

# Universitätsexperte IT-Sicherheit



## Universitätsexperte IT-Sicherheit

- » 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-it-sicherheit](http://www.techtitute.com/de/informatik/spezialisierung/spezialisierung-it-sicherheit)

# 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

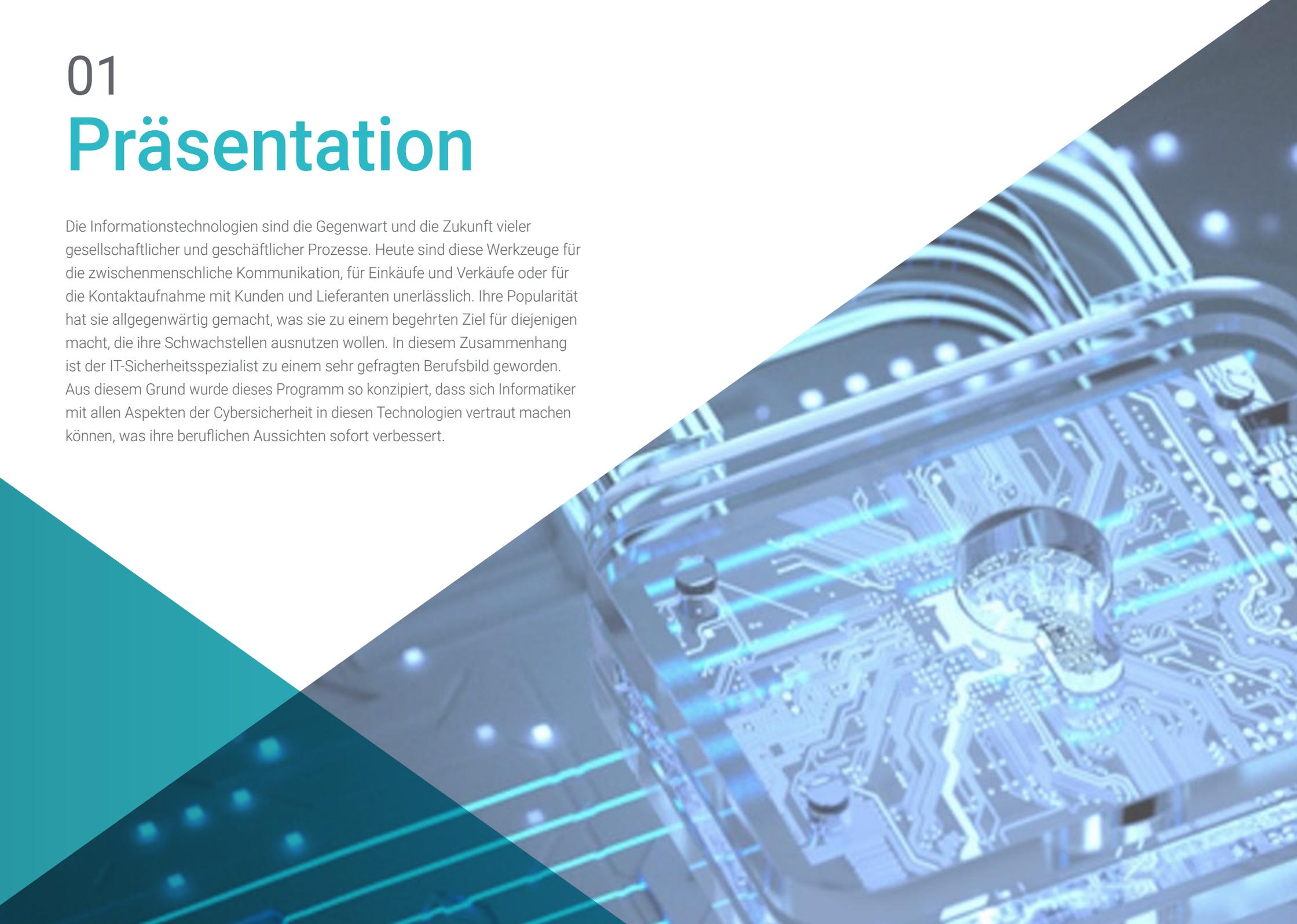
---

Seite 30

# 01

# Präsentation

Die Informationstechnologien sind die Gegenwart und die Zukunft vieler gesellschaftlicher und geschäftlicher Prozesse. Heute sind diese Werkzeuge für die zwischenmenschliche Kommunikation, für Einkäufe und Verkäufe oder für die Kontaktaufnahme mit Kunden und Lieferanten unerlässlich. Ihre Popularität hat sie allgegenwärtig gemacht, was sie zu einem begehrten Ziel für diejenigen macht, die ihre Schwachstellen ausnutzen wollen. In diesem Zusammenhang ist der IT-Sicherheitsspezialist zu einem sehr gefragten Berufsbild geworden. Aus diesem Grund wurde dieses Programm so konzipiert, dass sich Informatiker mit allen Aspekten der Cybersicherheit in diesen Technologien vertraut machen können, was ihre beruflichen Aussichten sofort verbessert.



“

*Mit diesem Programm können Sie sich auf IT-Sicherheit spezialisieren, was Ihnen große Karrierechancen in einem zunehmend gefragten IT-Bereich eröffnet"*

Der neue technologische Kontext erfordert von den Fachleuten eine Vertiefung der Kenntnisse, um sich an die bestehenden Veränderungen in der IT-Sicherheit anzupassen. Diese Informationstechnologien sind somit allgegenwärtig und werden in allen Arten von Geschäfts- und Sozialprozessen eingesetzt. Infolgedessen gibt es zahlreiche Aspekte, bei denen die Gefahr besteht, dass sie durch Schwachstellen ausgenutzt werden können.

Diese Situation ist für die Unternehmen sehr besorgniserregend, da sie sehen, wie unzureichende Sicherheit ihr Geschäft gefährden kann. Die Lösung liegt daher in der Einstellung von Fachkräften, die sich auf diesen Bereich spezialisiert haben. Aus diesem Grund sind IT-Sicherheitsspezialisten derzeit eines der gefragtesten und am meisten geschätzten Profile bei Unternehmen in verschiedenen Bereichen und Sektoren.

Um dieser Nachfrage gerecht zu werden, wird dieser Universitätsexperte in einem 100%igen Online-Format präsentiert, mit einem Lehrkörper von enormem internationalen Prestige in diesem Bereich der Cybersicherheit. Darüber hinaus werden die Inhalte dieses Programms in verschiedenen Multimedia-Formaten präsentiert: interaktive Zusammenfassungen, Videos, Fallstudien, Meisterkurse, praktische Aktivitäten usw. Alles mit dem Ziel, den Fachleuten die neuesten Entwicklungen im Bereich der Sicherheit in der Informationstechnologie zu vermitteln.

Dieser **Universitätsexperte in IT-Sicherheit** 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



*Mit diesem Programm werden Sie in der Lage sein, relevante Aspekte der IT-Sicherheit zu vertiefen, wie z.B. die sichere Entwicklung in der Kommunikation und im Softwarebetrieb"*

“

*Das 100%ige Online-Lernsystem von TECH ermöglicht es Ihnen, Ihre Arbeit und Ihr Studium miteinander zu verbinden, da es sich an alle Ihre persönlichen und beruflichen Umstände anpasst"*

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 situierendes 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.

*Das Dozententeam dieses Programms setzt sich aus berufstätigen Fachleuten zusammen, die mit allen aktuellen Entwicklungen in diesem Bereich der Cybersicherheit vertraut sind.*

*Ihr berufliches Profil wird durch die Absolvierung dieses Universitätsexperten, der mit zahlreichen multimedialen Mitteln unterrichtet wird, gestärkt.*



# 02 Ziele

Das Hauptziel dieses Universitätsexperten in IT-Sicherheit ist es, den Fachleuten die besten Werkzeuge an die Hand zu geben, damit sie sich an den neuen IT-Kontext anpassen können, der durch den Digitalisierungsprozess, der sich in allen Bereichen der Gesellschaft ausgebreitet hat, verändert wurde. Damit sind Sie bestens gerüstet, um als Spezialist für Cybersicherheit in einem Unternehmen zu arbeiten, das sein Geschäft vor neuen Cyber-Bedrohungen schützen will.



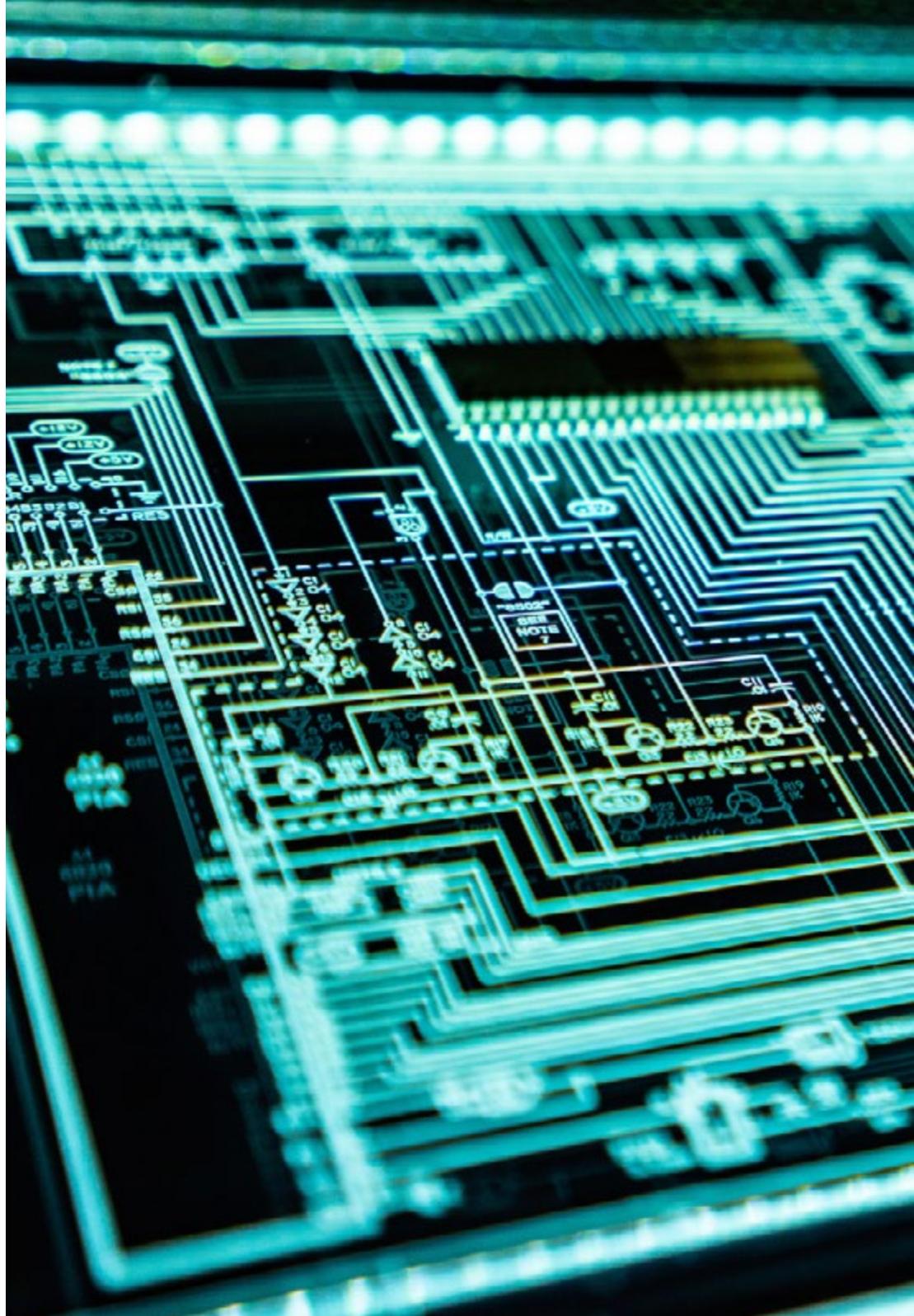
“

*Das Ziel von TECH ist es, Ihnen das aktuellste Wissen zu vermitteln, damit Sie Ihre Arbeit mit maximaler Sicherheit ausführen können und zu einem Referenzprofi in diesem Sektor werden"*



## Allgemeine Ziele

- ◆ Erarbeitung von Fachwissen über ein Informationssystem, die Arten und die zu berücksichtigenden Sicherheitsaspekte
- ◆ Identifizierung von Schwachstellen in einem Informationssystem
- ◆ Anwendung der am besten geeigneten Sicherheitsmaßnahmen in Abhängigkeit von den Bedrohungen
- ◆ Entwicklung der gesetzlichen Bestimmungen und Typisierung von Verbrechen, die ein Informationssystem angreifen
- ◆ Festlegung der Sicherheitspolitik und des Sicherheitsplans eines Unternehmens für Informationssysteme und Vervollständigung des Entwurfs und der Umsetzung des Notfallplans
- ◆ Spezialwissen über das Ökosystem der IT-Sicherheit generieren
- ◆ Wissen in Bezug auf Cybersicherheit auswerten
- ◆ Entwicklung von Best Practices für die sichere Entwicklung
- ◆ Darstellung der Risiken, die Unternehmen eingehen, wenn sie nicht über eine sichere Informationssicherheitsumgebung verfügen
- ◆ 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





## Spezifische Ziele

---

### Modul 1. Sicherheit in Design und Entwicklung von Systemen

- ◆ Bewertung der Sicherheit eines Informationssystems über alle seine Komponenten und Schichten hinweg
- ◆ Identifizierung aktueller Arten von Sicherheitsbedrohungen und Trends
- ◆ Festlegung von Sicherheitsrichtlinien durch Definition von Sicherheits- und Notfallrichtlinien und -plänen
- ◆ Analyse von Strategien und Tools zur Gewährleistung der Integrität und Sicherheit von Informationssystemen
- ◆ Anwendung spezifischer Techniken und Tools für jede Art von Angriff oder Sicherheitsschwachstelle
- ◆ Schutz der im Informationssystem gespeicherten vertraulichen Informationen
- ◆ Den rechtlichen Rahmen und die Typisierung des Verbrechens kennen, um die Vision mit der Typisierung des Täters und seines Opfers zu vervollständigen

### Modul 2. Sicherheit bei Kommunikation und Softwarebetrieb

- ◆ Entwicklung von Fachwissen über physische und logische Sicherheit
- ◆ Demonstration von Kenntnissen über Kommunikation und Netzwerke
- ◆ Identifizierung größerer bösartiger Angriffe
- ◆ Einen sicheren Entwicklungsrahmen einrichten
- ◆ Nachweis von Kenntnissen über die wichtigsten Vorschriften zum Management von Informationssicherheitssystemen
- ◆ Demonstration der Gründe für den Betrieb eines Betriebszentrums für Cybersicherheit
- ◆ Die Bedeutung von Cybersicherheitspraktiken für organisatorische Katastrophen demonstrieren

### Modul 3. 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



*Sie werden beruflich schnell vorankommen, denn Ihr neues Wissen macht Sie zu einem gefragten Spezialisten"*

# 03

## Kursleitung

IT-Sicherheit ist ein Bereich, der sich ständig weiterentwickelt und modernste Kenntnisse erfordert, die nur eine erfahrene Fachkraft bieten kann. Aus diesem Grund hat sich TECH bemüht, renommierte Fachleute auf diesem Gebiet mit dem Unterricht des Programms zu beauftragen, um den Studenten die besten Fähigkeiten zu vermitteln, die sie benötigen, um sich bei der Gestaltung des Schutzes eines jeden Unternehmens wirksam zu entwickeln.





“

*Dieses Programm ist genau das, was Sie brauchen: Sie werden die besten Spezialisten für IT-Sicherheit auf internationaler Ebene an Ihrer Seite haben"*

## 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. Nogales Ávila, Javier

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

### Hr. 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

### Fr. Jurado Jabonero, Lorena

- ◆ Leitung der Informationssicherheit (CISO) bei Grupo Pascual
- ◆ Hochschulabschluss in Computertechnik an der Universität Alfonso X El Sabio
- ◆ Technische Ingenieurin in Computer Management von der Polytechnischen Universität von Madrid
- ◆ Kenntnisse: ISO 27001, ISO 27701, ISO 22301, ISO 20000, RGPD/LOPDGDD, NIST CSF, CSA, ITIL, PCI, usw.

# 04

## Struktur und Inhalt

Um die vorgeschlagenen Ziele zu erreichen, wurde dieser Universitätsexperte in IT-Sicherheit in 3 spezialisierte Module unterteilt, die in 450 Lernstunden absolviert werden können. So wird der Informatiker im Laufe dieses Programms die neuesten Fortschritte in der Computersicherheit in der Kommunikation und im Softwarebetrieb, die Sicherheit in *Cloud Computing*-Umgebungen, die Sicherheit von Speichersystemen oder Autorisierungssystemen und viele andere relevante Aspekte in diesem Bereich kennenlernen.



“

*Dieses Programm wird Sie in die Lage versetzen,  
die besten forensischen Analysetechniken im  
Bereich der IT-Sicherheit anzuwenden"*

## Modul 1. Sicherheit in Design und Entwicklung von Systemen

- 1.1. Informationssysteme
  - 1.1.1. Domains eines Informationssystems
  - 1.1.2. Komponenten eines Informationssystems
  - 1.1.3. Aktivitäten eines Informationssystems
  - 1.1.4. Lebenszyklus eines Informationssystems
  - 1.1.5. Ressourcen eines Informationssystems
- 1.2. Informationssysteme. Typologie
  - 1.2.1. Typen von Informationssystemen
    - 1.2.1.1. Unternehmerisch
    - 1.2.1.2. Strategisch
    - 1.2.1.3. Je nach Anwendungsbereich
    - 1.2.1.4. Spezifisch
  - 1.2.2. Informationssysteme. Beispiele aus der Praxis
  - 1.2.3. Entwicklung von Informationssystemen: Etappen
  - 1.2.4. Methoden von Informationssystemen
- 1.3. Sicherheit von Informationssystemen. Rechtliche Implikationen
  - 1.3.1. Zugang zu Daten
  - 1.3.2. Sicherheitsbedrohungen: Schwachstellen
  - 1.3.3. Rechtliche Implikationen: Straftaten
  - 1.3.4. Verfahren zur Wartung von Informationssystemen
- 1.4. Sicherheit von Informationssystemen. Sicherheitsprotokolle
  - 1.4.1. Sicherheit von Informationssystemen
    - 1.4.1.1. Integrität
    - 1.4.1.2. Vertraulichkeit
    - 1.4.1.3. Verfügbarkeit
    - 1.4.1.4. Authentifizierung
  - 1.4.2. Sicherheitsdienste
  - 1.4.3. Protokolle zur Informationssicherheit. Typologie
  - 1.4.4. Empfindlichkeit von Informationssystemen
- 1.5. Sicherheit von Informationssystemen. Maßnahmen und Systeme zur Zugangskontrolle
  - 1.5.1. Sicherheitsmaßnahmen
  - 1.5.2. Art der Sicherheitsmaßnahmen
    - 1.5.2.1. Prävention
    - 1.5.2.2. Erkennung
    - 1.5.2.3. Korrektheit
  - 1.5.3. Kontrollsysteme für den Zugang. Typologie
  - 1.5.4. Kryptographie
- 1.6. Netzwerk- und Internetsicherheit
  - 1.6.1. *Firewalls*
  - 1.6.2. Digitale Identifizierung
  - 1.6.3. Viren und Würmer
  - 1.6.4. *Hacking*
  - 1.6.5. Beispiele und reale Fälle
- 1.7. Computerkriminalität
  - 1.7.1. Computerkriminalität
  - 1.7.2. Computerkriminalität. Typologie
  - 1.7.3. Computerkriminalität. Angriff. Typologien
  - 1.7.4. Der Fall der virtuellen Realität
  - 1.7.5. Profile von Tätern und Opfern. Typisierung von Verbrechen
  - 1.7.6. Computerkriminalität. Beispiele und reale Fälle
- 1.8. Sicherheitsplan für ein Informationssystem
  - 1.8.1. Sicherheitsplan. Ziele
  - 1.8.2. Sicherheitsplan. Planung
  - 1.8.3. Risikoplan. Analyse
  - 1.8.4. Sicherheitspolitik. Implementierung in der Organisation
  - 1.8.5. Sicherheitsplan. Implementierung in der Organisation
  - 1.8.6. Sicherheitsverfahren. Typen
  - 1.8.7. Sicherheitsplan. Beispiele

- 1.9. Plan für unvorhergesehene Ereignisse
  - 1.9.1. Plan für unvorhergesehene Ereignisse. Funktionen
  - 1.9.2. Notfallplan: Elemente und Ziele
  - 1.9.3. Plan für unvorhergesehene Ereignisse in der Organisation. Implementierung
  - 1.9.4. Plan für unvorhergesehene Ereignisse. Beispiele
- 1.10. Verwaltung der Sicherheit von Informationssystemen
  - 1.10.1. Gesetzliche Bestimmungen
  - 1.10.2. Normen
  - 1.10.3. Zertifizierungen
  - 1.10.4. Technologien

## Modul 2. Sicherheit bei Kommunikation und Softwarebetrieb

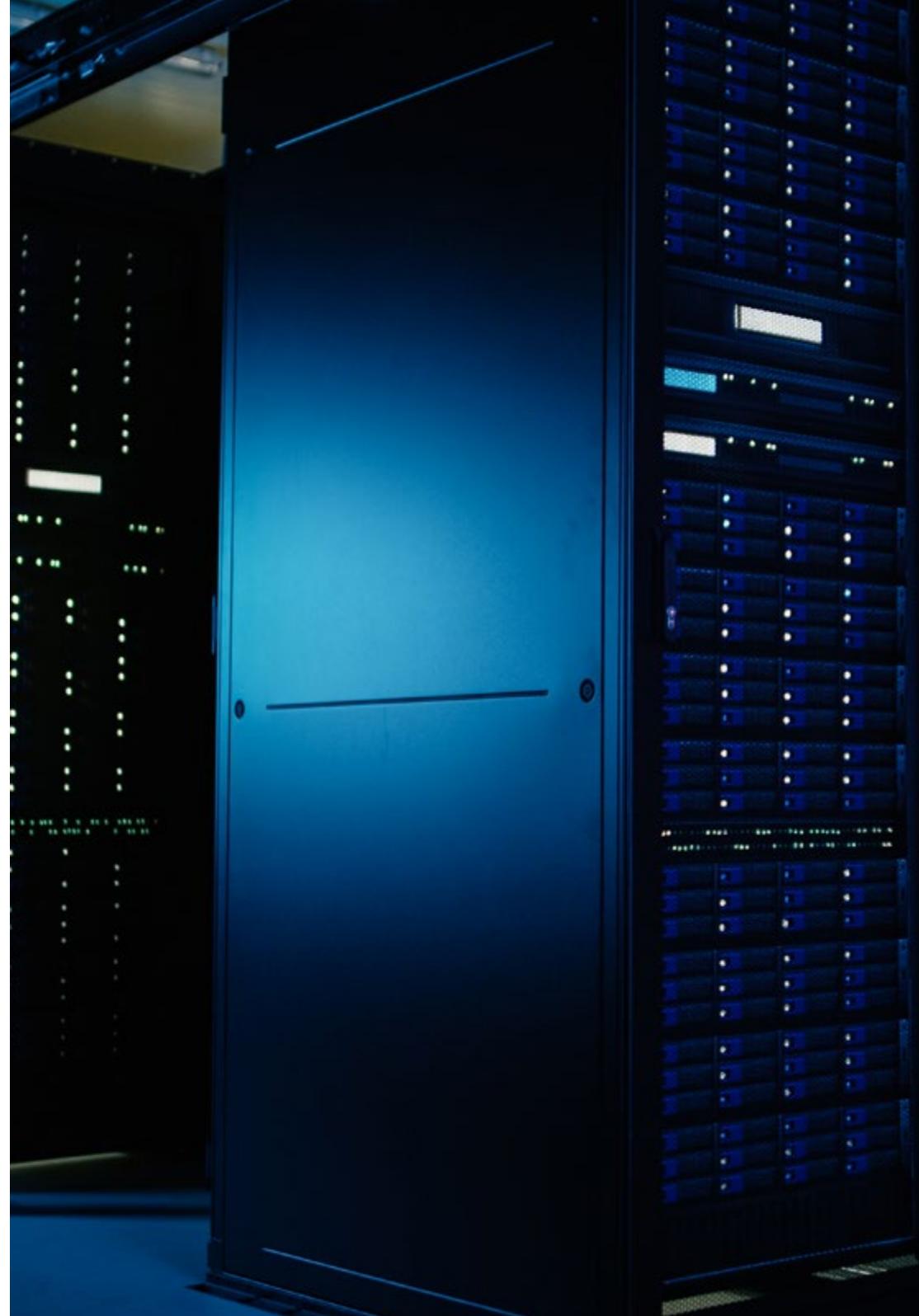
- 2.1. Computersicherheit bei Kommunikation und Softwarebetrieb
  - 2.1.1. Computersicherheit
  - 2.1.2. Cybersecurity
  - 2.1.3. Cloud-Sicherheit
- 2.2. Computersicherheit in der Kommunikation und im Softwarebetrieb. Typologie
  - 2.2.1. Physische Sicherheit
  - 2.2.2. Logische Sicherheit
- 2.3. Sicherheit in der Kommunikation
  - 2.3.1. Wichtigste Elemente
  - 2.3.2. Netzwerksicherheit
  - 2.3.3. Bewährte Praktiken
- 2.4. Cyberintelligenz
  - 2.4.1. Social Engineering
  - 2.4.2. *Deep web*
  - 2.4.3. *Phishing*
  - 2.4.4. *Malware*
- 2.5. Sichere Entwicklung in Kommunikation und Softwarebetrieb
  - 2.5.1. Sichere Entwicklung. HTTP-Protokoll
  - 2.5.2. Sichere Entwicklung. Lebenszyklus
  - 2.5.3. Sichere Entwicklung. PHP-Sicherheit
  - 2.5.4. Sichere Entwicklung. NET-Sicherheit
  - 2.5.5. Sichere Entwicklung. Bewährte Praktiken

- 2.6. Informationssicherheits-Managementsysteme in Kommunikation und Software
  - 2.6.1. GDPR
  - 2.6.2. ISO 27021
  - 2.6.3. ISO 27017/18
- 2.7. SIEM-Technologien
  - 2.7.1. SIEM-Technologien
  - 2.7.2. SOC Betrieb
  - 2.7.3. SIEM *Vendors*
- 2.8. Die Rolle der Sicherheit in Organisationen
  - 2.8.1. Rollen in Organisationen
  - 2.8.2. Die Rolle von IoT-Spezialisten in Unternehmen
  - 2.8.3. Anerkannte Zertifizierungen auf dem Markt
- 2.9. Forensische Analyse
  - 2.9.1. Forensische Analyse
  - 2.9.2. Forensische Analyse. Methodik
  - 2.9.3. Forensische Analyse. Tools und Implementierung
- 2.10. Cybersecurity heute
  - 2.10.1. Große Cyberangriffe
  - 2.10.2. Prognosen zur Beschäftigungsfähigkeit
  - 2.10.3. Herausforderungen

## Modul 3. Sicherheit in *Cloud*-Umgebungen

- 3.1. Sicherheit in *Cloud Computing*-Umgebungen
  - 3.1.1. Sicherheit in *Cloud Computing*-Umgebungen
  - 3.1.2. Sicherheit in *Cloud Computing*-Umgebungen. Bedrohungen und Sicherheitsrisiken
  - 3.1.3. Sicherheit in *Cloud Computing*-Umgebungen. Wichtige Sicherheitsaspekte
- 3.2. Arten von *Cloud* Infrastruktur
  - 3.2.1. Publikum
  - 3.2.2. Öffentlich
  - 3.2.3. Privat

- 3.3. Hybrid
  - 3.3.1. Vom Anbieter verwaltete Sicherheitselemente
  - 3.3.2. Vom Kunden verwaltete Elemente
  - 3.3.3. Definition der Sicherheitsstrategie
- 3.4. Mechanismen der Prävention
  - 3.4.1. Authentifizierungs-Management-Systeme
  - 3.4.2. Berechtigungsverwaltungssystem: Zugriffsrichtlinien
  - 3.4.3. Systeme zur Schlüsselverwaltung
- 3.5. Verbriefung von Systemen
  - 3.5.1. Verbriefung von Speichersystemen
  - 3.5.2. Sicherung von Datenbanksystemen
  - 3.5.3. Sichern von Daten bei der Übermittlung
- 3.6. Schutz der Infrastruktur
  - 3.6.1. Entwurf und Implementierung eines sicheren Netzwerks
  - 3.6.2. Sicherheit von Computerressourcen
  - 3.6.3. Tools und Ressourcen zum Schutz der Infrastruktur
- 3.7. Erkennung von Bedrohungen und Angriffen
  - 3.7.1. Auditing, *Logging* und Überwachungssysteme
  - 3.7.2. Ereignis- und Alarmsysteme
  - 3.7.3. SIEM-Systeme
- 3.8. Reaktion auf Vorfälle
  - 3.8.1. Plan zur Reaktion auf Vorfälle
  - 3.8.2. Geschäftskontinuität
  - 3.8.3. Forensische Analyse und Behebung von Vorfällen der gleichen Art



- 3.9. Sicherheit in öffentlichen *Clouds*
  - 3.9.1. AWS (Amazon Web Services)
  - 3.9.2. Microsoft Azure
  - 3.9.3. Google GCP
  - 3.9.4. Oracle Cloud
- 3.10. Regulierung und Compliance
  - 3.10.1. Compliance im Bereich Sicherheit
  - 3.10.2. Risikomanagement
  - 3.10.3. Menschen und Prozesse in Organisationen

“

*Der vollständigste und aktuellste Lehrplan auf dem Markt ist jetzt in Ihrer Reichweite. Schreiben Sie sich ein, Sie werden es nicht bereuen"*

# 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 IT-Sicherheit 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 IT-Sicherheit** 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 Technologische 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 IT-Sicherheit**

Anzahl der offiziellen Arbeitsstunden: **450 Std.**



\*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.

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  
IT-Sicherheit

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

# Universitätsexperte IT-Sicherheit