

# Corso Universitario Crittografia Avanzata



## Corso Universitario Crittografia Avanzata

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

Accesso al sito web: [www.techtitute.com/it/informatica/corso-universitario/crittografia-avanzata](http://www.techtitute.com/it/informatica/corso-universitario/crittografia-avanzata)

# Indice

01

Presentazione

---

*pag. 4*

02

Obiettivi

---

*pag. 8*

03

Direzione del corso

---

*pag. 12*

04

Struttura e contenuti

---

*pag. 16*

05

Metodologia di studio

---

*pag. 20*

06

Titolo

---

*pag. 30*

# 01

# Presentazione

La crittografia negli ultimi anni ha acquisito maggiore importanza. Non solo è una disciplina essenziale nella crittografia di chiavi e dati, ma è un elemento centrale in un nuovo campo tecnologico che sta vivendo un grande boom: la *Blockchain*. Per questo motivo, le aziende digitali e di sviluppo di applicazioni e altri strumenti informatici sono alla ricerca di specialisti in possesso di conoscenze avanzate in crittografia. Questo programma offre pertanto al professionista un approfondimento completo in questo settore, preparandolo a rispondere alle sfide attuali e future della sicurezza informatica. Tutto questo, basato su una metodologia di insegnamento online, grazie a cui gli studenti saranno in grado di combinare il loro lavoro e i loro studi in modo comodo e semplice.



“

*La crittografia è essenziale per la sicurezza informatica di aziende e tecnologie come la Blockchain. Pertanto, questo programma ti consentirà di progredire professionalmente in questo importante settore informatico"*

La crescente importanza della cibersicurezza ha dato una spinta enorme alla crittografia. Questa disciplina permette di codificare, cifrare e crittografare ogni tipo di dati, sia che si tratti di informazioni sensibili di una società, transazioni o di chiavi di accesso. Quindi, è fondamentale nel mondo digitale di oggi. Inoltre, l'emergere di altri settori come la *Blockchain* o l'intelligenza artificiale ha dato un ulteriore impulso in questo senso; quindi, è un settore con una grande domanda di professionisti specializzati.

Questo Corso Universitario in Crittografia Avanzata offre perciò la possibilità di approfondire le conoscenze in questo ambito, preparando l'informatico a rispondere a tutte le sfide presenti e future del settore. Durante questo programma il professionista approfondirà questioni come la steganografia e la steganalisi, la combinazione di cifre a blocchi, la crittografia asimmetrica o gli algoritmi quantistici.

Sulla base di un insegnamento 100% online, questo Corso Universitario permetterà all'informatico di crescere professionalmente grazie ai suoi contenuti aggiornati e al suo personale docente, composto da specialisti di crittografia che sono a conoscenza degli ultimi sviluppi in questo settore e delle loro applicazioni pratiche.

Questo **Corso Universitario in Crittografia Avanzata** 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 e/o al tutore, forum di discussione su questioni controverse e compiti di riflessione individuale
- ♦ Disponibilità di accesso ai contenuti da qualsiasi dispositivo fisso o portatile con una connessione internet



*Scopri le più recenti applicazioni della crittografia grazie a questo Corso Universitario, offerto in modalità 100% online"*

“ *Potrai approfondire lo studio delle migliori tecniche crittografiche a partire da numerose risorse multimediali: attività pratiche, riassunti multimediali, master class, ecc.* ”

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 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.

*Le aziende tecnologiche hanno bisogno di esperti in Crittografia Avanzata e questo Corso Universitario ti preparerà a migliorare professionalmente in questo campo.*

*Il sistema di apprendimento di TECH Global University ti permetterà di continuare a sviluppare la tua carriera professionale senza interruzioni o orari prestabiliti.*



# 02

## Obiettivi

Questo Corso Universitario in Crittografia Avanzata ha lo scopo principale di insegnare al professionista i migliori metodi crittografici, trasmettendogli, inoltre, le nuove applicazioni di questa importante disciplina. Diventerà così un informatico specializzato in crittografia in grado di risolvere diverse problematiche, sia in materia di sicurezza delle chiavi di accesso a un determinato sistema che nelle tecnologie emergenti come la *Blockchain*. Questo lo preparerà a lavorare in diversi settori, ampliando le sue prospettive di lavoro.



“

*Raggiungi tutti i tuoi obiettivi professionali  
specializzandoti in Crittografia Avanzata  
grazie a questo Corso Universitario"*



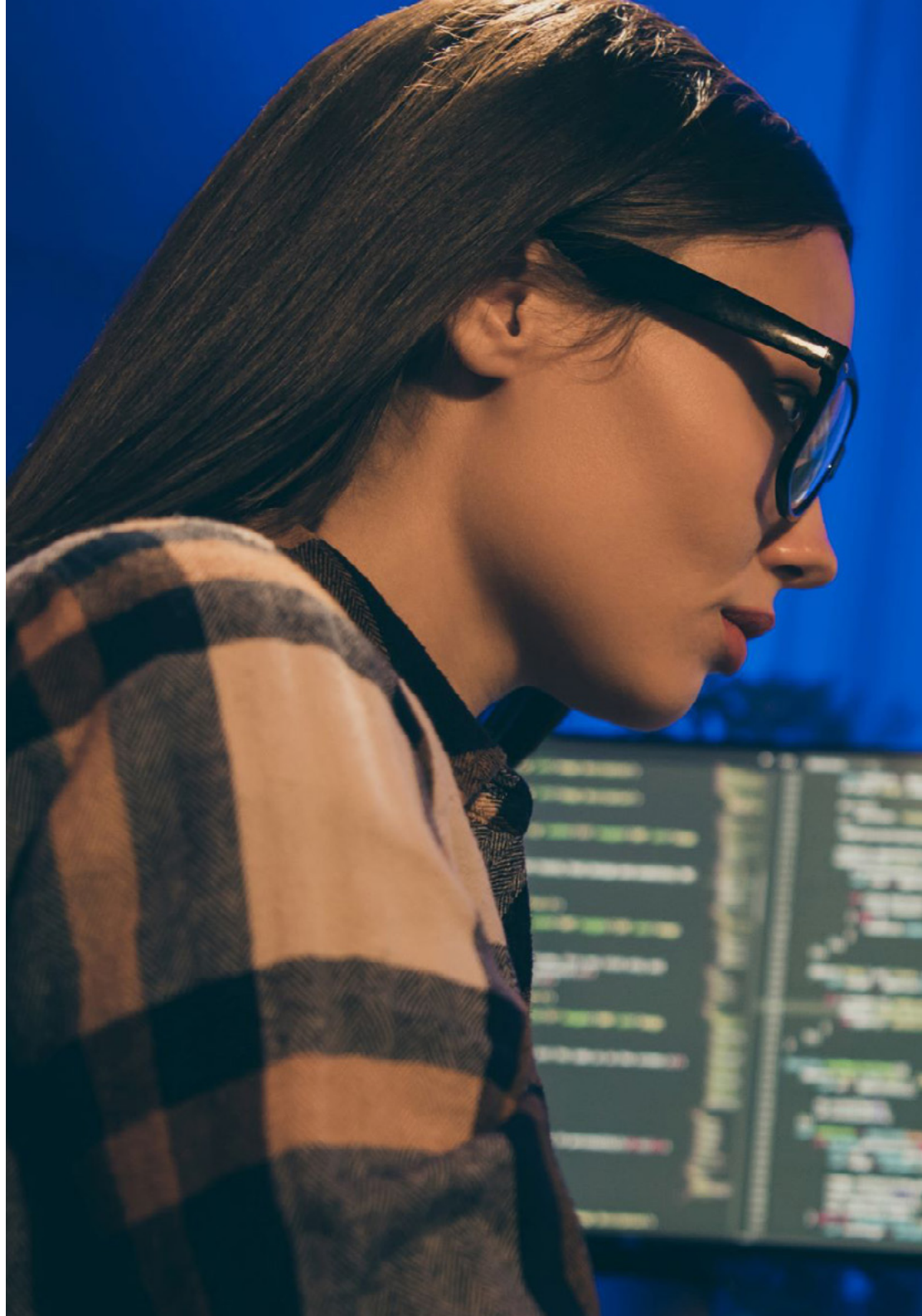
## Obiettivi generali

---

- ♦ 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

“

*La crittografia sarà essenziale per il tuo futuro professionale: iscriviti subito e preparati a ricevere importanti opportunità nel settore della sicurezza informatica”*





## Obiettivi specifici

---

- ◆ 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 pseudo-casuali
- ◆ 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

# 03

## Direzione del corso

La crittografia è un'area molto complessa, la quale richiede la migliore preparazione. L'emergere di nuovi settori tecnologici, per i quali la crittografia è un elemento fondamentale, ha favorito un grande boom in questo campo e la sua enorme difficoltà richiede l'affiancamento di specialisti per conoscerne i dettagli. Per questo TECH Global University ha riunito un prestigioso personale docente che guiderà lo studente durante l'intero processo di apprendimento, garantendo che tutti gli elementi chiave della crittografia attuale siano assimilati in modo rapido e semplice.



“

*Il personale docente di TECH Global University  
ti guiderà affinché le 150 ore di apprendimento  
di questo Corso Universitario siano efficaci e ti  
diano una spinta professionale"*

## Direzione



### Dott. Olalla Bonal, Martín

- ♦ Client Technical Specialist Blockchain in IBM
- ♦ Blockchain Technical Specialist in IBM SPGI
- ♦ Architetto *Blockchain*
- ♦ Architetto di Infrastrutture nel Settore Bancario
- ♦ Gestione di progetti e implementazione di soluzioni
- ♦ Tecnico di Elettronica Digitale
- ♦ Docente: Formazione Hyperledger Fabric per le aziende
- ♦ Docente: Formazione sulla Blockchain orientata al business nelle aziende

## Personale docente

### 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



“

*Il nostro personale docente ti fornirà  
le sue conoscenze in modo  
da mantenerti sempre aggiornato  
sulle ultime novità della disciplina”*

# 04

## Struttura e contenuti

Il Corso Universitario in Crittografia Avanzata è stato progettato per rispondere all'attuale domanda di specialisti in questa disciplina e il suo modulo specifico aiuterà il professionista ad approfondire aspetti rilevanti della sicurezza informatica come la crittografia asimmetrica, i certificati digitali, i protocolli di telefonia mobile, la protezione degli algoritmi in materia di calcolo quantistico o di distribuzione quantistica delle chiavi. Il tutto nel corso di 150 ore di apprendimento distribuite su 6 settimane.

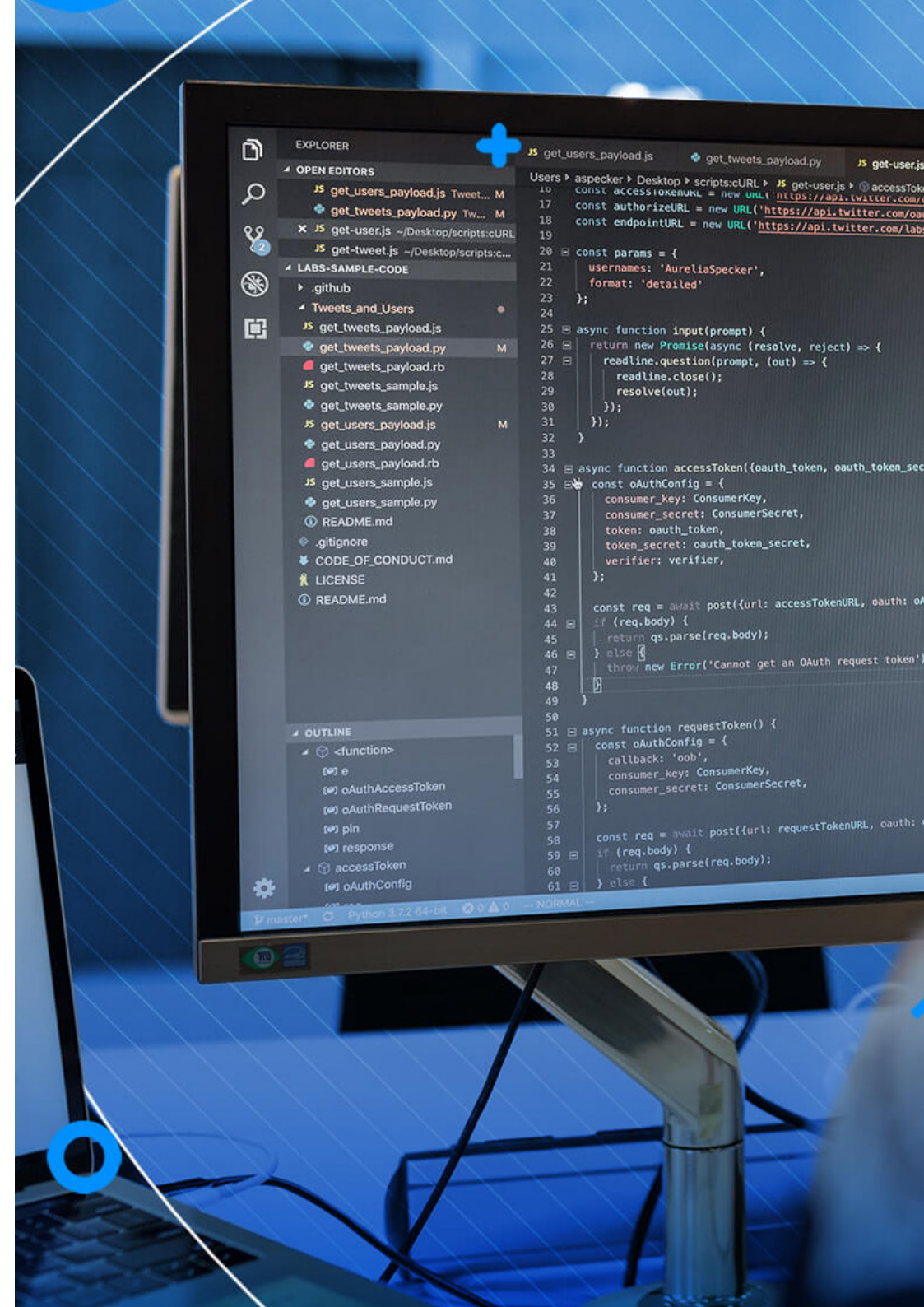


“

*Il programma più aggiornato in Crittografia Avanzata ti consentirà di conoscere tutti gli aspetti chiave della protezione degli algoritmi nel contesto del calcolo quantistico"*

## 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 esotici
- 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. Elaborazione dei dati in tempo reale
  - 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



*Questo programma ha tutto ciò che si possa desiderare: un personale docente di alto livello, una metodologia flessibile che si adegua alle esigenze del professionista e i contenuti più completi in crittografia e sicurezza informatica"*

05

# 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.



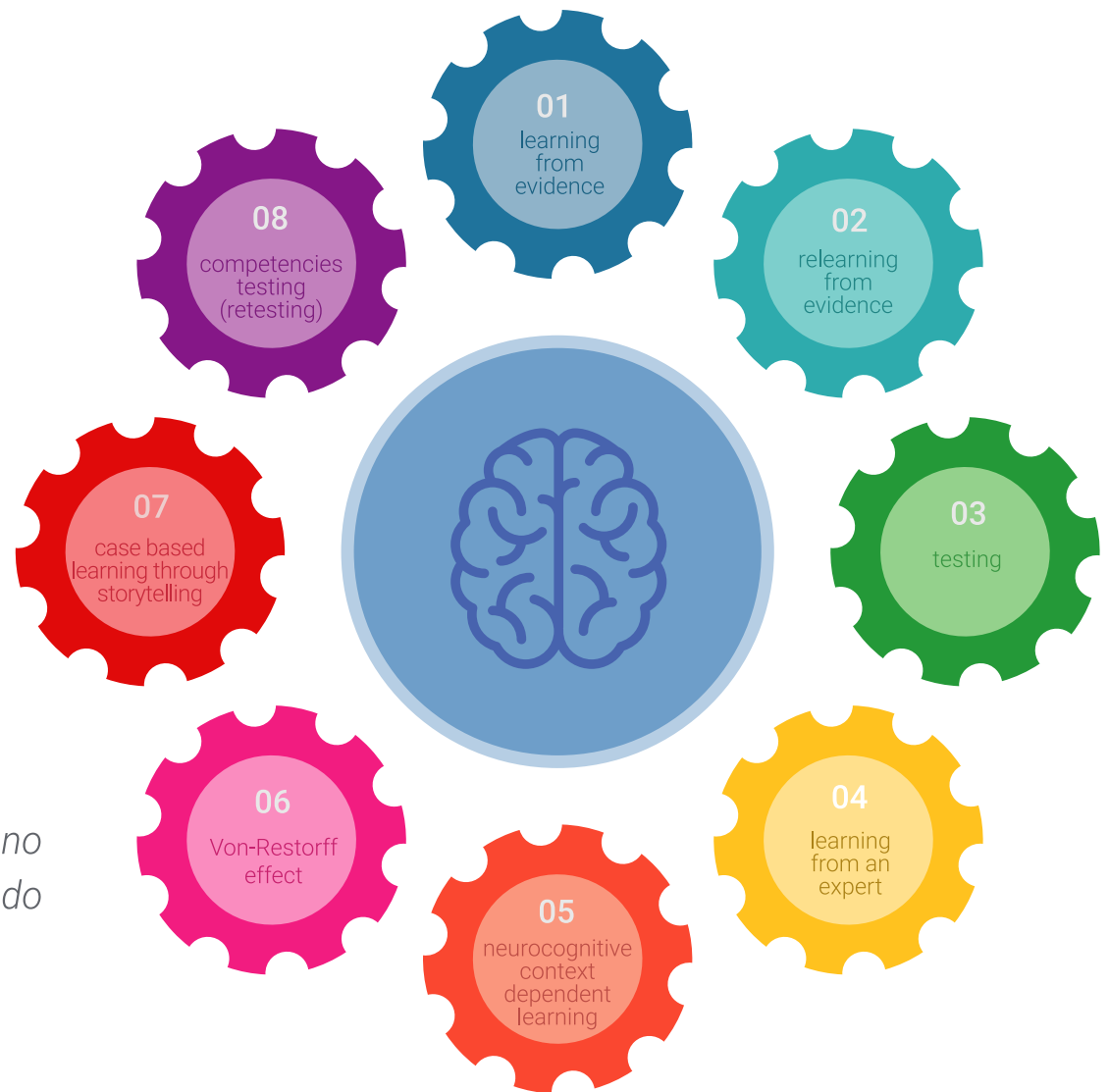
## Metodo Relearning

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.

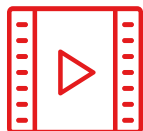
La valutazione degli studenti sulla qualità dell'insegnamento, la qualità dei materiali, la struttura del corso e i suoi obiettivi è eccellente. A questo proposito, l'istituzione è diventata la migliore università valutata dai suoi studenti secondo l'indice global score, ottenendo un 4,9 su 5

*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

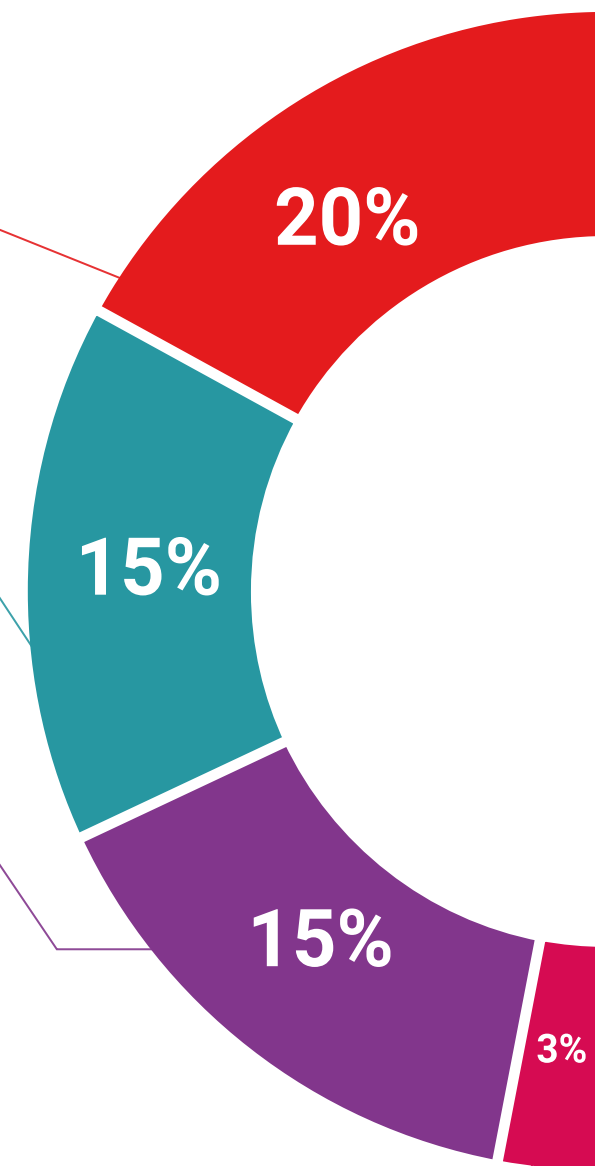
Presentiamo i contenuti in modo accattivante e dinamico tramite strumenti multimediali che includono audio, video, immagini, diagrammi e mappe concettuali per consolidare la conoscenza.

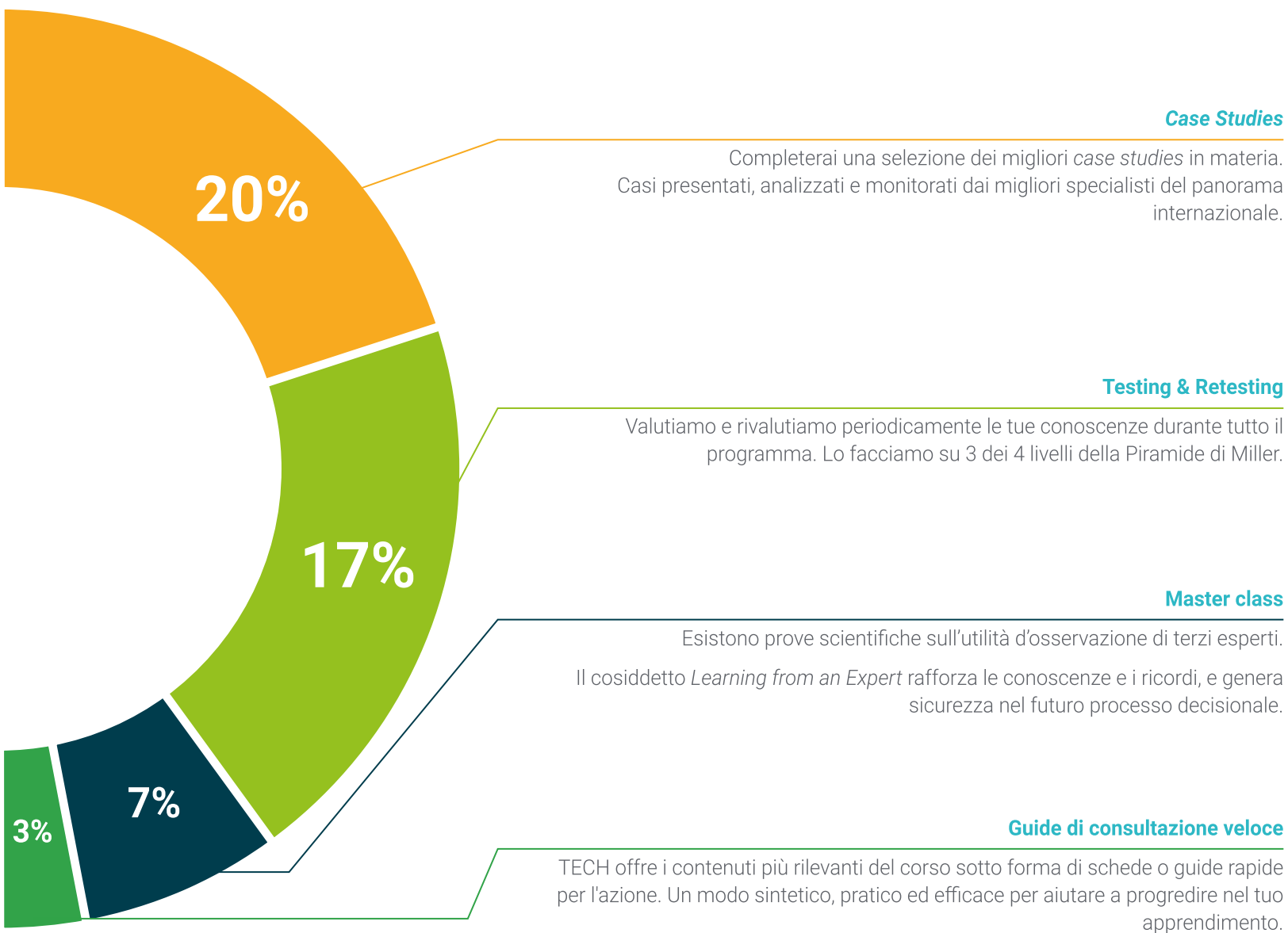
Questo esclusivo sistema di preparazione per la presentazione di contenuti multimediali è stato premiato da Microsoft come "Caso di successo in Europa".



#### Lecture 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.





# 06 Titolo

Il Corso Universitario in Crittografia Avanzata, oltre alla preparazione più rigorosa e aggiornata, il conseguimento di una qualifica di Corso 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 **Corso Universitario in Crittografia Avanzata** 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: **Corso Universitario in Crittografia Avanzata**

Modalità: **online**

Durata: **6 settimane**

Accreditamento: **6 ECTS**



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



## Corso Universitario Crittografia Avanzata

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

# Corso Universitario

## Crittografia Avanzata