

Universitätsexperte

Cybersecurity in Aufkommenden Technologien



Universitätsexperte Cybersecurity in Aufkommenden Technologien

- » Modalität: **online**
- » Dauer: **6 Monate**
- » Qualifizierung: **TECH Technologische Universität**
- » Aufwand: **16 Std./Woche**
- » Zeitplan: **in Ihrem eigenen Tempo**
- » Prüfungen: **online**

Internetzugang: www.techtitute.com/de/informatik/spezialisierung/spezialisierung-cybersecurity-aufkommenden-technologien

Index

01

Präsentation

Seite 4

02

Ziele

Seite 8

03

Kursleitung

Seite 12

04

Struktur und Inhalt

Seite 16

05

Methodik

Seite 22

06

Qualifizierung

Seite 30

01

Präsentation

In jüngster Zeit sind eine Reihe von Technologien aufgetaucht, die sich rasch durchgesetzt haben. Dies bringt nicht nur neue Dienste für Unternehmen, Nutzer und Kunden, sondern auch ein Sicherheitsproblem mit sich. Neue Technologien befinden sich naturgemäß in ständiger Entwicklung und haben ihren optimalen Schutzstatus noch nicht erreicht, weshalb sie angreifbar sind. Als Antwort auf diese Herausforderung wurde dieses Programm entwickelt, das es Informatikern ermöglicht, die besten Cybersicherheitsmethoden für das Internet der Dinge, *Cloud Computing* und *Blockchain* kennenzulernen. Auf diese Weise schärfen Sie Ihr berufliches Profil und bereiten sich auf die Herausforderungen der digitalen Sicherheit von heute und morgen vor.



“

Machen Sie sich bereit, sich mit diesem Universitätsexperten in Cybersicherheit in Bezug auf Cloud Computing, Blockchain oder das Internet der Dinge zu spezialisieren, was Sie zu einer gefragten Fachkraft in den besten Technologieunternehmen machen wird"

Aufkommende Technologien sind von Dauer. Sie kamen zu einem Zeitpunkt, als Lösungen für verschiedene Probleme benötigt wurden. So entwickelt sich beispielsweise das Internet der Dinge zu einem wesentlichen Bestandteil des Lebens vieler Menschen. Auch die *Blockchain* trägt dazu bei, zahlreiche Prozesse zu dezentralisieren, und *Cloud Computing* gewährleistet die Verfügbarkeit von Ressourcen aller Art, insbesondere von Daten oder Anwendungen, an jedem beliebigen Ort mit einfachem Zugang zu einer Netzverbindung.

Da es sich hierbei um sehr nützliche Elemente und Dienste handelt, nimmt ihre Beliebtheit rapide zu, was zu einem Mangel an Ausgewogenheit führt, da sie oft nicht ausreichend gesichert sind, da es sich um Technologien handelt, die noch nicht zu 100% entwickelt sind. Aus diesem Grund suchen immer mehr Unternehmen, sowohl im Bereich der Elektronik als auch in anderen Bereichen, nach Fachleuten, die sich auf die Cybersicherheit dieser Instrumente spezialisiert haben.

Dieser Universitätsexperte erforscht daher alle Möglichkeiten der Cybersicherheit in dieser Art von Technologie und garantiert dem Informatiker eine intensive und vollständige Vertiefung in diesem Bereich, was ihm einen entscheidenden beruflichen Impuls für seine Karriere gibt.

All dies geschieht über ein Online-Unterrichtssystem, das speziell für Berufstätige entwickelt wurde, die ihre Arbeit und ihr Studium auf bequeme und einfache Weise miteinander verbinden können. Darüber hinaus stehen Ihnen die besten Lehrkräfte zur Verfügung, die sich aus echten Spezialisten in diesem wichtigen Bereich der Cybersecurity zusammensetzen.

Dieser **Universitätsexperte in Cybersecurity in Aufkommenden Technologien** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- ♦ Die Entwicklung praktischer Fälle, die von Experten der Informatik und Cybersicherheit vorgestellt werden
- ♦ Der anschauliche, schematische und äußerst praxisnahe Inhalt soll wissenschaftliche und praktische Informationen zu den für die berufliche Praxis wesentlichen Disziplinen vermitteln
- ♦ Die praktischen Übungen, bei denen der Selbstbewertungsprozess zur Verbesserung des Lernens durchgeführt werden kann
- ♦ Ihr besonderer Schwerpunkt liegt auf innovativen Methoden
- ♦ Theoretische Vorträge, Fragen an den Experten, Diskussionsforen zu kontroversen Themen und individuelle Reflexionsarbeit
- ♦ Die Verfügbarkeit des Zugriffs auf die Inhalte von jedem festen oder tragbaren Gerät mit Internetanschluss



Unternehmen aller Art brauchen Spezialisten, um ihre Blockchain- oder internet der Dinge-Projekte optimal absichern zu können"



Das beste Online-Lehrsystem wird Ihnen zur Verfügung stehen, damit Sie in Ihrem eigenen Tempo lernen können, ohne starre Zeitpläne oder Unterbrechungen bei der Arbeit"

Zu den Lehrkräften des Programms gehören Fachleute aus der Branche, die ihre Berufserfahrung in diese Fortbildung einbringen, sowie renommierte Fachleute von Referenzgesellschaften und angesehenen Universitäten.

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

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

Dank dieses Programms können Sie mehr über die besten kryptografischen Methoden oder die bestehenden Arten von Cloud-Infrastrukturen erfahren.

Aufkommende Technologien sind die Gegenwart und die Zukunft: Spezialisieren Sie sich und verbessern Sie sofort Ihre Karriereaussichten.



02 Ziele

Das Hauptziel dieses Universitätsexperten in Cybersecurity in aufkommenden Technologien ist es, den Informatiker zu einem Referenzspezialisten in diesem Bereich zu machen und sich als perfekte Lösung für jedes Unternehmen zu positionieren, das *Blockchain*- oder *Cloud-Computing*-Projekte mit absoluter Sicherheit angehen möchte. Mit dem Abschluss dieses Programms verfügen Sie über ein perfektes Berufsprofil für das neue technologische und digitale Umfeld, das sich seit einiger Zeit durchgesetzt hat.





“

*Mit dem Abschluss dieses
Universitätsexperten werden
Sie die gefragteste Fachkraft in
Ihrem Umfeld sein“*



Allgemeine Ziele

- ◆ Untersuchung der Wissenschaft der Kryptologie und der Beziehung zu ihren Zweigen: Kryptographie, Kryptoanalyse, Steganographie und Stegoanalyse
- ◆ Analyse der Arten von Kryptographie nach der Art des Algorithmus und nach ihrer Verwendung
- ◆ Schlüsselverwaltungssysteme zusammenstellen
- ◆ Bewertung der verschiedenen praktischen Anwendungen
- ◆ Digitale Zertifikate prüfen
- ◆ Untersuchung der Public Key Infrastructure (PKI)
- ◆ Analyse der neuesten Trends und Herausforderungen
- ◆ Untersuchung des Prozesses der Entwicklung einer Sicherheitsstrategie bei der Bereitstellung von *Cloud*-Diensten für Unternehmen
- ◆ Die Sicherheitsbereiche in der *Cloud* identifizieren
- ◆ Analyse der Dienste und Tools in jedem der Sicherheitsbereiche
- ◆ Bewertung der Unterschiede in den spezifischen Implementierungen der verschiedenen *Public Cloud*-Anbieter
- ◆ Bewertung der IoT-Konnektivitätsoptionen für ein Projekt, mit Schwerpunkt auf LPWAN-Technologien
- ◆ Einführung in die grundlegenden Spezifikationen der wichtigsten LPWAN-Technologien für das IoT
- ◆ Entwicklung der Sicherheitspezifikationen für jede LPWAN-Technologie
- ◆ Vergleichende Analyse der Sicherheit von LPWAN-Technologien





Spezifische Ziele

Modul 1. Kryptographie in der IT

- ◆ Die grundlegenden Operationen (XOR, große Zahlen, Substitution und Transposition) und die verschiedenen Komponenten (One-Way-Funktionen, Hash, Zufallszahlengeneratoren) zusammenstellen
- ◆ Analyse kryptographischer Techniken
- ◆ Verschiedene kryptographische Algorithmen entwickeln
- ◆ Demonstration der Verwendung digitaler Signaturen und ihrer Anwendung in digitalen Zertifikaten
- ◆ Bewertung von Schlüsselverwaltungssystemen und der Bedeutung von kryptographischen Schlüssellängen
- ◆ Untersuchung von Algorithmen zur Schlüsselableitung
- ◆ Analyse des Lebenszyklus von Schlüsseln
- ◆ Auswertung von Blockchiffre- und Stromchiffre-Modi
- ◆ Pseudo-Zufallszahlengeneratoren bestimmen
- ◆ Entwicklung realer Kryptographie-Anwendungen, wie Kerberos, PGP oder Smart Cards
- ◆ Prüfung verwandter Verbände und Gremien, wie ISO, NIST oder NCSC
- ◆ Die Herausforderungen in der Kryptographie des Quantencomputings bestimmen

Modul 2. Sicherheit in *Cloud*-Umgebungen

- ◆ Identifizierung der Risiken bei der Bereitstellung einer öffentlichen *Cloud*-Infrastruktur
- ◆ Sicherheitsanforderungen definieren
- ◆ Entwicklung eines Sicherheitsplans für eine *Cloud*-Bereitstellung
- ◆ Identifizierung der *Cloud*-Dienste, die für die Ausführung eines Sicherheitsplans eingesetzt werden sollen

- ◆ Bestimmung der operativen Anforderungen für Präventionsmechanismen
- ◆ Festlegung von Leitlinien für ein *Logging*- und Überwachungssystem
- ◆ Maßnahmen zur Reaktion auf Vorfälle vorschlagen

Modul 3. Sicherheit der Kommunikation von IoT-Geräten

- ◆ Einführung in die vereinfachte IoT-Architektur
- ◆ Erklärung der Unterschiede zwischen allgemeinen Konnektivitätstechnologien und Konnektivitätstechnologien für das IoT
- ◆ Das Konzept des Eisernen Dreiecks der IoT-Konnektivität etablieren
- ◆ Analyse der Sicherheitsspezifikationen der LoRaWAN-Technologie, NB-IoT-Technologie und WiSUN-Technologie
- ◆ Die Wahl der richtigen IoT-Technologie für jedes Projekt begründen



Alle Ihre beruflichen Ziele sind zum Greifen nah: schreiben Sie sich ein und werden Sie Spezialist für Cybersecurity in aufkommenden Technologien"

03

Kursleitung

Die derzeitige komplexe Situation erfordert von den Fachleuten eine ständige Aktualisierung und Vertiefung ihrer Kenntnisse. Aufkommende Technologien sind nicht nur bahnbrechend, sondern verändern sich auch ständig, wenn neue Entwicklungen auftauchen. Aus diesem Grund ist es notwendig, die besten Spezialisten in diesem Bereich zu haben, und dieser Universitätsexperte hat sie, so dass der Informatiker in der Lage sein wird, mit allen neuesten Entwicklungen aus der Lehre von aktiven Fachleuten auf dem Laufenden zu bleiben.



“

Die erfahrensten Dozenten, die im Bereich der Cybersicherheit tätig sind, werden Ihnen die fortschrittlichsten Kenntnisse und Techniken vermitteln"

Leitung



Hr. Olalla Bonal, Martín

- Technischer Kundenspezialist Blockchain bei IBM
- *Blockchain* Architekt
- Infrastruktur Architekt im Bankwesen
- Projektleitung und Implementierung von Lösungen
- Techniker für digitale Elektronik
- Dozent: *Hyperledger Fabric*-Schulung für Unternehmen
- Dozent: Geschäftsorientierte *Blockchain*-Schulungen für Unternehmen

Professoren

Hr. Gómez Rodríguez, Antonio

- ◆ Ingenieur für Cloud-Lösungen bei Oracle
- ◆ Projektleitung bei der Sopra-Gruppe
- ◆ Projektleitung bei Everis
- ◆ Projektleitung bei der staatlichen Gesellschaft zur Verwaltung von Kulturprogrammen Andalusisches Ministerium für Kultur
- ◆ Analyst für Informationssysteme Sopra Group
- ◆ Hochschulabschluss in Telekommunikationstechnik an der Polytechnischen Universität von Katalonien
- ◆ Postgraduierter in Informationstechnologien und -systemen, Katalanisches Institut für Technologie
- ◆ E-Business Master, Wirtschaftshochschule La Salle

Hr. del Valle Arias, Jorge

- ◆ Smart Cities Business Growth Manager Spain in Itron Inc.
- ◆ IoT-Berater
- ◆ Leitung der IoT-Abteilung bei Diode Spanien
- ◆ Vertriebsleitung IoT & Cellular bei Aicox Soluciones
- ◆ Gründung und CEO von Sensor Intelligence
- ◆ Betriebsleitung bei Codium Networks
- ◆ Bereichsleitung Elektronik bei Aitemin
- ◆ Ingenieur für Telekommunikation von der Polytechnischen Universität von Madrid
- ◆ Executive MBA von der International Graduate School von La Salle in Madrid

Hr. Ortega, Octavio

- ◆ Programmierer für Computeranwendungen und Webentwicklung
- ◆ Web- und APPS-Design für Kunden, CRDS für die vom Instituto de Salud Carlos III durchgeführte Forschung, Online-Shops, Android-Anwendungen usw.
- ◆ Dozent für Computersicherheit
- ◆ Hochschulabschluss in Psychologie an der Universität Oberta de Catalunya (UOC)
- ◆ Höherer Techniker in Software-Analyse, Design und Lösungen
- ◆ Höherer Universitätstechniker in fortgeschrittener Programmierung



Sie werden in der Lage sein, auf alle Arten von Bedrohungen der Cybersicherheit angemessen zu reagieren. Schreiben Sie sich ein und werden Sie ein echter Spezialist“

04

Struktur und Inhalt

Dieser Universitätsexperte in Cybersecurity in aufkommenden Technologien besteht aus 3 spezialisierten Modulen, die in 450 Stunden intensiven Lernens erarbeitet werden. Ausgehend von dieser Struktur wird der Informatiker in der Lage sein, sich mit relevanten Aspekten der Cybersecurity zu befassen, z. B. mit den mathematischen Grundlagen der Kryptographie, der Verwendung von Algorithmen in der Sicherheit, der Sicherheit in öffentlichen *Clouds* und den wichtigsten Sicherheitslücken des IoT.





“

Dieses Programm enthält die umfassendsten Inhalte zum Thema Cybersecurity in Bezug auf neue Technologien. Warten Sie nicht länger und schreiben Sie sich ein"

Modul 1. Kryptographie in der IT

- 1.1. Kryptographie
 - 1.1.1. Kryptographie
 - 1.1.2. Mathematische Grundlagen
- 1.2. Kryptologie
 - 1.2.1. Kryptologie
 - 1.2.2. Kryptoanalyse
 - 1.2.3. Steganographie und Stegoanalyse
- 1.3. Kryptographische Protokolle
 - 1.3.1. Grundlegende Blöcke
 - 1.3.2. Grundlegende Protokolle
 - 1.3.3. Zwischengeschaltete Protokolle
 - 1.3.4. Erweiterte Protokolle
 - 1.3.5. Exoterische Protokolle
- 1.4. Kryptographische Techniken
 - 1.4.1. Länge des Schlüssels
 - 1.4.2. Handhabung der Tasten
 - 1.4.3. Arten von Algorithmen
 - 1.4.4. Zusammenfassende Funktionen. Hash
 - 1.4.5. Pseudo-Zufallszahlengeneratoren
 - 1.4.6. Verwendung von Algorithmen
- 1.5. Symmetrische Kryptographie
 - 1.5.1. Blockchiffren
 - 1.5.2. DES (*Data Encryption Standard*)
 - 1.5.3. RC4 Algorithmus
 - 1.5.4. AES (*Advanced Encryption Standard*)
 - 1.5.5. Kombination von Blockchiffren
 - 1.5.6. Ableitung des Schlüssels



- 1.6. Asymmetrische Kryptographie
 - 1.6.1. Diffie-Hellman
 - 1.6.2. DSA (*Digital Signature Algorithm*)
 - 1.6.3. RSA (*Rivest, Shamir y Adleman*)
 - 1.6.4. Elliptische Kurve
 - 1.6.5. Asymmetrische Kryptographie. Typologie
- 1.7. Digitale Zertifikate
 - 1.7.1. Digitale Unterschrift
 - 1.7.2. X509-Zertifikate
 - 1.7.3. Infrastruktur für öffentliche Schlüssel (PKI)
- 1.8. Implementierungen
 - 1.8.1. Kerberos
 - 1.8.2. IBM CCA
 - 1.8.3. *Pretty Good Privacy* (PGP)
 - 1.8.4. *ISO Authentication Framework*
 - 1.8.5. SSL und TLS
 - 1.8.6. Chipkarten als Zahlungsmittel (EMV)
 - 1.8.7. Protokolle für Mobiltelefonie
 - 1.8.8. *Blockchain*
- 1.9. Steganographie
 - 1.9.1. Steganographie
 - 1.9.2. Stegano-Analyse
 - 1.9.3. Anwendungen und Einsatzmöglichkeiten
- 1.10. Quantenkryptographie
 - 1.10.1. Quanten-Algorithmen
 - 1.10.2. Schutz von Algorithmen vor Quantenberechnungen
 - 1.10.3. Quantum Key Distribution

Modul 2. Sicherheit in *Cloud*-Umgebungen

- 2.1. Sicherheit in *Cloud Computing*-Umgebungen
 - 2.1.1. Sicherheit in *Cloud Computing*-Umgebungen
 - 2.1.2. Sicherheit in *Cloud Computing*-Umgebungen. Bedrohungen und Sicherheitsrisiken
 - 2.1.3. Sicherheit in *Cloud Computing*-Umgebungen. Wichtige Sicherheitsaspekte
- 2.2. Arten von *Cloud* Infrastruktur
 - 2.2.1. Publikum
 - 2.2.2. Öffentlich
 - 2.2.3. Privat
- 2.3. Hybrid
 - 2.3.1. Vom Anbieter verwaltete Sicherheitselemente
 - 2.3.2. Vom Kunden verwaltete Elemente
 - 2.3.3. Definition der Sicherheitsstrategie
- 2.4. Mechanismen der Prävention
 - 2.4.1. Authentifizierungs-Management-Systeme
 - 2.4.2. Berechtigungsverwaltungssystem: Zugriffsrichtlinien
 - 2.4.3. Systeme zur Schlüsselverwaltung
- 2.5. Verbriefung von Systemen
 - 2.5.1. Verbriefung von Speichersystemen
 - 2.5.2. Sicherung von Datenbanksystemen
 - 2.5.3. Sichern von Daten bei der Übermittlung
- 2.6. Schutz der Infrastruktur
 - 2.6.1. Entwurf und Implementierung eines sicheren Netzwerks
 - 2.6.2. Sicherheit von Computerressourcen
 - 2.6.3. Tools und Ressourcen zum Schutz der Infrastruktur
- 2.7. Erkennung von Bedrohungen und Angriffen
 - 2.7.1. Auditing, *Logging* und Überwachungssysteme
 - 2.7.2. Ereignis- und Alarmsysteme
 - 2.7.3. SIEM-Systeme

- 2.8. Reaktion auf Vorfälle
 - 2.8.1. Plan zur Reaktion auf Vorfälle
 - 2.8.2. Geschäftskontinuität
 - 2.8.3. Forensische Analyse und Behebung von Vorfällen der gleichen Art
- 2.9. Sicherheit in öffentlichen Clouds
 - 2.9.1. AWS (Amazon Web Services)
 - 2.9.2. Microsoft Azure
 - 2.9.3. Google GCP
 - 2.9.4. Oracle Cloud
- 2.10. Regulierung und Compliance
 - 2.10.1. Compliance im Bereich Sicherheit
 - 2.10.2. Risikomanagement
 - 2.10.3. Menschen und Prozesse in Organisationen

Modul 3. Sicherheit der Kommunikation von IoT-Geräten

- 3.1. Von der Telemetrie zum IoT
 - 3.1.1. Telemetrie
 - 3.1.2. M2M-Konnektivität
 - 3.1.3. Demokratisierung der Telemetrie
- 3.2. IoT-Referenzmodelle
 - 3.2.1. IoT-Referenzmodelle
 - 3.2.2. Vereinfachte IoT-Architektur
- 3.3. IoT-Sicherheitsschwachstellen
 - 3.3.1. IoT-Geräte
 - 3.3.2. IoT-Geräte. Kasuistik der Verwendung
 - 3.3.3. IoT-Geräte. Schwachstellen
- 3.4. IoT-Konnektivität
 - 3.4.1. PAN, LAN, WAN-Netzwerke
 - 3.4.2. Drahtlose Technologien außerhalb des IoT
 - 3.4.3. Drahtlose LPWAN-Technologien



- 3.5. LPWAN-Technologien
 - 3.5.1. Das eiserne Dreieck der LPWANs
 - 3.5.2. Freie Frequenzbänder vs. Lizenzierte Bänder
 - 3.5.3. LPWAN Technologie Optionen
- 3.6. LoRaWAN-Technologie
 - 3.6.1. LoRaWAN-Technologie
 - 3.6.2. LoRaWAN Anwendungsfälle. Ökosystem
 - 3.6.3. LoRaWAN Sicherheit
- 3.7. Sigfox Technologie
 - 3.7.1. Sigfox Technologie
 - 3.7.2. Sigfox Anwendungsfälle. Ökosystem
 - 3.7.3. Sicherheit in Sigfox
- 3.8. IoT-Mobilfunktechnologie
 - 3.8.1. IoT-Mobilfunktechnologie (NB-IoT und LTE-M)
 - 3.8.2. Anwendungsfälle für IoT-Mobilfunktechnologie Ökosystem
 - 3.8.3. IoT-Mobilfunktechnologie-Sicherheit
- 3.9. WiSUN Technologie
 - 3.9.1. WiSUN Technologie
 - 3.9.2. WiSUN Anwendungsfälle. Ökosystem
 - 3.9.3. Sicherheit in WiSUN
- 3.10. Andere IoT-Technologien
 - 3.10.1. Andere IoT-Technologien
 - 3.10.2. Anwendungsfälle und Ökosystem anderer IoT-Technologien
 - 3.10.3. Sicherheit in anderen IoT-Technologien

“ *Die besten Dozenten bringen Sie mit den neuesten Inhalten auf den neuesten Stand der Sicherheit in den neuen Technologien*”

05 Methodik

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

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





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

Fallstudie zur Kontextualisierung aller Inhalte

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

“

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



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



Die Studenten lernen durch gemeinschaftliche Aktivitäten und reale Fälle die Lösung komplexer Situationen in realen Geschäftsumgebungen.

Eine innovative und andersartige Lernmethode

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

“

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

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

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

Relearning Methodik

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

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

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

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

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



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

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

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

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



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



Studienmaterial

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

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



Meisterklassen

Die Nützlichkeit der Expertenbeobachtung ist wissenschaftlich belegt.

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



Fertigkeiten und Kompetenzen Praktiken

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



Weitere Lektüren

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





Fallstudien

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



Interaktive Zusammenfassungen

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

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



Prüfung und Nachprüfung

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



06

Qualifizierung

Der Universitätsexperte in Cybersecurity in Aufkommenden Technologien garantiert neben der strengsten und aktuellsten Ausbildung auch den Zugang zu einem von der TECH Technologischen Universität ausgestellten Diplom.



“

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

Dieser **Universitätsexperte in Cybersecurity in Aufkommenden Technologien** 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: **Universitätsexperte in Cybersecurity in Aufkommenden Technologien**
Anzahl der offiziellen Arbeitsstunden: **450 Std.**

zukunft

gesundheit vertrauen menschen
erziehung information tutoren
garantie akkreditierung unterricht
institutionen technologie lernen
gemeinschaft verpflichtung
persönliche betreuung innovation
wissen gegenwart qualität
online-Ausbildung
entwicklung institut
virtuelles Klassenzimmer

tech technologische
universität

Universitätsexperte

Cybersecurity in
Aufkommenden
Technologien

- » Modalität: online
- » Dauer: 6 Monate
- » Qualifizierung: TECH Technologische Universität
- » Aufwand: 16 Std./Woche
- » Zeitplan: in Ihrem eigenen Tempo
- » Prüfungen: online

Universitätsexperte

Cybersecurity in Aufkommenden
Technologien