

Esperto Universitario Cybersicurezza delle Tecnologie Emergenti



Esperto Universitario Cybersicurezza delle Tecnologie Emergenti

- » Modalità: online
- » Durata: 6 mesi
- » Titolo: TECH Università Tecnologica
- » Dedizione: 16 ore/settimana
- » Orario: a scelta
- » Esami: online

Accesso al sito web: www.techtute.com/it/informatica/specializzazione/specializzazione-cybersicurezza-tecnologie-emergenti/

Indice

01

Presentazione

pag. 4

02

Obiettivi

pag. 8

03

Direzione del corso

pag. 12

04

Struttura e contenuti

pag. 16

05

Metodologia

pag. 22

06

Titolo

pag. 30

01

Presentazione

Di recente sono emerse numerose tecnologie che si sono diffuse rapidamente. Questo, oltre ad aver fornito nuovi servizi alle aziende, a utenti e clienti, ha creato anche problemi di sicurezza. Le tecnologie emergenti per loro natura sono in continuo sviluppo e non hanno ancora raggiunto il loro stato ottimale di protezione, e sono quindi soggette ad attacchi. Per affrontare questa sfida è stato ideato questo programma, che consentirà all'informatico di apprendere i migliori metodi di cybersicurezza applicati all'internet delle cose, al *Cloud Computing* o alla *Blockchain*. Potrà così migliorare il suo profilo professionale, preparandosi ad affrontare le sfide presenti e future in materia di sicurezza digitale.





Specializzati in cybersicurezza applicata al Cloud Computing, alla Blockchain o all'Internet delle cose seguendo questo Esperto Universitario, che ti renderà un professionista molto richiesto dalle migliori aziende tecnologiche"

Le tecnologie emergenti sono destinate a rimanere. Sono nate in un momento in cui era necessario trovare soluzioni a vari problemi. Ad esempio, l'Internet delle cose si sta evolvendo fino a diventare un elemento essenziale nella vita di molte persone. La *Blockchain* sta inoltre contribuendo a decentralizzare molti processi e il *Cloud Computing* garantisce la disponibilità di risorse di ogni tipo, in particolare dati o applicazioni, ovunque, con un semplice accesso a una connessione di rete.

Trattandosi di elementi e servizi molto utili, la loro popolarità sta crescendo rapidamente e ciò sta causando uno squilibrio, in quanto spesso non dispongono di una sicurezza adeguata perché si tratta di tecnologie non ancora sviluppate al 100%. Per questo motivo, sempre più aziende, sia nel campo dell'elettronica che in altri settori, sono alla ricerca di professionisti specializzati in cybersicurezza applicata a questi strumenti.

Questo Esperto Universitario esplora quindi tutte le possibilità della cybersicurezza in questo tipo di tecnologia, garantendo all'informatico un approfondimento intensivo e completo nel campo, dandogli una spinta professionale decisiva nella sua carriera.

Tutto questo attraverso un sistema di apprendimento online appositamente ideato pensando nel professionista che lavora, il quale sarà in grado di coniugare il lavoro con gli studi in modo confortevole e semplice. Inoltre, avrà a disposizione il miglior personale docente composto da veri e propri specialisti in questo importante settore della sicurezza informatica.

Questo **Esperto Universitario in Cybersicurezza delle Tecnologie Emergenti** possiede il programma più completo e aggiornato del mercato. Le caratteristiche principali del programma sono:

- ◆ Sviluppo di casi pratici presentati da esperti in Informatica e Cybersecurity
- ◆ 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



Aziende di ogni tipo hanno bisogno di specialisti per garantire una sicurezza ottimale ai loro progetti blockchain o di internet delle cose"

“

Il miglior sistema di insegnamento online sarà a tua disposizione per permetterti di studiare al tuo ritmo, senza orari rigidi o la necessità di sospendere il tuo lavoro"

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.

Grazie a questo programma, potrai studiare in maniera approfondita i migliori metodi di crittografia o le tipologie di infrastrutture Cloud esistenti.

Le tecnologie emergenti sono il futuro: specializzati e migliora immediatamente le tue prospettive di carriera"



02

Obiettivi

L'obiettivo principale di questo Esperto Universitario in Cybersicurezza delle Tecnologie Emergenti è quello di rendere lo specialista IT un punto di riferimento in questo settore, in grado di lavorare per qualsiasi azienda che voglia intraprendere progetti in *Blockchain* o *Cloud Computing* in totale sicurezza. Completando questo programma, acquisirai un profilo professionale perfetto per lavorare nel nuovo ambiente tecnologico e digitale che si sta affermando da qualche tempo.



“

*Una volta completato questo
percorso universitario, diventerai
uno dei professionisti più ricercati
nel tuo settore”*



Obiettivi generali

- ◆ Esaminare la scienza della crittologia e il rapporto con le sue aree: crittografia, crittoanalisi, steganografia e steganalisi
- ◆ Analizzare i tipi di crittografia in base al tipo di algoritmo e al suo utilizzo
- ◆ Redigere sistemi di gestione delle chiavi
- ◆ Valutare le diverse applicazioni pratiche
- ◆ Esaminare i certificati digitali
- ◆ Analizzare l'infrastruttura a chiave pubblica (PKI)
- ◆ Analizzare le ultime tendenze e sfide
- ◆ Esaminare il processo di progettazione di una strategia di sicurezza per l'implementazione in azienda di servizi *Cloud*
- ◆ Identificare le aree di sicurezza nel *Cloud*
- ◆ Analizzare i servizi e gli strumenti in ogni ambito di sicurezza
- ◆ Valutare le differenze nelle implementazioni concrete dei diversi fornitori di *Cloud* pubblico
- ◆ Valutare le opzioni di connettività IoT per realizzare un progetto, con particolare attenzione alle tecnologie LPWAN
- ◆ Presentare le specifiche di base delle principali tecnologie LPWAN per l'IoT
- ◆ Sviluppare le specifiche di sicurezza per ogni tecnologia LPWAN
- ◆ Paragonare la sicurezza delle tecnologie LPWAN





Obiettivi specifici

Modulo 1. La crittografia nell'IT

- ◆ Completare le operazioni fondamentali (XOR, grandi numeri, sostituzione e trasposizione) e i vari componenti (funzioni One-Way, Hash, generatori di numeri casuali)
- ◆ Analizzare le tecniche crittografiche
- ◆ Sviluppare i diversi algoritmi crittografici
- ◆ Dimostrare l'uso delle firme digitali e la loro applicazione nei certificati digitali
- ◆ Valutare i sistemi di gestione delle crittografie e l'importanza della lunghezza delle chiavi crittografiche
- ◆ Esaminare gli algoritmi di derivazione delle chiavi crittografiche
- ◆ Analizzare il ciclo di vita delle chiavi crittografiche
- ◆ Valutare le modalità di cifratura a blocchi e di cifratura a flusso
- ◆ Determinare i generatori di numeri pseudocasuali
- ◆ Sviluppare casi reali di applicazioni crittografiche, come Kerberos, PGP o smart card
- ◆ Esaminare associazioni e organismi correlati, come ISO, NIST o NCSC
- ◆ Individuare gli ostacoli nella crittografia dell'informatica quantistica

Modulo 2. Sicurezza in ambienti Cloud

- ◆ Identificare i rischi di installazione di un'infrastruttura di Cloud pubblico
- ◆ Definire i requisiti di sicurezza
- ◆ Sviluppo di un piano di sicurezza per l'implementazione del Cloud
- ◆ Identificare i servizi Cloud da implementare per la realizzazione di un piano di sicurezza
- ◆ Determinare le misure operative necessarie per i meccanismi di prevenzione
- ◆ Stabilire linee guida per un sistema di Logging e monitoraggio
- ◆ Proporre azioni di risposta agli imprevisti

Modulo 3. Sicurezza delle Comunicazioni nei Dispositivi IoT

- ◆ Introdurre l'architettura IoT semplificata
- ◆ Spiegare le differenze tra le tecnologie di connettività generaliste e le tecnologie di connettività per l'IoT
- ◆ Stabilire il concetto di triangolo di ferro della connettività IoT
- ◆ Analizzare le specifiche di sicurezza della tecnologia LoRaWAN, NB-IoT e WiSUN
- ◆ Motivare la scelta della giusta tecnologia IoT per ogni progetto



I tuoi obiettivi professionali sono a portata di mano: iscriviti e diventa uno specialista in Cybersicurezza delle Tecnologie Emergenti"

03

Direzione del corso

La complessità della situazione attuale richiede che il professionista svolga un processo di aggiornamento e approfondimento costante. Le tecnologie emergenti non solo aprono nuovi orizzonti, ma mutano continuamente con l'emergere di nuovi sviluppi. Per questo motivo, è necessaria la presenza dei migliori specialisti in questo settore, come quelli che questo Esperto Universitario mette a disposizione in modo che l'informatico possa aggiornarsi sugli ultimi sviluppi della tecnologia sulla base dall'insegnamento di professionisti in attività.



“

I docenti più esperti, che lavorano nel settore della cybersicurezza, ti forniranno le conoscenze e le tecniche più avanzate"

Direzione



Dott. Olalla Bonal, Martín

- Client Technical Specialist Blockchain in IBM
- Architetto *Blockchain*
- Architetto di Infrastrutture nel Settore Bancario
- Gestione di progetti e implementazione di soluzioni
- Tecnico di Elettronica Digitale
- Docente: Training *Hyperledger Fabric* per le aziende
- Docente: Training *Blockchain* per il settore business delle aziende

Personale docente

Dott. Gómez Rodríguez, Antonio

- ◆ Ingegnere di soluzioni Cloud in Oracle
- ◆ Project Manager presso Sopra Group
- ◆ Project Manager presso Everis
- ◆ Project Manager nell'Azienda Pubblica della Gestione dei Programmi Culturali Consiglio della Cultura dell'Andalusia
- ◆ Analista di sistemi informativi. Sopra Group
- ◆ Laurea in Ingegneria delle Telecomunicazioni presso l'Università Politecnica della Catalogna
- ◆ Post-laurea in Tecnologie e Sistemi Informatici, Istituto Catalano di Tecnologia
- ◆ E-Business Master, Business School La Salle

Dott. del Valle Arias, Jorge

- ◆ Smart Cities Business Growth Manager Spain en Itron Inc.
- ◆ Consulente IoT
- ◆ Responsabile della Sezione IoT presso Diode Spagna
- ◆ Sales Manager IoT & Celular presso Aicox Soluciones
- ◆ Fondatore e CEO di Sensor Intelligence
- ◆ Direttore Operativo di Codium Networks
- ◆ Capo Area Elettronica di Aitemin
- ◆ Ingegnere delle Telecomunicazioni dell'Università Politecnica di Madrid
- ◆ Executive MBA presso la Scuola Internazionale di La Salle di Madrid

Dott. Ortega, Octavio

- ◆ Programmatore di applicazioni informatiche e sviluppo di siti web.
- ◆ Web design e APP per i clienti, CRDS per la ricerca condotta dall'Istituto di Salute Carlos III, negozi online, applicazioni per Android, ecc.
- ◆ Docente di Sicurezza Informatica
- ◆ Laurea in Psicologia presso l'Università Oberta di Catalunya
- ◆ Tecnico universitario superiore in Analisi, progettazione e soluzioni software
- ◆ Tecnico universitario superiore in Programmazione avanzata



Sarai in grado di affrontare in modo appropriato tutti i tipi di minacce legate alla cybersecurity. Iscriviti e diventa un ottimo specialista"

04

Struttura e contenuti

Questo Esperto Universitario in Cybersicurezza delle Tecnologie Emergenti è composto da 3 moduli specialistici che saranno svolti durante 450 ore di apprendimento intensivo. Grazie a ciò l'informatico sarà in grado di approfondire aspetti rilevanti della cybersecurity come le basi matematiche della crittografia, l'uso degli algoritmi nella sicurezza, la sicurezza nei *Cloud* pubblici e le principali vulnerabilità di sicurezza dell'IoT.



A hand with a manicured finger pointing at a signature on a document. The background is a teal and white geometric design.

“

Il programma possiede i contenuti più completi sulla cybersicurezza applicata alle tecnologie emergenti. Non esitare a iscriverti”

Modulo 1. La crittografia nell'IT

- 1.1. Crittografia
 - 1.1.1. Crittografia
 - 1.1.2. Fondamenti matematici
- 1.2. Crittologia
 - 1.2.1. Crittologia
 - 1.2.2. Crittoanalisi
 - 1.2.3. Steganografia e steganalisi
- 1.3. Protocolli crittografici
 - 1.3.1. Blocchi di base
 - 1.3.2. Protocolli di base
 - 1.3.3. Protocolli intermedi
 - 1.3.4. Protocolli avanzati
 - 1.3.5. Protocolli esoterici
- 1.4. Tecniche crittografiche
 - 1.4.1. Lunghezza della chiave di crittografia
 - 1.4.2. Gestione delle chiavi
 - 1.4.3. Tipi di algoritmi
 - 1.4.4. Funzioni di riepilogo. Hash
 - 1.4.5. Generatori di numeri pseudocasuali
 - 1.4.6. Uso degli algoritmi
- 1.5. Crittografia simmetrica
 - 1.5.1. Cifrari a blocchi
 - 1.5.2. DES (*Data Encryption Standard*)
 - 1.5.3. Algoritmo RC4
 - 1.5.4. AES (*Advanced Encryption Standard*)
 - 1.5.5. Combinazione di cifrari a blocchi
 - 1.5.6. Derivazione delle chiavi



- 1.6. Crittografia asimmetrica
 - 1.6.1. Diffie-Hellman
 - 1.6.2. DSA (*Digital Signature Algorithm*)
 - 1.6.3. RSA (*Rivest, Shamir y Adleman*)
 - 1.6.4. Curva ellittica
 - 1.6.5. Crittografia asimmetrica. Tipologia
- 1.7. Certificati digitali
 - 1.7.1. Firma digitale
 - 1.7.2. Certificati X509
 - 1.7.3. Infrastruttura a chiave pubblica (PKI)
- 1.8. Implementazione
 - 1.8.1. Kerberos
 - 1.8.2. IBM CCA
 - 1.8.3. *Pretty Good Privacy* (PGP)
 - 1.8.4. *ISO Authentication Framework*
 - 1.8.5. SSL e TLS
 - 1.8.6. Smart card nei mezzi di pagamento (EMV)
 - 1.8.7. Protocolli di telefonia mobile
 - 1.8.8. *Blockchain*
- 1.9. Steganografia
 - 1.9.1. Steganografia
 - 1.9.2. Steganalisi
 - 1.9.3. Applicazioni e usi
- 1.10. Crittografia quantistica
 - 1.10.1. Algoritmi quantistici
 - 1.10.2. Protezione degli algoritmi dalla computazione quantistica
 - 1.10.3. Distribuzione quantistica delle chiavi

Modulo 2. Sicurezza in ambienti *Cloud*

- 2.1. Sicurezza negli ambienti *Cloud Computing*
 - 2.1.1. Sicurezza negli ambienti *Cloud Computing*
 - 2.1.2. Sicurezza negli ambienti *Cloud Computing* Minacce e rischi per la sicurezza
 - 2.1.3. Sicurezza negli ambienti *Cloud Computing* Aspetti chiave della sicurezza
- 2.2. Tipi di infrastruttura *Cloud*
 - 2.2.1. Pubblico
 - 2.2.2. Privato
 - 2.2.3. Ibrido
- 2.3. Modello di gestione condivisa
 - 2.3.1. Caratteristiche di sicurezza gestite dal fornitore
 - 2.3.2. Elementi gestiti dal cliente
 - 2.3.3. Definizione della strategia di sicurezza
- 2.4. Meccanismi di prevenzione
 - 2.4.1. Sistema di gestione di autenticazione
 - 2.4.2. Sistema di gestione delle autorizzazioni: politiche di accesso
 - 2.4.3. Sistema di gestione dei codici
- 2.5. Protezione dei sistemi
 - 2.5.1. Protezione dei sistemi di archiviazione
 - 2.5.2. Protezione dei sistemi di database
 - 2.5.3. Protezione dei dati in transito
- 2.6. Protezione dell'infrastruttura
 - 2.6.1. Progettazione e implementazione di reti sicure
 - 2.6.2. Sicurezza delle risorse informatiche
 - 2.6.3. Strumenti e risorse per la protezione delle infrastrutture
- 2.7. Rilevamento di minacce e attacchi
 - 2.7.1. Sistemi di audit, *logging* e monitoraggio
 - 2.7.2. Sistemi di eventi e allarmi
 - 2.7.3. Sistemi SIEM
- 2.8. Risposta agli incidenti
 - 2.8.1. Piano di risposta agli incidenti
 - 2.8.2. La continuità operativa
 - 2.8.3. Analisi forense e riparazione di incidenti della stessa natura

- 2.9. Sicurezza nei Cloud pubblici
 - 2.9.1. AWS (Amazon Web Services)
 - 2.9.2. Microsoft Azure
 - 2.9.3. Google GCP
 - 2.9.4. Oracle Cloud
- 2.10. Regolamenti e conformità
 - 2.10.1. Conformità alle norme di sicurezza
 - 2.10.2. Gestione dei rischi
 - 2.10.3. Personale e procedure nelle organizzazioni

Modulo 3. Sicurezza delle comunicazioni nei dispositivi lo

- 3.1. Dalla telemetria all'loT
 - 3.1.1. Telemetria
 - 3.1.2. Connettività M2M
 - 3.1.3. Democratizzazione della telemetria
- 3.2. Modelli di riferimento loT
 - 3.2.1. Modello di riferimento loT
 - 3.2.2. Architettura loT semplificata
- 3.3. Vulnerabilità della sicurezza loT
 - 3.3.1. Dispositivi loT
 - 3.3.2. Dispositivi loT. Casi di utilizzo
 - 3.3.3. Dispositivi loT. Punti deboli
- 3.4. Connettività loT
 - 3.4.1. Reti PAN, LAN, WAN
 - 3.4.2. Tecnologie wireless non loT
 - 3.4.3. Tecnologie wireless LPWAN
- 3.5. Tecnologie LPWAN
 - 3.5.1. Il triangolo di ferro delle reti LPWAN
 - 3.5.2. Bande di frequenza libere vs. Bande con licenza
 - 3.5.3. Opzioni tecnologiche LPWAN



- 3.6. Tecnologia LoRaWAN
 - 3.6.1. Tecnologia LoRaWAN
 - 3.6.2. Casi d'uso di LoRaWAN. Ecosistema
 - 3.6.3. Sicurezza in LoRaWAN
- 3.7. Tecnologia Sigfox
 - 3.7.1. Tecnologia Sigfox
 - 3.7.2. Casi d'uso di Sigfox. Ecosistema
 - 3.7.3. Sicurezza in Sigfox
- 3.8. Tecnologia cellulare IoT
 - 3.8.1. Tecnologia cellulare IoT (NB-IoT e LTE-M)
 - 3.8.2. Casi d'uso cellulare IoT. Ecosistema
 - 3.8.3. Sicurezza cellulare IoT
- 3.9. Tecnologia WiSUN
 - 3.9.1. Tecnologia WiSUN
 - 3.9.2. Casi d'uso di WiSUN. Ecosistema
 - 3.9.3. Sicurezza di WiSUN
- 3.10. Altre tecnologie IoT
 - 3.10.1. Altre tecnologie IoT
 - 3.10.2. Casi d'uso ed ecosistema di altre tecnologie IoT
 - 3.10.3. Sicurezza in altre tecnologie IoT



I migliori docenti ti consentiranno di aggiornarti in materia di sicurezza nelle tecnologie emergenti con i contenuti più recenti"

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:



Materiali 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 Cybersicurezza delle Tecnologie Emergenti ti garantisce, oltre alla preparazione più rigorosa e aggiornata, l'accesso a 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 Cybersicurezza delle Tecnologie Emergenti** possiede il programma più completo e aggiornato del mercato.

Dopo aver superato la valutazione, lo studente riceverà mediante lettera certificata* con ricevuta di ritorno, la sua 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 Cybersicurezza delle Tecnologie Emergenti**

N. Ore Ufficiali: **450 o.**



*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.

futuro
salute fiducia persone
educazione informazione tutor
garanzia accreditamento insegnamento
istituzioni tecnologia apprendimento
comunità impegno
attenzione personalizzata innovazione
conoscenza presente qualità
formazione online
sviluppo istituzioni
classe virtuale lingue

tech università
tecnologica

Esperto Universitario
Cybersicurezza delle
Tecnologie Emergenti

- » Modalità: online
- » Durata: 6 mesi
- » Titolo: TECH Università Tecnologica
- » Dedizione: 16 ore/settimana
- » Orario: a scelta
- » Esami: online

Esperto Universitario Cybersicurezza delle Tecnologie Emergenti