

Master Specialistico

Computer Science, Cybersecurity e Data Analytics



Master Specialistico Computer Science, Cybersecurity e Data Analytics

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

Accesso al sito web: www.techtitute.com/it/informatica/master-specialistico/master-specialistico-computer-science-cybersecurity-data-analytics



Indice

01

Presentazione

02

Obiettivi

pag. 4

pag. 8

03

Competenze

04

Direzione del corso

pag. 20

05

Struttura e contenuti

pag. 34

06

Metodologia

07

Titolo

pag. 62

pag. 70

01

Presentazione

Nel mondo di oggi, che si muove verso la completa digitalizzazione, i professionisti dell'IT devono mantenere le proprie competenze costantemente aggiornate per poter continuare ad operare nel proprio settore in modo ottimale, evitando di perdere le novità che si stanno imponendo a un ritmo incessante. L'emergere di nuovi sistemi di generazione di dati e informazioni è ormai fondamentale per lo sviluppo di molte industrie e individui. Sono sempre di più i processi basilari, le operazioni e i compiti di qualsiasi tipo che vengono portati a termine mediante un dispositivo elettronico. Ma questo progresso comporta anche alcuni rischi, poiché tutti i tipi di dispositivi e applicazioni digitali possono essere soggetti ad attacchi informatici. Per questo motivo, è stato ideato un programma 100% online che si concentra ad affrontare tutte le linee di conoscenza necessarie per l'elaborazione e l'estrazione dei dati, l'approccio alla Cybersecurity e l'approfondimento dell'Informatica, seguendo una prospettiva teorica e pratica.



66

Diventa esperto di cybersecurity grazie alla padronanza dell'informatica e dell'analisi dei dati, migliorando notevolmente la tua possibilità di impiego in un settore sempre più dinamico"

Sotto la spinta dei continui progressi dell'informatica, non solo la tecnologia ha goduto di grandi miglioramenti, ma lo stesso hanno fatto gli strumenti digitali con cui oggi si svolgono molte attività. L'altra faccia della medaglia è che questi progressi hanno portato anche a un aumento delle vulnerabilità informatiche. Per questo motivo, sempre più aziende sono alla ricerca di professionisti specializzati in Cybersecurity in grado di fornire loro un'adeguata protezione contro tutti i tipi di attacchi informatici.

Iscrivendosi a questo Master Specialistico, l'informatico potrà approfondire aspetti quali la sicurezza nello sviluppo e nella progettazione di sistemi, le migliori tecniche di crittografia e la sicurezza negli ambienti di *Cloud Computing*. Questo programma si concentra inoltre sui fondamenti della programmazione e della struttura dei dati, sull'algoritmica e sulla complessità, nonché sulla progettazione avanzata di algoritmi, sulla programmazione avanzata, sui processori di linguaggio e sulla grafica computerizzata. Il tutto, con numerose risorse didattiche multimediali, tenuto da un personale docente tra i più prestigiosi e specializzati del settore.

D'altra parte, questo programma affronta, da una prospettiva tecnica e aziendale, la scienza dei dati, offrendo tutte le conoscenze necessarie per l'estrazione della conoscenza nascosta in essi. Gli informatici potranno così analizzare in dettaglio i diversi algoritmi, piattaforme e strumenti all'avanguardia per l'esplorazione, la visualizzazione, la manipolazione, l'elaborazione e l'analisi dei dati. Tutto questo, completato dallo sviluppo di competenze commerciali, è necessario per raggiungere un profilo di livello esecutivo in grado di prendere decisioni chiave in un'azienda.

Questo percorso didattico fornisce quindi al professionista gli strumenti e le competenze specifiche per svolgere con successo la propria attività professionale nell'ampio contesto dell'informatica. Lavorando su competenze chiave come la conoscenza della realtà e della realtà quotidiana in diverse aree informatiche e sviluppando la responsabilità nel monitoraggio e nella supervisione del proprio lavoro, oltre a competenze specifiche in ogni campo.

Con questa qualifica, gli informatici potranno specializzarsi in Computer Science, Cybersecurity e Data Analytics, rappresentando l'opportunità perfetta per migliorare la propria carriera professionale. Tutto questo sarà possibile grazie a un programma 100% online, che si adatta alle esigenze quotidiane dei professionisti. Sarà sufficiente disporre di un dispositivo con connessione a Internet per iniziare a lavorare per ottenere un profilo professionale completo con proiezione internazionale.

Questo **Master Specialistico in Computer Science, Cybersecurity e Data Analytics** possiede il programma più completo e aggiornato del mercato. Le caratteristiche principali del programma sono:

- ◆ Lo sviluppo di casi di studio pratici presentati da esperti in campo Informatico
- ◆ 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
- ◆ La sua particolare enfasi sulle metodologie innovative in Cybersecurity e in Data Analytics
- ◆ Lezioni teoriche, domande all'esperto e/o al tutor, forum di discussione su questioni controverse e compiti di riflessione individuale
- ◆ Contenuti disponibili da qualsiasi dispositivo fisso o portatile provvisto di connessione a internet



In modo agevole e semplice, potrai acquisire le conoscenze necessarie in Computer Science, Cybersecurity e Data Analytics per realizzare una programmazione informatica di qualità

“

TECH mette al tuo servizio un materiale didattico ampio e preciso, che incorpora tutti gli argomenti di interesse attuale, in modo che tu possa continuare a progredire nel campo dell'informatica”

Il personale docente del programma comprende rinomati specialisti del settore dell'Informatica, che forniscono agli studenti le competenze necessarie a intraprendere un percorso di studio eccellente.

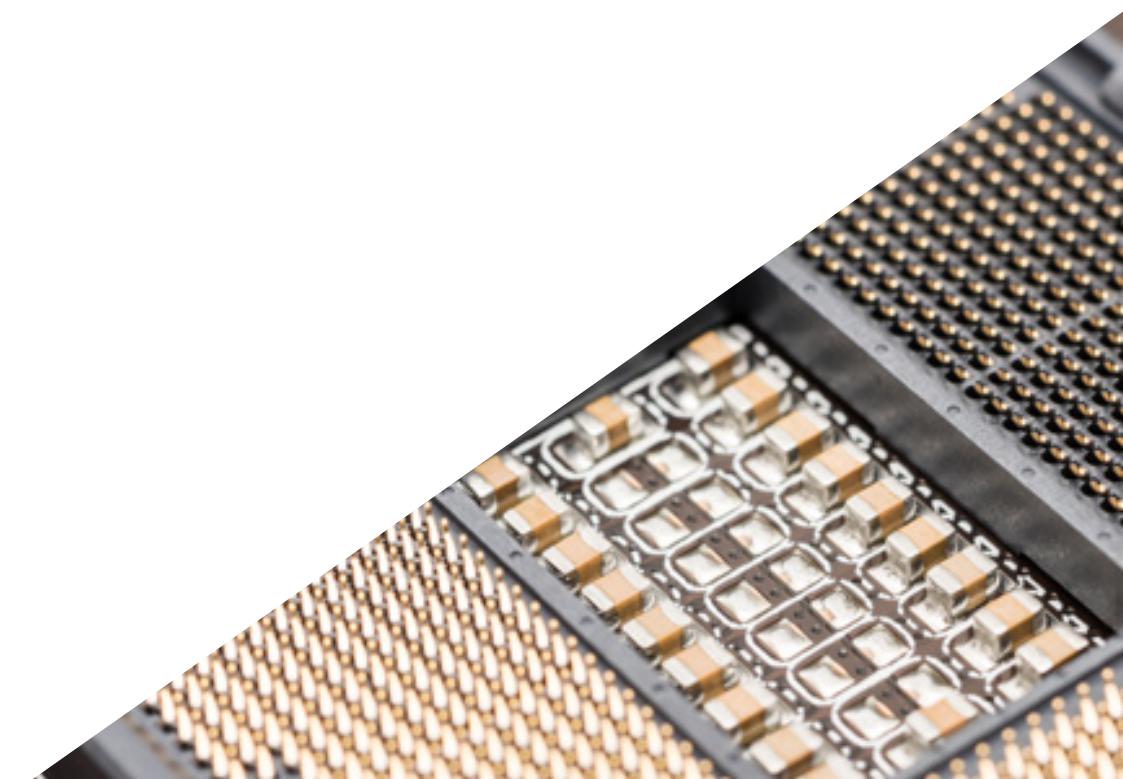
I contenuti multimediali, sviluppati in base alle ultime tecnologie educative, forniranno al professionista un apprendimento coinvolgente e localizzato, ovvero inserito in un contesto reale.

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.

Migliora a livello professionale determinando la creazione di dashboard e KPI in base al dipartimento in cui lavori.



Vieni a scoprire in prima persona le migliori tecniche di sicurezza applicate agli ambienti di Cloud Computing o alla tecnologia Blockchain.



02

Obiettivi

Il Master Specialistico in Computer Science, Cybersecurity e Data Analytics è stato creato appositamente per gli informatici che desiderano avanzare in questo campo in modo più rapido e con una reale qualità. Ecco perché è stato elaborato un programma basato su obiettivi realistici e di alto valore che ti faranno avanzare sul piano lavorativo. Il professionista si concentrerà sullo studio delle diverse tecniche, tecnologie e fasi necessarie all'informatica, in una prospettiva innovativa, completa e aggiornata.





66

TECH ti offre una qualifica di alta qualità che ti permetterà di intervenire con risolutezza nell'informatica, garantendo la sicurezza della tua azienda"



Obiettivi generali

- ◆ Essere aggiornati dal punto di vista scientifico e tecnologico, nonché prepararsi ad affrontare la pratica professionale dell'informatica e delle lingue in modo trasversale e versatile, adattandosi alle nuove tecnologie e alle innovazioni del settore
- ◆ Generare conoscenze specialistiche relative a un sistema informatico, ai tipi e agli aspetti della sicurezza da tenere in considerazione
- ◆ Identificare le debolezze di un sistema informatico
- ◆ Definire la regolamentazione giuridica e la perseguitabilità del delitto di attacco informatico
- ◆ Valutare diversi modelli di organizzazione della sicurezza per stabilire il modello più appropriato per l'azienda
- ◆ Identificare i quadri normativi applicabili e le relative basi normative
- ◆ Analizzare la struttura organizzativa e funzionale di un'area di sicurezza informatica (l'ufficio del CISO)
- ◆ Analizzare e sviluppare il concetto di rischio e incertezza nel contesto in cui viviamo
- ◆ Esaminare il modello di gestione del rischio basato sullo standard ISO 31.000
- ◆ Esaminare la scienza della crittologia e il rapporto con le sue aree: crittografia, crittoanalisi, steganografia e stegoanalisi
- ◆ Analizzare i tipi di crittografia in base al tipo di algoritmo e al suo utilizzo

- ◆ Esaminare i certificati digitali
- ◆ Analizzare l'infrastruttura a chiave pubblica (PKI)
- ◆ Sviluppare il concetto di gestione dell'identità
- ◆ Identificare i metodi di autenticazione
- ◆ Generare conoscenze specialistiche sull'ecosistema della sicurezza informatica
- ◆ Valutare le conoscenze di Cybersecurity
- ◆ Identificare le aree di sicurezza nel *Cloud*
- ◆ Analizzare i servizi e gli strumenti in ogni ambito di sicurezza
- ◆ Sviluppare le specifiche di sicurezza per ogni tecnologia LPWAN
- ◆ Paragonare la sicurezza delle tecnologie LPWAN
- ◆ Analizzare i vantaggi dell'applicazione delle tecniche di analisi di dati in ogni dipartimento dell'azienda
- ◆ Sviluppare le basi per comprendere le esigenze e le applicazioni di ogni dipartimento
- ◆ Generare conoscenze specialistiche per selezionare lo strumento corretto
- ◆ Proporre tecniche e obiettivi per essere il più produttivi possibile in base al dipartimento



Obiettivi specifici

Modulo 1. Fondamenti di programmazione

- ◆ Comprendere la struttura di base di un computer, il software e i linguaggi di programmazione di uso generale
- ◆ Imparare a progettare e interpretare gli algoritmi, che sono la base necessaria per lo sviluppo del software
- ◆ Comprendere gli elementi essenziali di un programma per computer, come i diversi tipi di dati, gli operatori, le indicazioni, le dichiarazioni, le istruzioni di I/O e di controllo
- ◆ Comprendere le diverse strutture dati disponibili nei linguaggi di programmazione generici, sia statici che dinamici, e acquisire le conoscenze essenziali sulla gestione dei file
- ◆ Comprendere le diverse tecniche di test del software e l'importanza di generare una buona documentazione insieme a un buon codice sorgente
- ◆ Imparare le basi del linguaggio di programmazione C++, uno dei linguaggi di programmazione più utilizzati al mondo

Modulo 2. Struttura dei Dati

- ◆ Imparare i fondamenti della programmazione in linguaggio C++, tra cui classi, variabili, espressioni condizionali e oggetti
- ◆ Comprendere i tipi di dati astratti, i tipi di strutture dati lineari, le strutture dati gerarchiche semplici e complesse e la loro implementazione in C++
- ◆ Comprendere il funzionamento di strutture dati avanzate diverse da quelle abituali
- ◆ Comprendere la teoria e la pratica relative all'uso di heap e code di priorità
- ◆ Imparare il funzionamento delle tabelle Hash, come i tipi di dati astratti e le funzioni
- ◆ Comprendere la teoria dei Grafi, gli algoritmi e i concetti avanzati dei Grafi

Modulo 3. Algoritmi e complessità

- ◆ Imparare le principali strategie per la progettazione di algoritmi, nonché i diversi metodi e misure per il loro calcolo
- ◆ Apprendere i principali algoritmi di ordinamento utilizzati nello sviluppo del software
- ◆ Capire come funzionano i diversi algoritmi ad albero, gli *Heaps* e i Grafi
- ◆ Comprendere il funzionamento degli algoritmi *Greedy*, la loro strategia e gli esempi del loro utilizzo nei principali problemi noti. Conoscere l'uso degli algoritmi *Greedy* sui Grafi
- ◆ Imparare le principali strategie di ricerca del cammino minimo, con l'approccio ai problemi essenziali del campo e agli algoritmi per la loro risoluzione
- ◆ Comprendere la tecnica del *Backtracking* e i suoi principali utilizzi, nonché altre tecniche alternative

Modulo 4. Progettazione avanzata degli algoritmi

- ◆ Approfondire la progettazione avanzata di algoritmi, analizzando algoritmi ricorsivi e divide et impera, nonché eseguendo analisi ammortizzate
- ◆ Comprendere i concetti di programmazione dinamica e gli algoritmi per i problemi NP
- ◆ Comprendere il funzionamento dell'ottimizzazione combinatoria, nonché i diversi algoritmi di randomizzazione e gli algoritmi paralleli
- ◆ Conoscere e comprendere il funzionamento dei diversi metodi di ricerca locali e candidati
- ◆ Imparare i meccanismi della verifica formale dei programmi e di quella iterativa, tra cui la logica del primo ordine e il sistema formale di Hoare
- ◆ Imparare il funzionamento di alcuni dei principali metodi numerici come il metodo di bisezione, di Newton - Raphson e il metodo della secante

Modulo 5. Programmazione avanzata

- ◆ Approfondire la conoscenza della programmazione, soprattutto in relazione alla programmazione orientata agli oggetti, e dei diversi tipi di relazioni tra classi esistenti
- ◆ Conoscere i diversi modelli di progettazione per i problemi orientati agli oggetti
- ◆ Imparare la programmazione guidata dagli eventi e lo sviluppo di *Interfaces* utente con Qt
- ◆ Acquisire le conoscenze essenziali della programmazione concorrente, dei processi e dei thread
- ◆ Imparare a gestire l'uso dei thread e della sincronizzazione, nonché a risolvere i problemi più comuni della programmazione concorrente
- ◆ Comprendere l'importanza della documentazione e dei test nello sviluppo del software

Modulo 6. Informatica teorica

- ◆ Comprendere i concetti matematici teorici essenziali alla base dell'Informatica, come la logica propositiva, la teoria dei set e i set numerabili e non numerabili
- ◆ Comprendere i concetti di linguaggi formali e grammatiche, nonché di macchine di Turing nelle loro diverse varianti
- ◆ Imparare a conoscere i diversi tipi di problemi indecidibili e intrattabili, comprese le diverse varianti di questi e i loro approcci
- ◆ Comprendere il funzionamento di diversi tipi di linguaggi basati sulla randomizzazione e di altri tipi di classi e grammatiche
- ◆ Conoscere altri sistemi di calcolo avanzati come il calcolo a membrana, il calcolo del DNA e il calcolo quantistico

Modulo 7. Teoria degli automi e linguaggi formali

- ◆ Comprendere la teoria degli automi e dei linguaggi formali, imparando i concetti di alfabeti, stringhe e linguaggi, nonché a eseguire dimostrazioni formali
- ◆ Approfondire la comprensione dei diversi tipi di automi finiti, deterministici o non deterministici
- ◆ Imparare i concetti di base e avanzati relativi ai linguaggi regolari e alle espressioni regolari, nonché l'applicazione del lemma di pompaggio e la chiusura dei linguaggi regolari
- ◆ Comprendere le grammatiche indipendenti dal contesto e il funzionamento degli automi a Pila
- ◆ Approfondire le forme normali, il lemma di pompaggio delle grammatiche indipendenti dal contesto e le proprietà dei linguaggi indipendenti dal contesto

Modulo 8. Processori linguistici

- ◆ Introdurre i concetti relativi al processo di compilazione e ai diversi tipi di analisi: lessicale, sintattica e semantica
- ◆ Conoscere il funzionamento di un analizzatore lessicale, la sua implementazione e il recupero degli errori
- ◆ Approfondire la conoscenza del parsing, sia top-down che bottom-up, ma con particolare attenzione ai diversi tipi di parser bottom-up
- ◆ Comprendere il funzionamento dei parser semantic, la tradizione della sintassi, la tabella dei simboli e i vari tipi
- ◆ Imparare i diversi meccanismi per la generazione di codice, sia in ambienti runtime che per la generazione di codice intermedio
- ◆ Gettare le basi dell'ottimizzazione del codice, compreso il riordino delle espressioni e l'ottimizzazione dei cicli

Modulo 9. Computer grafica e visualizzazione

- ◆ Introdurre i concetti essenziali della computer grafica e della visualizzazione al computer, come la teoria del colore e i suoi modelli e le proprietà della luce
- ◆ Comprendere il funzionamento delle primitive di output e dei loro algoritmi, sia per il disegno di linee che per il disegno di cerchi e riempimenti
- ◆ Approfondire le diverse trasformazioni 2D e 3D e i loro sistemi di coordinate e visualizzazione al computer
- ◆ Imparare a realizzare proiezioni e tagli 3D e a rimuovere le superfici nascoste
- ◆ Imparare la teoria relativa all'interpolazione e alle curve parametriche, nonché alle curve di Bézier e alle *B-Splines*

Modulo 10. Informatica bio-ispirata

- ◆ Introdurre il concetto di informatica bio-ispirata e comprendere il funzionamento dei diversi tipi di algoritmi di adattamento sociale e genetici
- ◆ Approfondire lo studio dei diversi modelli di calcolo evolutivo, conoscendone le strategie, la programmazione, gli algoritmi e i modelli basati sulla stima delle distribuzioni
- ◆ Comprendere le principali strategie di esplorazione-sfruttamento dello spazio per gli algoritmi genetici
- ◆ Comprendere il funzionamento della programmazione evolutiva applicata a problemi di apprendimento e a problemi multi-obiettivo
- ◆ Imparare i concetti essenziali relativi alle reti neurali e comprendere il funzionamento di casi d'uso reali applicati ad aree diverse come la ricerca medica, l'economia e la visione artificiale

Modulo 11. Sicurezza nella progettazione e nello sviluppo dei sistemi

- ◆ Valutare la sicurezza di un sistema informatico in tutti i suoi componenti e livelli
- ◆ Identificare i tipi di minacce alla sicurezza attualmente esistenti e le loro tendenze
- ◆ Stabilire le linee guida per la sicurezza definendo politiche, strategie e piani di sicurezza e contingenza
- ◆ Analizzare le strategie e gli strumenti per garantire l'integrità e la sicurezza dei sistemi informatici
- ◆ Applicare le tecniche e gli strumenti specifici per ogni tipo di attacco o violazione della sicurezza
- ◆ Proteggere le informazioni sensibili memorizzate nel sistema informatico
- ◆ Disporre del quadro giuridico e della caratterizzazione del reato, integrando la visione con la tipologia del reo e della sua vittima

Modulo 12. Strutture e modelli per la sicurezza delle informazioni

- ◆ Allineare il Master Plan per la Sicurezza agli obiettivi strategici dell'organizzazione
- ◆ Stabilire un quadro di gestione costante dei rischi come parte integrante del Master Plan sulla sicurezza
- ◆ Stabilire gli indicatori appropriati per il monitoraggio della messa in atto del SGSI
- ◆ Stabilire una strategia di sicurezza basata sulle policy
- ◆ Analizzare gli obiettivi e le procedure associate al piano di sensibilizzazione dei dipendenti, dei fornitori e dei partner
- ◆ Identificare, all'interno del quadro normativo, i regolamenti, le certificazioni e le leggi applicabili a ciascuna organizzazione
- ◆ Definire gli elementi fondamentali richiesti dallo standard ISO 27001:2013
- ◆ Implementare un modello di gestione della privacy in linea con il regolamento europeo GDPR/RGPD



Modulo 13. Gestione della sicurezza IT

- ◆ Identificare le diverse componenti che un'area di sicurezza informatica può presentare
- ◆ Sviluppare un modello di sicurezza basato su tre linee di difesa
- ◆ Presentare i diversi comitati periodici e straordinari in cui è coinvolta l'area della Cybersecurity
- ◆ Definire gli strumenti tecnologici che integrano le funzioni principali del team operativo di sicurezza (SOC)
- ◆ Valutare le misure di controllo dei punti di vulnerabilità appropriate per ogni scenario
- ◆ Sviluppare un quadro operativo per la sicurezza basato sul NIST CSF
- ◆ Specificare l'ambito di applicazione dei diversi tipi di audit (*RedTeam, Pentesting, Bug Bounty, ecc.*)
- ◆ Proporre le attività da svolgere dopo un incidente che coinvolge la sicurezza
- ◆ Creare un centro di comando per la sicurezza delle informazioni che comprenda tutti i soggetti interessati (autorità, clienti, fornitori, ecc.)

Modulo 14. Analisi dei rischi e ambiente di Sicurezza IT

- ◆ Esaminare, secondo una visione globale, il contesto in cui si opera
- ◆ Identificare i principali rischi e opportunità che possono influire sul raggiungimento degli obiettivi
- ◆ Analizzare i rischi sulla base delle migliori procedure a disposizione
- ◆ Valutare l'impatto potenziale di tali rischi e opportunità
- ◆ Sviluppare tecniche che ci consentano di affrontare i rischi e le opportunità in modo da massimizzare il nostro contributo di valore
- ◆ Approfondire le diverse tecniche di trasferimento del rischio e del valore

- ◆ Generare valore dalla progettazione di modelli specifici per la gestione agile del rischio
- ◆ Esaminare i risultati per proporre miglioramenti nella gestione dei progetti e dei processi fondati su modelli di gestione del rischio o *Risk-Driven*
- ◆ Innovare e trasformare i dati generali in informazioni rilevanti per il processo decisionale basato sul rischio

Modulo 15. La crittografia nell'IT

- ◆ Conoscere le operazioni fondamentali (XOR, grandi numeri, sostituzione e trasposizione) e i vari componenti (funzioni *One-Way*, *Hash*, generatori di numeri casuali)
- ◆ Analizzare le tecniche crittografiche
- ◆ Sviluppare i diversi algoritmi crittografici
- ◆ Dimostrare l'uso delle firme digitali e la loro applicazione nei certificati digitali
- ◆ Valutare i sistemi di gestione delle crittografie e l'importanza della lunghezza delle chiavi crittografiche
- ◆ Esaminare gli algoritmi di derivazione delle chiavi crittografiche
- ◆ Analizzare il ciclo di vita delle chiavi crittografiche
- ◆ Valutare le modalità di cifratura a blocchi e di cifratura a flusso
- ◆ Determinare i generatori di numeri pseudorandom
- ◆ Sviluppare casi reali di applicazioni crittografiche, come Kerberos, PGP o smart card
- ◆ Esaminare associazioni e organismi correlati, come ISO, NIST o NCSC
- ◆ Individuare gli ostacoli nella crittografia dell'informatica quantistica

Modulo 16. Gestione dell'identità e degli accessi nella sicurezza informatica

- ◆ Sviluppare il concetto di identità digitale
- ◆ Valutare il controllo dell'accesso fisico alle informazioni
- ◆ Giustificare l'autenticazione biometrica e l'autenticazione MFA
- ◆ Valutare gli attacchi legati alla confidenzialità delle informazioni
- ◆ Analizzare la federazione di identità
- ◆ Stabilire il controllo dell'accesso alla rete

Modulo 17. Sicurezza nelle comunicazioni e nel funzionamento del software

- ◆ Sviluppare competenze in materia di sicurezza fisica e logica
- ◆ Dimostrare la conoscenza delle comunicazioni e delle reti
- ◆ Identificare i principali attacchi dannosi
- ◆ Stabilire un quadro di sviluppo sicuro
- ◆ Dimostrare di conoscere le principali normative sui sistemi di gestione della sicurezza informatica
- ◆ Stabilire il funzionamento di un centro operativo per la Cybersecurity
- ◆ Dimostrare l'importanza delle pratiche di sicurezza informatica per i disastri organizzativi

Modulo 18. Sicurezza in ambienti cloud

- ◆ Identificare i rischi di installazione di un'infrastruttura in un *cloud* pubblico
- ◆ Definire i requisiti di sicurezza
- ◆ Stabilire un piano di sicurezza per l'implementazione in *cloud*
- ◆ Identificare i servizi *cloud* da implementare per la realizzazione di un piano di sicurezza
- ◆ Determinare le misure operative necessarie per i meccanismi di prevenzione
- ◆ Stabilire le Linee Guida per un sistema di *Logging* e per il monitoraggio
- ◆ Proporre interventi di risposta agli incidenti

Modulo 19. Sicurezza delle comunicazioni nei dispositivi IoT

- ◆ Introdurre l'architettura IoT semplificata
- ◆ Spiegare le differenze tra le tecnologie di connettività generaliste e le tecnologie di connettività per l'IoT
- ◆ Stabilire il concetto di triangolo di ferro della connettività IoT
- ◆ Analizzare le specifiche di sicurezza della tecnologia LoRaWAN, NB-IoT e WiSUN
- ◆ Motivare la scelta della giusta tecnologia IoT per ogni progetto

Modulo 20. Piano di continuità operativa associato alla sicurezza

- ◆ Presentare gli elementi chiave di ciascuna fase e analizzare le caratteristiche del piano di continuità operativa (BCP)
- ◆ Giustificare la necessità di un piano di continuità operativa
- ◆ Stabilire le mappe di successo e di rischio per ogni fase del piano di continuità operativa
- ◆ Specificare come viene stabilito un piano d'intervento per la realizzazione del BCP
- ◆ Valutare la completezza di un Piano di Continuità Operativa (BCP)
- ◆ Sviluppare l'implementazione di un piano di continuità operativa

Modulo 21. Data Analytics nell'organizzazione aziendale

- ◆ Sviluppare capacità analitiche per prendere decisioni di qualità
- ◆ Esaminare campagne di marketing e comunicazione efficaci
- ◆ Determinare la Creazione di dashboard e KPI in base al dipartimento
- ◆ Generare conoscenze specialistiche per sviluppare analisi predittive
- ◆ Proporre piani commerciali e di fidelizzazione basati su ricerche di mercato
- ◆ Sviluppare la capacità di ascoltare il cliente
- ◆ Applicare conoscenze statistiche, quantitative e tecniche in situazioni reali

Modulo 22. Gestione e manipolazione dei Dati e delle informazioni per la Data Science

- ◆ Eseguire l'Analisi di Dati
- ◆ Unificare dati diversi: ottenere la coerenza delle informazioni
- ◆ Produrre informazioni pertinenti ed efficaci per il processo decisionale
- ◆ Determinare le migliori pratiche per la gestione dei dati in base alla loro tipologia e ai loro usi
- ◆ Definire politiche di accesso e riutilizzo dei dati
- ◆ Garantire la sicurezza e l'accesso: disponibilità, integrità e riservatezza delle informazioni
- ◆ Esaminare gli strumenti per la gestione dei dati utilizzando i linguaggi di programmazione

Modulo 23. Dispositivi e piattaforme IoT come base per la Data Science

- ◆ Identificare cosa è IoT (*Internet of Things*) e IIoT (*Industrial Internet of Things*)
- ◆ Esaminare il consorzio di internet industriale
- ◆ Analizzare l'architettura di riferimento di IoT
- ◆ Affrontare i sensori e i dispositivi IoT e la loro classificazione
- ◆ Identificare i protocolli e le tecnologie di comunicazione utilizzati in IoT
- ◆ Esaminare le diverse piattaforme *Cloud* in IoT: scopo generale, industriale, open source
- ◆ Sviluppare meccanismi di scambio di Dati
- ◆ Stabilire i requisiti e le strategie di sicurezza
- ◆ Presentare le diverse aree di applicazione di IoT e IIoT

Modulo 24. Rappresentazione grafica per l'analisi dei Dati

- ◆ Generare competenze nella rappresentazione e nell'analisi dei dati
- ◆ Esaminare i diversi tipi di dati raggruppati
- ◆ Stabilire le rappresentazioni grafiche più comunemente utilizzate in diversi campi
- ◆ Determinare i principi di progettazione nella visualizzazione dei dati
- ◆ Presentare la narrazione grafica come strumento
- ◆ Analizzare i diversi strumenti software per l'analisi dei dati grafici ed esplorativi

Modulo 25. Strumenti di Data science

- ◆ Sviluppare le capacità di convertire i dati in informazioni da cui estrarre conoscenza
- ◆ Determinare le caratteristiche principali di un *Dataset*, la sua struttura, i suoi componenti e le implicazioni della sua distribuzione nella modellistica
- ◆ Fornire supporto al processo decisionale attraverso un'analisi preventiva e approfondita dei dati
- ◆ Sviluppare le competenze per risolvere casi pratici utilizzando le tecniche della data science
- ◆ Stabilire gli strumenti e i metodi generali più appropriati per la modellazione di ciascun *Dataset* a seconda della pre-elaborazione effettuata
- ◆ Valutare i risultati in modo analitico, comprendendo l'impatto della strategia scelta su diverse metriche
- ◆ Dimostrare una capacità critica dei risultati ottenuti dopo l'applicazione di metodi di pre-elaborazione o modellazione

Modulo 26. Data Mining. Selezione, pre-elaborazione e trasformazione

- ◆ Generare conoscenze specialistiche sui prerequisiti statistici per qualsiasi analisi e valutazione dei dati
- ◆ Sviluppare le competenze necessarie per l'identificazione, la preparazione e la trasformazione dei dati
- ◆ Valutare le diverse metodologie presentate e identificare vantaggi e svantaggi
- ◆ Esaminare i problemi in ambienti di dati ad alta dimensionalità
- ◆ Sviluppare l'implementazione degli algoritmi utilizzati per la pre-elaborazione dei dati
- ◆ Dimostrare la capacità di interpretare le visualizzazioni dei dati per l'analisi descrittiva
- ◆ Sviluppare una conoscenza avanzata delle diverse tecniche di preparazione dei dati esistenti per la pulizia, la normalizzazione e la trasformazione dei dati

Modulo 27. Prevedibilità e analisi dei fenomeni stocastici

- ◆ Analizzare le serie temporali
- ◆ Sviluppare la formulazione e le proprietà di base dei modelli di serie temporali univariate
- ◆ Esaminare la metodologia di modellazione e previsione delle serie temporali reali
- ◆ Determinare i modelli univariati includendo gli atipici
- ◆ Applicare modelli di regressione dinamica e applicare la metodologia di costruzione di tali modelli a partire da serie osservate
- ◆ Affrontare l'analisi spettrale delle serie temporali univariate, nonché gli aspetti fondamentali relativi all'inferenza basata sui periodogrammi e alla loro interpretazione
- ◆ Stimare la probabilità e la tendenza di una serie temporale per un determinato orizzonte temporale

Modulo 28. Progettazione e sviluppo di sistemi intelligenti

- ◆ Analizzare il passaggio dall'informazione alla conoscenza
- ◆ Sviluppare i diversi tipi di tecniche di apprendimento automatico
- ◆ Esaminare metriche e punteggi per quantificare la qualità dei modelli
- ◆ Implementare i diversi algoritmi di apprendimento automatico
- ◆ Identificare i modelli di ragionamento probabilistico
- ◆ Gettare le basi per l'apprendimento profondo
- ◆ Dimostrare le competenze acquisite per comprendere i diversi algoritmi di apprendimento automatico

Modulo 29. Architetture e sistemi ad alta intensità di dati

- ◆ Determinare i requisiti per i sistemi di utilizzo dei dati di massa
- ◆ Esaminare diversi modelli di dati e analizzare i database
- ◆ Analizzare le funzionalità chiave dei sistemi distribuiti e la loro importanza in diversi tipi di sistemi
- ◆ Valutare quali applicazioni di largo uso utilizzano i fondamenti dei sistemi distribuiti per progettare i loro sistemi
- ◆ Analizzare il modo in cui i database memorizzano e recuperano le informazioni
- ◆ Specificare i diversi modelli di replica e i problemi associati
- ◆ Sviluppare forme di partizionamento e transazioni distribuite
- ◆ Determinare i sistemi batch e i sistemi (quasi) in tempo reale

Modulo 30. Applicazione pratica della data science nei settori aziendali

- ◆ Analizzare lo stato dell'arte dell'intelligenza artificiale (AI) e dell'analisi di dati
- ◆ Sviluppare una conoscenza specializzata sulle tecnologie più utilizzate
- ◆ Generare una migliore comprensione della tecnologia attraverso i casi d'uso
- ◆ Analizzare le strategie scelte per selezionare le migliori tecnologie da implementare
- ◆ Determinare le aree di applicazione
- ◆ Esaminare i rischi reali e potenziali della tecnologia applicata
- ◆ Proporre i benefici derivanti dall'utilizzo
- ◆ Identificare le tendenze future in settori specifici



Raggiungi l'eccellenza portando a termine un programma che ti consentirà di acquisire conoscenze specialistiche in Computer Science, Cybersecurity e Data Analytics"

03

Competenze

Dopo aver superato le valutazioni di questo programma, l'informatico avrà acquisito le competenze necessarie per comprendere i principi fondamentali dell'informatica e la capacità di lavorare con linguaggi di programmazione e dati. Questo ti permetterà di ambire a una crescita professionale quotidiana in quest'area di specializzazione, diventando un'opportunità in grado di offrire conoscenze preziose al momento di prendere decisioni in merito al funzionamento dei dipartimenti di un'azienda.



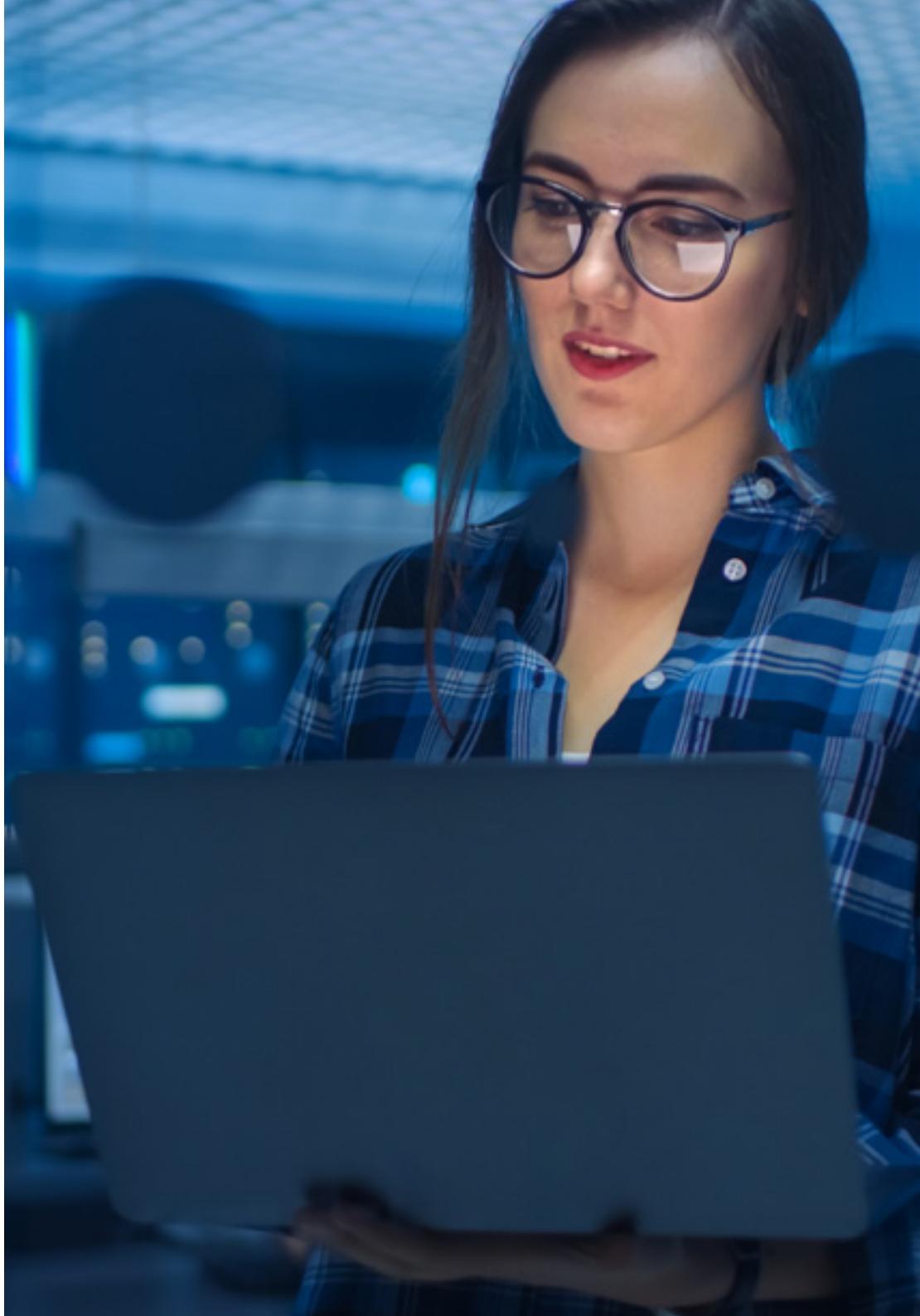
66

Acquisisci le competenze necessarie per avanzare a livello professionale, grazie a questo Master Specialistico che ti permetterà di tenerti aggiornato e di adattarti al nuovo ambiente informatico"



Competenze generali

- ◆ Eseguire correttamente il lavoro relativo ai computer e al linguaggio informatico
- ◆ Applicare le misure di sicurezza più appropriate in base alle minacce
- ◆ Determinare la politica e il piano di sicurezza del sistema informatico di un'azienda, ultimando la progettazione e l'implementazione del piano di contingenza
- ◆ Stabilire un programma di audit che soddisfi le esigenze di autovalutazione della sicurezza informatica all'interno dell'organizzazione
- ◆ Sviluppare un programma di analisi e monitoraggio dei punti di vulnerabilità e un piano di risposta agli incidenti di Cybersecurity
- ◆ Massimizzare le opportunità che si presentano ed eliminare l'esposizione a tutti i rischi potenziali derivanti dalla progettazione stessa
- ◆ Redigere sistemi di gestione delle chiavi
- ◆ Valutare la sicurezza informatica di un'azienda
- ◆ Analizzare i sistemi di accesso alle informazioni
- ◆ Definire le migliori pratiche per uno sviluppo sicuro
- ◆ Presentare i rischi che le aziende corrono se non dispongono di un ambiente di sicurezza informatica
- ◆ Sviluppare una prospettiva tecnica e aziendale sull'analisi dei dati
- ◆ Comprendere i più recenti algoritmi, piattaforme e strumenti per l'esplorazione, la visualizzazione, la manipolazione, l'elaborazione e l'analisi dei dati
- ◆ Implementare una visione aziendale necessaria per la valorizzazione come elemento chiave per il processo decisionale
- ◆ Essere in grado di affrontare i problemi specifici dell'analisi di dati





Competenze specifiche

- ◆ Progettare algoritmi per sviluppare programmi informatici e applicare il linguaggio di programmazione
- ◆ Comprendere e utilizzare la struttura dei dati informatici
- ◆ Utilizzare gli algoritmi necessari per risolvere i problemi informatici
- ◆ Conoscere a fondo la progettazione di algoritmi avanzati e i metodi di ricerca
- ◆ Eseguire compiti di programmazione informatica
- ◆ Comprendere e applicare la teoria alla base dell'informatica, come la matematica
- ◆ Conoscere la teoria degli automi e applicare il linguaggio informatico
- ◆ Conoscere le basi teoriche dei linguaggi di programmazione e le relative tecniche di elaborazione lessicale, sintattica e semantica
- ◆ Comprendere i concetti di base della matematica e della complessità computazionale per applicarli alla risoluzione di problemi computazionali
- ◆ Conoscere e applicare i principi fondamentali dell'informatica per realizzare nuovi sviluppi informatici
- ◆ Sviluppare un Sistema di Gestione della Sicurezza delle Informazioni (SGSI)
- ◆ Identificare gli elementi chiave che compongono un SGSI
- ◆ Applicare la metodologia MAGERIT per perfezionare il modello e progredire ulteriormente
- ◆ Progettare nuove metodologie di gestione del rischio basate sul concetto di *Agile Risk Management*
- ◆ Identificare, analizzare, valutare e gestire i rischi che il professionista deve affrontare da una nuova prospettiva aziendale basata su un modello *Risk-Driven* che permette non solo di sopravvivere nel proprio ambiente professionale, ma anche di apportare valore
- ◆ Esaminare il processo di progettazione di una strategia di sicurezza per l'implementazione in azienda di servizi *Cloud*

- ◆ Valutare le differenze nelle implementazioni concrete dei diversi fornitori di *Cloud* pubblico
- ◆ Valutare le opzioni di connettività IoT per realizzare un progetto, con particolare attenzione alle tecnologie LPWAN
- ◆ Presentare le specifiche di base delle principali tecnologie LPWAN per l'IoT
- ◆ Specializzarsi in *Data Science* da una prospettiva tecnica e di business
- ◆ Visualizzare i dati nel modo più appropriato per facilitare la condivisione e la comprensione da parte di diversi profili
- ◆ Affrontare le aree funzionali chiave dell'organizzazione in cui la scienza dei dati può apportare il massimo valore
- ◆ Sviluppare il ciclo di vita dei dati, la loro tipologia e le tecnologie e le fasi necessarie per la loro gestione
- ◆ Elaborare e manipolare i dati utilizzando linguaggi e librerie specifiche
- ◆ Sviluppare una conoscenza avanzata delle tecniche fondamentali di Data Mining per la selezione, la pre-elaborazione e la trasformazione dei dati
- ◆ Specializzarsi sui principali algoritmi di *Machine Learning* per estrarre la conoscenza nascosta dai dati
- ◆ Generare competenze sulle architetture e sui sistemi software necessari per l'uso intensivo dei dati
- ◆ Determinare come l'IoT possa essere una fonte di generazione di dati e informazioni chiave su cui applicare la *Data Science* per l'estrazione della conoscenza
- ◆ Analizzare i diversi modi di applicare la *Data Science* in diversi settori o verticali, imparando da esempi reali

04

Direzione del corso

Affrontare con successo il campo della Computer Science, della Cybersecurity e della Data Analytics richiede una comprensione approfondita e dettagliata della materia. È per questo motivo che TECH ha deciso di selezionare il miglior personale docente del settore. Gli informatici possono così contare sul supporto di professionisti rinomati che mettono a disposizione la loro pluriennale esperienza e preparazione. Gli informatici possono così avere la certezza di ricevere conoscenze aggiornate e specifiche su un settore in forte espansione a livello internazionale.



66

Potrai godere della guida e della supervisione di un personale docente costantemente aggiornato sugli ultimi sviluppi in materia di Cybersecurity e Data Analytics"

Direttore ospite internazionale

Il Dott. Jeremy Gibbons è considerato un'eminenza internazionale per i suoi contributi nel campo della **Metodologia di Programmazione** e le sue applicazioni in **Ingegneria del Software**. Per oltre due decenni, questo esperto associato al Dipartimento di Informatica dell'Università di Oxford ha promosso diversi progetti di sviluppo i cui risultati più tangibili sono applicati da informatici provenienti da varie parti del mondo.

Il suo lavoro copre aree come la **programmazione generica**, i metodi formali, la biologia computazionale, la bioinformatica e la progettazione di algoritmi con Haskell. Quest'ultimo argomento è stato ampiamente sviluppato insieme al suo mentore, il dottor Richard Bird.

Dal suo ruolo di **Direttore del Gruppo di Ricerca in Algebra di Programmazione**, Gibbons ha portato avanti i **Linguaggi di Programmazione Funzionale** e la **Teoria dei Modelli in Programmazione**. Allo stesso tempo, le applicazioni delle sue innovazioni sono state collegate al quadro sanitario, come dimostra la sua collaborazione con **CancerGrid** e **Datatype-Generic Programming**. A loro volta, queste e altre iniziative riflettono il tuo interesse per risolvere problemi pratici nella **ricerca sul cancro** e nell'**informatica clinica**.

Gibbons ha anche lasciato un'impronta significativa come **redattore capo** delle **pubblicazioni accademiche** in *The Journal of Functional Programming* e *The Programming Journal: The Art, Science, and Engineering of Programming*. Attraverso queste responsabilità ha svolto un intenso lavoro di **divulgazione e diffusione della conoscenza**. Inoltre, ha diretto diverse cattedre di studio collegate a istituzioni rinomate come l'Università di Oxford Brookes e l'Università di Auckland, in Nuova Zelanda.

D'altra parte, questo specialista è membro del gruppo di lavoro 2.1 sui linguaggi algoritmici e i calcoli della **Federazione internazionale per l'elaborazione delle informazioni (IFIP)**. Con questa organizzazione offre la manutenzione dei linguaggi di programmazione ALGOL 60 e ALGOL 68.



Dott. Gibbons, Jeremy

- Direttore del programma di ingegneria del software presso l'Università di Oxford, Regno Unito
- Vicedirettore del Laboratorio di Informatica e Dipartimento di Informatica dell'Università di Oxford
- Professore al Kellogg College, all'Università di Oxford Brookes e all'Università di Auckland della Nuova Zelanda
- Direttore del gruppo di ricerca algebra della programmazione
- Redattore capo delle riviste The Art, Science, and Engineering of Programming e Journal of Functional Programming
- Dottorato in scienze informatiche al l'Università di Oxford
- Laurea in informatica al l'Università di Edimburgo
- Membro di: Gruppo di lavoro 2.1 sui linguaggi algoritmici e i calcoli della Federazione internazionale per l'elaborazione delle informazioni (IFIP)

“

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

Direzione

**Dott. Olalla Bonal, Martín**

- Tecnico specialista in *Blockchain* su IBM SPGI
- Specialista di vendite tecniche in *Blockchain*. IBM
- Direttore di Architettura. *Blocknitive*
- Tecnico di elettronica digitale
- *Blockchain Architect -IT Infrastructure Architect* - Gestore di progetti IT. Aree di attività: Software, Infrastrutture, Telecomunicazioni

**Dott. Peralta Martín-Palomino, Arturo**

- CEO e CTO presso Prometheus Global Solutions
- CTO presso Korporate Technologies
- CTO presso Al Shephers GmbH
- Dottorato in Ingegneria Informatica conseguito presso l'Università di Castiglia La Mancia
- Dottorato in Economia Aziendale e Finanze conseguito presso l'Università Camilo José Cela Premio di Eccellenza del Dottorato
- Dottorato in Psicologia conseguito presso l'Università di Castiglia La Mancia
- Master in Tecnologie Informatiche Avanzate conseguito presso l'Università di Castiglia La Mancia
- Master MBA+E (Master in Amministrazione Aziendale e Ingegneria Organizzativa) conseguito presso l'Università di Castiglia La Mancia
- Professore associato nel corso di Laurea e Master in Ingegneria Informatica dell'Università di Castiglia La Mancia
- Professore del Master in Big Data e Data Science presso l'Università Internazionale di Valencia
- Professore del Master in Industria 4.0 e Master in Industrial Design e Sviluppo di prodotti
- Membro del Gruppo di Ricerca SMILe dell'Università di Castiglia La Mancia

Personale docente

Dott. Tobal Redondo, Javier

- ◆ Responsabile del programma di innovazione per le applicazioni di HUAWEI
- ◆ Responsabile della sicurezza informatica presso il dipartimento dei mezzi di pagamento. Amadeus IT Group
- ◆ Capo della sicurezza informatica presso FINTONIC, Servizi Finanziari
- ◆ Ingegnere dei servizi e architetto nell'area di Pianificazione e Architettura dei servizi e della sicurezza presso Amena / Orange Spagna
- ◆ Laurea in Informatica conseguita presso l'Università di Deusto, a Bilbao, in Spagna
- ◆ Studi post-laurea in Informatica Industriale. Scuola di Ingegneria Industriale. Bilbao

Dott. Gonzalo Alonso, Félix

- ◆ Direttore generale e fondatore. Smart REM Solutions
- ◆ Socio fondatore e responsabile dell'Ingegneria dei rischi e dell'Innovazione. Dynargy
- ◆ Direttore generale e socio fondatore. Risknova (Società di consulenza specializzata in tecnologia)
- ◆ Laurea in Ingegneria dell'Organizzazione Industriale conseguita presso l'Università Pontificia di Comillas ICAI
- ◆ Laurea in Ingegneria tecnica industriale con specialità in Elettronica Industriale conseguita presso l'Università Pontificia di Comillas ICAI
- ◆ Master in Direzione delle Assicurazioni conseguito presso ICEA (Istituto per la Collaborazione tra le Imprese di Assicurazione)

Dott. Sevillano Izquierdo, Javier

- ◆ Global Cyber Security Architect presso Vodafone Spagna
- ◆ Chief Technology Security Office (CTSO) presso Vodafone Spagna
- ◆ Responsabile della Sicurezza Tecnologica presso Bankia
- ◆ Responsabile della Sicurezza Tecnologica presso Caja Madrid
- ◆ Manager della Sicurezza del Sistema 4B
- ◆ Analista senior presso SEINCA
- ◆ Tecnico superiore in Informatica Aziendale proveniente dall'istituto Cibernos

Dott. Entrenas, Alejandro

- ◆ Entelgy Innotec
- ◆ Laurea in Ingegneria Tecnica dei Sistemi Informatici conseguita presso l'Università di Cordova
- ◆ Master in Gestione e Amministrazione della Sicurezza Informatica conseguito presso l'Università Politecnica di Madrid

Dott. Nogales Ávila, Javier

- ◆ Enterprise Cloud and sourcing senior consultant. Quint
- ◆ Cloud and Technology Consultant. Indra
- ◆ Associate Technology Consultant. Accenture
- ◆ Laurea dell'Università di Jaen e della University of Technology and Economics of Budapest (BME)
- ◆ Laurea in Ingegneria dell'Organizzazione Industriale

Dott. Gómez Rodríguez, Antonio

- ◆ Ingegnere delle soluzioni Cloud in Oracle
- ◆ Direttore di Progetti presso Sopra Group
- ◆ Direttore di Progetti presso Everis
- ◆ Project Manager presso la Società pubblica per la Gestione di Programmi Culturali del Consiglio della Cultura dell'Andalucia
- ◆ Analista di Sistemi Informatici presso Sopra Group
- ◆ Laurea in Ingegneria delle Telecomunicazioni conseguita presso l'Università Politecnica della Catalogna
- ◆ Studi post-laurea sulle Tecnologie e i Sistemi Informatici svolti presso l'Istituto Catalano di Tecnologia
- ◆ E-Business Master conseguito presso la Business School di La Salle

Dott. del Valle Arias, Jorge

- ◆ Direttore della Sezione IoT presso Diode Spagna
- ◆ Smart Cities Business Growth Manager Spain presso Itron Inc
- ◆ Consulente IoT
- ◆ Sales Manager IoT & Celular presso Aicox Soluciones
- ◆ Fondatore e CEO di Sensor Intelligence
- ◆ Direttore Operativo di Codium Networks
- ◆ Capo della Sezione di Elettronica di Aitemin
- ◆ Ingegnere delle Telecomunicazioni dell'Università Politecnica di Madrid
- ◆ Executive MBA conseguito presso l'International Graduate School di La Salle a Madrid

Dott. Gozalo Fernández, Juan Luis

- ◆ Ingegnere informatico
- ◆ Docente Associato di DevOps e Blockchain presso l'UNIR
- ◆ Ex-direttore Blockchain DevOps presso Alastria
- ◆ Direttore per lo Sviluppo dell'Applicazione Mobile di Tinkerlink presso Cronos Telecom
- ◆ Direttore IT del Banco Santander
- ◆ Direttore della Tecnologia di Gestione dei Servizi IT presso Barclays Bank Spagna
- ◆ Laurea in Ingegneria Informatica conseguita presso l'Università Nazionale di Educazione a Distanza (UNED)

Dott.ssa Jurado Jabonero, Lorena

- ◆ Responsabile della Sicurezza Informatica (CISO) presso Grupo Pascual
- ◆ Laurea in Ingegneria Informatica conseguita presso l'Università Alfonso X El Sabio
- ◆ Ingegnere Tecnica in Gestione Informatica proveniente dall'Università Politecnica di Madrid
- ◆ Conoscenze: ISO 27001, ISO 27701, ISO 22301, ISO 20000, RGPD/LOPDGDD, NIST CSF, CSA, ITIL, PCI, ecc.

Dott. Armero Fernández, Rafael

- ◆ Business Intelligence Consultant presso SDG Group
- ◆ Digital Engineer presso Mi-GSO
- ◆ Logistic Engineer presso Torrecid S.A.
- ◆ Quality Intern presso INDRA
- ◆ Laurea in Ingegneria Aerospaziale conseguita presso l'Università Politecnica di Valencia
- ◆ Master in Professional Development 4.0 conseguito presso l'Università di Alcalá de Henares

Dott. Peris Morillo, Luis Javier

- ◆ Technical Lead presso Capitole Consulting Leader di un team presso Inditex nell'unità di logistica della sua piattaforma aperta
- ◆ Senior Technical Lead e Delivery Lead Support presso HCL
- ◆ Agile Coach e Direttore di Operazioni presso Mirai Advisory
- ◆ Membro e Direttore Operativo della commissione di direzione e qualità
- ◆ Sviluppatore, Team Lead, Scrum Master, Agile Coach, Product Manager presso DocPath
- ◆ Ingegnere Superiore in Informatica proveniente dalla ESI di Ciudad Real (UCLM)
- ◆ Studi post-laurea in Gestione di Progetti svolti presso la CEOE - Confederazione Spagnola di Organizzazioni Aziendali
- ◆ +50 MOOC frequentati, impartiti da università riconosciute come l'Università di Stanford, del Michigan, del Yonsei, l'Università Politecnica di Madrid ecc.
- ◆ Diverse certificazioni, alcune delle più notevoli o recenti sono Azure Fundamentals

Dott.ssa Pedrajas Parabá, Elena

- ◆ Business Analyst presso Management Solutions a Madrid
- ◆ 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 Master in Data Science e Ingegneria Informatica

Dott. Montoro Montarroso, Andrés

- ◆ Membro del Gruppo di Ricerca SMIL dell'Università di Castiglia La Mancia
- ◆ Data Scientist presso Prometheus Global Solutions
- ◆ Laurea in Ingegneria Informatica conseguita presso l'Università di Castiglia La Mancia
- ◆ Master in Data Science e Computer Engineering conseguito presso l'Università di Granada
- ◆ Professore ospite addetto all'insegnamento della materia Sistemi Basati sulla Conoscenza presso la Scuola Superiore di Informatica di Ciudad Real, sede in cui ha anche tenuto la conferenza dal titolo: "Tecniche Avanzate di Intelligenza Artificiale: Ricerca e analisi dei potenziali radicali sui Social Media"
- ◆ Professore ospite addetto all'insegnamento della materia Data Mining presso la Scuola Superiore di Informatica di Ciudad Real, sede in cui ha tenuto la conferenza dal titolo: "Applicazioni del Processo di Linguaggio Naturale: Logica Sfocata per l'analisi dei messaggi sui social media"
- ◆ Relatore nel Seminario sulla Prevenzione della Corruzione in Amministrazioni Pubbliche e Intelligenza Artificiale. Facoltà di Scienze Giuridiche e Sociali di Toledo. Conferenza dal titolo "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 dal titolo "Analisi dei Sentimenti per la prevenzione dei messaggi di odio sui social media"

Dott. Fondón Alcalde, Rubén

- ◆ Business Analyst per il segmento PMI presso Vodafone Spagna
- ◆ Business Analyst per Southern Europe presso Vodafone Global Enterprise
- ◆ Consulente di processo senior presso Unisys per Telefónica Global Solutions
- ◆ Service Integration Leader presso Entelgy per Telefónica Global Solutions
- ◆ Laurea in Ingegneria delle Telecomunicazioni conseguita presso l'Università Europea di Madrid
- ◆ Master in *Big Data* e Analytics conseguito presso l'Università Internazionale di Valencia

Dott.ssa Fernández Meléndez, Galina

- ◆ Data Analyst presso ADN Mobile Solution
- ◆ Processi ETL, data mining, analisi e visualizzazione dei dati, creazione di KPI, progettazione e implementazione di dashboard, controllo di gestione Sviluppo in R, gestione di SQL
- ◆ Determinazione dei modelli, modellazione predittiva, apprendimento automatico
- ◆ Laurea in Amministrazione Aziendale. Università Bicentenaria di Aragua-Caracas
- ◆ Corso Universitario in Pianificazione e Finanza Pubblica. Scuola Venezuelan di Progettazione - Scuola di Finanza
- ◆ Master in Analisi dei Dati e Business Intelligence. Università di Oviedo
- ◆ MBA in Amministrazione e Direzione Aziendale conseguito presso la Scuola di Commercio Europea di Barcellona
- ◆ Master in *Big Data* e Business Intelligence conseguito presso la Scuola di Commercio Europea di Barcellona

Dott. Díaz Díaz-Chirón, Tobías

- ◆ Ricercatore nel laboratorio ArCO dell'Università di Castiglia La Mancia, gruppo dedicato a progetti relazionati con l'architettura e reti di computer
- ◆ Consulente presso Blue Telecom, società dedicata al settore delle telecomunicazioni
- ◆ Laurea in Ingegneria Informatica conseguita presso l'Università di Castiglia La Mancia

Dott.ssa Martínez Cerrato, Yésica

- ◆ Tecnica di prodotti per la sicurezza elettronica presso Securitas Seguridad Spagna
- ◆ Analista di Business intelligence presso Ricopia Technologies
- ◆ Responsabile delle nuove incorporazioni dei software di gestione commerciale (CRM, ERP, INTRANET), prodotti e procedure presso Ricopia Technologies di Alcalá de Henares
- ◆ Responsabile dei nuovi tirocinanti incorporati alle Classi di Informatica dell'Università di Alcalá
- ◆ Project Manager nell'area di Key Account Integration presso Correos y Telégrafos (Madrid)
- ◆ Professoressa di Informatica presso l'Associazione ASALUMA
- ◆ Tecnica informatica - Responsabile delle classi di informatica OTEC dell'Università di Alcalá
- ◆ Laurea in Ingegneria delle Comunicazioni Elettroniche conseguita presso la Scuola Politecnica dell'Università di Alcalá
- ◆ Borsa di studio specialistica come Tecnica Informatica in OTEC presso l'Università di Alcalá



Dott. Tato Sánchez, Rafael

- ◆ Gestione dei progetti. INDRA SISTEMAS S.A.
- ◆ Direttore tecnico. INDRA SISTEMAS S.A.
- ◆ Ingegnere di sistemi. ENA TRÁFICO S.A.U.
- ◆ IFCD048PO: Metodología di gestione e sviluppo di progetti di software con SCRUM
- ◆ Coursera: Machine Learning
- ◆ Udemy: Deep Learning A-Z Hands-on Artificial Neural Networks
- ◆ Coursera: IBM: Fundamentals of Scalable Data Science
- ◆ Coursera: IBM: Applied AI with Deep Learning
- ◆ Coursera: IBM: Advance Machine Learning and Signal Processing
- ◆ Ingegnere in Elettronica Industriale e Automatica proveniente dall'Università Europea di Madrid
- ◆ Master in Ingegneria Industriale abilitante conseguito presso l'Università Europea di Madrid
- ◆ Master in Industria 4.0 conseguito presso l'Università Internazionale di La Rioja (UNIR)
- ◆ Certificazione professionale. SSCE0110: Didattica per la formazione Professionale finalizzata all'occupazione

05

Struttura e contenuti

Questo Master Specialistico riunisce una serie di moduli specifici che permetteranno allo specialista IT di approfondire aspetti quali l'identificazione digitale, i sistemi di controllo degli accessi, l'architettura della sicurezza informatica, la struttura dell'area della sicurezza, i sistemi di gestione della sicurezza informatica nelle comunicazioni e nel funzionamento del software e lo sviluppo del piano di continuità operativa associato alla sicurezza. Nel contempo, vengono affrontate le tecniche più complete e moderne per l'elaborazione dei dati e l'estrazione della conoscenza, sia da un punto di vista teorico che pratico.



66

Tutte le aree tematiche che è necessario padroneggiare per lavorare con successo nel campo dell'informatica, raccolte in un programma di altissima qualità"

Modulo 1. Fondamenti di programmazione

- 1.1. Introduzione alla programmazione
 - 1.1.1. Struttura di base di un computer
 - 1.1.2. Software
 - 1.1.3. Linguaggi di programmazione
 - 1.1.4. Ciclo di vita di un'applicazione informatica
- 1.2. Progettazione dell'algoritmo
 - 1.2.1. Risoluzione dei problemi
 - 1.2.2. Tecniche descrittive
 - 1.2.3. Elementi e struttura di un algoritmo
- 1.3. Elementi di un programma
 - 1.3.1. Origine e caratteristiche del linguaggio C++
 - 1.3.2. L'ambiente di sviluppo
 - 1.3.3. Concetto di programma
 - 1.3.4. Tipi di Dati fondamentali
 - 1.3.5. Operatori
 - 1.3.6. Espressioni
 - 1.3.7. Frasi
 - 1.3.8. Input e output di Dati
- 1.4. Frasi di controllo
 - 1.4.1. Frasi
 - 1.4.2. Biforazioni
 - 1.4.3. Loop
- 1.5. Astrazione e modularità: funzioni
 - 1.5.1. Progettazione modulare
 - 1.5.2. Concetto di funzione e utilità
 - 1.5.3. Definizione di una funzione
 - 1.5.4. Flusso di esecuzione in una chiamata di funzione
 - 1.5.5. Prototipo di una funzione
 - 1.5.6. Restituzione dei risultati
 - 1.5.7. Chiamata di una funzione: parametri
 - 1.5.8. Passaggio di parametri per riferimento e per valore
 - 1.5.9. Area di identificazione
- 1.6. Strutture statiche di Dati
 - 1.6.1. Array
 - 1.6.2. Matrici. Poliedri
 - 1.6.3. Ricerca e ordinamento
 - 1.6.4. Stringhe. Funzioni di I/O per le stringhe
 - 1.6.5. Strutture. Unioni
 - 1.6.6. Nuovi tipi di Dati
- 1.7. Strutture dinamiche di Dati: puntatori
 - 1.7.1. Concetto. Definizione di puntatore
 - 1.7.2. Operatori e operazioni con i puntatori
 - 1.7.3. Array di puntatori
 - 1.7.4. Puntatori e Array
 - 1.7.5. Puntatori a stringhe
 - 1.7.6. Puntatori a strutture
 - 1.7.7. Indirezione multipla
 - 1.7.8. Puntatori a funzioni
 - 1.7.9. Passaggio di funzioni, strutture e Array come parametri di funzione
- 1.8. File
 - 1.8.1. Concetti di base
 - 1.8.2. Operazioni con i file
 - 1.8.3. Tipi di file
 - 1.8.4. Organizzazione dei file
 - 1.8.5. Introduzione ai file C++
 - 1.8.6. Gestione dei file
- 1.9. Ricorsività
 - 1.9.1. Definizione di ricorsività
 - 1.9.2. Tipi di ricorsività
 - 1.9.3. Vantaggi e svantaggi
 - 1.9.4. Considerazioni
 - 1.9.5. Conversione ricorsiva-iterativa
 - 1.9.6. La Pila di ricorsività

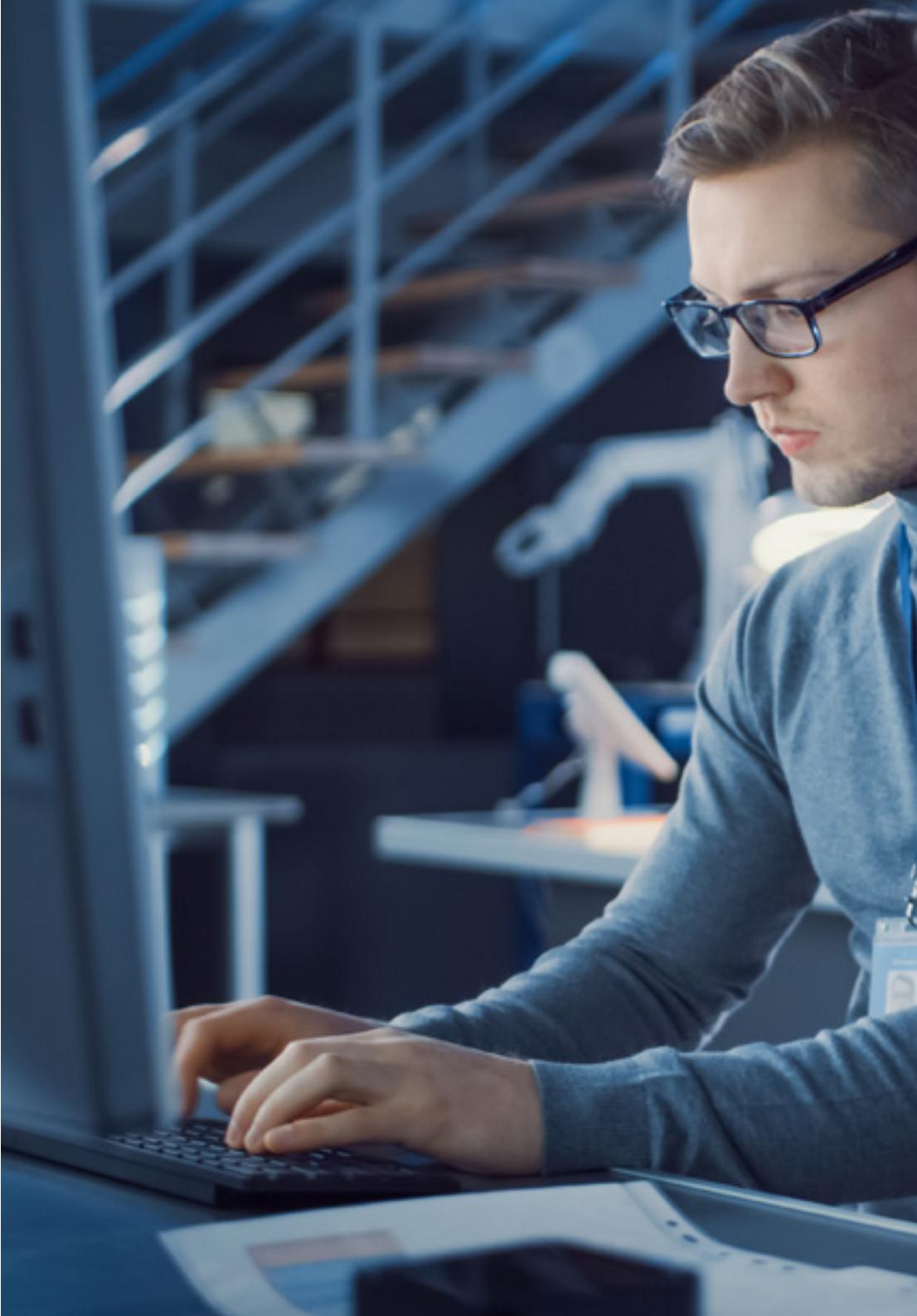
- 1.10. Test e documentazione
 - 1.10.1. Test del programma
 - 1.10.2. Test della scatola bianca
 - 1.10.3. Test della scatola nera
 - 1.10.4. Strumenti di test
 - 1.10.5. Documentazione di programma

Modulo 2. Struttura dei dati

- 2.1. Introduzione alla programmazione in C++
 - 2.1.1. Classi, costruttori, metodi e attributi
 - 2.1.2. Variabili
 - 2.1.3. Espressioni condizionali e loop
 - 2.1.4. Oggetti
- 2.2. Tipi di Dati astratti (ADT)
 - 2.2.1. Tipi di dati
 - 2.2.2. Strutture di base e ADT
 - 2.2.3. Vettori e Array
- 2.3. Strutture di Dati lineari
 - 2.3.1. ADT Lista. Definizione
 - 2.3.2. Liste collegate e doppiamente collegate
 - 2.3.3. Liste ordinate
 - 2.3.4. Liste in C++
 - 2.3.5. ADT Pila
 - 2.3.6. ADT Coda
 - 2.3.7. Pila e Coda in C++
- 2.4. Strutture di Dati gerarchiche
 - 2.4.1. ADT Albero
 - 2.4.2. Percorsi
 - 2.4.3. Alberi n-ari
 - 2.4.4. Alberi binari
 - 2.4.5. Alberi binari di ricerca
- 2.5. Strutture di Dati gerarchiche: alberi complessi
 - 2.5.1. Alberi perfettamente bilanciati o di altezza minima
 - 2.5.2. Alberi multipercorso
 - 2.5.3. Riferimenti bibliografici
- 2.6. Heap e Coda di priorità
 - 2.6.1. ADT Heap
 - 2.6.2. ADT Coda di priorità
- 2.7. Tabelle Hash
 - 2.7.1. ADT Tabella Hash
 - 2.7.2. Funzioni Hash
 - 2.7.3. Funzione Hash nelle tabelle Hash
 - 2.7.4. Ridispersione
 - 2.7.5. Tabelle Hash aperte
- 2.8. Grafi
 - 2.8.1. ADT Grafo
 - 2.8.2. Tipi di Grafi
 - 2.8.3. Rappresentazione grafica e operazioni di base
 - 2.8.4. Progettazione di Grafi
- 2.9. Algoritmi e concetti avanzati sui Grafi
 - 2.9.1. Problemi dei Grafi
 - 2.9.2. Algoritmi di percorso
 - 2.9.3. Algoritmi di percorso o di ricerca
 - 2.9.4. Altri algoritmi
- 2.10. Altre strutture di Dati
 - 2.10.1. Set
 - 2.10.2. Array paralleli
 - 2.10.3. Tabelle di simboli
 - 2.10.4. Tries

Modulo 3. Algoritmo e complessità

- 3.1. Introduzione alle strategie di progettazione degli algoritmi
 - 3.1.1. Ricorsività
 - 3.1.2. Divide et impera
 - 3.1.3. Altre strategie
- 3.2. Efficienza e analisi degli algoritmi
 - 3.2.1. Misure di efficienza
 - 3.2.2. Misurare le dimensioni dell'ingresso
 - 3.2.3. Misurare il tempo di esecuzione
 - 3.2.4. Caso peggiore, caso migliore e caso medio
 - 3.2.5. Notazione asintotica
 - 3.2.6. Criteri di analisi matematica per algoritmi non ricorsivi
 - 3.2.7. Analisi matematica degli algoritmi ricorsivi
 - 3.2.8. Analisi empirica degli algoritmi
- 3.3. Algoritmi di ordinamento
 - 3.3.1. Concetto di ordinamento
 - 3.3.2. Ordinamento della bolla
 - 3.3.3. Ordinamento per selezione
 - 3.3.4. Ordinamento per inserimento
 - 3.3.5. *Merge Sort*
 - 3.3.6. *Quicksort*
- 3.4. Algoritmi con alberi
 - 3.4.1. Concetto di albero
 - 3.4.2. Alberi binari
 - 3.4.3. Percorsi ad albero
 - 3.4.4. Rappresentare le espressioni
 - 3.4.5. Alberi binari ordinati
 - 3.4.6. Alberi binari bilanciati



- 3.5. Algoritmi con *Heaps*
 - 3.5.1. Gli *Heaps*
 - 3.5.2. L'algoritmo *Heapsort*
 - 3.5.3. Code di priorità
- 3.6. Algoritmi con Grafi
 - 3.6.1. Rappresentazione
 - 3.6.2. Percorso in larghezza
 - 3.6.3. Percorso in profondità
 - 3.6.4. Ordinamento topologico
- 3.7. Algoritmi Greedy
 - 3.7.1. La strategia Greedy
 - 3.7.2. Elementi della strategia Greedy
 - 3.7.3. Cambio di valuta
 - 3.7.4. Problema del viaggiatore
 - 3.7.5. Problema dello zaino
- 3.8. Ricerca di percorsi minimi
 - 3.8.1. Problema del percorso minimo
 - 3.8.2. Archi e cicli negativi
 - 3.8.3. Algoritmo di Dijkstra
- 3.9. Algoritmi Greedy sui Grafi
 - 3.9.1. L'albero a sovrapposizione minima
 - 3.9.2. Algoritmo di Prim
 - 3.9.3. Algoritmo di Kruskal
 - 3.9.4. Analisi della complessità
- 3.10. Backtracking
 - 3.10.1. Il Backtracking
 - 3.10.2. Tecniche alternative

Modulo 4. Progettazione avanzata degli algoritmi

- 4.1. Analisi di algoritmi ricorsivi e divide et impera
 - 4.1.1. Porre e risolvere equazioni di ricorrenza omogenee e non omogenee
 - 4.1.2. Panoramica della strategia divide et impera
- 4.2. Analisi ammortizzata
 - 4.2.1. Analisi aggregata
 - 4.2.2. Il metodo di contabilizzazione
 - 4.2.3. Il metodo del potenziale
- 4.3. Programmazione dinamica e algoritmi per problemi NP
 - 4.3.1. Caratteristiche della programmazione dinamica
 - 4.3.2. Indietro nel tempo: backtracking
 - 4.3.3. Ramificazione e potatura
- 4.4. Ottimizzazione combinatoria
 - 4.4.1. Rappresentazione del problema
 - 4.4.2. Ottimizzazione 1D
- 4.5. Algoritmi di randomizzazione
 - 4.5.1. Esempi di algoritmi di randomizzazione
 - 4.5.2. Il teorema di Buffon
 - 4.5.3. Algoritmo di Monte Carlo
 - 4.5.4. Algoritmo di Las Vegas
- 4.6. Ricerca locale e di candidati
 - 4.6.1. *Garcient Ascent*
 - 4.6.2. *Hill Climbing*
 - 4.6.3. *Simulated Annealing*
 - 4.6.4. *Tabu Search*
 - 4.6.5. Ricerca di candidati
- 4.7. Verifica formale dei programmi
 - 4.7.1. Specifica delle astrazioni funzionali
 - 4.7.2. Il linguaggio della logica del primo ordine
 - 4.7.3. Sistema formale di Hoare

- 4.8. Verifica di programmi iterativi
 - 4.8.1. Regole del sistema formale di Hoare
 - 4.8.2. Concetto di iterazioni invarianti
- 4.9. Metodi numerici
 - 4.9.1. Il metodo della bisezione
 - 4.9.2. Il metodo Newton-Raphson
 - 4.9.3. Il metodo della secante
- 4.10. Algoritmi paralleli
 - 4.10.1. Operazioni binarie parallele
 - 4.10.2. Operazioni in parallelo con i Grafi
 - 4.10.3. Parallelismo nel divide et impera
 - 4.10.4. Parallelismo nella programmazione dinamica

Modulo 5. Programmazione avanzata

- 5.1. Introduzione alla programmazione orientata agli oggetti
 - 5.1.1. Introduzione alla programmazione orientata agli oggetti
 - 5.1.2. Progettazione delle lezioni
 - 5.1.3. Introduzione a UML per la modellazione dei problemi
- 5.2. Relazioni tra lezioni
 - 5.2.1. Astrazione ed ereditarietà
 - 5.2.2. Concetti avanzati di ereditarietà
 - 5.2.3. Polimorfismo
 - 5.2.4. Composizione e aggregazione
- 5.3. Introduzione ai design pattern per i problemi orientati agli oggetti
 - 5.3.1. Cosa sono i design pattern?
 - 5.3.2. Pattern Factory
 - 5.3.4. Pattern Singleton
 - 5.3.5. Pattern Observer
 - 5.3.6. Pattern Composite

- 5.4. Eccezioni
 - 5.4.1. Quali sono le eccezioni?
 - 5.4.2. Gestione e acquisizione delle eccezioni
 - 5.4.3. Avvio delle eccezioni
 - 5.4.4. Creazione di eccezioni
- 5.5. Interfacce utente
 - 5.5.1. Introduzione a Qt
 - 5.5.2. Posizionamento
 - 5.5.3. Cosa sono gli eventi?
 - 5.5.4. Eventi: definizione e acquisizione
 - 5.5.5. Sviluppo di interfacce utente
- 5.6. Introduzione alla programmazione concorrente
 - 5.6.1. Introduzione alla programmazione concorrente
 - 5.6.2. Il concetto di processo e di thread
 - 5.6.3. Interazione tra processi o thread
 - 5.6.4. Thread in C++
 - 5.6.5. Vantaggi e svantaggi della programmazione concorrente
- 5.7. Gestione e sincronizzazione dei thread
 - 5.7.1. Ciclo di vita di un thread
 - 5.7.2. La classe *Thread*
 - 5.7.3. Pianificazione del thread
 - 5.7.4. Gruppi di thread
 - 5.7.5. Thread di tipo demoniaco
 - 5.7.6. Sincronizzazione
 - 5.7.7. Meccanismi di bloccaggio
 - 5.7.8. Meccanismi di comunicazione
 - 5.7.9. Monitor
- 5.8. Problemi comuni nella programmazione concorrente
 - 5.8.1. Il problema dei produttori-consumatori
 - 5.8.2. Il problema dei lettori e degli scrittori
 - 5.8.3. Il problema della cena dei filosofi
- 5.9. Documentazione e test del software
 - 5.9.1. Perché è importante documentare il software?
 - 5.9.2. Documentazione di progettazione
 - 5.9.3. Utilizzo di strumenti per la documentazione
- 5.10. Test di software
 - 5.10.1. Introduzione al test del software
 - 5.10.2. Tipi di test
 - 5.10.3. Test dell'unità
 - 5.10.4. Test di integrità
 - 5.10.5. Test di convalida
 - 5.10.6. Test del sistema

Modulo 6. Informatica teorica

- 6.1. Concetti matematici utilizzati
 - 6.1.1. Introduzione alla logica proposizionale
 - 6.1.2. Teoria delle relazioni
 - 6.1.3. Set numerabili e non numerabili
- 6.2. Linguaggi formali e grammatiche e introduzione alle macchine di Turing
 - 6.2.1. Linguaggi e grammatiche formali
 - 6.2.2. Problema decisionale
 - 6.2.3. La macchina di Turing
- 6.3. Estensioni per macchine di Turing, macchine di Turing vincolate e computer
 - 6.3.1. Tecniche di programmazione per macchine di Turing
 - 6.3.2. Estensioni per macchine di Turing
 - 6.3.3. Macchine di Turing vincolate
 - 6.3.4. Macchine di Turing e computer
- 6.4. Indecibilità
 - 6.4.1. Linguaggio non ricorsivo enumerabile
 - 6.4.2. Un problema indecidibile ricorsivamente enumerabile
- 6.5. Altri problemi indicibili
 - 6.5.1. Problemi indecidibili per le macchine di Turing
 - 6.5.2. Problema di post-corrispondenza (PCP)

- 6.6. Problemi intrattabili
 - 6.6.1. Le classi P e NP
 - 6.6.2. Un problema NP completo
 - 6.6.3. Problema di soddisfacibilità ristretta
 - 6.6.4. Altri problemi NP completi
- 6.7. Problemi di Co-NP e PS
 - 6.7.1. Complemento ai linguaggi NP
 - 6.7.2. Problemi risolvibili nello spazio polinomiale
 - 6.7.3. Problemi PS completi
- 6.8. Classi di linguaggi basati sulla randomizzazione
 - 6.8.1. Modello TM con casualità
 - 6.8.2. Le classi RP e ZPP
 - 6.8.3. Test di primalità
 - 6.8.4. Complessità del test di primalità
- 6.9. Altre classi e grammatiche
 - 6.9.1. Automi finiti probabilistici
 - 6.9.2. Automi cellulari
 - 6.9.3. Celle McCulloch e Pitts
 - 6.9.4. Grammatiche di Lindenmayer
- 6.10. Sistemi informatici avanzati
 - 6.10.1. Informatica di membrana: sistemi P
 - 6.10.2. Informatica a DNA
 - 6.10.3. Informatica quantistica
- 7.3. Automi finiti non deterministici
 - 7.3.1. Automi finiti non deterministici
 - 7.3.2. Equivalenza tra AFD e AFND
 - 7.3.3. Automi finiti con transizioni ϵ
- 7.4. Linguaggi ed espressioni regolari (I)
 - 7.4.1. Linguaggi ed espressioni regolari
 - 7.4.2. Automi finiti ed espressioni regolari
- 7.5. Linguaggi ed espressioni regolari (II)
 - 7.5.1. Conversione di espressioni regolari in automi
 - 7.5.2. Applicazioni delle espressioni regolari
 - 7.5.3. Algebra delle espressioni regolari
- 7.6. Pumping lemma e chiusura dei linguaggi regolari
 - 7.6.1. Pumping lemma
 - 7.6.2. Proprietà di chiusura dei linguaggi regolari
- 7.7. Equivalenza e minimizzazione degli automi
 - 7.7.1. Equivalenza di AF
 - 7.7.2. Minimizzazione di AF
- 7.8. Grammatiche indipendenti dal contesto (CIG)
 - 7.8.1. Grammatiche indipendenti dal contesto
 - 7.8.2. Alberi di derivazione
 - 7.8.3. Applicazioni delle GIC
 - 7.8.4. Ambiguità nelle grammatiche e nelle lingue
- 7.9. Automi a Pila e GIC
 - 7.9.1. Definizione di automi a Pila
 - 7.9.2. Lingue accettate da un automa a Pila
 - 7.9.3. Equivalenza tra automi a Pila e automi GIC
 - 7.9.4. Automatismo deterministico a Pila
- 7.10. Forme normali, schema di pumping GIC e proprietà delle LIC
 - 7.10.1. Forme normali di GIC
 - 7.10.2. Pumping lemma
 - 7.10.3. Proprietà di chiusura dei linguaggi
 - 7.10.4. Proprietà di decisioni dei LIC

Modulo 7: Teoria degli automi e linguaggi formali

- 7.1. Introduzione alla teoria degli automi
 - 7.1.1. Perché studiare la teoria degli automi?
 - 7.1.2. Introduzione alle dimostrazioni formali
 - 7.1.3. Altre forme di dimostrazione
 - 7.1.4. Induzione matematica
 - 7.1.5. Alfabeti, stringhe e lingue
- 7.2. Automi finiti deterministici
 - 7.2.1. Introduzione agli automi finiti
 - 7.2.2. Automi finiti deterministici
- 7.3. Automi finiti non deterministici
 - 7.3.1. Automi finiti non deterministici
 - 7.3.2. Equivalenza tra AFD e AFND
 - 7.3.3. Automi finiti con transizioni ϵ
- 7.4. Linguaggi ed espressioni regolari (I)
 - 7.4.1. Linguaggi ed espressioni regolari
 - 7.4.2. Automi finiti ed espressioni regolari
- 7.5. Linguaggi ed espressioni regolari (II)
 - 7.5.1. Conversione di espressioni regolari in automi
 - 7.5.2. Applicazioni delle espressioni regolari
 - 7.5.3. Algebra delle espressioni regolari
- 7.6. Pumping lemma e chiusura dei linguaggi regolari
 - 7.6.1. Pumping lemma
 - 7.6.2. Proprietà di chiusura dei linguaggi regolari
- 7.7. Equivalenza e minimizzazione degli automi
 - 7.7.1. Equivalenza di AF
 - 7.7.2. Minimizzazione di AF
- 7.8. Grammatiche indipendenti dal contesto (CIG)
 - 7.8.1. Grammatiche indipendenti dal contesto
 - 7.8.2. Alberi di derivazione
 - 7.8.3. Applicazioni delle GIC
 - 7.8.4. Ambiguità nelle grammatiche e nelle lingue
- 7.9. Automi a Pila e GIC
 - 7.9.1. Definizione di automi a Pila
 - 7.9.2. Lingue accettate da un automa a Pila
 - 7.9.3. Equivalenza tra automi a Pila e automi GIC
 - 7.9.4. Automatismo deterministico a Pila
- 7.10. Forme normali, schema di pumping GIC e proprietà delle LIC
 - 7.10.1. Forme normali di GIC
 - 7.10.2. Pumping lemma
 - 7.10.3. Proprietà di chiusura dei linguaggi
 - 7.10.4. Proprietà di decisioni dei LIC

Modulo 8. Processori linguistici

- 8.1. Introduzione al processo di compilazione
 - 8.1.1. Compilazione e interpretazione
 - 8.1.2. Ambiente di esecuzione del compilatore
 - 8.1.3. Processo di analisi
 - 8.1.4. Processo di sintesi
- 8.2. Analizzatore lessicale
 - 8.2.1. Che cos'è un analizzatore lessicale?
 - 8.2.2. Implementazione dell'analizzatore lessicale
 - 8.2.3. Azioni semantiche
 - 8.2.4. Recupero degli errori
 - 8.2.5. Problemi di implementazione
- 8.3. Parsing
 - 8.3.1. Che cos'è un parser?
 - 8.3.2. Concetti preliminari
 - 8.3.3. Parser top-down
 - 8.3.4. Parser bottom-up
- 8.4. Parsing top-down e parsing bottom-up
 - 8.4.1. Parser LL (1)
 - 8.4.2. Parser LR (0)
 - 8.4.3. Esempio di parser
- 8.5. Parsing avanzato bottom-up
 - 8.5.1. Parser SLR
 - 8.5.2. Parser LR (1)
 - 8.5.3. Parser LR (k)
 - 8.5.4. Parser LALR
- 8.6. Analisi semantica (I)
 - 8.6.1. Traduzione guidata dalla sintassi
 - 8.6.2. Tabella dei simboli
- 8.7. Analisi semantica (II)
 - 8.7.1. Controllo del tipo
 - 8.7.2. Il sottosistema dei tipi
 - 8.7.3. Equivalenza dei tipi e conversioni

8.8. Generazione del codice e ambiente di esecuzione

- 8.8.1. Aspetti progettuali
- 8.8.2. Ambiente di esecuzione
- 8.8.3. Organizzazione della memoria
- 8.8.4. Allocazione della memoria

8.9. Generazione di codice intermedio

- 8.9.1. Traduzione guidata dalla sintesi
- 8.9.2. Rappresentazioni intermedie
- 8.9.3. Esempi di traduzioni

8.10. Ottimizzazione del codice

- 8.10.1. Allocazione dei registri
- 8.10.2. Eliminazione delle allocazioni morte
- 8.10.3. Esecuzione in tempo di compilazione
- 8.10.4. Riordino delle espressioni
- 8.10.5. Ottimizzazione del loop

Modulo 9. Computer grafica e visualizzazione

9.1. Teoria del colore

- 9.1.1. Proprietà della luce
- 9.1.2. Modelli di colore
- 9.1.3. Lo standard CIE
- 9.1.4. *Profiling*

9.2. Primitive di output

- 9.2.1. Il controller video
- 9.2.2. Algoritmi per il disegno di linee
- 9.2.3. Algoritmi per il disegno di cerchi
- 9.2.4. Algoritmi di riempimento

9.3. Trasformazioni 2D, sistemi di coordinate 2D e ritaglio 2D

- 9.3.1. Trasformazioni geometriche di base
- 9.3.2. Coordinate omogenee
- 9.3.3. Trasformazione inversa
- 9.3.4. Composizione delle trasformazioni
- 9.3.5. Altre trasformazioni

- 9.3.6. Cambio di coordinate
- 9.3.7. Sistemi di coordinate 2D
- 9.3.8. Cambio di coordinate
- 9.3.9. Standardizzazione
- 9.3.10. Algoritmi di ritaglio
- 9.4. Trasformazioni 3D
 - 9.4.1. Traslazione
 - 9.4.2. Rotazione
 - 9.4.3. Scala
 - 9.4.4. Riflessione
 - 9.4.5. Cesoia
- 9.5. Visualizzazione e modifica delle coordinate 3D
 - 9.5.1. Sistemi di coordinate 3D
 - 9.5.2. Visualizzazione
 - 9.5.3. Cambio di coordinate
 - 9.5.4. Proiezione e standardizzazione
- 9.6. Proiezione e taglio 3D
 - 9.6.1. Proiezione ortogonale
 - 9.6.2. Proiezione parallela obliqua
 - 9.6.3. Proiezione prospettica
 - 9.6.4. Algoritmi di ritaglio 3D
- 9.7. Rimozione di superfici nascoste
 - 9.7.1. *Back-Face Removal*
 - 9.7.2. *Z-Buffer*
 - 9.7.3. Algoritmo del pittore
 - 9.7.4. Algoritmo di Warnock
 - 9.7.5. Rilevamento delle linee nascoste
- 9.8. Interpolazione e curve parametriche
 - 9.8.1. Interpolazione e approssimazione polinomiale
 - 9.8.2. Rappresentazione parametrica
 - 9.8.3. Polinomio di Lagrange
 - 9.8.4. Spline cubiche naturali
 - 9.8.5. Funzioni base
 - 9.8.6. Rappresentazione della matrice



- 9.9. Curve di Bézier
 - 9.9.1. Costruzione algebrica
 - 9.9.2. Forma a matrice
 - 9.9.3. Composizione
 - 9.9.4. Costruzione geometrica
 - 9.9.5. Algoritmo di disegno
- 9.10. *B-Splines*
 - 9.10.1. Il problema del controllo locale
 - 9.10.2. B-splines cubiche uniformi
 - 9.10.3. Funzioni di base e punti di controllo
 - 9.10.4. Deriva all'origine e molteplicità
 - 9.10.5. Rappresentazione della matrice
 - 9.10.6. B-splines non uniformi
- 10.7. Programmazione evolutiva applicata ai problemi di apprendimento
 - 10.7.1. Apprendimento Basato su Regole
 - 10.7.2 Metodi evolutivi nei problemi di selezione delle istanze
- 10.8. Problemi multi-obiettivo
 - 10.8.1. Concetto di dominanza
 - 10.8.2. Applicazione degli algoritmi evolutivi ai problemi multi-obiettivo
- 10.9. Reti neurali (I)
 - 10.9.1. Introduzione alle reti neurali
 - 10.9.2. Esempio pratico con le reti neurali
- 10.10. Reti neurali (II)
 - 10.10.1. Casi di utilizzo delle reti neurali nella ricerca medica
 - 10.10.2. Casi di utilizzo delle reti neurali in economia
 - 10.10.3. Casi di utilizzo delle reti neurali nella visione artificiale

Modulo 10: Informatica bio-ispirata

- 10.1. Introduzione all'informatica bio-ispirata
 - 10.1.1. Introduzione all'informatica bio-ispirata
- 10.2. Algoritmi di adattamento sociale
 - 10.2.1. Calcolo bio-ispirato basato su colonie di formiche
 - 10.2.2. Varianti degli algoritmi di colonia di formiche
 - 10.2.3. Elaborazione particellare basata su cloud
- 10.3. Algoritmi genetici
 - 10.3.1. Struttura generale
 - 10.3.2. Implementazioni dei principali operatori
- 10.4. Strategie spaziali di esplorazione-sfruttamento per algoritmi genetici
 - 10.4.1. Algoritmo CHC
 - 10.4.2. Problemi multimodali
- 10.5. Modelli di calcolo evolutivo (I)
 - 10.5.1. Strategie evolutive
 - 10.5.2. Programmazione evolutiva
 - 10.5.3. Algoritmi basati sull'evoluzione differenziale
- 10.6. Modelli di calcolo evolutivo (II)
 - 10.6.1. Modelli evolutivi basati sulla stima delle distribuzioni (EDA)
 - 10.6.2. Programmazione genetica

Modulo 11. Sicurezza nella progettazione e nello sviluppo dei sistemi

- 11.1. Sistemi di informazione
 - 11.1.1. Settori di un sistema di informazione
 - 11.1.2. Componenti di un sistema di informazione
 - 11.1.3. Attività di un sistema di informazione
 - 11.1.4. Ciclo di vita di un sistema di informazione
 - 11.1.5. Risorse di un sistema di informazione
- 11.2. Sistemi di informazione. Tipologia
 - 11.2.1. Tipi di sistemi di informazione
 - 11.2.1.1. Aziendali
 - 11.2.1.2. Strategici
 - 11.2.1.3. In base all'ambito di applicazione
 - 11.2.1.4. Specifici
 - 11.2.2. Sistemi di informazione. Esempi reali
 - 11.2.3. Evoluzione dei sistemi di informazione: le fasi
 - 11.2.4. Metodologie dei sistemi di informazione

- 11.3. Sicurezza dei sistemi di informazione. Implicazioni giuridiche
 - 11.3.1. Accesso ai Dati
 - 11.3.2. Minacce alla sicurezza: vulnerabilità
 - 11.3.3. Implicazioni giuridiche: reati penali
 - 11.3.4. Procedure per la manutenzione di un sistema di informazione
- 11.4. Sicurezza di un sistema di informazione. Protocolli di sicurezza
 - 11.4.1. Sicurezza di un sistema di informazione
 - 11.4.1.1. Integrità
 - 11.4.1.2. Riservatezza
 - 11.4.1.3. Disponibilità
 - 11.4.1.4. Autenticazione
 - 11.4.2. Servizi di sicurezza
 - 11.4.3. Protocolli di sicurezza delle informazioni Tipologia
 - 11.4.4. Sensibilità di un sistema informativo
- 11.5. Sicurezza in un sistema informativo. Misure e sistemi di controllo degli accessi
 - 11.5.1. Misure di sicurezza
 - 11.5.2. Tipo di misure di sicurezza
 - 11.5.2.1. Prevenzione
 - 11.5.2.2. Rilevamento
 - 11.5.2.3. Correzione
 - 11.5.3. Sistema di controllo degli accessi. Tipologia
 - 11.5.4. Crittografia
- 11.6. Sicurezza di rete e Internet
 - 11.6.1. *Firewall*
 - 11.6.2. Identificazione digitale
 - 11.6.3. Virus e worm
 - 11.6.4. *Hacking*
 - 11.6.5. Esempi e casi reali
- 11.7. Reati informatici
 - 11.7.1. Reato informatico
 - 11.7.2. Reati informatici. Tipologia
 - 11.7.3. Reato informatico. Attacco. Tipologie
 - 11.7.4. Il caso della Realtà Virtuale
 - 11.7.5. Profili dei colpevoli e delle vittime. Penalizzazione del reato
 - 11.7.6. Reati informatici. Esempi e casi reali
- 11.8. Piano di sicurezza in un sistema informatico
 - 11.8.1. Piano di sicurezza. Obiettivi
 - 11.8.2. Piano di sicurezza. Pianificazione
 - 11.8.3. Piano di rischio. Analisi
 - 11.8.4. Politica di sicurezza. Implementazione nell'organizzazione
 - 11.8.5. Piano di sicurezza. Implementazione nell'organizzazione
 - 11.8.6. Procedure di sicurezza. Tipologie
 - 11.8.7. Piani di sicurezza. Esempi
- 11.9. Piano di contingenza
 - 11.9.1. Piano di contingenza. Funzioni
 - 11.9.2. Piano di emergenza: elementi e obiettivi
 - 11.9.3. Piani di contingenza all'interno dell'organizzazione. Implementazione
 - 11.9.4. Piano di contingenza. Esempi
- 11.10. Governance della sicurezza dei sistemi informatici
 - 11.10.1. Normativa legale
 - 11.10.2. Standard
 - 11.10.3. Certificazioni
 - 11.10.4. Tecnologie

Modulo 12. Strutture e modelli per la sicurezza delle informazioni

- 12.1. Struttura di sicurezza delle informazioni
 - 12.1.1. ISMS/PDS
 - 12.1.2. Allineamento strategico
 - 12.1.3. Gestione del rischio
 - 12.1.4. Misurazione della performance
- 12.2. Modelli di sicurezza delle informazioni
 - 12.2.1. In base alle politiche di sicurezza
 - 12.2.2. In base agli strumenti di protezione
 - 12.2.3. In base alle apparecchiature di lavoro
- 12.3. Modello di sicurezza. Componenti chiave
 - 12.3.1. Identificazione dei rischi
 - 12.3.2. Definizione dei controlli
 - 12.3.3. Valutazione continua dei livelli di rischio
 - 12.3.4. Piano di sensibilizzazione per dipendenti, fornitori, partner, ecc.
- 12.4. Processo di gestione dei rischi
 - 12.4.1. Identificazione delle risorse
 - 12.4.2. Identificazione delle minacce
 - 12.4.3. Valutazione dei rischi
 - 12.4.4. Priorità dei controlli
 - 12.4.5. Rivalutazione e rischio residuo
- 12.5. Processi operativi e sicurezza delle informazioni
 - 12.5.1. Processi aziendali
 - 12.5.2. Valutazione del rischio in base ai parametri aziendali
 - 12.5.3. Analisi dell'impatto aziendale
 - 12.5.4. Operazioni aziendali e sicurezza delle informazioni
- 12.6. Processo di miglioramento continuo
 - 12.6.1. Il ciclo di Deming
 - 12.6.1.1. Pianificare
 - 12.6.1.2. Fare
 - 12.6.1.3. Verificare
 - 12.6.1.4. Agire
- 12.7. Architetture di sicurezza
 - 12.7.1. Selezione e omogeneizzazione delle tecnologie
 - 12.7.2. Gestione dell'identità. Autenticazione
 - 12.7.3. Gestione degli accessi. Autorizzazione
 - 12.7.4. Sicurezza dell'infrastruttura di rete
 - 12.7.5. Tecnologie e soluzioni di crittografia
 - 12.7.6. Sicurezza delle apparecchiature terminali (EDR)
- 12.8. Quadro normativo
 - 12.8.1. Regolamenti settoriali
 - 12.8.2. Certificazioni
 - 12.8.3. Legislazione
- 12.9. Standard ISO 27001
 - 12.9.1. Implementazione
 - 12.9.2. Certificazione
 - 12.9.3. Verifiche e penetration test
 - 12.9.4. Gestione continua del rischio
 - 12.9.5. Classificazione delle informazioni
- 12.10. Legislazione sulla privacy. RGPD (GDPR)
 - 12.10.1. Ambito di applicazione del Regolamento generale sulla protezione dei dati (RGPD)
 - 12.10.2. Dati personali
 - 12.10.3. Ruoli nel trattamento dei Dati personali
 - 12.10.4. Diritti ARCO
 - 12.10.5. Il DPO. Funzioni

Modulo 13. Gestione della sicurezza IT

- 13.1. Gestione della sicurezza
 - 13.1.1. Operazioni di sicurezza
 - 13.1.2. Aspetti giuridici e normativi
 - 13.1.3. Abilitazione all'esercizio dell'attività
 - 13.1.4. Gestione dei rischi
 - 13.1.5. Gestione dell'identità e degli accessi
- 13.2. Struttura dell'area di sicurezza. L'ufficio del CISO
 - 13.2.1. Struttura organizzativa. Posizione del CISO nella struttura
 - 13.2.2. Linee di difesa
 - 13.2.3. Organigramma dell'ufficio del CISO
 - 13.2.4. Gestione del bilancio
- 13.3. Governance della sicurezza
 - 13.3.1. Comitato per la sicurezza
 - 13.3.2. Comitato per il monitoraggio dei rischi
 - 13.3.3. Comitato per il controllo
 - 13.3.4. Comitato per le crisi
- 13.4. Governance della sicurezza. Funzioni
 - 13.4.1. Politiche e standard
 - 13.4.2. Piano generale di sicurezza
 - 13.4.3. Quadro di controllo
 - 13.4.4. Sensibilizzazione e corsi di aggiornamento
 - 13.4.5. Sicurezza della catena di approvvigionamento
- 13.5. Operazioni di sicurezza
 - 13.5.1. Gestione dell'identità e degli accessi
 - 13.5.2. Configurazione delle regole di sicurezza della rete. *Firewall*
 - 13.5.3. Gestione di piattaforme IDS/IPS
 - 13.5.4. Analisi dei punti deboli
- 13.6. Quadro di riferimento per la Cybersecurity. NIST CSF
 - 13.6.1. Metodologia NIST
 - 13.6.1.1. Identificare
 - 13.6.1.2. Proteggere
 - 13.6.1.3. Rilevare
 - 13.6.1.4. Rispondere
 - 13.6.1.5. Recuperare
- 13.7. Centro operativo di sicurezza (SOC). Funzioni
 - 13.7.1. Protezione. *Red Team, Pentesting, Threat Intelligence*
 - 13.7.2. Rilevamento. *SIEM, User Behavior Analytics, Fraud Prevention*
 - 13.7.3. Risposta
- 13.8. Verifiche di sicurezza
 - 13.8.1. Penetration test
 - 13.8.2. Esercizi di Red Team
 - 13.8.3. Verifiche del codice sorgente. Sviluppo sicuro
 - 13.8.4. Sicurezza dei componenti (*Software Supply Chain*)
 - 13.8.5. Analisi forense
- 13.9. Risposta agli incidenti
 - 13.9.1. Preparazione
 - 13.9.2. Rilevamento, analisi e reporting
 - 13.9.3. Contenimento, eliminazione e recupero
 - 13.9.4. Attività in seguito all'incidente
 - 13.9.4.1. Conservazione delle prove
 - 13.9.4.2. Analisi forense
 - 13.9.4.3. Gestire una violazione dei dati
- 13.10. Gestione delle vulnerabilità
 - 13.10.1. Analisi dei punti deboli
 - 13.10.2. Valutazione della vulnerabilità
 - 13.10.3. Base di sistema
 - 13.10.4. Vulnerabilità 0-day. *Zero-Day*

Modulo 14. Analisi dei rischi e ambiente di sicurezza IT

- 14.1. Analisi del contesto
 - 14.1.1. Analisi della situazione economica
 - 14.1.1.1. Ambienti VUCA
 - 14.1.1.1.1. Volatilità
 - 14.1.1.1.2. Incertezza
 - 14.1.1.1.3. Complessità
 - 14.1.1.1.4. Ambiguità
 - 14.1.1.2. Ambienti BANI
 - 14.1.1.2.1. Fragilità
 - 14.1.1.2.2. Ansia
 - 14.1.1.2.3. Non linearità
 - 14.1.1.2.4. Incomprensibilità
 - 14.1.2. Analisi del contesto generale PESTEL
 - 14.1.2.1. Politica
 - 14.1.2.2. Economica
 - 14.1.2.3. Sociale
 - 14.1.2.4. Tecnologica
 - 14.1.2.5. Ecologica/Ambientale
 - 14.1.2.6. Giuridica
 - 14.1.3. Analisi della situazione interna. SWOT
 - 14.1.3.1. Obiettivi
 - 14.1.3.2. Minacce
 - 14.1.3.3. Opportunità
 - 14.1.3.4. Punti di forza
- 14.2. Rischio e incertezza
 - 14.2.1. Rischio
 - 14.2.2. Gestione del rischio
 - 14.2.3. Standard di gestione del rischio
- 14.3. Linee guida per la gestione del rischio ISO 31.000:2018
 - 14.3.1. Oggetto
 - 14.3.2. Principi
 - 14.3.3. Quadro di riferimento
 - 14.3.4. Processo
- 14.4. Metodologia per l'analisi e la gestione dei rischi dei sistemi informatici (MAGERIT)
 - 14.4.1. Metodologia MAGERIT
 - 14.4.1.1. Obiettivi
 - 14.4.1.2. Metodologia
 - 14.4.1.3. Elementi
 - 14.4.1.4. Tecniche
 - 14.4.1.5. Strumenti disponibili (PILAR)
- 14.5. Trasferimento del rischio informatico
 - 14.5.1. Trasferimento del rischio
 - 14.5.2. Rischi informatici. Tipologia
 - 14.5.3. Assicurazione contro i rischi informatici
- 14.6. Metodologie agili per la gestione del rischio
 - 14.6.1. Metodologie agili
 - 14.6.2. Scrum per la gestione del rischio
 - 14.6.3. *Agile Risk Management*
- 14.7. Tecnologie per la gestione del rischio
 - 14.7.1. Intelligenza artificiale applicata alla gestione del rischio
 - 14.7.2. *Blockchain* e crittografia. Metodi di conservazione del valore
 - 14.7.3. Computazione quantistica Opportunità o minaccia
- 14.8. Mappatura dei rischi informatici basata su metodologie agili
 - 14.8.1. Rappresentare la probabilità e l'impatto in ambienti agili
 - 14.8.2. Il rischio come minaccia al valore
 - 14.8.3. Ri-evoluzione nella gestione dei progetti agili e nei processi basati sui KRI

- 14.9. *Risk-Driven* nella gestione del rischio
 - 14.9.1. *Risk Driven*
 - 14.9.2. *Risk-Driven* nella gestione del rischio
 - 14.9.3. Sviluppo di un modello di gestione aziendale orientato al rischio
- 14.10. Innovazione e trasformazione digitale nella gestione del rischio IT
 - 14.10.1. La gestione del rischio agile come fonte di innovazione aziendale
 - 14.10.2. Trasformare i Dati in informazioni utili per le decisioni
 - 14.10.3. Visione olistica dell'impresa tramite il rischio

Modulo 15. La crittografia nell'IT

- 15.1. Crittografia
 - 15.1.1. Crittografia
 - 15.1.2. Fondamenti matematici
- 15.2. Criptologia
 - 15.2.1. Criptologia
 - 15.2.2. Crittoanalisi
 - 15.2.3. Steganografia e stegoanalisi
- 15.3. Protocolli crittografici
 - 15.3.1. Blocchi di base
 - 15.3.2. Protocolli di base
 - 15.3.3. Protocolli intermedi
 - 15.3.4. Protocolli avanzati
 - 15.3.5. Protocolli esoterici
- 15.4. Tecniche crittografiche
 - 15.4.1. Lunghezza della chiave di crittografia
 - 15.4.2. Gestione delle chiavi
 - 15.4.3. Tipi di algoritmi
 - 15.4.4. Funzioni di riepilogo. *Hash*
 - 15.4.5. Generatori di numeri pseudocasuali
 - 15.4.6. Uso degli algoritmi
- 15.5. Crittografia simmetrica
 - 15.5.1. Cifrari a blocchi
 - 15.5.2. DES (*Data Encryption Standard*)
 - 15.5.3. Algoritmo RC4
- 15.5.4. AES (*Advanced Encryption Standard*)
- 15.5.5. Combinazione di cfrari a blocchi
- 15.5.6. Derivazione delle chiavi
- 15.6. Crittografia asimmetrica
 - 15.6.1. Diffie-Hellman
 - 15.6.2. DSA (*Digital Signature Algorithm*)
 - 15.6.3. RSA (Rivest, Shamir y Adleman)
 - 15.6.4. Curva ellittica
 - 15.6.5. Crittografia asimmetrica. Tipologia
- 15.7. Certificati digitali
 - 15.7.1. Firma digitale
 - 15.7.2. Certificati X509
 - 15.7.3. Infrastruttura a chiave pubblica (PKI)
- 15.8. Implementazione
 - 15.8.1. Kerberos
 - 15.8.2. IBM CCA
 - 15.8.3. *Pretty Good Privacy* (PGP)
 - 15.8.4. ISO Authentication Framework
 - 15.8.5. SSL e TLS
 - 15.8.6. Smart card nei mezzi di pagamento (EMV)
 - 15.8.7. Protocolli di telefonia mobile
 - 15.8.8. *Blockchain*
- 15.9. Steganografia
 - 15.9.1. Steganografia
 - 15.9.2. Stegoanalisi
 - 15.9.3. Applicazioni e usi
- 15.10. Crittografia quantistica
 - 15.10.1. Algoritmi quantistici
 - 15.10.2. Protezione degli algoritmi dalla computazione quantistica
 - 15.10.3. Distribuzione quantistica delle chiavi

Modulo 16. Gestione dell'identità e degli accessi nella sicurezza informatica

16.1. Gestione dell'identità e degli accessi (IAM)

- 16.1.1. Identità digitale
- 16.1.2. Gestione dell'identità
- 16.1.3. Federazione di identità

16.2. Controllo degli accessi fisici

- 16.2.1. Sistemi di protezione
- 16.2.2. Sicurezza delle aree
- 16.2.3. Strutture di recupero

16.3. Controllo logico degli accessi

- 16.3.1. Autenticazione: tipologia
- 16.3.2. Protocolli di autenticazione
- 16.3.3. Attacchi di autenticazione

16.4. Controllo logico degli accessi. Autenticazione MFA

- 16.4.1. Controllo logico degli accessi. Autenticazione MFA
- 16.4.2. Password. Importanza
- 16.4.3. Attacchi di autenticazione

16.5. Controllo logico degli accessi. Autenticazione biometrica

- 16.5.1. Controllo logico degli accessi. Autenticazione biometrica
- 16.5.1.1. Autenticazione biometrica. Requisiti

16.5.2. Funzionamento

16.5.3. Modelli e tecniche

16.6. Sistemi di gestione dell'autenticazione

- 16.6.1. *Single Sign-on*
- 16.6.2. Kerberos
- 16.6.3. Sistemi AAA

16.7. Sistemi di gestione dell'autenticazione: Sistemi AAA

- 16.7.1. TACACS
- 16.7.2. RADIUS
- 16.7.3. DIAMETER

16.8. Servizi per il controllo degli accessi

- 16.8.1. FW - Firewall
- 16.8.2. VPN - Reti private virtuali
- 16.8.3. IDS - Sistema di rilevamento delle intrusioni

16.9. Sistemi di controllo degli accessi alla rete

- 16.9.1. NAC
- 16.9.2. Architettura ed elementi
- 16.9.3. Funzionamento e standardizzazione

16.10. Accesso alle reti wireless

- 16.10.1. Tipi di reti wireless
- 16.10.2. Sicurezza nelle reti wireless
- 16.10.3. Attacchi alla rete wireless

Modulo 17. Sicurezza nelle comunicazioni e nel funzionamento del software

17.1. Sicurezza informatica nelle comunicazioni e nel funzionamento del software

- 17.1.1. Sicurezza Informatica
- 17.1.2. Cybersecurity
- 17.1.3. Sicurezza del cloud

17.2. Sicurezza informatica nelle comunicazioni e nel funzionamento del software. Tipologia

- 17.2.1. Sicurezza fisica
- 17.2.2. Sicurezza logica

17.3. Sicurezza nelle comunicazioni

- 17.3.1. Elementi principali
- 17.3.2. Sicurezza di rete
- 17.3.3. Le migliori prassi

17.4. Cyberintelligence

- 17.4.1. Ingegneria sociale
- 17.4.2. Deep Web
- 17.4.3. Phishing
- 17.4.4. Malware

- 17.5. Sviluppo sicuro nelle comunicazioni e nel funzionamento del software
 - 17.5.1. Sviluppo sicuro. Protocollo HTTP
 - 17.5.2. Sviluppo sicuro. Ciclo di vita
 - 17.5.3. Sviluppo sicuro. Sicurezza PHP
 - 17.5.4. Sviluppo sicuro. Sicurezza NET
 - 17.5.5. Sviluppo sicuro. Le migliori prassi
- 17.6. Sistemi di gestione della sicurezza delle informazioni nelle comunicazioni e nel controllo del software
 - 17.6.1. GDPR
 - 17.6.2. ISO 27021
 - 17.6.3. ISO 27017/18
- 17.7. Tecnologie SIEM
 - 17.7.1. Tecnologie SIEM
 - 17.7.2. Operazioni SOC
 - 17.7.3. SIEM vendors
- 17.8. Il ruolo della sicurezza nelle organizzazioni
 - 17.8.1. Ruoli nelle organizzazioni
 - 17.8.2. Il ruolo degli specialisti IoT nelle aziende
 - 17.8.3. Certificazioni riconosciute dal mercato
- 17.9. Analisi forense
 - 17.9.1. Analisi forense
 - 17.9.2. Analisi forense. Metodologia
 - 17.9.3. Analisi forense. Strumenti e implementazione
- 17.10. Cybersecurity oggi
 - 17.10.1. Principali attacchi informatici
 - 17.10.2. Previsioni di impiego
 - 17.10.3. Sfide

Modulo 18. Sicurezza negli ambienti *Cloud*

- 18.1. Sicurezza negli ambienti *Cloud Computing*
 - 18.1.1. Sicurezza negli ambienti *Cloud Computing*
 - 18.1.2. Sicurezza negli ambienti *Cloud Computing* Minacce e rischi per la sicurezza
 - 18.1.3. Sicurezza negli ambienti *Cloud Computing* Aspetti chiave della sicurezza
- 18.2. Tipi di infrastruttura *Cloud*
 - 18.2.1. Pubblico
 - 18.2.2. Privato
 - 18.2.3. Ibrido
- 18.3. Modello di gestione condivisa
 - 18.3.1. Caratteristiche di sicurezza gestite dal fornitore
 - 18.3.2. Elementi gestiti dal cliente
 - 18.3.3. Definizione della strategia di sicurezza
- 18.4. Meccanismi di prevenzione
 - 18.4.1. Sistemi di gestione dell'autenticazione
 - 18.4.2. Sistema di gestione delle autorizzazioni: politiche di accesso
 - 18.4.3. Sistemi di gestione delle chiavi
- 18.5. Protezione dei sistemi
 - 18.5.1. Protezione dei sistemi di archiviazione
 - 18.5.2. Protezione dei sistemi di Database
 - 18.5.3. Protezione dei Dati in transito
- 18.6. Protezione dell'infrastruttura
 - 18.6.1. Progettazione e implementazione di reti sicure
 - 18.6.2. Sicurezza delle risorse informatiche
 - 18.6.3. Strumenti e risorse per la protezione delle infrastrutture
- 18.7. Rilevamento di minacce e attacchi
 - 18.7.1. Sistemi di audit, *Logging* e monitoraggio
 - 18.7.2. Sistemi di eventi e allarmi
 - 18.7.3. Sistemi SIEM

- 18.8. Risposta agli incidenti
 - 18.8.1. Piano di risposta agli incidenti
 - 18.8.2. La continuità operativa
 - 18.8.3. Analisi forense e correzione di incidenti della stessa natura
- 18.9. Sicurezza nei *Cloud* pubblici
 - 18.9.1. AWS (Amazon Web Services)
 - 18.9.2. Microsoft Azure
 - 18.9.3. Google GCP
 - 18.9.4. Oracle Cloud
- 18.10. Regolamenti e conformità
 - 18.10.1. Conformità alle norme di sicurezza
 - 18.10.2. Gestione dei rischi
 - 18.10.3. Personale e procedure nelle organizzazioni

Modulo 19. Sicurezza delle comunicazioni nei dispositivi IoT

- 19.1. Dalla telemetria all'IoT
 - 19.1.1. Telemetria
 - 19.1.2. Connattività M2M
 - 19.1.3. Democratizzazione della telemetria
- 19.2. Modelli di riferimento IoT
 - 19.2.1. Modello di riferimento IoT
 - 19.2.2. Architettura IoT semplificata
- 19.3. Vulnerabilità della sicurezza IoT
 - 19.3.1. Dispositivi IoT
 - 19.3.2. Dispositivi IoT. Casi di utilizzo
 - 19.3.3. Dispositivi IoT. Punti deboli
- 19.4. Connattività IoT
 - 19.4.1. Reti PAN, LAN, WAN
 - 19.4.2. Tecnologie wireless non IoT
 - 19.4.3. Tecnologie wireless LPWAN
- 19.5. Tecnologie LPWAN
 - 19.5.1. Il triangolo di ferro delle reti LPWAN
 - 19.5.2. Bande di frequenza libere vs. Bande con licenza
 - 19.5.3. Opzioni tecnologiche LPWAN
- 19.6. Tecnologia LoRaWAN
 - 19.6.1. Tecnologia LoRaWAN
 - 19.6.2. Casi d'uso di LoRaWAN. Ecosistema
 - 19.6.3. Sicurezza in LoRaWAN
- 19.7. Tecnologia Sigfox
 - 19.7.1. Tecnologia Sigfox
 - 19.7.2. Casi d'uso di Sigfox. Ecosistema
 - 19.7.3. Sicurezza in Sigfox
- 19.8. Tecnologia cellulare IoT
 - 19.8.1. Tecnologia cellulare IoT (NB-IoT e LTE-M)
 - 19.8.2. Casi d'uso cellulare IoT. Ecosistema
 - 19.8.3. Sicurezza cellulare IoT
- 19.9. Tecnologia Wi-SUN
 - 19.9.1. Tecnologia Wi-SUN
 - 19.9.2. Casi d'uso di Wi-SUN. Ecosistema
 - 19.9.3. Sicurezza Wi-SUN
- 19.10. Altre tecnologie IoT
 - 19.10.1. Altre tecnologie IoT
 - 19.10.2. Casi d'uso ed ecosistema di altre tecnologie IoT
 - 19.10.3. Sicurezza in altre tecnologie IoT

Modulo 20. Piano di continuità operativa associato alla sicurezza

- 20.1. Piano di continuità operativa
 - 20.1.1. I piani di continuità operativa (BCP)
 - 20.1.2. Piano di continuità operativa (BCP). Aspetti chiave
 - 20.1.3. Piano di continuità operativa (BCP) per la valutazione dell'azienda
- 20.2. Parametri in un piano di continuità operativa (BCP)
 - 20.2.1. *Recovery Time Objective* (RTO) e *Recovery Point Objective* (RPO)
 - 20.2.2. Tempo massimo tollerabile (MTD)
 - 20.2.3. Livelli minimi di recupero (ROL)
 - 20.2.4. Obiettivo del punto di ripristino (RPO)
- 20.3. Progetti di continuità. Tipologia
 - 20.3.1. Piano di continuità operativa (BCP)
 - 20.3.2. Piano di continuità ICT
 - 20.3.3. Piano di ripristino in caso di disastro (DRP)
- 20.4. Gestione dei rischi connessi al BCP
 - 20.4.1. Analisi dell'impatto aziendale
 - 20.4.2. Vantaggi dell'implementazione di un BCP
 - 20.4.3. Mentalità basata sul rischio
- 20.5. Ciclo di vita di un piano di continuità operativa
 - 20.5.1. Fase 1: analisi dell'organizzazione
 - 20.5.2. Fase 2: determinazione della strategia di continuità
 - 20.5.3. Fase 3: risposta alla contingenza
 - 20.5.4. Fase 4: test, manutenzione e revisione
- 20.6. Fase di analisi organizzativa di un BCP
 - 20.6.1. Identificazione dei processi che rientrano nell'ambito di applicazione del BCP
 - 20.6.2. Identificazione delle aree aziendali critiche
 - 20.6.3. Identificazione delle dipendenze tra aree e processi
 - 20.6.4. Determinazione del MTD appropriato
 - 20.6.5. Prodotti. Creazione di un piano
- 20.7. Fase di determinazione della strategia di continuità in un BCP
 - 20.7.1. Ruoli nella fase di determinazione della strategia
 - 20.7.2. Compiti nella fase di determinazione della strategia
 - 20.7.3. Risultati da consegnare
- 20.8. Fase di risposta alla contingenza di un BCP
 - 20.8.1. Ruoli nella fase di risposta
 - 20.8.2. Compiti di questa fase
 - 20.8.3. Risultati da consegnare
- 20.9. Fase di test, manutenzione e revisione di un BCP
 - 20.9.1. Ruoli nella fase di test, manutenzione e revisione
 - 20.9.2. Lavori nella fase di test, manutenzione e revisione
 - 20.9.3. Risultati da consegnare
- 20.10. Standard ISO associati ai piani di continuità operativa (BCP)
 - 20.10.1. ISO 22301:2019
 - 20.10.2. ISO 22313:2020
 - 20.10.3. Altri standard ISO e internazionali correlati

Modulo 21. Analitica dei dati nell'organizzazione aziendale

- 21.1. Analisi di business
 - 21.1.1. Analisi di business
 - 21.1.2. Struttura del dato
 - 21.1.3. Fasi e elementi
- 21.2. Analisi dei dati nell'impresa
 - 21.2.1. Schede di valutazione e KPI per dipartimento
 - 21.2.2. Rapporto operativo, tattico e strategico
 - 21.2.3. Analisi dei dati applicata a ciascun dipartimento
 - 21.2.3.1. Marketing e comunicazione
 - 21.2.3.2. Commerciale
 - 21.2.3.3. Servizio clienti
 - 21.2.3.4. Acquisti



- 21.2.3.5. Amministrazione
- 21.2.3.6. Risorse Umane
- 21.2.3.7. Produzione
- 21.2.3.8. IT
- 21.3. Marketing e comunicazione
 - 21.3.1. KPI da misurare, applicazioni e benefici
 - 21.3.2. Sistemi di Marketing e *Data Warehouse*
 - 21.3.3. Implementazione di una struttura di analisi dei dati nel marketing
 - 21.3.4. Piano di marketing e comunicazione
 - 21.3.5. Strategia, previsione e gestione delle campagne
- 21.4. Commerciale e vendite
 - 21.4.1. Contributi dell'analisi dei dati nell'area commerciale
 - 21.4.2. Esigenze del dipartimento di vendite
 - 21.4.3. Studi di mercato
- 21.5. Servizio clienti
 - 21.5.1. Fidelizzazione
 - 21.5.2. Qualità personale e intelligenza emotiva
 - 21.5.3. Soddisfazione del cliente
- 21.6. Acquisti
 - 21.6.1. Analisi dei dati per le ricerche di mercato
 - 21.6.2. Analisi dei dati per le ricerche di concorrenza
 - 21.6.3. Altre applicazioni
- 21.7. Amministrazione
 - 21.7.1. Esigenze del dipartimento di Amministrazione
 - 21.7.2. *Data Warehouse* e analisi di rischio finanziario
 - 21.7.3. *Data Warehouse* e analisi di rischio di credito
- 21.8. Risorse umane
 - 21.8.1. Risorse Umane e benefici dell'analisi dei dati
 - 21.8.2. Strumenti di analisi dei dati nel dipartimento di Risorse Umane
 - 21.8.3. Applicazioni di analisi dei dati nel dipartimento di Risorse Umane

- 21.9. Produzione
 - 21.9.1. Analisi dei dati nel dipartimento di Produzione
 - 21.9.2. Applicazioni
 - 21.9.3. Benefici
- 21.10. IT
 - 21.10.1. Dipartimento di IT
 - 21.10.2. Analisi dei dati e trasformazione digitale
 - 21.10.3. Innovazione e produttività

Modulo 22. Gestione, manipolazione dei Dati e delle informazioni per la Data Science

- 22.1. Statistica. Variabili, indici e rapporti
 - 22.1.1. La Statistica
 - 22.1.2. Dimensioni statistiche
 - 22.1.3. Variabili, indici e rapporti
- 22.2. Tipologia del dato
 - 22.2.1. Qualitativi
 - 22.2.2. Quantitativi
 - 22.2.3. Caratterizzazione e categoria
- 22.3. Conoscenza dei Dati partendo dalle misurazioni
 - 22.3.1. Misure di centralizzazione
 - 22.3.2. Misure di dispersione
 - 22.3.3. Correlazione
- 22.4. Conoscenza dei Dati partendo dai grafici
 - 22.4.1. Visualizzazione in funzione al tipo di dato
 - 22.4.2. Interpretazione dell'informazione grafica
 - 22.4.3. Personalizzazione della grafica con R
- 22.5. Probabilità
 - 22.5.1. Probabilità
 - 22.5.2. Funzione della probabilità
 - 22.5.3. Distribuzione

- 22.6. Raccolta di Dati
 - 22.6.1. Metodologia di raccolta
 - 22.6.2. Strumenti di raccolta
 - 22.6.3. Canali di raccolta
- 22.7. Pulizia del dato
 - 22.7.1. Fasi di pulizia dei Dati
 - 22.7.2. Qualità del dato
 - 22.7.3. Manipolazione dei Dati (con R)
- 22.8. Analisi dei Dati, interpretazione e valutazione dei risultati
 - 22.8.1. Misure statistiche
 - 22.8.2. Indici di relazione
 - 22.8.3. Data Mining
- 22.9. Magazzino dati (*Data Warehouse*)
 - 22.9.1. Elementi
 - 22.9.2. Progettazione
- 22.10. Disponibilità del dato
 - 22.10.1. Accesso
 - 22.10.2. Utilità
 - 22.10.3. Sicurezza

Modulo 23. Dispositivi e piattaforme IoT come base per la Data Science

- 23.1. *Internet of Things*
 - 23.1.1. Internet del futuro, *Internet of Things*
 - 23.1.2. Il consorzio di internet industriale
- 23.2. Architettura di riferimento
 - 23.2.1. Architettura di riferimento
 - 23.2.2. Strati
 - 23.2.3. Componenti
- 23.3. Sensori e dispositivi IoT
 - 23.3.1. Componenti principali
 - 23.3.2. Sensori e azionatori

- 23.4. Comunicazioni e protocolli
 - 23.4.1. Protocolli. Modello OSI
 - 23.4.2. Tecnologie di comunicazione
- 23.5. Piattaforme Cloud per IoT e IIoT
 - 23.5.1. Piattaforme con proposito generale
 - 23.5.2. Piattaforme industriali
 - 23.5.3. Piattaforme con codice aperto
- 23.6. Gestione dei Dati su piattaforme IoT
 - 23.6.1. Meccanismi di gestione dei Dati. Dati aperti
 - 23.6.2. Scambio e visualizzazione dei Dati
- 23.7. Sicurezza in IoT
 - 23.7.1. Requisiti e aree di sicurezza
 - 23.7.2. Strategie di sicurezza in IIoT
- 23.8. Applicazioni IoT
 - 23.8.1. Cure intelligenti
 - 23.8.2. Salute e condizione fisica
 - 23.8.3. Casa intelligente
 - 23.8.4. Altre applicazioni
- 23.9. Applicazioni di IIoT
 - 23.9.1. Fabbricazione
 - 23.9.2. Trasporto
 - 23.9.3. Energia
 - 23.9.4. Agricoltura e allevamento
 - 23.9.5. Altri settori
- 23.10. Industria 4.0
 - 23.10.1. IoRT (*Internet of Robotics Things*)
 - 23.10.2. Fabbricazione additiva 3D
 - 23.10.3. Big Data Analytics

Modulo 24. Rappresentazione grafica per l'analisi dei Dati

- 24.1. Analisi esplorativa
 - 24.1.1. Rappresentazione per l'analisi delle informazioni
 - 24.1.2. Il valore della rappresentazione grafica
 - 24.1.3. Nuovi paradigmi della rappresentazione grafica
- 24.2. Ottimizzazione per la Data Science
 - 24.2.1. Gamma di colori e design
 - 24.2.2. La Gestalt nella rappresentazione grafica
 - 24.2.3. Errori da evitare e consigli
- 24.3. Fonti di Dati base
 - 24.3.1. Per la rappresentazione della qualità
 - 24.3.2. Per la rappresentazione della quantità
 - 24.3.3. Per la rappresentazione del tempo
- 24.4. Fonti di Dati complessi
 - 24.4.1. Archivi, liste e database (DB)
 - 24.4.2. Dati aperti
 - 24.4.3. Dati di generazione continua
- 24.5. Tipi di grafici
 - 24.5.1. Rappresentazioni di base
 - 24.5.2. Rappresentazione di blocchi
 - 24.5.3. Rappresentazione per l'analisi della dispersione
 - 24.5.4. Rappresentazioni circolari
 - 24.5.5. Rappresentazioni a bolla
 - 24.5.6. Rappresentazioni geografiche
- 24.6. Tipi di visualizzazione
 - 24.6.1. Comparativo e relazionale
 - 24.6.2. Distribuzione
 - 24.6.3. Gerarchia

- 24.7. Progettazione di report con rappresentazione grafica
 - 24.7.1. Applicazione dei grafici nei rapporti di marketing
 - 24.7.2. Applicazione dei grafici in dashboard e KPI
 - 24.7.3. Applicazione dei grafici nei piani strategici
 - 24.7.4. Altri usi: scienza, salute, business
- 24.8. Narrazione grafica
 - 24.8.1. Narrazione grafica
 - 24.8.2. Evoluzione
 - 24.8.3. Utilità
- 24.9. Strumenti per la visualizzazione
 - 24.9.1. Strumenti avanzati
 - 24.9.2. Software online
 - 24.9.3. Open Source
- 24.10. Nuove tecnologie per la visualizzazione dei Dati
 - 24.10.1. Sistemi per la virtualizzazione della realtà
 - 24.10.2. Sistemi per l'aumento e il miglioramento della realtà
 - 24.10.3. Sistemi intelligenti

Modulo 25. Strumenti di Data science

- 25.1. Data Science
 - 25.1.1. Data Science
 - 25.1.2. Strumenti avanzati per i Data scientist
- 25.2. Dati, informazioni e conoscenza
 - 25.2.1. Dati, informazioni e conoscenza
 - 25.2.2. Tipi di dati
 - 25.2.3. Fonti di Dati
- 25.3. Dai Dati all'informazione
 - 25.3.1. Analisi dei dati
 - 25.3.2. Tipi di analisi
 - 25.3.3. Estrazione di informazioni da un Dataset
- 25.4. Estrazione di informazioni tramite visualizzazione
 - 25.4.1. La visualizzazione come strumento di analisi
 - 25.4.2. Metodi di visualizzazione
 - 25.4.3. Visualizzazione di un set di Dati

- 25.5. Qualità dei Dati
 - 25.5.1. Dati di qualità
 - 25.5.2. Pulizia di Dati
 - 25.5.3. Pre-elaborazione base dei Dati
- 25.6. Dataset
 - 25.6.1. Arricchimento del Dataset
 - 25.6.2. La maledizione della dimensionalità
 - 25.6.3. Modifica del nostro set di Dati
- 25.7. Squilibrio
 - 25.7.1. Squilibrio di classe
 - 25.7.2. Tecniche di mitigazione dello squilibrio
 - 25.7.3. Equilibrio di un Dataset
- 25.8. Modelli non supervisionati
 - 25.8.1. Modelli non controllati
 - 25.8.2. Metodi
 - 25.8.3. Classificazione con modelli non controllati
- 25.9. Modelli supervisionati
 - 25.9.1. Modelli controllati
 - 25.9.2. Metodi
 - 25.9.3. Classificazione con modelli controllati
- 25.10. Strumenti e buone pratiche
 - 25.10.1. Buone pratiche per i Data scientist
 - 25.10.2. Il modello migliore
 - 25.10.3. Strumenti utili

Modulo 26. Data Mining Selezione, pre-elaborazione e trasformazione

- 26.1. Inferenza statistica
 - 26.1.1. Statistica descrittiva e Inferenza statistica
 - 26.1.2. Procedure parametriche
 - 26.1.3. Procedure non parametriche
- 26.2. Analisi esplorativa
 - 26.2.1. Analisi descrittiva
 - 26.2.2. Visualizzazione
 - 26.2.3. Preparazione dei Dati

- 26.3. Preparazione dei Dati
 - 26.3.1. Integrazione e pulizia di Dati
 - 26.3.2. Normalizzazione dei dati
 - 26.3.3. Trasformazione degli attributi
- 26.4. I valori mancanti
 - 26.4.1. Trattamenti dei valori mancanti
 - 26.4.2. Metodi di imputazione a massima verosimiglianza
 - 26.4.3. Imputazione di valori mancanti mediante apprendimento automatico
- 26.5. Rumore nei Dati
 - 26.5.1. Classi di rumore e attributi
 - 26.5.2. Filtraggio del rumore
 - 26.5.3. Effetto del rumore
- 26.6. La maledizione della dimensionalità
 - 26.6.1. *Oversampling*
 - 26.6.2. *Undersampling*
 - 26.6.3. Riduzione dei Dati multidimensionali
- 26.7. Da attributi continui a discreti
 - 26.7.1. Dati continui e Discreti
 - 26.7.2. Processo di discretizzazione
- 26.8. I Dati
 - 26.8.1. Selezione dei Dati
 - 26.8.2. Prospettiva e criteri di selezione
 - 26.8.3. Metodi di selezione
- 26.9. Selezione di istanze
 - 26.9.1. Metodi per la selezione di istanze
 - 26.9.2. Selezione di prototipi
 - 26.9.3. Metodi avanzati per la selezione di istanze
- 26.10. Pre-elaborazione dei Dati negli ambienti *Big Data*
 - 26.10.1. *Big Data*
 - 26.10.2. Pre-elaborazione classica e Massiva
 - 26.10.3. *Smart Data*

Modulo 27. Prevedibilità e analisi dei fenomeni stocastici

- 27.1. Serie temporale
 - 27.1.1. Serie temporale
 - 27.1.2. Utilità e applicabilità
 - 27.1.3. Casi di studio correlati
- 27.2. Serie temporali
 - 27.2.1. Andamento stagionale della serie temporale
 - 27.2.2. Variazioni tipiche
 - 27.2.3. Analisi dei residui
- 27.3. Tipologie
 - 27.3.1. Stazionarie
 - 27.3.2. Non stazionarie
 - 27.3.3. Trasformazioni e adattamenti
- 27.4. Schemi per le serie temporali
 - 27.4.1. Schema additivo (modello)
 - 27.4.2. Schema moltiplicativo (modello)
 - 27.4.3. Procedure per determinare il tipo di modello
- 27.5. Metodi di base di *Forecast*
 - 27.5.1. Media
 - 27.5.2. Naïve
 - 27.5.3. Naïve stagionale
 - 27.5.4. Confronto di metodi
- 27.6. Analisi dei residui
 - 27.6.1. Autocorrelazione
 - 27.6.2. ACF dei residui
 - 27.6.3. Test di correlazione
- 27.7. Regressione nel contesto delle serie temporali
 - 27.7.1. ANOVA
 - 27.7.2. Fondamenti
 - 27.7.3. Applicazione pratica
- 27.8. Modelli predittivi di serie temporali
 - 27.8.1. ARIMA
 - 27.8.2. Livellamento esponenziale

27.9. Manipolazione e analisi delle serie temporali con R

27.9.1. Preparazione dei Dati

27.9.2. Identificazione dei modelli

27.9.3. Analisi del modello

27.9.4. Previsione

27.10. Analisi grafica combinata con R

27.10.1. Situazioni tipiche

27.10.2. Applicazione pratica per la risoluzione di problemi semplici

27.10.3. Applicazione pratica per la risoluzione di problemi avanzati

Modulo 28. Progettazione e sviluppo di sistemi intelligenti

28.1. Pre-elaborazione dei Dati

28.1.1. Pre-elaborazione dei Dati

28.1.2. Trasformazione dei Dati

28.1.3. Data Mining

28.2. Apprendimento automatico

28.2.1. Apprendimento supervisionato e non

28.2.2. Apprendimento di rinforzo

28.2.3. Altri paradigmi di apprendimento

28.3. Algoritmi di classificazione

28.3.1. Apprendimento automatico indotto

28.3.2. SVM e KNN

28.3.3. Metriche e punteggi per la classificazione

28.4. Algoritmi di regressione

28.4.1. Regressione lineare, regressione logistica e modelli non lineari

28.4.2. Serie temporale

28.4.3. Metriche e punteggi per la regressione

28.5. Algoritmi di clustering

28.5.1. Tecniche di clustering gerarchico

28.5.2. Tecniche di clustering partizionale

28.5.3. Metriche e punteggi per il *clustering*

28.6. Tecniche di regole associative

28.6.1. Metodi per l'estrazione di regole

28.6.2. Metriche e punteggi per gli algoritmi di regole associative

28.7. Tecniche di classificazione avanzata: Multiclassificatori

28.7.1. Algoritmi di *bagging*

28.7.2. Classificatore *Random Forests*

28.7.3. "Boosting" per alberi decisionali

28.8. Modelli grafici probabilistici

28.8.1. Modelli probabilistici

28.8.2. Reti bayesiane: Proprietà, rappresentazione e parametrizzazione

28.8.3. Altri modelli grafici probabilistici

28.9. Reti neuronali

28.9.1. Apprendimento automatico con reti neuronali artificiali

28.9.2. Reti *feedforward*

28.10. Apprendimento profondo

28.10.1. Reti *feedforward* profonde

28.10.2. Reti neurali convoluzionali e modelli di sequenza

28.10.3. Strumenti per l'implementazione di reti neurali profonde

Modulo 29. Architetture e sistemi ad alta intensità di Dati

29.1. Requisiti non funzionali: I pilastri delle applicazioni Big Data

29.1.1. Affidabilità

29.1.2. Adattamento

29.1.3. Mantenimento

29.2. Modelli di Dati

29.2.1. Modello relazionale

29.2.2. Modello documentale

29.2.3. Modello di Dati tipo grafo

29.3. Database: Gestione dell'archiviazione e recupero dei Dati

29.3.1. Indici Hash

29.3.2. Archiviazione strutturata in *Log*

29.3.3. Alberi B

29.4. Formati di codifica dei Dati

29.4.1. Formati specifici di linguaggio

29.4.2. Formati standard

29.4.3. Formati di codifica binari

29.4.4. Flusso di Dati tra i processi

- 29.5. Risposta
 - 29.5.1. Obiettivi di risposta
 - 29.5.2. Modelli di risposta
 - 29.5.3. Problemi di risposta
- 29.6. Transazioni distribuite
 - 29.6.1. Transazione
 - 29.6.2. Protocolli per le transazioni distribuite
 - 29.6.3. Transazioni serializzabili
- 29.7. Suddivisione
 - 29.7.1. Forme di suddivisione
 - 29.7.2. Interazione dell'indice secondario e suddiviso
 - 29.7.3. Bilanciamento delle suddivisioni
- 29.8. Elaborazione dei *Dati Offline*
 - 29.8.1. Elaborazione per lotti
 - 29.8.2. File system distribuiti
 - 29.8.3. MapReduce
- 29.9. Elaborazione dei Dati in tempo reale
 - 29.9.1. Tipi di *Broker* di messaggi
 - 29.9.2. Rappresentazione dei Database come flussi di Dati
 - 29.9.3. Processo dei flussi di Dati
- 29.10. Applicazioni pratiche nell'azienda
 - 29.10.1. Coerenza nelle letture
 - 29.10.2. Approccio olistico ai Dati
 - 29.10.3. Scaling di un servizio distribuito
- 30.3. Servizi finanziari
 - 30.3.1. Implicazioni dell'IA e dell'analisi dei Dati nel settore dei servizi finanziari
 - 30.3.2. Uso nei servizi finanziari
 - 30.3.3. Potenziali rischi legati all'uso dell'IA
- 30.4. Retail
 - 30.4.1. Implicazioni dell'IA e dell'analisi dei Dati nel settore del *Retail*
 - 30.4.2. Uso nel *Retail*
 - 30.4.3. Potenziali rischi legati all'uso dell'IA
- 30.5. Industria 4.0
 - 30.5.1. Implicazioni dell'IA e dell'analisi dei Dati nell'Industria 4.0
 - 30.5.2. Uso nell'Industria 4.0
- 30.6. Rischi e tendenze nell'Industria 4.0
 - 30.6.1. Potenziali rischi legati all'uso dell'IA
- 30.7. Pubblica amministrazione
 - 30.7.1. Implicazioni dell'IA e dell'analisi dei Dati alla Pubblica Amministrazione
 - 30.7.2. Uso nella Pubblica Amministrazione
 - 30.7.3. Potenziali rischi legati all'uso dell'IA
- 30.8. Educazione
 - 30.8.1. Implicazioni dell'IA e dell'analisi dei Dati all'Istruzione
 - 30.8.2. Potenziali rischi legati all'uso dell'IA
- 30.9. Silvicoltura e agricoltura
 - 30.9.1. Implicazioni dell'IA e dell'analisi dei Dati alla silvicoltura e all'agricoltura
 - 30.9.2. Uso nella Silvicoltura e nell'Agricoltura
 - 30.9.3. Potenziali rischi legati all'uso dell'IA
- 30.10. Risorse umane
 - 30.10.1. Implicazioni dell'IA e dell'analisi dei Dati nella gestione di risorse umane
 - 30.10.2. Applicazioni pratiche nel mondo degli affari
 - 30.10.3. Potenziali rischi legati all'uso dell'IA

Modulo 30. Applicazione pratica della Data Science nei settori aziendali

- 30.1. Settore sanitario
 - 30.1.1. Implicazioni dell'IA e dell'analisi dei Dati nel settore sanitario
 - 30.1.2. Opportunità e sfide
- 30.2. Rischi e tendenze nel settore sanitario
 - 30.2.1. Uso nel settore sanitario
 - 30.2.2. Potenziali rischi legati all'uso dell'IA

06

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*.



66

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.

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

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

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

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





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

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

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

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

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



Materiale di studio

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

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



Master class

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

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



Pratiche di competenze e competenze

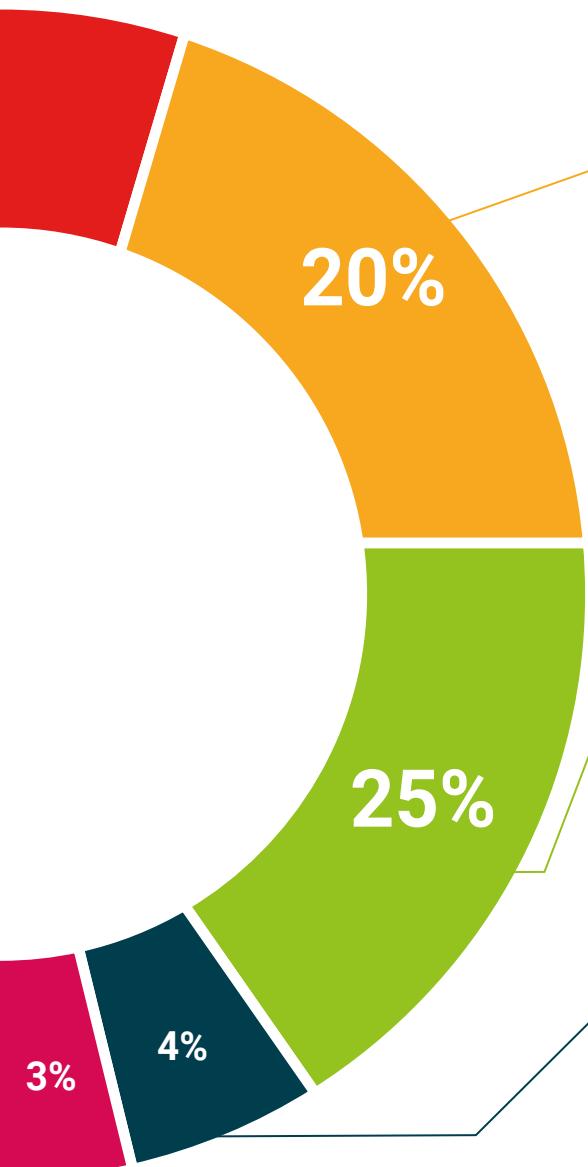
Svolgerai attività per sviluppare competenze e capacità specifiche in ogni area tematica. Pratiche e dinamiche per acquisire e sviluppare le competenze e le abilità che uno specialista deve sviluppare nel quadro della globalizzazione in cui viviamo.



Letture complementari

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





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

Casi di Studio



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".

Riepiloghi interattivi



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.

Testing & Retesting



07

Titolo

Il Master Specialistico in Computer Science, Cybersecurity e Data Analytics ti garantisce, oltre alla preparazione più rigorosa e aggiornata, l'accesso a una qualifica di Master Specialistico rilasciata da TECH Global University.



66

*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 di **Master Specialistico in Computer Science, Cybersecurity e Data Analytics** rilasciato da **TECH Global University**, la più grande università digitale del mondo.

TECH Global University è un'Università Ufficiale Europea riconosciuta pubblicamente dal Governo di Andorra ([bollettino ufficiale](#)). Andorra fa parte dello Spazio Europeo dell'Istruzione Superiore (EHEA) dal 2003. L'EHEA è un'iniziativa promossa dall'Unione Europea che mira a organizzare il quadro formativo internazionale e ad armonizzare i sistemi di istruzione superiore dei Paesi membri di questo spazio. Il progetto promuove valori comuni, l'implementazione di strumenti congiunti e il rafforzamento dei meccanismi di garanzia della qualità per migliorare la collaborazione e la mobilità tra studenti, ricercatori e accademici.



Questo titolo privato di **TECH Global University** è un programma europeo di formazione continua e aggiornamento professionale che garantisce l'acquisizione di competenze nella propria area di conoscenza, conferendo allo studente che supera il programma un elevato valore curriculare.

Titolo: Master Specialistico in Computer Science, Cybersecurity e Data Analytics

Modalità: online

Durata: 2 anni

Accreditamento: 120 ECTS

Master Specialistico in Computer Science, Cybersecurity e Data Analytics

Distribuzione generale del Programma

Corso	Insegnamento	ECTS	Codice	Corso	Insegnamento	ECTS	Codice
1 ^o	Fondamenti di programmazione	4	OB	2 ^o	Sicurezza nelle comunicazioni e nel funzionamento del software	4	OB
1 ^o	Struttura dei dati	4	OB	2 ^o	Sicurezza negli ambienti Cloud	4	OB
1 ^o	Algoritmo e complessità	4	OB	2 ^o	Sicurezza delle comunicazioni nei dispositivi IoT	4	OB
1 ^o	Progettazione avanzata degli algoritmi	4	OB	2 ^o	Piano di continuità operativa associato alla sicurezza	4	OB
1 ^o	Programmazione avanzata	4	OB	2 ^o	Analitica dei dati nell'organizzazione aziendale	4	OB
1 ^o	Informatica teorica	4	OB	3 ^o	Manipolazione dei Dati e delle informazioni per la Data Science	4	OB
1 ^o	Teoria degli autori e linguaggi formali	4	OB	3 ^o	Dispositivi e piattaforme IoT come base per la Data Science	4	OB
1 ^o	Progettatori di algoritmi	4	OB	3 ^o	Rappresentazione grafica per l'analisi dei Dati	4	OB
1 ^o	Computer grafica e visualizzazione	4	OB	3 ^o	Strumenti di Data science	4	OB
1 ^o	Informatica bio-ispirata	4	OB	3 ^o	Data Mining Selezione, pre-elaborazione e trasformazione	4	OB
2 ^o	Sicurezza nella progettazione e nello sviluppo dei sistemi	4	OB	3 ^o	Prevedibilità e analisi dei fenomeni stocastici Progettazione e sviluppo di sistemi intelligenti	4	OB
2 ^o	Strutture e modelli per la sicurezza delle informazioni	4	OB	3 ^o	Architetture e sistemi ad alta intensità di Dati	4	OB
2 ^o	Gestione della sicurezza IT	4	OB	3 ^o	Applicazione pratica della Data Science nei settori aziendali	4	OB
2 ^o	Analisi dei rischi e ambiente di sicurezza IT	4	OB				
2 ^o	La crittografia nell'IT	4	OB				
2 ^o	Gestione dell'identità e degli accessi nella sicurezza informatica	4	OB				

Dott. Pedro Navarro Illana
Rettore

tech global university

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



Master Specialistico
Computer Science,
Cybersecurity
e Data Analytics

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

Master Specialistico

Computer Science, Cybersecurity e Data Analytics

