

Executive Master

MBA in Cybersecurity
Management (CISO, Chief
Information Security Officer)

M B A C M C I S O





Executive Master MBA in Cybersecurity Management (CISO, Chief Information Security Officer)

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

Internetzugang: www.techtitute.com/de/wirtschaftsschule/masterstudiengang/masterstudiengang-mba-cybersecurity-management-ciso-chief-information-security-officer

Index

01

Willkommen

Seite 4

02

Warum an der TECH studieren?

Seite 6

03

Warum unser Programm?

Seite 10

04

Ziele

Seite 14

05

Kompetenzen

Seite 20

06

Struktur und Inhalt

Seite 26

07

Methodik

Seite 46

08

Profil unserer Studenten

Seite 54

09

Kursleitung

Seite 58

10

Auswirkung auf Ihre Karriere

Seite 82

11

Vorteile für Ihr Unternehmen

Seite 86

12

Qualifizierung

Seite 90

01

Willkommen

Die heutige Gesellschaft ist hyper-verbunden. Das Informationszeitalter ermöglicht es den Bürgern, mit einem Mausklick über alle Daten informiert zu sein. Das bedeutet aber auch, dass virtuelle Bedrohungen an der Tagesordnung sind und Unternehmen mehr denn je Gefahr laufen, Opfer von *Malware* zu werden, die ihre Produktion und Sicherheit beeinträchtigen oder sogar persönliche Daten von Kunden und Mitarbeitern preisgeben und ihre IT-Schwachstellen aufdecken kann. Während der Schutz in diesem Bereich die Aufgabe von IT-Spezialisten ist, entscheiden sich immer mehr *Chief Revenue Officers* und andere Manager dafür, sich auf diesen Bereich zu spezialisieren, um zu versuchen, Cyberkriminelle zu stoppen und zu vermeiden, das Ziel ihrer Angriffe zu werden. Aus diesem Grund hat TECH dieses Programm entwickelt, in dem Fachleute aus der Wirtschaft die relevantesten Informationen des Augenblicks erhalten, und zwar durch einen didaktischen Lehrplan, der für die Studenten leicht zu verstehen ist. Auf diese Weise und dank der erworbenen Kenntnisse wird der Absolvent in der Lage sein, mit vollem Erfolg als Chief Information Security Officer zu arbeiten, eine Position, die auf dem Vormarsch ist und große Wachstumschancen bietet.



MBA in Cybersecurity Management (CISO, Chief Information Security Officer)
TECH Technologische Universität



“

*Steigern Sie Ihre Kompetenzen im Bereich
Cybersecurity Management dank 10
Masterclasses, die von einem international
anerkannten Spezialisten gehalten werden”*

02

Warum an der TECH studieren?

TECH ist die weltweit größte 100%ige Online Business School. Es handelt sich um eine Elite-Business School mit einem Modell, das höchsten akademischen Ansprüchen genügt. Ein leistungsstarkes internationales Zentrum für die intensive Fortbildung von Führungskräften.



“

TECH ist eine Universität an der Spitze der Technologie, die dem Studenten alle Ressourcen zur Verfügung stellt, um ihm zu helfen, geschäftlich erfolgreich zu sein"

Bei TECH Technologische Universität



Innovation

Die Universität bietet ein Online-Lernmodell an, das modernste Bildungstechnologie mit höchster pädagogischer Genauigkeit verbindet. Eine einzigartige Methode mit höchster internationaler Anerkennung, die dem Studenten die Schlüssel für seine Entwicklung in einer Welt des ständigen Wandels liefert, in der Innovation der wesentliche Einsatz eines jeden Unternehmers sein muss.

"Die Erfolgsgeschichte von Microsoft Europa" für die Einbeziehung des neuen interaktiven Multivideosystems in unsere Programme.



Maximalforderung

Das Zulassungskriterium von TECH ist nicht wirtschaftlich. Sie brauchen keine große Investitionen zu tätigen, um bei TECH zu studieren. Um jedoch einen Abschluss bei TECH zu erlangen, werden die Grenzen der Intelligenz und der Kapazität des Studenten getestet. Die akademischen Standards von TECH sind sehr hoch...

95% | der Studenten von TECH schließen ihr Studium erfolgreich ab



Networking

Fachleute aus der ganzen Welt nehmen an der TECH teil, so dass der Student ein großes Netzwerk von Kontakten knüpfen kann, die für seine Zukunft nützlich sein werden.

+100.000 jährlich spezialisierte Manager
+200 verschiedene Nationalitäten



Empowerment

Der Student wird Hand in Hand mit den besten Unternehmen und Fachleuten von großem Prestige und Einfluss wachsen. TECH hat strategische Allianzen und ein wertvolles Netz von Kontakten zu den wichtigsten Wirtschaftsakteuren auf den 7 Kontinenten aufgebaut.

+500 | Partnerschaften mit den besten Unternehmen



Talent

Dieses Programm ist ein einzigartiger Vorschlag, um die Talente des Studenten in der Geschäftswelt zu fördern. Eine Gelegenheit für ihn, seine Anliegen und seine Geschäftsvision vorzutragen.

TECH hilft dem Studenten, sein Talent am Ende dieses Programms der Welt zu zeigen.



Multikultureller Kontext

Ein Studium bei TECH bietet dem Studenten eine einzigartige Erfahrung. Er wird in einem multikulturellen Kontext studieren. In einem Programm mit einer globalen Vision, dank derer er die Arbeitsweise in verschiedenen Teilen der Welt kennenlernen und die neuesten Informationen sammeln kann, die am besten zu seiner Geschäftsidee passen.

Unsere Studenten kommen aus mehr als 200 Ländern.

TECH strebt nach Exzellenz und hat zu diesem Zweck eine Reihe von Merkmalen, die sie zu einer einzigartigen Universität machen:



Analyse

TECH erforscht die kritische Seite des Studenten, seine Fähigkeit, Dinge zu hinterfragen, seine Problemlösungsfähigkeiten und seine zwischenmenschlichen Fähigkeiten.



Akademische Spitzenleistung

TECH bietet dem Studenten die beste Online-Lernmethodik. Die Universität kombiniert die *Relearning*-Methode (die international am besten bewertete Lernmethode für Aufbaustudien) mit der Fallstudie. Tradition und Avantgarde in einem schwierigen Gleichgewicht und im Rahmen einer anspruchsvollen akademischen Laufbahn.



Skaleneffekt

TECH ist die größte Online-Universität der Welt. Sie verfügt über ein Portfolio von mehr als 10.000 Hochschulabschlüssen. Und in der neuen Wirtschaft gilt: **Volumen + Technologie = disruptiver Preis**. Damit stellt TECH sicher, dass das Studium nicht so kostspielig ist wie an anderen Universitäten.



Mit den Besten lernen

Das Lehrteam von TECH erklärt im Unterricht, was sie in ihren Unternehmen zum Erfolg geführt hat, und zwar in einem realen, lebendigen und dynamischen Kontext. Lehrkräfte, die sich voll und ganz dafür einsetzen, eine hochwertige Spezialisierung zu bieten, die es dem Studenten ermöglicht, in seiner Karriere voranzukommen und sich in der Geschäftswelt zu profilieren.

Lehrkräfte aus 20 verschiedenen Ländern.



Bei TECH werden Sie Zugang zu den präzisesten und aktuellsten Fallstudien im akademischen Bereich haben"

03

Warum unser Programm?

Die Teilnahme am TECH-Programm bedeutet eine Vervielfachung der Chancen auf beruflichen Erfolg im Bereich der höheren Unternehmensführung.

Es ist eine Herausforderung, die Anstrengung und Hingabe erfordert, aber die Tür zu einer vielversprechenden Zukunft öffnet. Der Student wird von den besten Lehrkräften und mit den flexibelsten und innovativsten Lehrmethoden unterrichtet.



“

Wir verfügen über das renommierteste Dozententeam und den umfassendsten Lehrplan auf dem Markt, so dass wir Ihnen eine Fortbildung auf höchstem akademischen Niveau bieten können"

Dieses Programm bietet eine Vielzahl von beruflichen und persönlichen Vorteilen, darunter die Folgenden:

01

Einen deutlichen Schub für die Karriere des Studenten

Mit einem Studium bei TECH wird der Student seine Zukunft selbst in die Hand nehmen und sein volles Potenzial entfalten können. Durch die Teilnahme an diesem Programm wird er die notwendigen Kompetenzen erwerben, um in kurzer Zeit eine positive Veränderung in seiner Karriere zu erreichen.

70% der Teilnehmer dieser Spezialisierung erreichen in weniger als 2 Jahren eine positive Veränderung in ihrer Karriere.

02

Entwicklung einer strategischen und globalen Vision des Unternehmens

TECH bietet einen detaillierten Überblick über das allgemeine Management, um zu verstehen, wie sich jede Entscheidung auf die verschiedenen Funktionsbereiche des Unternehmens auswirkt.

Die globale Vision des Unternehmens von TECH wird Ihre strategische Vision verbessern.

03

Konsolidierung des Studenten in der Unternehmensführung

Ein Studium an der TECH öffnet die Türen zu einem beruflichen Panorama von großer Bedeutung, so dass der Student sich als hochrangiger Manager mit einer umfassenden Vision des internationalen Umfelds positionieren kann.

Sie werden mehr als 100 reale Fälle aus dem Bereich der Unternehmensführung bearbeiten.

04

Übernahme neuer Verantwortung

Während des Programms werden die neuesten Trends, Entwicklungen und Strategien vorgestellt, damit der Student seine berufliche Tätigkeit in einem sich verändernden Umfeld ausüben kann.

45% der Studenten werden intern befördert.

05

Zugang zu einem leistungsfähigen Netzwerk von Kontakten

TECH vernetzt seine Studenten, um ihre Chancen zu maximieren. Studenten mit den gleichen Sorgen und dem Wunsch zu wachsen. So wird es möglich sein, Partner, Kunden oder Lieferanten zu teilen.

Sie werden ein Netz von Kontakten finden, das für Ihre berufliche Entwicklung unerlässlich ist.

06

Rigoreuse Entwicklung von Unternehmensprojekten

Der Student wird eine tiefgreifende strategische Vision erlangen, die ihm helfen wird, sein eigenes Projekt unter Berücksichtigung der verschiedenen Bereiche des Unternehmens zu entwickeln.

20% unserer Studenten entwickeln ihre eigene Geschäftsidee.

07

Verbesserung von *Soft Skills* und Führungsqualitäten

TECH hilft dem Studenten, sein erworbenes Wissen anzuwenden und weiterzuentwickeln und seine zwischenmenschlichen Fähigkeiten zu verbessern, um eine Führungspersönlichkeit zu werden, die etwas bewirkt.

Verbessern Sie Ihre Kommunikations- und Führungsfähigkeiten und geben Sie Ihrer Karriere einen neuen Impuls.

08

Teil einer exklusiven Gemeinschaft sein

Der Student wird Teil einer Gemeinschaft von Elite-Managern, großen Unternehmen, renommierten Institutionen und qualifizierten Professoren der renommiertesten Universitäten der Welt sein: die Gemeinschaft der TECH Technologischen Universität.

Wir bieten Ihnen die Möglichkeit, sich mit einem Team von international anerkannten Dozenten zu spezialisieren.

04 Ziele

Dieses Programm von TECH wurde entwickelt, um die beruflichen Fähigkeiten von Managern zu stärken. Neben der hohen Spezialisierung in ihrem Tätigkeitsbereich bietet dieser Studiengang eine einzigartige Gelegenheit, sich in einem sehr wichtigen Bereich zu verbessern, da sie lernen, möglichen Internetbedrohungen vorzubeugen, die Unternehmen ernsthaften Schaden zufügen können. Auf diese Weise werden sie zu professionellen Experten in verschiedenen Bereichen, so dass sie in der Lage sind, alle Bereiche des Unternehmens zu kontrollieren und somit Chief Information Security Officers zu werden.



“

Verbessern Sie Ihre Fähigkeiten und erreichen Sie Ihre Karriereziele dank der hervorragenden Weiterbildung, die Ihnen TECH mit diesem Programm bietet“

**TECH macht sich die Ziele ihrer Studenten zu eigen
Gemeinsam arbeiten sie daran, diese zu erreichen**

Der MBA in Cybersecurity Management (CISO, Chief Information Security Officer) wird den Studenten zu Folgendem befähigen:

01

Analysieren der Rolle des Cybersecurity-Analysten

02

Erforschen des *Social Engineering* und seiner Methoden

03

Untersuchen von OSINT, HUMINT, OWASP, OSSTM PTEC, OWISAM-Methoden

04

Durchführen einer Risikoanalyse und Verstehen von Risikokennzahlen

05

Bestimmen des angemessenen Einsatzes von Anonymität und der Nutzung von Netzwerken wie TOR, I2P und Freenet

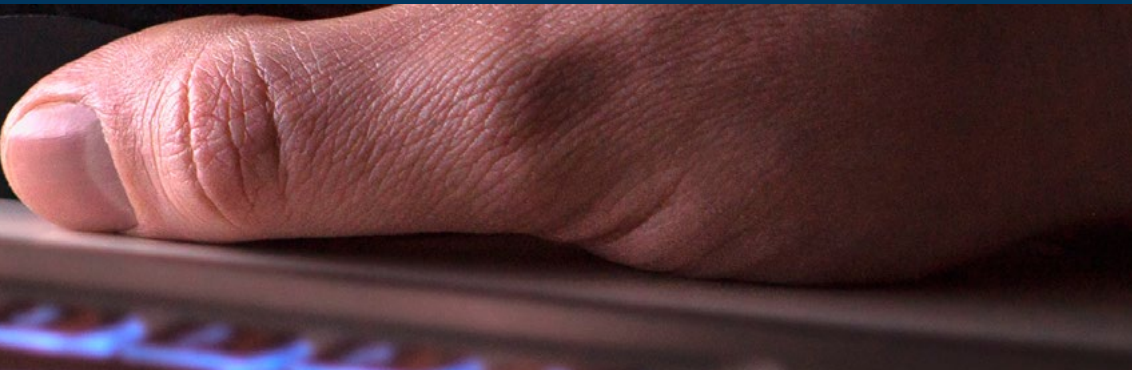


06

Zusammenstellen der aktuellen
Cybersicherheitsvorschriften

08

Entwickeln geeigneter Nutzungsrichtlinien



07

Generieren von Fachwissen zur Durchführung eines
Sicherheitsaudits

09

Entwickeln von Firewall-Lösungen auf Linux-Hosts
und bei Cloud-Anbietern

10

Bewerten von neuen Systemen zur Erkennung
von Bedrohungen und deren Weiterentwicklung
gegenüber herkömmlichen Lösungen

11

Analysieren der wichtigsten aktuellen mobilen Plattformen, ihrer Funktionen und Nutzung

12

Identifizieren, Analysieren und Bewerten der Sicherheitsrisiken von IoT-Projektteilen

13

Auswerten der erhaltenen Informationen und Entwickeln von Präventions- und Hacking-Mechanismen

14

Anwenden von *Reverse Engineering* auf die Cybersicherheitsumgebung

15

Spezifizieren der Tests, die mit der entwickelten Software durchgeführt werden sollen



16

Sammeln aller vorhandenen Beweise und Daten, um einen forensischen Bericht zu erstellen

18

Analysieren des aktuellen und zukünftigen Stands der IT-Sicherheit

19

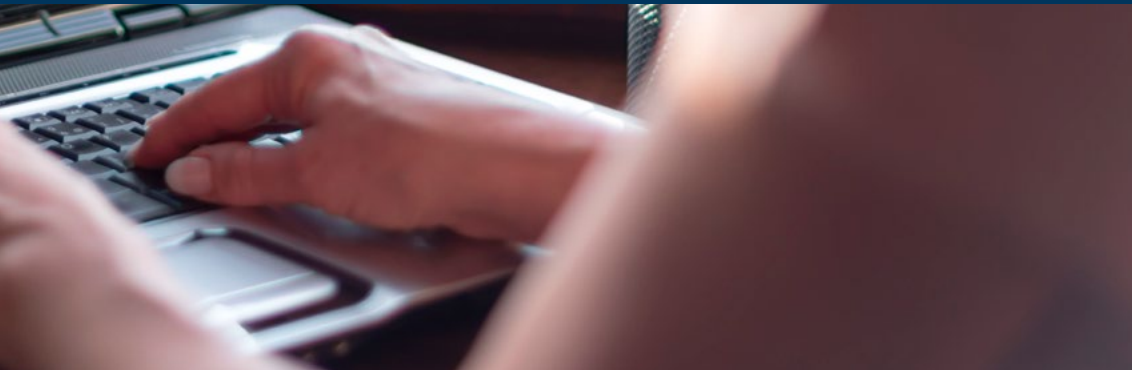
Untersuchen der Risiken neu aufkommender Technologien

17

Korrektes Präsentieren des forensischen Berichts

20

Zusammenstellen der verschiedenen Technologien in Bezug auf die Computersicherheit



05

Kompetenzen

Der MBA in Cybersecurity Management (CISO, Chief Information Security Officer) wurde entwickelt, um die Wettbewerbsfähigkeit von Fachleuten in der Wirtschaft zu verbessern. Daher werden die Studenten am Ende ihres Studiums die notwendigen Kompetenzen erworben haben, um eine qualitativ hochwertige und aktuelle Praxis basierend auf der innovativsten Lehrmethodik auszuüben. Zweifellos ein Programm, das ihre Qualifikation verbessert und es ihnen ermöglicht, in ihrer täglichen Praxis wettbewerbsfähiger zu sein, indem es alle relevanten Aspekte der IT-Sicherheit vereint, die Manager kennen und in die Praxis umsetzen müssen.





“

*Beschäftigen Sie sich mit dem Thema
Computersicherheit und verbessern
Sie Ihre Fähigkeiten, um potenzielle
Netzwerkbedrohungen zu kontrollieren"*

01

Kennen der Methoden, die im Bereich der Cybersicherheit verwendet werden

02

Bewerten jeder Art von Bedrohung, um eine optimale Lösung für jeden Fall zu finden

03

Erstellen von intelligenten Komplettlösungen zur Automatisierung des Verhaltens bei Zwischenfällen

04

Bewerten der Risiken im Zusammenhang mit Schwachstellen außerhalb und innerhalb des Unternehmens



05

Verstehen der Entwicklung und der Auswirkungen des IoT im Laufe der Zeit

06

Nachweisen, dass ein System verwundbar ist, es zu Präventionszwecken angreifen und solche Probleme lösen können

07

Wissen, wie man *Sandboxing* in verschiedenen Umgebungen anwendet

08

Kennen der Richtlinien, die ein guter Entwickler befolgen muss, um die notwendige Sicherheit zu gewährleisten



09

Durchführen von defensiven Sicherheitsmaßnahmen

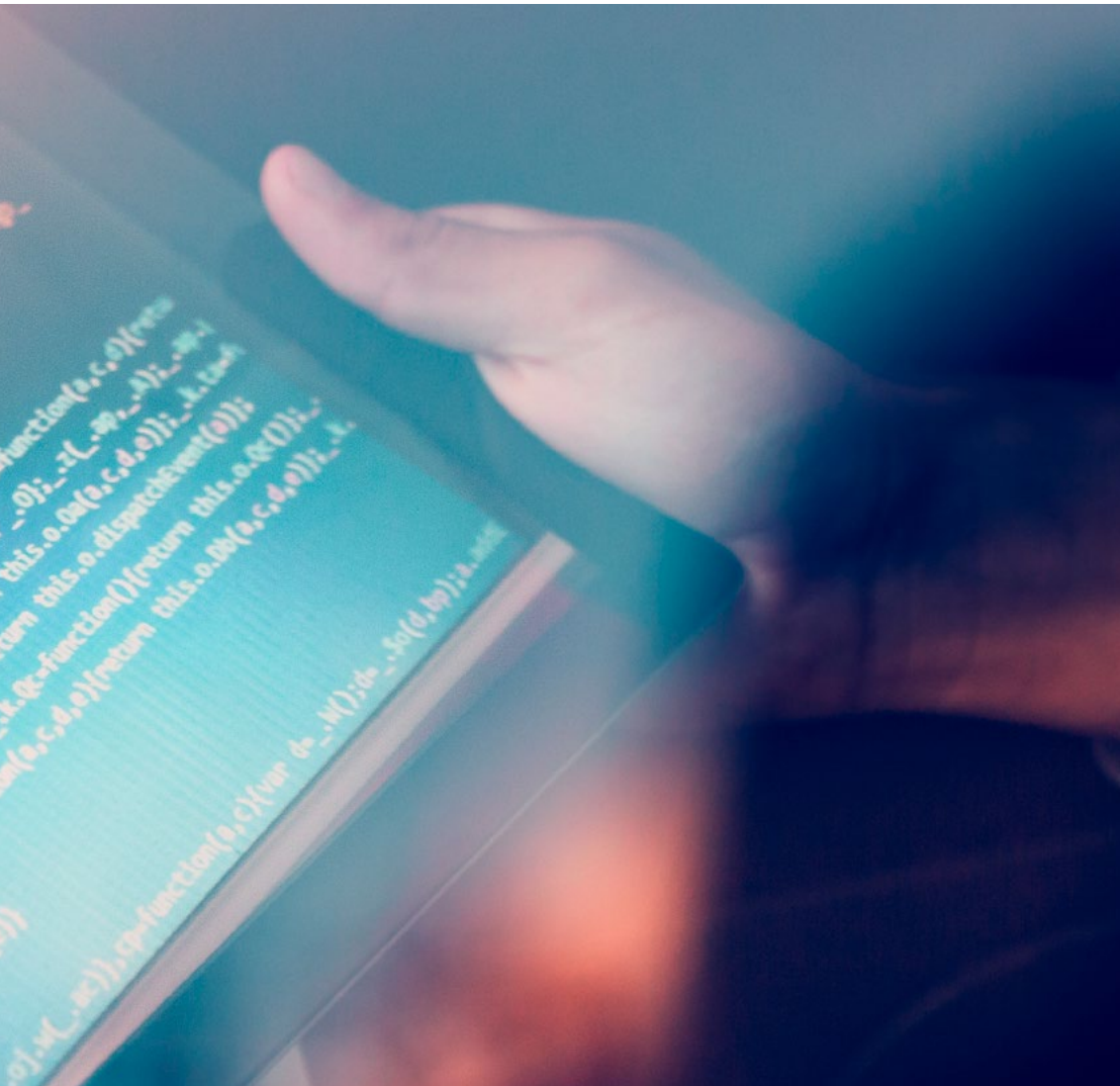
10

Verfügen über ein tiefgehendes und spezialisiertes Verständnis von Cybersicherheit

11

Implementieren von Sicherheitsprozessen für Smartphones und Handheld-Geräte





12

Kennen der Mittel zur Durchführung des so genannten ethischen *Hacking* und zum Schutz eines Unternehmens vor einem Cyberangriff

13

In der Lage sein, einen Cybersicherheitsvorfall zu untersuchen

14

Unterscheiden der verschiedenen verfügbaren Angriffs- und Verteidigungstechniken

06

Struktur und Inhalt

Dieses Programm der TECH wurde entwickelt, um die Spezialisierungsbedürfnisse von Geschäftsleuten zu befriedigen, die ihre Kenntnisse im Bereich der IT-Sicherheit erweitern möchten. Dies ist ein grundlegender Bereich, um potenzielle Bedrohungen, die ein großes Risiko für das Unternehmen darstellen können, kontrollieren zu können. Auf diese Weise werden sie durch den MBA spezifische Kenntnisse erwerben, die sie in ihrer beruflichen Praxis anwenden können. Dabei werden sie eine reine Online-Methode anwenden, die es ihnen ermöglicht, ihr Studium mit ihren übrigen täglichen Verpflichtungen zu verbinden.



“

Dieses Programm ist unverzichtbar, um mögliche Cyberangriffe in Ihrem Unternehmen aufzudecken“

Lehrplan

Der MBA in Cybersecurity Management (Chief Information Security Officer) der TECH Technologische Universität ist ein intensives Programm, das darauf ausgerichtet ist, die Entwicklung von Managementfähigkeiten zu fördern, die eine präzisere Entscheidungsfindung in unsicheren Umgebungen ermöglichen.

In 2.700 Unterrichtsstunden werden die Studenten die notwendigen Fähigkeiten erwerben, um sich in ihrer täglichen Praxis erfolgreich zu entwickeln. Es ist also ein echtes Eintauchen in reale Geschäftssituationen.

Dieses Programm befasst sich eingehend mit verschiedenen Bereichen des Unternehmens und soll Führungskräften die Cybersicherheit aus einer strategischen, internationalen und innovativen Perspektive vermitteln.

Ein speziell für die Studenten konzipierter Plan, der auf ihre berufliche Weiterentwicklung ausgerichtet ist und sie darauf vorbereitet, hervorragende Leistungen im Bereich des IT-

Sicherheitsmanagements zu erbringen. Ein Programm, das ihre Bedürfnisse und die ihres Unternehmens durch innovative, auf den neuesten Trends basierende Inhalte versteht und durch die beste Lehrmethodik und einen außergewöhnlichen Lehrkörper unterstützt wird.

Hinzu kommen 10 exklusive Masterclasses, die Teil des didaktischen Materials sind und an der Spitze von Technologie und Bildung stehen. Diese Lektionen wurden von einem international anerkannten Spezialisten für Intelligenz, Cybersicherheit und disruptive Technologien entwickelt. Nützliche Ressourcen, die der Führungskraft helfen, sich auf das Management der Cybersicherheit zu spezialisieren und die Abteilungen ihres Unternehmens, die sich diesem wichtigen Bereich widmen, effizient zu verwalten.

Das Programm erstreckt sich über 12 Monate und ist in 15 Module unterteilt:

Modul 1	Cyberintelligenz und Cybersicherheit
Modul 2	Host-Sicherheit
Modul 3	Netzwerksicherheit (Perimeter)
Modul 4	Smartphone-Sicherheit
Modul 5	IoT-Sicherheit
Modul 6	Ethisches <i>Hacking</i>
Modul 7	<i>Reverse Engineering</i>
Modul 8	Sichere Entwicklung
Modul 9	Forensische Analyse
Modul 10	Aktuelle und zukünftige Herausforderungen in der IT-Sicherheit
Modul 11	Führung, Ethik und soziale Verantwortung der Unternehmen
Modul 12	<i>Personal- und Talentmanagement</i>
Modul 13	<i>Wirtschaftlich-finanzielle Verwaltung</i>
Modul 14	<i>Kaufmännisches Management und strategisches Marketing</i>
Modul 15	Geschäftsleitung



Wo, wann und wie wird unterrichtet?

TECH bietet den Studenten die Möglichkeit, dieses Programm vollständig online zu absolvieren. Während dieser 12-monatigen Spezialisierung können sie jederzeit auf alle Inhalte dieses Programms zugreifen, so dass sie ihre Studienzzeit selbst verwalten können.

Eine einzigartige, wichtige und entscheidende Bildungserfahrung, um Ihre berufliche Entwicklung voranzutreiben und den endgültigen Sprung zu schaffen.

Modul 1. Cyberintelligenz und Cybersicherheit

1.1. Cyberintelligenz

- 1.1.1. Cyberintelligenz
 - 1.1.1.1. Die Intelligenz
 - 1.1.1.1.1. Intelligenz-Zyklus
 - 1.1.1.2. Cyberintelligenz
 - 1.1.1.3. Cyberintelligenz und Cybersicherheit
- 1.1.2. Der Informationsanalyst
 - 1.1.2.1. Die Rolle des Informationsanalysten
 - 1.1.2.2. Voreingenommenheit des Informationsanalysten bei der Bewertung von Aktivitäten

1.2. Cybersicherheit

- 1.2.1. Schichten der Sicherheit
- 1.2.2. Identifizierung von Cyber-Bedrohungen
 - 1.2.2.1. Externe Bedrohungen
 - 1.2.2.2. Interne Bedrohungen
- 1.2.3. Nachteilige Maßnahmen
 - 1.2.3.1. *Social Engineering*
 - 1.2.3.2. Häufig verwendete Methoden

1.3. Intelligente Tools und Techniken

- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. HUMIT
- 1.3.4. Linux-Distributionen und -Tools
- 1.3.5. OWISAM
- 1.3.6. OWISAP
- 1.3.7. PTES
- 1.3.8. OSSTM

1.4. Methoden der Bewertung

- 1.4.1. Informationsanalyse
- 1.4.2. Techniken zur Organisation der erworbenen Informationen
- 1.4.3. Verlässlichkeit und Glaubwürdigkeit von Informationsquellen
- 1.4.4. Methodologien der Analyse
- 1.4.5. Präsentation der Informationsanalyse

1.5. Audits und Dokumentation

- 1.5.1. Das IT-Sicherheitsaudit
- 1.5.2. Dokumentation und Berechtigungen für Audits
- 1.5.3. Arten von Audits
- 1.5.4. Lieferbare
 - 1.5.4.1. Technischer Bericht
 - 1.5.4.2. Bericht für die Geschäftsführung

1.6. Anonymität im Netz

- 1.6.1. Nutzung der Anonymität
- 1.6.2. Anonymisierungstechniken (Proxy, VPN)
- 1.6.3. TOR, Freenet und IP2-Netzwerke

1.7. Bedrohungen und Arten von Sicherheit

- 1.7.1. Arten von Bedrohungen
- 1.7.2. Physische Sicherheit
- 1.7.3. Netzwerksicherheit
- 1.7.4. Logische Sicherheit
- 1.7.5. Sicherheit von Webanwendungen
- 1.7.6. Sicherheit für mobile Geräte

1.8. Regulierung und Compliance

- 1.8.1. Datenschutz-Grundverordnung
- 1.8.2. Die nationale Cybersicherheitsstrategie 2019
- 1.8.3. ISO 27000-Familie
- 1.8.4. NIST Cybersecurity Framework
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. *Cloud*-Standards
- 1.8.8. SOX
- 1.8.9. ICP

1.9. Risikoanalyse und Metriken

- 1.9.1. Umfang der Risiken
- 1.9.2. Vermögenswerte
- 1.9.3. Bedrohungen
- 1.9.4. Schwachstellen
- 1.9.5. Risikobewertung
- 1.9.6. Risikobehandlung

1.10. Einschlägige Stellen für Cybersicherheit

- 1.10.1. NIST
- 1.10.2. ENISA
- 1.10.3. INCIBE
- 1.10.4. OEA
- 1.10.5. UNASUR-PROSUR

Modul 2. Host-Sicherheit

2.1. Sicherheitskopien

- 2.1.1. Strategien zur Datensicherung
- 2.1.2. Tools für Windows
- 2.1.3. Tools für Linux
- 2.1.4. Tools für MacOS

2.2. Benutzer-Antivirus

- 2.2.1. Arten von Antivirenprogrammen
- 2.2.2. Antivirus für Windows
- 2.2.3. Antivirus für Linux
- 2.2.4. Antivirus für MacOS
- 2.2.5. Antivirus für Smartphones

2.3. HIDS-Eindringlingsdetektoren

- 2.3.1. Methoden zur Erkennung von Eindringlingen
- 2.3.2. Sagan
- 2.3.3. Aide
- 2.3.4. Rkhunter

2.4. Lokale Firewall

- 2.4.1. *Firewalls* für Windows
- 2.4.2. *Firewalls* für Linux
- 2.4.3. *Firewalls* für MacOS

2.5. Passwortmanager

- 2.5.1. Password
- 2.5.2. LastPass
- 2.5.3. KeePass
- 2.5.4. StickyPassword
- 2.5.5. RoboForm

2.6. Phishing-Detektoren

- 2.6.1. Manuelle *Phishing*-Erkennung
- 2.6.2. *Anti-Phishing*-Tools

2.7. Spyware

- 2.7.1. Vermeidungsmechanismen
- 2.7.2. *Anti-Spyware*-Tools

2.8. Tracker

- 2.8.1. Maßnahmen zum Schutz des Systems
- 2.8.2. *Anti-Tracker*-Tools

2.9. EDR - End Point Detection and Response

- 2.9.1. Verhalten des EDR-Systems
- 2.9.2. Unterschiede zwischen EDR und Anti-Virus
- 2.9.3. Die Zukunft der EDR-Systeme

2.10. Kontrolle über die Software-Installation

- 2.10.1. Repositorien und Software-Speicher
- 2.10.2. Listen mit erlaubter oder verbotener Software
- 2.10.3. Update-Kriterien
- 2.10.4. Berechtigungen für die Software-Installation

Modul 3. Netzwerksicherheit (Perimeter)

3.1. Systeme zur Erkennung und Abwehr von Bedrohungen

- 3.1.1. Allgemeiner Rahmen für Sicherheitsvorfälle
- 3.1.2. Aktuelle Verteidigungssysteme: *Defense in Depth* und SOC
- 3.1.3. Aktuelle Netzwerkarchitekturen
- 3.1.4. Arten von Tools zur Erkennung und Verhinderung von Vorfällen
 - 3.1.4.1. Netzwerkbasierte Systeme
 - 3.1.4.2. Host-basierte Systeme
 - 3.1.4.3. Zentralisierte Systeme
- 3.1.5. Kommunikation und Erkennung von Instanzen/ Hosts, Containern und Serverless

3.2. Firewall

- 3.2.1. Arten von *Firewalls*
- 3.2.2. Angriffe und Schadensbegrenzung
- 3.2.3. Gängige *Firewalls* in *Kernel Linux*
 - 3.2.3.1. UFW
 - 3.2.3.2. *Nftables* und *iptables*
 - 3.2.3.3. FirewallD
- 3.2.4. Erkennungssysteme auf der Grundlage von Systemlogs
 - 3.2.4.1. TCP Wrappers
 - 3.2.4.2. BlockHosts und DenyHosts
 - 3.2.4.3. Fail2ban

3.3. Systeme zur Erkennung und Verhinderung von Eindringlingen (IDS/IPS)

- 3.3.1. Angriffe auf IDS/IPS
- 3.3.2. IDS/IPS-Systeme
 - 3.3.2.1. Snort
 - 3.3.2.2. Suricata

3.4. Firewalls der nächsten Generation (NGFW)

- 3.4.1. Unterschiede zwischen NGFW und traditionellen *Firewalls*
- 3.4.2. Kernkapazitäten
- 3.4.3. Business-Lösungen
- 3.4.4. *Firewalls* für *Cloud*-Dienste
 - 3.4.4.1. Cloud-VPC-Architektur
 - 3.4.4.2. Cloud ACLs
 - 3.4.4.3. Security Group

3.5. Proxy

- 3.5.1. Arten von *Proxys*
- 3.5.2. *Proxy*-Nutzung, Vor- und Nachteile

3.6. Antivirus-Engines

- 3.6.1. Allgemeiner Kontext von *Malware* und IOCS
- 3.6.2. Probleme mit Anti-Viren-Programmen

3.7. Mailschutzsysteme

- 3.7.1. Antispam
 - 3.7.1.1. *Whitelisting* und *Blacklisting*
 - 3.7.1.2. Bayessche Filter
- 3.7.2. *Mail Gateway* (MGW)

3.8. SIEM

- 3.8.1. Komponenten und Architektur
- 3.8.2. Korrelationsregeln und Anwendungsfälle
- 3.8.3. Aktuelle Herausforderungen von SIEM-Systemen

3.9. SOAR

- 3.9.1. SOAR und SIEM: Feinde oder Verbündete?
- 3.9.2. Die Zukunft der SOAR-Systeme

3.10. Andere netzwerkbasierende Systeme

- 3.10.1. WAF
- 3.10.2. NAC
- 3.10.3. *HoneyPots* und *HoneyNets*
- 3.10.4. CASB

Modul 4. Smartphone-Sicherheit

4.1. Die Welt der mobilen Geräte

- 4.1.1. Arten von mobilen Plattformen
- 4.1.2. IOS-Geräte
- 4.1.3. Android-Geräte

4.2. Verwaltung der mobilen Sicherheit

- 4.2.1. OWASP-Projekt für mobile Sicherheit
 - 4.2.1.1. Top 10 Schwachstellen
- 4.2.2. Kommunikation, Netzwerke und Verbindungsarten

4.3. Das mobile Gerät in der Unternehmensumgebung

- 4.3.1. Risiken
- 4.3.2. Sicherheitsrichtlinien
- 4.3.3. Geräteüberwachung
- 4.3.4. Verwaltung mobiler Geräte (MDM)

4.4. Datenschutz und Datensicherheit

- 4.4.1. Informationsstände
- 4.4.2. Datenschutz und Vertraulichkeit
 - 4.4.2.1. Zugriffsrechte
 - 4.4.2.2. Verschlüsselung
- 4.4.3. Sichere Speicherung von Daten
 - 4.4.3.1. Sichere Speicherung auf iOS
 - 4.4.3.2. Sichere Speicherung auf Android
- 4.4.4. Bewährte Praktiken bei der Applikationsentwicklung

4.5. Schwachstellen und Angriffsvektoren

- 4.5.1. Schwachstellen
- 4.5.2. Angriffsvektoren
 - 4.5.2.1. *Malware*
 - 4.5.2.2. Exfiltration von Daten
 - 4.5.2.3. Datenmanipulation

4.6. Wichtigste Bedrohungen

- 4.6.1. Ungezwungener Benutzer
- 4.6.2. *Malware*
 - 4.6.2.1. Arten von *Malware*
- 4.6.3. *Social Engineering*
 - 4.6.4. Datenleck
 - 4.6.5. Datendiebstahl

- 4.6.6. Ungesicherte WLAN-Netzwerke
- 4.6.7. Veraltete Software
- 4.6.8. Bösartige Anwendungen
- 4.6.9. Unsichere Passwörter
- 4.6.10. Schwache oder nicht vorhandene Sicherheitseinstellungen

- 4.6.11. Physischer Zugang
- 4.6.12. Verlust oder Diebstahl des Geräts
- 4.6.13. Impersonation (Integrität)
- 4.6.14. Schwache oder defekte Kryptographie
- 4.6.15. *Denial of Service* (DoS)

4.7. Große Angriffe

- 4.7.1. *Phishing*-Angriffe
- 4.7.2. Angriffe im Zusammenhang mit Kommunikationsmodi
- 4.7.3. *Smishing*-Angriffe
- 4.7.4. *Cryptojacking*-Angriffe
- 4.7.5. *Man in The Middle*

4.8. Hacking

- 4.8.1. *Rooting* und *Jailbreaking*
- 4.8.2. Anatomie eines mobilen Angriffs
 - 4.8.2.1. Ausbreitung der Bedrohung
 - 4.8.2.2. Installation von *Malware* auf dem Gerät
 - 4.8.2.3. Persistenz
 - 4.8.2.4. Ausführen der *Payload* und Extrahieren der Informationen
- 4.8.3. *Hacking* auf iOS-Geräten: Mechanismen und Tools
- 4.8.4. *Hacking* auf Android-Geräten: Mechanismen und Tools

4.9. Penetrationstests

- 4.9.1. iOS *Pentesting*
- 4.9.2. Android *PenTesting*
- 4.9.3. Hilfsmittel

4.10. Schutz und Sicherheit

- 4.10.1. Sicherheitseinstellungen
 - 4.10.1.1. Auf iOS-Geräten
 - 4.10.1.2. Auf Android-Geräten
- 4.10.2. Sicherheitsmaßnahmen
- 4.10.3. Schutz-Tools

Modul 5. IoT-Sicherheit

5.1. Geräte

- 5.1.1. Arten von Geräten
- 5.1.2. Standardisierte Architekturen
 - 5.1.2.1. ONEM2M
 - 5.1.2.2. IoTWF
- 5.1.3. Anwendungsprotokolle
- 5.1.4. Konnektivitätstechnologien

5.2. IoT-Geräte. Anwendungsbereiche

- 5.2.1. *SmartHome*
- 5.2.2. *SmartCity*
- 5.2.3. Transport
- 5.2.4. *Wearables*
- 5.2.5. Gesundheitssektor
- 5.2.6. IIoT

5.3. Kommunikationsprotokolle

- 5.3.1. MQTT
- 5.3.2. LWM2M
- 5.3.3. OMA-DM
- 5.3.4. TR-069

5.4. *SmartHome*

- 5.4.1. Hausautomatisierung
- 5.4.2. Netzwerke
- 5.4.3. Haushaltsgeräte
- 5.4.4. Überwachung und Sicherheit

5.5. *SmartCity*

- 5.5.1. Beleuchtung
- 5.5.2. Meteorologie
- 5.5.3. Sicherheit

5.6. Transport

- 5.6.1. Standort
- 5.6.2. Zahlungen leisten und Dienstleistungen in Anspruch nehmen
- 5.6.3. Konnektivität

5.7. *Wearables*

- 5.7.1. Intelligente Kleidung
- 5.7.2. Intelligenter Schmuck
- 5.7.3. Intelligente Uhren

5.8. Gesundheitssektor

- 5.8.1. Training/Herzfrequenzüberwachung
- 5.8.2. Überwachung von Patienten und älteren Menschen
- 5.8.3. Implantierbare Geräte
- 5.8.4. Chirurgische Roboter

5.9. Konnektivität

- 5.9.1. WLAN/Gateway
- 5.9.2. Bluetooth
- 5.9.3. Eingebettete Konnektivität

5.10. Sicherung

- 5.10.1. Dedizierte Netzwerke
- 5.10.2. Passwortmanager
- 5.10.3. Verwendung von verschlüsselten Protokollen
- 5.10.4. Tipps für die Verwendung

Modul 6. Ethisches Hacking
6.1. Arbeitsumgebung

- 6.1.1. Linux-Distributionen
 - 6.1.1.1. Kali Linux - Offensive Security
 - 6.1.1.2. Parrot OS
 - 6.1.1.3. Ubuntu
- 6.1.2. Virtualisierungssysteme
- 6.1.3. *Sandbox*
- 6.1.4. Einsatz von Labors

6.2. Methoden

- 6.2.1. OSSTM
- 6.2.2. OWASP
- 6.2.3. NIST
- 6.2.4. PTES
- 6.2.5. ISSAF

6.3. Footprinting

- 6.3.1. *Open Source Intelligence* (OSINT)
- 6.3.2. Suche nach Datenschutzverletzungen und Schwachstellen
- 6.3.3. Verwendung von passiven Tools

6.4. Netzwerk-Scans

- 6.4.1. Tools zum Scannen
 - 6.4.1.1. Nmap
 - 6.4.1.2. Hping3
 - 6.4.1.3. Andere Scan-Tools
- 6.4.2. Scanning-Techniken
- 6.4.3. Techniken zur Umgehung von *Firewalls* und IDS
- 6.4.4. *Banner Grabbing*
- 6.4.5. Netzwerk-Diagramme

6.5. Aufzählung

- 6.5.1. SMTP-Aufzählung
- 6.5.2. DNS-Aufzählung
- 6.5.3. NetBIOS- und Samba-Aufzählung
- 6.5.4. LDAP-Aufzählung
- 6.5.5. SNMP-Aufzählung
- 6.5.6. Andere Aufzählungstechniken

6.6. Scannen auf Schwachstellen

- 6.6.1. Lösungen zum Scannen auf Schwachstellen
 - 6.6.1.1. Qualys
 - 6.6.1.2. Nessus
 - 6.6.1.3. CFI LanGuard
- 6.6.2. Systeme zur Bewertung von Schwachstellen
 - 6.6.2.1. CVSS
 - 6.6.2.2. CVE
 - 6.6.2.3. NVD

6.7. Angriffe auf drahtlose Netzwerke

- 6.7.1. Methodik zum Hacken drahtloser Netzwerke
 - 6.7.1.1. WLAN *Discovery*
 - 6.7.1.2. Verkehrsanalyse
 - 6.7.1.3. *Aircrack*-Angriffe
 - 6.7.1.3.1. WEP-Angriffe
 - 6.7.1.3.2. WPA/WPA2-Angriffe
 - 6.7.1.4. *Evi-Twin*-Angriffe
 - 6.7.1.5. WPS-Angriffe
 - 6.7.1.6. *Jamming*
- 6.7.2. Tools für drahtlose Sicherheit

6.8. Hacking von Webservern

- 6.8.1. *Cross Site Scripting*
- 6.8.2. CSRF
- 6.8.3. *Session Hijacking*
- 6.8.4. *SQLinjection*

6.9. Ausnutzung von Schwachstellen

- 6.9.1. Verwendung von bekannten *Exploits*
- 6.9.2. Verwendung von *Metasploit*
- 6.9.3. Verwendung von *Malware*
 - 6.9.3.1. Definition und Umfang
 - 6.9.3.2. Generierung von *Malware*
 - 6.9.3.3. Umgehung von Anti-Virus-Lösungen

6.10. Persistenz

- 6.10.1. Installation von *Rootkits*
- 6.10.2. Verwendung von Ncat
- 6.10.3. Verwendung von geplanten Aufgaben für *Backdoors*
- 6.10.4. Benutzer erstellen
- 6.10.5. HIDS aufspüre

Modul 7. Reverse Engineering

7.1. Compiler

- 7.1.1. Arten von Code
- 7.1.2. Compiler-Phasen
- 7.1.3. Symboltabelle
- 7.1.4. Fehler-Handler
- 7.1.5. GCC Compiler

7.2. Arten der Compiler-Analyse

- 7.2.1. Lexikalische Analyse
 - 7.2.1.1. Terminologie
 - 7.2.1.2. Lexikalische Komponenten
 - 7.2.1.3. LEX. Lexikalischer Analysator

7.2.2. Syntaktische Analyse

- 7.2.2.1. Kontextfreie Grammatiken
- 7.2.2.2. Arten des Parsing
 - 7.2.2.2.1. Top-down-Parsing
 - 7.2.2.2.2. Bottom-up-Parsing

7.2.2.3. Syntaktische Bäume und Ableitungen

- 7.2.2.4. Arten von Parsern
 - 7.2.2.4.1. LR-Parser (*Left to Right*)
 - 7.2.2.4.2. LALR-Parser

7.2.3. Semantische Analyse

- 7.2.3.1. Attribut-Grammatiken
- 7.2.3.2. S-Attribute
- 7.2.3.3. L-Attribute

7.3. Montage-Datenstrukturen

- 7.3.1. Variablen
- 7.3.2. Arrays
- 7.3.3. Zeiger
- 7.3.4. Strukturen
- 7.3.5. Objekte

7.4. Assembly-Code-Strukturen

- 7.4.1. Auswahl-Strukturen
 - 7.4.1.1. *If, else if, Else*
 - 7.4.1.2. *Switch*
- 7.4.2. Iterations-Strukturen
 - 7.4.2.1. *For*
 - 7.4.2.2. *While*
 - 7.4.2.3. Verwendung des *Break*
- 7.4.3. Funktionen

7.5. x86-Hardware-Architektur

- 7.5.1. x86-Prozessorarchitektur
- 7.5.2. x86-Datenstrukturen
- 7.5.3. x86-Codestrukturen

7.6. ARM-Hardwarearchitektur

- 7.6.1. ARM-Prozessorarchitektur
- 7.6.2. ARM-Datenstrukturen
- 7.6.3. ARM-Codestrukturen

7.7. Statische Codeanalyse

- 7.7.1. Disassembler
- 7.7.2. IDA
- 7.7.3. Code-Rekonstrukteure

7.8. Dynamische Codeanalyse

- 7.8.1. Verhaltensanalyse
 - 7.8.1.1. Kommunikation
 - 7.8.1.2. Überwachung
- 7.8.2. Linux-Code-Debugger
- 7.8.3. Windows-Code-Debugger

7.9. Sandbox

- 7.9.1. *Sandbox*-Architektur
- 7.9.2. *Sandbox*-Umgehung
- 7.9.3. Erkennungstechniken
- 7.9.4. Ausweichtechniken
- 7.9.5. Gegenmaßnahmen
- 7.9.6. *Sandbox* in Linux
- 7.9.7. *Sandbox* in Windows
- 7.9.8. *Sandbox* in MacOS
- 7.9.9. *Sandbox* in Android

7.10. Malware-Scans

- 7.10.1. Methoden zur Analyse des *Malware*
- 7.10.2. Techniken zur Verschleierung von *Malware*
 - 7.10.2.1. Ausführbare Verschleierung
 - 7.10.2.2. Einschränkung der Ausführungsumgebungen
- 7.10.3. Tools zur Analyse des *Malware*

Modul 8. Sichere Entwicklung**8.1. Sichere Entwicklung**

- 8.1.1. Qualität, Funktionalität und Sicherheit
- 8.1.2. Vertraulichkeit, Integrität und Verfügbarkeit
- 8.1.3. Lebenszyklus der Softwareentwicklung

8.2. Phase der Anforderungen

- 8.2.1. Kontrolle der Authentifizierung
- 8.2.2. Kontrolle von Rollen und Privilegien
- 8.2.3. Risikoorientierte Anforderungen
- 8.2.4. Genehmigung von Privilegien

8.3. Analyse- und Entwurfsphasen

- 8.3.1. Komponentenzugriff und Systemverwaltung
- 8.3.2. Prüfpfade
- 8.3.3. Sitzungsmanagement
- 8.3.4. Historische Daten
- 8.3.5. Angemessene Fehlerbehandlung
- 8.3.6. Trennung der Funktionen

8.4. Phase der Implementierung und Kodierung

- 8.4.1. Absicherung der Entwicklungsumgebung
- 8.4.2. Ausarbeitung der technischen Dokumentation
- 8.4.3. Sichere Kodierung
- 8.4.4. Sicherheit der Kommunikation

8.5. Gute sichere Kodierungspraktiken

- 8.5.1. Validierung von Eingabedaten
- 8.5.2. Verschlüsselung der Ausgabedaten
- 8.5.3. Programmierstil
- 8.5.4. Handhabung des Änderungsprotokolls
- 8.5.5. Kryptographische Praktiken
- 8.5.6. Fehler- und Protokollverwaltung
- 8.5.7. Dateiverwaltung
- 8.5.8. Speicherverwaltung
- 8.5.9. Standardisierung und Wiederverwendung von Sicherheitsfunktionen

8.6. Vorbereitung und *Hardening* von Servern

- 8.6.1. Verwaltung von Benutzern, Gruppen und Rollen auf dem Server
- 8.6.2. Software-Installation
- 8.6.3. *Hardening* des Servers
- 8.6.4. Robuste Konfiguration der Anwendungsumgebung

8.7. DB-Vorbereitung und *Hardening*

- 8.7.1. Optimierung der DB-Engine
- 8.7.2. Erstellung eines eigenen Benutzers für die Anwendung
- 8.7.3. Zuweisung der erforderlichen Berechtigungen an den Benutzer
- 8.7.4. *Hardening* der DB

8.8. Testphase

- 8.8.1. Qualitätskontrolle bei Sicherheitskontrollen
- 8.8.2. Stufenweise Code-Inspektion
- 8.8.3. Überprüfung der Konfigurationsverwaltung
- 8.8.4. Black-Box-Tests

8.9. Vorbereitungen für den Übergang zur Produktion

- 8.9.1. Änderungskontrolle durchführen
- 8.9.2. Durchführen der Produktionsumstellung
- 8.9.3. *Rollback*-Prozedur durchführen
- 8.9.4. Tests in der Vorproduktionsphase

8.10. Erhaltungsphase

- 8.10.1. Risikobasierte Versicherung
- 8.10.2. White-Box-Tests zur Wartung der Sicherheit
- 8.10.3. Black-Box-Tests zur Wartung der Sicherheit

Modul 9. Forensische Analyse

9.1. Datenerfassung und Replikation

- 9.1.1. Volatile Datenerfassung
 - 9.1.1.1. System-Informationen
 - 9.1.1.2. Netzwerk-Informationen
 - 9.1.1.3. Reihenfolge der Volatilität
- 9.1.2. Statische Datenerfassung
 - 9.1.2.1. Erstellung eines doppelten Bildes
 - 9.1.2.2. Erstellung eines Dokuments für die Überwachungskette
- 9.1.3. Methoden zur Validierung der erfassten Daten
 - 9.1.3.1. Methoden für Linux
 - 9.1.3.2. Methoden für Windows

9.2. Bewertung und Beseitigung von Anti-Forensik-Techniken

- 9.2.1. Ziele der Anti-Forensik-Techniken
- 9.2.2. Löschung von Daten
 - 9.2.2.1. Löschung von Daten und Dateien
 - 9.2.2.2. Dateiwiederherstellung
 - 9.2.2.3. Wiederherstellung von gelöschten Partitionen
- 9.2.3. Passwortschutz
- 9.2.4. Steganographie
- 9.2.5. Sicheres Löschen von Geräten
- 9.2.6. Verschlüsselung

9.3. Betriebssystem-Forensik

- 9.3.1. Windows-Forensik
- 9.3.2. Linux-Forensik
- 9.3.3. Mac-Forensik

9.4. Netzwerk-Forensik

- 9.4.1. Log-Analyse
- 9.4.2. Korrelation der Daten
- 9.4.3. Netzwerk-Untersuchung
- 9.4.4. Schritte der forensischen Netzwerkanalyse

9.5. Web-Forensik

- 9.5.1. Untersuchung von Webangriffen
- 9.5.2. Angriffserkennung
- 9.5.3. Standort der IP-Adresse

9.6. Datenbank-Forensik

- 9.6.1. MSSQL-Forensik
- 9.6.2. MySQL-Forensik
- 9.6.3. PostgreSQL-Forensik
- 9.6.4. MongoDB-Forensik

9.7. Cloud-Forensik

- 9.7.1. Arten von *Cloud*-Verbrechen
 - 9.7.1.1. *Cloud* als Thema
 - 9.7.1.2. *Cloud* als Objekt
 - 9.7.1.3. *Cloud* als Werkzeug
- 9.7.2. Herausforderungen der *Cloud*-Forensik
- 9.7.3. Untersuchung von *Cloud*-Speicherdiensten
- 9.7.4. Forensische Analyse-Tools für die *Cloud*

9.8. Untersuchung von E-Mail-Verbrechen

- 9.8.1. Mail-Systeme
 - 9.8.1.1. *Mail Clients*
 - 9.8.1.2. Mail-Server
 - 9.8.1.3. SMTP-Server
 - 9.8.1.4. POP3-Server
 - 9.8.1.5. IMAP4-Server
- 9.8.2. Mail-Verbrechen
- 9.8.3. Mail-Nachricht
 - 9.8.3.1. Standard-Kopfzeilen
 - 9.8.3.2. Erweiterte Kopfzeilen
- 9.8.4. Schritte bei der Untersuchung dieser Verbrechen
- 9.8.5. Tools für die E-Mail-Forensik

9.9. Mobile forensische Analyse

- 9.9.1. Zellulare Netzwerke
 - 9.9.1.1. Arten von Netzwerken
 - 9.9.1.2. CDR-Inhalt
- 9.9.2. *Subscriber Identity Module* (SIM)
- 9.9.3. Logische Akquisition
- 9.9.4. Physische Akquisition
- 9.9.5. Dateisystem-Erfassung

9.10. Forensische Berichte schreiben und einreichen

- 9.10.1. Wichtige Aspekte eines forensischen Berichts
- 9.10.2. Klassifizierung und Arten von Berichten
- 9.10.3. Leitfaden zum Schreiben eines Berichts
- 9.10.4. Präsentation des Berichts
 - 9.10.4.1. Vorbereitung auf die Zeugenaussage
 - 9.10.4.2. Hinterlegung
 - 9.10.4.3. Der Umgang mit den Medien

Modul 10. Aktuelle und zukünftige Herausforderungen in der IT-Sicherheit

10.1. Blockchain-Technologie

- 10.1.1. Anwendungsbereiche
- 10.1.2. Garantie der Vertraulichkeit
- 10.1.3. Garantie der Nicht Abstreitbarkeit

10.2. Digitales Geld

- 10.2.1. Bitcoins
- 10.2.2. Kryptowährungen
- 10.2.3. Schürfen von Kryptowährungen
- 10.2.4. Schneeballsysteme
- 10.2.5. Andere mögliche Verbrechen und Probleme

10.3. Deepfake

- 10.3.1. Auswirkungen auf die Medien
- 10.3.2. Gefahren für die Gesellschaft
- 10.3.3. Erkennungsmechanismen

10.4. Die Zukunft der künstlichen Intelligenz

- 10.4.1. Künstliche Intelligenz und kognitives Computing
- 10.4.2. Anwendungen zur Vereinfachung des Kundendienstes

10.5. Digitale Privatsphäre

- 10.5.1. Wert der Daten im Netzwerk
- 10.5.2. Verwendung von Daten im Netzwerk
- 10.5.3. Datenschutz und Verwaltung digitaler Identitäten

10.6. Cyber-Konflikte, Cyber-Kriminelle und Cyber-Angriffe

- 10.6.1. Auswirkungen der Cybersicherheit auf internationale Konflikte
- 10.6.2. Folgen von Cyberangriffen auf die allgemeine Bevölkerung
- 10.6.3. Arten von Cyber-Kriminellen. Schutzmaßnahmen

10.7. Telearbeit

- 10.7.1. Revolution der Telearbeit während und nach Covid19
- 10.7.2. Engpässe beim Zugang
- 10.7.3. Variation der Angriffsfläche
- 10.7.4. Bedürfnisse der Arbeiter

10.8. Aufkommende Wireless-Technologien

- 10.8.1. WPA3
- 10.8.2. 5G
- 10.8.3. Millimeter-Wellen
- 10.8.4. Trend zu *Get Smart* anstelle von *Get More*

10.9. Künftige Adressierung in Netzwerken

- 10.9.1. Aktuelle Probleme mit der IP-Adressierung
- 10.9.2. IPv6
- 10.9.3. IPv4+
- 10.9.4. Vorteile von IPv4+ gegenüber IPv4
- 10.9.5. Vorteile von IPv6 gegenüber IPv4

10.10. Die Herausforderung, das Bewusstsein für eine frühzeitige und kontinuierliche Schulung der Bevölkerung zu schärfen

- 10.10.1. Aktuelle Strategien der Regierung
- 10.10.2. Der Widerstand der Menschen gegen das Lernen
- 10.10.3. Ausbildungspläne, die von den Unternehmen angenommen werden müssen

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

- 10.8.1. 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 Personalmanagement

- 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, Ausbildung 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



“

*Dieses Programm wird Ihnen
neue Wege für Ihr berufliches
Weiterkommen eröffnen"*

07

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"

Die TECH Business School verwendet die Fallstudie, um alle Inhalte zu kontextualisieren.

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”



Dieses Programm bereitet Sie darauf vor, geschäftliche Herausforderungen in einem unsicheren Umfeld zu meistern und Ihr Unternehmen erfolgreich zu machen.



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

Eine innovative und andersartige Lernmethode

Dieses TECH-Programm ist eine intensive Spezialisierung, die von Grund auf neu geschaffen wurde, um Managern Herausforderungen und Geschäftsentscheidungen auf höchstem Niveau zu bieten, sowohl auf nationaler als auch auf internationaler Ebene. 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 geschäftliche Realität berücksichtigt wird.

“ *Sie werden durch gemeinschaftliche Aktivitäten und reale Fälle lernen, komplexe Situationen in realen Geschäftsumgebungen zu lösen“*

Die Fallmethode ist das am weitesten verbreitete Lernsystem an den besten Business Schools 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 werden wir bei der Fallmethode konfrontiert, einer handlungsorientierten Lernmethode. Während des gesamten Programms 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.

Unser Online-System ermöglicht es Ihnen, Ihre Zeit und Ihr Lerntempo zu organisieren und an Ihren Zeitplan anzupassen. Sie können die Inhalte von jedem festen oder mobilen Gerät mit Internetanschluss abrufen.

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 Wirtschaftshochschule ist die einzige spanischsprachige Schule, 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 kombinieren wir jedes dieser Elemente konzentrisch. 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.



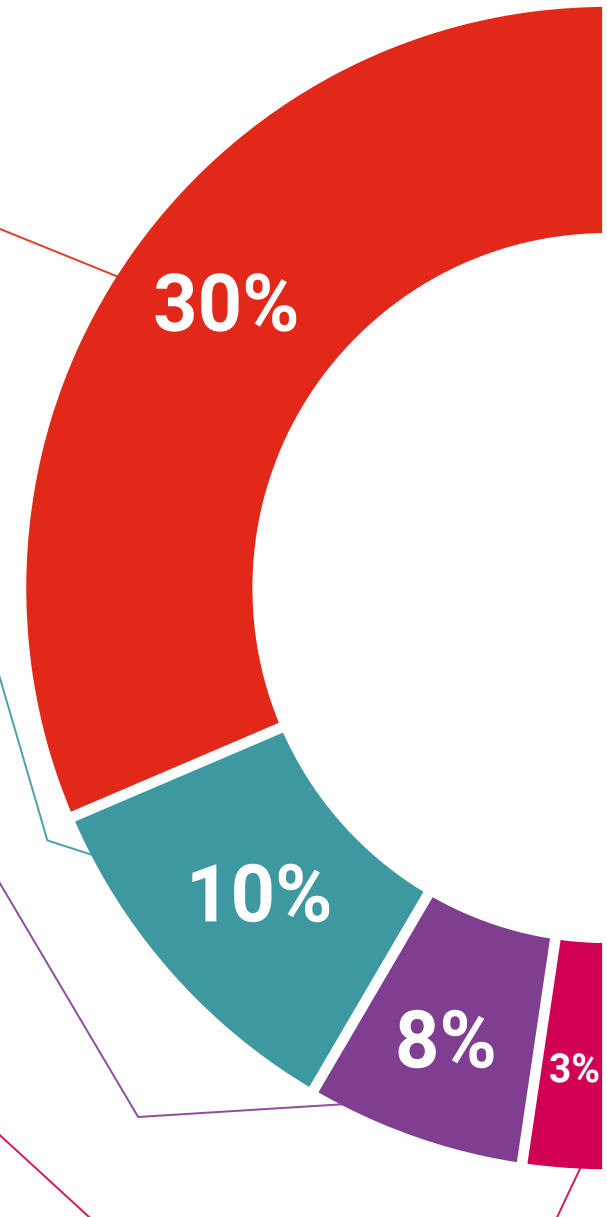
Übungen zu Managementfähigkeiten

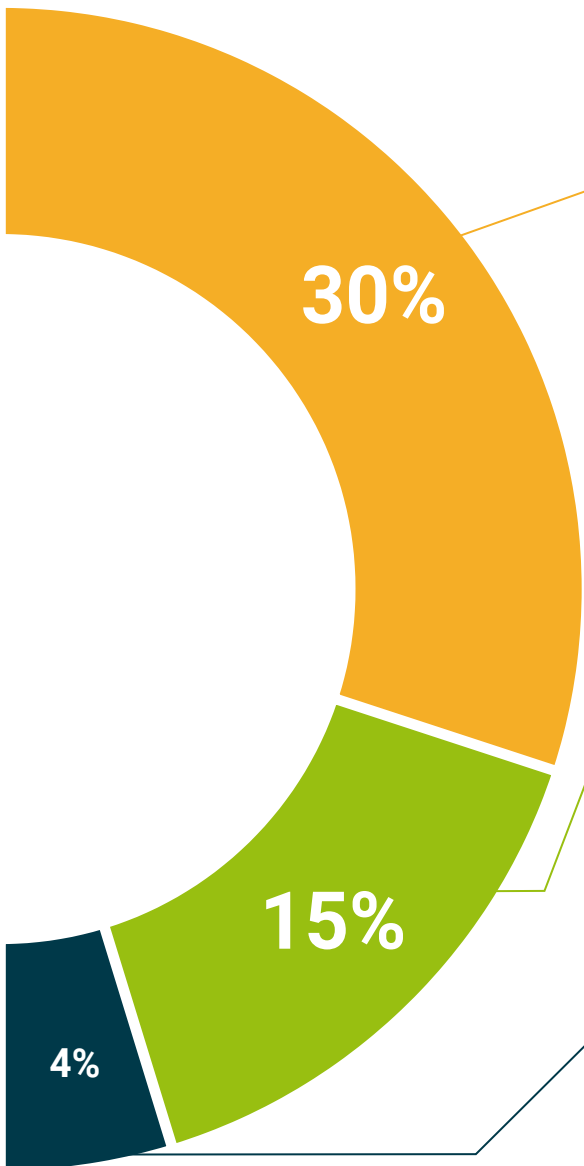
Sie werden Aktivitäten durchführen, um spezifische Managementfähigkeiten in jedem Fachbereich zu entwickeln. Übungen und Aktivitäten zum Erwerb und zur Entwicklung der Fähigkeiten und Fertigkeiten, die ein leitender Angestellter im Rahmen der Globalisierung, in der wir leben, entwickeln muss.



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. Fälle, die von den besten Experten in Senior Management der internationalen Szene präsentiert, analysiert und betreut werden.



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.



08

Profil unserer Studenten

Der MBA in Cybersecurity Management (Chief Information Security Officer) ist ein Programm, das sich an Fachleute richtet, die ihre Fähigkeiten durch eine hochwertige Weiterbildung verbessern möchten. Studenten, die ihr Wissen in einem anderen Bereich, der mit der Wirtschaft verbunden ist, wie z. B. IT, aber insbesondere IT-Sicherheit, vertiefen möchten. Ein Programm, das sich an erfahrene Fachleute richtet, die an eine höhere Spezialisierung als Methode zur persönlichen und beruflichen Weiterentwicklung glauben.





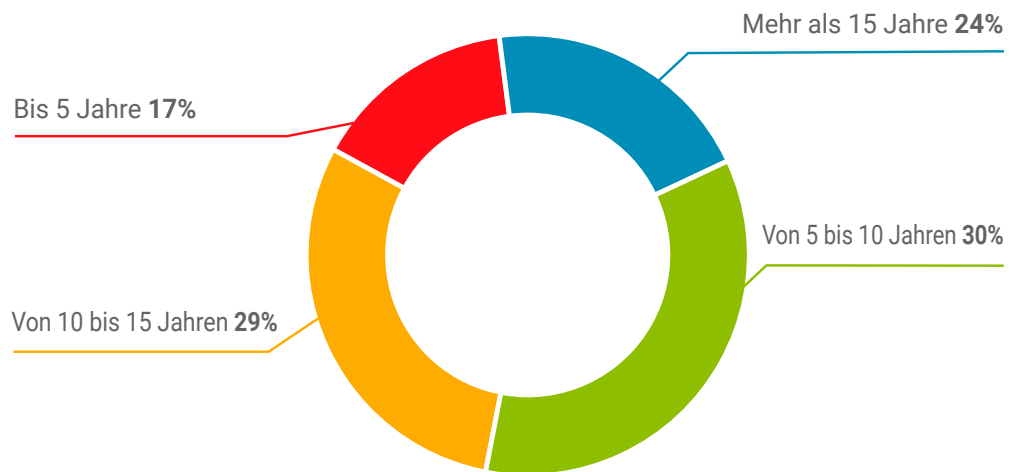
“

TECH-Studenten sind Berufstätige mit umfassender Erfahrung, die sich beruflich weiterentwickeln wollen“

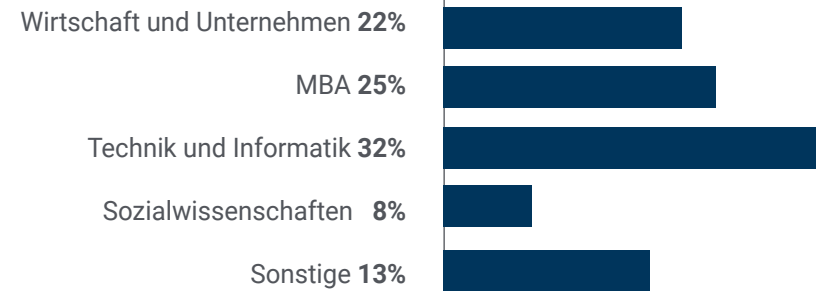
Durchschnittliches Alter

Zwischen **35** und **45** Jahren

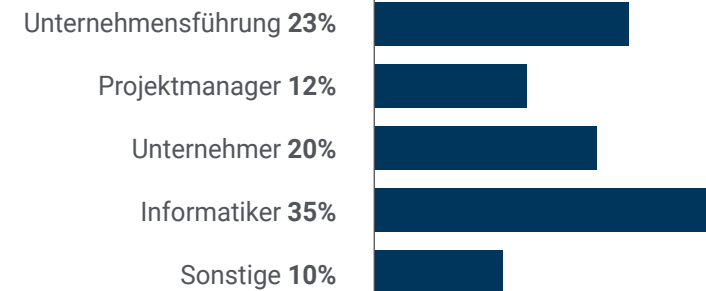
Jahre der Erfahrung



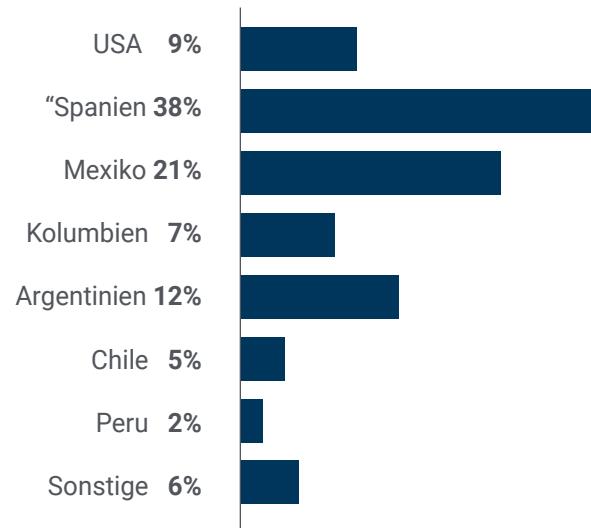
Ausbildung



Akademisches Profil



Geografische Verteilung



Jaime Díaz

Chief Revenue Officer

"In dem geschäftlichen Umfeld, in dem ich arbeite, gehen wir mit vielen vertraulichen Informationen und relevanten Daten um, die in den falschen Händen zu einem großen Problem für das Unternehmen werden können. Deshalb habe ich schon seit einiger Zeit darüber nachgedacht, meine Kenntnisse im Bereich der Cybersicherheit zu erweitern, mit dem Ziel, selbst alle Prozesse zu kontrollieren, die für eine Cyber-Bedrohung besonders anfällig sein könnten. Dank dieses TECH-Programms konnte ich meine Fähigkeiten verbessern und bin selbstbewusster in meiner Arbeit geworden"

09

Kursleitung

Die Dozenten dieses MBA in Cybersecurity Management (Chief Information Security Officer) sind Fachleute mit umfangreicher Erfahrung in diesem Bereich, sowohl beruflich als auch in der Lehre. Dank ihrer Spezialisierung auf diesem Gebiet verfügen sie über die notwendige Qualifizierung, um den Studenten ein umfassendes und hochwertiges Studium der Bereiche zu bieten, die ihnen bei ihrer täglichen Arbeit in der Geschäftswelt nützlich sein werden. Es handelt sich zweifellos um Menschen, die an höhere Bildung als Möglichkeit glauben, sich beruflich weiterzuentwickeln und die Wettbewerbsfähigkeit eines Unternehmens zu verbessern.



“

*Ein erfahrener Lehrkörper zur Unterstützung
Ihrer Spezialisierung in Cybersicherheit"*

Internationaler Gastdirektor

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

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

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



Dr. Lemieux, Frederic

- Direktor des Masterstudiengangs in Cybersecurity Risk Management an der Georgetown University
- Direktor des Masterstudiengangs in Technology Management an der Georgetown University
- Direktor des Masterstudiengangs in Applied Intelligence an der Georgetown University
- Professor für Praktika an der Georgetown University
- Promotion in Kriminologie an der School of Criminology der Universität von Montreal
- Hochschulabschluss in Soziologie und Nebenfach Psychologie an der Universität Laval
- Mitglied von New Program Roundtable Committee, Georgetown University

“

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

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

“

TECH verfügt über eine angesehene und spezialisierte Gruppe von internationalen Gastdirektoren, die wichtige Führungspositionen in den innovativsten Unternehmen auf dem Weltmarkt innehaben"

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 Luminare 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"

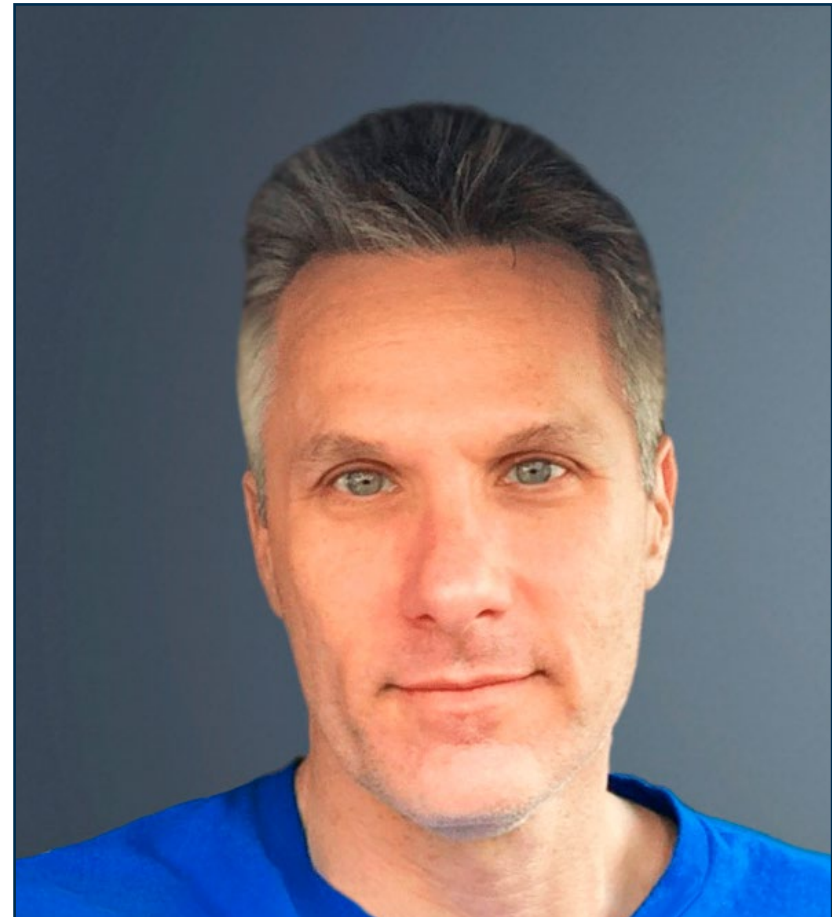
Internationaler Gastdirektor

Scott Stevenson ist ein angesehenes 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



Fr. Fernández Sapena, Sonia

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



Professoren

Hr. Catalá Barba, José Francisco

- Elektroniker mit Erfahrung in Cybersicherheit
- Entwickler von mobilen Anwendungen
- Elektroniker im mittleren Führungsstab des spanischen Verteidigungsministeriums
- Elektroniker im Ford-Werk in Valencia

Hr. Jiménez Ramos, Álvaro

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

Fr. Marcos Sbarbaro, Victoria Alicia

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

Hr. Peralta Alonso, Jon

- ♦ Senior Consultant - Datenschutz und Cybersicherheit
- ♦ Jurist / Rechtsberater bei Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- ♦ Rechtsberater / Praktikant in einer professionellen Kanzlei: Óscar Padura
- ♦ Hochschulabschluss in Jura an der Öffentlichen Universität des Baskenlandes
- ♦ Masterstudiengang in Datenschutzbeauftragter an der EIS Innovative School
- ♦ Masterstudiengang in Anwaltschaft an der Öffentlichen Universität des Baskenlandes
- ♦ Masterstudiengang in Zivilprozessrecht an der Internationalen Universität Isabel I de Castilla
- ♦ Dozent im Masterstudiengang für Datenschutz, Cybersicherheit und IKT-Recht





Hr. Redondo, Jesús Serrano

- ♦ Webentwickler und Cybersecurity-Techniker
- ♦ Web-Entwickler bei Roams, Palencia
- ♦ *FrontEnd*-Entwickler bei Telefónica, Madrid
- ♦ *FrontEnd*-Entwickler bei Best Pro Consulting SL, Madrid
- ♦ Installateur für Telekommunikationseinrichtungen und -dienste bei Grupo Zener, Castilla und León
- ♦ Installateur für Telekommunikationsanlagen und -dienste bei Lican Comunicaciones SL, Castilla und León
- ♦ Zertifikat in Computersicherheit, CFTIC Getafe, Madrid
- ♦ Höhere Berufsausbildung in Telekommunikations- und Computersysteme vom IES Trinidad Arroyo, Palencia
- ♦ Höhere Berufsausbildung in elektrotechnischen Installationen für Mittel- und Niederspannungsnetze vom IES Trinidad Arroyo, Palencia
- ♦ Fortbildung in Reverse Engineering, Stenografie und Verschlüsselung an der Incibe Hacker Academy

“ *TECH hat das Dozententeam für dieses Programm sorgfältig ausgewählt, damit Sie von den besten Spezialisten von heute lernen können* ”

10

Auswirkung auf Ihre Karriere

Der Abschluss dieses MBA in Cybersecurity Management (Chief Information Security Officer) wird die Qualifizierung von Geschäftsleuten um ein Plus an Qualität erweitern, da er all das Wissen bietet, das, auch wenn es von der täglichen Arbeit völlig entfernt zu sein scheint, sehr nützlich sein kann, um jene Computerprozesse zu kontrollieren, die ein schädliches externes Element beherbergen können, das die gesamte Organisation betrifft. Aus diesem Grund ist eine höhere Spezialisierung in diesem Bereich nicht nur für die persönliche und berufliche Entwicklung der Studenten wichtig, sondern auch für die Unternehmen, in denen sie arbeiten.



“

TECH stellt ihren Studenten alle akademischen Ressourcen zur Verfügung, damit sie sich die notwendigen Fähigkeiten aneignen können, die sie zum Erfolg führen werden“

Der Erwerb dieses MBA wird es den Studenten ermöglichen, die notwendige Wettbewerbsfähigkeit zu erlangen, um einen radikalen Wechsel in ihrer Karriere zu vollziehen.

Sind Sie bereit, den Sprung zu wagen? Es erwartet Sie eine hervorragende berufliche Weiterentwicklung

Der MBA in Cybersecurity Management (Chief Information Security Officer) der TECH Technologische Universität ist ein intensives und sehr wertvolles Programm, das darauf abzielt, die Arbeitsfähigkeiten der Studenten in einem Bereich mit weitreichenden Kompetenzen zu verbessern. Es ist zweifellos eine einmalige Gelegenheit, sich beruflich, aber auch persönlich zu verbessern, denn es bedeutet Anstrengung und Hingabe.

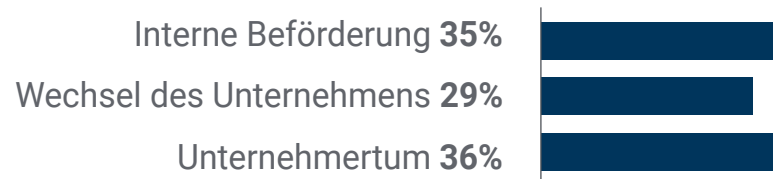
Studenten, die sich selbst verbessern, eine positive Veränderung auf professioneller Ebene herbeiführen und sich mit den Besten austauschen möchten, werden bei TECH ihren Platz finden.

Ein Programm mit einem hohen akademischen Niveau, das Ihre Karriere zum Erfolg führt.

Zeitpunkt des Wandels



Art des Wandels



Gehaltsverbesserung

Der Abschluss dieses Programms bedeutet für unsere Studenten eine Gehaltserhöhung von mehr als **25,22%**



11

Vorteile für Ihr Unternehmen

Der MBA in Cybersecurity Management (Chief Information Security Officer) trägt dazu bei, dass die Talente des Unternehmens ihr volles Potenzial entfalten können indem er hochrangige Führungskräfte spezialisiert. Auf diese Weise werden Geschäftsleute in der Lage sein, die Qualität ihres Unternehmens zu steigern, indem sie über die notwendigen Fähigkeiten zur Steuerung von Prozessen der Cybersicherheit verfügen. Ein Programm, das sich an die Studenten anpasst, so dass sie die notwendigen Werkzeuge erwerben, die sie anschließend in ihrer täglichen Praxis anwenden können, um einen großen Nutzen für ihr Unternehmen zu erzielen.





“

Ein unverzichtbares Programm für Geschäftsleute, die mögliche Probleme mit Cybersicherheit kontrollieren und bewältigen wollen"

Die Entwicklung und Bindung von Talenten in Unternehmen ist die beste langfristige Investition.

01

Wachsendes Talent und intellektuelles Kapital

Die Fachkraft wird neue Konzepte, Strategien und Perspektiven in das Unternehmen einbringen, die relevante Veränderungen bewirken können.

02

Bindung von Führungskräften mit hohem Potenzial und Vermeidung der Abwanderung von Fachkräften

Dieses Programm stärkt die Verbindung zwischen dem Unternehmen und der Fachkraft und eröffnet neue Wege für die berufliche Entwicklung innerhalb des Unternehmens.

03

Aufbau von Akteuren des Wandels

Die Fachkraft wird in der Lage sein, in unsicheren und krisenhaften Zeiten Entscheidungen zu treffen und der Organisation zu helfen, Hindernisse zu überwinden.

04

Verbesserte Möglichkeiten zur internationalen Expansion

Dank dieses Programms wird das Unternehmen mit den wichtigsten Märkten der Weltwirtschaft in Kontakt kommen.



05

Entwicklung eigener Projekte

Die Fachkraft kann an einem realen Projekt arbeiten oder neue Projekte im Bereich FuE oder *Business Development* ihres Unternehmens entwickeln.

06

Gesteigerte Wettbewerbsfähigkeit

Dieses Programm wird die Fachkräfte mit den Fähigkeiten ausstatten, neue Herausforderungen anzunehmen und so das Unternehmen voranzubringen.

12

Qualifizierung

Der MBA in Cybersecurity Management (CISO, Chief Information Security Officer) 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 Cybersecurity Management (CISO, Chief Information Security Officer)** 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: **Executive Master MBA in Cybersecurity Management (CISO, Chief Information Security Officer)**

Modalität: **online**

Dauer: **12 Monate**



*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.



Executive Master

MBA in Cybersecurity
Management (CISO, Chief
Information Security Officer)

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

Executive Master

MBA in Cybersecurity
Management (CISO, Chief
Information Security Officer)

