

Universitätsexperte

Sicherheit in der Software-Entwicklung



## Universitätsexperte Sicherheit in der Software-Entwicklung

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

Internetzugang: [www.techtute.com/de/informatik/spezialisierung/spezialisierung-sicherheit-software-entwicklung](http://www.techtute.com/de/informatik/spezialisierung/spezialisierung-sicherheit-software-entwicklung)

# 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

Dieser hochwertige Studiengang ermöglicht es den Studenten, den Prozess der Informationssicherheit und seine Auswirkungen auf die Vertraulichkeit, Integrität, Verfügbarkeit und die wirtschaftlichen Kosten sowie die Probleme im Zusammenhang mit der Softwaresicherheit, ihren Schwachstellen und ihrer Klassifizierung zu verstehen.

Dank dieses Programms, das sich durch eine hohe wissenschaftliche Präzision auszeichnet, erwerben die Studenten die Kenntnisse, die für die interne Kontrolle der Informatik sowie für die Bewertung und Aufdeckung der Schwachstellen von Online-Anwendungen erforderlich sind.



“

*Spezialisieren Sie sich auf  
Computersysteme mit Fachleuten,  
die über umfassende Erfahrung in  
diesem Bereich verfügen”*

Dieser komplette Studiengang in Sicherheit in der Software-Entwicklung bietet IT-Fachkräften die Möglichkeit, fundierte Kenntnisse und eine Fortbildung in der Verwaltung und Überwachung von qualitativ hochwertiger und sicherer Software zu erwerben, die vordefinierten Anforderungen entspricht.

Dieser Universitätsexperte ist auf Studenten im Bereich Sicherheit in der Software-Entwicklung spezialisiert, um ihnen die Kenntnisse und Werkzeuge zu vermitteln, die für den Entwurf und die Kontrolle komplexer Systeme erforderlich sind, die eine zuverlässige Antwort auf die gestellten Probleme bieten.

Das Hauptziel dieser Weiterbildung besteht darin, die Studenten in die Lage zu versetzen, wesentliche qualitative Verbesserungen vorzunehmen, die neue Lösungen für die spezifischen Probleme bieten, mit denen sie konfrontiert werden. Sie zielt auch darauf ab, Fachleute fortzubilden, die in der Lage sind, einen systematischen und quantifizierbaren Ansatz für die Entwicklung und Wartung von Software zu verwenden, und die außerdem vertiefte Kenntnisse in der Computerprogrammierung, der Implementierung und der Planung von Computersystemen aus einer praktischen und an die aktuelle Realität angepassten Perspektive erwerben.

Mit diesem Studiengang verfügen Sie über die modernsten Lehrmittel und haben die Möglichkeit, einen Lehrplan zu absolvieren, der die besten Kenntnisse in diesem Bereich vereint. Eine Gruppe von wissenschaftlich hochkarätigen Dozenten mit umfangreicher internationaler Erfahrung vermittelt Ihnen die umfassendsten und aktuellsten Informationen über die neuesten Fortschritte und Techniken im Bereich des *Software Engineering* und der Informationssysteme.

Der Lehrplan deckt die wichtigsten aktuellen Themen im Bereich Sicherheit in der Software-Entwicklung so ab, dass die Studenten darauf vorbereitet sind, in diesem Bereich zu arbeiten. Es handelt sich also nicht nur um einen weiteren Titel in der Tasche, sondern um ein echtes Lernwerkzeug, mit dem die Themen des Fachgebiets auf moderne, objektive Weise und mit der Fähigkeit, sie auf der Grundlage der neuesten Informationen zu beurteilen, angegangen werden können.

Da es sich um einen 100%igen Online-Experten handelt, ist man nicht an feste Zeiten oder die Notwendigkeit, sich an einen anderen physischen Ort zu begeben, gebunden, sondern kann zu jeder Tageszeit auf die Inhalte zugreifen und so sein Arbeits- oder Privatleben mit seinem akademischen Leben in Einklang bringen.

Wer sich von anderen abheben will und in der Lage sein möchte, komplexe systemtechnische Projekte zu entwerfen und zu entwickeln, liegt mit diesem Programm genau richtig.

Dieser **Universitätsexperte in Sicherheit in der Software-Entwicklung** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

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



*Der Erwerb dieses Universitätsexperten wird den Fachleuten der Sicherheit in der Software-Entwicklung die Möglichkeit geben, an der Spitze der neuesten Entwicklungen in diesem Sektor zu stehen*

“

*Dieser Universitätsexperte ist die beste Investition, die Sie bei der Auswahl eines Auffrischungsprogramms im Bereich der Sicherheit in der Software-Entwicklung tätigen können. TECH bietet Ihnen Qualität und freien Zugang zu den Inhalten"*

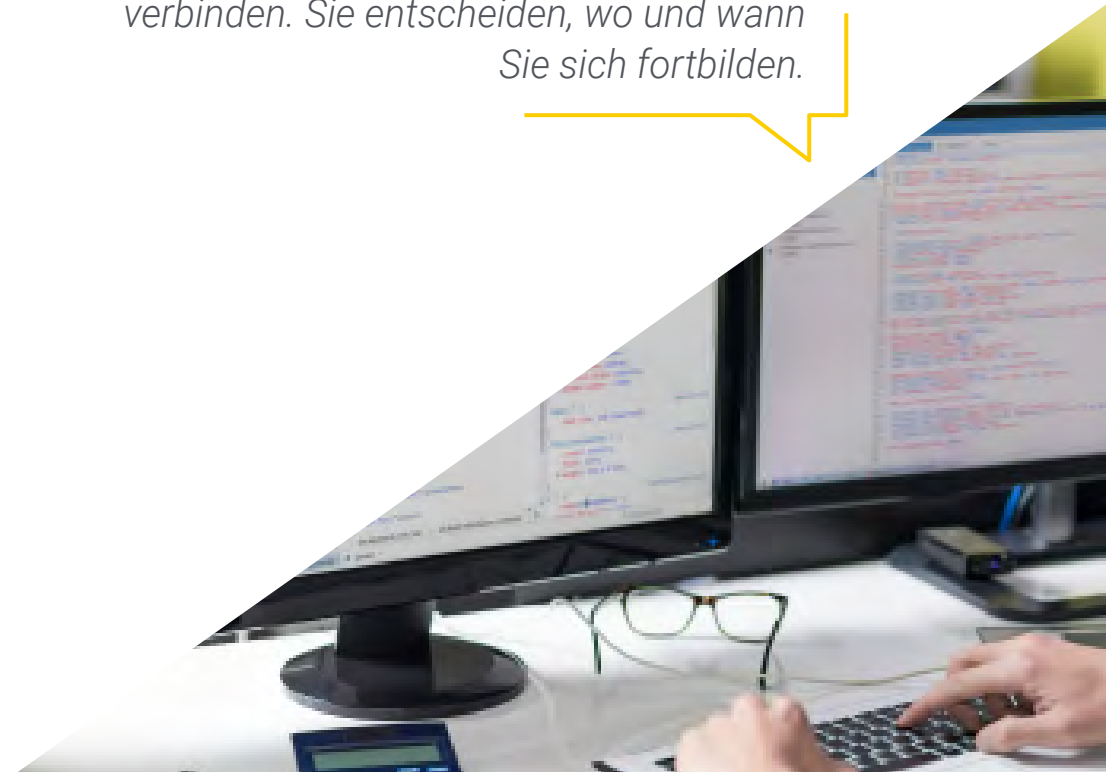
Das Dozententeam besteht aus Experten aus dem Bereich der Sicherheit in der Software-Entwicklung, die ihre Berufserfahrung in diese Fortbildung einbringen, sowie aus anerkannten Fachleuten aus führenden Unternehmen und renommierten Universitäten.

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

Das Konzept dieses Programms konzentriert sich auf problemorientiertes Lernen, bei dem die Fachkraft versuchen muss, die verschiedenen Situationen aus der beruflichen Praxis zu lösen, die während des gesamten Studiengangs gestellt werden. Dazu steht ihr ein innovatives interaktives Videosystem zur Verfügung, das von anerkannten und erfahrenen Experten für Sicherheit in der Software-Entwicklung erarbeitet wurde.

*Diese Fortbildung verfügt über das beste didaktische Material, das Ihnen ein kontextbezogenes Studium ermöglicht, das Ihr Lernen erleichtern wird.*

*Dieser 100%ige Online-Universitätsexperte wird es Ihnen ermöglichen, Ihr Studium mit Ihrer beruflichen Tätigkeit zu verbinden. Sie entscheiden, wo und wann Sie sich fortbilden.*



# 02 Ziele

Das Programm in Sicherheit in der Software-Entwicklung zielt darauf ab, die Leistung von Fachleuten zu erleichtern, damit sie sich die wichtigsten neuen Erkenntnisse in diesem Bereich aneignen und erlernen können, die es ihnen ermöglichen, ihren Beruf mit höchster Qualität und Professionalität auszuüben.







“

*Das Ziel von TECH ist es, dass Sie die beste Fachkraft in Ihrem Bereich werden. Und dafür hat sie die beste Methodik und den besten Inhalt"*



## Allgemeine Ziele

---

- ◆ Erwerben neuer Kenntnisse im Bereich Sicherheit in der Software-Entwicklung
- ◆ Erwerben neuer Fähigkeiten in Bezug auf neue Technologien und die neuesten Software-Entwicklungen
- ◆ Bearbeiten der Daten, die bei der Software-Entwicklung anfallen

“

*Durch die Verbesserung Ihrer Fähigkeiten im Bereich der Sicherheit in der Software-Entwicklung werden Sie wettbewerbsfähiger sein. Bilden Sie sich weiter und bringen Sie Ihre Karriere in Schwung"*





## Spezifische Ziele

---

### Modul 1. Sicherheitsmanagement

- ◆ Kennen des Prozesses der Informationssicherheit, seiner Auswirkungen auf Vertraulichkeit, Integrität, Verfügbarkeit und wirtschaftliche Kosten
- ◆ Erlernen der Anwendung bewährter Sicherheitspraktiken bei der Verwaltung von Informationstechnologiediensten
- ◆ Aneignen von Kenntnissen für die ordnungsgemäße Zertifizierung von Sicherheitsprozessen
- ◆ Verstehen von Authentifizierungsmechanismen und -methoden für die Zugangskontrolle sowie den Prozess der Zugangsprüfung
- ◆ Verstehen von Sicherheitsmanagementprogrammen, Risikomanagement und der Gestaltung von Sicherheitsstrategien
- ◆ Erlernen von Geschäftscontinuitätsplänen, ihren Phasen und ihrem Wartungsprozess
- ◆ Kennen der Verfahren für den korrekten Schutz des Unternehmens durch DMZ-Netze, den Einsatz von Systemen zur Erkennung von Eindringlingen und andere Methoden

### Modul 2. Softwaresicherheit

- ◆ Verstehen der Probleme im Zusammenhang mit der Softwaresicherheit, ihrer Schwachstellen und deren Klassifizierung
- ◆ Kennen der Entwurfsgrundsätze, Methoden und Standards der Softwaresicherheit
- ◆ Verstehen der Anwendung von Sicherheit in den verschiedenen Phasen des Software-Lebenszyklus
- ◆ Aneignen der erforderlichen Kenntnisse für sichere Softwarecodierung und Validierungstechniken
- ◆ Aneignen der Methoden und Verfahren zur Gewährleistung der Sicherheit bei der Entwicklung und Bereitstellung von *Cloud*-Diensten
- ◆ Verstehen der Grundlagen der Kryptologie und der verschiedenen derzeit verfügbaren Verschlüsselungstechniken

### Modul 3. Sicherheitsprüfung

- ◆ Aneignen der Kenntnisse, die für die korrekte Durchführung des internen IT-Prüfungs- und Kontrollprozesses erforderlich sind
- ◆ Verstehen der für die Sicherheitsüberprüfung von Systemen und Netzen durchzuführenden Verfahren
- ◆ Verstehen der verschiedenen Hilfsmittel, Methoden und anschließenden Analysen während der Sicherheitsprüfung von Internet und mobilen Geräten
- ◆ Erlernen der Eigenschaften und Einflussfaktoren, die Geschäftsrisiken bedingen und die richtige Umsetzung eines angemessenen Risikomanagements bestimmen
- ◆ Erlernen von Maßnahmen zur Risikominderung sowie von Methoden zur Umsetzung eines Informationssicherheitsmanagementsystems und der zu verwendenden Vorschriften und Normen
- ◆ Verstehen der Verfahren zur Durchführung eines Sicherheitsaudits, seiner Nachvollziehbarkeit und der Präsentation der Ergebnisse

### Modul 4. Sicherheit bei Online-Anwendungen

- ◆ Aneignen der erforderlichen Kenntnisse zur Bewertung und Erkennung von Schwachstellen in Online-Anwendungen
- ◆ Verstehen der Sicherheitsrichtlinien und -standards, die auf Online-Anwendungen anzuwenden sind
- ◆ Erlernen der Verfahren, die bei der Entwicklung von Web-Applikationen und ihrer anschließenden Validierung durch Analyse und Sicherheitstests anzuwenden sind
- ◆ Erlernen der Sicherheitsmaßnahmen für die Bereitstellung und Produktion von Web-Applikationen
- ◆ Verstehen der Konzepte, Funktionen und Technologien, die bei der Sicherheit von Webdiensten anzuwenden sind, sowie der Sicherheitstests und Schutzmaßnahmen
- ◆ Aneignen der Verfahren für ethisches Hacking, Malware-Analyse und forensische Analyse
- ◆ Kennen der Maßnahmen zur Abschwächung und Eindämmung von Zwischenfällen bei Webdiensten
- ◆ Aneignen von Kenntnissen über die Anwendung von *Best-Practice*-Techniken für die Entwicklung und Implementierung von Online-Anwendungen sowie über die häufigsten Fehler

# 03

## Kursleitung

Dieses akademische Programm verfügt über den spezialisiertesten Lehrkörper auf dem aktuellen Bildungsmarkt. Es handelt sich um Spezialisten, die von TECH ausgewählt wurden, um den gesamten Studiengang zu entwickeln. Auf diese Weise haben sie auf der Grundlage ihrer eigenen Erfahrung und der neuesten Erkenntnisse die aktuellsten Inhalte entworfen, die eine Qualitätsgarantie für ein so relevantes Thema bieten.



“

*TECH bietet Ihnen den spezialisiertesten  
Lehrkörper in diesem Fachgebiet. Schreiben  
Sie sich jetzt ein und genießen Sie die  
Qualität, die Sie verdienen”*



## Internationaler Gastdirektor

Darren Pulsipher ist ein sehr erfahrener Softwarearchitekt, ein Innovator mit einer hervorragenden internationalen Erfolgsbilanz in der Software- und Firmwareentwicklung. Er verfügt über hoch entwickelte Kommunikations-, Projektmanagement- und Geschäftsfähigkeiten, die es ihm ermöglicht haben, große globale Initiativen zu leiten.

Im Laufe seiner Karriere hatte er auch leitende Positionen mit großer Verantwortung inne, wie z. B. die des Chefarchitekten für Lösungen für den öffentlichen Sektor bei der Intel Corporation, wo er moderne Geschäfte, Prozesse und Technologien für Kunden, Partner und Benutzer im öffentlichen Sektor vorantrieb. Darüber hinaus gründete er Yoly Inc., wo er auch als CEO fungierte, und arbeitete an der Entwicklung eines Tools zur Aggregation und Diagnose sozialer Netzwerke auf der Grundlage von Software as a Service (SaaS), das Big Data und Web 2.0-Technologien nutzt.

Darüber hinaus war er in anderen Unternehmen tätig, unter anderem als leitender Ingenieur bei Dell Technologies, wo er die Abteilung Big Data in der Cloud leitete und Teams in den USA und China führte, um große Projekte zu verwalten und Geschäftsbereiche für eine erfolgreiche Integration umzustrukturieren. Er war auch Chief Information Officer bei XanGo, wo er Projekte wie Helpdesk-Support, Produktionssupport und Lösungsentwicklung leitete.

Zu den vielen Spezialgebieten, in denen er Experte ist, gehören Edge-to-Cloud-Technologie, Cybersicherheit, generative künstliche Intelligenz, Softwareentwicklung, Netzwerktechnologie, Cloud-native Entwicklung und das Container-Ökosystem. Sein Wissen gibt er über den wöchentlichen Podcast und die Newsletter „Embracing Digital Transformation“ weiter, die er produziert und präsentiert hat und die Organisationen dabei helfen, die digitale Transformation durch den Einsatz von Menschen, Prozessen und Technologie erfolgreich zu meistern.



## Hr. Pulsipher, Darren

---

- Chefarchitekt für Lösungen für den öffentlichen Sektor bei Intel, Kalifornien, USA
- Moderator und Produzent von „Embracing Digital Transformation“, Kalifornien
- Gründer und CEO von Yoly Inc., Arkansas
- Leitender Ingenieur bei Dell Technologies, Arkansas
- Chief Information Officer bei XanGo, Utah
- Leitender Architekt bei Cadence Design Systems, Kalifornien
- Leitender Projektprozessmanager bei Lucent Technologies, Kalifornien
- Software-Ingenieur bei Cemax-Icon, Kalifornien
- Software-Ingenieur bei ISG Technologies, Kanada
- MBA in Technologiemanagement von der Universität von Phoenix
- Hochschulabschluss in Informatik und Elektrotechnik von der Brigham Young University

“

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

# 04

## Struktur und Inhalt

Die Struktur der Inhalte wurde von den besten Fachleuten für Softwaresicherheit entworfen, die über umfangreiche Erfahrung und anerkanntes Ansehen in ihrem Beruf verfügen und sich der Vorteile bewusst sind, die die neueste Bildungstechnologie für die Hochschulbildung bringen kann.





“

*TECH verfügt über das vollständigste und aktuellste wissenschaftliche Programm auf dem Markt. TECH strebt nach Exzellenz und will, dass auch Sie sie erreichen”*

## Modul 1. Sicherheitsmanagement

- 1.1. Informationssicherheit
  - 1.1.1. Einführung
  - 1.1.2. Die Sicherheit von Informationen setzt Vertraulichkeit, Integrität und Verfügbarkeit voraus
  - 1.1.3. Sicherheit ist eine wirtschaftliche Frage
  - 1.1.4. Sicherheit ist ein Prozess
  - 1.1.5. Die Klassifizierung von Informationen
  - 1.1.6. Informationssicherheit ist Risikomanagement
  - 1.1.7. Sicherheit ist mit Sicherheitskontrollen verbunden
  - 1.1.8. Sicherheit ist sowohl physisch als auch logisch
  - 1.1.9. Sicherheit betrifft Menschen
- 1.2. Die Fachkraft für Informationssicherheit
  - 1.2.1. Einführung
  - 1.2.2. Informationssicherheit als Beruf
  - 1.2.3. Zertifizierungen (ISC)2
  - 1.2.4. Die Norm ISO 27001
  - 1.2.5. Bewährte Sicherheitspraktiken im IT-Service-Management
  - 1.2.6. Reifegradmodelle für die Informationssicherheit
  - 1.2.7. Andere Zertifizierungen, Standards und professionelle Ressourcen
- 1.3. Zugangskontrolle
  - 1.3.1. Einführung
  - 1.3.2. Anforderungen an die Zugangskontrolle
  - 1.3.3. Authentifizierungsmechanismen
  - 1.3.4. Genehmigungsverfahren
  - 1.3.5. Zugang zu Buchhaltung und Rechnungsprüfung
  - 1.3.6. *Triple A*-Technologien
- 1.4. Programme, Verfahren und Richtlinien zur Informationssicherheit
  - 1.4.1. Einführung
  - 1.4.2. Programme für das Sicherheitsmanagement
  - 1.4.3. Risikomanagement
  - 1.4.4. Gestaltung der Sicherheitspolitik
- 1.5. Pläne zur Aufrechterhaltung des Geschäftsbetriebs
  - 1.5.1. Einführung in BCPs
  - 1.5.2. Phase I und II
  - 1.5.3. Phase III und IV
  - 1.5.4. Aufrechterhaltung der BCP
- 1.6. Verfahren für den korrekten Schutz des Unternehmens
  - 1.6.1. DMZ-Netzwerke
  - 1.6.2. Systeme zur Erkennung von Eindringlingen
  - 1.6.3. Zugriffskontrolllisten
  - 1.6.4. Vom Angreifer lernen: *Honeypot*
- 1.7. Sicherheitsarchitektur. Prävention
  - 1.7.1. Überblick. Aktivitäten und Schichtenmodell
  - 1.7.2. Perimeter-Verteidigung (*Firewalls*, WAFs, IPS etc...)
  - 1.7.3. Endpunktschutz (Geräte, Server und Dienste)
- 1.8. Sicherheitsarchitektur. Erkennung
  - 1.8.1. Überblick über Erkennung und Überwachung
  - 1.8.2. *Logs*, verschlüsselte Verkehrsunterbrechung, Aufzeichnung und *Siems*
  - 1.8.3. Warnungen und Informationen
- 1.9. Sicherheitsarchitektur. Reaktion
  - 1.9.1. Reaktion. Produkte, Dienstleistungen und Ressourcen
  - 1.9.2. Management von Zwischenfällen
  - 1.9.3. CERTS und CSIRTs
- 1.10. Sicherheitsarchitektur. Wiederherstellung
  - 1.10.1. Ausfallsicherheit, Konzepte, Geschäftsanforderungen und Vorschriften
  - 1.10.2. IT-Resilienz-Lösungen
  - 1.10.3. Krisenmanagement und Governance

## Modul 2. Softwaresicherheit

- 2.1. Software-Sicherheitsprobleme
  - 2.1.1. Einführung in die Problematik der Softwaresicherheit
  - 2.1.2. Schwachstellen und ihre Klassifizierung
  - 2.1.3. Sichere Software-Eigenschaften
  - 2.1.4. Referenzen
- 2.2. Grundsätze des Software-Sicherheitsdesigns
  - 2.2.1. Einführung
  - 2.2.2. Grundsätze des Software-Sicherheitsdesigns
  - 2.2.3. Arten von S-SDLC
  - 2.2.4. Softwaresicherheit in S-SDLC-Phasen
  - 2.2.5. Methodologien und Normen
  - 2.2.6. Referenzen
- 2.3. Sicherheit im Software-Lebenszyklus in der Anforderungs- und Entwurfsphase
  - 2.3.1. Einführung
  - 2.3.2. Angriffsmodellierung
  - 2.3.3. Missbrauchsfälle
  - 2.3.4. Entwicklung von Sicherheitsanforderungen
  - 2.3.5. Risikoanalyse. Architektonisch
  - 2.3.6. Entwurfsmuster
  - 2.3.7. Referenzen
- 2.4. Sicherheit im Software-Lebenszyklus in den Phasen Kodierung, Test und Betrieb
  - 2.4.1. Einführung
  - 2.4.2. Risikobasierte Sicherheitsprüfungen
  - 2.4.3. Code-Überprüfung
  - 2.4.4. Penetrationstests
  - 2.4.5. Sicherheitsmaßnahmen
  - 2.4.6. Externe Überprüfung
  - 2.4.7. Referenzen
- 2.5. Sichere Kodierungsanwendungen I
  - 2.5.1. Einführung
  - 2.5.2. Sichere Kodierungspraktiken
  - 2.5.3. Eingabeverarbeitung und Validierung
  - 2.5.4. Speicherüberlauf
  - 2.5.5. Referenzen
- 2.6. Sichere Kodierungsanwendungen II
  - 2.6.1. Einführung
  - 2.6.2. *Integers Overflows*, Abbruchfehler und Probleme mit Typkonvertierungen zwischen Ganzzahlen
  - 2.6.3. Fehler und Ausnahmen
  - 2.6.4. Datenschutz und Vertraulichkeit
  - 2.6.5. Privilegierte Programme
  - 2.6.6. Referenzen
- 2.7. Sicherheit in der Entwicklung und in der Cloud
  - 2.7.1. Entwicklungssicherheit; Methodik und Praxis
  - 2.7.2. PaaS, IaaS, CaaS und SaaS-Modelle
  - 2.7.3. Sicherheit in der Cloud und für Cloud-Dienste
- 2.8. Verschlüsselung
  - 2.8.1. Grundlagen der Kryptologie
  - 2.8.2. Symmetrische und asymmetrische Verschlüsselung
  - 2.8.3. Verschlüsselung im Ruhezustand und bei der Übermittlung
- 2.9. Orchestrierung und Automatisierung der Sicherheit (SOAR)
  - 2.9.1. Komplexität der manuellen Verarbeitung; Notwendigkeit der Automatisierung von Aufgaben
  - 2.9.2. Produkte und Dienstleistungen
  - 2.9.3. SOAR-Architektur
- 2.10. Sicherheit der Telearbeit
  - 2.10.1. Bedarf und Szenarien
  - 2.10.2. Produkte und Dienstleistungen
  - 2.10.3. Sicherheit der Telearbeit

### Modul 3. Sicherheitsprüfung

- 3.1. Einführung in Informationssysteme und deren Prüfung
  - 3.1.1. Einführung in Informationssysteme und die Rolle der IT-Prüfung
  - 3.1.2. Definitionen der Begriffe "IT-Audit" und "interne IT-Kontrolle"
  - 3.1.3. Funktionen und Ziele der IT-Prüfung
  - 3.1.4. Unterschiede zwischen interner Kontrolle und IT-Audit
- 3.2. Interne Kontrolle von Informationssystemen
  - 3.2.1. Funktionsschema eines Datenverarbeitungszentrums
  - 3.2.2. Klassifizierung der Kontrollen von Informationssystemen
  - 3.2.3. Die Goldene Regel
- 3.3. Der Prozess und die Phasen der Prüfung von Informationssystemen
  - 3.3.1. Risikobewertung (RRA) und andere IT-Prüfungsmethoden
  - 3.3.2. Durchführung einer Prüfung der Informationssysteme. Prüfungsphasen
  - 3.3.3. Grundlegende Fähigkeiten des Wirtschaftsprüfers für Informationssysteme
- 3.4. Technische Sicherheitsüberprüfung von Systemen und Netzen
  - 3.4.1. Technische Sicherheitsaudits. Penetrationstests. Vorläufige Konzepte
  - 3.4.2. Audits der Systemsicherheit. Hilfsmittel
  - 3.4.3. Audits der Netzwerksicherheit. Hilfsmittel
- 3.5. Technische Prüfung der Sicherheit von Internet und mobilen Geräten
  - 3.5.1. Internet-Sicherheitprüfung. Hilfsmittel
  - 3.5.2. Prüfung der Sicherheit von mobilen Geräten. Hilfsmittel
  - 3.5.3. Anhang 1. Aufbau des Kurzberichts und des technischen Berichts
  - 3.5.4. Anhang 2. Inventar der Werkzeuge
  - 3.5.5. Anhang 3. Methoden
- 3.6. Managementsystem für die Informationssicherheit
  - 3.6.1. IS-Sicherheit: Eigenschaften und Einflussfaktoren
  - 3.6.2. Unternehmensrisiken und Risikomanagement: Implementierung von Kontrollen
  - 3.6.3. Informationssicherheitsmanagementsystem (ISMS): Konzept und kritische Erfolgsfaktoren
  - 3.6.4. ISMS - PDCA-Modell
  - 3.6.5. ISMS ISO-IEC 27001: organisatorischer Kontext
  - 3.6.6. Abschnitt 4. Organisatorischer Kontext
  - 3.6.7. Abschnitt 5. Führung
  - 3.6.8. Abschnitt 6. Planung
  - 3.6.9. Abschnitt 7. Support
  - 3.6.10. Abschnitt 8. Operation
  - 3.6.11. Abschnitt 9. Leistungsbewertung
  - 3.6.12. Abschnitt 10. Verbesserung
  - 3.6.13. Anhang zu ISO 27001/ISO-IEC 27002: Zielsetzungen und Kontrollen
  - 3.6.14. ISMS-Audit
- 3.7. Durchführung der Prüfung
  - 3.7.1. Verfahren
  - 3.7.2. Techniken
- 3.8. Rückverfolgbarkeit
  - 3.8.1. Methoden
  - 3.8.2. Analyse
- 3.9. Gewahrsam
  - 3.9.1. Techniken
  - 3.9.2. Ergebnisse
- 3.10. Berichterstattung und Präsentation von Beweisen
  - 3.10.1. Arten von Berichten
  - 3.10.2. Analyse der Daten
  - 3.10.3. Vorlage von Beweismitteln

## Modul 4. Sicherheit bei Online-Anwendungen

- 4.1. Schwachstellen und Sicherheitsprobleme in Online-Anwendungen
  - 4.1.1. Einführung in die Sicherheit von Online-Anwendungen
  - 4.1.2. Sicherheitsschwachstellen beim Entwurf von Webanwendungen
  - 4.1.3. Sicherheitsschwachstellen bei der Implementierung von Webanwendungen
  - 4.1.4. Sicherheitsschwachstellen bei der Bereitstellung von Webanwendungen
  - 4.1.5. Offizielle Listen von Sicherheitslücken
- 4.2. Richtlinien und Standards für die Sicherheit von Online-Anwendungen
  - 4.2.1. Säulen der Sicherheit von Online-Anwendungen
  - 4.2.2. Sicherheitspolitik
  - 4.2.3. Managementsystem für die Informationssicherheit
  - 4.2.4. Sicherer Lebenszyklus der Softwareentwicklung
  - 4.2.5. Standards für die Anwendungssicherheit
- 4.3. Sicherheit beim Entwurf von Webanwendungen
  - 4.3.1. Einführung in die Sicherheit von Webanwendungen
  - 4.3.2. Sicherheit beim Entwurf von Webanwendungen
- 4.4. Prüfung der Online-Sicherheit von Webanwendungen
  - 4.4.1. Analyse und Prüfung der Sicherheit von Webanwendungen
  - 4.4.2. Sicherheit bei der Bereitstellung und Produktion von Webanwendungen
- 4.5. Sicherheit von Webdiensten
  - 4.5.1. Einführung in die Sicherheit von Webdiensten
  - 4.5.2. Sicherheitsfunktionen und -technologien für Webdienste
- 4.6. Prüfung der Online-Sicherheit und des Schutzes von Webdiensten
  - 4.6.1. Bewertung der Sicherheit von Webdiensten
  - 4.6.2. Online-Schutz. *Firewalls* und *Gateways* XML
- 4.7. Ethisches *Hacking*, *Malware* und *Forensic*
  - 4.7.1. Ethisches *Hacking*
  - 4.7.2. Analyse von *Malware*
  - 4.7.3. Forensische Analyse
- 4.8. Auflösung von Vorfällen bei Webdiensten
  - 4.8.1. Überwachung
  - 4.8.2. Instrumente zur Leistungsmessung
  - 4.8.3. Eindämmungsmaßnahmen
  - 4.8.4. Analyse der Grundursache
  - 4.8.5. Proaktives Problemmanagement
- 4.9. Bewährte Verfahren zur Gewährleistung der Anwendungssicherheit
  - 4.9.1. Handbuch für bewährte Praktiken bei der Entwicklung von Online-Anwendungen
  - 4.9.2. Handbuch für bewährte Praktiken bei der Umsetzung von Online-Anwendungen
- 4.10. Häufige Fehler, die die Anwendungssicherheit untergraben
  - 4.10.1. Häufige Entwicklungsfehler
  - 4.10.2. Häufige Fehler beim Hosting
  - 4.10.3. Häufige Fehler in der Produktion



*Ein umfassendes und multidisziplinäres Fortbildungsprogramm, das es Ihnen ermöglicht, sich in Ihrer Karriere zu profilieren, indem Sie die neuesten Fortschritte auf dem Gebiet des Software-Sicherheitsmanagements und der -Prüfung verfolgen*

# 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 Sicherheit in der Software-Entwicklung 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 **Universitätsexperte in Sicherheit in der Software-Entwicklung** 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 Sicherheit in der Software-Entwicklung**

Anzahl der offiziellen Arbeitsstunden: **600 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 institutionen  
virtuelles Klassenzimmer

**tech** technologische  
universität

Universitätsexperte  
Sicherheit in der  
Software-Entwicklung

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

# Universitätsexperte

## Sicherheit in der Software-Entwicklung