Privater Masterstudiengang

Verwaltung der Cybersicherheitspolitik im Unternehmen

tech technologische universität

tech technologische universität

Privater Masterstudiengang
Verwaltung der Cybersicherheitspolitik im Unternehmen

- Modalität: **online**
- Dauer: **12 Monate**
- Qualifizierung: **TECH Technologische Universität**
- Aufwand: **16 Std./Woche**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Internetzugang: www.techtitute.com/de/informatik/masterstudiengang/masterstudiengang-verwaltung-cybersicherheitspolitik-unternehmen

Index

01

Präsentation

Die zunehmende Abhängigkeit vieler Unternehmen und Wirtschaftszweige von virtuellen Umgebungen hat dazu geführt, dass Cyberkriminalität und Cyberangriffe auf alle Arten von Organisationen übergegriffen haben. Unabhängig von Größe und Standort stellen Bedrohungen der Cybersicherheit eine reale Gefahr dar, die zu erheblichen Verlusten an Zeit, Geld und Daten führen kann. Aus diesem Grund werden Informatiker mit speziellen Kenntnissen im Bereich der Verwaltung von Cybersicherheitspolitiken in Unternehmen immer wichtiger und ihnen eröffnen sich zahlreiche Möglichkeiten für die berufliche und persönliche Entwicklung. Dieser Studiengang bietet IT-Fachkräften eine unschlagbare Gelegenheit, ihre Karriere voranzutreiben und dabei von einem Team von Experten mit umfassender Erfahrung auf diesem Gebiet unterstützt zu werden. Da das Studium zu 100% online stattfindet, ist es mit jeder Art von Tätigkeit oder Verpflichtung vereinbar.

Schreiben Sie sich jetzt ein und erhalten Sie Zugang zu spezialisierten Inhalten in den Bereichen Richtlinien des Incident Managements, Software- und Hardware-Sicherheit und praktische Sicherheitswiederherstellung"

Jeden Tag greifen Tausende von Cyberkriminellen Unternehmen auf der ganzen Welt an, sogar über Tausende von Kilometern hinweg, was die Cybersicherheit zu einem wichtigen Thema in der modernen Unternehmenslandschaft gemacht hat. Schwachstellen in Unternehmen, die auf virtuelle Umgebungen angewiesen sind, können von Kriminellen aller Art ausgenutzt werden, um sensible Daten zu stehlen oder den Zugriff auf diese Daten gegen Lösegeld zu verhindern.

Aus diesem Grund ist die korrekte Verwaltung der Cybersicherheitspolitik im Unternehmen eine große Verantwortung, denn diese verantwortungsvolle Position ist für den spezialisierten Informatiker von hohem Prestige und wirtschaftlicher Bedeutung. Wenn Sie also den Schritt wagen und sich mit Themen wie Auditsystemen zur Erkennung von Bedrohungen oder sicheren Kommunikationsprotokollen befassen, können Sie direkt in eine Schlüsselposition in jedem Unternehmen aufsteigen.

Für diesen privaten Masterstudiengang hat eine Gruppe von Dozenten, die von TECH sorgfältig ausgewählt wurden, didaktische Inhalte von hoher Qualität vorbereitet. In 10 umfassenden Modulen werden die Informatiker ihre Kompetenzen in der Umsetzung von physischen und umweltbedingten Sicherheitsrichtlinien, Managementsystemen für die Informationssicherheit, Überwachungsinstrumenten und vielen anderen Kompetenzen erweitern, die sie zu einem wertvollen Aktivposten in jeder Institution machen.

All dies mit dem unbestreitbaren Vorteil, dass sie nicht an Präsenzveranstaltungen oder festen Terminen teilnehmen müssen, da das gesamte Programm online unterrichtet wird. Die didaktischen Inhalte können von jedem Gerät mit Internetanschluss heruntergeladen und nach Abschluss des Studiums sogar als Nachschlagewerk verwendet werden. Die Studenten können ihr Studienpensum ihrem eigenen Rhythmus anpassen und das Studium mit ihrer normalen beruflichen Tätigkeit oder mit anspruchsvolleren Aufgaben kombinieren.

Dieser **Privater Masterstudiengang in Verwaltung der Cybersicherheitspolitik im Unternehmen** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- Die Entwicklung von Fallstudien, die von Experten der Cybersicherheit und Informatik präsentiert werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt vermittelt alle für die berufliche Praxis unverzichtbaren technischen und praktischen Informationen
- Er enthält praktische Übungen, in denen der Selbstbewertungsprozess durchgeführt werden kann, um das Lernen zu verbessern
- Sein besonderer Schwerpunkt liegt auf innovativen Methoden
- 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

Positionieren Sie sich als ein zuverlässiger Manager der Cybersicherheitspolitik, der in der Lage ist, auf alle Arten von Situationen und unvorhergesehene Ereignisse im Bereich der IT-Sicherheit zu reagieren”

Integrieren Sie in Ihre tägliche Arbeit die wirksamsten Praktiken zur Abwehr von Angriffen, die von einem Team aus spezialisierten Dozenten perfektioniert wurden"

Sie erhalten Zugang zu einem multimedialen Lehrplan, der durch spezielle Themen wie Sicherheitsrichtlinien für das Management, Klassifizierung von IT-Risiken und Hijacking ergänzt wird.

Sie können selbst entscheiden, wann, wo und wie Sie das gesamte Kurspensum absolvieren möchten und haben die Freiheit, den Lehrplan in Ihrem eigenen Tempo zu absolvieren.

Zu den Dozenten des Programms gehören Fachleute aus der Branche, die ihre Erfahrungen aus ihrer Arbeit in diese Weiterbildung einbringen, sowie anerkannte Spezialisten 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. Zu diesem Zweck wird sie von einem innovativen interaktiven Videosystem unterstützt, das von renommierten Experten entwickelt wurde.

02

Ziele

Da Cyber-Sicherheit in der heutigen Geschäftswelt ein so wichtiges Thema ist, spielen Informatiker in diesem Studiengang eine zentrale Rolle bei der Bewältigung dieser Probleme. Aus diesem Grund sind die Ziele, die während des gesamten Studiums verfolgt werden, sehr vielfältig, wobei der Schwerpunkt auf der Vermittlung aktueller theoretischer Inhalte liegt, die auf den neuesten Fortschritten im Bereich der Computersicherheit basieren.

Sie verfügen über ein Nachschlagewerk zum Thema Verwaltung der Cybersicherheitspolitik, das Ihnen helfen wird, Ihre Karriere als Computerexperte im Bereich der digitalen Sicherheit voranzutreiben"

Allgemeine Ziele

- Vertiefen der Schlüsselkonzepte der Informationssicherheit
- Entwickeln der notwendigen Maßnahmen zur Gewährleistung guter Informationssicherheitspraktiken
- Entwickeln der verschiedenen Methoden zur Durchführung einer umfassenden Bedrohungsanalyse
- Installieren und Erlernen der verschiedenen Tools, die bei der Behandlung und Vorbeugung von Vorfällen eingesetzt werden

Mit der didaktischen Methode von TECH erreichen Sie Ihre ehrgeizigsten Ziele schneller als Sie denken"

Spezifische Ziele

Modul 1. Informationssicherheits-Managementsystem (ISMS)

- Analysieren der Vorschriften und Standards, die derzeit für ISMS gelten
- Entwickeln der Phasen, die für die Implementierung eines ISMS in einem Unternehmen erforderlich sind
- Analysieren des Managements von Informationssicherheitsvorfällen und der Implementierungsverfahren

Modul 2. Organisatorische Aspekte der Informationssicherheitspolitik

- Implementieren eines ISMS im Unternehmen
- Bestimmen, welche Abteilungen die Implementierung des Sicherheitsmanagementsystems abdecken soll
- Implementieren der notwendigen Sicherheitsmaßnahmen im Betrieb

Modul 3. Sicherheitspolitiken für die Analyse von Bedrohungen in Informationssystemen

- Analysieren der Bedeutung von Bedrohungen
- Bestimmen der Phasen des präventiven Bedrohungsmanagements
- Vergleichen verschiedener Methoden des Bedrohungsmanagements

Modul 4. Praktische Umsetzung von Sicherheitspolitiken für Software und Hardware

- Bestimmen, was Authentifizierung und Identifizierung ist
- Analysieren der verschiedenen existierenden Authentifizierungsmethoden und ihrer praktischen Umsetzung
- Implementieren der richtigen Zugriffskontrollpolitik für Software und Systeme
- Ermitteln der wichtigsten aktuellen Identifizierungstechnologien
- Generieren von Fachwissen über die verschiedenen Methoden, die für die Absicherung von Systemen existieren

Modul 5. Richtlinien für das Management von Sicherheitsvorfällen

- Entwickeln von Fachwissen über den Umgang mit Vorfällen, die durch Computersicherheitsereignisse verursacht werden
- Festlegen der Arbeitsweise eines Teams zur Bearbeitung von Sicherheitsvorfällen
- Analysieren der verschiedenen Phasen des Managements von IT-Sicherheitsvorfällen
- Untersuchen von standardisierten Protokollen für den Umgang mit Sicherheitszwischenfällen

Modul 6. Implementierung von physischen und umweltbezogenen Sicherheitspolitiken im Unternehmen

- Analysieren der Begriffe Sicherer Bereich und Sicherer Perimeter
- Untersuchen der Biometrie und biometrischer Systeme
- Umsetzen der richtigen Sicherheitsrichtlinien für die physische Sicherheit
- Entwickeln der geltenden Vorschriften für sichere Bereiche von Computersystemen

Modul 7. Richtlinien für sichere Kommunikation im Unternehmen

- Sichern eines Kommunikationsnetzwerks durch Partitionierung des Netzwerks
- Analysieren der verschiedenen Verschlüsselungsalgorithmen, die in Kommunikationsnetzwerken verwendet werden
- Implementieren verschiedener Verschlüsselungstechniken im Netzwerk wie TLS, VPN oder SSH

Modul 8. Praktische Umsetzung von Sicherheitspolitiken im Angesicht von Angriffen

- Bestimmen der verschiedenen realen Angriffe auf unser Informationssystem
- Bewerten der verschiedenen Sicherheitsmaßnahmen zur Eindämmung von Angriffen
- Implementieren der technischen Maßnahmen zur Abschwächung der wichtigsten Bedrohungen

Modul 9. Überwachungswerkzeuge in Sicherheitspolitiken für Informationssysteme

- Entwickeln des Konzepts der Überwachung und der Implementierung von Metriken
- Konfigurieren von Audit-Trails auf Systemen und Überwachungsnetzwerken
- Zusammenstellen der besten Systemüberwachungstools, die derzeit auf dem Markt sind

Modul 10. Praktische Sicherheitspolitiken für die Notfallwiederherstellung

- Generieren von Fachwissen über das Konzept der Kontinuität der Informationssicherheit
- Entwickeln eines Business-Continuity-Plans
- Analysieren eines IKT-Kontinuitätsplans
- Entwerfen eines Wiederherstellungsplans für den Katastrophenfall

03

Kompetenzen

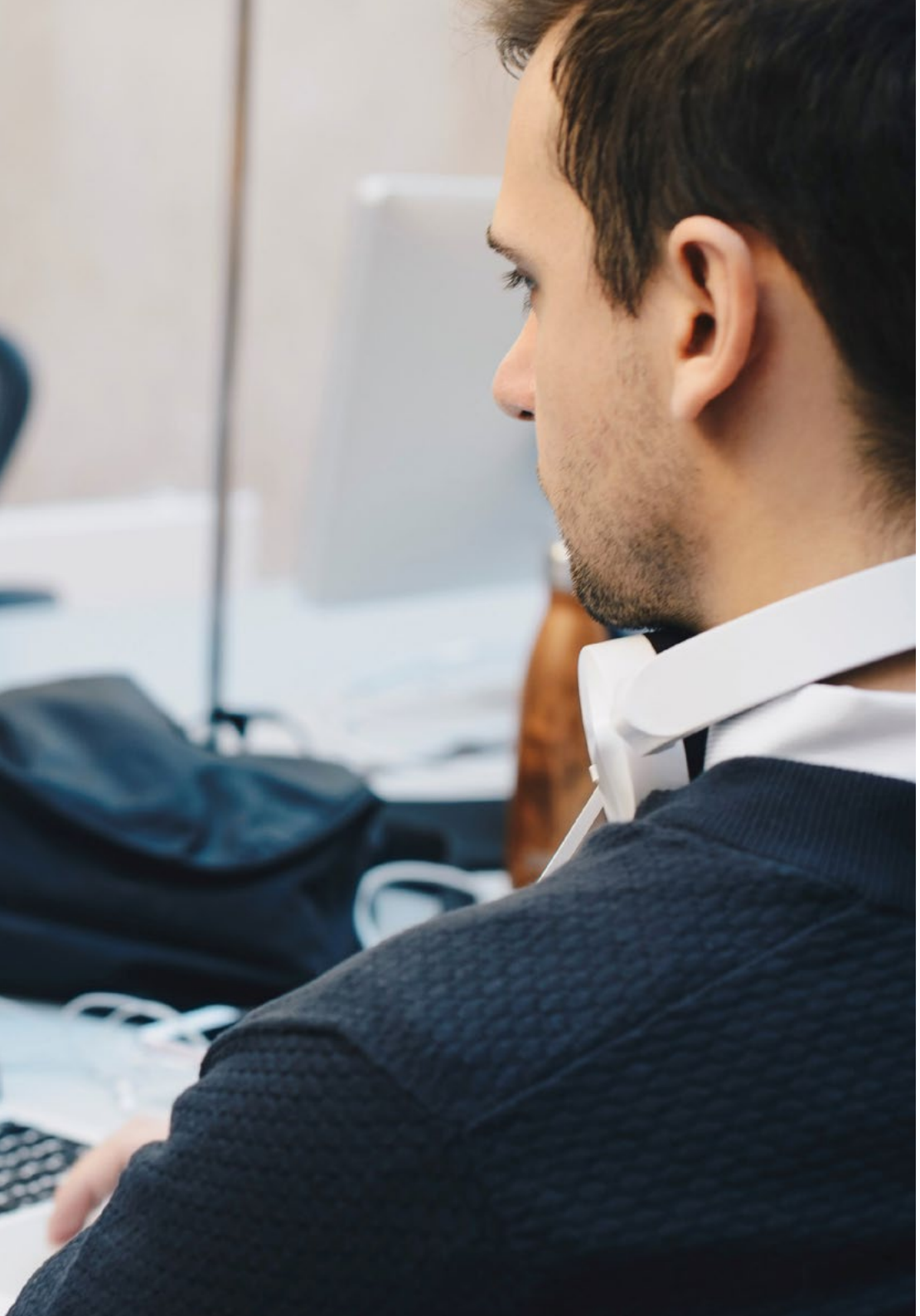
Um die erweiterten und spezialisierten Kompetenzen zu entwickeln, über die ein auf Cybersicherheitspolitik spezialisierter Informatiker verfügen muss, hat TECH ein außergewöhnliches Dozententeam zusammengestellt. Durch die praktische Kombination ihrer Berufserfahrung mit den neuesten Entwicklungen im Bereich der digitalen Sicherheit werden die Informatiker in die Lage versetzt, jedes behandelte Thema in einem viel breiteren Kontext zu sehen.

Sie werden eine Reihe von Kompetenzen erwerben, die Ihre zentrale Rolle in jedem Cyber-Strategieplan Ihres Unternehmens unterstreichen"

Allgemeine Kompetenzen

- Implementieren und Entwickeln eines Business-Continuity-Plans in Übereinstimmung mit jeder Art von Einrichtung und ihren Bedürfnissen
- Entwickeln einer Geschäftsprozessanalyse
- Analysieren von Audit-Methoden
- Beurteilen der Notwendigkeit einer forensischen Computeranalyse für die eingehende Untersuchung von aufgezeichneten Vorfällen

Sie können Ihre Job- und Gehaltsaussichten verbessern, indem Sie sich auf das derzeit wichtigste Thema, die Cybersicherheit, spezialisieren"



Spezifische Kompetenzen

- Bestimmen der Einbindung eines ISMS in die interne Organisation des Unternehmens sowie dessen Status
- Festlegen der Sicherheitsrichtlinien im Unternehmen
- Bestimmen, welche Maßnahmen wir bei Lieferanten und bei der Wartung von Informationssystemen umsetzen müssen
- Generieren von Fachwissen über die Kontrolle von Bedrohungen
- Bestimmen der Phasen des präventiven Bedrohungsmanagements
- Entwickeln von Methoden für die Analyse von Computerbedrohungen
- Klassifizieren von Bedrohungen nach Auswirkungen und Schweregrad
- Entwickeln einer eigenen Methodik für die präventive Analyse und Überwachung von Bedrohungen
- Implementieren einer korrekten Zugriffskontrollpolitik für Netzwerke und Dienste
- Analysieren der Bedeutung einer korrekten Handhabung von Sicherheitszwischenfällen
- Zusammenstellen der verschiedenen biometrischen Systeme, die es gibt
- Untersuchen der Biometrie und biometrischer Systeme
- Implementieren der richtigen physischen Sicherheitsrichtlinien und physischen Zugangskontrollsysteme in Datenverarbeitungszentren
- Implementieren eines sicheren Netzwerks
- Untersuchen der Schwachstellen von mobilen und IoT-Plattformen und wie man sie vermeidet
- Erkennen der Arten von *Social Engineering* und lernen, wie man sie entschärfen kann
- Analysieren des Konzepts der Überwachung und der Implementierung von Metriken
- Bestimmen des Bedarfs an Kontinuität der Informationssicherheit

04

Kursleitung

Alle Experten, die TECH für diesen privaten Masterstudiengang ausgewählt hat, verfügen über umfangreiche Erfahrung im Bereich des IT-Servicemanagements, wobei der Schwerpunkt stets auf der Cybersicherheit und der korrekten Ausführung von Protokollen liegt. Gerade diese Erfahrung verleiht dem gesamten Studiengang einen hohen Qualitätsaspekt, da die Informatiker aufgrund des sehr praktischen Charakters des Studiengangs alle neuen Kenntnisse sofort anwenden und ihre Fähigkeiten noch vor Abschluss des Studiums verbessern können.

Sie werden von einer Gruppe von Dozenten unterstützt und betreut, die sich voll und ganz für Ihre berufliche Weiterentwicklung in Richtung Verwaltung von Cybersicherheitspolitiken einsetzen"

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)
- Computer- Ingenieurin an der Universität von Alcalá de Henares von Madrid
- Masterstudiengang in DevOps: Docker und Kubernetes, Cas-Training
- Microsoft Azure Security Techonologies, E-Council

Professoren

Hr. Solana Villarias, Fabián

- Berater für Informationstechnologie
- Entwickler und Administrator von Umfragediensten bei Investigación, Planificación y Desarrollo, SA
- Spezialist für Finanzmärkte und IT-Systempflege bei Iberia Financial Software
- Webentwickler und Spezialist für Barrierefreiheit bei Indra
- Hochschulabschluss in Systemtechnik an der Universität von Wales/CESINE
- Universitätskurs in technischem Ingenieurwesen in Computer Systems Engineering an der Universität von Wales/CESINE

Fr. López García, Rosa María

- Spezialistin für Management-Informationen
- Dozentin am Linux Professional Institute
- Mitarbeiterin der Hackerkademie Incibe
- Cybersecurity Talent Captain bei Teamciberhack
- Verwaltungs-, Buchhaltungs- und Finanzmanagerin bei Integra2Transportes
- Verwaltungsassistentin für den Einkauf von Ressourcen im Bildungszentrum Cardenal Marcelo Espínola
- Höhere Technikerin in Cybersicherheit und ethischem Hacking
- Mitglied von Ciberpatrulla

Hr. Oropesiano Carrizosa, Francisco

- Computer-Ingenieur
- Mikroinformatiker, Netzwerktechniker und Sicherheitstechniker bei Cas-Training
- Entwickler für Webdienste, CMS, e-Commerce, UI und UX bei Fersa Reparaciones
- Manager für Webdienste, Inhalte, Mail und DNS bei Oropesia Web & Network
- Grafiker und Designer für Webanwendungen bei Xarxa Sakai Projectes
- Universitätskurs in Computersystemen an der Universität von Alcalá de Henares
- Masterstudiengang in DevOps: Docker and Kubernetes von Cyber Business Center
- Techniker für Netzwerke und Computersicherheit von der Universität der Balearischen Inseln
- Experte in Grafikdesign von der Polytechnischen Universität von Madrid

Hr. Ortega López, Florencio

- Sicherheitsberater (Identitätsmanagement) bei der SIA-Gruppe
- IKT- und Sicherheitsberater als Freiberufler
- Ausbilder in der IT-Branche
- Hochschulabschluss in technischem Wirtschaftsingenieurwesen an der Universität von Alcalá de Henares
- Masterstudiengang für Lehrkräfte von der UNIR
- MBA in Unternehmensführung und Verwaltung vom IDE-CESEM
- Masterstudiengang in Management der Informationstechnologie vom IDE-CESEM
- Certified Information Security Management (CISM) von ISACA

Hr. Peralta Alonso, Jon

- Senior Consultant - Datenschutz und Cybersicherheit, Altia
- Rechtsanwalt/Rechtsbeistand, Arriaga Asociados Asesoramiento Jurídico y Económico, SL
- Rechtsberater/Praktikant, Professionelles Büro: Oscar Padura
- Hochschulabschluss in Jura, Öffentliche Universität des Baskenlandes
- Masterstudiengang in Datenschutzbeauftragter, EIS Innovative School
- Masterstudiengang in Rechtswissenschaften, Öffentliche Universität des Baskenlandes
- Masterstudiengang in Zivilprozessrecht, Internationale Universität Isabel I de Castilla
- Dozent im Masterstudiengang für Datenschutz, Cybersicherheit und IKT-Recht

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

05

Struktur und Inhalt

TECH hat bei der Entwicklung aller Inhalte dieses Programms die *Relearning*-Methode angewandt. Dies bedeutet, dass die wichtigsten Grundlagen und Konzepte im Bereich der Verwaltung von Cybersicherheitspolitiken Schritt für Schritt über den gesamten Lehrplan hinweg vermittelt werden, was zu einem wesentlich effizienteren und schnelleren Lernprozess führt. Die Studenten haben Zugang zu zahlreichen detaillierten Videos, Übungen zur Selbstbewertung und ergänzender Lektüre, die speziell für jedes Thema des Programms erstellt und ausgewählt wurden.

Das gesamte multimediale Material dieses privaten Masterstudiengangs wird Ihnen helfen, sich viel tiefer, schneller und umfassender zu spezialisieren"

Modul 1. Informationssicherheits-Managementsystem (ISMS)

1.1. Informationssicherheit. Schlüsselaspekte
- 1.1.1. Informationssicherheit
  - 1.1.1.1. Vertraulichkeit
  - 1.1.1.2. Integrität
  - 1.1.1.3. Verfügbarkeit
  - 1.1.1.4. Maßnahmen zur Informationssicherheit

1.2. Managementsystem für die Informationssicherheit
- 1.2.1. Modelle für das Management der Informationssicherheit
- 1.2.2. Dokumente für die Implementierung eines ISMS
- 1.2.3. ISMS-Stufen und Kontrollen

1.3. Internationale Normen und Standards
- 1.3.1. Internationale Normen zur Informationssicherheit
- 1.3.2. Ursprung und Entwicklung des Standards
- 1.3.3. Internationale Standards für das Management der Informationssicherheit
- 1.3.4. Andere Referenzstandards

1.4. ISO/IEC 27000-Normen
- 1.4.1. Zweck und Anwendungsbereich
- 1.4.2. Aufbau der Norm
- 1.4.3. Zertifizierung
- 1.4.4. Phasen der Akkreditierung
- 1.4.5. Vorteile der ISO/IEC 27.000-Normen

1.5. Entwurf und Implementierung eines allgemeinen Informationssicherheitssystems
- 1.5.1. Phasen der Implementierung eines allgemeinen Informationssicherheitssystems
- 1.5.2. Business Continuity Plan

1.6. Phase I: Diagnose
- 1.6.1. Vorläufige Diagnose
- 1.6.2. Identifizierung der Ebene der Schichtung
- 1.6.3. Grad der Einhaltung von Standards/Normen

1.7. Phase II: Vorbereitung
- 1.7.1. Organisatorischer Kontext
- 1.7.2. Analyse der geltenden Sicherheitsvorschriften
- 1.7.3. Umfang des allgemeinen Informationssicherheitssystems
- 1.7.4. Richtlinien des allgemeinen Informationssicherheitssystems
- 1.7.5. Zielsetzungen des allgemeinen Informationssicherheitssystems

1.8. Phase III: Planung
- 1.8.1. Klassifizierung der Vermögenswerte
- 1.8.2. Risikobewertung
- 1.8.3. Identifizierung von Bedrohungen und Risiken

1.9. Phase IV: Umsetzung und Überwachung
- 1.9.1. Analyse der Ergebnisse
- 1.9.2. Zuweisung von Verantwortlichkeiten
- 1.9.3. Zeitplan für den Aktionsplan
- 1.9.4. Überwachung und Audits

1.10. Sicherheitsrichtlinien für das Incident Management
- 1.10.1. Phasen
- 1.10.2. Kategorisierung von Vorfällen
- 1.10.3. Verfahren für Zwischenfälle und Zwischenfallmanagement

Modul 2. Organisatorische Aspekte der Informationssicherheitspolitik

2.1. Interne Organisation
- 2.1.1. Zuweisung von Verantwortlichkeiten
- 2.1.2. Trennung der Aufgaben
- 2.1.3. Kontakte mit Behörden
- 2.1.4. Informationssicherheit in der Projektverwaltung

2.2. Vermögensverwaltung
- 2.2.1. Verantwortung für Vermögenswerte
- 2.2.2. Klassifizierung der Informationen
- 2.2.3. Handhabung von Speichermedien

2.3. Sicherheitspolitiken in Geschäftsprozessen
- 2.3.1. Analyse der anfälligen Geschäftsprozesse
- 2.3.2. Analyse der Auswirkungen auf das Geschäft
- 2.3.3. Einstufung der Prozesse in Bezug auf die geschäftlichen Auswirkungen

2.4. Sicherheitspolitiken in Verbindung mit dem Personalwesen
  2.4.1. Vor der Einstellung
  2.4.2. Während der Rekrutierung
  2.4.3. Beendigung oder Wechsel der Stelle
2.5. Sicherheitsrichtlinien auf Managementebene
  2.5.1. Managementrichtlinien zur Informationssicherheit
  2.5.2. BIA - Analyse der Auswirkungen
  2.5.3. Wiederherstellungsplan als Sicherheitspolitik
2.6. Anschaffung und Wartung von Informationssystemen
  2.6.1. Anforderungen an die Sicherheit von Informationssystemen
  2.6.2. Entwicklung und Unterstützung der Datensicherheit
  2.6.3. Testdaten
2.7. Sicherheit bei Lieferanten
  2.7.1. IT-Sicherheit mit Zulieferern
  2.7.2. Management der Bereitstellung des Dienstes mit Garantie
  2.7.3. Sicherheit der Lieferkette
2.8. Operative Sicherheit
  2.8.1. Operative Verantwortlichkeiten
  2.8.2. Schutz vor bösartigem Code
  2.8.3. Sicherungskopien
  2.8.4. Aktivitätsprotokolle und Überwachung
2.9. Sicherheitsmanagement und Vorschriften
  2.9.1. Einhaltung der gesetzlichen Vorschriften
  2.9.2. Überprüfung der Informationssicherheit
2.10. Sicherheit im Business Continuity Management
  2.10.1. Kontinuität der Informationssicherheit
  2.10.2. Redundanzen

Modul 3. Sicherheitspolitiken für die Analyse von Bedrohungen in Informationssystemen

3.1. Bedrohungsmanagement in Sicherheitsrichtlinien
  3.1.1. Das Risikomanagement
  3.1.2. Das Sicherheitsrisiko
  3.1.3. Methodologien im Bedrohungsmanagement
  3.1.4. Implementierung von Methoden
3.2. Phasen des Managements von Bedrohungen
  3.2.1. Identifizierung
  3.2.2. Analyse
  3.2.3. Standort
  3.2.4. Schutzmaßnahmen
3.3. Auditsysteme zur Lokalisierung von Bedrohungen
  3.3.1. Klassifizierung und Informationsfluss
  3.3.2. Analyse der anfälligen Prozesse
3.4. Risikoklassifizierung
  3.4.1. Arten von Risiko
  3.4.2. Berechnung der Gefahrenwahrscheinlichkeit
  3.4.3. Residuales Risiko
3.5. Risikobehandlung
  3.5.1. Umsetzung von Schutzmaßnahmen
  3.5.2. Übertragung oder Übernahme
3.6. Risikokontrolle
  3.6.1. Kontinuierlicher Risikomanagementprozess
  3.6.2. Implementierung von Sicherheitsmetriken
  3.6.3. Strategisches Modell der Metriken für die Informationssicherheit
3.7. Praktische Methoden für die Analyse und Kontrolle von Bedrohungen
  3.7.1. Katalog der Bedrohungen
  3.7.2. Katalog der Kontrollmaßnahmen
  3.7.3. Katalog der Sicherheitsvorkehrungen
3.8. ISO 27005-Norm
  3.8.1. Identifizierung von Risiken
  3.8.2. Risikoanalyse
  3.8.3. Risikobewertung

3.9. Matrix der Risiken, Auswirkungen und Bedrohungen
  3.9.1. Daten, Systeme und Personal
  3.9.2. Wahrscheinlichkeit der Bedrohung
  3.9.3. Ausmaß des Schadens
3.10. Gestaltung von Phasen und Prozessen in der Gefahrenanalyse
  3.10.1. Identifizierung der kritischen Elemente der Organisation
  3.10.2. Bestimmung der Bedrohungen und Auswirkungen
  3.10.3. Analyse der Auswirkungen und Risiken
  3.10.4 Methoden

Modul 4. Praktische Umsetzung von Sicherheitspolitiken für Software und Hardware

4.1. Praktische Umsetzung von Sicherheitspolitiken für Software und Hardware
  4.1.1. Implementierung von Identifizierung und Autorisierung
  4.1.2. Implementierung von Identifizierungstechniken
  4.1.3. Technische Maßnahmen zur Autorisierung
4.2. Identifizierungs- und Autorisierungstechniken
  4.2.1. Kennung und OTP
  4.2.2. USB-Token oder PKI-*Smartcard*
  4.2.3. Der Schlüssel "Vertrauliche Verteidigung"
  4.2.4. Aktive RFID
4.3. Sicherheitspolitiken für den Zugang zu Software und Systemen
  4.3.1. Implementierung von Politiken zur Zugriffskontrolle
  4.3.2. Umsetzung von Politiken für den Zugang zur Kommunikation
  4.3.3. Arten von Sicherheitstools für die Zugriffskontrolle
4.4. Verwaltung des Benutzerzugriffs
  4.4.1. Verwaltung von Zugriffsrechten
  4.4.2. Trennung von Rollen und Zugriffsfunktionen
  4.4.3. Implementierung von Zugriffsrechten in Systemen
4.5. Kontrolle des Zugriffs auf Systeme und Anwendungen
  4.5.1. Mindestzugriffsregel
  4.5.2. Sichere Anmeldetechnologien
  4.5.3. Passwort-Sicherheitsrichtlinien
4.6. Technologien für Identifikationssysteme
  4.6.1. Aktives Verzeichnis
  4.6.2. OTP
  4.6.3. PAP, CHAP
  4.6.4. KERBEROS, DIAMETER, NTLM
4.7. CIS-Kontrollen für Bastionierungssysteme
  4.7.1. Allgemeine CIS-Kontrollen
  4.7.2. Grundlegende CIS-Kontrollen
  4.7.3. Organisatorische CIS-Kontrollen
4.8. Operative Sicherheit
  4.8.1. Schutz vor bösartigem Code
  4.8.2. Sicherungskopien
  4.8.3. Aktivitätsprotokollierung und Überwachung
4.9. Management von technischen Schwachstellen
  4.9.1. Technische Schwachstellen
  4.9.2. Management von technischen Schwachstellen
  4.9.3. Einschränkungen bei der Software-Installation
4.10. Umsetzung der Sicherheitspraktiken
  4.10.1. Logische Schwachstellen
  4.10.2. Implementierung von Verteidigungsrichtlinien

Modul 5. Richtlinien für das Management von Sicherheitsvorfällen

5.1. Richtlinien und Verbesserungen für das Management von Sicherheitsvorfällen in der Informationssicherheit
  5.1.1. Management von Zwischenfällen
  5.1.2. Verantwortlichkeiten und Verfahren
  5.1.3. Event-Benachrichtigung
5.2. Systeme zur Erkennung und Verhinderung von Eindringlingen (IDS/IPS)
  5.2.1. Daten zur Systemleistung
  5.2.2. Arten von Intrusion Detection Systemen
  5.2.3. Kriterien für den Standort von IDS/IPS

5.3. Reaktion auf Sicherheitsvorfälle
  5.3.1. Verfahren zum Sammeln von Informationen
  5.3.2. Verfahren zur Überprüfung der Intrusion
  5.3.3. CERT-Gremien
5.4. Benachrichtigung über einen Einbruchsversuch und Managementprozess
  5.4.1. Verantwortlichkeiten im Benachrichtigungsprozess
  5.4.2. Klassifizierung von Vorfällen
  5.4.3. Lösung und Wiederherstellungsprozess
5.5. Forensische Analyse als Sicherheitspolitik
  5.5.1. Volatile und nichtvolatile Beweise
  5.5.2. Analyse und Sammlung von elektronischen Beweismitteln
    5.5.2.1. Analyse von elektronischen Beweismitteln
    5.5.2.2. Sammlung von elektronischen Beweismitteln
5.6. Werkzeuge für Intrusion Detection und Prevention Systeme (IDS/IPS)
  5.6.1. *Snort*
  5.6.2. Suricata
  5.6.3. Solar-Winds
5.7. Tools zur Zentralisierung von Ereignissen
  5.7.1. SIM
  5.7.2. SEM
  5.7.3. SIEM
5.8. CCN-STIC Sicherheitsleitfaden 817
  5.8.1. Management von Cybervorfällen
  5.8.2. Metriken und Indikatoren
5.9. NIST SP800-61
  5.9.1. Fähigkeit zur Reaktion auf Computer-Sicherheitsvorfälle
  5.9.2. Umgang mit einem Vorfall
  5.9.3. Koordinierung und Informationsaustausch
5.10. ISO 27035-Norm
  5.10.1. ISO 27035-Norm. Grundsätze des Vorfallsmanagements
  5.10.2. Richtlinien für die Entwicklung eines Vorfallsmanagementplans
  5.10.3. Richtlinien für die Reaktion auf Vorfälle

Modul 6. Implementierung von physischen und umweltbezogenen Sicherheitspolitiken im Unternehmen

6.1. Sichere Bereiche
  6.1.1. Physischer Sicherheitsbereich
  6.1.2. Arbeiten in Sicherheitsbereichen
  6.1.3. Sicherheit von Büros, Geschäftsräumen und Ressourcen
6.2. Physische Zugangskontrollen
  6.2.1. Richtlinien zur physischen Zugangskontrolle
  6.2.2. Physische Zugangskontrollsysteme
6.3. Schwachstellen beim physischen Zugang
  6.3.1. Die wichtigsten physischen Schwachstellen
  6.3.2. Umsetzung von Schutzmaßnahmen
6.4. Physiologische biometrische Systeme
  6.4.1. Fingerabdruck
  6.4.2. Gesichtserkennung
  6.4.3. Iris- und Retina-Erkennung
  6.4.4. Andere physiologische biometrische Systeme
6.5. Verhaltensbiometrische Systeme
  6.5.1. Erkennung von Unterschriften
  6.5.2. Erkennung von Schriftzeichen
  6.5.3. Spracherkennung
  6.5.4. Andere biometrische Verhaltenssysteme
6.6. Risikomanagement in der Biometrie
  6.6.1. Implementierung biometrischer Systeme
  6.6.2. Schwachstellen biometrischer Systeme
6.7. Implementierung von Richtlinien in *Hosts*
  6.7.1. Installation der Verkabelung, Bereitstellung und Sicherheit
  6.7.2. Platzierung der Geräte
  6.7.3. Verlassen der Geräte außerhalb des Gebäudes
  6.7.4. Unbeaufsichtigte Computerausrüstung und Sicherungspolitik beim Verlassen des Arbeitsplatzes

6.8. Umweltschutz
- 6.8.1. Feuerschutzsysteme
- 6.8.2. Schutzsysteme bei Erdbeben
- 6.8.3. Erdbebenschutzsysteme

6.9. Sicherheit von Datenverarbeitungszentren
- 6.9.1. Sicherheitstüren
- 6.9.2. Videoüberwachungssysteme (CCTV)
- 6.9.3. Sicherheitskontrolle

6.10. Internationale Vorschriften zur physischen Sicherheit
- 6.10.1. IEC 62443-2-1 (europäisch)
- 6.10.2. NERC CIP-005-5 (USA)
- 6.10.3. NERC CIP-014-2 (USA)

Modul 7. Richtlinien für sichere Kommunikation im Unternehmen

7.1. Verwaltung der Netzwerksicherheit
- 7.1.1. Netzwerkkontrolle und -überwachung
- 7.1.2. Netzwerk-Trennung
- 7.1.3. Netzwerk-Sicherheitssysteme

7.2. Sichere Kommunikationsprotokolle
- 7.2.1. TCP/IP-Modell
- 7.2.2. IPSEC-Protokoll
- 7.2.3. TLS-Protokoll

7.3. TLS 1,3 Protokoll
- 7.3.1. Phasen eines TLS1.3-Prozesses
- 7.3.2. *Handshake*-Protokoll
- 7.3.3. Registrierungsprotokoll
- 7.3.4. Unterschiede zu TLS 1.2

7.4. Kryptographische Algorithmen
- 7.4.1. In der Kommunikation verwendete kryptographische Algorithmen
- 7.4.2. *Cipher-Suites*
- 7.4.3. Erlaubte kryptographische Algorithmen für TLS 1.3

7.5. *Digest*-Funktionen
- 7.5.1. MD6
- 7.5.2. SHA

7.6. PKI. Infrastruktur für den öffentlichen Schlüssel
- 7.6.1. PKI und ihre Einrichtungen
- 7.6.2. Digitales Zertifikat
- 7.6.3. Arten von digitalen Zertifikaten

7.7. Tunnel- und Transportkommunikation
- 7.7.1. Tunnel-Kommunikation
- 7.7.2. Transport-Kommunikation
- 7.7.3. Verschlüsselte Tunnel-Implementierung

7.8. SSH. *Secure Shell*
- 7.8.1. SSH. Sichere Kapsel
- 7.8.2. Betrieb von SSH
- 7.8.3. SSH-Tools

7.9. Prüfung kryptographischer Systeme
- 7.9.1. Prüfung der Integrität
- 7.9.2. Testen von kryptographischen Systemen

7.10. Kryptografische Systeme
- 7.10.1. Schwachstellen in kryptographischen Systemen
- 7.10.2. Kryptografische Sicherheitsvorkehrungen

Modul 8. Praktische Umsetzung von Sicherheitspolitiken im Angesicht von Angriffen

8.1. *System Hacking*
- 8.1.1. Risiken und Schwachstellen
- 8.1.2. Gegenmaßnahmen

8.2. DoS in Dienstleistungen
- 8.2.1. Risiken und Schwachstellen
- 8.2.2. Gegenmaßnahmen

8.3. *Session Hijacking*
- 8.3.1. Der *Hijacking*-Prozess
- 8.3.2. Gegenmaßnahmen zum *Hijacking*

8.4. Umgehung von IDS, Firewalls und Honeypots
- 8.4.1. Ausweichtechniken
- 8.4.2. Implementierung von Gegenmaßnahmen

8.5. *Hacking Web Servers*
- 8.5.1. Angriffe auf Webserver
- 8.5.2. Implementierung von Abwehrmaßnahmen

8.6. *Hacking Web Applications*
- 8.6.1. Angriffe auf Webanwendungen
- 8.6.2. Implementierung von Abwehrmaßnahmen

8.7. *Hacking Wireless Networks*
- 8.7.1. Schwachstellen im Wifi-Netzwerk
- 8.7.2. Implementierung von Abwehrmaßnahmen

8.8. *Hacking Mobile Platforms*
- 8.8.1. Schwachstellen von mobilen Plattformen
- 8.8.2. Implementierung von Gegenmaßnahmen

8.9. *Ransomware*
- 8.9.1. Schwachstellen, die *Ransomware* verursachen
- 8.9.2. Implementierung von Gegenmaßnahmen

8.10. *Social Engineering*
- 8.10.1. Arten von *Social Engineering*
- 8.10.2. Gegenmaßnahmen für *Social Engineering*

Modul 9. Überwachungswerkzeuge in Sicherheitspolitiken für Informationssysteme

9.1. Richtlinien für die Überwachung von Informationssystemen
- 9.1.1. System-Überwachung
- 9.1.2. Metriken
- 9.1.3. Arten von Metriken

9.2. Auditing und Logging in Systemen
- 9.2.1. Auditing und Logging in Systemen
- 9.2.2. Auditing und Logging in Windows
- 9.2.3. Auditing und Logging in Linux

9.3. SNMP-Protokoll. *Simple Network Management Protocol*
- 9.3.1. SNMP-Protokoll
- 9.3.2. Betrieb von SNMP
- 9.3.3. SNMP-Tools

9.4. Netzwerk-Überwachung
- 9.4.1. Netzwerküberwachung in Kontrollsystemen
- 9.4.2. Überwachungstools für Kontrollsysteme

9.5. Nagios. System zur Netzwerküberwachung
- 9.5.1. Nagios
- 9.5.2. Betrieb von Nagios
- 9.5.3. Installation von Nagios

9.6. Zabbix. System zur Netzwerküberwachung
- 9.6.1. Zabbix
- 9.6.2. Betrieb von Zabbix
- 9.6.3. Installation von Zabbix

9.7. Cacti. System zur Netzwerküberwachung
- 9.7.1. Cacti
- 9.7.2. Betrieb von Cacti
- 9.7.3. Installation von Cacti

9.8. Pandora. System zur Netzwerküberwachung
- 9.8.1. Pandora
- 9.8.2. Betrieb von Pandora
- 9.8.3. Installation von Pandora

9.9. SolarWinds. System zur Netzwerküberwachung
- 9.9.1. SolarWinds
- 9.9.2. Betrieb von SolarWinds
- 9.9.3. Installation von SolarWinds

9.10. Regelungen zur Überwachung
- 9.10.1. CIS-Kontrollen zur Prüfung und Registrierung
- 9.10.2. NIST 800-123 (USA)

Modul 10. Praktische Sicherheitspolitiken für die Notfallwiederherstellung

10.1. DRP. *Disaster-Recovery-Plan*
- 10.1.1. Zweck eines DRP
- 10.1.2. Vorteile eines DRP
- 10.1.3. Konsequenzen, wenn Sie keinen DRP haben oder diesen nicht auf dem neuesten Stand halten

10.2. Leitfaden für die Definition eines DRP (*Disaster Recovery Plan*)
- 10.2.1. Umfang und Ziele
- 10.2.2. Entwurf der Wiederherstellungsstrategie
- 10.2.3. Zuweisung von Rollen und Verantwortlichkeiten
- 10.2.4. Inventarisierung von Hardware, Software und Diensten
- 10.2.5. Toleranz für Ausfallzeiten und Datenverluste
- 10.2.6. Festlegen der spezifischen Arten von DRPs, die erforderlich sind
- 10.2.7. Umsetzung eines Plans zur Fortbildung, Sensibilisierung und Kommunikation

10.3. Umfang und Ziele eines DRP (*Disaster Recovery Plan*)
- 10.3.1. Sicherstellung der Reaktionsfähigkeit
- 10.3.2. Technologische Komponenten
- 10.3.3. Umfang der Kontinuitätspolitik

10.4. Entwurf einer DRP-Strategie (*Disaster Recovery*)
- 10.4.1. *Disaster-Recovery*-Strategie
- 10.4.2. Budget
- 10.4.3. Personelle und materielle Ressourcen
- 10.4.4. Gefährdete Managementpositionen
- 10.4.5. Technologie
- 10.4.6. Daten

10.5. Kontinuität der Informationsprozesse
- 10.5.1. Planung der Kontinuität
- 10.5.2. Implementierung der Kontinuität
- 10.5.3. Überprüfung der Kontinuitätsbewertung

10.6. Umfang eines BCP (*Business Continuity Plan*)
- 10.6.1. Bestimmung der kritischsten Prozesse
- 10.6.2. Asset-basierter Ansatz
- 10.6.3. Prozessorientierter Ansatz

10.7. Implementierung von gesicherten Geschäftsprozessen
- 10.7.1. Vorrangige Aktivitäten (PA)
- 10.7.2. Ideale Wiederherstellungszeiten (IRT)
- 10.7.3. Überlebensstrategien

10.8. Analyse der Organisation
- 10.8.1. Sammeln von Informationen
- 10.8.2. Analyse der geschäftlichen Auswirkungen (BIA)
- 10.8.3. Organisatorische Risikoanalyse

10.9. Reaktion auf Notfälle
- 10.9.1. Krisenplan
- 10.9.2. Wiederherstellungspläne für das Betriebsumfeld
- 10.9.3. Verfahren für technische Arbeiten oder Zwischenfälle

10.10. Internationale Norm ISO 27031 BCP
- 10.10.1. Ziele
- 10.10.2. Begriffe und Definitionen
- 10.10.3. Operation

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 hinter sich lässt und Sie durch zyklische Lehrsysteme führt: eine Art des Lernens, die sich als äußerst effektiv erwiesen hat, insbesondere in Fächern, die Auswendiglernen erfordern"

Fallstudie zur Kontextualisierung aller Inhalte

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

Mit TECH werden Sie eine Art des Lernens erleben, die an den Grundlagen der traditionellen Universitäten auf der ganzen Welt rüttelt"

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

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

Eine innovative und andersartige Lernmethode

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

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

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

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

Relearning Methodology

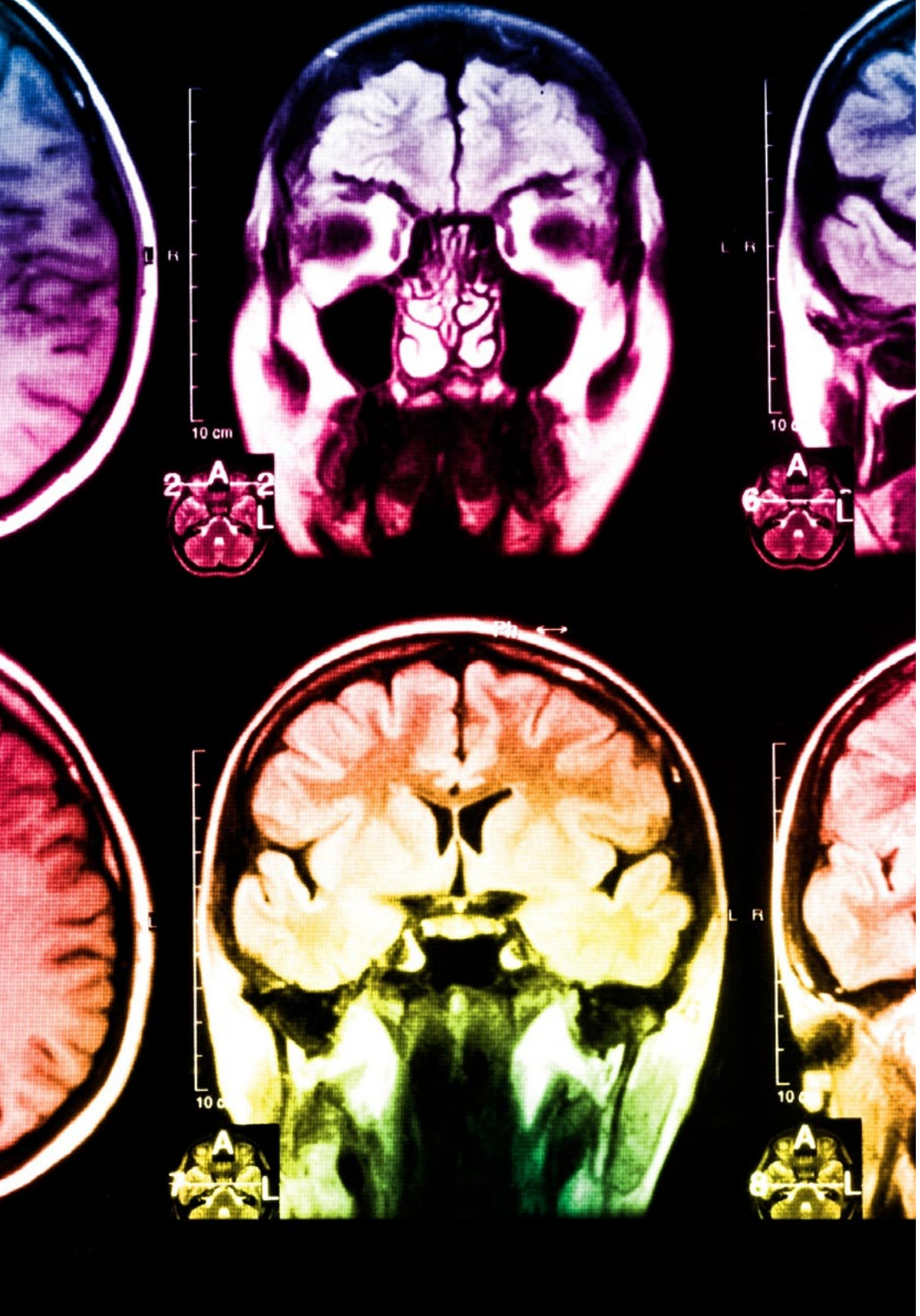
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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

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

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

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



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

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

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

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

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

Studienmaterial

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

Diese Inhalte werden dann auf das audiovisuelle Format angewendet, um die Online-Arbeitsmethode von TECH zu schaffen. All dies mit den neuesten Techniken, die in jedem einzelnen der Materialien, die dem Studenten zur Verfügung gestellt werden, qualitativ hochwertige Elemente bieten.

Meisterklassen

Die Nützlichkeit der Expertenbeobachtung ist wissenschaftlich belegt.

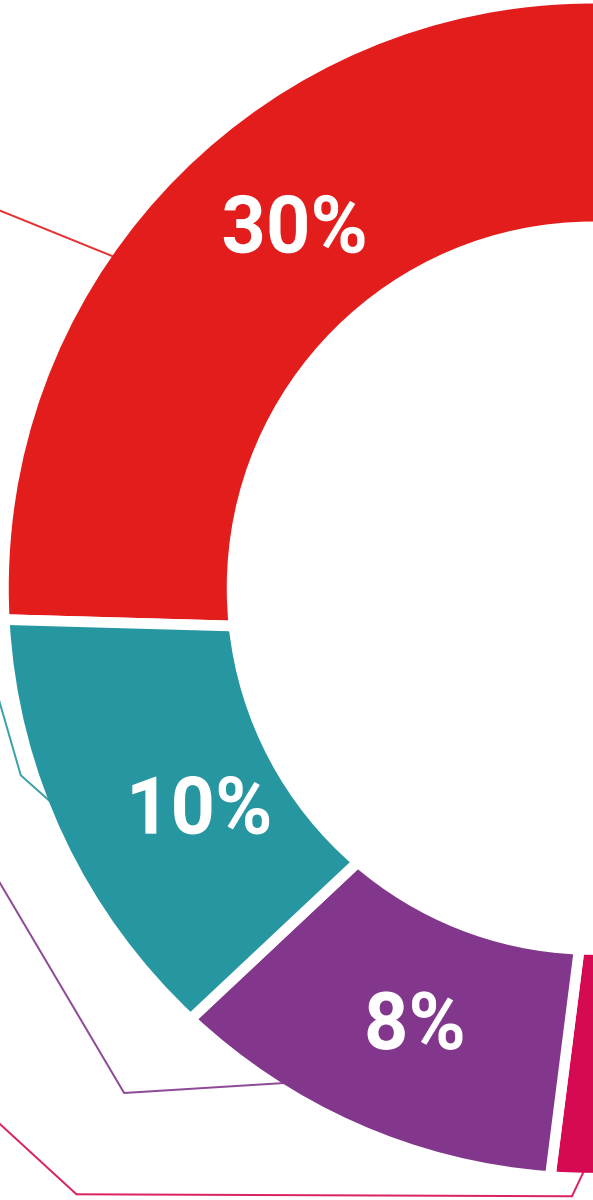
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

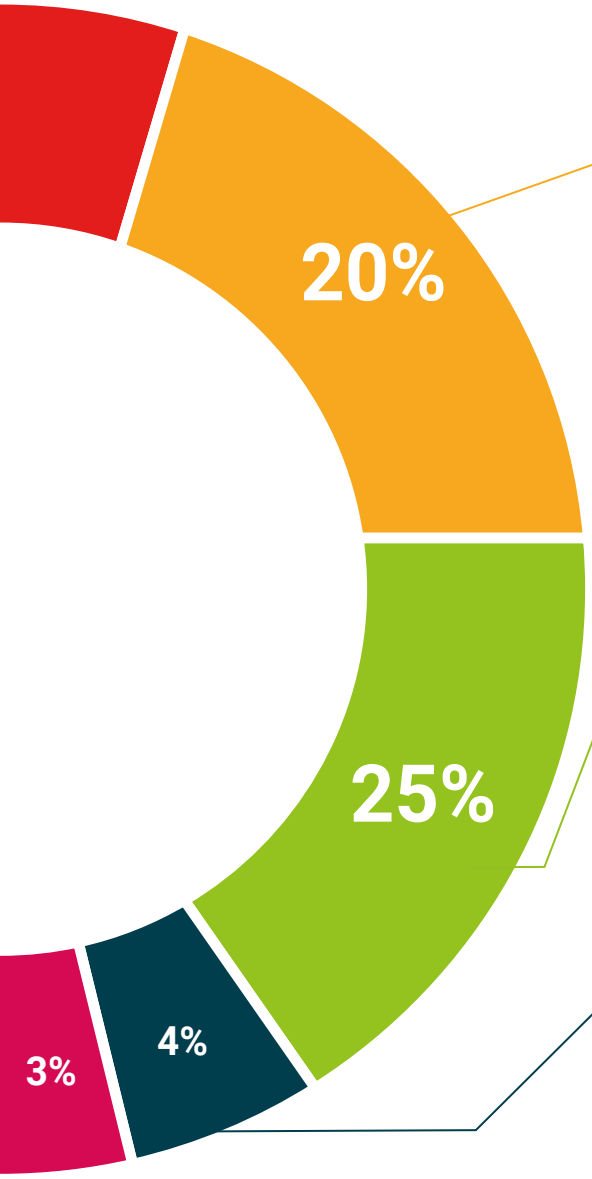
Übungen für Fertigkeiten und Kompetenzen

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

Weitere Lektüren

Aktuelle Artikel, Konsensdokumente und internationale Leitfäden, u. a. In der virtuellen Bibliothek von TECH hat der Student Zugang zu allem, was er für seine Fortbildung benötigt.





Case Studies

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

Interaktive Zusammenfassungen

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

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

Testing & Retesting

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

07

Qualifizierung

Der Privater Masterstudiengang in Verwaltung der Cybersicherheitspolitik im Unternehmen 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 **Privater Masterstudiengang in Verwaltung der Cybersicherheitspolitik im Unternehmen** enthält das vollständigste und aktuellste Programm auf dem Markt.

Sobald der Student die Prüfungen bestanden hat, erhält er/sie per Post* mit Empfangsbestätigung das entsprechende Diplom, ausgestellt von der **TECH Technologischen Universität.**

Das von **TECH Technologische Universität** ausgestellte Diplom drückt die erworbene Qualifikation aus und entspricht den Anforderungen, die in der Regel von Stellenbörsen, Auswahlprüfungen und Berufsbildungsausschüssen verlangt werden.

Titel: **Privater Masterstudiengang in Verwaltung der Cybersicherheitspolitik im Unternehmen**

Anzahl der offiziellen Arbeitsstunden: **1.500 Std.**


tech technologische universität

Verleiht dieses

DIPLOM

an

Herr/Frau _____, mit Ausweis-Nr. _____

Für den erfolgreichen Abschluss und die Akkreditierung des Programms

PRIVATER MASTERSTUDIENGANG

in

Verwaltung der Cybersicherheitspolitik im Unternehmen

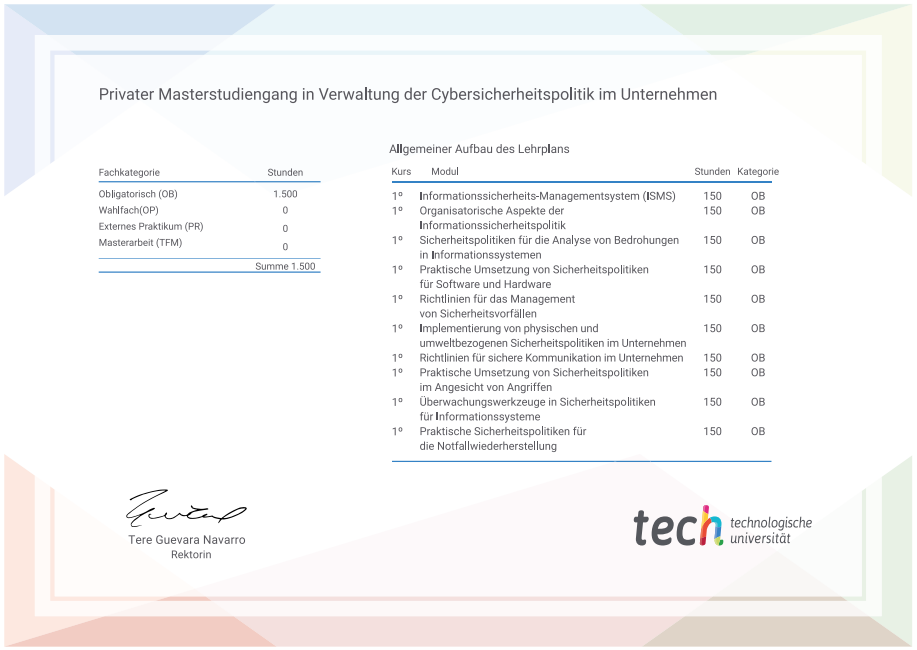
Es handelt sich um einen von dieser Universität verliehenen Abschluss, mit einer Dauer von 1.500 Stunden, mit Anfangsdatum tt/mm/jjjj und Enddatum tt/mm/jjjj.

TECH ist eine private Hochschuleinrichtung, die seit dem 28. Juni 2018 vom Ministerium für öffentliche Bildung anerkannt ist.

Zum 17. Juni 2020

Tere Guevara Navarro
Rektorin

einzigartiger Code TECH: AFWOR23S techtitute.com/titel


Privater Masterstudiengang in Verwaltung der Cybersicherheitspolitik im Unternehmen

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

Allgemeiner Aufbau des Lehrplans

Kurs	Modul	Stunden	Kategorie
1°	Informationssicherheits-Managementsystem (ISMS)	150	OB
1°	Organisatorische Aspekte der Informationssicherheitspolitik	150	OB
1°	Sicherheitspolitiken für die Analyse von Bedrohungen in Informationssystemen	150	OB
1°	Praktische Umsetzung von Sicherheitspolitiken für Software und Hardware	150	OB
1°	Richtlinien für das Management von Sicherheitsvorfällen	150	OB
1°	Implementierung von physischen und umweltbezogenen Sicherheitspolitiken im Unternehmen	150	OB
1°	Richtlinien für sichere Kommunikation im Unternehmen	150	OB
1°	Praktische Umsetzung von Sicherheitspolitiken im Angesicht von Angriffen	150	OB
1°	Überwachungswerkzeuge in Sicherheitspolitiken für Informationssysteme	150	OB
1°	Praktische Sicherheitspolitiken für die Notfallwiederherstellung	150	OB

Tere Guevara Navarro
Rektorin

tech technologische universität

*Haager Apostille. Für den Fall, dass der Student die Haager Apostille für sein Papierdiplom beantragt, wird TECH EDUCATION die notwendigen Vorkehrungen treffen, um diese gegen eine zusätzliche Gebühr zu beschaffen.

tech technologische universität

Privater Masterstudiengang

Verwaltung der Cybersicherheitspolitik im Unternehmen

- Modalität: **online**
- Dauer: **12 Monate**
- Qualifizierung: **TECH Technologische Universität**
- Aufwand: **16 Std./Woche**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Privater Masterstudiengang

Verwaltung der Cybersicherheitspolitik im Unternehmen

tech technologische universität