

# Esperto Universitario

## Sicurezza nell'Ingegneria del Software



**tech** università  
tecnologica  
**Esperto Universitario**

## Sicurezza nell'Ingegneria del Software

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

Accesso al sito web: [www.techitute.com/it/informatica/specializzazione/specializzazione-sicurezza-ingegneria-software](http://www.techitute.com/it/informatica/specializzazione/specializzazione-sicurezza-ingegneria-software)

# Indice

01

Presentazione

---

*pag. 4*

02

Obiettivi

---

*pag. 8*

03

Direzione del corso

---

*pag. 12*

03

Struttura e contenuti

---

*pag. 16*

04

Metodologia

---

*pag. 22*

05

Titolo

---

*pag. 30*

# 01

# Presentazione

Grazie a questa preparazione lo studente imparerà come si esegue il processo di sicurezza delle informazioni, le sue implicazioni sulla riservatezza, integrità, disponibilità e costi economici, oltre a comprendere i problemi relativi alla sicurezza del software, le sue vulnerabilità e la sua classificazione.

Grazie a questo programma di alto valore scientifico, il professionista acquisirà le conoscenze necessarie a eseguire il controllo interno del computer e valutare e rilevare le vulnerabilità delle applicazioni online.





*Specializzati nei sistemi informatici con professionisti di grande esperienza nel settore"*

Questo programma completo in Sicurezza nell'Ingegneria del Software consentirà ai professionisti del settore IT di approfondire e conoscere i processi di gestione e follow up di software sicuri e di qualità che soddisfino i requisiti richiesti.

Questo Esperto Universitario permette agli studenti di specializzarsi in Sicurezza nell'Ingegneria del Software fornendo loro le conoscenze e gli strumenti necessari a progettare e controllare sistemi complessi che aiutino a risolvere gli eventuali problemi che sorgano in modo affidabile.

L'obiettivo principale di questa specializzazione è fornire allo studente gli strumenti necessari a realizzare progressi qualitativi e ad implementare soluzioni ai problemi specifici legati al software che gli si presentino. Il programma si propone inoltre di preparare i professionisti affinché utilizzino un approccio sistematico allo sviluppo e alla gestione del software e maturino conoscenze approfondite in programmazione informatica, implementazione e pianificazione dei sistemi informatici, avvalendosi di una prospettiva pratica e adattata alla realtà attuale.

Durante la specializzazione, avrà a disposizione le risorse didattiche più avanzate e l'opportunità di studiare le tematiche più approfondite della disciplina, oltre a un personale docente di altissimo livello e di grande esperienza internazionale che gli fornirà le informazioni più complete e aggiornate sui progressi e le tecniche più recenti nel campo dell'Ingegneria dei Software e dei Sistemi Informatici.

Il programma copre i principali argomenti attuali in Sicurezza in dell'Ingegneria del Software, in modo che coloro che siano in grado di padroneggiarli possano lavorare in questo campo. Si tratta di un vero e proprio strumento di apprendimento realista focalizzato su differenti tematiche di questa specializzazione, inserite in un contesto moderno e critico.

Trattandosi di un Esperto in modalità 100% online, lo studente non è condizionato da orari fissi o dalla necessità di recarsi in una sede fisica, ma può accedere ai contenuti in qualsiasi momento della giornata, conciliando la propria vita lavorativa o personale con quella accademica.

Se vuoi fare la differenza ed essere in grado di ideare e sviluppare progetti complessi di Ingegneria dei Sistemi, questo è il programma che fa per te.

Questo **Esperto Universitario in Sicurezza nell'Ingegneria del Software** possiede il programma più completo e aggiornato del mercato. Le caratteristiche principali del programma sono:

- ◆ Sviluppo di casi di studio presentati da esperti in Sicurezza nell'Ingegneria del Software
- ◆ 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 relative alla Sicurezza nell'Ingegneria del Software
- ◆ 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



*La realizzazione di questo Esperto Universitario permetterà ai professionisti della Sicurezza nell'Ingegneria del Software di essere all'avanguardia nel settore"*

“

*Questo Esperto Universitario è il miglior investimento che tu possa fare nella scelta di un programma di aggiornamento delle tue conoscenze nel campo della Sicurezza nell'Ingegneria del Software. Ti offriamo qualità e libero accesso ai contenuti”*

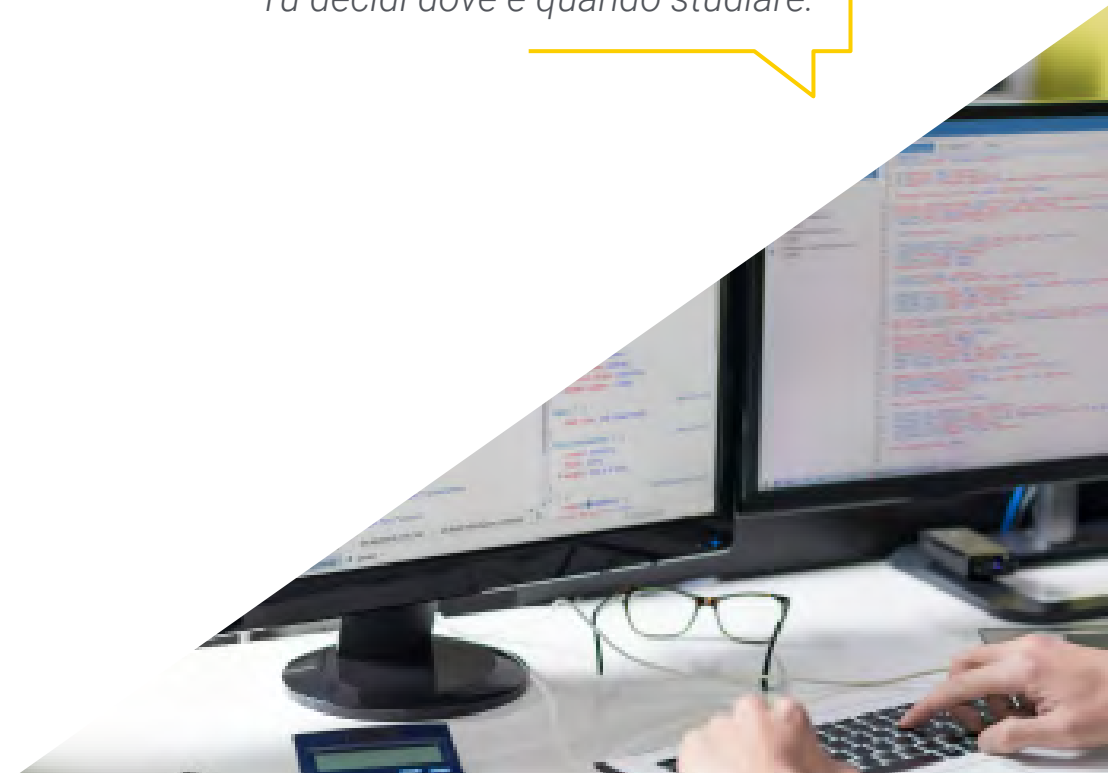
Il personale docente del programma comprende rinomati professionisti in materia di Sicurezza nell'Ingegneria del Software, nonché riconosciuti specialisti appartenenti a società scientifiche e università prestigiose, che forniscono agli studenti le competenze necessarie a intraprendere un percorso di studio eccellente.

I contenuti multimediali, sviluppati in base alle ultime tecnologie educative, forniranno al professionista un apprendimento coinvolgente e localizzato, ovvero inserito in un contesto reale.

La creazione di questo programma è incentrata sull'Apprendimento Basato su Problemi, mediante il quale lo specialista deve cercare di risolvere le diverse situazioni che gli si presentano durante il corso. Lo studente potrà usufruire di un innovativo sistema di video interattivi creati da esperti di rinomata fama in Sicurezza nell'Ingegneria del Software, che vantano un'ampia esperienza di insegnamento.

*Questa specializzazione raccoglie i migliori materiali didattici, il che ti permetterà uno studio contestuale che faciliterà l'apprendimento.*

*Questo Esperto Universitario in modalità 100% online ti permetterà di conciliare gli studi con la tua attività professionale. Tu decidi dove e quando studiare.*



# 02 Obiettivi

Il programma in Sicurezza nell'Ingegneria del Software ha l'obiettivo di facilitare le prestazioni del professionista affinché possa acquisire e conoscere le principali novità del settore, che gli consentiranno di esercitare la propria professione con la massima qualità e professionalità.







“

*Il nostro obiettivo è farti diventare il miglior professionista del tuo settore. Per questo abbiamo a disposizione la metodologia e i contenuti migliori”*



## Obiettivi generali

---

- ◆ Acquisire nuove conoscenze in materia di Sicurezza nell'ingegneria del Software
- ◆ Acquisire nuove competenze in termini di nuove tecnologie e di ultimi sviluppi nel settore software
- ◆ Elaborare i dati generati dalle attività di Ingegneria del Software

“

*Migliorare le tue competenze nell'ambito della Sicurezza nell'Ingegneria del Software ti permetterà di essere più competitivo. Continua a specializzarti e dai una svolta alla tua carriera”*





## Obiettivi specifici

---

### Modulo 1. Gestione della sicurezza

- ◆ Comprendere il processo di sicurezza delle informazioni, le sue implicazioni in termini di riservatezza, integrità, disponibilità e costi economici
- ◆ Apprendere l'uso di buone pratiche di sicurezza nella gestione dei servizi informatici
- ◆ Acquisire le conoscenze per una corretta certificazione dei processi di sicurezza
- ◆ Comprendere i meccanismi e i metodi di autenticazione per il controllo degli accessi, nonché il processo di verifica degli accessi
- ◆ Comprendere i programmi di gestione della sicurezza, la gestione del rischio e la progettazione delle politiche di sicurezza
- ◆ Imparare a conoscere i piani di continuità aziendale, le loro fasi e il processo di manutenzione
- ◆ Conoscere le procedure per la corretta protezione dell'azienda attraverso reti DMZ, l'utilizzo di sistemi di rilevamento dell'intruso e altre metodologie

### Modulo 2. Sicurezza del Software

- ◆ Comprendere i problemi di sicurezza del software, le vulnerabilità e la loro classificazione
- ◆ Conoscere i principi di progettazione, le metodologie e gli standard di sicurezza del software
- ◆ Comprendere l'applicazione della sicurezza nelle diverse fasi del ciclo di vita del software
- ◆ Acquisire le conoscenze necessarie per la codifica sicura del software e le tecniche di validazione
- ◆ Assimilare metodologie e processi per garantire la sicurezza durante lo sviluppo e l'erogazione di servizi cloud
- ◆ Comprendere le basi della crittologia e le diverse tecniche di crittografia oggi esistenti

### Modulo 3. Audit sulla Sicurezza

- ◆ Acquisire le conoscenze necessarie per la corretta esecuzione del processo di audit e di controllo interno dell'IT
- ◆ Comprendere i processi da eseguire per l'audit di sicurezza di sistemi e reti
- ◆ Comprendere i diversi strumenti di supporto, le metodologie e le successive analisi durante l'audit della sicurezza di Internet e dei dispositivi mobili
- ◆ Apprendere le proprietà e i fattori di influenza che condizionano i rischi aziendali e determinare la corretta implementazione di un'adeguata gestione del rischio
- ◆ Conoscere le misure di mitigazione del rischio, nonché le metodologie di implementazione di un Sistema di Gestione della Sicurezza delle Informazioni e le normative e gli standard da utilizzare
- ◆ Comprendere le procedure per condurre l'audit di sicurezza, la sua tracciabilità e la presentazione dei risultati

### Modulo 4. Sicurezza nelle Applicazioni Online

- ◆ Acquisire le conoscenze necessarie per valutare e rilevare le vulnerabilità nelle applicazioni online
- ◆ Comprendere le politiche e gli standard di sicurezza da applicare alle applicazioni online
- ◆ Conoscere le procedure da utilizzare durante lo sviluppo di applicazioni web e la loro successiva validazione attraverso analisi e test di sicurezza
- ◆ Conoscere le misure di sicurezza per l'implementazione e la produzione di applicazioni web
- ◆ Comprendere i concetti, le funzioni e le tecnologie da applicare alla sicurezza dei servizi web, nonché i test di sicurezza e le misure di protezione
- ◆ Assimilare le procedure di Hacking etico, analisi del malware e forense
- ◆ Conoscere le misure di mitigazione e contenimento degli incidenti sui servizi web
- ◆ Acquisire le conoscenze per l'implementazione delle tecniche di best practice per lo sviluppo e l'implementazione di applicazioni online, nonché gli errori più comuni

# 03

## Direzione del corso

Questo programma accademico dispone del personale docente più specializzato dell'attuale mercato educativo. Si tratta di specialisti selezionati da TECH per sviluppare l'intero percorso educativo. In questo modo, basandosi sulla propria esperienza e sulle ultime evidenze, hanno progettato i contenuti più aggiornati che offrono garanzia di qualità in una materia così rilevante.



“

*TECH mette a tua disposizione il personale docente più specializzato nell'area di studio. Iscriviti subito e approfitta della qualità che ti meriti”*



## Direttore Ospite Internazionale

Darren Pulsipher è un architetto di software di grande esperienza, un innovatore con un notevole background internazionale nello sviluppo di software e firmware. In effetti, possiede competenze altamente sviluppate in comunicazione, gestione di progetti e affari, che gli hanno permesso di guidare importanti iniziative a livello globale.

Ha inoltre ricoperto incarichi di alto livello nel corso della sua carriera, come Architetto Capo delle Soluzioni per il Settore Pubblico presso Intel, dove ha promosso attività, processi e tecnologie moderne per clienti, partner e utenti del settore pubblico. Inoltre, ha fondato Yoly Inc., dove ha anche ricoperto il ruolo di CEO, lavorando per sviluppare uno strumento di aggregazione e diagnosi dei social media basato sul Software as a Service (SaaS), utilizzando tecnologie Big Data e Web 2.0.

Inoltre, ha lavorato in altre società, come senior engineering director presso Dell Technologies, dove ha diretto la Business Unit Big Data Cloud, guidando i team negli Stati Uniti e in Cina per la gestione di grandi progetti e la ristrutturazione delle divisioni aziendali per la loro integrazione di successo. Ha anche lavorato come Chief Information Officer presso XanGo, dove ha gestito progetti come il supporto Help Desk, il supporto alla produzione e lo sviluppo di soluzioni.

Tra le molteplici specializzazioni in cui è esperto, spiccano la tecnologia Edge to Cloud, la sicurezza informatica, l'intelligenza artificiale generativa, lo sviluppo software, la tecnologia di rete, lo sviluppo nativo nel cloud e l'ecosistema dei container. Conoscenze che ha condiviso attraverso il podcast e la newsletter settimanale "Embracing Digital Transformation", che ha prodotto e presentato, aiutando le organizzazioni a navigare con successo nella trasformazione digitale sfruttando le persone, i processi e la tecnologia.



## Dott. Pulsipher, Darren

---

- Architetto Capo delle Soluzioni per il Settore Pubblico presso Intel, California, USA
- Presentatore e produttore di "Embracing Digital Transformation", California
- Fondatore e CEO di Yoly Inc., Arkansas
- Senior Engineering Director presso Dell Technologies, Arkansas
- Chief Information Officer presso XanGo, Utah
- Architetto senior in Cadence Design Systems, California
- Senior Manager dei processi di progetto presso Lucent Technologies, California
- Ingegnere del software a Cemax-Icon, California
- Ingegnere del software presso ISG Technologies, Canada
- MBA in gestione della tecnologia presso l'Università di Phoenix
- Laurea in informatica e ingegneria elettrica presso la Brigham Young University

“

*Grazie a TECH potrai  
apprendere con i migliori  
professionisti del mondo”*

# 03

## Struttura e contenuti

La struttura dei contenuti è stata ideata dai migliori esperti del settore della Sicurezza nell'Ingegneria del Software, con una vasta esperienza e un riconosciuto prestigio nella professione, e consapevoli dei vantaggi che le più recenti tecnologie educative possono apportare nel campo dell'istruzione superiore.





“

*Disponiamo del programma scientifico più completo e aggiornato del mercato. Puntiamo all'eccellenza e a darti gli strumenti affinché anche tu possa raggiungerla”*

## Modulo 1. Gestione della Sicurezza

- 1.1. Sicurezza delle informazioni
  - 1.1.1. Introduzione
  - 1.1.2. La sicurezza delle informazioni implica riservatezza, integrità e disponibilità.
  - 1.1.3. La sicurezza è una questione economica
  - 1.1.4. La sicurezza è un processo
  - 1.1.5. Classificazione delle informazioni
  - 1.1.6. La sicurezza delle informazioni comporta la gestione del rischio
  - 1.1.7. La sicurezza si articola con i controlli di sicurezza
  - 1.1.8. La sicurezza è sia fisica che logica
  - 1.1.9. La sicurezza coinvolge le persone
- 1.2. Il professionista della sicurezza informatica
  - 1.2.1. Introduzione
  - 1.2.2. Sicurezza delle informazioni come professione
  - 1.2.3. Certificazioni (ISC)2
  - 1.2.4. Standard ISO 27001
  - 1.2.5. Buone pratiche di sicurezza nella gestione dei servizi IT
  - 1.2.6. Modelli di gestione della sicurezza delle informazioni
  - 1.2.7. Altre certificazioni, standard e risorse professionali
- 1.3. Controlli di accesso
  - 1.3.1. Introduzione
  - 1.3.2. Requisiti per il controllo degli accessi
  - 1.3.3. Meccanismi di autenticazione
  - 1.3.4. Metodi di autorizzazione
  - 1.3.5. Contabilità e revisione degli accessi
  - 1.3.6. Tecnologie «Tripla A»
- 1.4. Programmi, processi e politiche di sicurezza delle informazioni
  - 1.4.1. Introduzione
  - 1.4.2. Programmi di gestione della sicurezza
  - 1.4.3. Gestione dei rischi
  - 1.4.4. Progettazione della politica di sicurezza
- 1.5. Piano di continuità di un business
  - 1.5.1. Introduzione ai BCP
  - 1.5.2. Fase I e II
  - 1.5.3. Fase III e IV
  - 1.5.4. Manutenzione del BCP
- 1.6. Procedure per la corretta protezione dell'azienda
  - 1.6.1. Reti DMZ
  - 1.6.2. Sistemi di rilevamento delle intrusioni
  - 1.6.3. Requisiti per il controllo degli accessi
  - 1.6.4. Imparare dall'attaccante: *Honeypot*
- 1.7. Architettura di sicurezza. Prevenzione
  - 1.7.1. Visione generale. Attività e modello a strati
  - 1.7.2. Difesa perimetrale (*firewall*, WAF, IPS, ecc..)
  - 1.7.3. Difesa degli endpoint (apparecchiature, server e servizi)
- 1.8. Architettura di sicurezza. Screening
  - 1.8.1. Rilevamento e monitoraggio della panoramica
  - 1.8.2. *Log*, interruzione del traffico crittografato, registrazione e *Siem*
  - 1.8.3. Allarmi e intelligence
- 1.9. Architettura di sicurezza. Reazione
  - 1.9.1. Reazione. Prodotti, servizi e risorse
  - 1.9.2. Gestione degli incidenti
  - 1.9.3. CERT e CSIRT
- 1.10. Architettura di sicurezza. Recupero
  - 1.10.1. Resilienza, concetti, requisiti aziendali e standard
  - 1.10.2. Soluzioni IT di Resilienza
  - 1.10.3. Gestione della crisi e Governance

## Modulo 2. Sicurezza nel Software

- 2.1. Problemi di sicurezza del software
  - 2.1.1. Introduzione ai problemi di sicurezza del software
  - 2.1.2. Vulnerabilità e loro classificazione
  - 2.1.3. Proprietà di un software sicuro
  - 2.1.4. Riferimenti
- 2.2. Principi di progettazione per la sicurezza del software
  - 2.2.1. Introduzione
  - 2.2.2. Principi di progettazione per la sicurezza del software
  - 2.2.3. Tipi di S-SDLC
  - 2.2.4. Sicurezza del software nelle fasi S-SDLC
  - 2.2.5. Metodologie e standard
  - 2.2.6. Riferimenti
- 2.3. Sicurezza del ciclo di vita del software nelle fasi dei requisiti e di progettazione
  - 2.3.1. Introduzione
  - 2.3.2. Modellazione degli attacchi
  - 2.3.3. Casi di abuso
  - 2.3.4. Ingegneria dei requisiti di sicurezza
  - 2.3.5. Analisi dei rischi. Architettonici
  - 2.3.6. Modelli di design
  - 2.3.7. Riferimenti
- 2.4. Sicurezza del ciclo di vita del software nelle fasi di test, operazione e codificazione
  - 2.4.1. Introduzione
  - 2.4.2. Test di sicurezza basati sul rischio
  - 2.4.3. Revisione del codice
  - 2.4.4. Test di penetrazione
  - 2.4.5. Operazioni di sicurezza
  - 2.4.6. Revisione esterna
  - 2.4.7. Riferimenti
- 2.5. Codifica sicura applicazioni I
  - 2.5.1. Introduzione
  - 2.5.2. Pratiche di codifica sicure
  - 2.5.3. Gestione e convalida delle voci
  - 2.5.4. Overflow di memoria
  - 2.5.5. Riferimenti
- 2.6. Codifica sicura applicazioni II
  - 2.6.1. Introduzione
  - 2.6.2. *Integers Overflows*, errori di troncamento e problemi con le conversioni di tipo tra numeri interi
  - 2.6.3. Errori ed eccezioni
  - 2.6.4. Privacy e riservatezza
  - 2.6.5. Programmi privilegiati
  - 2.6.6. Riferimenti
- 2.7. Sicurezza nello sviluppo e nel cloud
  - 2.7.1. Sicurezza nello sviluppo: metodologia e pratica
  - 2.7.2. Modelli PaaS, IaaS, CaaS e SaaS
  - 2.7.3. Sicurezza nel cloud e per i servizi Cloud
- 2.8. Crittografia
  - 2.8.1. Fondamenti di Crittologia
  - 2.8.2. Crittografia simmetrica e asimmetrica
  - 2.8.3. Crittografia a riposo e in transito
- 2.9. Orchestrazione e automazione della sicurezza (SOAR)
  - 2.9.1. Complessità dell'elaborazione manuale; necessità di automatizzare le attività
  - 2.9.2. Prodotti e servizi
  - 2.9.3. Architettura SOAR
- 2.10. Sicurezza del telelavoro
  - 2.10.1. Necessità e scenari
  - 2.10.2. Prodotti e servizi
  - 2.10.3. Sicurezza del telelavoro

### Modulo 3. Audit sulla Sicurezza

- 3.1. Introduzione ai sistemi informativi e al loro audit
  - 3.1.1. Introduzione ai sistemi informativi e al ruolo dell'audit informatico
  - 3.1.2. Definizioni di "Audit IT" e "controllo interno IT"
  - 3.1.3. Funzioni e obiettivi dell'audit IT
  - 3.1.4. Differenze tra controllo interno e audit IT
- 3.2. Controlli interni dei Sistemi Informatici
  - 3.2.1. Organigramma funzionale di un centro di elaborazione dati
  - 3.2.2. Classificazione dei controlli dei sistemi informativi
  - 3.2.3. La Regola d'Oro
- 3.3. Il processo e le fasi dell'audit dei Sistemi Informatici
  - 3.3.1. Valutazione del rischio e altre metodologie di audit IT
  - 3.3.2. Esecuzione di un audit dei sistemi informativi. Fasi di audit
  - 3.3.3. Competenze fondamentali dell'audit dei sistemi informativi
- 3.4. Audit tecnico di sicurezza di sistemi e reti
  - 3.4.1. Audit tecnici di sicurezza. Test di intrusione. Concetti preliminari
  - 3.4.2. Audit di sicurezza del sistema. Strumenti di supporto
  - 3.4.3. Audit di sicurezza delle reti. Strumenti di supporto
- 3.5. Audit tecnico di sicurezza di internet e dispositivi mobili
  - 3.5.1. Audit di sicurezza di internet. Strumenti di supporto
  - 3.5.2. Audit di sicurezza di dispositivi mobili. Strumenti di supporto
  - 3.5.3. Allegato 1. Struttura della relazione esecutiva e della relazione tecnica
  - 3.5.4. Allegato 2. Inventario degli strumenti
  - 3.5.5. Allegato 3. Metodologie
- 3.6. Sistema di gestione di sicurezza delle informazioni
  - 3.6.1. Sicurezza IS: proprietà e fattori di influenza
  - 3.6.2. Rischio d'impresa e gestione del rischio: implementazione dei controlli
  - 3.6.3. Sistema di gestione della sicurezza delle informazioni (ISMS): concetto e fattori critici di successo
  - 3.6.4. ISMS-Modello PDCA
  - 3.6.5. ISMS ISO-IEC 27001: contesto organizzativo
  - 3.6.6. Paragrafo 4. Contesto organizzativo
  - 3.6.7. Paragrafo 5. Leadership
  - 3.6.8. Paragrafo 6. Pianificazione
  - 3.6.9. Paragrafo 7. Supporto
  - 3.6.10. Paragrafo 8. Operazione
  - 3.6.11. Paragrafo 9. Valutazione delle prestazioni
  - 3.6.12. Paragrafo 10. Miglioramento
  - 3.6.13. Allegato alla ISO 27001/ISO-IEC 27002: obiettivi e controlli
  - 3.6.14. Audit ISMS
- 3.7. Conduzione dell'audit
  - 3.7.1. Procedure
  - 3.7.2. Tecniche
- 3.8. Tracciabilità
  - 3.8.1. Metodologie
  - 3.8.2. Analisi
- 3.9. Custodia
  - 3.9.1. Tecniche
  - 3.9.2. Risultati
- 3.10. Relazioni e presentazione delle prove
  - 3.10.1. Tipi di rapporti
  - 3.10.2. Analisi dei dati
  - 3.10.3. Presentazione delle prove

## Modulo 4. Sicurezza nelle applicazioni online

- 4.1. Vulnerabilità e problemi di sicurezza nelle applicazioni online
  - 4.1.1. Introduzione alla sicurezza delle applicazioni online
  - 4.1.2. Vulnerabilità di sicurezza nella progettazione di applicazioni web
  - 4.1.3. Vulnerabilità di sicurezza nell'implementazione di applicazioni web
  - 4.1.4. Vulnerabilità di sicurezza nel deployment di applicazioni web
  - 4.1.5. Elenchi ufficiali di vulnerabilità di sicurezza
- 4.2. Politiche e standard per la sicurezza delle applicazioni online
  - 4.2.1. Fondamenti sicurezza delle applicazioni online
  - 4.2.2. Politiche di sicurezza
  - 4.2.3. Sistema di gestione di sicurezza delle informazioni
  - 4.2.4. Cicli di vita dello sviluppo sicuro del software
  - 4.2.5. Standard di sicurezza delle applicazioni
- 4.3. Sicurezza nella progettazione di applicazioni web
  - 4.3.1. Introduzione alla sicurezza delle applicazioni web
  - 4.3.2. Sicurezza nella progettazione di applicazioni web
- 4.4. Test di sicurezza e protezione online di applicazioni web
  - 4.4.1. Analisi e test di sicurezza delle applicazioni web
  - 4.4.2. Sicurezza del deployment e produzione di applicazioni web
- 4.5. Sicurezza dei servizi web
  - 4.5.1. Introduzione alla sicurezza dei servizi web
  - 4.5.2. Funzioni e tecnologia di sicurezza dei servizi web
- 4.6. Test di sicurezza e protezione online dei servizi web
  - 4.6.1. Valutazione di sicurezza dei servizi web
  - 4.6.2. Protezione online. Firewalls e Gateways XML
- 4.7. Hacking etico, malware e forensic
  - 4.7.1. *Hacking* etico
  - 4.7.2. Analisi del *Malware*
  - 4.7.3. Analisi Forense
- 4.8. Risoluzione degli imprevisti per i servizi web
  - 4.8.1. Monitoraggio
  - 4.8.2. Strumenti di misurazione delle performance
  - 4.8.3. Misure di contenimento
  - 4.8.4. Analisi delle cause principali
  - 4.8.5. Gestione proattiva dei problemi
- 4.9. Pratiche corrette per garantire la sicurezza delle applicazioni
  - 4.9.1. Manuale di pratiche corrette per lo sviluppo di applicazioni online
  - 4.9.2. Manuale di buone pratiche nell'implementazione di applicazioni online
- 4.10. Errori comuni che minano la sicurezza delle applicazioni
  - 4.10.1. Errori comuni nello sviluppo
  - 4.10.2. Errori comuni nel hosting
  - 4.10.3. Errori comuni nella produzione



*Un programma didattico completo e multidisciplinare che ti permetterà di eccellere nella tua carriera, seguendo gli ultimi progressi relativi alle Risorse Idriche e alla Sostenibilità Idrica Urbana”*

# 04

# Metodologia

Questo programma ti offre un modo differente di imparare. La nostra metodologia si sviluppa in una modalità di apprendimento ciclico: ***il Relearning***.

Questo sistema di insegnamento viene applicato nelle più prestigiose facoltà di medicina del mondo ed è considerato uno dei più efficaci da importanti pubblicazioni come il ***New England Journal of Medicine***.



“

*Scopri il Relearning, un sistema che abbandona l'apprendimento lineare convenzionale, per guidarti attraverso dei sistemi di insegnamento ciclici: una modalità di apprendimento che ha dimostrato la sua enorme efficacia, soprattutto nelle materie che richiedono la memorizzazione”*

## Caso di Studio per contestualizzare tutti i contenuti

Il nostro programma offre un metodo rivoluzionario per sviluppare le abilità e le conoscenze. Il nostro obiettivo è quello di rafforzare le competenze in un contesto mutevole, competitivo e altamente esigente.

“

*Con TECH potrai sperimentare un modo di imparare che sta scuotendo le fondamenta delle università tradizionali in tutto il mondo”*



*Avrai accesso a un sistema di apprendimento basato sulla ripetizione, con un insegnamento naturale e progressivo durante tutto il programma.*





*Imparerai, attraverso attività collaborative e casi reali, la risoluzione di situazioni complesse in ambienti aziendali reali.*

## Un metodo di apprendimento innovativo e differente

Questo programma di TECH consiste in un insegnamento intensivo, creato ex novo, che propone le sfide e le decisioni più impegnative in questo campo, sia a livello nazionale che internazionale. Grazie a questa metodologia, la crescita personale e professionale viene potenziata, effettuando un passo decisivo verso il successo. Il metodo casistico, la tecnica che sta alla base di questi contenuti, garantisce il rispetto della realtà economica, sociale e professionale più attuali.

“ *Il nostro programma ti prepara ad affrontare nuove sfide in ambienti incerti e a raggiungere il successo nella tua carriera* ”

Il Metodo Casistico è stato il sistema di apprendimento più usato nelle migliori Scuole di Informatica del mondo da quando esistono. Sviluppato nel 1912 affinché gli studenti di Diritto non imparassero la legge solo sulla base del contenuto teorico, il metodo casistico consisteva nel presentare loro situazioni reali e complesse per prendere decisioni informate e giudizi di valore su come risolverle. Nel 1924 fu stabilito come metodo di insegnamento standard ad Harvard.

Cosa dovrebbe fare un professionista per affrontare una determinata situazione?

Questa è la domanda con cui ti confrontiamo nel metodo dei casi, un metodo di apprendimento orientato all'azione. Durante il corso, gli studenti si confronteranno con diversi casi di vita reale. Dovranno integrare tutte le loro conoscenze, effettuare ricerche, argomentare e difendere le proprie idee e decisioni.

## Metodologia Relearning

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

Potenziamo il Caso di Studio con il miglior metodo di insegnamento 100% online: il Relearning.

*Nel 2019 abbiamo ottenuto i migliori risultati di apprendimento di tutte le università online del mondo.*

In TECH imparerai con una metodologia all'avanguardia progettata per formare i manager del futuro. Questo metodo, all'avanguardia della pedagogia mondiale, si chiama Relearning.

La nostra università è l'unica autorizzata a utilizzare questo metodo di successo. Nel 2019, siamo riusciti a migliorare il livello di soddisfazione generale dei nostri studenti (qualità dell'insegnamento, qualità dei materiali, struttura del corso, obiettivi...) rispetto agli indicatori della migliore università online.



Nel nostro programma, l'apprendimento non è un processo lineare, ma avviene in una spirale (impariamo, disimpariamo, dimentichiamo e re-impariamo). Pertanto, combiniamo ciascuno di questi elementi in modo concentrico. Questa metodologia ha formato più di 650.000 laureati con un successo senza precedenti in campi diversi come la biochimica, la genetica, la chirurgia, il diritto internazionale, le competenze manageriali, le scienze sportive, la filosofia, il diritto, l'ingegneria, il giornalismo, la storia, i mercati e gli strumenti finanziari. Tutto questo in un ambiente molto esigente, con un corpo di studenti universitari con un alto profilo socio-economico e un'età media di 43,5 anni.

*Il Relearning ti permetterà di apprendere con meno sforzo e più performance, impegnandoti maggiormente nella tua specializzazione, sviluppando uno spirito critico, difendendo gli argomenti e contrastando le opinioni: un'equazione diretta al successo.*

Dalle ultime evidenze scientifiche nel campo delle neuroscienze, non solo sappiamo come organizzare le informazioni, le idee, le immagini e i ricordi, ma sappiamo che il luogo e il contesto in cui abbiamo imparato qualcosa è fondamentale per la nostra capacità di ricordarlo e immagazzinarlo nell'ippocampo, per conservarlo nella nostra memoria a lungo termine.

In questo modo, e in quello che si chiama Neurocognitive Context-dependent E-learning, i diversi elementi del nostro programma sono collegati al contesto in cui il partecipante sviluppa la sua pratica professionale.



Questo programma offre i migliori materiali didattici, preparati appositamente per i professionisti:



### Materiali di studio

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

Questi contenuti sono poi applicati al formato audiovisivo che supporterà la modalità di lavoro online di TECH. Tutto questo, con le ultime tecniche che offrono componenti di alta qualità in ognuno dei materiali che vengono messi a disposizione dello studente.



### Master class

Esistono evidenze scientifiche sull'utilità dell'osservazione di esperti terzi.

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



### Pratiche di competenze e competenze

Svolgerai attività per sviluppare competenze e capacità specifiche in ogni area tematica. Pratiche e dinamiche per acquisire e sviluppare le competenze e le abilità che uno specialista deve sviluppare nel quadro della globalizzazione in cui viviamo.



### Letture complementari

Articoli recenti, documenti di consenso e linee guida internazionali, tra gli altri. Nella biblioteca virtuale di TECH potrai accedere a tutto il materiale necessario per completare la tua specializzazione.





#### Casi di Studio

Completerai una selezione dei migliori casi di studio scelti appositamente per questo corso. Casi presentati, analizzati e monitorati dai migliori specialisti del panorama internazionale.



#### Riepiloghi interattivi

Il team di TECH presenta i contenuti in modo accattivante e dinamico in pillole multimediali che includono audio, video, immagini, diagrammi e mappe concettuali per consolidare la conoscenza.

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



#### Testing & Retesting

Valutiamo e rivalutiamo periodicamente le tue conoscenze durante tutto il programma con attività ed esercizi di valutazione e autovalutazione, affinché tu possa verificare come raggiungi progressivamente i tuoi obiettivi.



# 05 Titolo

L'Esperto Universitario in Sicurezza nell'Ingegneria del Software ti garantisce, oltre alla preparazione più rigorosa e aggiornata, l'accesso a una qualifica di Esperto Universitario rilasciata da TECH Università Tecnologica.



“

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

Questo **Esperto Universitario in Sicurezza nell'Ingegneria del Software** possiede il programma più completo e aggiornato del mercato.

Dopo aver superato la valutazione, lo studente riceverà mediante lettera certificata\* con ricevuta di ritorno, la sua corrispondente qualifica di **Esperto Universitario** rilasciata da **TECH Università Tecnologica**.

Il titolo rilasciato da **TECH Università Tecnologica** esprime la qualifica ottenuta nell'Esperto Universitario, e riunisce tutti i requisiti comunemente richiesti da borse di lavoro, concorsi e commissioni di valutazione di carriere professionali.

Titolo: **Esperto Universitario in Sicurezza nell'Ingegneria del Software**

N° Ore Ufficiali: **600 o.**



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



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

**tech** università  
tecnologica

**Esperto Universitario**  
Sicurezza nell'Ingegneria  
del Software

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

Esperto Universitario

Sicurezza nell'Ingegneria del Software