Master Specialistico

Secure Information Management

tech global university

tech global university

Master Specialistico
Secure Information Management

- Modalità: **online**
- Durata: **2 anni**
- Titolo: **TECH Global University**
- Accreditamento: **120 ECTS**
- Orario: **a tua scelta**
- Esami: **online**

Accesso al sito web: www.techtitute.com/it/informatica/master-specialistico/master-specialistico-secure-information-management

Indice

01

Presentazione del programma

Nell'attuale era digitale, le attività di diversi settori sono gestite in modo integrato attraverso internet. L'intrattenimento, il lavoro e la comunicazione con amici e familiari dipendono sempre più da strumenti e risorse online. Ogni giorno vengono trasferite enormi quantità di informazioni, da semplici dati nelle conversazioni sui social media e nelle app di messaggistica a informazioni personali e professionali sensibili ospitate su piattaforme bancarie o aziendali. Questo panorama richiede specialisti in grado di gestire e proteggere le informazioni in diversi contesti, dando la priorità alla loro sicurezza. È per questo che TECH ha progettato questo programma in Ingegneria del Software, focalizzato sulla formazione di professionisti con le competenze necessarie per gestire e proteggere le informazioni in modo efficace, affrontare le attuali sfide digitali e contribuire a creare ambienti tecnologici più sicuri e affidabili.

La protezione dei dati è fondamentale per affrontare le minacce continue. Potresti essere il custode di quelle preziose informazioni"

Ogni secondo, migliaia di dati vengono generati, condivisi e memorizzati nell'ambiente digitale. Dai pagamenti online e l'accesso ai servizi educativi al coordinamento delle attività aziendali o alla protezione delle identità digitali, la tecnologia è diventata un pilastro fondamentale che trasforma continuamente il modo in cui viviamo e lavoriamo. Queste interazioni generano e trasferiscono enormi quantità di dati in qualsiasi momento, dalle informazioni personali ai file sensibili relativi a aziende e istituzioni. Questo flusso costante di dati mette in risalto la necessità di una gestione adeguata per garantire la loro sicurezza e privacy.

Gestire e proteggere questi dati non è un compito semplice, poiché richiede una combinazione di competenze altamente specializzate in settori quali la sicurezza informatica e la gestione delle informazioni. Queste discipline, sebbene distinte, devono integrarsi per affrontare le complesse sfide dell'attuale ambiente digitale. In questo contesto, il Master Specialistico in Secure Information Management rappresenta un'opportunità unica per ingegneri e informatici interessati ad acquisire una visione globale che consenta loro di padroneggiare entrambe le aree e posizionarsi come leader in un settore in costante crescita.

Molte aziende e istituzioni si trovano di fronte alla necessità di proteggere dati critici e altamente sensibili, ma non hanno esperti in grado di garantire una gestione efficace, la conservazione e il monitoraggio delle loro informazioni digitali. Per rispondere a questa domanda, TECH ha progettato un programma che combina i migliori contenuti con un personale docente con una comprovata esperienza professionale. Questo approccio assicura che gli studenti acquisiscano gli strumenti e le conoscenze necessari per eccellere nel mercato del lavoro e accedere a posizioni strategiche in organizzazioni che vogliono rafforzare la sicurezza delle informazioni.

Questo **Master Specialistico in Secure Information Management** possiede il programma più completo e aggiornato del mercato. Le sue caratteristiche principali sono:

- Sviluppo di casi di studio presentati da esperti in Secure Information Management
- 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 del Secure Information Management
- Lezioni teoriche, domande all'esperto, forum di discussione su argomenti controversi e lavoro di riflessione individuale
- Disponibilità di accesso ai contenuti da qualsiasi dispositivo fisso o portatile dotato di connessione a Internet

Acquisisci le competenze necessarie per garantire la sicurezza e gestire efficacemente i dati in un ambiente digitale competitivo"

Consolida le tue conoscenze teoriche con le numerose risorse pratiche incluse in questo Master Specialistico in Secure Information Management"

Scopri la metodologia didattica più innovativa progettata da TECH per garantire un apprendimento immersivo e contestualizzato.

Accedi a un programma 100% online che ti permette di studiare al tuo ritmo, in qualsiasi momento e da qualsiasi parte del mondo.

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 lo specialista deve cercare di risolvere le diverse situazioni che gli si presentano durante il corso. Lo studente potrà usufruire di un innovativo sistema di video interattivi creati da esperti di rinomata fama.

02

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 lavorativo del 99%. Inoltre, TECH dispone di un enorme personale docente, composto da oltre 6.000 professori di altissimo prestigio internazionale.

Studia nella più grande Università digitale del mondo. Il futuro inizia in TECH"

La migliore università online del 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

Il personale docente di TECH è composto da oltre 6.000 docenti di massimo prestigio internazionale. Professori, ricercatori e alti dirigenti multinazionali, tra cui Isaiah Covington, allenatore dei Boston Celtics; Magda Romanska, ricercatrice principale dell'Harvard MetaLAB; Ignacio Wistumba, presidente del dipartimento di patologia molecolare traslazionale dell'MD Anderson Cancer Center; 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 propri, accreditati di specialistica e di laurea nel mondo. In totale, più di 14.000 titoli universitari, in dieci lingue diverse, ci rendono la più grande istituzione educativa del mondo.

I piani di studio più completi del panorama universitario

TECH offre i programmi 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 corsi 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 al nostro accordo con la più grande lega di basket, offriamo ai nostri 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 meglio valutata al mondo nei principali portali di recesioni, 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 materiali didattici che compongono questo Master Specialistico in Secure Information Management sono stati sviluppati da un team di esperti in sicurezza informatica e gestione dei dati. In questo modo, il piano di studi approfondisce le principali minacce digitali e le metodologie più avanzate per la protezione e la gestione delle informazioni. Ciò consentirà agli studenti di identificare rischi specifici e sviluppare soluzioni efficaci per garantire la sicurezza dei dati in vari ambienti professionali. Il piano di studi affronta anche gli strumenti più innovativi del settore, promuovendo strategie volte a proteggere le risorse digitali delle organizzazioni.

Contribuirai alla protezione dei dati sensibili e alla creazione di sistemi sicuri che garantiscano la continuità operativa delle imprese e delle istituzioni"

Modulo 1. Analitica dei dati nell'organizzazione aziendale

1.1. Analisi di business
- 1.1.1. Analisi di business
- 1.1.2. Struttura del dato
- 1.1.3. Fasi e elementi

1.2. Analisi dei dati nell'impresa
- 1.2.1. Schede di valutazione e KPI dipartimentali
- 1.2.2. Rapporto operativo, tattico e strategico
- 1.2.3. Analisi dei dati applicata a ciascun dipartimento
  - 1.2.3.1. Marketing e comunicazione
  - 1.2.3.2. Commerciale
  - 1.2.3.3. Servizio clienti
  - 1.2.3.4. Acquisti
  - 1.2.3.5. Amministrazione
  - 1.2.3.6. Risorse Umane
  - 1.2.3.7. Produzione
  - 1.2.3.8. IT

1.3. Marketing e comunicazione
- 1.3.1. KPI da misurare, applicazioni e benefici
- 1.3.2. Sistemi di Marketing e *Data Warehouse*
- 1.3.3. Implementazione di una struttura di analisi dei dati nel marketing
- 1.3.4. Piano di marketing e comunicazione
- 1.3.5. Strategia, previsione e gestione delle campagne

1.4. Commerciale e vendite
- 1.4.1. Contributi dell'analisi dei dati nell'area commerciale
- 1.4.2. Esigenze del dipartimento di vendite
- 1.4.3. Studi di mercato

1.5. Servizio clienti
- 1.5.1. Fidelizzazione
- 1.5.2. Qualità personale e intelligenza emotiva
- 1.5.3. Soddisfazione del cliente

1.6. Acquisti
- 1.6.1. Analisi dei dati per le ricerche di mercato
- 1.6.2. Analisi dei dati per le ricerche di concorrenza
- 1.6.3. Altre applicazioni

1.7. Amministrazione
- 1.7.1. Esigenze del dipartimento di amministrazione
- 1.7.2. *Data Warehouse* e analisi di rischio finanziario
- 1.7.3. *Data Warehouse* e analisi di rischio di credito

1.8. Risorse Umane
- 1.8.1. HR e benefici dell'analisi dei dati
- 1.8.2. Strumenti di analisi dei dati nel dipartimento di HR
- 1.8.3. Applicazioni di analisi dei dati nel dipartimento di HR

1.9. Produzione
- 1.9.1. Analisi dei dati nel dipartimento di produzione
- 1.9.2. Applicazioni
- 1.9.3. Benefici

1.10. IT
- 1.10.1. Dipartimento di IT
- 1.10.2. Analisi dei dati e trasformazione digitale
- 1.10.3. Innovazione e produttività

Modulo 2. Gestione di dati e informazioni per la Data Science

2.1. Statistica: Variabili, indici e rapporti
- 2.1.1. La Statistica
- 2.1.2. Dimensioni statistiche
- 2.1.3. Variabili, indici e rapporti

2.2. Tipologia del dato
- 2.2.1. Qualitativi
- 2.2.2. Quantitativi
- 2.2.3. Caratterizzazione e categoria

2.3. Conoscenza dei dati delle misurazioni
- 2.3.1. Misure di centralizzazione
- 2.3.2. Misure di dispersione
- 2.3.3. Correlazione

2.4. Conoscenza dei dati dei grafici
  2.4.1. Visualizzazione in funzione al tipo di dato
  2.4.2. Interpretazione dell'informazione grafica
  2.4.3. Personalizzazione della grafica con R
2.5. Probabilità
  2.5.1. Probabilità
  2.5.2. Funzione di probabilità
  2.5.3. Distribuzione
2.6. Raccolta di dati
  2.6.1. Metodologia di raccolta
  2.6.2. Strumenti di raccolta
  2.6.3. Canali di raccolta
2.7. Pulizia del dato
  2.7.1. Fasi di pulizia dei dati
  2.7.2. Qualità del dato
  2.7.3. Elaborazione dei dati (con R)
2.8. Analisi dei dati, interpretazione e valutazione dei risultati
  2.8.1. Misure statistiche
  2.8.2. Indici di relazione
  2.8.3. Data Mining
2.9. Archiviazione dei dati (*Datawarehouse*)
  2.9.1. Elementi
  2.9.2. Progettazione
2.10. Disponibilità del dato
  2.10.1. Accesso
  2.10.2. Utilità
  2.10.3. Sicurezza

Modulo 3. Dispositivi e piattaforme IoT come base per la Data Science

3.1. *Internet of Things*
  3.1.1. Internet del futuro, *Internet of Things*
  3.1.2. Il consorzio di internet industriale
3.2. Architettura di riferimento
  3.2.1. Architettura di riferimento
  3.2.2. Livelli
  3.2.3. Componenti
3.3. Sensori e dispositivi IoT
  3.3.1. Componenti principali
  3.3.2. Sensori e azionatori
3.4. Comunicazioni e protocolli
  3.4.1. Protocolli: Modello OSI
  3.4.2. Tecnologie di comunicazione
3.5. Piattaforme *Cloud* per IoT e IIoT
  3.5.1. Piattaforme con proposito generale
  3.5.2. Piattaforme industriali
  3.5.3. Piattaforme con codice aperto
3.6. Gestione dei dati in piattaforme IoT
  3.6.1. Meccanismi di gestione di dati: Dati aperti
  3.6.2. Scambio e visualizzazione dei dati
3.7. Sicurezza in IoT
  3.7.1. Requisiti e aree di sicurezza
  3.7.2. Strategie di sicurezza in IIoT
3.8. Applicazioni IoT
  3.8.1. Cure intelligenti
  3.8.2. Salute e condizione fisica
  3.8.3. Casa intelligente
  3.8.4. Altre applicazioni
3.9. Applicazioni di IIoT
  3.9.1. Fabbricazione
  3.9.2. Trasporto
  3.9.3. Energia
  3.9.4. Agricoltura e allevamento
  3.9.5. Altri settori
3.10. Industria 4.0
  3.10.1. IoRT *(Internet of Robotics Things)*
  3.10.2. Fabbricazione additiva 3D
  3.10.3. *Big Data Analytics*

Modulo 4. Rappresentazione grafica per l'analisi dei dati

4.1. Analisi esplorativa
- 4.1.1. Rappresentazione per l'analisi delle informazioni
- 4.1.2. Il valore della rappresentazione grafica
- 4.1.3. Nuovi paradigmi della rappresentazione grafica

4.2. Ottimizzazione per la Data Science
- 4.2.1. Gamma di colori e design
- 4.2.2. La Gestalt nella rappresentazione grafica
- 4.2.3. Errori da evitare e consigli

4.3. Fonti di dati base
- 4.3.1. Per la rappresentazione della qualità
- 4.3.2. Per la rappresentazione della quantità
- 4.3.3. Per la rappresentazione del tempo

4.4. Fonti di dati complessi
- 4.4.1. Archivi, liste e database (DB)
- 4.4.2. Dati aperti
- 4.4.3. Dati di generazione continua

4.5. Tipi di grafici
- 4.5.1. Rappresentazioni di base
- 4.5.2. Rappresentazione di blocchi
- 4.5.3. Rappresentazione per l'analisi della dispersione
- 4.5.4. Rappresentazioni circolari
- 4.5.5. Rappresentazioni a bolla
- 4.5.6. Rappresentazioni geografiche

4.6. Tipi di visualizzazione
- 4.6.1. Comparativo e relazionale
- 4.6.2. Distribuzione
- 4.6.3. Gerarchia

4.7. Progettazione di report con rappresentazione grafica
- 4.7.1. Applicazione dei grafici nei report di marketing
- 4.7.2. Applicazione dei grafici in dashboard e KPI
- 4.7.3. Applicazione dei grafici nei piani strategici
- 4.7.4. Altri usi: scienza, salute, business

4.8. Narrazione grafica
- 4.8.1. Narrazione grafica
- 4.8.2. Evoluzione
- 4.8.3. Utilità

4.9. Strumenti per la visualizzazione
- 4.9.1. Strumenti avanzati
- 4.9.2. Software online
- 4.9.3. *Open Source*

4.10. Nuove tecnologie per la visualizzazione dei dati
- 4.10.1. Sistemi per la virtualizzazione della realtà
- 4.10.2. Sistemi per l'aumento e il miglioramento della realtà
- 4.10.3. Sistemi intelligenti

Modulo 5. Strumenti di Data Science

5.1. Data Science
- 5.1.1. Data Science
- 5.1.2. Strumenti avanzati per i data scientist

5.2. Dati, informazioni e conoscenza
- 5.2.1. Dati, informazioni e conoscenza
- 5.2.2. Tipi di dati
- 5.2.3. Fonti di dati

5.3. Dai dati all'informazione
- 5.3.1. Analisi dei dati
- 5.3.2. Tipi di analisi
- 5.3.3. Estrazione di informazioni da un *Dataset*

5.4. Estrazione di informazioni tramite visualizzazione
- 5.4.1. La visualizzazione come strumento di analisi
- 5.4.2. Metodi di visualizzazione
- 5.4.3. Visualizzazione di un insieme di dati

5.5. Qualità dei dati
- 5.5.1. Dati di qualità
- 5.5.2. Pulizia di dati
- 5.5.3. Pre-elaborazione base dei dati

5.6. *Dataset*
- 5.6.1. Arricchimento del *Dataset*
- 5.6.2. La maledizione della dimensionalità
- 5.6.3. Modifica di un insieme di dati

5.7. Squilibrio
- 5.7.1. Squilibrio di classe
- 5.7.2. Tecniche di mitigazione dello squilibrio
- 5.7.3. Equilibrio di un *Dataset*

5.8. Modelli non supervisionati
- 5.8.1. Modello non supervisionato
- 5.8.2. Metodi
- 5.8.3. Classificazione con modelli non supervisionati

5.9. Modelli supervisionati
- 5.9.1. Modello supervisionato
- 5.9.2. Metodi
- 5.9.3. Classificazione con modelli supervisionati

5.10. Strumenti e best practice
- 5.10.1. Best practice per i data scientist
- 5.10.2. Il modello migliore
- 5.10.3. Strumenti utili

Modulo 6. Data Mining: selezione, pre-elaborazione e trasformazione

6.1. Inferenza statistica
- 6.1.1. Statistica descrittiva vs Inferenza statistica
- 6.1.2. Procedure parametriche
- 6.1.3. Procedure non parametriche

6.2. Analisi esplorativa
- 6.2.1. Analisi descrittiva
- 6.2.2. Visualizzazione
- 6.2.3. Preparazione dei dati

6.3. Preparazione dei dati
- 6.3.1. Integrazione e pulizia di dati
- 6.3.2. Standardizzazione dei dati
- 6.3.3. Trasformazione degli attributi

6.4. I valori mancanti
- 6.4.1. Trattamenti dei valori mancanti
- 6.4.2. Metodi di imputazione a massima verosimiglianza
- 6.4.3. Imputazione di valori mancanti mediante apprendimento automatico

6.5. Rumore nei dati
- 6.5.1. Classi di rumore e attributi
- 6.5.2. Filtraggio del rumore
- 6.5.3. Effetto del rumore

6.6. La maledizione della dimensionalità
- 6.6.1. *Oversampling*
- 6.6.2. *Undersampling*
- 6.6.3. Riduzione dei dati multidimensionali

6.7. Da attributi continui a discreti
- 6.7.1. Dati continui vs discreti
- 6.7.2. Processo di discretizzazione

6.8. I dati
- 6.8.1. Selezione dei dati
- 6.8.2. Prospettiva e criteri di selezione
- 6.8.3. Metodi di selezione

6.9. Selezione di istanze
- 6.9.1. Metodi per la selezione di istanze
- 6.9.2. Selezione di prototipi
- 6.9.3. Metodi avanzati per la selezione di istanze

6.10. Pre-elaborazione dei dati negli ambienti *Big Data*
- 6.10.1. *Big Data*
- 6.10.2. Pre-elaborazione "classica" vs massiva
- 6.10.3. *Smart Data*

Modulo 7. Prevedibilità e analisi dei fenomeni stocastici

7.1. Serie temporale
- 7.1.1. Serie temporale
- 7.1.2. Utilità e applicabilità
- 7.1.3. Casi di studio correlati

7.2. Serie temporali
- 7.2.1. Andamento stagionale della serie temporale
- 7.2.2. Variazioni tipiche
- 7.2.3. Analisi dei residui

7.3. Tipologie
- 7.3.1. Stazionarie
- 7.3.2. Non stazionarie
- 7.3.3. Trasformazioni e adattamenti

7.4. Schemi per le serie temporali
- 7.4.1. Schema additivo (modello)
- 7.4.2. Schema moltiplicano (modello)
- 7.4.3. Procedure per determinare il tipo di modello

7.5. Metodi di base di *forecast*
- 7.5.1. Media
- 7.5.2. *Naïve*
- 7.5.3. *Naïve* stagionale
- 7.5.4. Confronto di metodi

7.6. Analisi dei residui
- 7.6.1. Autocorrelazione
- 7.6.2. ACF dei residui
- 7.6.3. Test di correlazione

7.7. Regressione nel contesto delle serie temporali
- 7.7.1. ANOVA
- 7.7.2. Fondamenti
- 7.7.3. Applicazione pratica

7.8. Modelli predittivi di serie temporali
- 7.8.1. ARIMA
- 7.8.2. Livellamento esponenziale

7.9. Manipolazione e analisi delle Serie Temporali con R
- 7.9.1. Preparazione dei dati
- 7.9.2. Identificazione dei modelli
- 7.9.3. Analisi del modello
- 7.9.4. Previsione

7.10. Analisi grafica combinata con R
- 7.10.1. Situazioni tipiche
- 7.10.2. Applicazione pratica per la risoluzione di problemi semplici
- 7.10.3. Applicazione pratica per la risoluzione di problemi avanzati

Modulo 8. Progettazione e sviluppo di sistemi intelligenti

8.1. Pre-elaborazione dei dati
- 8.1.1. Pre-elaborazione dei dati
- 8.1.2. Trasformazione dei dati
- 8.1.3. Data Mining

8.2. Apprendimento Automatico
- 8.2.1. Apprendimento supervisionato e non
- 8.2.2. Apprendimento per rinforzo
- 8.2.3. Altri paradigmi di apprendimento

8.3. Algoritmi di classificazione
- 8.3.1. Apprendimento Automatico Indotto
- 8.3.2. SVM e KNN
- 8.3.3. Metriche e punteggi per la classificazione

8.4. Algoritmi di regressione
- 8.4.1. Regressione lineare, regressione logistica e modelli non lineari
- 8.4.2. Serie temporali
- 8.4.3. Metriche e punteggi per la regressione

8.5. Algoritmi di clustering
- 8.5.1. Tecniche di clustering gerarchico
- 8.5.2. Tecniche di clustering partizionale
- 8.5.3. Metriche e punteggi per il *clustering*

8.6. Tecniche di regole associative
- 8.6.1. Metodi per l'estrazione di regole
- 8.6.2. Metriche e punteggi per gli algoritmi di regole associative

8.7. Tecniche di classificazione avanzata: Multiclassificatori
- 8.7.1. Algoritmi di *bagging*
- 8.7.2. Classificatore *Random Forests*
- 8.7.3. *Boosting* per alberi decisionali

8.8. Modelli grafici probabilistici
- 8.8.1. Modelli probabilistici
- 8.8.2. Reti bayesiane: Proprietà, rappresentazione e parametrizzazione
- 8.8.3. Altri modelli grafici probabilistici

8.9. Reti neuronali
- 8.9.1. Apprendimento automatico con reti neuronali artificiali
- 8.9.2. Reti *feedforward*

8.10. Deep Learning
- 8.10.1. Reti *feedforward* profonde
- 8.10.2. Reti neurali convoluzionali e modelli di sequenza
- 8.10.3. Strumenti per l'implementazione di reti neurali profonde

Modulo 9. Architetture e sistemi ad alta intensità di dati

9.1. Requisiti non funzionali: I pilastri delle applicazioni di big data
- 9.1.1. Affidabilità
- 9.1.2. Adattamento
- 9.1.3. Mantenimento

9.2. Modelli di dati
- 9.2.1. Modello relazionale
- 9.2.2. Modello documentale
- 9.2.3. Modello di dati di rete

9.3. Database: Gestione di archiviazione e recupero dei dati
- 9.3.1. Indice hash
- 9.3.2. Archiviazione strutturata in log
- 9.3.3. Alberi B

9.4. Formati di codifica dei dati
- 9.4.1. Formati specifici di linguaggio
- 9.4.2. Formati standard
- 9.4.3. Formati di codifica binari
- 9.4.4. Flusso di dati tra i processi

9.5. Risposta
- 9.5.1. Obiettivi di risposta
- 9.5.2. Modelli di risposta
- 9.5.3. Problemi di risposta

9.6. Transazioni distribuite
- 9.6.1. Transazione
- 9.6.2. Protocolli per le transazioni distribuite
- 9.6.3. Transazioni serializzabili

9.7. Suddivisione
- 9.7.1. Forme di suddivisione
- 9.7.2. Interazione dell'indice secondario e suddiviso
- 9.7.3. Bilanciamento delle suddivisioni

9.8. Elaborazione dei dati *offline*
- 9.8.1. Elaborazione per lotti
- 9.8.2. File system distribuiti
- 9.8.3. *MapReduce*

9.9. Elaborazione dei dati in tempo reale
- 9.9.1. Tipi di *broker* di messaggi
- 9.9.2. Rappresentazione dei database come flussi di dati
- 9.9.3. Processo dei flussi di dati

9.10. Applicazioni pratiche nell'azienda
- 9.10.1. Coerenza nelle letture
- 9.10.2. Approccio olistico ai dati
- 9.10.3. Scaling di un servizio distribuito

Modulo 10. Applicazione pratica della Data Science nei settori aziendali

10.1. Settore sanitario
- 10.1.1. Implicazioni dell'IA e dell'analisi dei dati nel settore sanitario
- 10.1.2. Opportunità e sfide

10.2. Rischi e tendenze nel settore sanitario
- 10.2.1. Uso nel settore sanitario
- 10.2.2. Potenziali rischi legati all'uso dell'IA

10.3. Servizi finanziari
- 10.3.1. Implicazioni dell'IA e dell'analisi dei dati nel settore dei servizi finanziari
- 10.3.2. Uso nei servizi finanziari
- 10.3.3. Potenziali rischi legati all'uso dell'IA

10.4. Retail
- 10.4.1. Implicazioni dell'IA e dell'analisi dei dati nel settore del retail
- 10.4.2. Uso nel settore del retail
- 10.4.3. Potenziali rischi legati all'uso dell'IA

10.5. Industria 4.0.
- 10.5.1. Implicazioni dell'IA e dell'analisi dei Dati nell'Industria 4.0
- 10.5.2. Uso nell'Industria 4.0

10.6. Rischi e tendenze nell'Industria 4.0
- 10.6.1. Potenziali rischi legati all'uso dell'IA

10.7. Pubblica amministrazione
- 10.7.1. Implicazioni dell'IA e dell'analisi dei dati nella Pubblica Amministrazione
- 10.7.2. Uso nella Pubblica Amministrazione
- 10.7.3. Potenziali rischi legati all'uso dell'IA

10.8. Educazione
- 10.8.1. Implicazioni dell'IA e dell'analisi dei dati all'Istruzione
- 10.8.2. Potenziali rischi legati all'uso dell'IA

10.9. Silvicoltura e agricoltura
- 10.9.1. Implicazioni dell'IA e dell'analisi dei dati alla silvicoltura e all'agricoltura
- 10.9.2. Uso nella silvicoltura e nell'agricoltura
- 10.9.3. Potenziali rischi legati all'uso dell'IA

10.10. Risorse Umane
- 10.10.1. Implicazioni dell'IA e dell'analisi dei dati nella gestione di Risorse Umane
- 10.10.2. Applicazioni pratiche nel mondo degli affari
- 10.10.3. Potenziali rischi legati all'uso dell'IA

Modulo 11. Cyberintelligence e Cibersicurezza

11.1. Cyberintelligence
- 11.1.1. Cyberintelligence
  - 11.1.1.1. L'intelligence
    - 11.1.1.1.1. Ciclo dell'intelligence
  - 11.1.1.2. Cyberintelligence
  - 11.1.1.3. Cyberintelligence e Cibersicurezza
- 11.1.2. L'analista di intelligence
  - 11.1.2.1. Il ruolo dell'analista di intelligence
  - 11.1.2.2. I pregiudizi dell'analista di intelligence nell'attività valutativa

11.2. Cibersicurezza
- 11.2.1. Livelli di sicurezza
- 11.2.2. Identificazione delle minacce informatiche
  - 11.2.2.1. Minacce esterne
  - 11.2.2.2. Minacce interne
- 11.2.3. Azioni avverse
  - 11.2.3.1. Ingegneria sociale
  - 11.2.3.2. Metodi comunemente utilizzati

11.3. Tecniche e Strumenti delle intelligence
- 11.3.1. OSINT
- 11.3.2. SOCMINT
- 11.3.3. HUMIT
- 11.3.4. Distribuzioni e strumenti Linux
- 11.3.5. OWISAM
- 11.3.6. OWISAP
- 11.3.7. PTES
- 11.3.8. OSSTM

11.4. Metodologie di valutazione
- 11.4.1. L'analisi di intelligence
- 11.4.2. Tecniche di organizzazione delle informazioni acquisite
- 11.4.3. Affidabilità e credibilità delle fonti di informazione
- 11.4.4. Metodologie di analisi
- 11.4.5. Presentazione dei risultati dell'intelligence

11.5. Audit e documentazione
- 11.5.1. L'audit della sicurezza informatica
- 11.5.2. Documentazione e permessi per l'audit
- 11.5.3. Tipi di audit
- 11.5.4. Deliverable
  - 11.5.4.1. Rapporto tecnico
  - 11.5.4.2. Relazione esecutiva

11.6. Anonimato in rete
- 11.6.1. Uso dell'anonimato
- 11.6.2. Tecniche di anonimato (Proxy, VPN)
- 11.6.3. Reti TOR, Freenet e IP2

11.7. Minacce e tipi di sicurezza
- 11.7.1. Tipologie di minacce
- 11.7.2. Sicurezza fisica
- 11.7.3. Sicurezza di rete
- 11.7.4. Sicurezza logica
- 11.7.5. Sicurezza delle applicazioni web
- 11.7.6. Sicurezza sui dispositivi mobili

11.8. Normativa e *compliance*
- 11.8.1. GDPR
- 11.8.2. La strategia nazionale di cybersecurity per il 2019
- 11.8.3. Famiglia ISO 27000
- 11.8.4. Quadro di sicurezza informatica NIST
- 11.8.5. PIC
- 11.8.6. ISO 27032
- 11.8.7. Normative *Cloud*
- 11.8.8. SOX
- 11.8.9. PCI

11.9. Analisi dei rischi e metriche
- 11.9.1. Portata dei rischi
- 11.9.2. I cespiti
- 11.9.3. Le minacce
- 11.9.4. Punti deboli
- 11.9.5. Valutazione del rischio
- 11.9.6. Trattamento del rischio

11.10. Importanti organismi di cybersecurity
- 11.10.1. NIST
- 11.10.2. ENISA
- 11.10.3. INCIBE
- 11.10.4. OEA
- 11.10.5. UNASUR-PROSUR

Modulo 12. Sicurezza in host

12.1. Backup
- 12.1.1. Strategie per i backup
- 12.1.2. Strumenti per Windows
- 12.1.3. Strumenti per Linux
- 12.1.4. Strumenti per MacOS

12.2. Antivirus utente
- 12.2.1. Tipi di antivirus
- 12.2.2. Antivirus per Windows
- 12.2.3. Antivirus per Linux
- 12.2.4. Antivirus per MacOS
- 12.2.5. Antivirus per smartphone

12.3. Rilevatori di intrusione-HIDS
- 12.3.1. Metodi di rilevamento delle intrusioni
- 12.3.2. *Sagan*
- 12.3.3. *Aide*
- 12.3.4. *Rkhunter*

12.4. *Firewall* locale
- 12.4.1. *Firewall* per Windows
- 12.4.2. *Firewall* per Linux
- 12.4.3. *Firewall* per MacOS

12.5. Gestori di password
- 12.5.1. *Password*
- 12.5.2. *LastPass*
- 12.5.3. *KeePass*
- 12.5.4. *StickyPassword*
- 12.5.5. *RoboForm*

12.6. Rilevatori di *phishing*
- 12.6.1. Rilevamento manuale del *phishing*
- 12.6.2. Strumenti *antiphishing*

12.7. *Spyware*
- 12.7.1. Meccanismi di prevenzione
- 12.7.2. Strumenti *antispyware*

12.8. Tracciatori
- 12.8.1. Misure di protezione del sistema
- 12.8.2. Strumenti anti-tracker

12.9. EDR - *End Point Detection and Response*
- 12.9.1. Comportamento del sistema EDR
- 12.9.2. Differenze tra EDR e antivirus
- 12.9.3. Il futuro dei sistemi EDR

12.10. Controllo dell'installazione del software
- 12.10.1. Repository e negozi di software
- 12.10.2. Elenchi di software consentiti o vietati
- 12.10.3. Criteri di aggiornamento
- 12.10.4. Privilegi per l'installazione di software

Modulo 13. Sicurezza di rete (perimetro)

13.1. Sistemi di rilevamento e prevenzione delle minacce
- 13.1.1. Quadro generale per gli incidenti di sicurezza
- 13.1.2. Sistemi di difesa attuali: *Defense in Depth* e SOC
- 13.1.3. Le attuali architetture di rete
- 13.1.4. Tipi di strumenti di rilevamento e prevenzione degli incidenti
  - 13.1.4.1. Sistemi basati sulla rete
  - 13.1.4.2. Sistemi basati su host
  - 13.1.4.3. Sistemi centralizzati
- 13.1.5. Comunicazione e rilevamento di istanze/*host*, container e *serverless*

13.2. *Firewall*
- 13.2.1. Tipi di *firewall*
- 13.2.2. Attacchi e contenimento
- 13.2.3. *Firewalls* comuni nel kernel Linux
  - 13.2.3.1. UFW
  - 13.2.3.2. Nftables e iptables
  - 13.2.3.3. *Firewalld*
- 13.2.4. Sistemi di rilevamento basati sui log di sistema
  - 13.2.4.1. TCP *Wrappers*
  - 13.2.4.2. *BlockHosts* e *DenyHosts*
  - 13.2.4.3. Fai2ban

13.3. Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)
- 13.3.1. Attacchi agli IDS/IPS
- 13.3.2. Sistemi IDS/IPS
  - 13.3.2.1. *Snort*
  - 13.3.2.2. Suricata

13.4. *Firewall* di nuova generazione (NGFW)
- 13.4.1. Differenze tra NGFW e Firewall tradizionali
- 13.4.2. Funzionalità chiave
- 13.4.3. Soluzioni commerciali
- 13.4.4. Firewall per servizi *Cloud*
  - 13.4.4.1. Architettura *Cloud* VPC
  - 13.4.4.2. ACL per il*Cloud*
  - 13.4.4.3. *Security Group*

13.5. Proxy
- 13.5.1. Tipi di Proxy
- 13.5.2. Uso di Proxy: Vantaggi e svantaggi

13.6. Motori antivirus
- 13.6.1. Contesto generale del *Malware* degli IoC
- 13.6.2. Problemi del motore antivirus

13.7. Sistemi di protezione della posta
- 13.7.1. Antispam
  - 13.7.1.1. Whitelisting e blacklisting
  - 13.7.1.2. Filtri bayesiani
- 13.7.2. *Mail Gateway* (MGW)

13.8. SIEM
- 13.8.1. Componenti e architettura
- 13.8.2. Regole di correlazione e casi d'uso
- 13.8.3. Sfide attuali per i sistemi SIEM

13.9. SOAR
- 13.9.1. SOAR e SIEM: nemici o alleati
- 13.9.2. Il futuro dei sistemi SOAR

13.10. Altri sistemi basati sulla rete
- 13.10.1. WAF
- 13.10.2. NAC
- 13.10.3. HoneyPots e HoneyNets
- 13.10.4. CASB

Modulo 14. Sicurezza degli smartphone

14.1. Il mondo dei dispositivi mobili
- 14.1.1. Tipi di piattaforme mobili
- 14.1.2. Dispositivi IOS
- 14.1.3. Dispositivi Android

14.2. Gestione della sicurezza mobile
- 14.2.1. Progetto OWASP sulla Sicurezza Mobile
  - 14.2.1.1. I 10 punti deboli più importanti
- 14.2.2. Comunicazioni, reti e modalità di connessione

14.3. Il dispositivo mobile in ambito aziendale
- 14.3.1. Rischi
- 14.3.2. Politiche di sicurezza
- 14.3.3. Monitoraggio del dispositivo
- 14.3.4. Gestione dei dispositivi mobili (MDM)

14.4. Privacy degli utenti e sicurezza dei dati
- 14.4.1. Stati di informazione
- 14.4.2. Protezione dei dati e riservatezza
  - 14.4.2.1. Permessi
  - 14.4.2.2. Crittografia
- 14.4.3. Archiviazione sicura dei dati
  - 14.4.3.1. Archiviazione sicura su iOS
  - 14.4.3.2. Archiviazione sicura su Android
- 14.4.4. Buone pratiche nello sviluppo di applicazioni

14.5. Punti deboli e vettori di attacco
- 14.5.1. Vulnerabilità
- 14.5.2. Vettori di attacco
  - 14.5.2.1. *Malware*
  - 14.5.2.2. Infiltrazione di dati
  - 14.5.2.3. Manipolazione dei dati

14.6. Principali minacce
- 14.6.1. Utente non obbligato
- 14.6.2. *Malware*
  - 14.6.2.1. Tipi di *Malware*
- 14.6.3. Ingegneria sociale
- 14.6.4. Perdite di dati
- 14.6.5. Furto di informazioni
- 14.6.6. Reti *Wifi* non sicure
- 14.6.7. Software obsoleto
- 14.6.8. Applicazioni dannose
- 14.6.9. Password insicure
- 14.6.10. Impostazioni di sicurezza deboli o inesistenti
- 14.6.11. Accesso fisico
- 14.6.12. Perdita o furto del dispositivo
- 14.6.13. Furto d'identità (Integrità)
- 14.6.14. Criptografia debole o non funzionante
- 14.6.15. Negazione del servizio (DoS)

14.7. Principali attacchi
- 14.7.1. Attacchi di *phishing*
- 14.7.2. Attacchi legati alle modalità di comunicazione
- 14.7.3. Attacchi di *smishing*
- 14.7.4. Attacchi di *Criptojacking*
- 14.7.5. *Man in the Middle*

14.8. *Hacking*
- 14.8.1. *Rooting e jailbreaking*
- 14.8.2. Anatomia di un attacco mobile
  - 14.8.2.1. Propagazione della minaccia
  - 14.8.2.2. Installazione di *Malware* sul dispositivo
  - 14.8.2.3. Persistenza
  - 14.8.2.4. Esecuzione del *Payload* ed estrazione delle informazioni
- 14.8.3. *Hacking* sui dispositivi iOS: meccanismi e strumenti
- 14.8.4. *Hacking* sui dispositivi Android: meccanismi e strumenti

14.9. Test di intrusione
- 14.9.1. *iOS PenTesting*
- 14.9.2. *Android PenTesting*
- 14.9.3. Strumenti

14.10. Sicurezza e protezione
- 14.10.1. Impostazioni di sicurezza
  - 14.10.1.1. Su dispositivi iOS
  - 14.10.1.2. Su dispositivi Android
- 14.10.2. Misure di sicurezza
- 14.10.3. Strumenti di protezione

Modulo 15. Sicurezza in IoT

15.1. Dispositivi
- 15.1.1. Tipi di dispositivi
- 15.1.2. Architetture standardizzate
  - 15.1.2.1. ONEM2M
  - 15.1.2.2. IoTWF
- 15.1.3. Protocolli di applicazione
- 15.1.4. Tecnologie di connettività

15.2. Dispositivi IoT: Aree di applicazione
- 15.2.1. *SmartHome*
- 15.2.2. *SmartCity*
- 15.2.3. Trasporto
- 15.2.4. *Wearables*
- 15.2.5. Settore sanitario
- 15.2.6. IioT

15.3. Protocolli di comunicazione
- 15.3.1. MQTT
- 15.3.2. LWM2M
- 15.3.3. OMA-DM
- 15.3.4. TR-069

15.4. *SmartHome*
- 15.4.1. Automazione domestica
- 15.4.2. Reti
- 15.4.3. Elettrodomestici
- 15.4.4. Sorveglianza e sicurezza

15.5. *SmartCity*
- 15.5.1. Illuminazione
- 15.5.2. Meteorologia
- 15.5.3. Sicurezza

15.6. Trasporto
- 15.6.1. Localizzazione
- 15.6.2. Effettuare pagamenti e ottenere servizi
- 15.6.3. Connettività

15.7. *Wearables*
- 15.7.1. Abiti intelligenti
- 15.7.2. Gioielli intelligenti
- 15.7.3. Smartwatch

15.8. Settore sanitario
- 15.8.1. Monitoraggio dell'esercizio e della frequenza cardiaca
- 15.8.2. Monitoraggio di pazienti e anziani
- 15.8.3. Impiantabili
- 15.8.4. Robot chirurgici

15.9. Connettività
- 15.9.1. *Wi-Fi/Gateway*
- 15.9.2. *Bluetooth*
- 15.9.3. Connettività integrata

15.10. Cartolarizzazione
- 15.10.1. Reti dedicate
- 15.10.2. Gestione password
- 15.10.3. Utilizzo di protocolli criptati
- 15.10.4. Suggerimenti per l'uso

Modulo 16. *Hacking* etico

16.1. Ambiente di lavoro
- 16.1.1. Distribuzioni Linux
  - 16.1.1.1. Kali Linux - Offensive Security
  - 16.1.1.2. Parrot OS
  - 16.1.1.3. Ubuntu
- 16.1.2. Sistemi di virtualizzazione
- 16.1.3. *Sandbox*
- 16.1.4. Distribuzione dei laboratori

16.2. Metodologie
- 16.2.1. OSSTM
- 16.2.2. OWASP
- 16.2.3. NIST
- 16.2.4. PTES
- 16.2.5. ISSAF

16.3. *Footprinting*
- 16.3.1. Intelligence open source (OSINT)
- 16.3.2. Ricerca di violazioni dei dati e punti deboli
- 16.3.3. Utilizzo di strumenti passivi

16.4. Scansione di rete
- 16.4.1. Strumenti di scansione
  - 16.4.1.1. Nmap
  - 16.4.1.2. Hping3
  - 16.4.1.3. Altri strumenti di scansione
- 16.4.2. Tecniche di Scansione
- 16.4.3. Tecniche di elusione di *firewall* e IDS
- 16.4.4. *Banner Grabbing*
- 16.4.5. Diagrammi di rete

16.5. Enumerazione
- 16.5.1. Enumerazione SMTP
- 16.5.2. Enumerazione DNS
- 16.5.3. Enumerazione NetBIOS e Samba
- 16.5.4. Enumerazione LDAP
- 16.5.5. Enumerazione SNMP
- 16.5.6. Altre tecniche di Enumerazione

16.6. Analisi delle vulnerabilità
- 16.6.1. Soluzioni per l'Analisi dei punti deboli
  - 16.6.1.1. Qualys
  - 16.6.1.2. Nessus
  - 16.6.1.3. CFI LanGuard
- 16.6.2. Sistemi di punteggio dei punti deboli
  - 16.6.2.1. CVSS
  - 16.6.2.2. CVE
  - 16.6.2.3. NVD

16.7. Attacchi alle reti *wireless*
- 16.7.1. Metodologia di *hacking* nelle reti wireless
  - 16.7.1.1. Wi-fi Discovery
  - 16.7.1.2. Analisi del traffico
  - 16.7.1.3. Attacchi *aircrack*
    - 16.7.1.3.1. Attacchi WEP
    - 16.7.1.3.2. Attacchi WPA/WPA2
  - 16.7.1.4. Attacchi *Evil Twin*
  - 16.7.1.5. Attacchi WPS
  - 16.7.1.6. *Jamming*
- 16.7.2. Strumenti per la sicurezza wireless

16.8. Hacking di server web
- 16.8.1. *Cross site Scripting*
- 16.8.2. CSRF
- 16.8.3. *Sessione Hijacking*
- 16.8.4. *SQLinjection*

16.9. Sfruttamento dei punti deboli
- 16.9.1. Utilizzo di *Exploit* noti
- 16.9.2. Utilizzo di *metasploit*
- 16.9.3. Utilizzo di *malware*
  - 16.9.3.1. Definizione e campo di applicazione
  - 16.9.3.2. Generazione di *Malware*
  - 16.9.3.3. Bypassare le soluzioni antivirus

16.10. Persistenza
- 16.10.1. Installazione di Rootkit
- 16.10.2. Utilizzo di Ncat
- 16.10.3. Utilizzo di attività pianificate per le Backdoor
- 16.10.4. Creazione di utenti
- 16.10.5. Rilevamento HIDS

Modulo 17. Ingegneria inversa

17.1. I compilatori
- 17.1.1. Tipi di codici
- 17.1.2. Fasi di un compilatore
- 17.1.3. Tabella dei simboli
- 17.1.4. Gestione degli errori
- 17.1.5. Compilatore GCC

17.2. Tipi di analisi nei compilatori
- 17.2.1. Analisi lessicale
  - 17.2.1.1. Terminologia
  - 17.2.1.2. Componenti lessicali
  - 17.2.1.3. Analizzatore lessicale LEX
- 17.2.2. Analisi sintattica
  - 17.2.2.1. Grammatiche libere dal contesto
  - 17.2.2.2. Tipi di analisi sintattica
    - 17.2.2.2.1. Analisi discendente
    - 17.2.2.2.2. Analisi ascendente
  - 17.2.2.3. Alberi sintattici e derivazioni
  - 17.2.2.4. Tipi di analizzatori sintattici
    - 17.2.2.4.1. Analizzatori LR (*Left To Right*)
    - 17.2.2.4.2. Analizzatori LALR
- 17.2.3. Analisi semantica
  - 17.2.3.1. Grammatiche di attributi
  - 17.2.3.2. Attribuiti a S
  - 17.2.3.3. Attribuiti a L

17.3. Strutture dati dell'assemblatore
- 17.3.1. Variabili
- 17.3.2. Array
- 17.3.3. Puntatori
- 17.3.4. Struttura
- 17.3.5. Obiettivi

17.4. Strutture del codice assembly
- 17.4.1. Strutture di selezione
  - 17.4.1.1. If, else if, Else
  - 17.4.1.2. Switch
- 17.4.2. Strutture di iterazione
  - 17.4.2.1. For
  - 17.4.2.2. While
  - 17.4.2.3. Uso del break
- 17.4.3. Funzioni

17.5. Architettura Hardware x86
- 17.5.1. Architettura dei processori x86
- 17.5.2. Strutture dati x86
- 17.5.3. Strutture di codice x86

17.6. Architettura Hardware ARM
- 17.6.1. Architettura dei processori ARM
- 17.6.2. Strutture dati ARM
- 17.6.3. Strutture di codice ARM

17.7. Analisi del codice statico
- 17.7.1. Disassemblatori
- 17.7.2. IDA
- 17.7.3. Ricostruttori di codici

17.8. Analisi dinamica del codice
- 17.8.1. Analisi del comportamento
  - 17.8.1.1. Comunicazioni
  - 17.8.1.2. Monitoraggio
- 17.8.2. Debugger di codice Linux
- 17.8.3. Debugger di codice Windows

17.9. *Sandbox*
- 17.9.1. Architettura di un *Sandbox*
- 17.9.2. Elusione della *Sandbox*
- 17.9.3. Tecniche di rilevamento
- 17.9.4. Tecniche di evasione
- 17.9.5. Contromisure
- 17.9.6. *Sandbox* su Linux
- 17.9.7. *Sandbox* su Windows
- 17.9.8. *Sandbox* su MacOS
- 17.9.9. *Sandbox* su Android

17.10. Analisi dei malware
- 17.10.1. Metodi di analisi dei *malware*
- 17.10.2. Tecniche di offuscamento del *malware*
  - 17.10.2.1. Offuscamento degli eseguibili
  - 17.10.2.2. Limitazione degli ambienti di esecuzione
- 17.10.3. Strumenti di analisi dei *malware*

Modulo 18. Sviluppo sicuro

18.1. Sviluppo sicuro
- 18.1.1. Qualità, funzionalità e sicurezza
- 18.1.2. Riservatezza, integrità e disponibilità
- 18.1.3. Ciclo di vita dello sviluppo del software

18.2. Fase dei requisiti
- 18.2.1. Controllo dell'autenticazione
- 18.2.2. Controllo dei ruoli e dei privilegi
- 18.2.3. Requisiti orientati al rischio
- 18.2.4. Approvazione dei privilegi

18.3. Fasi di analisi e progettazione
- 18.3.1. Accesso ai componenti e amministrazione del sistema
- 18.3.2. Tracce di audit
- 18.3.3. Gestione delle sessioni
- 18.3.4. Dati storici
- 18.3.5. Gestione appropriata degli errori
- 18.3.6. Separazione delle funzioni

18.4. Fase di implementazione e codifica
- 18.4.1. Protezione dell'ambiente di sviluppo
- 18.4.2. Preparazione della documentazione tecnica
- 18.4.3. Codifica sicura
- 18.4.4. Sicurezza nelle comunicazioni

18.5. Buone pratiche di codifica sicura
- 18.5.1. Convalida dei dati di ingresso
- 18.5.2. Codifica dei dati di uscita
- 18.5.3. Stile di programmazione
- 18.5.4. Gestione dei log delle modifiche
- 18.5.5. Pratiche crittografiche
- 18.5.6. Gestione degli errori e dei log
- 18.5.7. Gestione degli archivi
- 18.5.8. Gestione della memoria
- 18.5.9. Standardizzazione e riutilizzo delle funzioni di sicurezza

18.6. Preparazione del server e *hardening*
- 18.6.1. Gestione di utenti, gruppi e ruoli sul server
- 18.6.2. Installazione software
- 18.6.3. *Hardening* del server
- 18.6.4. Configurazione robusta del contesto di applicazione

18.7. Preparazione della Base di Dati e dell'*hardening*
- 18.7.1. Ottimizzazione del motore della Base di Dati
- 18.7.2. Creare un proprio utente per l'applicazione
- 18.7.3. Assegnazione dei privilegi necessari all'utente
- 18.7.4. *Hardening* della Base di Dati

18.8. Fase di test
- 18.8.1. Controllo qualità negli audit di sicurezza
- 18.8.2. Ispezione del codice per fasi
- 18.8.3. Verifica della gestione delle configurazioni
- 18.8.4. Modello black box

18.9. Preparare il passaggio alla produzione
- 18.9.1. Eseguire il controllo delle modifiche
- 18.9.2. Eseguire la procedura di cambio produzione
- 18.9.3. Eseguire la procedura di *rollback*
- 18.9.4. Test di pre-produzione

18.10. Fase di mantenimento
- 18.10.1. Garanzia basata sul rischio
- 18.10.2. Test di manutenzione della sicurezza white box
- 18.10.3. Test di manutenzione della sicurezza black box

Modulo 19. Analisi forense

19.1. Acquisizione e riproduzione dei dati
- 19.1.1. Acquisizione della memoria volatile
  - 19.1.1.1. Informazioni sul sistema
  - 19.1.1.2. Informazioni di rete
  - 19.1.1.3. Ordine di volatilità
- 19.1.2. Acquisizione dei dati statici
  - 19.1.2.1. Creazione di un'immagine duplicata
  - 19.1.2.2. Preparazione di un documento per la catena di custodia
- 19.1.3. Metodi di validazione dei dati acquisiti
  - 19.1.3.1. Metodi per Linux
  - 19.1.3.2. Metodi per Windows

19.2. Valutazione e fallimento delle tecniche anti-forensi
- 19.2.1. Obiettivi delle tecniche anti-forensi
- 19.2.2. Cancellazione dei dati
  - 19.2.2.1. Cancellazione di dati e file
  - 19.2.2.2. Recupero dei file
  - 19.2.2.3. Recupero di partizioni eliminate
- 19.2.3. Protezione con password
- 19.2.4. Steganografia
- 19.2.5. Cancellazione sicura del dispositivo
- 19.2.6. Crittografia

19.3. Analisi forense del sistema operativo
- 19.3.1. Analisi forense di Windows
- 19.3.2. Analisi forense di Linux
- 19.3.3. Analisi forense di Mac

19.4. Analisi forense della rete
- 19.4.1. Analisi dei Log
- 19.4.2. Correlazione dei dati
- 19.4.3. Ricerca di rete
- 19.4.4. Passi da seguire nell'analisi forense della rete

19.5. Analisi forense del Web
- 19.5.1. Indagine sugli attacchi web
- 19.5.2. Rilevamento degli attacchi
- 19.5.3. Localizzazione degli indirizzi IP

19.6. Analisi forense dei Database
- 19.6.1. Analisi forense in MSSQL
- 19.6.2. Analisi forense in MySQL
- 19.6.3. Analisi forense in PostgreSQL
- 19.6.4. Analisi forense in MongoDB

19.7. Analisi forense nel *cloud*
- 19.7.1. Tipi di crimini nel *cloud*
  - 19.7.1.1. *Cloud* come soggetto
  - 19.7.1.2. *Cloud* come oggetto
  - 19.7.1.3. *Cloud* come strumento
- 19.7.2. Sfide dell'analisi forense nel *cloud*
- 19.7.3. Investigazione dei servizi di archiviazione nel *cloud*
- 19.7.4. Strumenti di analisi forense per il *cloud*

19.8. Investigazione dei crimini informatici via email
- 19.8.1. Sistemi di posta elettronica
  - 19.8.1.1. Clienti di posta
  - 19.8.1.2. Server di posta
  - 19.8.1.3. Server SMTP
  - 19.8.1.4. Server POP3
  - 19.8.1.5. Server IMAP4
- 19.8.2. Reati di posta elettronica
- 19.8.3. Messaggio di posta elettronica
  - 19.8.3.1. Intestazioni standard
  - 19.8.3.2. Intestazioni estese
- 19.8.4. Fasi dell'indagine su questi reati
- 19.8.5. Strumenti forensi per la posta elettronica

19.9. Analisi forense dei cellulari
- 19.9.1. Reti cellulari
  - 19.9.1.1. Tipi di reti
  - 19.9.1.2. Contenuti del CDR
- 19.9.2. *Subscriber Identity Module* (SIM)
- 19.9.3. Acquisizione logica
- 19.9.4. Acquisizione fisica
- 19.9.5. Acquisizione del file system

19.10. Stesura e presentazione del rapporto forense
- 19.10.1. Aspetti importanti di un rapporto forense
- 19.10.2. Classificazione e tipi di rapporti
- 19.10.3. Guida alla stesura di un rapporto
- 19.10.4. Presentazione del rapporto
  - 19.10.4.1. Preparazione preventiva alla testimonianza
  - 19.10.4.2. Deposizione
  - 19.10.4.3. Rapporti con i media

Modulo 20. Le sfide attuali e future della sicurezza informatica

20.1. Tecnologia *blockchain*
- 20.1.1. Ambiti di applicazione
- 20.1.2. Garanzia di riservatezza
- 20.1.3. Garanzia di non ripudio

20.2. Moneta digitale
- 20.2.1. I Bitcoin
- 20.2.2. Criptovalute
- 20.2.3. Mining di criptovalute
- 20.2.4. Schemi piramidali
- 20.2.5. Altri potenziali reati e problemi

20.3. *Deepfake*
- 20.3.1. Impatto mediatico
- 20.3.2. Pericoli per la società
- 20.3.3. Meccanismi di rilevamento

20.4. Il futuro dell'intelligenza artificiale
- 20.4.1. Intelligenza artificiale e cognitive computing
- 20.4.2. Utilizzi per semplificare il servizio clienti

20.5. Privacy digitale
- 20.5.1. Valore dei dati in rete
- 20.5.2. Utilizzo dei dati in rete
- 20.5.3. Privacy e gestione dell'identità digitale

20.6. Cyber conflitti, criminalità informatica e attacchi informatici
- 20.6.1. L'impatto della sicurezza informatica sui conflitti internazionali
- 20.6.2. Conseguenze degli attacchi informatici sulla popolazione generale
- 20.6.3. Tipi di criminali informatici. Misure di protezione

20.7. Lavoro da remoto
- 20.7.1. La rivoluzione dello smartworking durante e dopo il Covid19
- 20.7.2. Collo di bottiglia durante l'accesso
- 20.7.3. Variazione della superficie di attacco
- 20.7.4. Necessità dei lavoratori

20.8. Tecnologie *Wireless* emergenti
- 20.8.1. WPA3
- 20.8.2. 5G
- 20.8.3. Onde millimetriche
- 20.8.4. Tendenza di *Get Smart* anziché *Get more*

20.9. Futuro dell'indirizzamento nelle reti
- 20.9.1. Problemi attuali con l'indirizzamento IP
- 20.9.2. IPv6
- 20.9.3. IPv4+
- 20.9.4. Vantaggi di IPv4+ rispetto a IPv4
- 20.9.5. Vantaggi dell'IPv6 rispetto all'IPv4

20.10. La sfida alla prevenzione e alla sensibilizzazione delle persone
- 20.10.1. Le attuali strategie governative
- 20.10.2. Resistenza da parte delle persone all'apprendimento
- 20.10.3. Programmi di aggiornamento che devono essere adottati dalle aziende

Imparerai attraverso casi reali progettati in ambienti di apprendimento simulati che riflettono le sfide attuali nella gestione dei dati e della sicurezza informatica"

04

Obiettivi didattici

L'obiettivo principale del Master Specialistico in Secure Information Management è quello di fornire agli studenti conoscenze di eccellenza in due aree fondamentali e complementari dell'informatica e dell'ingegneria: la gestione dei dati negli ambienti digitali e la sicurezza informatica. Questo programma combina entrambe le discipline per formare i professionisti nell'implementazione di soluzioni avanzate, consentendo loro di affrontare le sfide del lavoro con gli strumenti necessari per gestire e proteggere le informazioni sensibili nelle loro organizzazioni.

Trasforma la tua carriera con questo innovativo Master Specialistico, progettato per segnare un punto di svolta nella tua specializzazione in gestione dei dati e sicurezza informatica"

Obiettivi generali

- Sviluppare una conoscenza avanzata nell'analisi dei dati e nella sicurezza informatica per ottimizzare i processi aziendali con strumenti e tecniche innovative
- Implementare strategie di sicurezza efficaci per prevenire le minacce digitali su sistemi, reti e dispositivi mobili
- Risolvere le sfide della sicurezza informatica attraverso audit, reverse engineering e analisi forense basata sulle prove
- Anticipare le tendenze tecnologiche applicando soluzioni rivoluzionarie che proteggono risorse digitali e sistemi avanzati

Guida la gestione dei dati e della sicurezza informatica nell'ambiente digitale con questo programma di specializzazione"

Obiettivi specifici

Modulo 1. Analitica dei dati nell'organizzazione aziendale

- Sviluppare competenze nell'uso delle tecniche di analisi dei dati
- Generare informazioni preziose che guidano il processo decisionale strategico nelle organizzazioni imprenditoriali, migliorando l'efficienza e la competitività

Modulo 2. Gestione e manipolazione dei dati e delle informazioni per la Data Science

- Formare nella gestione efficiente e la manipolazione di grandi volumi di dati
- Applicare metodologie e strumenti per strutturare, ripulire e trasformare i dati informazioni utili per progetti di data science

Modulo 3. Dispositivi e piattaforme IoT come base per la Data Science

- Fornire le conoscenze necessarie su piattaforme e dispositivi di Internet of Things e la loro integrazione nella Data Science
- Approfondire l'acquisizione, l'elaborazione e l'analisi dei dati in tempo reale

Modulo 4. Rappresentazione grafica per l'analisi dei dati

- Rappresentare graficamente i dati utilizzando strumenti e tecniche avanzate di visualizzazione
- Facilitare la comprensione di modelli, tendenze e relazioni all'interno di grandi set di dati

Modulo 5. Strumenti di Data Science

- Specializzarsi nell'uso di strumenti e software specifici per la Data Science, come Python
- Approfondire la raccolta, l'analisi e la presentazione dei dati in diversi contesti professionali

Modulo 6. Data Mining: Selezione, pre-elaborazione e trasformazione

- Fornire le conoscenze e le competenze necessarie per applicare le tecniche di Data Mining
- Analizzare la selezione, il pre-elaborazione e la trasformazione dei dati per estrarre modelli e tendenze significativi

Modulo 7. Prevedibilità e analisi dei fenomeni stocastici

- Sviluppare competenze nella modellazione e nell'analisi di fenomeni stocastici
- Utilizzare metodi statistici avanzati per prevedere comportamenti e tendenze

  in ambienti incerti e dinamici

Modulo 8. Progettazione e sviluppo di sistemi intelligenti

- Specializzarsi nella progettazione e nello sviluppo di sistemi intelligenti, integrando le tecniche
- Creare soluzioni automatizzate che risolvono problemi complessi in modo efficiente

Modulo 9. Architetture e sistemi ad alta intensità di dati

- Fornire conoscenze sulla creazione di architetture di sistemi capaci di elaborare grandi volumi di dati in modo efficiente
- Utilizzare tecnologie avanzate come database distribuiti e elaborazione parallela

Modulo 10. Applicazione pratica della Data Science nei settori aziendali

- Sviluppare la capacità di applicare pratiche di Data Science in vari settori aziendali
- Integrare le conoscenze acquisite per migliorare il processo decisionale, l'ottimizzazione dei processi e l'innovazione aziendale

Modulo 11. Cyberintelligence e Cibersicurezza
- Fornire le conoscenze e le competenze necessarie per applicare tecniche di cyberintelligence e cibersicurezza
- Proteggere i sistemi e le reti aziendali dalle minacce informatiche e garantire l'integrità dei dati

Modulo 12. Sicurezza in Host
- Specializzarsi nell'implementazione di misure di sicurezza nei sistemi host
- Garantire la protezione dei server e delle applicazioni critiche utilizzando strumenti e buone pratiche di sicurezza informatica

Modulo 13. Sicurezza di rete (perimetro)
- Fornire conoscenze sulla protezione delle reti e dei sistemi informatici a livello perimetrale
- Gestire firewall, VPN e altri strumenti per garantire la sicurezza nell'infrastruttura di rete dell'azienda

Modulo 14. Sicurezza degli smartphone
- Sviluppare competenze per garantire la sicurezza sui dispositivi mobili
- Comprendere le vulnerabilità comuni e applicare misure preventive per proteggere le informazioni e le applicazioni su smartphone

Modulo 15. Sicurezza in IoT
- Fornire le competenze necessarie per implementare soluzioni di sicurezza su dispositivi IoT
- Proteggere le reti e i sistemi che interconnettono dispositivi e garantire la riservatezza e l'integrità dei dati generati

Modulo 16. Hacking etico
- Specializzarsi nelle pratiche di hacking etico, insegnando a condurre penetration test controllati
- Identificare le vulnerabilità nei sistemi informatici per migliorare la sicurezza prima che possano essere sfruttate dagli aggressori

Modulo 17. Ingegneria inversa
- Fornire conoscenze sulle tecniche di reverse engineering, consentendo l'analisi, e comprendere il funzionamento di software e hardware
- Rilevare i problemi di sicurezza o migliorare la funzionalità dei sistemi esistenti

Modulo 18. Sviluppo sicuro
- Specializzarsi nello sviluppo di software sicuro, insegnando buone pratiche di codifica e sicurezza durante il ciclo di vita del software
- Essere in grado di prevenire le vulnerabilità e proteggere i sistemi informatici dagli attacchi

Modulo 19. Analisi forense
- Sviluppare le competenze necessarie per condurre indagini forensi digitali
- Utilizzare strumenti e tecniche avanzati per recuperare, analizzare e preservare le prove elettroniche in incidenti di sicurezza informatica

Modulo 20. Le sfide attuali e future della sicurezza informatica
- Esplorare le sfide attuali e future nel campo della sicurezza informatica, analizzando le minacce emergenti e le nuove tecnologie di protezione
- Approfondire le strategie per mitigare i rischi in un ambiente tecnologico in costante cambiamento

05

Opportunità professionali

Al termine di questo Master Specialistico in Secure Information Management, i professionisti avranno acquisito una solida conoscenza delle strategie più avanzate nella sicurezza informatica e nella gestione dei dati digitali. Gli studenti saranno preparati a progettare e implementare soluzioni che garantiscano la protezione delle informazioni sensibili e ottimizzino i processi di analisi e processo decisionale in ambienti aziendali. In questo modo, miglioreranno le loro prospettive di lavoro e assumeranno ruoli specializzati come analisti di sicurezza informatica, consulenti di intelligence o gestori di dati critici.

Garantirai la sicurezza delle risorse digitali e sarai fondamentale per la trasformazione digitale delle organizzazioni"

Profilo dello studente

Lo studente del Master Specialistico in Secure Information Management sarà un professionista altamente qualificato per gestire e proteggere le informazioni negli ambienti digitali. Avrà una conoscenza avanzata in settori come la sicurezza informatica, l'intelligenza digitale e l'analisi dei dati, oltre a competenze pratiche nella progettazione e implementazione di strategie di difesa contro le minacce. Il suo profilo combina una profonda conoscenza tecnica con competenze strategiche che permetteranno di guidare progetti in settori aziendali chiave.

Diventerai un leader nella protezione dei dati e nella sicurezza informatica, collaborando con le aziende per affrontare le sfide dell'ambiente digitale.

- **Gestione della sicurezza:** Sviluppare la capacità di identificare i rischi, implementare strategie di difesa multistrato e garantire la riservatezza, l'integrità e la disponibilità dei dati
- **Analisi critica e problem solving:** Applicare tecniche avanzate per valutare i sistemi, individuare le vulnerabilità e progettare soluzioni su misura per diversi ambienti tecnologici
- **Competenze tecniche e digitali:** Gestire strumenti di analisi avanzati dei dati, della sicurezza informatica e dei sistemi di intelligence, che consentono di guidare progetti di innovazione tecnologica
- **Pensiero strategico:** Progetterai politiche di sicurezza e strategie aziendali che rispondono alle esigenze attuali e future dell'ambiente digitale
- **Collaborazione interdisciplinare:** Lavorare con team multidisciplinari per affrontare sfide complesse e garantire la sicurezza di reti, piattaforme IoT e dispositivi mobili

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

1. **Direttore di Cibersicurezza:** Leader incaricato di coordinare i team e progettare strategie per proteggere le risorse digitali nelle grandi organizzazioni
2. **Analista di Dati:** Progetta sistemi di analisi predittiva e visualizzazione per ottimizzare il processo decisionale
3. **Consulente per l'Intelligenza Digitale:** Consulente specializzato nella fornitura di soluzioni avanzate basate su intelligence e analisi dei rischi
4. **Specialista in IoT e sicurezza:** Progetta misure di protezione per dispositivi connessi e ambienti industriali
5. **Hacker Etico:** Valutazione delle vulnerabilità per correggere i bug nei sistemi aziendali e prevenire gli attacchi informatici
6. **Audit della Sicurezza:** Ispettore che esegue audit e analisi forensi per garantire la conformità
7. **Responsabile dei Dati Aziendali:** Amministratore responsabile della progettazione e gestione di sistemi di storage e analisi per migliorare l'efficienza operativa

Completa questo programma e si distingue come specialista nelle aree più richieste dell'ambiente digitale"

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.

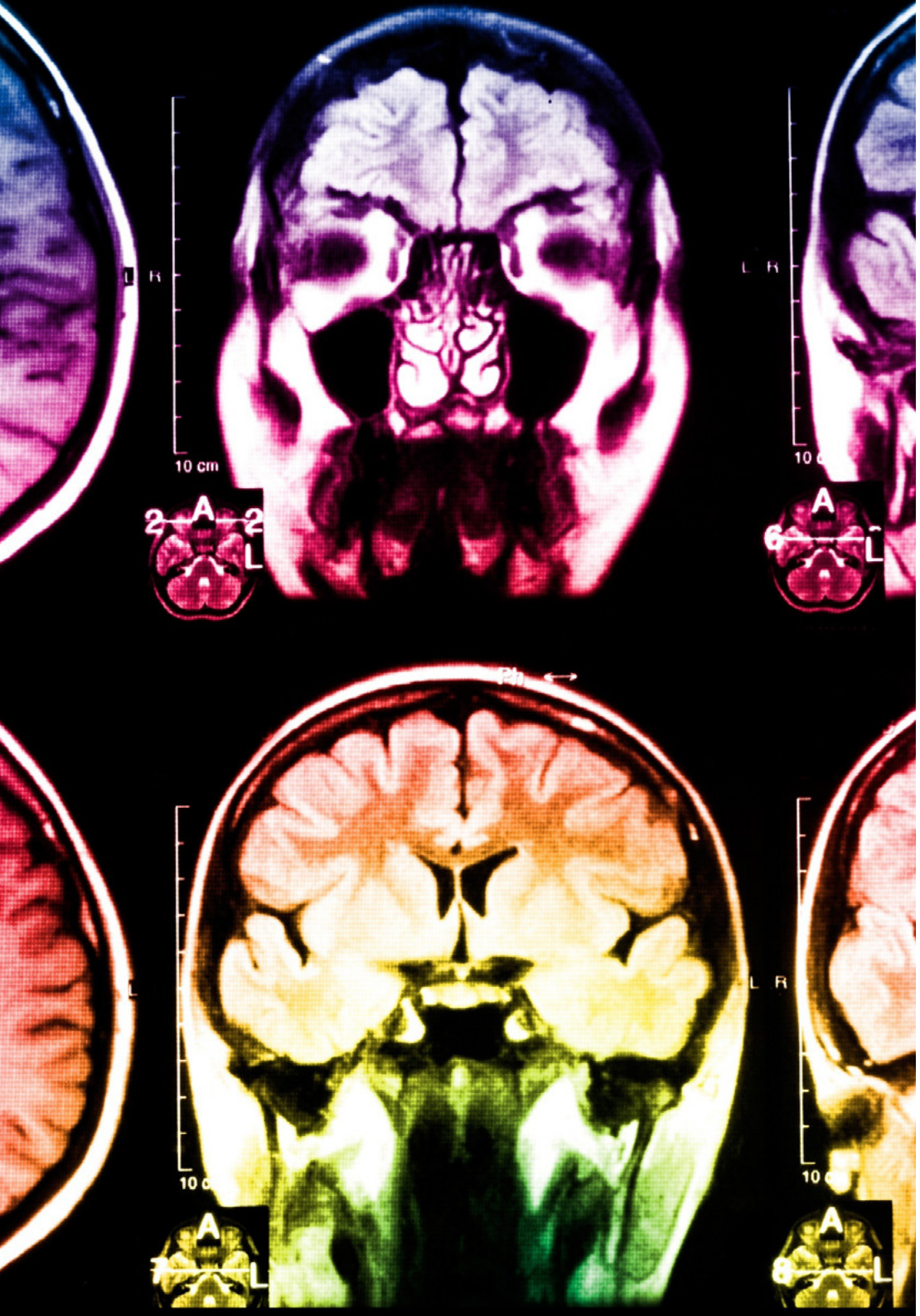
Inoltre, anche per favorire al massimo il contatto tra mentore e studente, viene fornita una vasta gamma di possibilità di comunicazione, sia in tempo reale che differita (messaggistica interna, forum di discussione, servizio di assistenza telefonica, e-mail di contatto con segreteria tecnica, chat e 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 conferma di ciò, l'istituto è diventato il migliore valutato dai suoi studenti sulla piattaforma di recensioni Trustpilot, ottenendo un punteggio di 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.

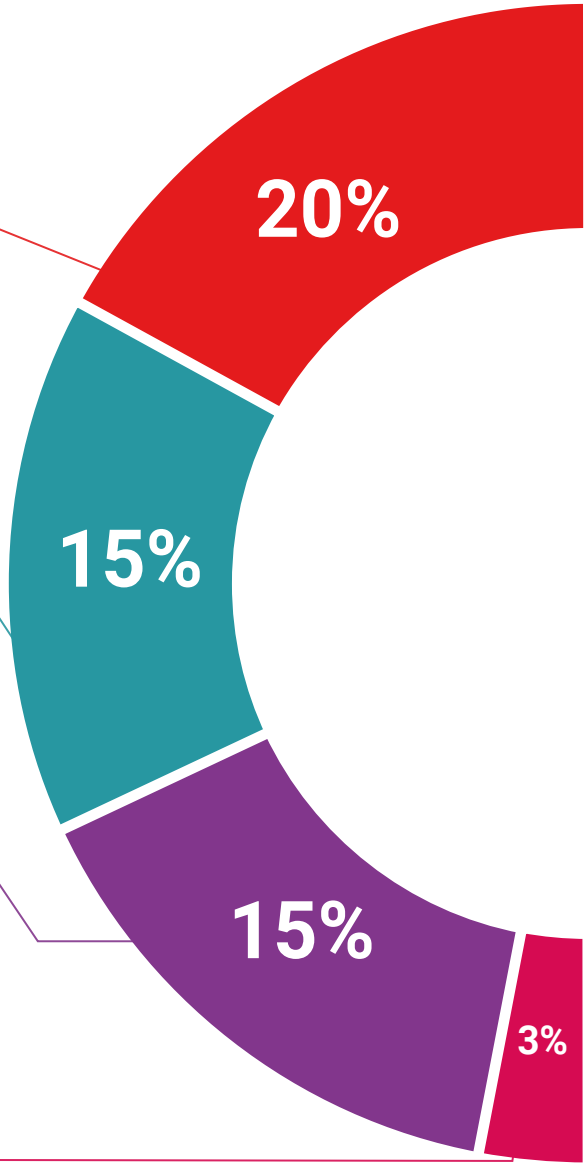
Riepiloghi interattivi

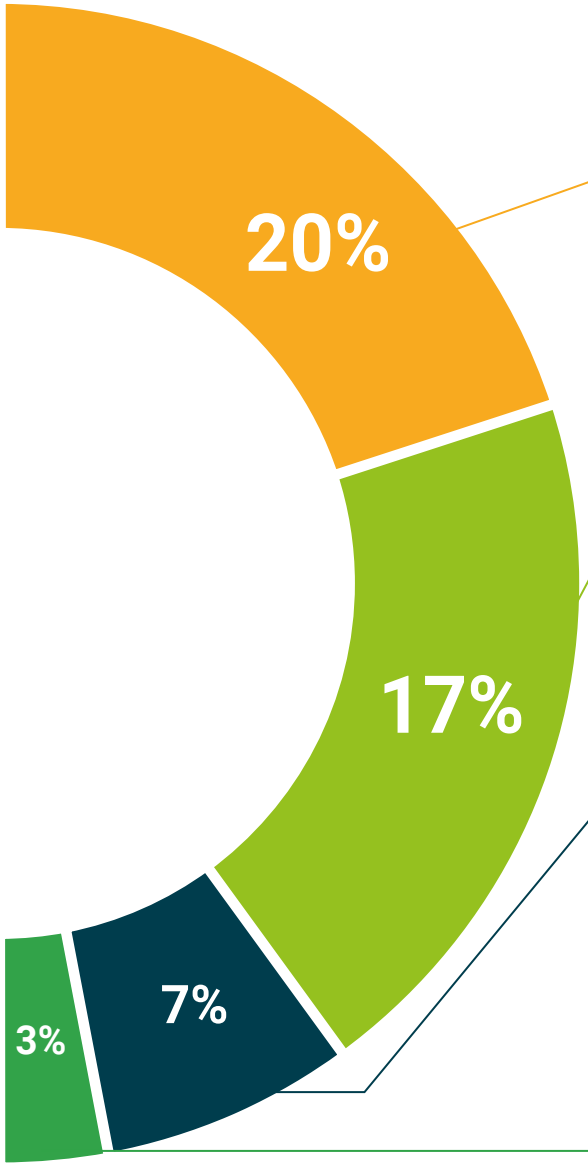
Presentiamo i contenuti in modo accattivante e dinamico tramite strumenti multimediali che includono audio, video, immagini, diagrammi e mappe concettuali per consolidare la conoscenza.

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

Questa qualifica è impartita da professionisti di riferimento nella sicurezza informatica e gestione dei dati digitali. La loro esperienza assicura che gli studenti ricevano contenuti completi e aggiornati, direttamente applicabili alle loro carriere. Il personale docente di questo Master Specialistico in Secure Information Management condivide quindi le conoscenze, formando specialisti altamente qualificati e richiesti da grandi aziende a livello internazionale.

Trionfa grazie ai migliori e acquisisci le conoscenze e le competenze chiave per essere leader nella gestione dei dati e della sicurezza informatica nell'ambiente digitale"

Direttore Ospite Internazionale

Il Dottor Frederic Lemieux è riconosciuto a livello internazionale come esperto innovativo e leader ispiratore nei settori di **Intelligence**, **Sicurezza Nazionale, Sicurezza Interna, Cibersicurezza** e **Tecnologie Dirompenti.** Il suo impegno costante e i suoi contributi rilevanti alla Ricerca e all'Educazione lo pongono come una figura chiave nella promozione della sicurezza e della comprensione delle tecnologie emergenti di oggi. Nel corso della sua carriera professionale, ha ideato e diretto programmi accademici all'avanguardia presso diverse istituzioni rinomate, tra cui **l'Università di Montreal**, la **la George Washington University** e la **Georgetown University.**.

Nel corso della sua vasta esperienza, ha pubblicato molti libri importanti, tutti relativi a **intelligence criminale, polizia, minacce informatiche e sicurezza internazionale.** Ha inoltre contribuito in modo significativo al campo della sicurezza informatica pubblicando numerosi articoli in riviste accademiche, che esaminano il controllo del crimine durante i grandi disastri, l'antiterrorismo, le agenzie di intelligence e la cooperazione di polizia. Inoltre, è stato relatore e relatore principale in varie conferenze nazionali e internazionali, affermandosi come punto di riferimento nell'ambiente accademico e professionale.

Il Dottor Lemieux ha ricoperto ruoli editoriali e di valutazione in diverse organizzazioni accademiche, private e governative, a testimonianza della sua influenza e del suo impegno per l'eccellenza nel suo campo di competenza. La sua prestigiosa carriera accademica lo ha portato a ricoprire il ruolo di Professore di Pratica e Direttore di Facoltà dei programmi MPS in **Intelligence applicata, Gestione del rischio di Cibersicurezza, Gestione della Tecnologia e Gestione della tecnologia dell'Informazione**, presso la **Georgetown University.**

Dott. Lemieux, Frederic

- Direttore del Master in Cybersecurity Risk Management a Georgetown, Washington, Stati Uniti
- Direttore del Masterin Technology Management presso la Georgetown University
- Direttore del Master in Applied Intelligence presso la Georgetown University
- Docente di Tirocini presso la Georgetown University
- Dottorato in Criminologia presso la Scuola di Criminologia dell'Università di Montreal
- Laurea in Sociologia, Minor Degree in Psicologia, Università di Laval
- Membro di: New Program Roundtable Committee presso la Georgetown University

Grazie a TECH potrai apprendere dai migliori professionisti del mondo"

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 conseguito presso l'Università di Castiglia-La Mancha
- Membro del Gruppo di Ricerca SMILE

Dott.ssa Fernández Sapena, Sonia

- Istruttrice in Sicurezza Informatica e Hacking Etico presso il Centro di Riferimento Nazionale per l'Informatica e le Telecomunicazioni di Getafe, Madrid
- Istruttrice certificata E-Council
- Formatrice nelle seguenti certificazioni: EXIN Ethical Hacking Foundation e EXIN Cyber & IT Security Foundation, Madrid
- Esperta Formatrice accreditata dal CAM per i seguenti certificati di professionalità: Sicurezza informatica (IFCT0190), Gestione di reti voce e dati (IFCM0310), Amministrazione di reti dipartimentali (IFCT0410), Gestione degli allarmi nelle reti di telecomunicazione (IFCM0410), Operatore di reti voce e dati (IFCM0110) e Amministrazione di servizi Internet (IFCT0509)
- Collaboratrice esterna CSO/SSA (*Chief Security Officer/Senior Security Architect*) presso l'Università delle Isole Baleari
- Laurea in Ingegneria Informatica presso l'Università di Alcalá de Henares a Madrid
- Master in DevOps: Docker and Kubernetes, Cas-Training
- Microsoft Azure Security Techonologies, E-Council

Personale docente

Dott. Montoro Montarroso, Andrés

- Membro del Gruppo di Ricerca SMIL dell'Università di Castiglia-La Mancha
- Ricercatore presso l'Università di Granada
- Scienziato dei Dati presso Prometeus Global Solutions
- Vicepresidente e Developer Software presso CireBits
- Dottorato in Tecnologia dell'Informazione Avanzata presso l'Università di Castiglia-La Mancha
- Laurea in Ingegneria Informatica presso l'Università di Castilla-La Mancha
- Master in Data Science e Computer Engineering conseguito presso l'Università di Granada
- Docente invitato nella materia dei Sistemi basati sulla conoscenza presso la Escuela Superior de Informática de Ciudad Real, tenendo la lezione: *Tecniche Avanzate di Intelligenza Artificiale: Ricerca e analisi di potenziali radicali nei Social Media*
- Docente ospite in materia di Data Mining presso la Scuola Superiore di Informatica di Ciudad Real, tenendo la lezione: *"Applicazioni dell'Elaborazione del Linguaggio Naturale: Logica sfocata per l'analisi dei messaggi sui social media"*
- Relatore al Seminario sulla Prevenzione della Corruzione nelle Pubbliche Amministrazioni e l'Intelligenza Artificiale presso la Facoltà di Giurisprudenza e Scienze Sociali di Toledo, tenendo la conferenza: *"Tecniche di Intelligenza Artificiale"*
- Relatore nel primo Seminario Internazionale di Diritto Amministrativo e Intelligenza Artificiale (DAIA) Organizzatore presso il Centro di Studi Europei Luis Ortega Álvarez e presso l'Istituto di Ricerca TransJus, Conferenza intitolata *Analisi dei Sentimenti per la prevenzione dei messaggi di odio sui social media*

Dott. Peris Morillo, Luis Javier

- Senior Technical Lead e Delivery Lead Support presso HCL Technologies
- Redattore tecnico presso Baeldung
- Agile Coach e Direttore Operativo presso Mirai Advisory
- Sviluppatore, Team Lead, Scrum Master, Agile Coach e Product Manager presso DocPath
- Tecnologo presso ARCO
- Laurea in Ingegneria Informatica presso l'Università di Castiglia-La Mancha
- Post-laurea in Gestione dei progetti presso il (CEOE)

Dott.ssa Fernández Meléndez, Galina

- Specialista in Big Data
- Analista Dati presso Aresi Gestión de Fincas
- Data Analyst presso ADN Mobile Solution
- Laurea in Economia Aziendale presso l'Università Bicentenaria di Aragua, Caracas, Venezuela
- Diploma in Pianificazione e Finanza Pubblica presso la Scuola Venezuelana di Pianificazione e Finanza Pubblica
- Master in Analisi dei Dati e Business Intelligence presso l'Università di Oviedo
- MBA in Business Administration e Management presso la European Business School di Barcellona
- Master in Big Data e Business Intelligence presso la Business School Europea di Barcellona

Dott.ssa Pedrajas Parabá, María Elena

- New Technologies and Digital Transformation Consultant presso Management Solutions
- Ricercatrice presso il Dipartimento di Informatica e Analisi Numerica dell'Università di Cordoba

- Ricercatrice presso il Centro Singolare di Ricerca in Tecnologie Intelligenti di Santiago de Compostela
- Laurea in Ingegneria Informatica presso l'Università di Cordoba
- Master in Data Science e Computer Engineering presso l'Università di Granada
- Master Privato in Business Consulting presso l'Università Pontificia di Comillas

Dott.ssa Martínez Cerrato, Yésica

- Responsabile della formazione tecnica presso Securitas Seguridad España
- Specialista in Educazione, Business e Marketing
- *Product Manager* in Sicurezza Elettronica presso Securitas Seguridad España
- Analista di Business Intelligence presso Ricopia Technologies
- Tecnico informatico e responsabile delle aule informatiche OTEC presso l'Università di Alcalá de Henares
- Collaboratrice dell'Associazione ASALUMA
- Laurea in Ingegneria delle Comunicazioni conseguita presso la Scuola Politecnica dell'Università di Alcalá de Henares

Dott. Fondón Alcalde, Rubén

- Analista EMEA presso Amazon Web Services
- Analista Aziendale per la Gestione del Valore del Cliente presso Vodafone Spagna
- Responsabile dell'Integrazione dei Servizi di Entelgy presso Telefónica Global Solutions
- Online Account Manager per i server cloni presso EDM Electronics
- Responsabile dell'Implementazione di Servizi Internazionali presso Vodafone Global Enterprise
- Consulente di Soluzioni per Spagna e Portogallo presso Telvent Global Services
- Busess Analyst nel Sud Europa presso Vodafone Global Enterprise
- Ingegnere delle Telecomunicazioni presso l'Università Europea di Madrid
- Master in Big Data e Analytics presso l'Università Internazionale di Valencia

Dott. Díaz Díaz-Chirón, Tobías

- Ricercatore presso il laboratorio ArCO dell'Università di Castiglia-La Mancha
- Consulente presso Blue Telecom
- Freelance dedicato principalmente al settore delle telecomunicazioni, specializzato in reti 4G/5G
- OpenStack: deploy and administration
- Ingegnere Senior in Informatica presso l'Università di Castiglia-La Mancha
- Specializzazione in Architettura e reti di computer
- Professore associato presso l'Università di Castiglia-La Mancha
- Relatore in corsi di Sepecam sull'amministrazione delle reti

Dott. Tato Sánchez, Rafael

- Direttore Tecnico presso Indra Sistemas SA
- Ingegnere di Sistemi presso ENA TRÁFICO SAU
- Master in Industria 4.0. presso l'Università in Internet
- Master in Ingegneria Industriale presso l'Università Europea
- Laurea in Ingegneria Elettronica Industriale e Automatica presso l'Università Europea
- Ingegnere Tecnico Industriale presso l'Università Politecnica di Madrid

Dott.ssa Marcos Sbarbaro, Victoria Alicia

- Sviluppatrice di Applicazioni Mobili Native Android presso B60 Regno Unito
- Analista programmatore per la gestione, il coordinamento e la documentazione dell'ambiente di allarme di sicurezza virtualizzato
- Analista Programmatrice di applicazioni Java per ATM
- Esperta di Sviluppo di *Software* per Applicazioni per la Convalida della Firma e la Gestione dei Documenti
- Tecnico di Sistemi per la Migrazione delle Apparecchiature e per Gestione, Manutenzione e Formazione dei Dispositivi Mobili PDA
- Ingegnere Tecnico di Sistemi Informatici presso l'Università Aperta della Catalogna
- Master in Sicurezza Informatica e Hacking Etico Ufficiale EC- Council e CompTIA dalla Scuola Professionale di Nuove Tecnologie CICE

Dott. Catalá Barba, José Francisco

- Tecnico Elettronico Esperto di Cibersicurezza
- Sviluppatore di Applicazioni Mobile
- Tecnico Elettronico presso il Comando Intermedio del Ministero della Difesa della Spagna
- Tecnico Elettronico presso Factoría Ford Sita a Valencia

Dott. Armero Fernández, Rafael

- Business Intelligence Consultant presso SDG Group
- Digital Engineer presso MI-GSO
- Logistic Engineer presso Torrecid SA
- Quality Intern presso INDRA
- Laurea in Ingegneria Aerospaziale presso l'Università Politecnica di Valencia
- Master in Professional Development 4.0 conseguito presso l'Università di Alcalá

Dott. Peralta Alonso, Jon

- Consulente senior per la protezione dei dati e la cybersecurity presso Altia
- Avvocato / Consulente legale presso Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- Consulente legale/tirocinante presso uno studio legale professionale: Óscar Padura
- Laurea in Giurisprudenza presso l'Università Pubblica dei Paesi Baschi
- Master in Protezione dei dati personali conseguito presso la EIS Innovative School
- Master Universitario in Giurisprudenza presso l'Università Pubblica dei Paesi Baschi
- Master specialistico in pratica del contenzioso civile presso l'Università Internazionale Isabel I di Castiglia
- Docente del Master in Protezione dei dati personali, Cibersicurezza e Diritto delle TIC

Dott. Redondo, Jesús Serrano

- Sviluppatore Web e Tecnico di Cibersicurezza
- Sviluppatore Web presso Roams, Palencia
- Sviluppatore FrontEnd presso Telefónica, Madrid
- Sviluppatore FrontEnd presso Best Pro Consulting SL, Madrid
- Installatore di Apparecchiature e Servizi di Telecomunicazione presso il Grupo Zener, Castilla y León
- Installatore di Apparecchiature e Servizi di Telecomunicazione presso Lican Comunicaciones SL, Castilla y León
- Certificato in Sicurezza Informatica, CFTIC Getafe, Madrid
- Tecnico Superiore in Telecomunicazioni e Sistemi Informatici presso IES Trinidad Arroyo, Palencia
- Tecnico superiore in Installazioni Elettrotecniche MT e BT dell'IES Trinidad Arroyo, Palencia
- Preparazione al Reverse Engineering, alla Stenografia e alla Crittografia con Incibe Hacker Academy

Dott. Jiménez Ramos, Álvaro

- Analista di Cibersicurezza
- Analista Senior di Sicurezza presso The Workshop
- Analista di Cibersicurezza L1 presso Axians
- Analista di Cibersicurezza L2 presso Axians
- Analista di Cibersicurezza presso SACYR S.A.
- Laurea in Ingegneria Telematica presso l'Università Politecnica di Madrid
- Master in Cibersicurezza e Hacking Etico realizzato presso il CICE
- Corso avanzato di Cibersicurezza presso Deusto Formación

Cogli l'occasione per conoscere gli ultimi sviluppi in questo campo e applicarli alla tua pratica quotidiana"

08

Titolo

Il Master Specialistico in Secure Information Management garantisce, oltre alla preparazione più rigorosa e aggiornata, il conseguimento di una qualifica di Master Specialistico 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 **Master Specialistico in Secure Information Management** rilasciato da **TECH Global University**, la più grande università digitale del mondo.

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: **Master Specialistico in Secure Information Management**

Modalità: **online**

Durata: **2 anni**

Accreditamento: **120 ECTS**

tech global university

Dott. _____, con documento d'identità _____ ha superato con successo e ottenuto il titolo di:

Master Specialistico in Secure Information Management

Si tratta di un titolo di studio privato corrispondente a 3600 ore di durata equivalente a 120 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

Master Specialistico in Secure Information Management

Distribuzione generale del Programma

Corso	Insegnamento	ECTS	Codice
1°	Analitica dei dati nell'organizzazione aziendale	6	OB
1°	Gestione e manipolazione dei dati e delle informazioni per la Data Science	6	OB
1°	Dispositivi e piattaforme IoT come base per la Data Science	6	OB
1°	Rappresentazione grafica per l'analisi dei dati	6	OB
1°	Strumenti di Data Science	6	OB
1°	Data Mining: Selezione, pre-elaborazione e trasformazione	6	OB
1°	Prevedibilità e analisi dei fenomeni stocastici	6	OB
1°	Progettazione e sviluppo di sistemi intelligenti	6	OB
1°	Architetture e sistemi ad alta intensità di dati	6	OB
1°	Applicazione pratica della Data Science nei settori aziendali	6	OB

Corso	Insegnamento	ECTS	Codice
2°	Cyberintelligence e Cibersicurezza	6	OB
2°	Sicurezza in Host	6	OB
2°	Sicurezza di rete (perimetro)	6	OB
2°	Sicurezza degli smartphone	6	OB
2°	Sicurezza in IoT	6	OB
2°	Hacking etico	6	OB
2°	Ingegneria inversa	6	OB
2°	Sviluppo sicuro	6	OB
2°	Analisi forense	6	OB
2°	Le sfide attuali e future della sicurezza informatica	6	OB

Dott. Pedro Navarro Illana
Rettore

tech global university

*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

Master Specialistico
Secure Information Management

- Modalità: **online**
- Durata: **2 anni**
- Titolo: **TECH Global University**
- Accreditamento: **120 ECTS**
- Orario: **a tua scelta**
- Esami: **online**

Master Specialistico

Secure Information Management

tech global university