Esperto Universitario

Cibersicurezza Preventiva

tech università tecnologica

Esperto Universitario

Cibersicurezza Preventiva

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

Accesso al sito web: www.techtitute.com/it/informatica/specializzazione/specializzazione-cibersicurezza-preventiva

Indice

01

Presentazione

Quando si usano dei dispositivi mobili vengono messi in gioco numerosi dati di cui i programmi hanno bisogno per svolgere le loro funzioni. Questo tipo di fiducia che l'utente ripone nella tecnologia che usa quotidianamente comporta l'assunzione di un elevato rischio che queste informazioni vengano violate attraverso attacchi informatici. L'evoluzione continua di nuovi modi di ottenere questi dati promuove che lo sviluppo di sistemi preventivi debba essere costante, agendo in anticipo e dando risposte rapide ed efficaci ad ogni nuova minaccia. Lo specialista che lavora in questo campo è quindi obbligato ad una costante specializzazione che gli permetta di aggiornare pienamente le sue conoscenze, un compito complesso data la velocità dei cambiamenti nel settore. Questo Esperto Universitario è la risposta più immediata e di alta qualità alle esigenze di preparazione su Cibersicurezza Preventiva del mercato dell'insegnamento online.

Migliora le tue capacità di intervento in materia di Cibersicurezza Preventiva con il programma più completo e aggiornato in questo campo"

Attualmente nessuna azienda è esente da un attacco informatico e quindi subisce le diverse conseguenze che ne derivano. Indipendentemente dalle dimensioni, sarà esposta a furti di informazioni, ricatti, sabotaggi, ecc. È necessario quindi condurre studi periodici sulle vulnerabilità e i rischi e determinare la superficie di attacco, motivo per cui devono essere realizzati sempre più studi periodici su possibili vulnerabilità e rischi. Ogni impresa dovrà verificare se è conforme alle norme e alle leggi del Paese in cui si trova ed essere a conoscenza dei possibili danni monetari o immateriali, ad esempio la sua reputazione.

Questo programma offre uno studio aggiornato in Cyberintelligence e Cibersicurezza. Tratta a fondo aspetti fondamentali quali il ciclo dell'intelligence, le relative fonti, l'ingegneria sociale, la metodologia OSINT, HUMINT, l'anonimizzazione, l'analisi del rischio, le metodologie esistenti (OWASP, OWISAM, OSSTM, PTES) e le normative vigenti in materia di cibersicurezza. Inoltre, esamina i principali organismi internazionali in materia di sicurezza informatica, analizzando il loro ambito di interventi e la loro posizione di fronte a diversi problemi.

Tutti gli sviluppatori si trovano di fronte alla sfida di realizzare software di qualità e sicuri, poiché nell'ecosistema applicativo attuale qualsiasi vulnerabilità del codice o del sistema causerà perdite, esposizione e furto di dati, nonché altri problemi dovuti ad attacchi informatici. È dovere dello sviluppatore conoscere bene i diversi ambienti e le fasi che attraverserà il suo codice e assicurarsi che operi, in ognuno di essi, nel modo più efficiente e sicuro. Inoltre, deve conoscere le esigenze e le dipendenze di cui ha bisogno la loro applicazione per funzionare e cercare di ridurre al minimo l'uso di moduli e funzionalità, per minimizzare le possibilità di attacco. Comprendere le metodologie e il tipo di test da eseguire ridurrà quindi il tempo di risoluzione dei problemi e di verifica del codice.

Questo **Esperto Universitario in Cibersicurezza Preventiva** 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

Un programma che ti insegnerà a lavorare riducendo le possibilità di attacco e ottimizzando la risoluzione dei problemi"

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

Scopri come sviluppare codici applicativi di sicurezza adottando strategie che riducono la vulnerabilità.

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

Questo Esperto Universitario darà una spinta importante alla 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 a realizzare di intervenire con qualità, sviluppando inoltre competenze trasversali che consentano di affrontare situazioni complesse elaborando risposte mirate e precise.

Scopri e applica le metodologie più interessanti in materia di Cibersicurezza Preventiva e impara a sviluppare applicazioni con i sistemi di prevenzione più efficaci del momento"

Obiettivi generali

- Analizzare il ruolo dell'analista di cibersicurezza
- Approfondire la comprensione dell'ingegneria sociale e dei suoi metodi
- Esaminare le metodologie OSINT, HUMINT, OWASP, PTEC. OSSTM, OWISAM
- Condurre l'analisi dei rischi e comprendere le metriche di rischio
- Determinare l'uso appropriato dell'anonimato e l'uso di reti come TOR, I2P e *Freenet*
- Raccogliere le normative esistenti in materia di cibersicurezza
- Generare conoscenze specialistiche per condurre un audit di sicurezza
- Analizzare i diversi sistemi esistenti
- Valutare le informazioni ottenute e sviluppare meccanismi di prevenzione e *Hacking*
- Stabilire priorità nello studio e nella risoluzione delle vulnerabilità
- Dimostrare che un sistema è vulnerabile, attaccarlo in modo proattivo e risolvere tali problemi
- Determinare le linee guida che un buon sviluppatore deve seguire per conformarsi ai requisiti di sicurezza necessari
- Stabilire una metodologia appropriata per lo sviluppatore e per l'ambiente di produzione
- Specificare i test da eseguire sul software sviluppato

Obiettivi specifici

Modulo 1. Cyberintelligence e cibersicurezza

- Sviluppare le metodologie utilizzate in materia di sicurezza informatica
- Esaminare il ciclo dell'intelligence e stabilirne l'applicazione nella cyberintelligence
- Determinare il ruolo dell'analista di intelligence e gli ostacoli all'attività di evacuazione
- Analizzare le metodologie OSINT, OWISAM, OSSTM, PTES, OWASP
- Stabilire gli strumenti più comuni per la produzione di intelligence
- Condurre un'analisi dei rischi e comprendere le metriche utilizzate
- Concretizzare le opzioni per l'anonimato e l'uso di reti come TOR, I2P, *FreeNet*
- Dettagliare le normative vigenti in materia di cyber-sicurezza

Modulo 2. *Hacking* etico

- Esaminare i metodi IOSINT
- Raccogliere le informazioni disponibili sui media pubblici
- Eseguire la scansione delle reti per ottenere informazioni in maniera attiva
- Sviluppare laboratori di prova
- Analizzare gli strumenti per le prestazioni del *Pentesting*
- Catalogare e valutare le diverse vulnerabilità dei sistemi
- Concretizzare le diverse metodologie di *Hacking*

Modulo 3. Sviluppo sicuro

- Stabilire i requisiti necessari per il corretto funzionamento di un'applicazione in modo sicuro
- Esaminare i file di *Log* per comprendere i messaggi di errore
- Analizzare i diversi eventi e decidere cosa mostrare all'utente e cosa salvare nei *Log*
- Generare un codice sanificato, facilmente verificabile e di qualità
- Valutare la documentazione appropriata per ogni fase di sviluppo
- Concretizzare il comportamento del server per ottimizzare il sistema
- Elaborare un codice modulare, riutilizzabile e mantenibile

Imparerai a ottimizzare i sistemi applicando requisiti che consentano di garantire la massima sicurezza e usabilità delle applicazioni"

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 corso la visione più diretta e immediata delle caratteristiche reali dell'intervento in questo campo fornendo una panoramica contestuale del massimo interesse.

Professionisti esperti del settore ti guideranno 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
- 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*. E-Council. Madrid


SHARE
HTML
JUST MAKE
THE BEST
THINGS!
CREATIVE
LAYOUT
CONTENT

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 nell'ambito delle attività di preventive. 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 Preventiva sviluppati in modo strutturato e da un approccio di studio incentrato sull'efficienza"

Modulo 1. Cyberintelligence e cibersicurezza

1.1. Cyberintelligence
- 1.1.1. Cyberintelligence
  - 1.1.1.1. L'intelligence
    - 1.1.1.1.1. Ciclo di intelligence
  - 1.1.1.2. Cyberintelligence
    - 1.1.1.3. Cyberintelligence e cibersicurezza
- 1.1.2. Intelligenza
  - 1.1.2.1. Ciclo di intelligence
  - 1.1.2.2. Cyberintelligence
  - 1.1.2.3. Cyberintelligence e cibersicurezza
- 1.1.3. L'analista di intelligence
  - 1.1.3.1. Il ruolo dell'analista di intelligence
  - 1.1.3.2. I pregiudizi dell'analista di intelligence nell'attività valutativa

1.2. Cibersicurezza
- 1.2.1. Livelli di sicurezza
  - 1.2.2. Identificazione delle minacce informatiche
    - 1.2.2.1. Minacce esterne
    - 1.2.2.2. Minacce interne
- 1.2.3. Azioni avverse
    - 1.2.3.1. Ingegneria sociale
    - 1.2.3.2. Metodi comunemente utilizzati

1.3. Tecniche e Strumenti delle intelligence
- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. Humit
- 1.3.4. Distribuzioni e strumenti *Linux*
- 1.3.5. OWISAM
- 1.3.6. OWASP
- 1.3.7. PTES
- 1.3.8. OSSTMM

1.4. Metodologie di valutazione
- 1.4.1. L'analisi di intelligence
- 1.4.2. Tecniche di organizzazione delle informazioni acquisite
- 1.4.3. Affidabilità e credibilità delle fonti di informazione
- 1.4.4. Metodologie di analisi
- 1.4.5. Presentazione dei risultati dell'intelligence

1.5. Audit e documentazione
- 1.5.1. Audit della sicurezza informatica
- 1.5.2. Documentazione e permessi per l'audit
- 1.5.3. Tipi di audit
- 1.5.4. Consegna
  - 1.5.4.1. Rapporto tecnico
  - 1.5.4.2. Rapporto esecutivo

1.6. Anonimato in rete
- 1.6.1. Uso dell'anonimato
- 1.6.2. Tecniche di anonimato (*Proxy*, VPN)
- 1.6.3. Reti TOR, *Freenet* e IP2

1.7. Minacce e tipi di sicurezza
- 1.7.1. Tipologie di minacce
- 1.7.2. Sicurezza fisica
- 1.7.3. Sicurezza di rete
- 1.7.4. Sicurezza logica
- 1.7.5. Sicurezza delle applicazioni web
- 1.7.6. Sicurezza sui dispositivi mobili

1.8. Regolamenti e *Compliance*
- 1.8.1. GDPR
- 1.8.2. La strategia nazionale di cybersecurity per il 2019
- 1.8.3. Famiglia ISO 27000
- 1.8.4. Quadro di sicurezza informatica NIST
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. Normativa sul *Cloud*
- 1.8.8. SOX
- 1.8.9. PCI

1.9. Analisi del rischio e parametri di misurazione
- 1.9.1. Portata dei rischi
- 1.9.2. I cespiti
- 1.9.3. Le minacce
- 1.9.4. Punti deboli
- 1.9.5. Valutazione dei rischi
- 1.9.6. Trattamento del rischio

1.10. Importanti organismi di cibersicurezza
- 1.10.1. NIST
- 1.10.2. ENISA
- 1.10.3. INCIBE
- 1.10.4. OEA
- 1.10.5. UNASUR PROSUR

Modulo 2. Hacking Etico

2.1. Ambiente di lavoro
- 2.1.1. Distribuzioni *Linux*
  - 2.1.1.1. *Kali Linux - Offensive Security*
  - 2.1.1.2. *Parrot* OS
  - 2.1.1.3. *Ubuntu*
- 2.1.2. Sistemi di virtualizzazione
- 2.1.3. *Sandbox*
- 2.1.4. Distribuzione dei laboratori

2.2. Metodologie
- 2.2.1. OSSTMM
- 2.2.2. OWASP
- 2.2.3. NIST
- 2.2.4. PTES
- 2.2.5. ISSAF

2.3. *Footprinting*
- 2.3.1. Intelligence open source (OSINT)
- 2.3.2. Ricerca di violazioni dei dati e punti deboli
- 2.3.3. Utilizzo di strumenti passivi

2.4. Scansione di rete
- 2.4.1. Strumenti di scansione
  - 2.4.1.1. *Nmap*
  - 2.4.1.2. *Hping3*
  - 2.4.1.3. Altri strumenti di scansione
- 2.4.2. Tecniche di scansione
- 2.4.3. Tecniche di elusione di *firewall* e IDS
- 2.4.4. *Banner grabbing*
- 2.4.5. Diagrammi di rete

2.5. Enumerazione
- 2.5.1. Enumerazione SMTP
- 2.5.2. Enumerazione DNS
- 2.5.3. Enumerazione NetBIOS e Samba
- 2.5.4. Enumerazione LDAP
- 2.5.5. Enumerazione SNMP
- 2.5.6. Altre tecniche di Enumerazione

2.6. Analisi delle vulnerabilità
- 2.6.1. Soluzioni per l'Analisi dei punti deboli
  - 2.6.1.1. *Qualys*
  - 2.6.1.2. *Nessus*
  - 2.6.1.3. CFI *LanGuard*
- 2.6.2. Sistemi di punteggio dei punti deboli
  - 2.6.2.1. CVSS
  - 2.6.2.2. CVE
  - 2.6.2.3. NVD

2.7. Attacchi alle reti wireless
- 2.7.1. Metodologia di *hacking* nelle reti wireless
  - 2.7.1.1. WiFi *discovery*
  - 2.7.1.2 Analisi del traffico
  - 2.7.1.3 Attacchi *aircrack*
    - 2.7.1.3.1. Attacchi WEP
    - 2.7.1.3.2. Attacchi WPA/WPA2

2.7.1.4. Attacchi di *Evil Twin*
2.7.1.5. Attacchi WPS
2.7.1.6. *Jamming*
2.7.2. Strumenti per la sicurezza wireless
2.8. Hacking di server web
2.8.1. *Cross site Scripting*
2.8.2. CSRF
2.8.3. *Session Hijacking*
2.8.4. SQL *injection*
2.9. Sfruttamento dei punti deboli
2.9.1. Utilizzo di *exploit* noti
2.9.2. Utilizzo di *metasploit*
2.9.3. Utilizzo di *malware*
2.9.3.1. Definizione e campo di applicazione
2.9.3.2. Generazione di *malware*
2.9.3.3. Bypassare le soluzioni antivirus
2.10. Persistenza
2.10.1. Installazione di *Rootkit*
2.10.2. Utilizzo di Ncat
2.10.3. Utilizzo di attività pianificate per le *Backdoor*
2.10.4. Creazione di utenti
2.10.5. Rilevamento HIDS

Modulo 3. Sviluppo sicuro

3.1. Sviluppo sicuro
3.1.1. Qualità, funzionalità e sicurezza
3.1.2. Riservatezza, integrità e disponibilità
3.1.3. Ciclo di vita dello sviluppo del software
3.2. Fase dei requisiti
3.2.1. Controllo dell'autenticazione
3.2.2. Controllo dei ruoli e dei privilegi
3.2.3. Requisiti orientati al rischio
3.2.4. Approvazione dei privilegi

3.3. Fasi di analisi e progettazione
- 3.3.1. Accesso ai componenti e amministrazione del sistema
- 3.3.2. Tracce di audit
- 3.3.3. Gestione delle sessioni
- 3.3.4. Dati storici
- 3.3.5. Gestione appropriata degli errori
- 3.3.6. Separazione delle funzioni

3.4. Fase di implementazione e codifica
- 3.4.1. Protezione dell'ambiente di sviluppo
- 3.4.2. Preparazione della documentazione tecnica
- 3.4.3. Codifica sicura
- 3.4.4. Sicurezza nelle comunicazioni

3.5. Buone pratiche di codifica sicura
- 3.5.1. Convalida dei dati di ingresso
- 3.5.2. Codifica dei dati di uscita
- 3.5.3. Stile di programmazione
- 3.5.4. Gestione dei log delle modifiche
- 3.5.5. Pratiche crittografiche
- 3.5.6. Gestione degli errori e dei *log*
- 3.5.7. Gestione degli archivi
- 3.5.8. Gestione della memoria
- 3.5.9. Standardizzazione e riutilizzo delle funzioni di sicurezza

3.6. Preparazione del server e *hardening*
- 3.6.1. Gestione di utenti, gruppi e ruoli sul server
- 3.6.2. Installazione software
- 3.6.3. *Hardening* del server
- 3.6.4. Configurazione robusta del contesto di applicazione

3.7. Preparazione della Base di Dati e dell'*hardening*
- 3.7.1. Ottimizzazione del motore della Base di Dati
- 3.7.2. Creare un proprio utente per l'applicazione
- 3.7.3. Assegnazione dei privilegi necessari all'utente
- 3.7.4. *Hardening* dei database

3.8. Fase di test
- 3.8.1. Controllo qualità negli audit di sicurezza
- 3.8.2. Ispezione del codice per fasi
- 3.8.3. Verifica della gestione delle configurazioni
- 3.8.4. Test black box

3.9. Preparare il passaggio alla produzione
- 3.9.1. Eseguire il controllo delle modifiche
- 3.9.2. Eseguire la procedura di cambio produzione
- 3.9.3. Eseguire la procedura di *rollback*
- 3.9.4. Test di pre-produzione

3.10. Fase di manutenzione
- 3.10.1. Garanzia basata sul rischio
- 3.10.2. Test di manutenzione della sicurezza white box
- 3.10.3. Test di manutenzione della sicurezza black box

Un'esperienza di specializzazione unica e decisiva per crescere a livello professionale"

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

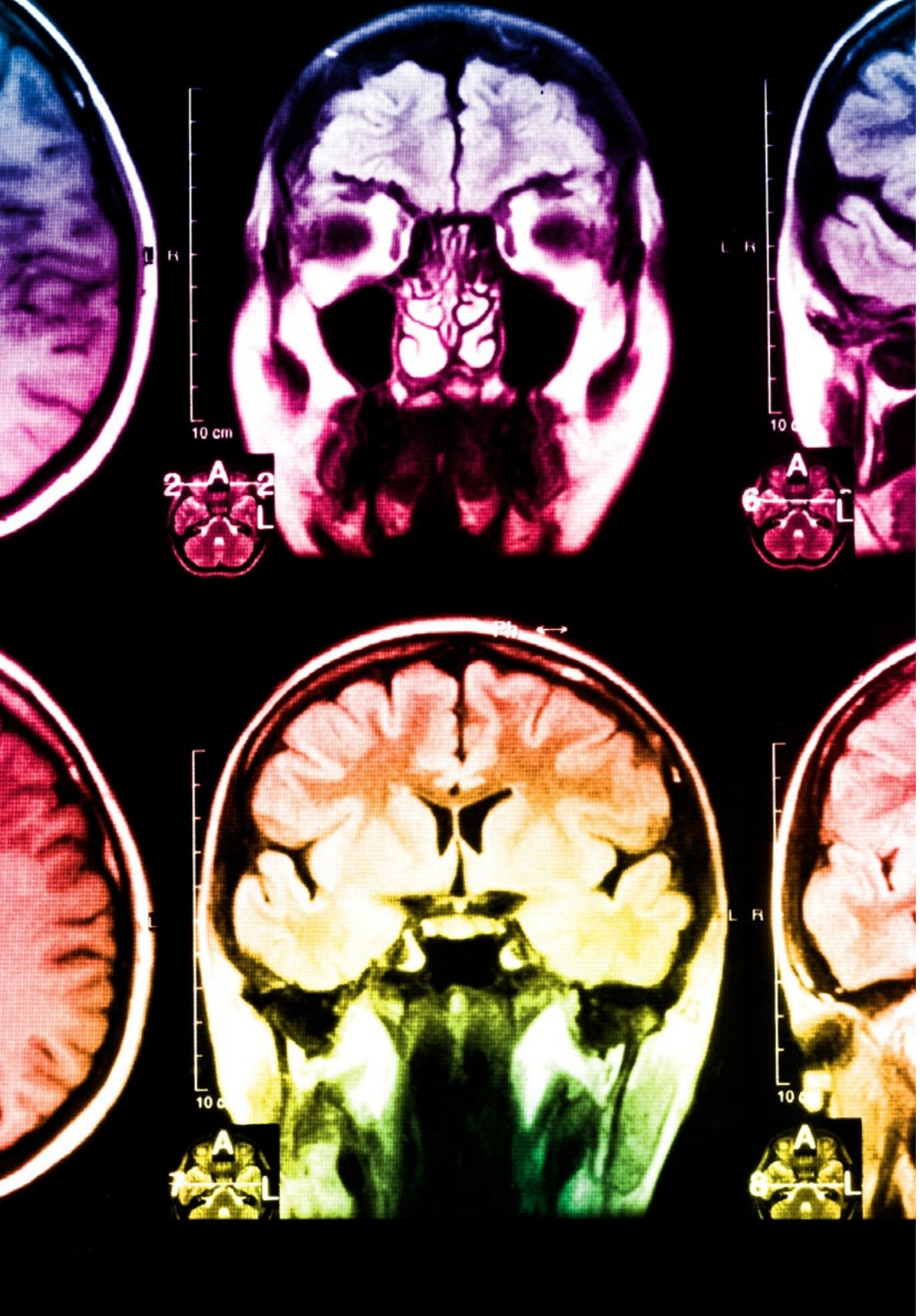
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

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.

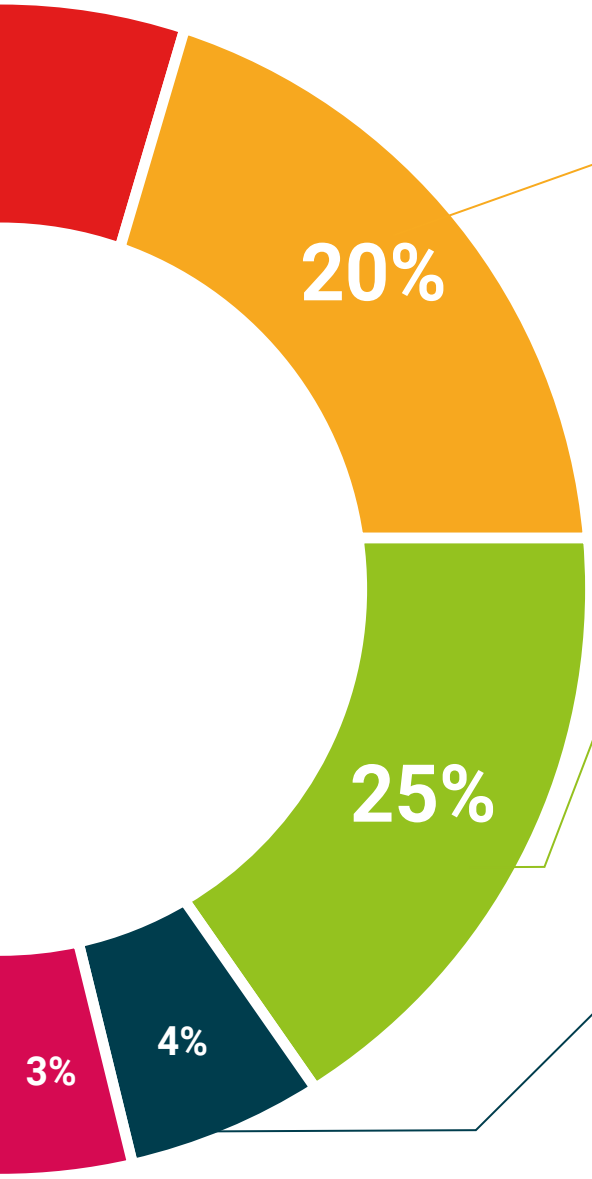
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

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 Preventiva 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 Preventiva** possiede il programma 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 Preventiva**

Ore Ufficiali: **450**


tech università tecnologica

Conferisce il presente

DIPLOMA

a

Dott./Dott.ssa _____, con documento d'identità nº_____

Per aver completato con esito positivo e accreditato il programma di

ESPERTO UNIVERSITARIO

in

Cibersicurezza Preventiva

Si tratta di un titolo rilasciato da questa Università ed equivalente a 450 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 Preventiva

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

Esperto Universitario

Cibersicurezza Preventiva

tech università tecnologica