias, Jorge

- Smart City Solutions & Software Business Development Manager Spanien, Itron, Inc
- IoT-Berater
- Interim IoT Business Director, TCOMET
- Leiter der Geschäftseinheit IoT, Industrie 4.0, Diode Spanien
- Bereichsleiter für IoT und Telekommunikation, Aicox Soluciones
- Technischer Leiter (CTO) und Leiter der Geschäftsentwicklung, TELYC-Beratung
- Gründer und CEO von Sensor Intelligence
- Leiter der Abteilung Betrieb und Projekte, Codio
- Betriebsleitung bei Codium Networks
- Leitender Hardware- und Firmware-Designer, AITEMIN
- Regionaler Leiter der HF-Planung und -Optimierung - LMDS 3,5-GHz-Netz, Clearwire
- Ingenieur für Telekommunikation von der Polytechnischen Universität von Madrid
- Executive MBA von der International Graduate School von La Salle in Madrid
- Masterstudiengang in Erneuerbare Energien, CEPYME

Hr. Gonzalo Alonso, Félix

- Geschäftsleitung und Gründer von Smart REM Solutions
- Gründungspartner und Leitung von Risk Engineering und Innovation, Dynargy
- Geschäftsführender Direktor und Gründungspartner, Risknova (Spezialisiertes Sachverständigenbüro für Technologie)
- Hochschulabschluss in Ingenieurwesen für industrielle Organisation an der Päpstlichen Universität Comillas ICAI
- Hochschulabschluss in Industrietechnik, Spezialisierung auf Industrieelektronik, Päpstliche Universität Comillas ICAI
- Masterstudiengang in Versicherungsmanagement von ICEA (Institut für die Zusammenarbeit von Versicherungsgesellschaften)

Dr. Entrenas, Alejandro

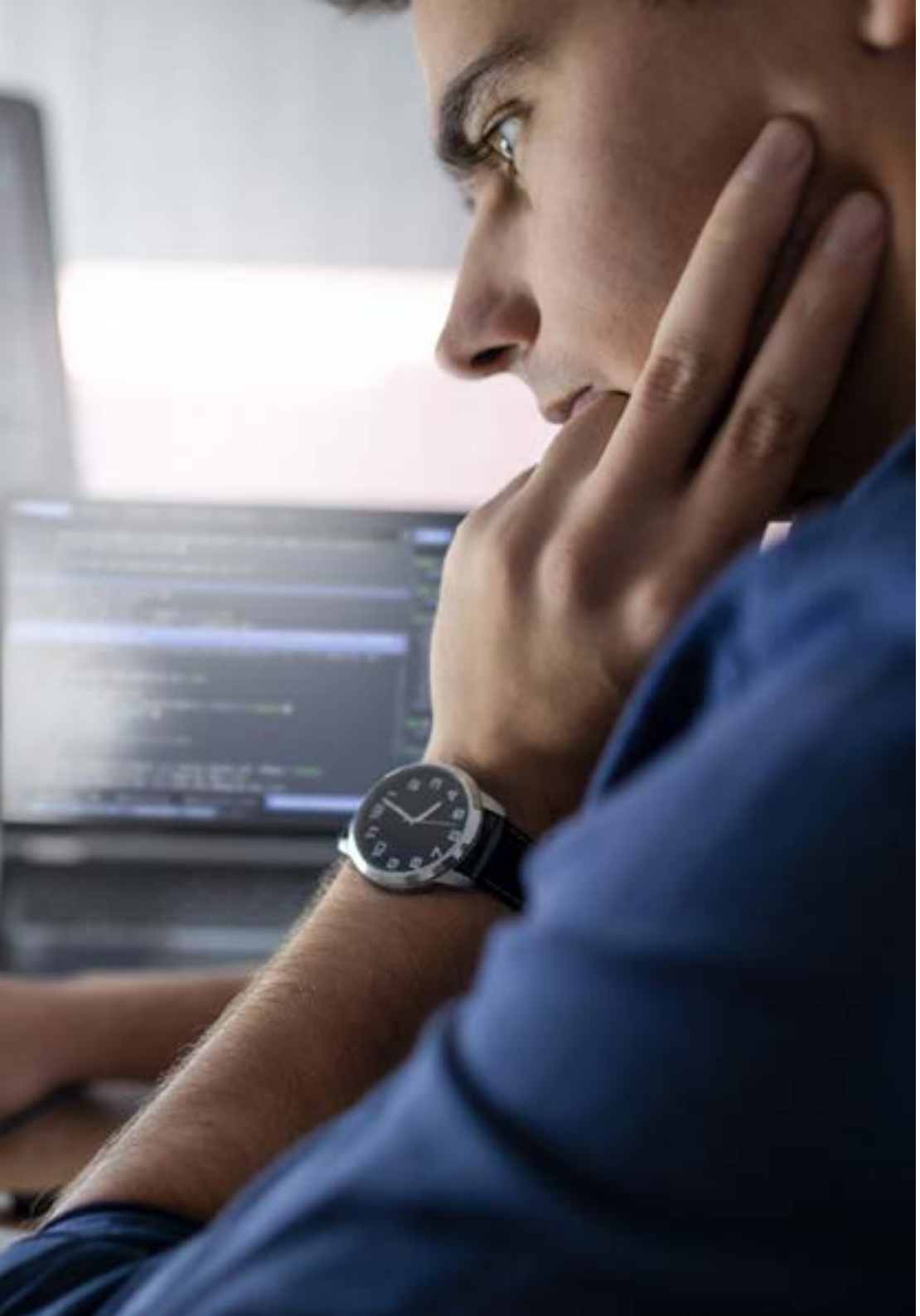
- Projektleiter für Cybersicherheit, Entelgy Innotec Security
- Berater für Cybersicherheit, Entelgy
- Analyst für Informationssicherheit, Innovery Spanien
- Analyst für Informationssicherheit, Atos
- Hochschulabschluss in Technischem Ingenieurwesen im Bereich Computersysteme an der Universität von Cordoba
- Masterstudiengang in Informationssicherheitsmanagement von der Polytechnischen Universität von Madrid
- ITIL v4 Foundation-Zertifikat für IT-Service-Management, ITIL Certified

Hr. Ortega Esteban, Octavio

- Spezialist für Marketing und Webentwicklung
- Programmierer für Computeranwendungen und Webentwicklung
- *Chief Operating Officer* bei Smallsquid SL
- Verwalter für E-Commerce bei Ortega y Serrano
- Dozent für Zertifizierungskurse in Computer und Kommunikation
- Dozent für Computersicherheitskurse
- Hochschulabschluss in Psychologie an der Offenen Universität von Katalonien (UOC)
- Höhere Berufsausbildung in *Softwareanalyse*, -design und -lösungen
- Höhere Berufsausbildung in fortgeschrittener Programmierung

Hr. Embid Ruiz, Mario

- Rechtsanwalt mit Spezialisierung auf IKT und Datenschutz bei Martínez-Echevarría Abogados
- Juristischer Leiter von Branddocs SL
- Risikoanalyst im KMU-Segment bei BBVA
- Dozent in universitären Aufbaustudiengängen im Bereich Recht
- Hochschulabschluss in Jura an der Universität Rey Juan Carlos
- Hochschulabschluss in Betriebswirtschaft und Management an der Universität Rey Juan Carlos in Madrid
- Masterstudiengang in Recht der neuen Technologien, Internet und audiovisuelle Medien am Studienzentrum der Universität Villanueva



Dr. Gozalo Fernández, Juan Luis

- Blockchain-basierter Produktmanager für Open Canarias
- Blockchain DevOps Manager bei Alastria
- Direktor für Service Level Technologie bei Santander Spanien
- Manager für die Entwicklung der mobilen Anwendung Tinkerlink bei Cronos Telecom
- Technischer Direktor für IT-Service-Management bei Barclays Bank Spanien
- Hochschulabschluss in Computertechnik an der UNED
- Spezialisierung auf *Deep Learning* bei DeepLearning.ai

Dr. Jurado Jabonero, Lorena

- Leitung der Informationssicherheit (CISO) bei Grupo Pascual
- Cybersecurity Manager bei KPMG, Spanien
- Beraterin für IT-Prozesse und Infrastrukturprojektkontrolle und -management bei Bankia
- Ingenieurin für Verwertungswerkzeuge bei Dalkia
- Entwicklung bei der Banco Popular Gruppe
- Anwendungsentwicklerin von der Polytechnischen Universität von Madrid
- Hochschulabschluss in Computertechnik an der Universität Alfonso X El Sabio
- Technische Ingenieurin in Computer Management von der Polytechnischen Universität von Madrid
- Certified Data Privacy Solutions Engineer (CDPSE) von ISACA

05

Struktur und Inhalt

Dieser MBA in Fortgeschrittenes Cybersecurity Management (CISO) ist in 10 spezialisierte Module gegliedert, die es den Fachleuten ermöglichen, Aspekte wie die digitale Identifizierung, Zugangskontrollsysteme, die Architektur der Informationssicherheit, die Struktur des Sicherheitsbereichs, Managementsysteme für die Informationssicherheit in der Kommunikation und im Softwarebetrieb oder die Entwicklung des mit der Sicherheit verbundenen *Business Continuity Plans* zu vertiefen. Dadurch erhält der Informatiker ein umfassendes Verständnis aller relevanten Themen der aktuellen Cybersicherheit.

Sie werden keinen vollständigeren und innovativeren Inhalt als diesen finden, um sich auf fortgeschrittenes Cybersecurity Management zu spezialisieren"

Modul 1. Sicherheit in Design und Entwicklung von Systemen

1.1. Informationssysteme
- 1.1.1. Domains eines Informationssystems
- 1.1.2. Komponenten eines Informationssystems
- 1.1.3. Aktivitäten eines Informationssystems
- 1.1.4. Lebenszyklus eines Informationssystems
- 1.1.5. Ressourcen eines Informationssystems

1.2. Informationssysteme. Typologie
- 1.2.1. Typen von Informationssystemen
  - 1.2.1.1. Unternehmerisch
  - 1.2.1.2. Strategisch
  - 1.2.1.3. Je nach Anwendungsbereich
  - 1.2.1.4. Spezifisch
- 1.2.2. Informationssysteme. Beispiele aus der Praxis
- 1.2.3. Entwicklung von Informationssystemen: Etappen
- 1.2.4. Methoden von Informationssystemen

1.3. Sicherheit von Informationssystemen. Rechtliche Implikationen
- 1.3.1. Zugang zu Daten
- 1.3.2. Sicherheitsbedrohungen: Schwachstellen
- 1.3.3. Rechtliche Implikationen: Straftaten
- 1.3.4. Verfahren zur Wartung von Informationssystemen

1.4. Sicherheit von Informationssystemen. Sicherheitsprotokolle
- 1.4.1. Sicherheit von Informationssystemen
  - 1.4.1.1. Integrität
  - 1.4.1.2. Vertraulichkeit
  - 1.4.1.3. Verfügbarkeit
  - 1.4.1.4. Authentifizierung
- 1.4.2. Sicherheitsdienste
- 1.4.3. Protokolle zur Informationssicherheit. Typologie
- 1.4.4. Empfindlichkeit von Informationssystemen

1.5. Sicherheit von Informationssystemen. Maßnahmen und Systeme zur Zugangskontrolle
- 1.5.1. Sicherheitsmaßnahmen
- 1.5.2. Art der Sicherheitsmaßnahmen
  - 1.5.2.1. Prävention
  - 1.5.2.2. Erkennung
  - 1.5.2.3. Korrektheit
- 1.5.3. Kontrollsysteme für den Zugang. Typologie
- 1.5.4. Kryptographie

1.6. Netzwerk- und Internetsicherheit
- 1.6.1. Firewalls
- 1.6.2. Digitale Identifizierung
- 1.6.3. Viren und Würmer
- 1.6.4. *Hacking*
- 1.6.5. Beispiele und reale Fälle

1.7. Computerkriminalität
- 1.7.1. Computerkriminalität
- 1.7.2. Computerkriminalität. Typologie
- 1.7.3. Computerkriminalität. Angriff. Typologien
- 1.7.4. Der Fall der virtuellen Realität
- 1.7.5. Profile von Tätern und Opfern. Typisierung von Verbrechen
- 1.7.6. Computerkriminalität. Beispiele und reale Fälle

1.8. Sicherheitsplan für ein Informationssystem
- 1.8.1. Sicherheitsplan. Ziele
- 1.8.2. Sicherheitsplan. Planung
- 1.8.3. Risikoplan. Analyse
- 1.8.4. Sicherheitspolitik. Implementierung in der Organisation
- 1.8.5. Sicherheitsplan. Implementierung in der Organisation
- 1.8.6. Sicherheitsverfahren. Typen
- 1.8.7. Sicherheitsplan. Beispiele

1.9. Plan für unvorhergesehene Ereignisse
- 1.9.1. Plan für unvorhergesehene Ereignisse. Funktionen
- 1.9.2. Notfallplan: Elemente und Ziele
- 1.9.3. Plan für unvorhergesehene Ereignisse in der Organisation. Implementierung
- 1.9.4. Plan für unvorhergesehene Ereignisse. Beispiele

1.10. Verwaltung der Sicherheit von Informationssystemen
- 1.10.1. Gesetzliche Bestimmungen
- 1.10.2. Normen
- 1.10.3. Zertifizierungen
- 1.10.4. Technologien

Modul 2. Architekturen und Modelle für die Informationssicherheit

2.1. Architektur der Informationssicherheit
- 2.1.1. ISMS / ISDP
- 2.1.2. Strategische Ausrichtung
- 2.1.3. Risikomanagement
- 2.1.4. Leistungsmessung

2.2. Modelle der Informationssicherheit
- 2.2.1. Richtlinienbasierte Sicherheitsmodelle
- 2.2.2. Basierend auf Schutz-Tools
- 2.2.3. Teambasiert

2.3. Sicherheitsmodell. Wichtige Komponenten
- 2.3.1. Identifizierung von Risiken
- 2.3.2. Definition von Kontrollen
- 2.3.3. Kontinuierliche Bewertung des Risikoniveaus
- 2.3.4. Sensibilisierungsplan für Mitarbeiter, Lieferanten, Partner usw

2.4. Prozess der Risikoverwaltung
- 2.4.1. Identifizierung von Vermögenswerten
- 2.4.2. Identifizierung von Bedrohungen
- 2.4.3. Risikobewertung
- 2.4.4. Priorisierung der Kontrollen
- 2.4.5. Neubeurteilung und Restrisiko

2.5. Geschäftsprozesse und Informationssicherheit
- 2.5.1. Geschäftsprozesse
- 2.5.2. Risikobewertung auf der Grundlage geschäftlicher Parameter
- 2.5.3. Analyse der Auswirkungen auf das Geschäft
- 2.5.4. Geschäftsbetrieb und Informationssicherheit

2.6. Prozess zur kontinuierlichen Verbesserung
- 2.6.1. Der Deming-Zyklus
  - 2.6.1.1. Planung
  - 2.6.1.2. Machen
  - 2.6.1.3. Prüfen
  - 2.6.1.4. Agieren

2.7. Sicherheitsarchitekturen
- 2.7.1. Auswahl und Homogenisierung von Technologien
- 2.7.2. Identitätsmanagement. Authentifizierung
- 2.7.3. Zugriffsverwaltung. Autorisierung
- 2.7.4. Sicherheit der Netzwerkinfrastruktur
- 2.7.5. Verschlüsselungstechnologien und -lösungen
- 2.7.6. Sicherheit der Endgeräte (EDR)

2.8. Der rechtliche Rahmen
- 2.8.1. Regulatorischer Rahmen
- 2.8.2. Zertifizierungen
- 2.8.3. Gesetzgebung

2.9. Der ISO 27001-Standard
- 2.9.1. Implementierung
- 2.9.2. Zertifizierung
- 2.9.3. Audits und Penetrationstests
- 2.9.4. Laufendes Risikomanagement
- 2.9.5. Klassifizierung der Informationen

2.10. Gesetzgebung zum Datenschutz. RGPD (GDPR)
- 2.10.1. Anwendungsbereich der Allgemeinen Datenschutzverordnung (GDPR)
- 2.10.2. Persönliche Daten
- 2.10.3. Rollen bei der Verarbeitung von personenbezogenen Daten
- 2.10.4. ARCO-Rechte
- 2.10.5. Der DSB. Funktionen

Modul 3. IT-Sicherheitsmanagement

3.1. Sicherheitsmanagement
- 3.1.1. Sicherheitsmaßnahmen
- 3.1.2. Rechtliche und regulatorische Aspekte
- 3.1.3. Geschäftliche Freigabe
- 3.1.4. Risikomanagement
- 3.1.5. Identitäts- und Zugriffsmanagement

3.2. Struktur des Sicherheitsbereichs. Das Büro des CISO
- 3.2.1. Organisatorische Struktur. Position des CISO in der Struktur
- 3.2.2. Verteidigungslinien
- 3.2.3. Organigramm des Büros des CISO
- 3.2.4. Haushaltsführung

3.3. Sicherheitsmanagement
- 3.3.1. Sicherheitsausschuss
- 3.3.2. Ausschuss für Risikoüberwachung
- 3.3.3. Prüfungsausschuss
- 3.3.4. Krisenausschuss

3.4. *Security Governance*. Funktionen
- 3.4.1. Politiken und Standards
- 3.4.2. Masterplan für Sicherheit
- 3.4.3. *Dashboards*
- 3.4.4. Sensibilisierung und Schulung
- 3.4.5. Sicherheit der Lieferkette

3.5. Sicherheitsmaßnahmen
- 3.5.1. Identitäts- und Zugriffsmanagement
- 3.5.2. Konfiguration von Netzwerksicherheitsregeln. *Firewalls*
- 3.5.3. Verwaltung der IDS/IPS-Plattform
- 3.5.4. Scannen auf Schwachstellen

3.6. Cybersecurity-Rahmenwerk. NIST CSF
- 3.6.1. NIST-Methodik
  - 3.6.1.1. Identifizieren
  - 3.6.1.2. Schützen
  - 3.6.1.3. Erkennen
  - 3.6.1.4. Reagieren
  - 3.6.1.5. Zurückgewinnen

3.7. Sicherheitsoperationszentrum (SOC). Funktionen
- 3.7.1. Schutz. *Red Team, Pentesting, Threat Intelligence*
- 3.7.2. Erkennung. SIEM, *User Behavior Analytics, Fraud Prevention*
- 3.7.3. Antwort

3.8. Sicherheitsaudits
- 3.8.1. Penetrationstests
- 3.8.2. Übungen des *Red Team*
- 3.8.3. Quellcode-Prüfungen. Sichere Entwicklung
- 3.8.4. Komponentensicherheit (*Software Supply Chain*)
- 3.8.5. Forensische Analyse

3.9. Reaktion auf Vorfälle
- 3.9.1. Vorbereitung
- 3.9.2. Erkennung, Analyse und Berichterstattung
- 3.9.3. Eindämmung, Ausrottung und Wiederherstellung
- 3.9.4. Aktivitäten nach dem Vorfall
  - 3.9.4.1. Aufbewahrung von Beweisen
  - 3.9.4.2. Forensische Analyse
  - 3.9.4.3. Lücken-Management
- 3.9.5. Offizielle Leitfäden für das Management von Cybervorfällen

3.10. Management von Schwachstellen
- 3.10.1. Scannen auf Schwachstellen
- 3.10.2. Bewertung der Anfälligkeit
- 3.10.3. Verstärkung des Systems
- 3.10.4. *Zero-Day*-Sicherheitslücken. *Zero-Day*

Modul 4. Risikoanalyse und IT-Sicherheitsumgebung

4.1. Analyse des Umfelds
- 4.1.1. Analyse der wirtschaftlichen Lage
  - 4.1.1.1. VUCA-Umgebungen
    - 4.1.1.1.1. Volatil
    - 4.1.1.1.2. Ungewiss
    - 4.1.1.1.3. Komplex
    - 4.1.1.1.4. Mehrdeutig
  - 4.1.1.2. BANI-Umgebungen
    - 4.1.1.2.1. Spröde
    - 4.1.1.2.2. Ängstlich
    - 4.1.1.2.3. Nicht-linear
    - 4.1.1.2.4. Unverständlich
- 4.1.2. Analyse des allgemeinen Umfelds. PESTEL
  - 4.1.2.1. Politisch
  - 4.1.2.2. Wirtschaft
  - 4.1.2.3. Sozial
  - 4.1.2.4. Technologisch
  - 4.1.2.5. Ökologisch/Umweltbezogen
  - 4.1.2.6. Legal
- 4.1.3. Analyse der internen Situation. SWOT
  - 4.1.3.1. Ziele
  - 4.1.3.2. Bedrohungen
  - 4.1.3.3. Gelegenheiten
  - 4.1.3.4. Stärken

4.2. Risiko und Ungewissheit
- 4.2.1. Risiko
- 4.2.2. Risikomanagement
- 4.2.3. Standards für das Risikomanagement

4.3. ISO 31.000:2018 Richtlinien zum Risikomanagement
- 4.3.1. Objekt
- 4.3.2. Grundsätze
- 4.3.3. Referenzrahmen
- 4.3.4. Prozess

4.4. Methodik für die Analyse und das Management von Risiken in Informationssystemen (MAGERIT)
- 4.4.1. MAGERIT Methodik
  - 4.4.1.1. Ziele
  - 4.4.1.2. Methode
  - 4.4.1.3. Elemente
  - 4.4.1.4. Techniken
  - 4.4.1.5. Verfügbare Tools (PILAR)

4.5. Übertragung von Cyber-Risiken
- 4.5.1. Risikotransfer
- 4.5.2. Cyberrisiken. Typologie
- 4.5.3. Versicherung gegen Cyberrisiken

4.6. Agile Methoden für das Risikomanagement
- 4.6.1. Agile Methoden
- 4.6.2. Scrum für das Risikomanagement
- 4.6.3. *Agile Risk Management*

4.7. Technologien für das Risikomanagement
- 4.7.1. Künstliche Intelligenz für das Risikomanagement
- 4.7.2. *Blockchain* und Kryptographie. Methoden zur Werterhaltung
- 4.7.3. Quantencomputing. Potenzial oder Bedrohung

4.8. IT-Risiko-Mapping auf der Grundlage agiler Methoden
- 4.8.1. Darstellung von Wahrscheinlichkeiten und Auswirkungen in agilen Umgebungen
- 4.8.2. Risiko als Bedrohung für den Wert
- 4.8.3. Neuentwicklung von agilem Projektmanagement und agilen Prozessen auf der Grundlage von KRIs

4.9. *Risk Driven* im Risikomanagement
- 4.9.1. *Risk Driven*
- 4.9.2. *Risk Driven* im Risikomanagement
- 4.9.3. Entwicklung eines risikoorientierten Geschäftsführungsmodells

4.10. Innovation und digitale Transformation im IT-Risikomanagement
- 4.10.1. Agiles Risikomanagement als Quelle für geschäftliche Innovation
- 4.10.2. Umwandlung von Daten in entscheidungsrelevante Informationen
- 4.10.3. Ganzheitliche Betrachtung des Unternehmens durch Risiko

Modul 5. Kryptographie in der IT

5.1. Kryptographie
- 5.1.1. Kryptographie
- 5.1.2. Mathematische Grundlagen

5.2. Kryptologie
- 5.2.1. Kryptologie
- 5.2.2. Kryptoanalyse
- 5.2.3. Steganographie und Stegoanalyse

5.3. Kryptographische Protokolle
- 5.3.1. Grundlegende Blöcke
- 5.3.2. Grundlegende Protokolle
- 5.3.3. Zwischengeschaltete Protokolle
- 5.3.4. Erweiterte Protokolle
- 5.3.5. Exoterische Protokolle

5.4. Kryptographische Techniken
- 5.4.1. Länge des Schlüssels
- 5.4.2. Handhabung der Tasten
- 5.4.3. Arten von Algorithmen
- 5.4.4. Zusammenfassende Funktionen. *Hash*
- 5.4.5. Pseudo-Zufallszahlengeneratoren
- 5.4.6. Verwendung von Algorithmen

5.5. Symmetrische Kryptographie
- 5.5.1. Blockchiffren
- 5.5.2. DES (*Data Encryption Standard*)
- 5.5.3. RC4 Algorithmus
- 5.5.4. AES (*Advanced Encryption Standard*)
- 5.5.5. Kombination von Blockchiffren
- 5.5.6. Ableitung des Schlüssels

5.6. Asymmetrische Kryptographie
- 5.6.1. Diffie-Hellman
- 5.6.2. DSA (*Digital Signature Algorithm*)
- 5.6.3. RSA (Rivest, Shamir und Adleman)
- 5.6.4. Elliptische Kurve
- 5.6.5. Asymmetrische Kryptographie. Typologie

5.7. Digitale Zertifikate
- 5.7.1. Digitale Unterschrift
- 5.7.2. X509-Zertifikate
- 5.7.3. Infrastruktur für öffentliche Schlüssel (PKI)

5.8. Implementierungen
- 5.8.1. Kerberos
- 5.8.2. IBM CCA
- 5.8.3. *Pretty Good Privacy* (PGP)
- 5.8.4. ISO *Authentication Framework*
- 5.8.5. SSL und TLS
- 5.8.6. Chipkarten als Zahlungsmittel (EMV)
- 5.8.7. Protokolle für Mobiltelefonie
- 5.8.8. *Blockchain*

5.9. Steganographie
- 5.9.1. Steganographie
- 5.9.2. Stegano-Analyse
- 5.9.3. Anwendungen und Einsatzmöglichkeiten

5.10. Quantenkryptographie
- 5.10.1. Quanten-Algorithmen
- 5.10.2. Schutz von Algorithmen vor Quantenberechnungen
- 5.10.3. Quantum Key Distribution

Modul 6. Identitäts- und Zugriffsmanagement in der IT-Sicherheit

6.1. Identitäts- und Zugriffsmanagement (IAM)
- 6.1.1. Digitale Identität
- 6.1.2. Identitätsmanagement
- 6.1.3. Identitätsföderation

6.2. Physische Zugangskontrolle
- 6.2.1. Schutzsysteme
- 6.2.2. Bereichssicherheit
- 6.2.3. Wiederherstellungseinrichtungen

6.3. Logische Zugriffskontrolle
- 6.3.1. Authentifizierung: Typologie
- 6.3.2. Authentifizierungsprotokolle
- 6.3.3. Angriffe zur Authentifizierung

6.4. Logische Zugriffskontrolle. MFA-Authentifizierung
- 6.4.1. Logische Zugriffskontrolle. MFA-Authentifizierung
- 6.4.2. Passwörter. Bedeutung
- 6.4.3. Angriffe zur Authentifizierung

6.5. Logische Zugriffskontrolle. Biometrische Authentifizierung
- 6.5.1. Logische Zugriffskontrolle. Biometrische Authentifizierung
  - 6.5.1.1. Biometrische Authentifizierung. Anforderungen
- 6.5.2. Funktionsweise
- 6.5.3. Modelle und Techniken

6.6. Authentifizierungs-Management-Systeme
- 6.6.1. *Single sign on*
- 6.6.2. Kerberos
- 6.6.3. AAA-Systeme

6.7. Authentifizierung-Management-Systeme: AAA-Systeme
- 6.7.1. TACACS
- 6.7.2. RADIUS
- 6.7.3. DIAMETER

6.8. Kontrollsysteme für den Zugang
- 6.8.1. FW - Firewalls
- 6.8.2. VPN - Virtuelle private Netzwerke
- 6.8.3. IDS - *Intrusion Detection System*

6.9. Netzwerk-Zugangskontrollsysteme
- 6.9.1. NAC
- 6.9.2. Architektur und Elemente
- 6.9.3. Betrieb und Standardisierung

6.10. Zugang auf drahtlose Netzwerke
- 6.10.1. Arten von drahtlosen Netzwerken
- 6.10.2. Sicherheit für drahtlose Netzwerke
- 6.10.3. Angriffe auf drahtlose Netzwerke

Modul 7. Sicherheit bei Kommunikation und Softwarebetrieb

7.1. Computersicherheit bei Kommunikation und Softwarebetrieb
- 7.1.1. Computersicherheit
- 7.1.2. Cybersicherheit
- 7.1.3. *Cloud*-Sicherheit

7.2. Computersicherheit in der Kommunikation und im Softwarebetrieb. Typologie
- 7.2.1. Physische Sicherheit
- 7.2.2. Logische Sicherheit

7.3. Sicherheit in der Kommunikation
- 7.3.1. Wichtigste Elemente
- 7.3.2. Netzwerksicherheit
- 7.3.3. Bewährte Praktiken

7.4. Cyberintelligenz
- 7.4.1. *Social Engineering*
- 7.4.2. *Deep Web*
- 7.4.3. *Phishing*
- 7.4.4. *Malware*

7.5. Sichere Entwicklung in Kommunikation und Softwarebetrieb
- 7.5.1. Sichere Entwicklung. HTTP-Protokoll
- 7.5.2. Sichere Entwicklung. Lebenszyklus
- 7.5.3. Sichere Entwicklung. PHP-Sicherheit
- 7.5.4. Sichere Entwicklung. NET-Sicherheit
- 7.5.5. Sichere Entwicklung. Bewährte Praktiken

7.6. Informationssicherheits-Managementsysteme in Kommunikation und Software
- 7.6.1. GDPR
- 7.6.2. ISO 27021
- 7.6.3. ISO 27017/18

7.7. SIEM-Technologien
- 7.7.1. SIEM-Technologien
- 7.7.2. SOC Betrieb
- 7.7.3. SIEM *Vendors*

7.8. Die Rolle der Sicherheit in Organisationen
- 7.8.1. Rollen in Organisationen
- 7.8.2. Die Rolle von IoT-Spezialisten in Unternehmen
- 7.8.3. Anerkannte Zertifizierungen auf dem Markt

7.9. Forensische Analyse
- 7.9.1. Forensische Analyse
- 7.9.2. Forensische Analyse. Methodik
- 7.9.3. Forensische Analyse. Tools und Implementierung

7.10. Cybersecurity heute
- 7.10.1. Große Cyberangriffe
- 7.10.2. Prognosen zur Beschäftigungsfähigkeit
- 7.10.3. Herausforderungen

Modul 8. Sicherheit in Cloud-Umgebungen

8.1. Sicherheit in *Cloud-Computing*-Umgebungen
- 8.1.1. Sicherheit in *Cloud-Computing*-Umgebungen
- 8.1.2. Sicherheit in *Cloud-Computing*-Umgebungen. Bedrohungen und Sicherheitsrisiken
- 8.1.3. Sicherheit in *Cloud-Computing*-Umgebungen. Wichtige Sicherheitsaspekte

8.2. Arten von *Cloud*-Infrastrukturen
- 8.2.1. Öffentlich
- 8.2.2. Privat
- 8.2.3. Hybrid

8.3. Modell der gemeinsamen Verwaltung
- 8.3.1. Vom Anbieter verwaltete Sicherheitselemente
- 8.3.2. Vom Kunden verwaltete Elemente
- 8.3.3. Definition der Sicherheitsstrategie

8.4. Mechanismen der Prävention
- 8.4.1. Authentifizierungs-Management-Systeme
- 8.4.2. Berechtigungsverwaltungssystem: Zugriffsrichtlinien
- 8.4.3. Systeme zur Schlüsselverwaltung

8.5. Sicherung von Systemen
- 8.5.1. Sicherung von Speichersystemen
- 8.5.2. Sicherung von Datenbanksystemen
- 8.5.3. Sichern von Daten bei der Übermittlung

8.6. Schutz der Infrastruktur
- 8.6.1. Entwurf und Implementierung eines sicheren Netzwerks
- 8.6.2. Sicherheit von Computerressourcen
- 8.6.3. Tools und Ressourcen zum Schutz der Infrastruktur

8.7. Erkennung von Bedrohungen und Angriffen
- 8.7.1. Auditing, *Logging* und Überwachungssysteme
- 8.7.2. Ereignis- und Alarmsysteme
- 8.7.3. SIEM-Systeme

8.8. Reaktion auf Vorfälle
- 8.8.1. Plan zur Reaktion auf Vorfälle
- 8.8.2. Geschäftskontinuität
- 8.8.3. Forensische Analyse und Behebung von Vorfällen der gleichen Art

8.9. Sicherheit in öffentlichen *Clouds*
- 8.9.1. AWS (Amazon Web Services)
- 8.9.2. Microsoft Azure
- 8.9.3. Google GCP
- 8.9.4. Oracle Cloud

8.10. Regulierung und Compliance
- 8.10.1. Compliance im Bereich Sicherheit
- 8.10.2. Risikomanagement
- 8.10.3. Menschen und Prozesse in Organisationen

Modul 9. Sicherheit der Kommunikation von IoT-Geräten

9.1. Von der Telemetrie zum IoT
- 9.1.1. Telemetrie
- 9.1.2. M2M-Konnektivität
- 9.1.3. Demokratisierung der Telemetrie

9.2. IoT-Referenzmodelle
- 9.2.1. IoT-Referenzmodelle
- 9.2.2. Vereinfachte IoT-Architektur

9.3. IoT-Sicherheitsschwachstellen
- 9.3.1. IoT-Geräte
- 9.3.2. IoT-Geräte. Kasuistik der Verwendung
- 9.3.3. IoT-Geräte. Schwachstellen

9.4. IoT-Konnektivität
- 9.4.1. PAN, LAN, WAN-Netzwerke
- 9.4.2. Drahtlose Technologien außerhalb des IoT
- 9.4.3. Drahtlose LPWAN-Technologien

9.5. LPWAN-Technologien
- 9.5.1. Das eiserne Dreieck der LPWANs
- 9.5.2. Freie Frequenzbänder vs. Lizensierte Bänder
- 9.5.3. LPWAN-Technologie-Optionen

9.6. LoRaWAN-Technologie
- 9.6.1. LoRaWAN-Technologie
- 9.6.2. LoRaWAN-Anwendungsfälle. Ökosystem
- 9.6.3. LoRaWAN-Sicherheit

9.7. Sigfox-Technologie
- 9.7.1. Sigfox-Technologie
- 9.7.2. Sigfox-Anwendungsfälle. Ökosystem
- 9.7.3. Sicherheit in Sigfox

9.8. IoT-Mobilfunktechnologie
- 9.8.1. IoT-Mobilfunktechnologie (NB-IoT und LTE-M)
- 9.8.2. Anwendungsfälle für IoT-Mobilfunktechnologie Ökosystem
- 9.8.3. IoT-Mobilfunktechnologie-Sicherheit

9.9. WiSUN-Technologie
- 9.9.1. WiSUN-Technologie
- 9.9.2. WiSUN-Anwendungsfälle. Ökosystem
- 9.9.3. Sicherheit in WiSUN

9.10. Andere IoT-Technologien
- 9.10.1. Andere IoT-Technologien
- 9.10.2. Anwendungsfälle und Ökosystem anderer IoT-Technologien
- 9.10.3. Sicherheit in anderen IoT-Technologien

Modul 10. Business Continuity Plan in Verbindung mit Sicherheit

10.1. *Business Continuity Plan*
- 10.1.1. Pläne für die Geschäftskontinuität (BCP)
- 10.1.2. Plan für die Geschäftskontinuität (BCP). Schlüsselaspekte
- 10.1.3. *Business Continuity Plan* (BCP) für die Unternehmensbewertung

10.2. Metriken in einem *Business Continuity Plan* (BCP)
- 10.2.1. *Recovery Time Objective* (RTO) und *Recovery Point Objective* (RPO)
- 10.2.2. Maximal verträgliche Zeit (MTD)
- 10.2.3. Mindestanforderungen für die Wiederherstellung (ROL)
- 10.2.4. Wiederherstellungspunkt-Ziel (RPO)

10.3. Kontinuitätsprojekte. Typologie
- 10.3.1. Plan für die Geschäftskontinuität (BCP)
- 10.3.2. IKT-Kontinuitätsplan (ICTCP)
- 10.3.3. Plan zur Wiederherstellung im Katastrophenfall (DRP)

10.4. Risikomanagement im Zusammenhang mit dem BCP
- 10.4.1. Analyse der Auswirkungen auf das Geschäft
- 10.4.2. Vorteile der Implementierung eines BCP
- 10.4.3. Risikobasiertes Denken

10.5. Lebenszyklus eines *Business Continuity Plans*
- 10.5.1. Phase 1: Analyse der Organisation
- 10.5.2. Phase 2: Festlegung der Kontinuitätsstrategie
- 10.5.3. Phase 3: Reaktion auf Notfälle
- 10.5.4. Phase 4: Tests, Wartung und Überprüfung

10.6. Phase der Organisationsanalyse eines BCP
- 10.6.1. Identifizierung der Prozesse, die in den Geltungsbereich des BCP fallen
- 10.6.2. Identifizierung von kritischen Geschäftsbereichen
- 10.6.3. Identifizierung von Abhängigkeiten zwischen Bereichen und Prozessen
- 10.6.4. Bestimmung der geeigneten MTD
- 10.6.5. Liefergegenstände. Erstellung eines Plans

10.7. Phase der Festlegung der Kontinuitätsstrategie in einem BCP
- 10.7.1. Rollen in der Phase der Strategiebestimmung
- 10.7.2. Aufgaben in der Phase der Strategiefestlegung
- 10.7.3. Lieferbare

10.8. Phase der Notfallmaßnahmen eines BCP
- 10.8.1. Rollen in der Reaktionsphase
- 10.8.2. Aufgaben in dieser Phase
- 10.8.3. Lieferbare

10.9. Test-, Wartungs- und Überarbeitungsphase eines BCP
- 10.9.1. Rollen in der Test-, Wartungs- und Überprüfungsphase
- 10.9.2. Aufgaben in der Test-, Wartungs- und Überprüfungsphase
- 10.9.3. Lieferbare

10.10. ISO-Normen im Zusammenhang mit *Business Continuity Plans* (BCP)
- 10.10.1. ISO 22301:2019
- 10.10.2. ISO 22313:2020
- 10.10.3. Andere verwandte ISO- und internationale Normen

Modul 11. Führung, Ethik und soziale Verantwortung der Unternehmen

11.1. Globalisierung und Governance
- 11.1.1. Governance und Corporate Governance
- 11.1.2. Grundlagen der Corporate Governance in Unternehmen
- 11.1.3. Die Rolle des Verwaltungsrats im Rahmen der Corporate Governance

11.2. Führung
- 11.2.1. Führung. Ein konzeptioneller Ansatz
- 11.2.2. Führung in Unternehmen
- 11.2.3. Die Bedeutung der Führungskraft im Management

11.3. *Cross Cultural Management*
- 11.3.1. Konzept des *Cross Cultural Management*
- 11.3.2. Beiträge zum Wissen über Nationalkulturen
- 11.3.3. Diversitätsmanagement

11.4. Managemententwicklung und Führung
- 11.4.1. Konzept der Managemententwicklung
- 11.4.2. Konzept der Führung
- 11.4.3. Theorien der Führung
- 11.4.4. Führungsstile
- 11.4.5. Intelligenz in der Führung
- 11.4.6. Die Herausforderungen der Führung heute

11.5. Wirtschaftsethik
- 11.5.1. Ethik und Moral
- 11.5.2. Wirtschaftsethik
- 11.5.3. Führung und Ethik in Unternehmen

11.6. Nachhaltigkeit
- 11.6.1. Nachhaltigkeit und nachhaltige Entwicklung
- 11.6.2. Agenda 2030
- 11.6.3. Nachhaltige Unternehmen

11.7. Soziale Verantwortung des Unternehmens
- 11.7.1. Die internationale Dimension der sozialen Verantwortung der Unternehmen
- 11.7.2. Umsetzung der sozialen Verantwortung der Unternehmen
- 11.7.3. Auswirkungen und Messung der sozialen Verantwortung der Unternehmen

11.8. Verantwortungsvolle Management-Systeme und -Tools
- 11.8.1. CSR: Soziale Verantwortung der Unternehmen
- 11.8.2. Wesentliche Aspekte für die Umsetzung einer verantwortungsvollen Managementstrategie
- 11.8.3. Schritte zur Umsetzung eines Managementsystems für die soziale Verantwortung von Unternehmen
- 11.8.4. CSR-Instrumente und -Standards

11.9. Multinationale Unternehmen und Menschenrechte
- 11.9.1. Globalisierung, multinationale Unternehmen und Menschenrechte
- 11.9.2. Multinationale Unternehmen und internationales Recht
- 11.9.3. Rechtsinstrumente für multinationale Unternehmen in der Menschenrechtsgesetzgebung

11.10. Rechtliches Umfeld und *Corporate Governance*
- 11.10.1. Internationale Einfuhr- und Ausfuhrnormen
- 11.10.2. Geistiges und gewerbliches Eigentum
- 11.10.3. Internationales Arbeitsrecht

Modul 12. Personal- und Talentmanagement

12.1. Strategisches Management von Menschen
- 12.1.1. Strategisches Management und Humanressourcen
- 12.1.2. Strategisches Management von Menschen

12.2. Kompetenzbasiertes HR-Management
- 12.2.1. Analyse des Potenzials
- 12.2.2. Vergütungspolitik
- 12.2.3. Karriere-/Nachfolge-Pläne

12.3. Leistungsbewertung und Leistungsmanagement
- 12.3.1. Leistungsmanagement
- 12.3.2. Leistungsmanagement: Ziel und Prozesse

12.4. Innovation im Talent- und Personalmanagement
- 12.4.1. Modelle für strategisches Talentmanagement
- 12.4.2. Identifizierung, Schulung und Entwicklung von Talenten
- 12.4.3. Loyalität und Bindung
- 12.4.4. Proaktivität und Innovation

12.5. Motivation
- 12.5.1. Die Natur der Motivation
- 12.5.2. Erwartungstheorie
- 12.5.3. Theorien der Bedürfnisse
- 12.5.4. Motivation und finanzieller Ausgleich

12.6. Entwicklung von Hochleistungsteams
- 12.6.1. Hochleistungsteams: selbstverwaltete Teams
- 12.6.2. Methoden für das Management selbstverwalteter Hochleistungsteams

12.7. Änderungsmanagement
- 12.7.1. Änderungsmanagement
- 12.7.2. Art der Prozesse des Änderungsmanagements
- 12.7.3. Etappen oder Phasen im Änderungsmanagement

12.8. Verhandlungsführung und Konfliktmanagement
- 12.8.1. Verhandlung
- 12.8.2. Management von Konflikten
- 12.8.3. Krisenmanagement

12.9. Kommunikation der Führungskräfte
- 12.9.1. Interne und externe Kommunikation in der Geschäftswelt
- 12.9.2. Abteilungen für Kommunikation
- 12.9.3. Der Verantwortliche für die Kommunikation des Unternehmens. Das Profil des Dircom

12.10. Produktivität, Anziehung, Bindung und Aktivierung von Talenten
- 12.10.1. Produktivität
- 12.10.2. Anziehung und Bindung von Talenten

Modul 13. Wirtschaftlich-finanzielle Verwaltung

13.1. Wirtschaftliches Umfeld
- 13.1.1. Makroökonomisches Umfeld und das nationale Finanzsystem
- 13.1.2. Finanzinstitutionen
- 13.1.3. Finanzmärkte
- 13.1.4. Finanzielle Vermögenswerte
- 13.1.5. Andere Einrichtungen des Finanzsektors

13.2. Buchhaltung
- 13.2.1. Grundlegende Konzepte
- 13.2.2. Die Vermögenswerte des Unternehmens
- 13.2.3. Die Verbindlichkeiten des Unternehmens
- 13.2.4. Das Nettovermögen des Unternehmens
- 13.2.5. Die Gewinn- und Verlustrechnung

13.3. Informationssysteme und *Business Intelligence*
- 13.3.1. Grundlagen und Klassifizierung
- 13.3.2. Phasen und Methoden der Kostenzuweisung
- 13.3.3. Wahl der Kostenstelle und Auswirkung

13.4. Haushalts- und Verwaltungskontrolle
- 13.4.1. Das Haushaltsmodell
- 13.4.2. Das Kapitalbudget
- 13.4.3. Das Betriebsbudget
- 13.4.5. Cash-Budget
- 13.4.6. Haushaltsüberwachung

13.5. Finanzmanagement
- 13.5.1. Die finanziellen Entscheidungen des Unternehmens
- 13.5.2. Die Finanzabteilung
- 13.5.3. Bargeldüberschüsse
- 13.5.4. Mit der Finanzverwaltung verbundene Risiken
- 13.5.5. Risikomanagement der Finanzverwaltung

13.6. Finanzielle Planung
- 13.6.1. Definition der Finanzplanung
- 13.6.2. Zu ergreifende Maßnahmen bei der Finanzplanung
- 13.6.3. Erstellung und Festlegung der Unternehmensstrategie
- 13.6.4. Die *Cash-Flow*-Tabelle
- 13.6.5. Die Tabelle des Betriebskapitals

13.7. Finanzielle Unternehmensstrategie
- 13.7.1. Unternehmensstrategie und Finanzierungsquellen
- 13.7.2. Produkte zur Unternehmensfinanzierung

13.8. Strategische Finanzierungen
- 13.8.1. Selbstfinanzierung
- 13.8.2. Erhöhung der Eigenmittel
- 13.8.3. Hybride Ressourcen
- 13.8.4. Finanzierung durch Intermediäre

13.9. Finanzanalyse und -planung
- 13.9.1. Analyse der Bilanz
- 13.9.2. Analyse der Gewinn- und Verlustrechnung
- 13.9.3. Analyse der Rentabilität

13.10. Analyse und Lösung von Fällen/Problemen
- 13.10.1. Finanzinformationen über Industria de Diseño y Textil, S.A. (INDITEX)

Modul 14. Kaufmännisches Management und strategisches Marketing

14.1. Kaufmännisches Management
- 14.1.1. Konzeptioneller Rahmen des kaufmännischen Managements
- 14.1.2. Kaufmännische Strategie und Planung
- 14.1.3. Die Rolle der kaufmännischen Leiter

14.2. Marketing
- 14.2.1. Marketingkonzept
- 14.2.2. Grundlagen des Marketings
- 14.2.3. Marketingaktivitäten des Unternehmens

14.3. Strategisches Marketingmanagement
- 14.3.1. Konzept des strategischen Marketings
- 14.3.2. Konzept der strategischen Marketingplanung
- 14.3.3. Phasen des Prozesses der strategischen Marketingplanung

14.4. Digitales Marketing und elektronischer Handel
- 14.4.1. Ziele des digitalen Marketings und des elektronischen Handels
- 14.4.2. Digitales Marketing und die dabei verwendeten Medien
- 14.4.3. Elektronischer Handel. Allgemeiner Kontext
- 14.4.4. Kategorien des elektronischen Handels
- 14.4.5. Vor- und Nachteile des E-Commerce im Vergleich zum traditionellen Handel

14.5. Digitales Marketing zur Stärkung der Marke
- 14.5.1. Online-Strategien zur Verbesserung des Rufs Ihrer Marke
- 14.5.2. *Branded Content & Storytelling*

14.6. Digitales Marketing zur Anwerbung und Bindung von Kunden
- 14.6.1. Strategien für Loyalität und Engagement über das Internet
- 14.6.2. *Visitor Relationship Management*
- 14.6.3. Hypersegmentierung

14.7. Verwaltung digitaler Kampagnen
- 14.7.1. Was ist eine digitale Werbekampagne?
- 14.7.2. Schritte zum Start einer Online-Marketing-Kampagne
- 14.7.3. Fehler bei digitalen Werbekampagnen

14.8. Verkaufsstrategie
- 14.8.1. Verkaufsstrategie
- 14.8.2. Verkaufsmethoden

14.9. Unternehmenskommunikation
- 14.9.1. Konzept
- 14.9.2. Bedeutung der Kommunikation in der Organisation
- 14.9.3. Art der Kommunikation in der Organisation
- 14.9.4. Funktionen der Kommunikation in der Organisation
- 14.9.5. Elemente der Kommunikation
- 14.9.6. Kommunikationsprobleme
- 14.9.7. Szenarien der Kommunikation

14.10. Kommunikation und digitaler Ruf
- 14.10.1. Online-Reputation
- 14.10.2. Wie misst man die digitale Reputation?
- 14.10.3. Online-Reputationstools
- 14.10.4. Online-Reputationsbericht
- 14.10.5. Online-*Branding*

Modul 15. Geschäftsleitung

15.1. General Management
- 15.1.1. Konzept des General Management
- 15.1.2. Die Tätigkeit des Generaldirektors
- 15.1.3. Der Generaldirektor und seine Aufgaben
- 15.1.4. Transformation der Arbeit der Direktion

15.2. Der Manager und seine Aufgaben. Organisationskultur und Ansätze
- 15.2.1. Der Manager und seine Aufgaben. Organisationskultur und Ansätze

15.3. Operations Management
- 15.3.1. Bedeutung des Managements
- 15.3.2. Die Wertschöpfungskette
- 15.3.3. Qualitätsmanagement

15.4. Rhetorik und Schulung von Pressesprechern
- 15.4.1. Zwischenmenschliche Kommunikation
- 15.4.2. Kommunikationsfähigkeit und Einflussnahme
- 15.4.3. Kommunikationsbarrieren

15.5. Persönliche und organisatorische Kommunikationsmittel
- 15.5.1. Zwischenmenschliche Kommunikation
- 15.5.2. Instrumente der zwischenmenschlichen Kommunikation
- 15.5.3. Kommunikation in der Organisation
- 15.5.4. Werkzeuge in der Organisation

15.6. Krisenkommunikation
- 15.6.1. Krise
- 15.6.2. Phasen der Krise
- 15.6.3. Nachrichten: Inhalt und Momente

15.7. Einen Krisenplan vorbereiten
- 15.7.1. Analyse der potenziellen Probleme
- 15.7.2. Planung
- 15.7.3. Angemessenheit des Personals

15.8. Emotionale Intelligenz
- 15.8.1. Emotionale Intelligenz und Kommunikation
- 15.8.2. Durchsetzungsvermögen, Einfühlungsvermögen und aktives Zuhören
- 15.8.3. Selbstwertgefühl und emotionale Kommunikation

15.9. *Personal Branding*
- 15.9.1. Strategien für den Aufbau einer persönlichen Marke
- 15.9.2. Regeln des Personal Branding
- 15.9.3. Instrumente zum Aufbau einer persönlichen Marke

15.10. Führungsrolle und Teammanagement
- 15.10.1. Leadership und Führungsstile
- 15.10.2. Führungsqualitäten und Herausforderungen
- 15.10.3. Management von Veränderungsprozessen
- 15.10.4. Leitung multikultureller Teams

Die besten Dozenten und ein innovatives Lehrsystem in Kombination mit dem vollständigsten und aktuellsten Lehrplan: das ist eine großartige Gelegenheit, um als Informatiker voranzukommen"

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 hinter sich lässt 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 an den Grundlagen der traditionellen Universitäten auf der ganzen Welt rüttelt"

Sie werden Zugang zu einem Lernsystem haben, das auf Wiederholung basiert, mit natürlichem und progressivem Unterricht während des gesamten Lehrplans.

Der Student wird durch gemeinschaftliche Aktivitäten und reale Fälle lernen, wie man komplexe Situationen in realen Geschäftsumgebungen löst.

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 Jurastudenten das Recht nicht nur auf der Grundlage theoretischer Inhalte erlernen. Sie bestand darin, ihnen reale komplexe Situationen zu präsentieren, damit sie fundierte Entscheidungen treffen und Werturteile darüber fällen konnten, wie diese zu lösen sind. Sie wurde 1924 als Standardlehrmethode in Harvard etabliert.

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 Studenten mit mehreren realen Fällen konfrontiert. Sie müssen ihr gesamtes Wissen integrieren, recherchieren, argumentieren und ihre Ideen und Entscheidungen verteidigen.

Relearning Methodology

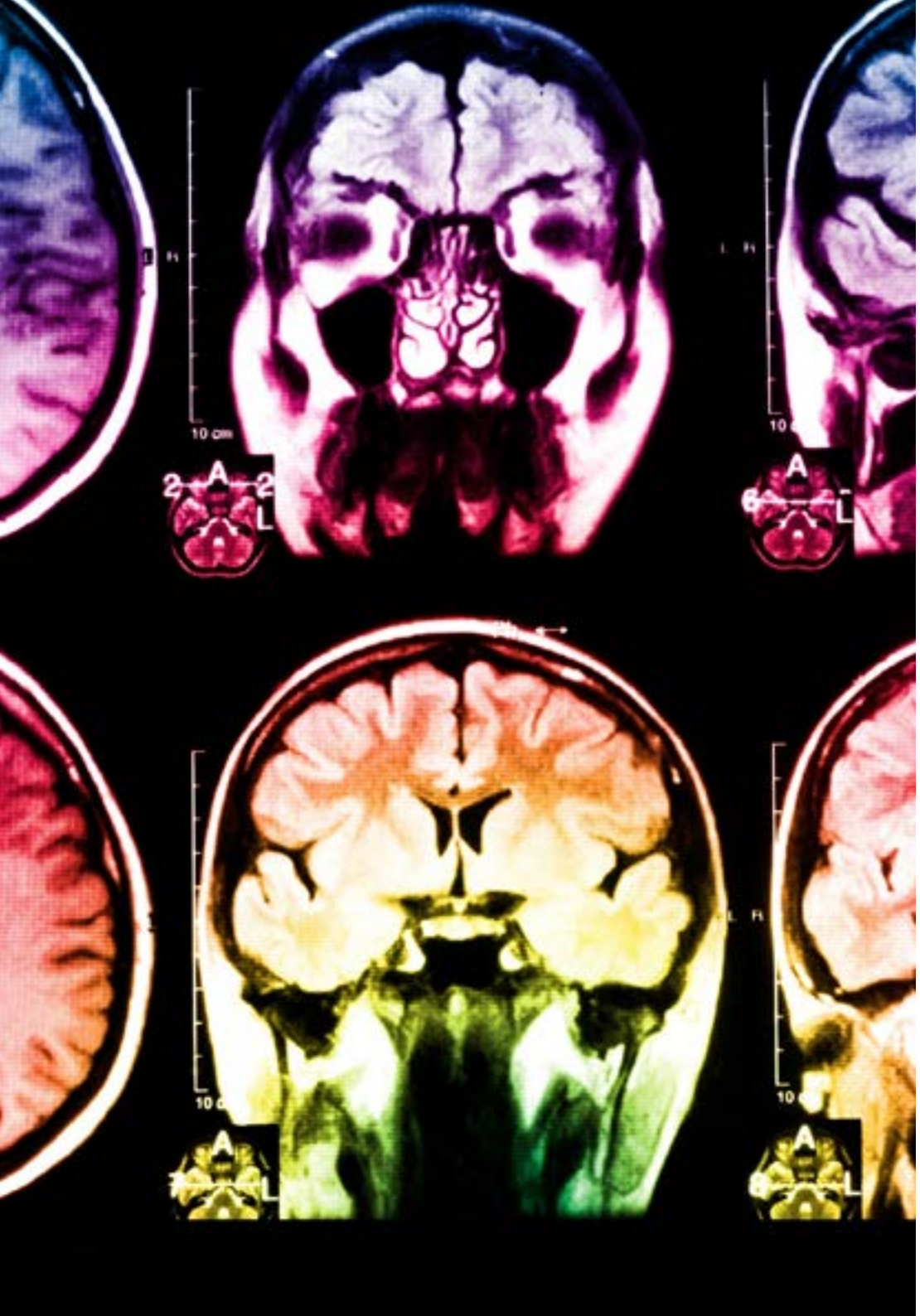
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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 zu spezialisieren. 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 spanischsprachigen Online-Universität 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 fortgebildet. 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 Ihre Spezialisierung 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 Neurocognitive Context-Dependent E-Learning 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 Online-Arbeitsmethode von TECH zu schaffen. All dies mit den neuesten Techniken, die in jedem einzelnen der Materialien, die dem Studenten zur Verfügung gestellt werden, qualitativ hochwertige Elemente bieten.

Meisterklassen

Die Nützlichkeit der Expertenbeobachtung ist wissenschaftlich belegt.

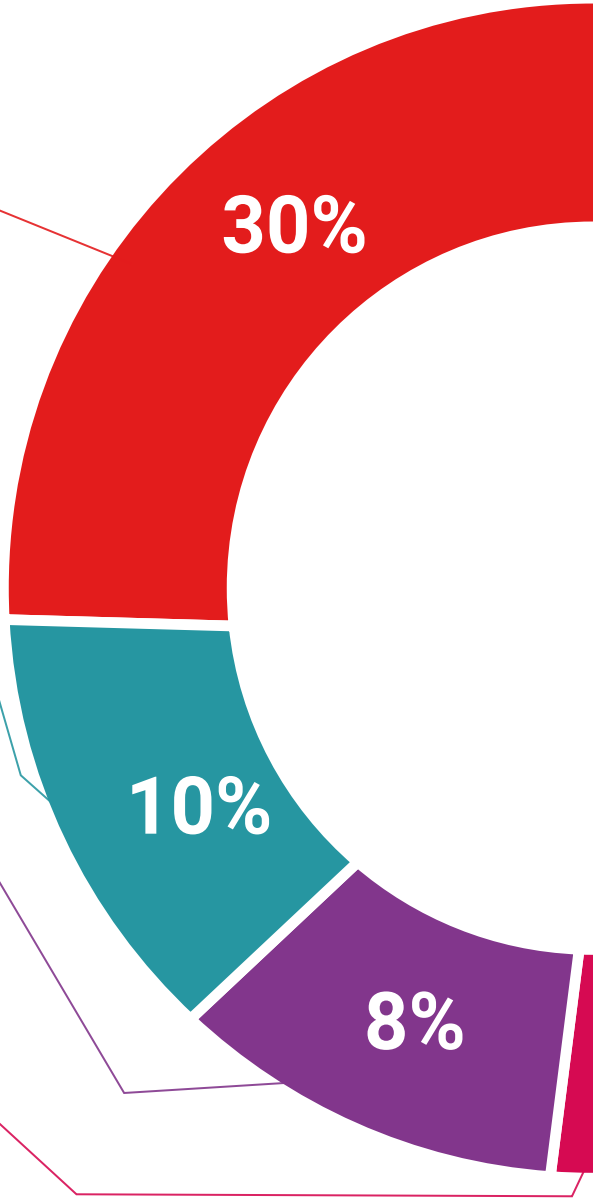
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

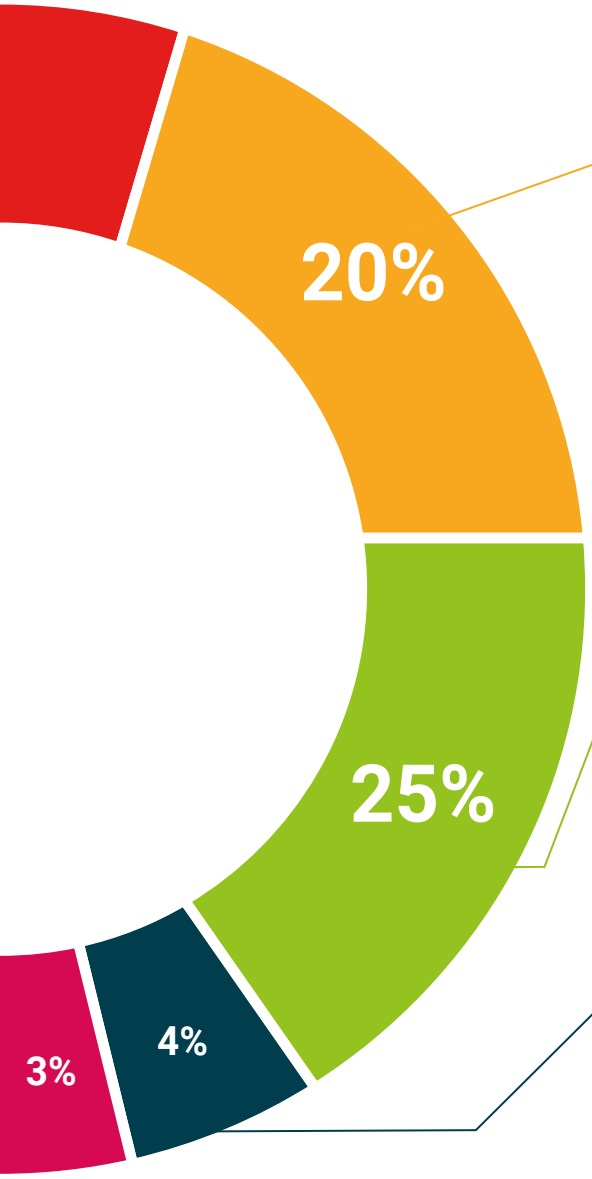
Übungen für Fertigkeiten und Kompetenzen

Sie werden Aktivitäten durchführen, um spezifische Kompetenzen und Fertigkeiten in jedem Fachbereich zu entwickeln. Übungen und Aktivitäten 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 hat der Student Zugang zu allem, was er für seine Fortbildung benötigt.





Case Studies

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.

Testing & Retesting

Die Kenntnisse des Studenten werden während des gesamten Programms regelmäßig durch Bewertungs- und Selbsteinschätzungsaktivitäten und -übungen beurteilt und neu bewertet, so dass der Student überprüfen kann, wie er seine Ziele erreicht.

07

Qualifizierung

Der MBA in Fortgeschrittenes Cybersecurity Management (CISO) garantiert neben der präzisesten und aktuellsten Fortbildung 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 **MBA in Fortgeschrittenes Cybersecurity Management (CISO)** 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: **Privater Masterstudiengang in MBA in Fortgeschrittenes Cybersecurity Management (CISO)**

Modalität: **online**

Dauer: **12 Monate**


tech technologische universität

Verleiht dieses

DIPLOM

an

Herr/Frau _____, mit Ausweis-Nr. _____

Für den erfolgreichen Abschluss und die Akkreditierung des Programms

PRIVATER MASTERSTUDIENGANG

in

MBA in Fortgeschrittenes Cybersecurity Management (CISO)

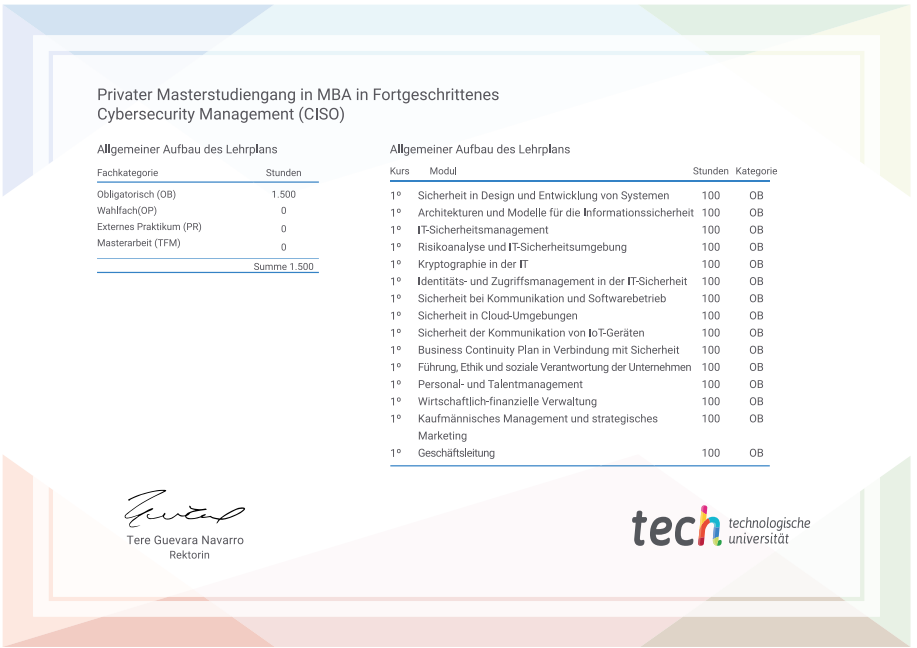
Es handelt sich um einen von dieser Universität verliehenen Abschluss, mit einer Dauer von 1.500 Stunden, mit Anfangsdatum tt/mm/jjjj und Enddatum tt/mm/jjjj.

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


Privater Masterstudiengang in MBA in Fortgeschrittenes Cybersecurity Management (CISO)

Allgemeiner Aufbau des Lehrplans

Fachkategorie	Stunden
Obligatorisch (OB)	1.500
Wahlfach(OP)	0
Externes Praktikum (PR)	0
Masterarbeit (TFM)	0
	Summe 1.500

Allgemeiner Aufbau des Lehrplans

Kurs	Modul	Stunden	Kategorie
1°	Sicherheit in Design und Entwicklung von Systemen	100	OB
1°	Architekturen und Modelle für die Informationssicherheit	100	OB
1°	IT-Sicherheitsmanagement	100	OB
1°	Risikoanalyse und IT-Sicherheitsumgebung	100	OB
1°	Kryptographie in der IT	100	OB
1°	Identitäts- und Zugriffsmanagement in der IT-Sicherheit	100	OB
1°	Sicherheit bei Kommunikation und Softwarebetrieb	100	OB
1°	Sicherheit in Cloud-Umgebungen	100	OB
1°	Sicherheit der Kommunikation von IoT-Geräten	100	OB
1°	Business Continuity Plan in Verbindung mit Sicherheit	100	OB
1°	Führung, Ethik und soziale Verantwortung der Unternehmen	100	OB
1°	Personal- und Talentmanagement	100	OB
1°	Wirtschaftlich-finanzielle Verwaltung	100	OB
1°	Kaufmännisches Management und strategisches Marketing	100	OB
1°	Geschäftsleitung	100	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

Privater Masterstudiengang

MBA in Fortgeschrittenes Cybersecurity Management (CISO)

- Modalität: **online**
- Dauer: **12 Monate**
- Qualifizierung: **TECH Technologische Universität**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Privater Masterstudiengang

MBA in Fortgeschrittenes Cybersecurity Management (CISO)

tech technologische universität