Esperto Universitario

Analisi e Rilevamento delle Minacce di Cibersicurezza con Intelligenza Artificiale

tech global university

tech global university

Esperto Universitario
Analisi e Rilevamento delle Minacce di Cibersicurezza con Intelligenza Artificiale

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

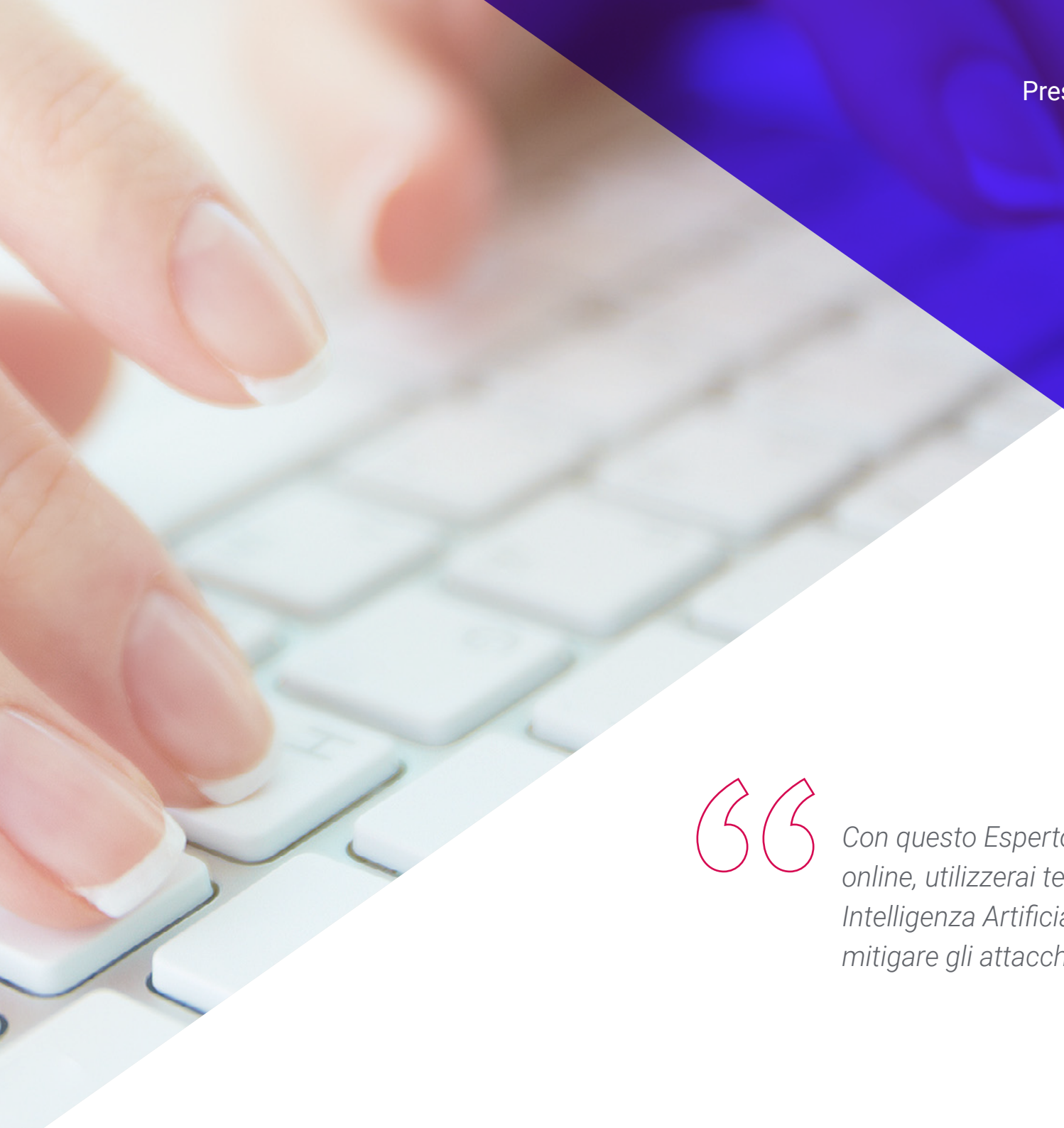
Accesso al sito web: **www.techtitute.com/it/intelligenza-artificiale/esperto-universitario/esperto-analisi-rilevamento-minacce-cibersicurezza-intelligenza-artificiale**

Indice

01

Presentazione del programma

L'identificazione precoce delle minacce informatiche è fondamentale per prevenire danni alle infrastrutture digitali delle organizzazioni. Tuttavia, le minacce continuano ad evolversi a una velocità senza precedenti, rendendo difficile l'uso di strumenti tradizionali per mitigare i rischi. Di fronte a questo, l'Intelligenza Artificiale ha rivoluzionato l'analisi della Cibersicurezza consentendo l'automazione del processo di identificazione delle minacce e il miglioramento della precisione dei sistemi di rilevamento. Gli esperti devono quindi utilizzare le tecniche di apprendimento automatico più innovative per identificare i modelli di comportamento anomali e anticipare gli attacchi informatici. Con l'obiettivo di facilitare questo lavoro, TECH propone una rivoluzionaria qualifica universitaria focalizzata sull'Analisi e il Rilevamento delle Minacce di Cibersicurezza con Intelligenza Artificiale.



Con questo Esperto Universitario, 100% online, utilizzerai tecniche innovative di Intelligenza Artificiale per identificare e mitigare gli attacchi digitali in tempo reale"

Secondo un nuovo rapporto delle Nazioni Unite, si stima che i costi globali degli attacchi informatici raggiungeranno i 10,5 miliardi di dollari l'anno prossimo. Questa crescita è in parte dovuta alla sofisticazione dei metodi di attacco, che rende le tecniche tradizionali di rilevamento insufficienti. In questo contesto, l'Intelligenza Artificiale è diventata uno strumento chiave nella prevenzione delle minacce, consentendo ai sistemi di identificare modelli anomali e rispondere agli incidenti in tempo reale. Ecco perché è importante che i professionisti sviluppino competenze avanzate per implementare sistemi intelligenti che migliorino l'efficienza e la precisione del rilevamento delle minacce informatiche.

In questo scenario, TECH presenta un pionieristico Esperto Universitario in Analisi e Rilevamento delle Minacce di Cibersicurezza con Intelligenza Artificiale. Ideato dai leader in questo settore, il percorso accademico approfondirà i fattori che comprendono dalla valutazione delle minacce assistite da sistemi intelligenti o l'applicazione di modelli generativi nella simulazione di attacchi fino alla creazione di un sistema di difesa predittivo con supporto ChatGPT. In questo modo, gli studenti acquisiranno competenze avanzate per progettare e implementare soluzioni di cibersicurezza basate sull'Intelligenza Artificiale, consentendo loro di anticipare e neutralizzare le minacce in modo proattivo.

D'altra parte, questo programma universitario si basa su un formato 100% online, di facile accesso da qualsiasi dispositivo con connessione internet e senza orari prestabiliti. TECH, inoltre, utilizza il suo metodo didattico dirompente *Relearning*, in modo che gli esperti possano approfondire i contenuti senza ricorrere a tecniche che comportano uno sforzo supplementare, come la memorizzazione. In questo senso, l'unica cosa di cui i professionisti avranno bisogno è avere un dispositivo elettronico con accesso a internet (come un cellulare, tablet o computer) per accedere ai materiali didattici più completi sul mercato e godere di un'esperienza di prima classe.

Questo **Esperto Universitario in Analisi e Rilevamento delle Minacce di Cibersicurezza con Intelligenza Artificiale** possiede il programma educativo più completo e aggiornato del mercato. Le sue caratteristiche principali sono:

- Sviluppo di casi pratici presentati da esperti con una profonda conoscenza della Cibersicurezza e dell'Intelligenza Artificiale, che applicano questi strumenti per il rilevamento, la prevenzione e l'attenuazione delle minacce informatiche in ambienti tecnologici avanzati
- 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
- Particolare enfasi è posta sulle metodologie innovative
- Lezioni teoriche, domande all'esperto e/o al tutor, forum di discussione su questioni controverse e compiti di riflessione individuale
- Disponibilità di accesso ai contenuti da qualsiasi dispositivo fisso o portatile dotato di connessione a Internet

> *Implementerai sistemi di rilevamento degli intrusi basati sull'Intelligenza Artificiale, ottimizzando la protezione delle infrastrutture critiche"*

Padroneggi gli algoritmi di Apprendimento Automatico per anticipare e neutralizzare i reati informatici"

Applicherai tecniche di analisi dei dati per identificare modelli e comportamenti anomali nelle reti informatiche.

Grazie al sistema Relearning non dovrai investire una grande quantità di ore di studio e ti concentrerai sui concetti più rilevanti.

Il personale docente del programma comprende rinomati specialisti del settore e altre aree correlate, 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 il professionista 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

Perché studiare in TECH?

TECH è la più grande università digitale del mondo. Con un catalogo eccezionale di oltre 14.000 programmi accademici disponibili in 11 lingue, si posiziona come leader in termini di occupabilità, con un tasso di inserimento professionale del 99%. Inoltre, dispone di un enorme personale docente, composto da oltre 6.000 professori di altissimo prestigio internazionale.

Studia presso la più grande università digitale del mondo e assicurati il successo professionale. Il futuro inizia con TECH"

La migliore università online al mondo secondo FORBES

La prestigiosa rivista Forbes, specializzata in affari e finanza, ha definito TECH "la migliore università online del mondo". Lo hanno recentemente affermato in un articolo della loro edizione digitale, che riporta il caso di successo di questa istituzione: "grazie all'offerta accademica che offre, alla selezione del suo personale docente e a un metodo innovativo di apprendimento orientato alla formazione dei professionisti del futuro".

Il miglior personale docente internazionale top

Il personale docente di TECH è composto da oltre 6.000 docenti di massimo prestigio internazionale. Professori, ricercatori e dirigenti di multinazionali, tra cui Isaiah Covington, allenatore dei Boston Celtics; Magda Romanska, ricercatrice principale presso MetaLAB ad Harvard; Ignacio Wistumba, presidente del dipartimento di patologia molecolare traslazionale di MD Anderson Cancer Center; o D.W Pine, direttore creativo della rivista TIME, ecc.

La più grande università digitale del mondo

TECH è la più grande università digitale del mondo. Siamo la più grande istituzione educativa, con il migliore e più ampio catalogo educativo digitale, cento per cento online e che copre la maggior parte delle aree di conoscenza. Offriamo il maggior numero di titoli di studio, diplomi e corsi post-laurea nel mondo. In totale, più di 14.000 corsi universitari, in undici lingue diverse, che ci rendono la più grande istituzione educativa del mondo.

I piani di studio più completi del panorama universitario

TECH offre i piani di studio più completi del panorama universitario, con argomenti che coprono concetti fondamentali e, allo stesso tempo, i principali progressi scientifici nelle loro specifiche aree scientifiche. Inoltre, questi programmi sono continuamente aggiornati per garantire agli studenti l'avanguardia accademica e le competenze professionali più richieste. In questo modo, i titoli universitari forniscono agli studenti un vantaggio significativo per elevare le loro carriere verso il successo.

Un metodo di apprendimento unico

TECH è la prima università ad utilizzare il *Relearning* in tutte le sue qualifiche. Si tratta della migliore metodologia di apprendimento online, accreditata con certificazioni internazionali di qualità docente, disposte da agenzie educative prestigiose. Inoltre, questo modello accademico dirompente è integrato con il "Metodo Casistico", configurando così una strategia di insegnamento online unica. Vengono inoltre implementate risorse didattiche innovative tra cui video dettagliati, infografiche e riassunti interattivi.

L'università online ufficiale dell'NBA

TECH è l'università online ufficiale dell'NBA. Grazie ad un accordo con la più grande lega di basket, offre ai suoi studenti programmi universitari esclusivi, nonché una vasta gamma di risorse educative incentrate sul business della lega e su altre aree dell'industria sportiva. Ogni programma presenta un piano di studi con un design unico e relatori ospiti eccezionali: professionisti con una distinta carriera sportiva che offriranno la loro esperienza nelle materie più rilevanti.

Leader nell'occupabilità

TECH è riuscita a diventare l'università leader nell'occupabilità. Il 99% dei suoi studenti ottiene un lavoro nel campo accademico che hanno studiato, prima di completare un anno dopo aver terminato uno qualsiasi dei programmi universitari. Una cifra simile riesce a migliorare la propria carriera professionale immediatamente. Tutto questo grazie ad una metodologia di studio che basa la sua efficacia sull'acquisizione di competenze pratiche, assolutamente necessarie per lo sviluppo professionale.

Google Partner Premier

Il gigante americano della tecnologia ha conferito a TECH il logo Google Partner Premier. Questo premio, accessibile solo al 3% delle aziende del mondo, conferisce valore all'esperienza efficace, flessibile e adattata che questa università offre agli studenti. Il riconoscimento non solo attesta il massimo rigore, rendimento e investimento nelle infrastrutture digitali di TECH, ma fa anche di questa università una delle compagnie tecnologiche più all'avanguardia del mondo.

L'università meglio valutata dai suoi studenti

Gli studenti hanno posizionato TECH come l'università più valutata al mondo nei principali portali di opinione, evidenziando il suo punteggio più alto di 4,9 su 5, ottenuto da oltre 1.000 recensioni. Questi risultati consolidano TECH come l'istituzione universitaria di riferimento a livello internazionale, riflettendo l'eccellenza e l'impatto positivo del suo modello educativo.

03

Piano di studi

I contenuti didattici che compongono questo Esperto Universitario sono stati elaborati da esperti riconosciuti nell'uso dell'Intelligenza Artificiale nella Cibersicurezza. Quindi, il piano di studi approfondirà questioni che vanno dall'uso di ChatGPT per l'analisi dei rischi o la formazione algoritmica a sofisticate tecniche di modellazione predittiva. Grazie a questo, gli studenti saranno in grado di applicare soluzioni avanzate di Intelligenza Artificiale per il rilevamento e la mitigazione delle minacce informatiche in tempo reale.

Approfondirai la creazione di protocolli di risposta automatizzati che consentano un recupero efficiente dei sistemi colpiti da un attacco informatico"

Modulo 1. Cibersicurezza e analisi delle minacce moderne con ChatGPT

1.1. Introduzione alla Cibersicurezza: minacce attuali e ruolo dell'Intelligenza Artificiale
- 1.1.1. Definizioni e concetti di base di Cibersicurezza
- 1.1.2. Tipi di minacce informatiche moderne
- 1.1.3. Ruolo dell'Intelligenza Artificiale nell'evoluzione della Cibersicurezza

1.2. Riservatezza, integrità e disponibilità (CIA) nell'era dell'Intelligenza Artificiale
- 1.2.1. Fondamenti del modello CIA nella Cibersicurezza
- 1.2.2. Principi di sicurezza applicati nel contesto dell'Intelligenza Artificiale
- 1.2.3. Sfide e considerazioni della CIA nei sistemi guidati dall'Intelligenza Artificiale

1.3. Uso di ChatGPT per l'analisi dei rischi e degli scenari di minaccia
- 1.3.1. Fondamenti dell'analisi del rischio nella Cibersicurezza
- 1.3.2. Capacità di ChatGPT di identificare e valutare scenari di minaccia
- 1.3.3. Vantaggi e limiti dell'analisi del rischio con l'Intelligenza Artificiale

1.4. ChatGPT nel rilevamento delle vulnerabilità critiche
- 1.4.1. Principi di rilevamento delle vulnerabilità nei sistemi informatici
- 1.4.2. Funzionalità di ChatGPT a supporto del rilevamento delle vulnerabilità
- 1.4.3. Considerazioni etiche e di sicurezza sull'uso dell'Intelligenza Artificiale nel rilevamento dei difetti

1.5. Analisi *malware* e *ransomware* assistita dall'Intelligenza Artificiale
- 1.5.1. Principi di base dell'analisi *malware* e *ransomware*
- 1.5.2. Tecniche di Intelligenza Artificiale applicate all'identificazione di codice maligno
- 1.5.3. Sfide tecniche e operative nell'analisi *malware* assistita dall'Intelligenza Artificiale

1.6. Identificazione degli attacchi comuni assistiti dall'Intelligenza Artificiale: *phishing*, social engineering ed exploit
- 1.6.1. Classificazione degli attacchi: *phishing*, social engineering e exploit
- 1.6.2. Tecniche di Intelligenza Artificiale per l'identificazione e l'analisi di attacchi comuni
- 1.6.3. Difficoltà e limiti dei modelli di Intelligenza Artificiale nella rilevazione degli attacchi

1.7. ChatGPT nell'addestramento e nella simulazione delle minacce informatiche
- 1.7.1. Fondamenti della simulazione delle minacce per la formazione sulla Cibersicurezza
- 1.7.2. Funzionalità di ChatGPT per la progettazione di scenari di simulazione
- 1.7.3. Vantaggi della simulazione delle minacce come strumento di formazione

1.8. Politiche di sicurezza informatica con raccomandazioni di Intelligenza Artificiale
- 1.8.1. Principi per la formulazione delle politiche di Cibersicurezza
- 1.8.2. Ruolo dell'Intelligenza Artificiale nella generazione di raccomandazioni di sicurezza
- 1.8.3. Componenti chiave delle politiche di sicurezza basate sull'Intelligenza Artificiale

1.9. Sicurezza dei dispositivi IoT e ruolo dell'Intelligenza Artificiale
- 1.9.1. Fondamenti della sicurezza nell'Internet of Things (IoT)
- 1.9.2. Capacità dell'Intelligenza Artificiale di mitigare le vulnerabilità dei dispositivi IoT
- 1.9.3. Sfide e considerazioni specifiche dell'Intelligenza Artificiale per la sicurezza dell'IoT

1.10. Strumenti di valutazione e risposta alle minacce assistiti dall'Intelligenza Artificiale
- 1.10.1. Principi di valutazione delle minacce alla Cibersicurezza
- 1.10.2. Caratteristiche delle risposte automatiche assistite dall'Intelligenza Artificiale
- 1.10.3. Fattori critici per l'efficacia delle risposte informatiche che utilizzano l'Intelligenza Artificiale

Modulo 2. Rilevamento e prevenzione delle intrusioni con modelli di Intelligenza Artificiale Generativa

2.1. Fondamenti dei sistemi IDS/IPS e ruolo dell'Intelligenza Artificiale
- 2.1.1. Definizione e principi di base dei sistemi IDS e IPS
- 2.1.2. Principali tipi e configurazioni di IDS/IPS
- 2.1.3. Contributo dell'Intelligenza Artificiale all'evoluzione dei sistemi di rilevamento e prevenzione

2.2. Utilizzo di Gemini per il rilevamento delle anomalie di rete
- 2.2.1. Concetti e tipi di anomalie del traffico di rete
- 2.2.2. Caratteristiche di Gemini per l'analisi dei dati di rete
- 2.2.3. Vantaggi del rilevamento delle anomalie nella prevenzione delle intrusioni

2.3. Gemini e l'identificazione dei modelli di intrusione
  2.3.1. Principi di identificazione e classificazione dei modelli di intrusione
  2.3.2. Tecniche di Intelligenza Artificiale applicate al rilevamento di schemi di minacce
  2.3.3. Tipi di pattern e comportamenti anomali nella sicurezza delle reti
2.4. Applicazione di modelli generativi nella simulazione di attacchi
  2.4.1. Fondamenti dei modelli generativi di Intelligenza Artificiale
  2.4.2. Uso di modelli generativi per ricreare scenari di attacco
  2.4.3. Vantaggi e limiti della simulazione di attacchi tramite l'Intelligenza Artificiale generativa
2.5. *Clustering* e la classificazione degli eventi tramite l'Intelligenza Artificiale
  2.5.1. Fondamenti di *clustering* e classificazione nel rilevamento delle intrusioni
  2.5.2. Algoritmi comuni di *clustering* applicati alla Cibersicurezza
  2.5.3. Ruolo dell'Intelligenza Artificiale nel miglioramento dei metodi di classificazione degli eventi
2.6. Gemini nella generazione di profili comportamentali
  2.6.1. Concetti di profilazione dell'utente e del dispositivo
  2.6.2. Applicazione dei modelli generativi nella profilazione
  2.6.3. Vantaggi della profilazione comportamentale nel rilevamento delle minacce
2.7. Analisi dei *Big Data* per la prevenzione delle intrusioni
  2.7.1. Importanza dei *Big Data* nel rilevamento dei modelli di sicurezza
  2.7.2. Metodi di elaborazione di grandi volumi di dati in Cibersicurezza
  2.7.3. Applicazioni dell'Intelligenza Artificiale nell'analisi e nella prevenzione basate sui *Big Data*
2.8. Riduzione dei dati e selezione delle caratteristiche rilevanti con l'Intelligenza Artificiale
  2.8.1. Principi di riduzione della dimensionalità in grandi volumi di dati
  2.8.2. Selezione delle caratteristiche per migliorare l'efficienza dell'analisi dell'Intelligenza Artificiale
  2.8.3. Tecniche di riduzione dei dati applicate alla Cibersicurezza
2.9. Valutazione dei modelli di Intelligenza Artificiale nel rilevamento delle intrusioni
  2.9.1. Criteri di valutazione dei modelli di Intelligenza Artificiale nella Cibersicurezza
  2.9.2. Indicatori di performance e di accuratezza dei modelli
  2.9.3. Importanza della validazione e della valutazione continua nell'Intelligenza Artificiale
2.10. Implementazione di un sistema di rilevamento delle intrusioni potenziato dall'Intelligenza Artificiale Generativa
  2.10.1. Nozioni di base per l'implementazione di un sistema di rilevamento delle intrusioni
  2.10.2. Integrazione dell'Intelligenza Artificiale generativa nei sistemi IDS/IPS
  2.10.3. Aspetti fondamentali per la configurazione e la manutenzione dei sistemi basati sull'Intelligenza Artificiale

Modulo 3. Modelli predittivi per la difesa proattiva nella Cibersicurezza utilizzando ChatGPT

3.1. Analisi predittiva nella Cibersicurezza: tecniche e applicazioni con l'Intelligenza Artificiale
  3.1.1. Concetti di base dell'analisi predittiva nella sicurezza
  3.1.2. Tecniche predittive nel campo della Cibersicurezza
  3.1.3. Applicazione dell'Intelligenza Artificiale nell'anticipazione delle minacce informatiche
3.2. Modelli di regressione e classificazione supportati da ChatGPT
  3.2.1. Principi di regressione e classificazione nella previsione delle minacce
  3.2.2. Tipi di modelli di classificazione nella Cibersicurezza
  3.2.3. Assistenza di ChatGPT nell'interpretazione dei modelli predittivi
3.3. Identificazione delle minacce emergenti con le previsioni di ChatGPT
  3.3.1. Concetti di rilevamento delle minacce emergenti
  3.3.2. Tecniche per identificare nuovi modelli di attacco
  3.3.3. Limiti e precauzioni nella previsione di nuove minacce

3.4. Reti neurali per anticipare gli attacchi informatici
- 3.4.1. Fondamenti delle reti neurali applicate alla Cibersicurezza
- 3.4.2. Architetture comuni per il rilevamento e la previsione degli attacchi
- 3.4.3. Sfide nell'implementazione delle reti neurali nella difesa informatica

3.5. Uso di ChatGPT per la simulazione di scenari di minaccia
- 3.5.1. Concetti di base della simulazione delle minacce nella Cibersicurezza
- 3.5.2. Funzionalità di ChatGPT per lo sviluppo di simulazioni predittive
- 3.5.3. Fattori da considerare nella progettazione di scenari simulati

3.6. Algoritmi di apprendimento rinforzato per l'ottimizzazione della difesa
- 3.6.1. Introduzione all'apprendimento per rinforzo nella Cibersicurezza
- 3.6.2. Algoritmi di rinforzo applicati alle strategie di difesa
- 3.6.3. Vantaggi e sfide dell'apprendimento per rinforzo negli ambienti di Cibersicurezza

3.7. Simulazione di minacce e risposte con ChatGPT
- 3.7.1. Principi di simulazione delle minacce e loro rilevanza nella difesa informatica
- 3.7.2. Risposte automatiche e ottimizzate agli attacchi simulati
- 3.7.3. Vantaggi della simulazione per migliorare la preparazione informatica

3.8. Valutazione di accuratezza ed efficacia dei modelli predittivi di Intelligenza Artificiale
- 3.8.1. Indicatori chiave per la valutazione dei modelli predittivi
- 3.8.2. Metodologie di valutazione dell'accuratezza nei modelli di Cibersicurezza
- 3.8.3. Fattori critici per l'efficacia dei modelli di Intelligenza Artificiale nella Cibersicurezza

3.9. Intelligenza Artificiale nella gestione degli incidenti e nelle risposte automatiche
- 3.9.1. Fondamenti della gestione degli incidenti di Cibersicurezza
- 3.9.2. Ruolo dell'Intelligenza Artificiale nel processo decisionale in tempo reale
- 3.9.3. Sfide e opportunità nell'automazione della risposta

3.10. Costruire un sistema di difesa predittivo con il supporto di ChatGPT
- 3.10.1. Principi di progettazione di un sistema di difesa proattiva
- 3.10.2. Integrazione di modelli predittivi in ambienti di Cibersicurezza
- 3.10.3. Componenti chiave di un sistema di difesa predittivo basato sull'Intelligenza Artificiale

Utilizzerai software all'avanguardia come TensorFlow per addestrare modelli di apprendimento automatico che rafforzano le soluzioni di Cibersicurezza nei diversi ambienti organizzativi"

04

Obiettivi didattici

Attraverso questo programma universitario, i professionisti acquisiranno le competenze avanzate per condurre con successo strategie di Cibersicurezza in ambienti tecnologici avanzati. Attraverso un approccio pratico, svilupperai competenze fondamentali per implementare sistemi di rilevamento, valutare i rischi e creare difese proattive supportate dall'Intelligenza Artificiale, rafforzare la propria capacità di proteggere le infrastrutture digitali e rispondere in modo efficiente alle minacce informatiche emergenti.

Otterrai competenze avanzate nel rilevamento delle intrusioni e nell'analisi predittiva per guidare le strategie di difesa proattiva negli ambienti digitali"

Obiettivi generali

- Analizzare le principali minacce informatiche moderne e la loro evoluzione nel contesto dell'Intelligenza Artificiale
- Identificare modelli anomali nei sistemi digitali utilizzando strumenti avanzati di Intelligenza Artificiale
- Sviluppare strategie di rilevamento e prevenzione delle intrusioni utilizzando modelli generativi e predittivi
- Implementare sistemi di difesa proattivi basati su tecniche di analisi predittiva e apprendimento automatico
- Progettare simulazioni di attacchi informatici per valutare le vulnerabilità e ottimizzare le difese
- Applicare algoritmi di Intelligenza Artificiale nella gestione degli incidenti e risposte automatizzate
- Ottimizzare la sicurezza dei dispositivi connessi mitigando i rischi specifici dell'IoT
- Valutare l'efficacia e la precisione dei modelli di Intelligenza Artificiale applicati alla Cibersicurezza
- Sviluppare politiche di sicurezza informatica basate su raccomandazioni basate sull'Intelligenza Artificiale
- Promuovere l'uso etico e responsabile dell'Intelligenza Artificiale nella protezione di sistemi e dati

Obiettivi specifici

Modulo 1. Cibersicurezza e analisi delle minacce moderne con ChatGPT

- Comprendere i concetti fondamentali della sicurezza informatica, comprese le minacce moderne e il modello CIA
- Utilizzare ChatGPT per l'analisi dei rischi, il rilevamento delle vulnerabilità e la simulazione di scenari di minaccia
- Sviluppare competenze per progettare politiche di sicurezza informatica efficaci e proteggere i dispositivi IoT tramite l'Intelligenza Artificiale
- Implementare strategie avanzate di gestione delle minacce utilizzando l'Intelligenza Artificiale generativa per anticipare potenziali attacchi
- Valutare l'impatto delle minacce moderne sulle infrastrutture critiche mediante tecniche di simulazione assistita da Intelligenza Artificiale
- Progettare soluzioni personalizzate per la protezione delle reti aziendali, basate

  in strumenti avanzati di Intelligenza Artificiale

Modulo 2. Rilevamento e prevenzione delle intrusioni con modelli di Intelligenza Artificiale Generativa

- Padroneggiare le tecniche di rilevamento delle anomalie e degli schemi di intrusione con strumenti come Gemini
- Applicare modelli generativi per simulare attacchi informatici e migliorare la prevenzione di intrusioni
- Implementare sistemi IDS/IPS avanzati ottimizzati con l'Intelligenza Artificiale, sviluppando profili comportamentali e analizzando Big Data in tempo reale
- Progettare architetture di sicurezza integrate con l'Intelligenza Artificiale per la protezione degli ambienti multi-utente e dei sistemi distribuiti
- Utilizzare modelli generativi per anticipare attacchi mirati e sviluppare contromisure in tempo reale
- Integrare l'analisi predittiva nei sistemi di rilevamento per la gestione dinamica di minacce emergenti

Modulo 3. Modelli predittivi per la difesa proattiva nella Cibersicurezza utilizzando ChatGPT

- Progettare modelli predittivi avanzati basati su reti neurali e apprendimento per il rinforzo
- Implementare simulazioni di scenari di minaccia per addestrare i team e migliorare la preparazione agli incidenti
- Valutare e ottimizzare i sistemi di difesa proattiva, integrando l'Intelligenza Artificiale generativa nel processo decisionale e nell'automazione delle risposte
- Sviluppare *framework* di difesa predittiva adattabili alle infrastrutture critiche e ai sistemi aziendali
- Utilizzare l'analisi predittiva per identificare le vulnerabilità emergenti prima di essere sfruttate
- Integrare l'Intelligenza Artificiale generativa nei processi decisionali strategici per il miglioramento continuo dei sistemi difensivi

05

Opportunità professionali

Dopo aver completato questo Esperto Universitario di TECH, i professionisti saranno altamente qualificati per assumere ruoli chiave come Analista di Cibersicurezza, Specialista di Rilevamento delle Minacce, Consulente per i Sistemi di Difesa Proattiva o Esperto in Protezione delle Infrastrutture Digitali. Inoltre, la loro attenzione all'uso dell'Intelligenza Artificiale applicata consentirà loro di guidare progetti innovativi in ambienti aziendali, governativi e tecnologici avanzati.

Stai cercando di diventare Chief Information Security Officer? Raggiungi tale obiettivo con questo programma universitario in pochi mesi”

Profilo dello studente

Lo studente di questa qualifica sarà un professionista altamente qualificato per affrontare le sfide della sicurezza digitale attuale. Con una conoscenza avanzata dell'Intelligenza Artificiale, sarà preparato per creare strategie di protezione, implementare sistemi per il rilevamento delle minacce e gestire gli incidenti in tempo reale. La sua padronanza di strumenti innovativi e l'approccio etico lo posizioneranno come un esperto in grado di proteggere le infrastrutture critiche e guidare i progetti in ambienti tecnologici sofisticati.

Fornirai consulenza completa alle organizzazioni sull'integrazione di sistemi intelligenti per rafforzare le loro infrastrutture digitali.

- **Adattabilità tecnologica:** Capacità di incorporare in modo efficiente nuovi strumenti, tecniche e metodologie basate sull'Intelligenza Artificiale, adattandosi rapidamente ai progressi tecnologici e applicandoli in vari ambienti di lavoro con standard elevati
- **Comunicazione efficace:** Capacità di esprimere idee, risultati e strategie in modo chiaro e strutturato, adattando il linguaggio tecnico per renderlo comprensibile sia ai team multidisciplinari che a un pubblico non specializzato nel settore tecnologico
- **Gestione dei progetti:** Capacità di pianificare, organizzare e coordinare progetti di cibersicurezza, monitorando l'implementazione delle soluzioni e garantendo il rispetto di scadenze, risorse e obiettivi strategici in contesti dinamici e mutevoli
- **Collaborazione interdisciplinare:** Capacità di lavorare in modo efficace con team diversi, integrando conoscenze e prospettive da settori come Cibersicurezza, Intelligenza Artificiale, tecnologia e gestione aziendale, al fine di raggiungere obiettivi comuni e generare soluzioni complete

Dopo aver completato il programma potrai utilizzare le tue conoscenze e competenze nei seguenti ruoli:

1. **Analista di Cibersicurezza Specializzato in Intelligenza Artificiale:** Responsabile di identificare vulnerabilità e minacce nei sistemi digitali utilizzando strumenti avanzati di Intelligenza Artificiale per proteggere le reti e i dati critici.
2. **Specialista in Rilevamento di Intrusioni nei Sistemi:** Responsabile di implementare e gestire sistemi di rilevamento intrusione potenziati da Intelligenza Artificiale per evitare accessi non autorizzati nelle infrastrutture digitali.
3. **Consulente per la Sicurezza dei Dispositivi Connessi:** Responsabile della mitigazione dei rischi associati ai dispositivi IoT, garantendo la loro sicurezza in ambienti aziendali e domestici.
4. **Specialista in Analisi Predittiva delle Minacce Informatiche:** Si concentra sull'anticipazione di potenziali attacchi applicando modelli e tecniche predittive di apprendimento automatico.
5. **Analista di Risposta agli Incidenti con Intelligenza Artificiale:** Responsabile di gestire e automatizzare la risposta agli incidenti informatici utilizzando strumenti di Intelligenza Artificiale.
6. **Revisore di Vulnerabilità Assistito da Intelligenza Artificiale:** Responsabile di valutare i sistemi digitali per rilevare le lacune di sicurezza e proporre soluzioni efficaci con il supporto di strumenti di Intelligenza Artificiale.

Progetterai soluzioni avanzate di Cibersicurezza basate sull'Intelligenza Artificiale per rilevare e prevenire le minacce informatiche"

06

Metodologia di studio

TECH è la prima università al mondo che combina la metodologia dei ***case studies*** con il ***Relearning***, un sistema di apprendimento 100% online basato sulla ripetizione diretta.

Questa strategia dirompente è stata concepita per offrire ai professionisti l'opportunità di aggiornare le conoscenze e sviluppare competenze in modo intensivo e rigoroso. Un modello di apprendimento che pone lo studente al centro del processo accademico e gli conferisce tutto il protagonismo, adattandosi alle sue esigenze e lasciando da parte le metodologie più convenzionali.

TECH ti prepara ad affrontare nuove sfide in ambienti incerti e a raggiungere il successo nella tua carriera"

Lo studente: la priorità di tutti i programmi di TECH

Nella metodologia di studio di TECH lo studente è il protagonista assoluto.
Gli strumenti pedagogici di ogni programma sono stati selezionati tenendo conto delle esigenze di tempo, disponibilità e rigore accademico che, al giorno d'oggi, non solo gli studenti richiedono ma le posizioni più competitive del mercato.

Con il modello educativo asincrono di TECH, è lo studente che sceglie il tempo da dedicare allo studio, come decide di impostare le sue routine e tutto questo dalla comodità del dispositivo elettronico di sua scelta. Lo studente non deve frequentare lezioni presenziali, che spesso non può frequentare. Le attività di apprendimento saranno svolte quando si ritenga conveniente. È lo studente a decidere quando e da dove studiare.

In TECH NON ci sono lezioni presenziali (che poi non potrai mai frequentare)"

I piani di studio più completi a livello internazionale

TECH si caratterizza per offrire i percorsi accademici più completi del panorama universitario. Questa completezza è raggiunta attraverso la creazione di piani di studio che non solo coprono le conoscenze essenziali, ma anche le più recenti innovazioni in ogni area.

Essendo in costante aggiornamento, questi programmi consentono agli studenti di stare al passo con i cambiamenti del mercato e acquisire le competenze più apprezzate dai datori di lavoro. In questo modo, coloro che completano gli studi presso TECH ricevono una preparazione completa che fornisce loro un notevole vantaggio competitivo per avanzare nelle loro carriere.

Inoltre, potranno farlo da qualsiasi dispositivo, pc, tablet o smartphone.

> *Il modello di TECH è asincrono, quindi ti permette di studiare con il tuo pc, tablet o smartphone dove, quando e per quanto tempo vuoi"*

Case studies o Metodo Casistico

Il Metodo Casistico è stato il sistema di apprendimento più usato nelle migliori facoltà del mondo. Sviluppato nel 1912 per consentire agli studenti di Giurisprudenza non solo di imparare le leggi sulla base di contenuti teorici, ma anche di esaminare situazioni complesse reali. In questo modo, potevano prendere decisioni e formulare giudizi di valore fondati su come risolverle. Nel 1924 fu stabilito come metodo di insegnamento standard ad Harvard.

Con questo modello di insegnamento, è lo studente stesso che costruisce la sua competenza professionale attraverso strategie come il *Learning by doing* o il *Design Thinking*, utilizzate da altre istituzioni rinomate come Yale o Stanford.

Questo metodo, orientato all'azione, sarà applicato lungo tutto il percorso accademico che lo studente intraprende insieme a TECH. In questo modo, affronterà molteplici situazioni reali e dovrà integrare le conoscenze, ricercare, argomentare e difendere le sue idee e decisioni. Tutto ciò con la premessa di rispondere al dubbio di come agirebbe nel posizionarsi di fronte a specifici eventi di complessità nel suo lavoro quotidiano.

Metodo *Relearning*

In TECH i *case studies* vengono potenziati con il miglior metodo di insegnamento 100% online: il *Relearning*.

Questo metodo rompe con le tecniche di insegnamento tradizionali per posizionare lo studente al centro dell'equazione, fornendo il miglior contenuto in diversi formati. In questo modo, riesce a ripassare e ripete i concetti chiave di ogni materia e impara ad applicarli in un ambiente reale.

In questa stessa linea, e secondo molteplici ricerche scientifiche, la ripetizione è il modo migliore per imparare. Ecco perché TECH offre da 8 a 16 ripetizioni di ogni concetto chiave in una stessa lezione, presentata in modo diverso, con l'obiettivo di garantire che la conoscenza sia completamente consolidata durante il processo di studio.

Il Relearning ti consentirà di apprendere con meno sforzo e più rendimento, coinvolgendoti maggiormente nella specializzazione, sviluppando uno spirito critico, difendendo gli argomenti e contrastando opinioni: un'equazione diretta al successo.

Un Campus Virtuale 100% online con le migliori risorse didattiche

Per applicare efficacemente la sua metodologia, TECH si concentra sul fornire agli studenti materiali didattici in diversi formati: testi, video interattivi, illustrazioni, mappe della conoscenza, ecc. Tutto ciò progettato da insegnanti qualificati che concentrano il lavoro sulla combinazione di casi reali con la risoluzione di situazioni complesse attraverso la simulazione, lo studio dei contesti applicati a ogni carriera e l'apprendimento basato sulla ripetizione, attraverso audio, presentazioni, animazioni, immagini, ecc.

Le ultime prove scientifiche nel campo delle Neuroscienze indicano l'importanza di considerare il luogo e il contesto in cui si accede ai contenuti prima di iniziare un nuovo apprendimento. Poter regolare queste variabili in modo personalizzato favorisce che le persone possano ricordare e memorizzare nell'ippocampo le conoscenze per conservarle a lungo termine. Si tratta di un modello denominato *Neurocognitive context-dependent e-learning,* che viene applicato in modo consapevole in questa qualifica universitaria.

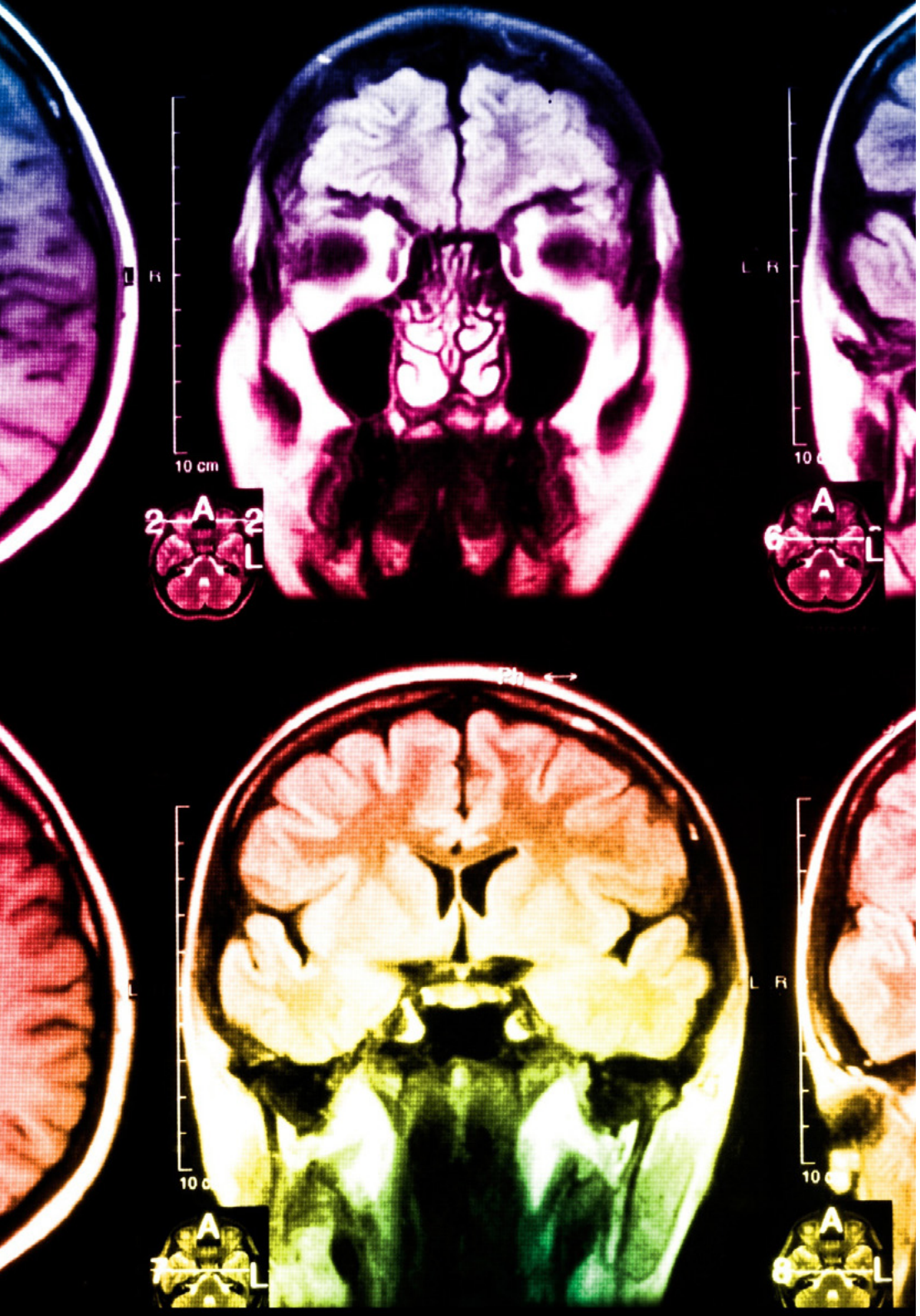
Inoltre, anche per favorire al massimo il contatto tra mentore e studente, viene fornita una vasta gamma di possibilità di comunicazione, sia in tempo reale che differita (messaggistica interna, forum di discussione, servizio di assistenza telefonica, e-mail di contatto con segreteria tecnica, chat e videoconferenza).

Inoltre, questo completo Campus Virtuale permetterà agli studenti di TECH di organizzare i loro orari di studio in base alla loro disponibilità personale o agli impegni lavorativi. In questo modo avranno un controllo globale dei contenuti accademici e dei loro strumenti didattici, il che attiva un rapido aggiornamento professionale.

> *La modalità di studio online di questo programma ti permetterà di organizzare il tuo tempo e il tuo ritmo di apprendimento, adattandolo ai tuoi orari"*

L'efficacia del metodo è giustificata da quattro risultati chiave:

1. Gli studenti che seguono questo metodo non solo raggiungono l'assimilazione dei concetti, ma sviluppano anche la loro capacità mentale, attraverso esercizi che valutano situazioni reali e l'applicazione delle conoscenze.
2. L'apprendimento è solidamente fondato su competenze pratiche che permettono allo studente di integrarsi meglio nel mondo reale.
3. L'assimilazione di idee e concetti è resa più facile ed efficace, grazie all'uso di situazioni nate dalla realtà.
4. La sensazione di efficienza dello sforzo investito diventa uno stimolo molto importante per gli studenti, che si traduce in un maggiore interesse per l'apprendimento e in un aumento del tempo dedicato al corso.



La metodologia universitaria più apprezzata dagli studenti

I risultati di questo innovativo modello accademico sono riscontrabili nei livelli di soddisfazione globale degli studenti di TECH.

La valutazione degli studenti sulla qualità dell'insegnamento, la qualità dei materiali, la struttura del corso e i suoi obiettivi è eccellente. A questo proposito, l'istituzione è diventata la migliore università valutata dai suoi studenti secondo l'indice global score, ottenendo un 4,9 su 5

Accedi ai contenuti di studio da qualsiasi dispositivo con connessione a Internet (computer, tablet, smartphone) grazie al fatto che TECH è aggiornato sull'avanguardia tecnologica e pedagogica.

Potrai imparare dai vantaggi dell'accesso a ambienti di apprendimento simulati e dall'approccio di apprendimento per osservazione, ovvero Learning from an expert.

In questo modo, il miglior materiale didattico sarà disponibile, preparato con attenzione:

Materiale di studio

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

Questi contenuti sono poi applicati al formato audiovisivo che supporterà la nostra modalità di lavoro online, impiegando le ultime tecnologie che ci permettono di offrirti una grande qualità per ogni elemento che metteremo al tuo servizio.

Capacità e competenze pratiche

I partecipanti svolgeranno attività per sviluppare competenze e abilità specifiche in ogni area tematica. Pratiche e dinamiche per acquisire e sviluppare le competenze e le abilità che uno specialista deve possedere nel mondo globalizzato in cui viviamo.

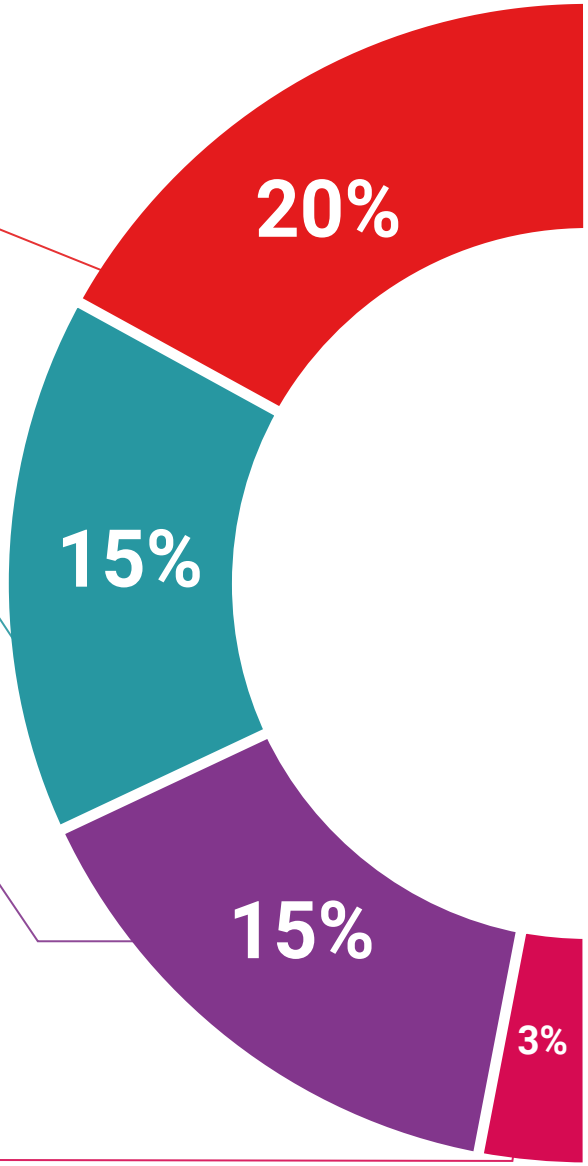
Riepiloghi interattivi

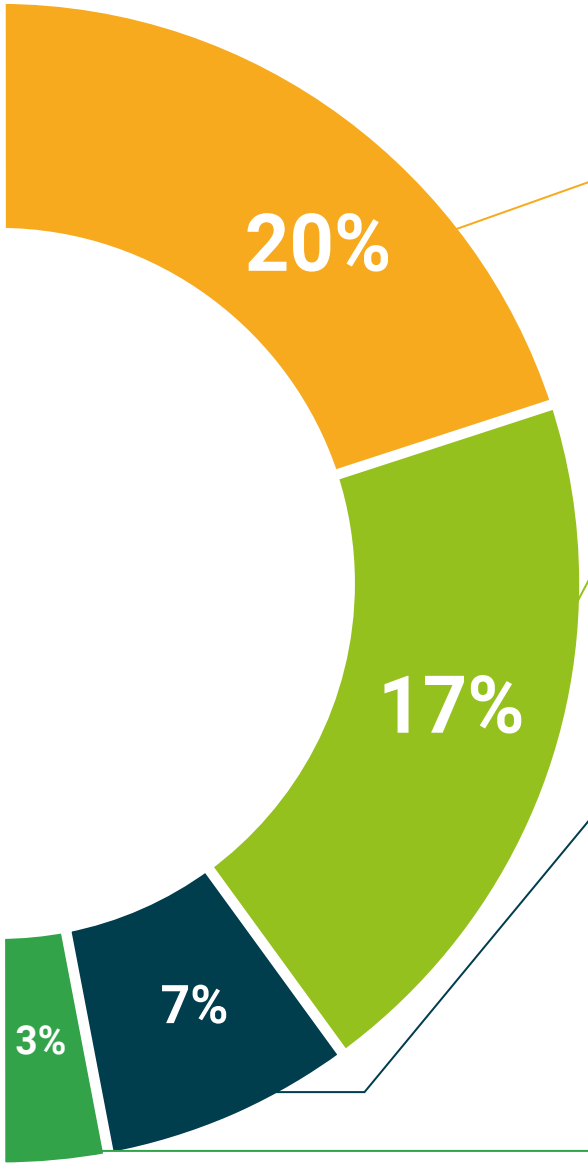
Presentiamo i contenuti in modo accattivante e dinamico tramite strumenti multimediali che includono audio, video, immagini, diagrammi e mappe concettuali per consolidare la conoscenza.

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

Letture complementari

Articoli recenti, documenti di consenso, guide internazionali... Nella biblioteca virtuale di TECH potrai accedere a tutto il materiale necessario per completare la tua specializzazione.





Case Studies

Completerai una selezione dei migliori *case studies* in materia. Casi presentati, analizzati e monitorati dai migliori specialisti del panorama internazionale.

Testing & Retesting

Valutiamo e rivalutiamo periodicamente le tue conoscenze durante tutto il programma. Lo facciamo su 3 dei 4 livelli della Piramide di Miller.

Master class

Esistono prove scientifiche sull'utilità d'osservazione di terzi esperti.

Il cosiddetto *Learning from an Expert* rafforza le conoscenze e i ricordi, e genera sicurezza nel futuro processo decisionale.

Guide di consultazione veloce

TECH offre i contenuti più rilevanti del corso sotto forma di schede o guide rapide per l'azione. Un modo sintetico, pratico ed efficace per aiutare a progredire nel tuo apprendimento.

07

Personale docente

La premessa fondamentale di TECH è quella di offrire le qualifiche universitarie più complete e aggiornate del panorama accademico, per cui seleziona con rigore il suo personale docente. Per la progettazione e l'insegnamento di questo Esperto Universitario, ha riunito gli specialisti più importanti nel campo dell'Analisi e del Rilevamento delle Minacce di Cibersicurezza con Intelligenza Artificiale. Hanno quindi elaborato diversi contenuti didattici che si distinguono per la loro eccellente qualità e per l'adeguamento alle esigenze del mercato del lavoro. In questo modo, gli studenti si immergeranno in un'esperienza ad alta intensità che amplierà notevolmente i loro orizzonti professionali.

Un personale docente esperto, altamente specializzato nell'uso dell'Intelligenza Artificiale nella Cibersicurezza, ti guiderà durante l'intero processo di apprendimento e risolverà i dubbi che possono sorgere"

Direzione

Dott. Peralta Martín-Palomino, Arturo

- CEO e CTO presso Prometeus Global Solutions
- CTO presso Korporate Technologies
- CTO presso AI Shephers GmbH
- Consulente e Assessore Aziendale Strategico presso Alliance Medical
- Direttore di Design e Sviluppo presso DocPath
- Dottorato in Ingegneria Informatica presso l'Università di Castiglia-La Mancha
- Dottorato in Economia Aziendale e Finanza conseguito presso l'Università Camilo José Cela
- Dottorato in Psicologia presso l'Università di Castiglia-La Mancha
- Master in Executive MBA presso l'Università Isabel I
- Master in Direzione Commerciale e Marketing presso l'Università Isabel I
- Master in Big Data presso la Formación Hadoop
- Master in Tecnologie Informatiche Avanzate presso l'Università di Castiglia-La Mancha
- Membro di: Gruppo di Ricerca SMILE

Personale docente

Dott. Del Rey Sánchez, Alejandro

- Responsabile dell'implementazione dei programmi per migliorare l'attenzione tattica in caso di emergenza
- Laurea in Ingegneria dell'Organizzazione Industriale
- Certificazione in *Big Data* e *Business Analytics*
- Certificazione in Microsoft Excel Avanzato, VBA, KPI e DAX
- Certificazione in CIS Sistemi di Telecomunicazione e Informazione

Un'esperienza di formazione unica, chiave e decisiva per promuovere il tuo sviluppo professionale"

08

Titolo

L'Esperto Universitario in Analisi e Rilevamento delle Minacce di Cibersicurezza con Intelligenza Artificiale garantisce, oltre alla preparazione più rigorosa e aggiornata, il conseguimento di 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 privato di **Esperto Universitario in Analisi e Rilevamento delle Minacce di Cibersicurezza con Intelligenza Artificiale** 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 Analisi e Rilevamento delle Minacce di Cibersicurezza con Intelligenza Artificiale**

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 Analisi e Rilevamento delle Minacce di Cibersicurezza con Intelligenza Artificiale

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

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

tech global university

Esperto Universitario
Analisi e Rilevamento delle Minacce di Cibersicurezza con Intelligenza Artificiale

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

Esperto Universitario

Analisi e Rilevamento delle Minacce di Cibersicurezza con Intelligenza Artificiale

tech global university