Esperto Universitario
Cibersicurezza Difensiva

tech università tecnologica

tech università tecnologica

Esperto Universitario
Cibersicurezza Difensiva

- Modalità: **online**
- Durata: **6 mesi**
- Titolo: **TECH Università Tecnologica**
- Orario: **a scelta**
- Esami: **online**

Accesso al sito web: www.techtitute.com/it/informatica/esperto-universitario/specializzazione-cibersicurezza-difensiva

Indice

01

Presentazione

Oggigiorno, quando la vita quotidiana è direttamente legata all'uso dei dispositivi mobili, conoscere le possibili vulnerabilità che provoca il fatto di utilizzarli è una necessità imperiosa per i professionisti dei settori tecnologici. Con l'evoluzione dei modelli è stata raggiunta una capacità inedita di impiegarli per qualsiasi lavoro, che li ha resi strumenti altamente sofisticati che accedono anche a dati sensibili personali e aziendali. Questo programma approfondirà tutti i modi in cui possono verificarsi attacchi informatici, sviluppando poi le strategie di sicurezza informatica difensiva più innovative ed efficaci del momento. Un percorso educativo di alto livello che consentirà di lavorare come specialista in questo campo.

Il percorso più completo sui pericoli e sulle vulnerabilità dei dispositivi mobili, così come sulla loro protezione informatica"

La sicurezza domestica e aziendale deve essere strutturata a strati, come una catena, la cui forza dipenderà dal suo anello più debole. Questo Esperto Universitario presenta le principali minacce di cui possono essere oggetto i computer degli utenti e i server in modo che siano in grado di prendere le misure appropriate e di prestare attenzione a qualsiasi evenienza.

Più nuove funzionalità ci sono e più comunichiamo tra di noi, più siamo esposti ad attacchi. In altre parole, le possibilità e i modi in cui i cybercriminali possono raggiungere i loro obiettivi sono in aumento. Motivo per cui i sistemi di difesa e monitoraggio della sicurezza devono evolversi continuamente. Perché in un mondo in cui il telelavoro e i servizi cloud sono sempre più diffusi, un *firewall* perimetrale tradizionale non è più sufficiente. In questo Esperto Universitario viene pertanto posto l'accento sull'importanza di concepire una difesa a più livelli, nota anche come "*Defense in Depth*", comprendendo tutti gli aspetti di una rete aziendale, dove alcuni dei concetti e dei sistemi che verranno discussi possono essere utilizzati e applicati anche in un ambiente domestico.

La sicurezza totale non esiste, ma se conosciamo i tipi di attacchi che affrontiamo, i rischi a cui siamo esposti e se disponiamo delle informazioni necessarie per affrontarli, avremo fatto un importante passo avanti e aggiunto un ulteriore livello di sicurezza alle nostre informazioni.

Questo **Esperto Universitario in Cibersicurezza Difensiva** possiede il programma più completo e aggiornato del mercato. Le caratteristiche principali del programma sono:

- Sviluppo di casi di studio presentati da esperti
- Contenuti grafici, schematici ed eminentemente pratici che forniscono informazioni scientifiche e pratiche sulle discipline essenziali per l'esercizio della professione
- Esercizi pratici che offrono un processo di autovalutazione per migliorare l'apprendimento
- Speciale enfasi sulle metodologie innovative
- Lezioni teoriche, domande all'esperto, forum di discussione su questioni controverse e compiti di riflessione individuale
- Contenuti disponibili da qualsiasi dispositivo fisso o mobile dotato di connessione a internet

Basa il tuo lavoro sulle conoscenze più approfondite dei tipi di rischio attualmente esistenti e sui mezzi di difesa applicabili in ciascun caso"

Un percorso di studi completo che ti permetterà di conoscere quali sono e come operano le attuali minacce informatiche come base per sviluppare strategie difensive"

Con un approccio completamente focalizzato sulla pratica, questo Esperto Universitario eleverà le tue capacità al livello di uno specialista.

Un processo educativo di prim'ordine creato per essere gestibile e flessibile, con la metodologia più interessante dell'insegnamento online.

Il personale docente del programma comprende rinomati professionisti del settore, nonché specialisti riconosciuti appartenenti a società e università prestigiose, che forniscono agli studenti le competenze necessarie a intraprendere un percorso di studio eccellente.

I contenuti multimediali, sviluppati in base alle ultime tecnologie educative, forniranno al professionista un apprendimento coinvolgente e localizzato, ovvero inserito in un contesto reale.

La creazione di questo programma è incentrata sull'Apprendimento Basato su Problemi, mediante il quale lo specialista deve cercare di risolvere le diverse situazioni che gli si presentano durante il corso. Lo studente potrà usufruire di un innovativo sistema di video interattivi creati da esperti di rinomata fama.

02

Obiettivi

Realizzare questo Esperto Universitario permette di aumentare in modo esponenziale la capacità di intervento in questo campo. Basato su obiettivi realistici e di alto interesse, questo processo di studio è mirato all'acquisizione delle conoscenze teoriche e pratiche necessarie ad intervenire con qualità, sviluppando inoltre competenze trasversali che consentano di affrontare situazioni complesse elaborando risposte mirate e precise.

Un aggiornamento completo su tutti gli aspetti che la sicurezza informatica difensiva ha sviluppato negli ultimi tempi"

Obiettivi generali

- Valutare la sicurezza dei computer degli utenti e dei server
- Esaminare le potenziali minacce in base all'ambiente di utilizzo
- Analizzare le soluzioni per ogni minaccia
- Sviluppare politiche di utilizzo appropriate
- Analizzare il quadro generale, l'importanza della difesa multistrato e dei sistemi di monitoraggio
- Esaminare i sistemi di rilevamento e prevenzione delle minacce più importanti
- Sviluppare soluzioni *firewall* su *Host Linux* e provider *Cloud*
- Valutare i nuovi sistemi di rilevamento delle minacce e la loro evoluzione rispetto alle soluzioni più tradizionali
- Generare soluzioni intelligenti complete per automatizzare il comportamento in caso di imprevisti
- Analizzare le principali piattaforme mobili attuali, le loro caratteristiche e il loro utilizzo
- Esaminare le vulnerabilità e le minacce esistenti, nonché i principali vettori di attacco
- Saper valutare i rischi associati alle vulnerabilità interne ed esterne all'azienda
- Identificare gli strumenti e le linee guida per la protezione dei dispositivi mobili
- Analizzare l'IoT in diversi settori oggi
- Esaminare l'evoluzione e l'impatto dell'IoT
- Determinare le parti di un progetto IoT
- Identificare, analizzare e valutare i rischi per la sicurezza delle parti di un progetto IoT

Obiettivi specifici

Modulo 1. Sicurezza in Host

- Specificare le politiche di *Backup* dei dati personali e professionali
- Valutare i diversi strumenti per fornire soluzioni a problemi di sicurezza specifici
- Stabilire i meccanismi per avere un sistema aggiornato
- Eseguire la scansione dell'apparecchiatura per individuare eventuali intrusi
- Determinare le regole di accesso al sistema
- Esaminare e classificare la posta per prevenire le frodi
- Generare elenchi di software consentiti

Modulo 2. Sicurezza di Rete (Perimetrale)

- Analizzare le attuali architetture di rete per identificare il perimetro da proteggere
- Sviluppare configurazioni specifiche di *firewall* e *Linux* per mitigare gli attacchi più comuni
- Raccogliere le soluzioni più comunemente utilizzate, come *Snort* e *Suricata*, e la loro configurazione
- Esaminare i diversi livelli aggiuntivi forniti dai *firewall* di nuova generazione e dalle funzionalità di rete negli ambienti *Cloud*
- Identificare gli strumenti per la protezione della rete e dimostrare perché sono fondamentali per una difesa a più livelli

Modulo 3. Sicurezza degli *smartphone*

- Esaminare i diversi vettori di attacco per evitare di diventare un bersaglio facile
- Determinare i principali attacchi e tipi di *Malware* a cui sono esposti gli utenti di dispositivi mobili
- Analizzare i dispositivi più recenti per stabilire una configurazione più sicura
- Specificare i passaggi principali per eseguire un test di intrusione su entrambe le piattaforme iOS e Android
- Sviluppare una conoscenza specialistica dei diversi strumenti di protezione e sicurezza
- Stabilire le migliori pratiche di programmazione orientata al mobile

Modulo 4. Sicurezza in IoT

- Analizzare le principali architetture IoT
- Esame delle tecnologie di connettività
- Sviluppare i principali protocolli di attuazione
- Specificare i diversi tipi di dispositivi esistenti
- Valutare i livelli di rischio e le vulnerabilità note
- Sviluppare politiche di utilizzo sicuro
- Stabilire condizioni d'uso appropriate per questi dispositivi

03

Direzione del corso

I docenti di questo programma sono stati scelti per la loro eccezionale competenza in questo campo. Combinano l'esperienza tecnica e pratica con l'insegnamento, offrendo agli studenti un supporto di primo livello per raggiungere i loro obiettivi. Contribuiscono quindi a offrire al programma la visione più diretta e immediata delle caratteristiche reali dell'intervento in questo campo, fornendo una panoramica contestuale del massimo interesse.

Questo corso offre una prospettiva diretta su una professione in costante movimento, grazie a professionisti esperti che forniranno la visione più realistica di questo lavoro"

Direttore Ospite Internazionale

Il Dott. Frederic Lemieux è riconosciuto a livello internazionale come esperto innovativo e leader ispiratore nei settori dell'**Intelligence, della Sicurezza Nazionale, della Sicurezza Interna, Cybersecurity** e delle **Tecnologie Dirompenti**. La sua dedizione costante e i suoi contributi rilevanti alla ricerca e all'istruzione lo posizionano come figura chiave nella promozione della sicurezza e della comprensione delle tecnologie emergenti di oggi. Nel corso della sua carriera professionale, ha ideato e condotto programmi accademici all'avanguardia presso diverse istituzioni rinomate, come l'**Università di Montreal,** la **George Washington University** e la **Georgetown University**.

Nel corso della sua vasta esperienza, ha pubblicato molti libri importanti, tutti relativi all'**intelligence criminale, alla polizia, alle minacce informatiche e alla sicurezza internazionale**. Ha anche contribuito in modo significativo al campo della cybersecurity pubblicando numerosi articoli su riviste accademiche che esaminano il controllo del crimine durante i grandi disastri, l'antiterrorismo, le agenzie di intelligence e la cooperazione di polizia. Inoltre, ha partecipato come relatore a diverse conferenze nazionali e internazionali, affermandosi come un importante accademico e professionista.

Lemieux ha ricoperto ruoli editoriali e di valutazione in diverse organizzazioni accademiche, private e governative, a testimonianza della sua influenza e del suo impegno per l'eccellenza nel suo campo di competenza. La sua prestigiosa carriera accademica lo ha portato a ricoprire il ruolo di Professore di Pratica e Direttore di Facoltà dei programmi MPS in **Intelligence Applicata, Gestione del Rischio di Cybersecurity, Gestione della Tecnologia e Gestione della Tecnologia dell'Informazione** presso la Georgetown University.

Dott. Lemieux, Frederic

- Ricercatore in Intelligence, Cybersecurity e Tecnologie dirompenti presso la Georgetown University
- Direttore del Master in Information Technology Management della Georgetown University
- Direttore del Master in Technology Management presso la Georgetown University
- Direttore del Master in Cybersecurity Risk Management dell'Università di Georgetow
- Direttore del Master in Applied Intelligence presso la Georgetown University
- Professore di Tirocini presso la Georgetown University
- Laurea in Sociologia, Minor Degree in Psicologia, Università Laval
- Dottorato di ricerca in Criminologia presso la School of Criminology dell'Università di Montreal
- Membro di: New Program Roundtable Committee, presso la Georgetown University

Grazie a TECH potrai imparare con i migliori professionisti del mondo"

Direzione

Dott.ssa Fernández Sapena, Sonia

- Formatrice in Sicurezza Informatica e Hacking Etico. Centro di Riferimento Nazionale per l'Informatica e le Telecomunicazioni di Getafe. Madrid
- Istruttrice certificata da E-Council. Madrid
- Formatrice nelle seguenti certificazioni: EXIN Ethical Hacking Foundation e EXIN Cyber & IT Security Foundation. Madrid
- Formatrice esperta accreditata dal CAM per i seguenti certificati di professionalità: Sicurezza Informatica (IFCT0190), Gestione di Reti di Voce e dati (IFCM0310), Amministrazione di Reti dipartimentali (IFCT0410), Gestione degli Allarmi nelle reti di telecomunicazione (IFCM0410), Operatore di Reti di voce e dati (IFCM0110) e Amministrazione di servizi internet (IFCT0509)
- Collaboratrice esterna CSO/SSA (Chief Security Officer/Senior Security Architect). Università delle Isole Baleari
- Ingegnere informatica. Università di Alcalá de Henares. Madrid
- Master in DevOps: Docker and Kubernetes. Cas-Training. Madrid
- Microsoft Azure Security Techonologies. Microsoft Azure Security Techonologies. Madrid

Personale docente

Dott. Catalá Barba, José Francisco

- Quadro intermedio nel MINISDEF. Diversi compiti e responsabilità all'interno del GOE III, come l'amministrazione e la gestione degli imprevisti della rete interna, l'attuazione di programmi su misura per le diverse aree, i corsi di formazione per gli utenti della rete e per il personale del gruppo in generale
- Tecnico elettronico nella Fabbrica Ford di Almusafes, a Valencia, si occupa di programmazione di robot, PLC, riparazione e manutenzione
- Tecnico Elettronico
- Sviluppatore di applicazioni per dispositivi mobili

Dott. Jiménez Ramos, Álvaro

- Analista Senior per la sicurezza presso The Workshop
- Analista di sicurezza informatica L1 presso Axians
- Analista di sicurezza informatica L2 presso Axians
- Analista di sicurezza informatica presso SACYR S.A.
- Laurea in Ingegneria Telematica conseguita presso l'Università Politecnica di Madrid
- Master in Cibersicurezza e Hacking Etico realizzato presso il CICE
- Corso Avanzato sulla Cibersicurezza organizzato da Deusto Formación

Dott.ssa Marcos Sbarbaro, Victoria Alicia

- Sviluppatrice di Applicazioni Mobili Native Android presso B60. Regno Unito
- Analista e Programmatrice per la gestione, il coordinamento e la documentazione dei sistemi di sicurezza e allarme virtualizzati in client
- Analista e Programmatrice di applicazioni Java per bancomat in client
- Professionista dello Sviluppo Software per la convalida della firma e la gestione dei documenti in client
- Tecnico di sistema per la migrazione delle apparecchiature e per la gestione, la manutenzione e la formazione dei dispositivi mobili PDA in client
- Ingegneria tecnica dei Sistemi Informatici. Università Politecnica della Catalogna
- Master Universitario in Sicurezza Informatica e Hacking Etico organizzato da EC-Council e CompTIA presso la Scuola Professionale di Nuove Tecnologie CICE

Dott. Peralta Alonso, Jon

- Avvocato / DPO presso Altia Consultores S.A.
- Docente del Master in Protezione dei Dati Personali, Cybersecurity e Diritto dell'ICT. Università Pubblica dei Paesi Baschi (UPV-EHU)
- Avvocato / Consulente legale. Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Consulente legale / Apprendista. Studio professionale: Oscar Padura
- Laurea in Giurisprudenza Università Pubblica dei Paesi Baschi
- Master in Protezione dei Dati. EIS Innovative School
- Master Universitario in Giurisprudenza. Università Pubblica dei Paesi Baschi
- Master in Pratica del Contenzioso Civile. Università Internazionale Isabella I di Castiglia

04

Struttura e contenuti

Questo Esperto Universitario offre un'analisi completa di ciascuno dei campi che il professionista della sicurezza informatica deve conoscere nell'ambito delle attività di difesa. Il programma è strutturato quindi in modo che lo studente acquisisca in maniera efficiente concetti complementari che ne favoriscano l'internalizzazione e consolidino quanto studiato, dotandolo di capacità di intervento efficaci. Un percorso ad alta intensità e di grande qualità creato per preparare i migliori professionisti del settore.

In questo corso troverai aspetti relativi all'intervento in materia di cibersicurezza difensiva sviluppati in modo strutturato e da un approccio di studio incentrato sull'efficienza"

Modulo 1. Sicurezza in *Host*

1.1. Copie di backup
- 1.1.1. Strategie per i backup
- 1.1.2. Strumenti per Windows
- 1.1.3. Strumenti per Linux
- 1.1.4. Strumenti per MacOS

1.2. Antivirus per l'utente
- 1.2.1. Tipi di antivirus
- 1.2.2. Antivirus per Windows
- 1.2.3 Antivirus per Linux
- 1.2.4. Antivirus per MacOS
- 1.2.5. Antivirus per smartphone

1.3. Rilevatori di intrusione - HIDS
- 1.3.1. Metodi di rilevamento delle intrusioni
- 1.3.2. Sagan
- 1.3.3 Aide
- 1.3.4. *Rkhunter*

1.4. *Firewall* locale
- 1.4.1. *Firewall* per Windows
- 1.4.2. *Firewall* per Linux
- 1.4.3. *Firewall* per MacOS

1.5. Gestire le password
- 1.5.1. Password
- 1.5.2. *LastPass*
- 1.5.3. *KeePass*
- 1.5.4. *Sticky password*
- 1.5.5. RoboForm

1.6. Rilevatori di *phishing*
- 1.6.1. Rilevamento manuale del *phishing*
- 1.6.2. Strumenti *antiphishing*

1.7. *Spyware*
- 1.7.1. Meccanismi di prevenzione
- 1.7.2. Strumenti *antispyware*

1.8. Tracciatori
- 1.8.1. Misure di protezione del sistema
- 1.8.2. Strumenti anti-tracciamento

1.9. *EDR - End point Detection and Response*
- 1.9.1. Comportamento del sistema EDR
- 1.9.2. Differenze tra EDR e antivirus
- 1.9.3. Il futuro dei sistemi EDR

1.10. Controllo sull'installazione del software
- 1.10.1. Repository e negozi di software
- 1.10.2. Elenchi di software consentiti o vietati
- 1.10.3. Criteri di aggiornamento
- 1.10.4. Privilegi per l'installazione di software

Modulo 2. Sicurezza di Rete (Perimetrale)

2.1. Sistemi di rilevamento e prevenzione delle minacce
- 2.1.1. Quadro generale per gli incidenti di sicurezza
- 2.1.2. Sistemi di difesa attuali: *defense in depth* e SOC
- 2.1.3. Le attuali architetture di rete
- 2.1.4. Tipi di strumenti di rilevamento e prevenzione degli incidenti
  - 2.1.4.1. Sistemi basati sulla rete
  - 2.1.4.2. Sistemi basati su *Host*
  - 2.1.4.3. Sistemi centralizzati
- 2.1.5. Comunicazione e rilevamento di istanze/*host*, container e *serverless*

2.2. *Firewall*
- 2.2.1. Tipi di *Firewall*
- 2.2.2. Attacchi e contenimento
- 2.2.3. *Firewalls* comuni nel *Kernel* Linux
  - 2.2.3.1. UFW
  - 2.2.3.2. Nftables e iptables
  - 2.2.3.3. *FirewallD*
- 2.2.4. Sistemi di rilevamento basati sui *log* di sistema
  - 2.2.4.1. TCP *wrappers*
  - 2.2.4.2. *BlockHosts* e *DenyHosts*
  - 2.2.4.3. Fail2Ban

2.3. Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)
- 2.3.1. Attacchi agli IDS/IPS
- 2.3.2. Sistemi IDS/IPS
  - 2.3.2.1. *Snort*
  - 2.3.2.2. Suricata

2.4. *Firewall* di nuova generazione (NGFW)
- 2.4.1. Differenze tra NGFW e *Firewall* tradizionali
- 2.4.2. Funzionalità chiave
- 2.4.3. Soluzioni commerciali
- 2.4.4. *Firewall* per servizi *Cloud*
  - 2.4.4.1. Architettura VPC del Cloud
  - 2.4.4.2. ACL per il*Cloud*
  - 2.4.4.3. *Security Group*

2.5. *Proxy*
- 2.5.1. Tipi di *Proxy*
- 2.5.2. Uso di *Proxy*. Vantaggi e svantaggi

2.6. Motori antivirus
- 2.6.1. Contesto generale del *Malware* degli IoC
- 2.6.2. Problemi del motore antivirus

2.7. Sistemi di protezione della posta
- 2.7.1. Antispam
  - 2.7.1.1. Liste bianche e nere
  - 2.7.1.2. Filtri bayesiani
- 2.7.2. *Mail Gateway*(MGW)

2.8. SIEM
- 2.8.1. Componenti e architettura
- 2.8.2. Regole di correlazione e casi d'uso
- 2.8.3. Sfide attuali per i sistemi SIEM

2.9. SOAR
- 2.9.1. SOAR e SIEM: nemici o alleati
- 2.9.2. Il futuro dei sistemi SOAR

2.10. Altri Sistemi basati sulla rete
- 2.10.1. WAF
- 2.10.2. NAC
- 2.10.3. *HoneyPots* e *HoneyNets*
- 2.10.4. CASB

Modulo 3. Sicurezza degli smartphone

3.1. Il mondo dei dispositivi mobili
- 3.1.1. Tipi di piattaforme mobili
- 3.1.2. Dispositivi IOS
- 3.1.3. Dispositivi Android

3.2. Gestione della sicurezza mobile
- 3.2.1. Progetto OWASP sulla Sicurezza mobile
  - 3.2.1.1. I 10 punti deboli più importanti
- 3.2.2. Comunicazioni, reti e modalità di connessione

3.3. Il dispositivo mobile in ambito aziendale
- 3.3.1. Rischi
- 3.3.2. Politiche di sicurezza
- 3.3.3. Monitoraggio del dispositivo
- 3.3.4. Gestione dei dispositivi mobili (MDM)

3.4. Privacy degli Utenti e sicurezza dei dati
- 3.4.1. Stati di informazione
- 3.4.2. Protezione dei dati e riservatezza
  - 3.4.2.1. Permessi
  - 3.4.2.2. Crittografia
- 3.4.3. Archiviazione sicura dei dati
  - 3.4.3.1. Archiviazione sicura su iOS
  - 3.4.3.2. Archiviazione sicura su Android
- 3.4.4. Buone pratiche nello sviluppo di applicazioni

3.5. Punti deboli e vettori di attacco
- 3.5.1. Vulnerabilità
- 3.5.2. Vettori di attacco
  - 3.5.2.1. *Malware*
  - 3.5.2.2. Infiltrazione di dati
  - 3.5.2.3. Manipolazione dei dati

3.6. Principali minacce
- 3.6.1. Utente non obbligato
- 3.6.2. *Malware*
  - 3.6.2.1. Tipi di *Malware*
- 3.6.3. Ingegneria sociale
- 3.6.4. Perdite di dati
- 3.6.5. Furto di informazioni
- 3.6.6. Reti WiFi non sicure
- 3.6.7. Software obsoleto
- 3.6.8. Applicazioni dannose
- 3.6.9. Password insicure
- 3.6.10. Impostazioni di sicurezza deboli o inesistenti
- 3.6.11. Accesso fisico
- 3.6.12. Perdita o furto del dispositivo
- 3.6.13. Furto d'identità (Integrità)
- 3.6.14. Criptografia debole o non funzionante
- 3.6.15. Negazione del servizio (DoS)

3.7. Principali attacchi
- 3.7.1. Attacchi di *phishing*
- 3.7.2. Attacchi legati alle modalità di comunicazione
- 3.7.3. Attacchi di *smishing*
- 3.7.4. Attacchi di *Criptojacking*
- 3.7.5. *Man in the middle*

3.8. *Hacking*
- 3.8.1. *Rooting* e *Jailbreaking*
- 3.8.2. Anatomia di un attacco mobile
  - 3.8.2.1. Propagazione della minaccia
  - 3.8.2.2. Installazione di *Malware* sul dispositivo
  - 3.8.2.3. Persistenza
  - 3.8.2.4. Esecuzione del *Payload* ed estrazione delle informazioni
- 3.8.3. Hacking sui dispositivi iOS: meccanismi e strumenti
- 3.8.4. Hacking sui dispositivi Android: meccanismi e strumenti

3.9. Test di intrusione
- 3.9.1. iOS *pentesting*
- 3.9.2. Android *pentesting*
- 3.9.3. Strumenti

3.10. Sicurezza e protezione
- 3.10.1. Impostazioni di sicurezza
  - 3.10.1.1. Su dispositivi iOS
  - 3.10.1.2. Su dispositivi Android
- 3.10.2. Misure di sicurezza
- 3.10.3. Strumenti di protezione

Modulo 4. Sicurezza in IoT

4.1. Dispositivi
- 4.1.1. Tipi di dispositivi
- 4.1.2. Architetture standardizzate
  - 4.1.2.1. OneM2M
  - 4.1.2.2. IoTWF
- 4.1.3. Protocolli di implementazione
- 4.1.4. Tecnologie di connettività

4.2. Dispositivi IoT. Aree di applicazione
- 4.2.1. SmartHome
- 4.2.2. SmartCity
- 4.2.3. Trasporto
- 4.2.4. *Wearable*
- 4.2.5. Settore sanitario
- 4.2.6. IIoT

4.3. Protocolli di comunicazione
- 4.3.1. MQTT
- 4.3.2. LWM2M
- 4.3.3 OMA-DM
- 4.3.4. TR-069

4.4. SmartHome
- 4.4.1. Domotica
- 4.4.2. Reti
- 4.4.3. Elettrodomestici
- 4.4.4. Sorveglianza e sicurezza

4.5. SmartCity
- 4.5.1. Illuminazione
- 4.5.2. Meteorologia
- 4.5.3. Sicurezza

4.6. Trasporto
- 4.6.1. Localizzazione
- 4.6.2. Effettuare pagamenti e ottenere servizi
- 4.6.3. Connettività

4.7. Wearable
- 4.7.1. Abiti intelligenti
- 4.7.2. Gioielli intelligenti
- 4.7.3. Smartwatch

4.8. Settore sanitario
- 4.8.1. Monitoraggio dell'esercizio e della frequenza cardiaca
- 4.8.2. Monitoraggio di pazienti e anziani
- 4.8.3. Impiantabili
- 4.8.4. Robot chirurgici

4.9. Connettività
- 4.9.1. WiFi
- 4.9.2. Bluetooth
- 4.9.3. Connettività integrata

4.10. Cartolarizzazione
- 4.10.1. Reti dedicate
- 4.10.2. Gestione password
- 4.10.3. Utilizzo di protocolli criptati
- 4.10.4. Suggerimenti per l'uso

05

Metodologia

Questo programma ti offre un modo differente di imparare. La nostra metodologia si sviluppa in una modalità di apprendimento ciclico: ***il Relearning***.

Questo sistema di insegnamento viene applicato nelle più prestigiose facoltà di medicina del mondo ed è considerato uno dei più efficaci da importanti pubblicazioni come il ***New England Journal of Medicine.***

Scopri il Relearning, un sistema che abbandona l'apprendimento lineare convenzionale, per guidarti attraverso dei sistemi di insegnamento ciclici: una modalità di apprendimento che ha dimostrato la sua enorme efficacia, soprattutto nelle materie che richiedono la memorizzazione"

Caso di Studio per contestualizzare tutti i contenuti

Il nostro programma offre un metodo rivoluzionario per sviluppare le abilità e le conoscenze. Il nostro obiettivo è quello di rafforzare le competenze in un contesto mutevole, competitivo e altamente esigente.

Con TECH potrai sperimentare un modo di imparare che sta scuotendo le fondamenta delle università tradizionali in tutto il mondo"

Avrai accesso a un sistema di apprendimento basato sulla ripetizione, con un insegnamento naturale e progressivo durante tutto il programma.

Imparerai, attraverso attività collaborative e casi reali, la risoluzione di situazioni complesse in ambienti aziendali reali.

Un metodo di apprendimento innovativo e differente

Questo programma di TECH consiste in un insegnamento intensivo, creato ex novo, che propone le sfide e le decisioni più impegnative in questo campo, sia a livello nazionale che internazionale. Grazie a questa metodologia, la crescita personale e professionale viene potenziata, effettuando un passo decisivo verso il successo. Il metodo casistico, la tecnica che sta alla base di questi contenuti, garantisce il rispetto della realtà economica, sociale e professionale più attuali.

> *Il nostro programma ti prepara ad affrontare nuove sfide in ambienti incerti e a raggiungere il successo nella tua carriera"*

Il Metodo Casistico è stato il sistema di apprendimento più usato nelle migliori Scuole di Informatica del mondo da quando esistono. Sviluppato nel 1912 affinché gli studenti di Diritto non imparassero la legge solo sulla base del contenuto teorico, il metodo casistico consisteva nel presentare loro situazioni reali e complesse per prendere decisioni informate e giudizi di valore su come risolverle. Nel 1924 fu stabilito come metodo di insegnamento standard ad Harvard.

Cosa dovrebbe fare un professionista per affrontare una determinata situazione? Questa è la domanda con cui ti confrontiamo nel metodo dei casi, un metodo di apprendimento orientato all'azione. Durante il corso, gli studenti si confronteranno con diversi casi di vita reale. Dovranno integrare tutte le loro conoscenze, effettuare ricerche, argomentare e difendere le proprie idee e decisioni.

Metodologia Relearning

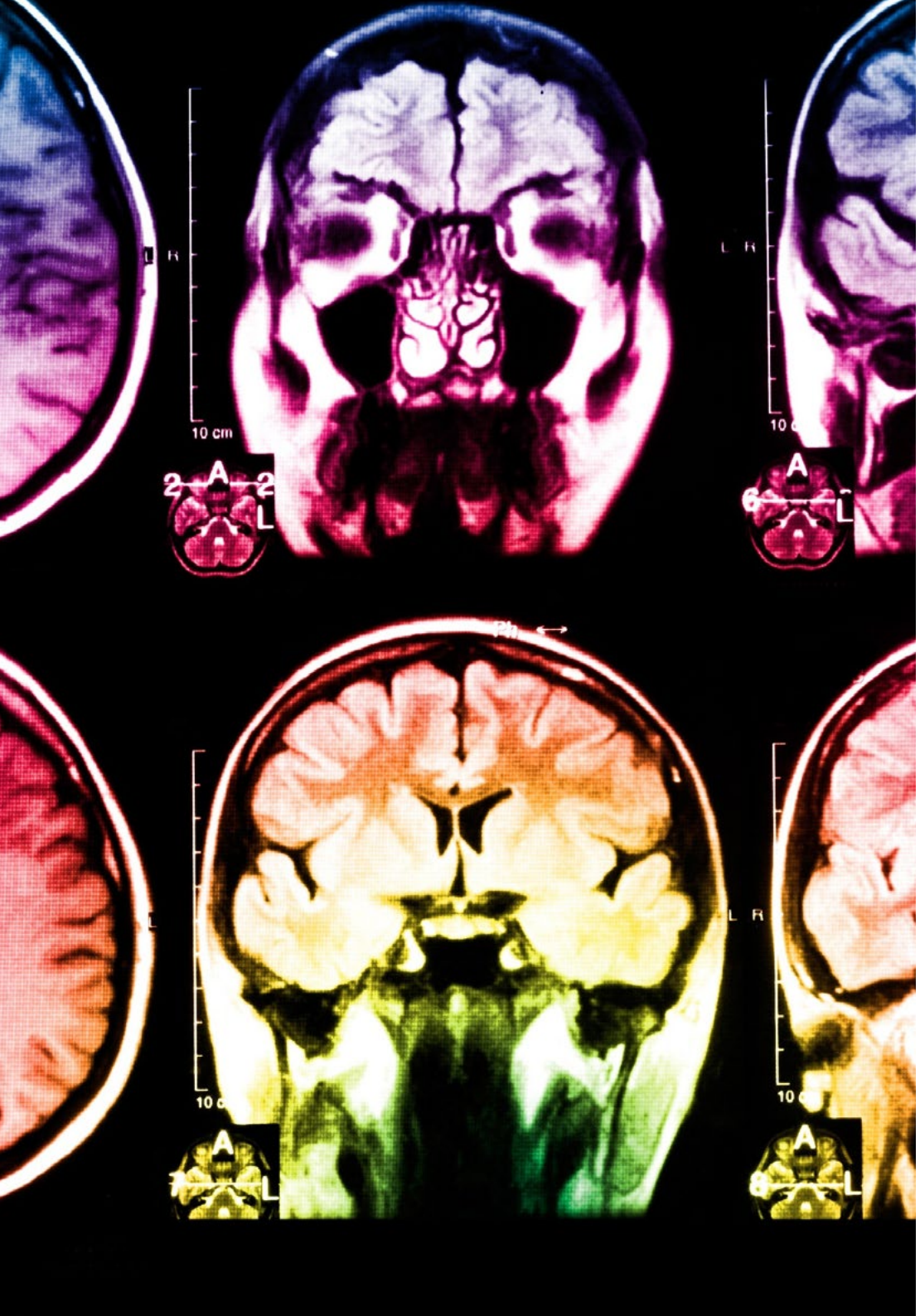
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

Potenziamo il Caso di Studio con il miglior metodo di insegnamento 100% online: il Relearning.

Nel 2019 abbiamo ottenuto i migliori risultati di apprendimento di tutte le università online del mondo.

In TECH imparerai con una metodologia all'avanguardia progettata per formare i manager del futuro. Questo metodo, all'avanguardia della pedagogia mondiale, si chiama Relearning.

La nostra università è l'unica autorizzata a utilizzare questo metodo di successo. Nel 2019, siamo riusciti a migliorare il livello di soddisfazione generale dei nostri studenti (qualità dell'insegnamento, qualità dei materiali, struttura del corso, obiettivi...) rispetto agli indicatori della migliore università online.



Nel nostro programma, l'apprendimento non è un processo lineare, ma avviene in una spirale (impariamo, disimpariamo, dimentichiamo e re-impariamo). Pertanto, combiniamo ciascuno di questi elementi in modo concentrico. Questa metodologia ha formato più di 650.000 laureati con un successo senza precedenti in campi diversi come la biochimica, la genetica, la chirurgia, il diritto internazionale, le competenze manageriali, le scienze sportive, la filosofia, il diritto, l'ingegneria, il giornalismo, la storia, i mercati e gli strumenti finanziari. Tutto questo in un ambiente molto esigente, con un corpo di studenti universitari con un alto profilo socio-economico e un'età media di 43,5 anni.

Il Relearning ti permetterà di apprendere con meno sforzo e più performance, impegnandoti maggiormente nella tua specializzazione, sviluppando uno spirito critico, difendendo gli argomenti e contrastando le opinioni: un'equazione diretta al successo.

Dalle ultime evidenze scientifiche nel campo delle neuroscienze, non solo sappiamo come organizzare le informazioni, le idee, le immagini e i ricordi, ma sappiamo che il luogo e il contesto in cui abbiamo imparato qualcosa è fondamentale per la nostra capacità di ricordarlo e immagazzinarlo nell'ippocampo, per conservarlo nella nostra memoria a lungo termine.

In questo modo, e in quello che si chiama Neurocognitive Context-dependent E-learning, i diversi elementi del nostro programma sono collegati al contesto in cui il partecipante sviluppa la sua pratica professionale.

Questo programma offre i migliori materiali didattici, preparati appositamente per i professionisti:

Materiale di studio

Tutti i contenuti didattici sono creati appositamente per il corso dagli specialisti che lo impartiranno, per fare in modo che lo sviluppo didattico sia davvero specifico e concreto.

Questi contenuti sono poi applicati al formato audiovisivo che supporterà la modalità di lavoro online di TECH. Tutto questo, con le ultime tecniche che offrono componenti di alta qualità in ognuno dei materiali che vengono messi a disposizione dello studente.

Master class

Esistono evidenze scientifiche sull'utilità dell'osservazione di esperti terzi.

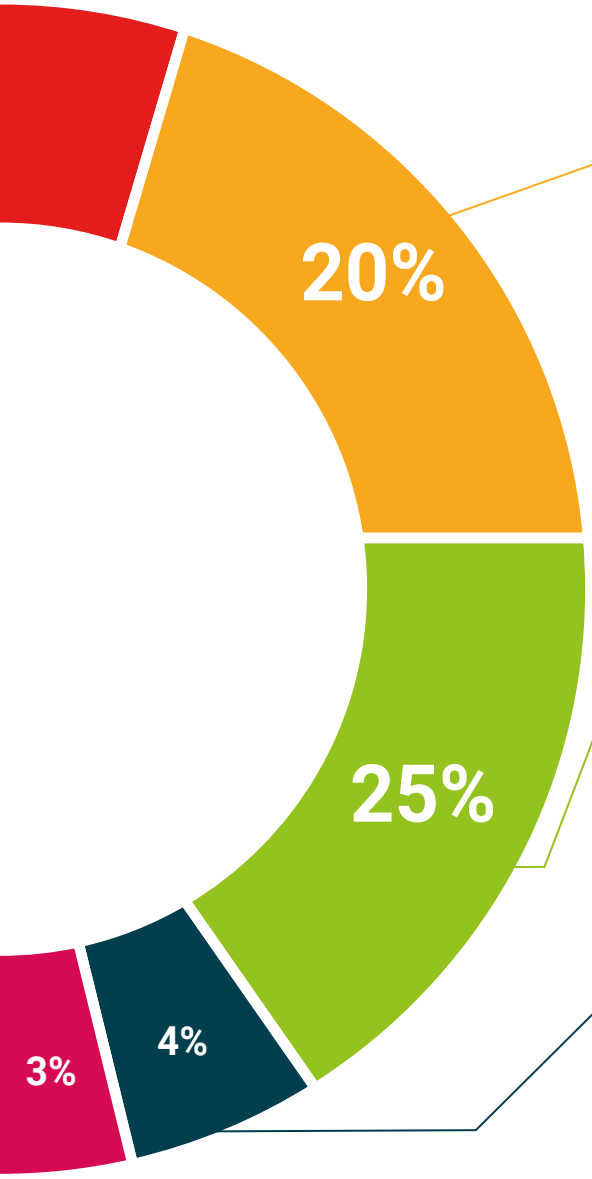
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

Pratiche di competenze e competenze

Svolgerai attività per sviluppare competenze e capacità specifiche in ogni area tematica. Pratiche e dinamiche per acquisire e sviluppare le competenze e le abilità che uno specialista deve sviluppare nel quadro della globalizzazione in cui viviamo.

Letture complementari

Articoli recenti, documenti di consenso e linee guida internazionali, tra gli altri. Nella biblioteca virtuale di TECH potrai accedere a tutto il materiale necessario per completare la tua specializzazione.



Casi di Studio

Completerai una selezione dei migliori casi di studio scelti appositamente per questo corso. Casi presentati, analizzati e monitorati dai migliori specialisti del panorama internazionale.

Riepiloghi interattivi

Il team di TECH presenta i contenuti in modo accattivante e dinamico in pillole multimediali che includono audio, video, immagini, diagrammi e mappe concettuali per consolidare la conoscenza.

Questo esclusivo sistema di specializzazione per la presentazione di contenuti multimediali è stato premiato da Microsoft come "Caso di successo in Europa".

Testing & Retesting

Valutiamo e rivalutiamo periodicamente le tue conoscenze durante tutto il programma con attività ed esercizi di valutazione e autovalutazione, affinché tu possa verificare come raggiungi progressivamente i tuoi obiettivi.

06

Titolo

L'Esperto Universitario in Cibersicurezza Difensiva garantisce, oltre alla preparazione più rigorosa e aggiornata, il conseguimento di una qualifica di Esperto Universitario rilasciata da TECH Università Tecnologica.

Porta a termine questo programma e ricevi la tua qualifica universitaria senza spostamenti o fastidiose formalità”

Questo **Esperto Universitario in Cibersicurezza Difensiva** possiede il programma scientifico più completo e aggiornato del mercato.

Dopo aver superato le valutazioni, lo studente riceverà, mediante lettera certificata con ricevuta di ritorno, la corrispondente qualifica di **Esperto Universitario** rilasciata da **TECH Università Tecnologica**.

Il titolo rilasciato da **TECH Università Tecnologica** esprime la qualifica ottenuta nell'Esperto Universitario, e riunisce tutti i requisiti comunemente richiesti da borse di lavoro, concorsi e commissioni di valutazione di carriere professionali..

Titolo: **Esperto Universitario in Cibersicurezza Difensiva**

Ore Ufficiali: **600**


tech università tecnologica

Conferisce il presente

DIPLOMA

a

Dott./Dott.ssa _____, con documento d'identità n°_____

Per aver completato con esito positivo e accreditato il programma di

ESPERTO UNIVERSITARIO

in

Cibersicurezza Difensiva

Si tratta di un titolo rilasciato da questa Università ed equivalente a 600 ore, con data di inizio gg/mm/aaaa e con data di fine gg/mm/aaaa.

TECH è un Istituto Privato di Istruzione Superiore riconosciuto dal Ministero della Pubblica Istruzione a partire dal 28 giugno 2018.

In data 7 Giugno 2020

Tere Guevara Navarro
Rettrice

codice unico TECH: AFWORD23S techtitute.com/titulos

*Apostille dell'Aia. Se lo studente dovesse richiedere che il suo diploma cartaceo sia provvisto di Apostille dell'Aia, TECH EDUCATION effettuerà le gestioni opportune per ottenerla pagando un costo aggiuntivo.

tech università tecnologica

Esperto Universitario
Cibersicurezza Difensiva

- Modalità: **online**
- Durata: **6 mesi**
- Titolo: **TECH Università Tecnologica**
- Orario: **a scelta**
- Esami: **online**

Esperto Universitario
Cibersicurezza Difensiva

tech università tecnologica