Esperto Universitario
Cibersicurezza Correttiva e Perizia Forense

tech global university

tech global university

Esperto Universitario
Cibersicurezza Correttiva e Perizia Forense

- Modalità: **online**
- Durata: **6 mesi**
- Titolo: **TECH Global University**
- Accreditamento: **18 ECTS**
- Orario: **a scelta**
- Esami: **online**

Accesso al sito web: www.techtitute.com/it/informatica/specializzazione/specializzazione-cibersicurezza-correttiva-perizia-forense

Indice

01

Presentazione

In un mondo che cambia e si evolve ogni giorno, con tecnologie che emergono e vengono adottate rapidamente senza essere ancora comprovate al 100%, dobbiamo essere pronti ad affrontare molte sfide e prevedere l'impatto che avranno sulla società. Questo programma prepara l'ingegnere informatico ad indagare su un incidente di sicurezza informatica una volta che si è verificato, dotandolo di conoscenze e meccanismi per ottenere, analizzare e riportare tutte le sue scoperte, dato che dal momento in cui un perito forense individua la scena del crimine e decide, in modo non distruttivo, di acquisire le prove, ha bisogno di linee guida per collegare i dati ottenuti da diverse fonti e giungere a conclusioni irrefutabili.

Acquisisci la capacità di fornire gli elementi chiave per indagare su un incidente di sicurezza informatica con le conoscenze più aggiornate nella perizia forense in questo settore"

Nell'ambiente informatico sono vari i motivi per cui applichiamo diverse Tecniche di Ingegneria Inversa, allo scopo di capire e conoscere meglio un software, un protocollo di comunicazione o un algoritmo.

Una delle applicazioni più conosciute di Ingegneria Inversa è l'analisi del *malware* che, attraverso diverse tecniche come il *sandboxing*, permetterà di capire e conoscere il software dannoso oggetto di studio e, così, lo sviluppo di un software in grado di rilevarlo e contrastarlo, come nel caso degli antivirus che lavorano su firme.

A volte la vulnerabilità non si trova nel codice sorgente, ma viene introdotta dal compilatore che genera il codice macchina. La conoscenza dell'Ingegneria Inversa, e quindi di come otteniamo il codice macchina, ci permetterà di rilevare tali vulnerabilità.

Per poter realizzare queste azioni è necessario conoscere i diversi scenari, comprendere le diverse tecnologie ed essere in grado di spiegarle in diversi linguaggi a seconda del pubblico a cui il rapporto si rivolge. La quantità di reati che un perito forense deve affrontare richiede abilità, intuizione e serenità per affrontare questo compito estremamente importante poiché dal suo corretto svolgimento può dipendere il verdetto di un processo.

Il professionista di questo settore deve avere una visione ampia e periferica per individuare non solo i benefici di queste tecnologie, ma anche i possibili danni. Questo programma prepara a capire che cosa verrà, come può influenzare le professioni attuali, come possono essere esercitate e cosa può accadere in un futuro a volte incerto.

Questo **Esperto Universitario in Cibersicurezza Correttiva e Perizia Forense** 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

Comprendi le basi e le modalità di funzionamento di un malware come base per creare modalità efficaci di affrontarlo"

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

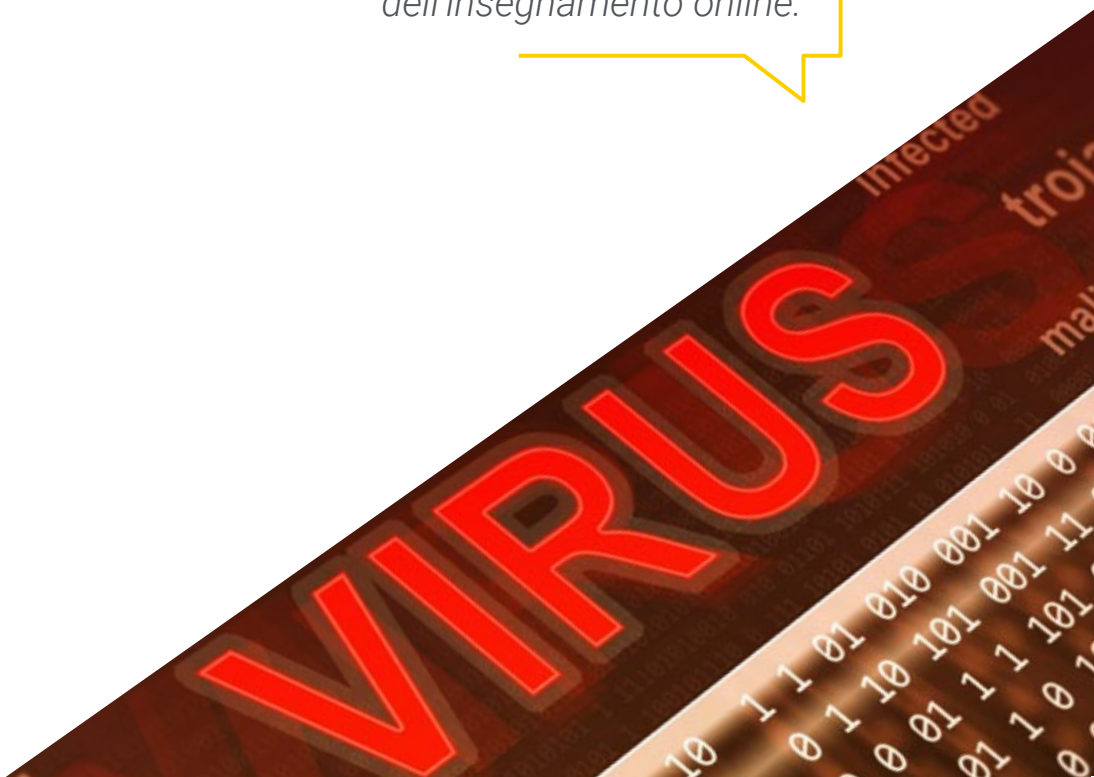
Un apprendimento che ti permetterà di intervenire come esperto forense in cibersicurezza, nell'area legale.

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 riconosciuti specialisti appartenenti a società scientifiche 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

Questo Esperto Universitario amplia la capacità di intervento in questo campo degli studenti, in modo rapido e semplice. Basato su obiettivi realistici e di alto interesse, questo processo di studio è mirato all'acquisizione delle conoscenze teoriche e pratiche necessarie a realizzare di intervenire con qualità sviluppando inoltre competenze trasversali che consentano di affrontare situazioni complesse, elaborando risposte mirate e precise.

Un apprendimento intensivo in materia di Cibersicurezza Correttiva e Perizia Forense che ti permetterà di ampliare le tue prospettive di lavoro in un campo pieno di opportunità professionali"

Obiettivi generali

- Analizzare l'Ingegneria Inversa e le sue diverse tecniche
- Esaminare le diverse architetture e come influenzano l'Ingegneria Inversa
- Determinare in quali condizioni utilizzare le diverse tecniche di Ingegneria Inversa
- Applicare l'Ingegneria Inversa all'ambiente della cibersicurezza
- Raccogliere tutte le prove e i dati esistenti per realizzare un rapporto forense
- Analizzare i dati e metterli in collegamento
- Preservare le prove per realizzare un rapporto forense
- Presentare regolarmente il rapporto forense
- Analizzare lo stato attuale e futuro della sicurezza informatica
- Esaminare i rischi delle tecnologie nuove ed emergenti
- Raccogliere le diverse tecnologie in relazione alla sicurezza informatica

Obiettivi specifici

Modulo 1. Ingegneria inversa

- Analizzare le fasi di un compilatore
- Esaminare l'architettura del processore x86 e l'architettura del processore ARM
- Determinare i diversi tipi di analisi
- Applicare il *Sandboxing* in diversi ambienti
- Sviluppare diverse tecniche di analisi del *Malware*
- Stabilire strumenti orientati all'analisi del *Malware*

Modulo 2. Analisi forense

- Identificare i diversi elementi che rivelano un reato
- Generare conoscenze specializzate per ottenere dati da diversi supporti prima che vadano persi
- Recuperare i dati cancellati intenzionalmente
- Analizzare i Log e le registrazioni del sistema
- Determinare il modo in cui i dati vengono duplicati per non alterare gli originali
- Dimostrare che le prove sono coerenti
- Generare un rapporto solido e senza interruzioni
- Presentare le conclusioni in modo coerente
- Stabilire come difendere la relazione davanti all'autorità competente
- Concretizzare le strategie per un telelavoro sicuro

Modulo 3. Le sfide attuali e future della sicurezza informatica

- Esaminare l'uso delle criptovalute, l'impatto sull'economia e la sicurezza
- Analizzare la situazione degli utenti e il grado di analfabetismo digitale
- Determinare l'ambito di utilizzo di *blockchain*
- Presentare alternative a IPv4 nell'indirizzamento di rete
- Sviluppare strategie per formare la popolazione all'uso corretto delle tecnologie
- Generare conoscenze specialistiche per affrontare nuove sfide di sicurezza ed evitare il phishing
- Concretizzare le strategie per un telelavoro sicuro

Acquisisci le competenze necessarie a preparare e presentare una relazione completa e di qualità all'autorità competente"

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.

Docenti esperti in cibersicurezza ti accompagneranno in ogni fase dello studio e ti forniranno la visione più realistica su 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
- Istruttrice 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 docentet

Dott. Redondo, Jesús Serrano

- Sviluppatore FrontEnd Junior e Tecnico di Cybersecurity Junior
- Sviluppatore FrontEnd presso Telefónica, a Madrid
- Sviluppatore FrontEnd. Best Pro Consulting SL di Madrid
- Installatore di apparecchiature e servizi di Telecomunicazione. Grupo Zener di Castiglia e Leon
- Installatore di apparecchiature e servizi di Telecomunicazione. Lican Comunicaciones SL di Castiglia e Leon
- Certificato in Sicurezza Informatica. CFTIC Getafe di Madrid
- Tecnico Senior: Sistemi di Telecomunicazione e Informatica. IES Trinidad Arroyo di Palencia
- Tecnico Senior: Impianti Elettrotecnici MT e BT. IES Trinidad Arroyo di Palencia
- Formazione in Reverse Engineering, stenografia, crittografia. Accademia Hacker Incibe (Talenti Incibe)

Un percorso di crescita professionale stimolante, pensato per mantenere vivo l'interesse e la motivazione durante l'intera durata del programma"

04

Struttura e contenuti

Questo Esperto Universitario offre un'analisi completa di ciascuno dei campi di conoscenza che il professionista della sicurezza informatica deve conoscere riguardo alla cibersicurezza correttiva e alla perizia forense. 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.

Una gran varietà di concetti relativi alla Cibersicurezza Correttiva e alla Perizia Forense sviluppati in modo strutturato in un approccio di studio incentrato sull'efficienza"

Modulo 1. Ingegneria Inversa

1.1. Compilatori
- 1.1.1. Tipi di codici
- 1.1.2. Fasi di un compilatore
- 1.1.3. Tabelle di simboli
- 1.1.4. Gestione degli errori
- 1.1.5. Compilatore GCC

1.2. Tipi di analisi nei compilatori
- 1.2.1. Analisi lessicale
  - 1.2.1.1. Terminologia
  - 1.2.1.2. Componenti lessicali
  - 1.2.1.3. Analizzatore lessicale LEX
- 1.2.2. Parsing
  - 1.2.2.1. Grammatiche libere dal contesto
  - 1.2.2.2. Tipi di analisi sintattica
    - 1.2.2.2.1. Analisi top-down
    - 1.2.2.2.2. Analisi bottom-up
  - 1.2.2.3. Alberi sintattici e derivazioni
  - 1.2.2.4. Tipi di parser
    - 1.2.2.4.1. Analizzatori LR (*Left to Right*)
    - 1.2.2.4.2. Analizzatori LALR
- 1.2.3. Analisi semantica
  - 1.2.3.1. Grammatiche degli attributi
  - 1.2.3.2. Grammatica attribuita a S
  - 1.2.3.3. Grammatica attribuita a L

1.3. Strutture dati dell'assembly
- 1.3.1. Variabili
- 1.3.2. Array
- 1.3.3. Puntatori
- 1.3.4. Struttura
- 1.3.5. Oggetti

1.4. Strutture del codice assembly
- 1.4.1. Strutture di selezione
  - 1.4.1.1. If, else if, Else
  - 1.4.1.2. *Switch*
- 1.4.2. Strutture di iterazione
  - 1.4.2.1. *For*
  - 1.4.2.2. *While*
  - 1.4.2.3. Uso del *break*
- 1.4.3. Funzioni

1.5. Architettura Hardware x86
- 1.5.1. Architettura dei processori x86
- 1.5.2. Strutture dati x86
- 1.5.3. Strutture di codice x86

1.6. Architettura Hardware ARM
- 1.6.1. Architettura dei processori ARM
- 1.6.2. Strutture dati ARM
- 1.6.3. Strutture di codice ARM

1.7. Analisi statica del codice
- 1.7.1. Disassemblatori
- 1.7.2. IDA
- 1.7.3. Ricostruttori di codici

1.8. Analisi dinamica del codice
- 1.8.1. Analisi del comportamento
  - 1.8.1.1. Comunicazioni
  - 1.8.1.2. Monitoraggio
- 1.8.2. Debugger di codice Linux
- 1.8.3. Debugger di codice Windows

1.9. *Sandbox*
- 1.9.1. Architettura di un *Sandbox*
- 1.9.2. Elusione della *Sandbox*
- 1.9.3. Tecniche di rilevamento
- 1.9.4. Tecniche di elusione
- 1.9.5. Contromisure
- 1.9.6. *Sandbox* su Linux
- 1.9.7. *Sandbox* su Windows
- 1.9.8. *Sandbox* su MacOS
- 1.9.9. *Sandbox* su Android

1.10. Analisi dei *malware*
- 1.10.1. Metodi di analisi dei *malware*
- 1.10.2. Tecniche di offuscamento del *malware*
  - 1.10.2.1. Offuscamento degli eseguibili
  - 1.10.2.2. Limitazione degli spazi di esecuzione
- 1.10.3. Strumenti di analisi dei *malware*

Modulo 2. Analisi Forense

2.1. Acquisizione e riproduzione dei dati
- 2.1.1. Acquisizione della memoria volatile
  - 2.1.1.1. Informazioni di sistema
  - 2.1.1.2. Informazioni di rete
  - 2.1.1.3. Ordine di volatilità
- 2.1.2. Acquisizione dei dati statici
  - 2.1.2.1. Creazione di un'immagine duplicata
  - 2.1.2.2. Preparare un documento di catena di custodia
- 2.1.3. Metodi di validazione dei dati acquisiti
  - 2.1.3.1. Metodi in Linux
  - 2.1.3.2. Metodi in Windows

2.2. Valutazione e fallimento delle tecniche anti-forensi
- 2.2.1. Obiettivi delle tecniche anti-forensi
- 2.2.2. Cancellazione dei dati
  - 2.2.2.1. Cancellazione di dati e file
  - 2.2.2.2. Recupero dei file
  - 2.2.2.3. Recupero di partizioni eliminate
- 2.2.3. Protezione con password
- 2.2.4. Steganografia
- 2.2.5. Cancellazione sicura del dispositivo
- 2.2.6. Crittografia

2.3. Analisi forense del sistema operativo
- 2.3.1. Analisi forense di Windows
- 2.3.2. Analisi forense di Linux
- 2.3.3. Analisi forense di Mac

2.4. Analisi forense della rete
- 2.4.1. Analisi dei *Log*
- 2.4.2. Correlazione dei dati
- 2.4.3. Ricerca di rete
- 2.4.4. Passi da seguire nell'analisi forense della rete

2.5. Analisi forense del Web
- 2.5.1. Indagine sugli attacchi web
- 2.5.2. Rilevamento degli attacchi
- 2.5.3. Localizzazione degli indirizzi IP

2.6. Analisi forense dei Database
- 2.6.1. Analisi forense in MSSQL
- 2.6.2. Analisi forense in MySQL
- 2.6.3. Analisi forense in PostgreSQL
- 2.6.4. Analisi forense in MongoDB

2.7. Analisi forense in Cloud
- 2.7.1. Tipi di reati nel Cloud
  - 2.7.1.1. Cloud come soggetto
  - 2.7.1.2. Cloud come oggetto
  - 2.7.1.3. Cloud come strumento
- 2.7.2. Problematiche dell'analisi forense in Cloud
- 2.7.3. Ricerca sui servizi di archiviazione in Cloud
- 2.7.4. Strumenti di analisi forense per il Cloud

2.8. Indagine sui reati di posta elettronica
- 2.8.1. Sistemi di posta elettronica
  - 2.8.1.1. Client di posta elettronica
  - 2.8.1.2. Server di posta elettronica
  - 2.8.1.3. Server SMTP
  - 2.8.1.4. Server POP3
  - 2.8.1.5. Server IMAP4
- 2.8.2. Reati di posta elettronica
- 2.8.3. Messaggio di posta elettronica
  - 2.8.3.1. Intestazioni standard
  - 2.8.3.2. Intestazioni estese
- 2.8.4. Fasi dell'indagine su questi reati
- 2.8.5. Strumenti forensi per la posta elettronica

2.9. Analisi forense dei cellulari
- 2.9.1. Reti cellulari
  - 2.9.1.1. Tipi di reti
  - 2.9.1.2. Contenuti del CdR
- 2.9.2. *Subscriber Identity Module* (SIM)
- 2.9.3. Acquisizione logica
- 2.9.4. Acquisizione fisica
- 2.9.5. Acquisizione del file system

2.10. Scrittura e presentazione di rapporti forensi
- 2.10.1. Aspetti importanti di un rapporto forense
- 2.10.2. Classificazione e tipi di rapporti
- 2.10.3. Guida alla stesura di un rapporto
- 2.10.4. Presentazione del rapporto
  - 2.10.4.1. Preparazione preliminare per la testimonianza
  - 2.10.4.2. Deposizione
  - 2.10.4.3. Rapporti con i media

Modulo 3. Sfide Presenti e Future nella Sicurezza Informatica

3.1. Tecnologia *blockchain*
- 3.1.1. Ambiti di applicazione
- 3.1.2. Garanzia di riservatezza
- 3.1.3. Garanzia di non ripudio

3.2. Moneta digitale
- 3.2.1. I Bitcoin
- 3.2.2. Criptovalute
- 3.2.3. Mining di criptovalute
- 3.2.4. Schemi piramidali
- 3.2.5. Altri potenziali reati e problemi

3.3. *Deepfake*
- 3.3.1. Impatto mediatico
- 3.3.2. Pericoli per la società
- 3.3.3. Meccanismi di rilevamento

3.4. Il futuro dell'intelligenza artificiale
- 3.4.1. Intelligenza artificiale e cognitive computing
- 3.4.2. Utilizzi per semplificare il servizio clienti

3.5. Privacy digitale
- 3.5.1. Valore dei dati in rete
- 3.5.2. Utilizzo dei dati in rete
- 3.5.3. Privacy e gestione dell'identità digitale

3.6. Conflitti informatici, criminali informatici e attacchi informatici
- 3.6.1. L'impatto della sicurezza informatica sui conflitti internazionali
- 3.6.2. Conseguenze degli attacchi informatici sulla popolazione generale
- 3.6.3. Tipi di criminali informatici. Misure di protezione

3.7. Smartworking
- 3.7.1. La rivoluzione dello smartworking durante e dopo il COVID-19
- 3.7.2. Collo di bottiglia durante l'accesso
- 3.7.3. Variazione della superficie di attacco
- 3.7.4. Necessità dei lavoratori

3.8. Tecnologie *Wireless* emergenti
- 3.8.1. WPA3
- 3.8.2. 5G
- 3.8.3 Onde millimetriche
- 3.8.4. Tendenza a "*Get Smart*" invece di "*Get more*"

3.9. L'indirizzamento futuro nelle reti
- 3.9.1. Problemi attuali con l'indirizzamento IP
- 3.9.2. IPv6
- 3.9.3 IPv4+
- 3.9.4. Vantaggi di IPv4+ rispetto a IPv4
- 3.9.5. Vantaggi dell'IPv6 rispetto all'IPv4

3.10. La sfida alla prevenzione e alla sensibilizzazione delle persone
- 3.10.1. Le attuali strategie governative
- 3.10.2. Resistenza da parte delle persone all'apprendimento
- 3.10.3. Programmi di aggiornamento che devono essere adottati dalle aziende

Un programma che avrà un grande impatto sulle tue competenze e che ti permetterà di intervenire in modo efficiente nel campo della Cibersicurezza Correttiva e della Perizia Forense con risorse di ultima generazione"

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

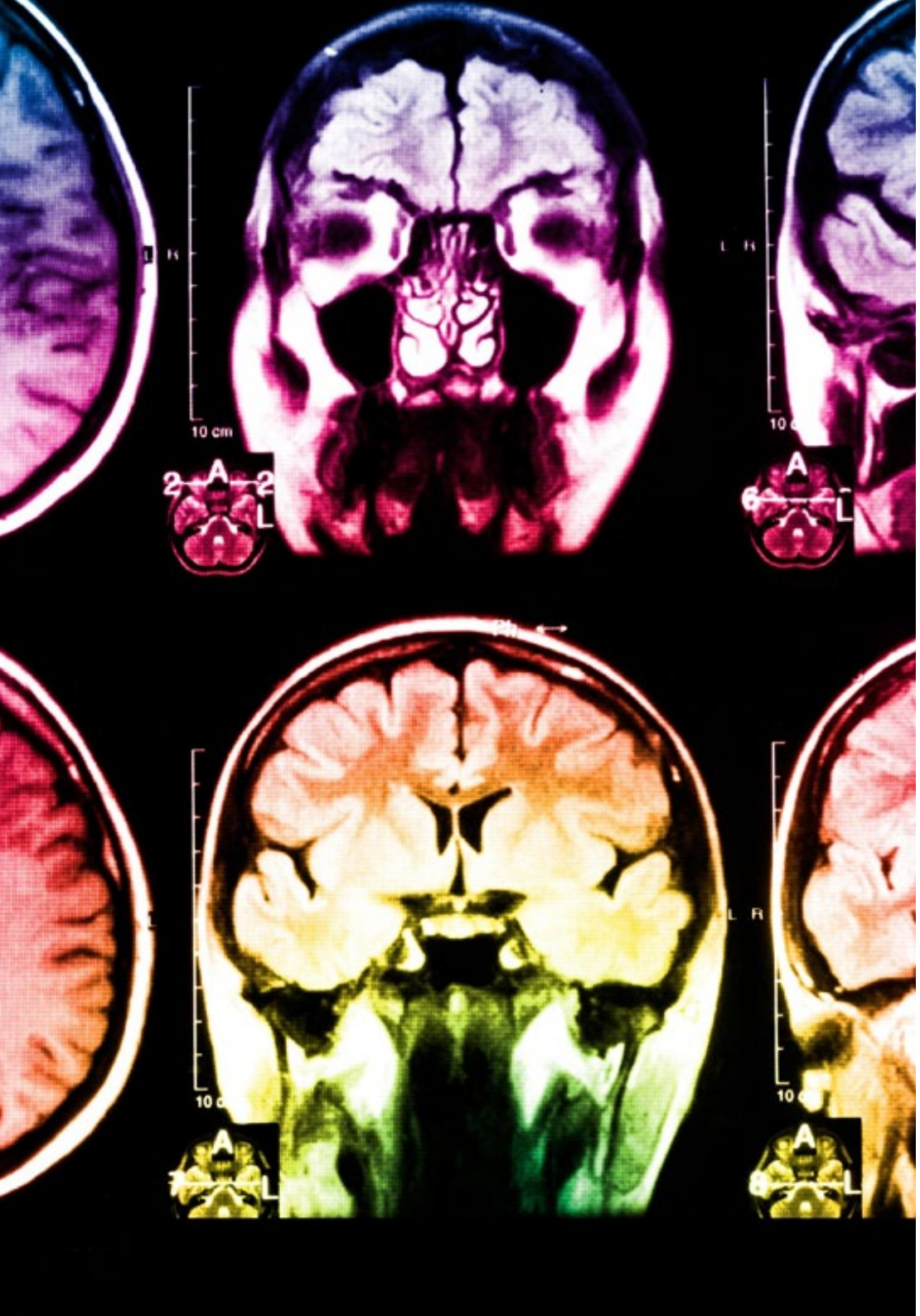
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

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.

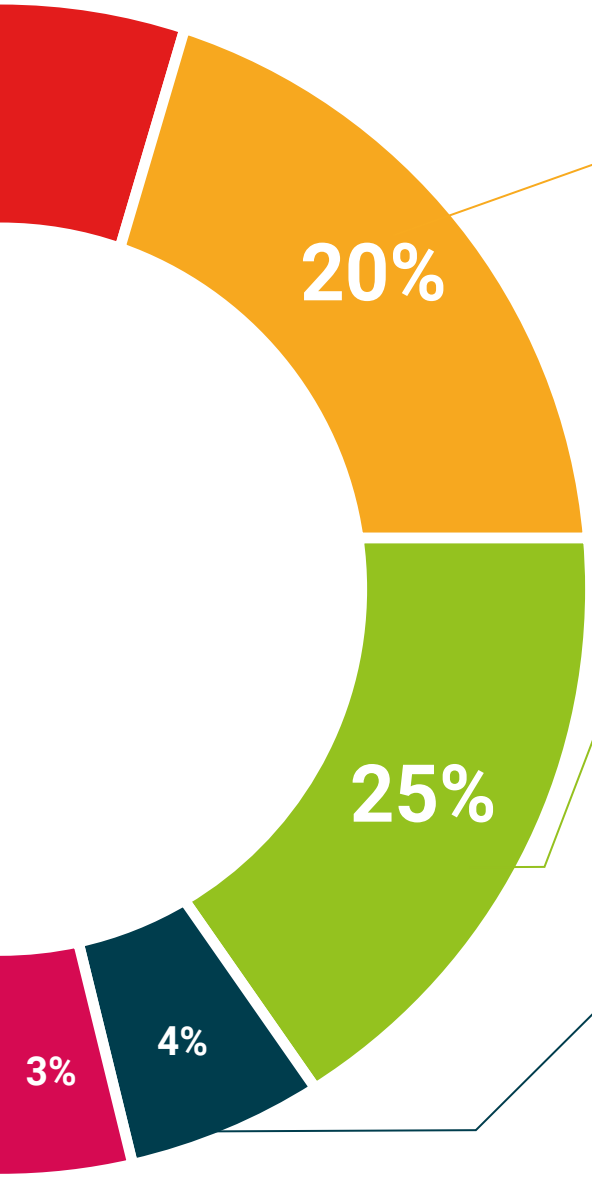
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

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 Correttiva e Perizia Forense ti garantisce, oltre alla preparazione più rigorosa e aggiornata, l'accesso a una qualifica di Esperto Universitario rilasciata da TECH Global University.

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

Questo programma ti consentirà di ottenere il titolo di studio di **Esperto Universitario in Cibersicurezza Correttiva e Perizia Forense** rilasciato da **TECH Global University**, la più grande università digitale del mondo.

TECH Global University è un'Università Ufficiale Europea riconosciuta pubblicamente dal Governo di Andorra ***(bollettino ufficiale)***. Andorra fa parte dello Spazio Europeo dell'Istruzione Superiore (EHEA) dal 2003. L'EHEA è un'iniziativa promossa dall'Unione Europea che mira a organizzare il quadro formativo internazionale e ad armonizzare i sistemi di istruzione superiore dei Paesi membri di questo spazio. Il progetto promuove valori comuni, l'implementazione di strumenti congiunti e il rafforzamento dei meccanismi di garanzia della qualità per migliorare la collaborazione e la mobilità tra studenti, ricercatori e accademici.

Questo titolo privato di **TECH Global University** è un programma europeo di formazione continua e aggiornamento professionale che garantisce l'acquisizione di competenze nella propria area di conoscenza, conferendo allo studente che supera il programma un elevato valore curriculare.

Titolo: **Esperto Universitario in Cibersicurezza Correttiva e Perizia Forense**

Modalità: **online**

Durata: **6 mesi**

Accreditamento: **18 ECTS**


tech global university

Dott _____, con documento d'identità _____ ha superato con successo e ottenuto il titolo di:

Esperto Universitario in Cibersicurezza Correttiva e Perizia Forense

Si tratta di un titolo di studio privato corrispondente a 540 horas di durata equivalente a 18 ECTS, con data di inizio dd/mm/aaaa e data di fine dd/mm/aaaa.

TECH Global University è un'università riconosciuta ufficialmente dal Governo di Andorra il 31 de gennaio 2024, appartenente allo Spazio Europeo dell'Istruzione Superiore (EHEA).

In Andorra la Vella, 28 febbraio 2024

Dott. Pedro Navarro Illana
Rettore

código único TECH: AFWOR23S techtitute.com/titulos

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

tech global university

Esperto Universitario
Cibersicurezza Correttiva e Perizia Forense

- Modalità: **online**
- Durata: **6 mesi**
- Titolo: **TECH Global University**
- Accreditamento: **18 ECTS**
- Orario: **a scelta**
- Esami: **online**

Esperto Universitario
Cibersicurezza Correttiva e Perizia Forense

tech global university