Master
Telematica

tech global university

tech global university

Master

Telematica

- Modalità: **online**
- Durata: **12 mesi**
- Titolo: **TECH Global University**
- Accreditamento: **60 ECTS**
- Orario: **a scelta**
- Esami: **online**

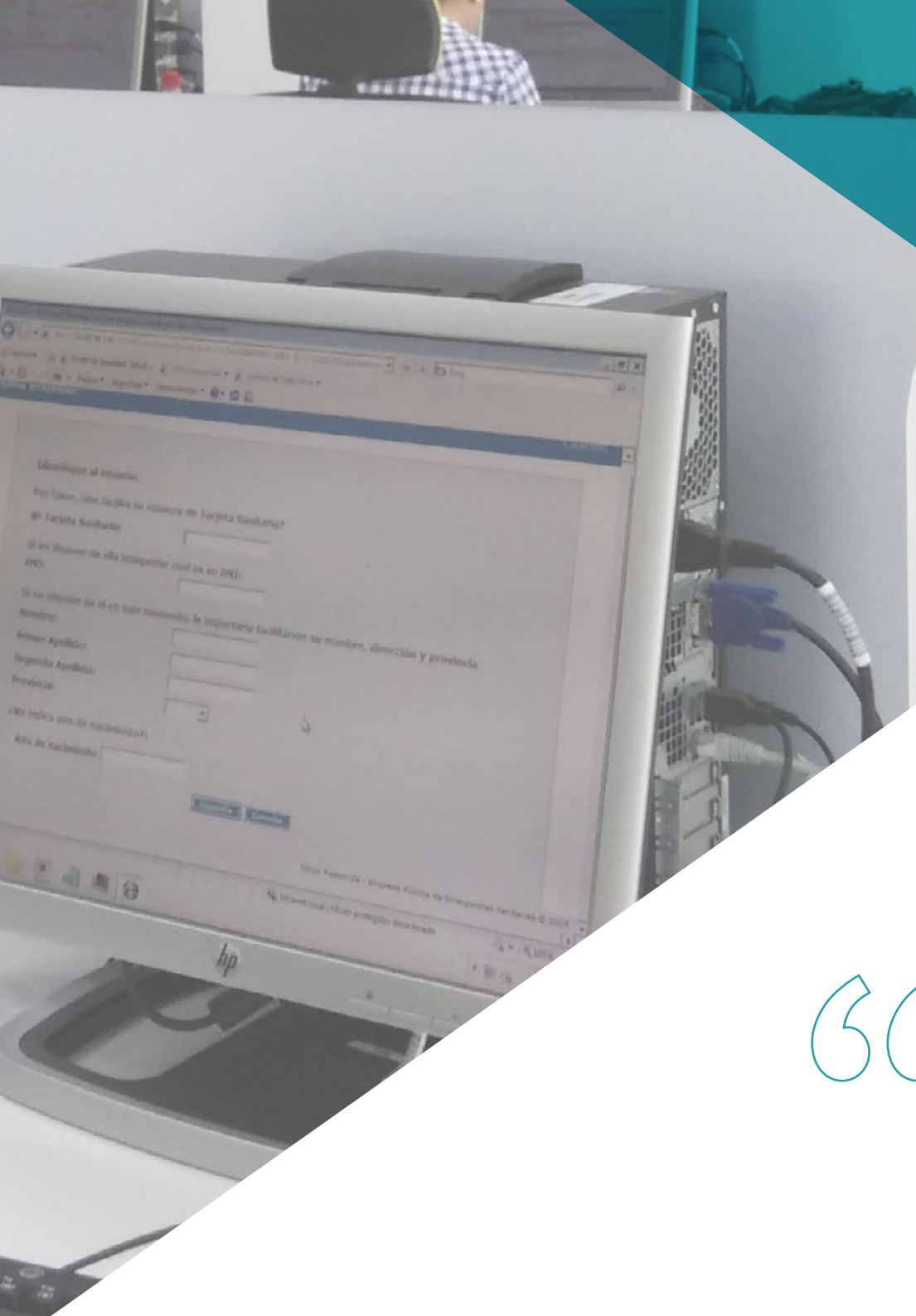
Accesso al sito web: www.techtitute.com/it/informatica/master/master-telematica

Indice

01

Presentazione

L'informatica e la tecnologia della comunicazione si combinano nella Telematica per rispondere allo sviluppo e all'implementazione di tecniche, processi, conoscenze e dispositivi che consentono l'invio e la ricezione efficiente di dati. Questo campo di lavoro e la costante incorporazione dei progressi tecnologici richiedono un aggiornamento permanente e di ampio respiro. Questo studio offre l'aggiornamento o la specializzazione di qualità di cui il professionista ha bisogno con un programma aggiornato e altamente qualificato. Un corso di alta qualità che permetterà di progredire nella propria professione.



Completo, completamente aggiornato e adattabile alle tue disponibilità, questo programma è uno strumento di alta qualità per l'informatico che desidera ampliare le proprie competenze reali"

I progressi nelle telecomunicazioni sono costanti, poiché si tratta di uno dei settori in più rapida evoluzione. È quindi necessario disporre di esperti in informatica in grado di adattarsi a questi cambiamenti e di avere una conoscenza diretta dei nuovi strumenti e delle nuove tecniche che stanno emergendo in questo campo.

Il programma in Telematica tratta tutte le materie coinvolte in questo campo. Il suo studio ha un chiaro vantaggio rispetto ad altri Master che si concentrano su blocchi specifici, impedendo agli studenti di conoscere le interrelazioni con altre aree incluse nel campo multidisciplinare delle telecomunicazioni. Il personale docente di questo programma, inoltre, ha effettuato un'attenta selezione di ciascuna delle materie di questa specializzazione, per offrire allo studente un'opportunità di studio il più possibile completa e sempre legata all'attualità.

Questo programma è rivolto a coloro che sono interessati a raggiungere un livello superiore di conoscenza della Telematica. L'obiettivo principale è consentire agli studenti di applicare le conoscenze acquisite in questo programma nel mondo reale, in un ambiente di lavoro che riproduce le condizioni che potrebbero incontrare nel loro futuro, in modo rigoroso e realistico.

Trattandosi inoltre di un programma 100% online, lo studente non è condizionato da orari fissi o dalla necessità di spostarsi in un altro luogo fisico, ma può accedere ai contenuti in qualsiasi momento della giornata, conciliando il suo lavoro o la sua vita personale con quella accademica.

Questo **Master in Telematica** possiede il programma più completo e aggiornato del mercato. Le caratteristiche principali del programma sono:

- Sviluppo di casi pratici presentati da esperti in Telematica
- Contenuti grafici, schematici ed eminentemente pratici che forniscono informazioni scientifiche e pratiche sulle discipline essenziali per l'esercizio della professione
- Esercizi pratici con cui è possibile valutare sé stessi per migliorare l'apprendimento
- Speciale enfasi sulle metodologie innovative in ambito della Telematica
- Lezioni teoriche, domande all'esperto, forum di discussione su temi controversi e lavoro di riflessione individuale
- Contenuti disponibili da qualsiasi dispositivo fisso o portatile provvisto di connessione a internet

Includi nelle tue competenze la capacità di intervenire nei diversi campi della telematica, con un percorso di apprendimento che darà impulso al tuo sviluppo professionale"

Questo programma è il miglior investimento che tu possa fare nella scelta di un programma di aggiornamento delle tue conoscenze in Telematica"

Il materiale didattico con cui svilupperai il tuo studio è un compendio di alta qualità che ti permetterà di avanzare in modo comodo e semplice.

Questo programma 100% online ti permetterà di conciliare i tuoi studi con l'attività professionale.

Il personale docente comprende professionisti del settore, che forniscono agli studenti le competenze necessarie a intraprendere un percorso di studio eccellente.

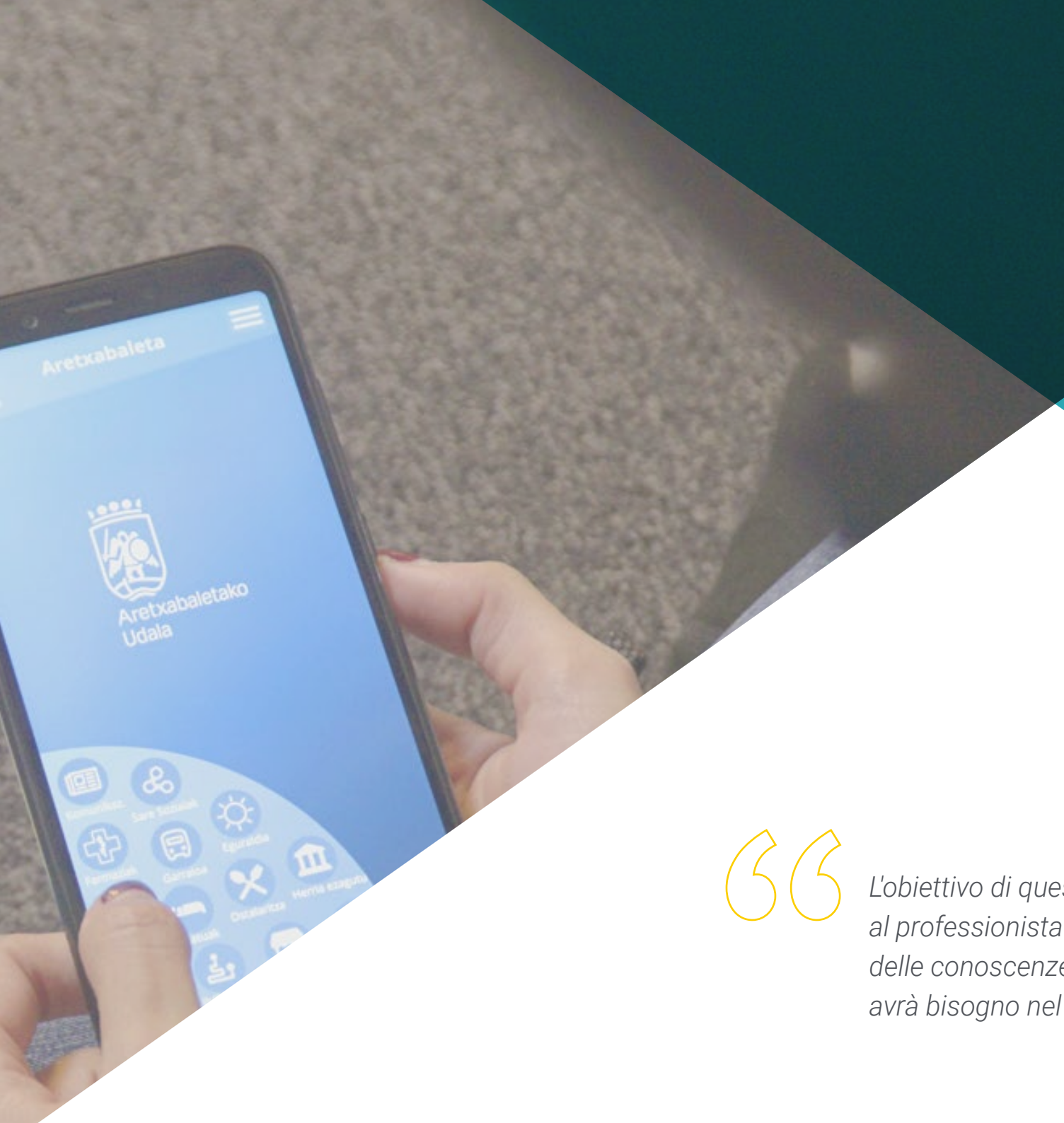
I contenuti multimediali, sviluppati in base alle ultime tecnologie educative, forniranno al professionista un apprendimento coinvolgente e localizzato, ovvero inserito in un contesto reale.

La creazione di questo programma è incentrata sull'Apprendimento Basato sui Problemi, mediante il quale il professionista deve cercare di risolvere le diverse situazioni di pratica professionale che gli si presentano durante il corso. Lo studente potrà usufruire di un innovativo sistema di video interattivi creati da esperti di rinomata fama nel settore della Telematica.

02

Obiettivi

Il programma in Telematica si propone di offrire agli informatici uno studio completo e aggiornato di tutte le aree coinvolte nell'intervento telematico, con la sicurezza e la qualità di un programma creato con un criterio di totale eccellenza.



L'obiettivo di questo programma è fornire al professionista una panoramica completa delle conoscenze teoriche e pratiche di cui avrà bisogno nel campo della Telematica"

Obiettivo generale

- Capacitare gli studenti affinché siano in grado di sviluppare applicazioni telematiche, analizzare dati o svolgere compiti di sicurezza digitale, ecc.

Un'opportunità creata per i professionisti alla ricerca di un corso intensivo ed efficace con cui compiere un significativo passo avanti nell'esercizio della propria attività"

Obiettivi specifici

Reti di computer

- Acquisire le conoscenze essenziali delle reti informatiche su internet
- Comprendere il funzionamento dei diversi livelli che definiscono un sistema in rete, come i livelli di applicazione, trasporto, rete e collegamento
- Comprendere la composizione delle LAN, la loro topologia e i loro elementi di rete e interconnessione
- Imparare a conoscere il funzionamento dell'indirizzamento IP e il subnetting
- Comprendere la struttura delle reti wireless e mobili, compresa la nuova rete 5G
- Conoscere i diversi meccanismi di sicurezza della rete e i diversi protocolli di sicurezza di internet

Sistemi distribuiti

- Padroneggiare i principi di base dei sistemi distribuiti
- Imparare a caratterizzare e classificare i sistemi distribuiti in base a una serie di parametri di base
- Comprendere i diversi tipi di modelli utilizzati nei sistemi distribuiti
- Comprendere le attuali architetture che implementano il concetto di sistema di file distribuito
- Essere in grado di analizzare gli algoritmi di sincronizzazione dei processi e degli oggetti, la definizione degli orologi logici e la coerenza temporale delle informazioni
- Comprendere il sistema di denominazione utilizzato in Internet, noto come DNS (Domain Name System)
- Conoscere il funzionamento dell'indirizzamento IP e del subnetting

Sicurezza nei sistemi e nelle reti di comunicazione

- Ottenere una panoramica sulla sicurezza, la crittografia e le crittoanalisi classiche
- Comprendere i fondamenti della crittografia simmetrica e asimmetrica e i loro principali algoritmi
- Analizzare la natura degli attacchi di rete e i diversi tipi di architetture di sicurezza
- Comprendere le tecniche di protezione del sistema e di sviluppo del codice sicuro
- Conoscere i componenti essenziali di ***botnets*** e spam, oltre che del malware e del codice dannoso
- Porre le basi per l'analisi forense nel mondo del software e del controllo informatico

Reti e infrastrutture aziendali

- Padroneggiare gli aspetti avanzati dell'interconnessione delle infrastrutture, essenziali per la progettazione e la pianificazione di reti ad alta velocità
- Conoscere le principali caratteristiche e tecnologie delle reti di trasporto
- Comprendere le architetture WAN classiche, All-Ethernet, MPLS, VPN
- Analizzare gli aspetti fondamentali dell'evoluzione delle reti verso le NGN (Next Generation Networks)
- Comprendere i requisiti avanzati di QoS, routing, controllo della congestione e affidabilità
- Conoscere e saper applicare gli standard di rete internazionali

Architetture di sicurezza

- Comprendere i principi di base della sicurezza informatica
- Padroneggiare gli standard di sicurezza informatica e i processi di certificazione
- Analizzare le basi organizzative e crittografiche su cui si fondano le tecnologie di sicurezza
- Identificare le principali minacce e vulnerabilità dei diversi elementi coinvolti nelle TIC, nonché le loro cause
- Approfondire gli strumenti di sicurezza di rete e delle loro funzioni specifiche
- Saper applicare le tecnologie che compongono un'architettura di sicurezza ICT, nelle sue diverse prospettive

Centri dati, funzionamento della rete e servizi

- Essere in grado di progettare, operare, gestire e mantenere reti, servizi e contenuti forniti attraverso un Data Center
- Conoscere tutti gli elementi essenziali che compongono un Data Center e gli standard e le certificazioni esistenti
- Analizzare l'impatto economico di un'infrastruttura di Data Center in termini di prestazioni ed efficienza
- Identificare gli elementi hardware di un Data Center in infrastrutture reali
- Comprendere le implicazioni di sicurezza delle diverse soluzioni per l'offerta di servizi da parte dei fornitori di mercato
- Comprendere il funzionamento del processo di virtualizzazione
- Comprendere i vantaggi, i benefici e i modelli di adozione del Cloud

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 interfacce 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

Ingegneria dei sistemi e dei servizi di rete

- Padroneggiare i concetti fondamentali dell'ingegneria dei servizi
- Conoscere i principi di base della gestione della configurazione di sistemi software in evoluzione
- Conoscere le tecnologie e gli strumenti per la fornitura di servizi telematici
- Conoscere i diversi stili architetturali di un sistema software, comprenderne le differenze e saper scegliere quello più appropriato in base ai requisiti del sistema
- Comprendere i processi di validazione e verifica e la loro relazione con le altre fasi del ciclo di vita
- Essere in grado di integrare sistemi per l'acquisizione, la rappresentazione, l'elaborazione, la memorizzazione, la gestione e la presentazione di informazioni multimediali per la realizzazione di servizi di telecomunicazione e applicazioni telematiche

- Conoscere gli elementi comuni per la progettazione dettagliata di un sistema software
- Acquisire competenze di programmazione, simulazione e validazione di servizi e applicazioni telematiche, in rete e distribuite
- Comprendere il processo e le attività di transizione, configurazione, implementazione e funzionamento
- Comprendere i processi di gestione, automazione e ottimizzazione della rete

Audit dei Sistemi Informativi

- Padroneggiare i concetti, gli standard e le metodologie principali dell'audit dei sistemi
- Conoscere gli elementi organizzativi e il quadro giuridico degli audit
- Ottenere una guida di riferimento per la progettazione di nuovi sistemi di controllo interno informatico
- Comprendere e identificare i rischi derivanti dagli sviluppi tecnologici
- Rilevare come i diversi sistemi informativi soddisfino o meno i requisiti di sicurezza desiderati
- Essere in grado di realizzare un processo di miglioramento continuo della sicurezza informatica

Gestione di Progetti

- Comprendere i concetti fondamentali del project management e del ciclo di vita della Gestione dei Progetti
- Comprendere le diverse fasi della gestione del progetto, come l'avvio, la pianificazione, la gestione degli *stakeholder* e il campo di applicazione
- Pianificare una tabella di marcia per la gestione del tempo, lo sviluppo del budget e la risposta ai rischi
- Comprendere il funzionamento della gestione della qualità nei progetti, compresi la pianificazione, la garanzia, il controllo, i concetti statistici e gli strumenti disponibili
- Comprendere il funzionamento dei processi di approvvigionamento, esecuzione, monitoraggio, controllo e chiusura di un progetto
- Acquisire le conoscenze essenziali relative alla responsabilità professionale nella gestione dei progetti

03

Competenze

Dopo aver superato le valutazioni del programma in Telematica, gli studenti avranno acquisito le competenze necessarie per intervenire in modo sicuro e aggiornato nei diversi ambiti di lavoro che la Telematica sviluppa. Un processo di crescita delle competenze che farà la differenza nella loro carriera professionale.

Acquisisci le competenze di uno specialista di telematica, inizia a intervenire in questo settore con la visione di un professionista all'avanguardia"

Competenza generale

- Sviluppare applicazioni telematiche e svolgere compiti di sicurezza digitale

Specializzarsi con i migliori ed essere all'avanguardia nell'intervento professionale"

Competenze specifiche

- Conoscere l'intera struttura delle reti di computer
- Padroneggiare i sistemi distribuiti e saperli classificare
- Eseguire compiti di sicurezza su sistemi e reti di comunicazione
- Applicare gli standard internazionali per le reti
- Padroneggiare tutte le procedure di sicurezza informatica
- Progettare e gestire centri dati
- Eseguire compiti di programmazione, individuare eventuali problemi e risolverli
- Conoscere l'intero processo di progettazione dei sistemi
- Condurre audit di sistema e migliorare la sicurezza informatica
- Conoscere tutte le fasi della gestione di un progetto e il suo ciclo di vita per saperle gestire

04

Direzione del corso

Docenti esperti con un ampio curriculum nell'area delle soluzioni IT e dello sviluppo e ricerca software, guidano questo Master per fornire gli strumenti e le conoscenze necessarie al professionista focalizzato sulla qualità nei processi di sviluppo software e sugli strumenti più avanzati per implementare processi DevOps e sistemi per l'assicurazione della qualità. Questo team di professionisti guiderà lo studente in ogni momento, per raggiungere gli obiettivi a distanza, trattandosi di un programma totalmente online e seguendo la metodologia più all'avanguardia implementata da TECH.

Insegnanti specializzati si impegnano a fornire i migliori contenuti e a rendere il processo di apprendimento un'esperienza agile e dinamica. Chiariranno i tuoi dubbi e ti accompagneranno lungo tutto il percorso"

Direttrice Ospite Internazionale

Sinan Akkaya è un leader tecnologico di riferimento con una vasta esperienza internazionale in Ingegneria, gestione e leadership, specializzato in reti di accesso e nella costruzione e gestione di infrastrutture aziendali. In questo senso, ha dimostrato una grande capacità di guidare team e progetti su larga scala, concentrandosi sull'implementazione di tecnologie avanzate, innovazione e sviluppo dei prodotti. La sua esperienza spazia dalla pianificazione strategica all'implementazione operativa di complesse soluzioni di rete wireless e sistemi di comunicazione.

In qualità di Direttore di Ingegneria delle Reti di Accesso Radio presso AT&T, ha guidato le attività di Ingegneria di Rete e delle Radiofrequenze per la regione della California settentrionale e del Nevada, dove ha supervisionato l'implementazione delle reti 4G e 5G, e l'espansione della rete a oltre 900 siti. Sotto la sua guida, la regione ha raggiunto il più alto EBITDA della società, evidenziando la capacità di gestire grandi budget, ottimizzare i costi operativi e garantire le prestazioni della rete. Inoltre, ha svolto un ruolo chiave nell'implementazione di tecnologie emergenti come Massive MIMO e 5G mm-wave, nonché nella direzione di servizi come FirstNet, focalizzati sulla sicurezza pubblica.

Ha lavorato anche come consulente per grandi operatori di telecomunicazioni, OEM e aziende globali, fornendo consulenza tecnica e strategica per ottimizzare le reti e migliorare la qualità dei servizi. Ha anche supervisionato team multidisciplinari, gestito investimenti di rete per oltre 500 milioni di dollari all'anno e apportato contributi significativi all'espansione e all'ottimizzazione delle reti di telecomunicazione. A sua volta, è stato un oratore frequente in conferenze internazionali, dove ha condiviso la sua conoscenza e visione sulle tendenze tecnologiche e le strategie per l'evoluzione delle reti wireless.

Dott.St. Akkaya, Sinan

- Direttore di Ingegneria delle Reti di Accesso Radio presso AT&T, San Ramon, California, Stati Uniti
- Responsabile di Ingegneria delle Radiofrequenze presso AT&T
- Ingegnere Capo di Radiofrequenza presso Wireless Facilities International
- Ingegnere di Radiofrequenza presso Lightbridge Communications Corporation
- Ingegnere di Progettazione Radiofonica presso Turkcell
- Product Manager presso General Electric
- Master in Ingegneria Elettrica ed Elettronica presso l'Università di Newcastle
- Laurea in Ingegneria Elettrica ed Elettronica presso l'Università Tecnica Orta Doğu
- Membro di: American Heart Association

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

05

Struttura e contenuti

La struttura dei contenuti è stata progettata dai migliori professionisti del settore informatico delle telecomunicazioni. Un corso intensivo e completo che comprende tutti gli aspetti che l'informatico che lavora nella Telematica deve gestire con sicurezza, sviluppato in modo strutturato ed efficiente per lo studente.

Disponiamo del programma più completo e aggiornato del mercato. Noi puntiamo all'eccellenza e facciamo in modo che anche tu la raggiunga"

Reti di computer

1.1. Reti di computer su internet
  1.1.1. Reti e internet
  1.1.2. Architettura dei protocolli
1.2. Il livello applicativo
  1.2.1. Modello e protocolli
  1.2.2. Servizi FTP e SMTP
  1.2.3. Servizio DNS
  1.2.4. Modello di funzionamento HTTP
  1.2.5. Formati dei messaggi HTTP
  1.2.6. Interazione con metodi avanzati
1.3. Il livello di trasporto
  1.3.1. Comunicazione tra processi
  1.3.2. Trasporto orientato alla connessione: TCP e SCTP
1.4. Il livello di rete
  1.4.1. Commutazione di circuiti e di pacchetti
  1.4.2. Il protocollo IP (v4 e v6)
  1.4.3. Algoritmi di instradamento
1.5. Il livello di collegamento
  1.5.1. Livello di collegamento e tecniche di rilevamento e correzione degli errori
  1.5.2. Collegamenti e protocolli di accesso
  1.5.3. Indirizzamento a livello di collegamento
1.6. Reti LAN
  1.6.1. Topologie di rete
  1.6.2. Elementi di rete e interconnessione
1.7. Indirizzamento IP
  1.7.1. Indirizzamento IP e *Subnetting*
  1.7.2. Panoramica: una richiesta HTTP
1.8. Reti wireless e mobili
  1.8.1. Reti e servizi mobili 2G, 3G e 4G
  1.8.2. Reti 5G
1.9. Sicurezza nelle reti
  1.9.1. Fondamenti di sicurezza delle comunicazioni
  1.9.2. Controllo degli accessi
  1.9.3. Sicurezza dei sistemi
  1.9.4. Fondamenti di crittografia
  1.9.5. Firma digitale
1.10. Protocolli di sicurezza su internet
  1.10.1. Sicurezza IP e reti private virtuali (VPN)
  1.10.2. Sicurezza web con SSL/TLS

Sistemi distribuiti

2.1. Introduzione al calcolo distribuito
  2.1.1. Concetti di base
  2.1.2. Calcolo monolitico, distribuito, parallelo e cooperativo
  2.1.3. Vantaggi, svantaggi e sfide dei sistemi distribuiti
  2.1.4. Concetti preliminari sui sistemi operativi: processi e concorrenza
  2.1.5. Background delle reti
  2.1.6. Concetti preliminari sull'ingegneria del software
  2.1.7. Organizzazione del manuale
2.2. Paradigmi di calcolo distribuito e di comunicazione interprocesso
  2.2.1. Comunicazione tra processi
  2.2.2. Sincronizzazione degli eventi
    2.2.2.1. Scenario 1: invio sincrono e ricezione sincrona
    2.2.2.2. Scenario 2: invio asincrono e ricezione sincrona
    2.2.2.3. Scenario 3: invio sincrono e ricezione asincrona
    2.2.2.4. Scenario 4: invio asincrono e ricezione asincrona
  2.2.3. Interblocchi e timer
  2.2.4. Rappresentazione e codifica dei dati
  2.2.5. Classificazione e descrizione dei paradigmi di calcolo distribuito
  2.2.6. Java come ambiente di sviluppo per sistemi distribuiti

2.3. API di *Sockets*
- 2.3.1. API Socket, tipi e differenze
- 2.3.2. Prese Datagram
- 2.3.3. Prese *Stream*
- 2.3.4. Soluzione agli interblocchi: timer ed eventi non bloccanti
- 2.3.5. Sicurezza dei *Sockets*

2.4 Paradigma di comunicazione client-server
- 2.4.1. Caratteristiche e concetti fondamentali dei sistemi client-server distribuiti
- 2.4.2. Processo di progettazione e implementazione di un sistema client-server
- 2.4.3. Problemi di indirizzamento non orientato alla connessione con i client anonimi
- 2.4.4. Server iterativi e concorrenti
- 2.4.5. Informazioni sulla sessione e sullo stato
  - 2.4.5.1. Informazioni sulla sessione
  - 2.4.5.2. Informazioni sullo stato globale
- 2.4.6. Clienti complessi che ricevono risposte asincrone dal lato server
- 2.4.7. Server complessi che fungono da intermediari tra più clienti

2.5. Comunicazione di gruppo
- 2.5.1. Introduzione al multicast e usi comuni
- 2.5.2. Affidabilità e gestione nei sistemi multicast
- 2.5.3. Implementazione Java di sistemi multicast
- 2.5.4. Esempio di utilizzo della comunicazione di gruppo tra pari
- 2.5.5. Implementazioni multicast affidabili
- 2.5.6. Multicast a livello di applicazione

2.6. Oggetti distribuiti
- 2.6.1. Introduzione agli oggetti distribuiti
- 2.6.2. Architettura di un'applicazione basata su oggetti distribuiti
- 2.6.3. Tecnologie dei sistemi a oggetti distribuiti
- 2.6.4. Livelli software Java RMI lato cliente e lato server
- 2.6.5. API per oggetti distribuiti Java RMI
- 2.6.6. Fasi di costruzione di un'applicazione RMI
- 2.6.7. Utilizzo di *Callback* in RMI
- 2.6.8. Download dinamico della cache degli oggetti remoti e del gestore della sicurezza RMI

2.7. Applicazioni Internet I: HTML, XML, HTTP
- 2.7.1. Introduzione alle Applicazioni Internet I
- 2.7.2. Linguaggio HTML
- 2.7.3. Linguaggio XML
- 2.7.4. Protocollo Internet HTTP
- 2.7.5. Utilizzo di contenuti dinamici: gestione dei moduli e CGI
- 2.7.6. Gestione della sessione Internet e dei dati di stato

2.8. CORBA
- 2.8.1. Introduzione a CORBA
- 2.8.2. Architettura CORBA
- 2.8.3. Linguaggio di descrizione delle interfacce in CORBA
- 2.8.4. Protocolli di interoperabilità GIOP
- 2.8.5. Riferimenti a oggetti remoti IOR
- 2.8.6. Servizio di denominazione CORBA
- 2.8.7. Esempio di IDL Java
- 2.8.8. Fasi di progettazione, compilazione ed esecuzione in Java IDL

2.9. Applicazioni Internet II: Applet, Servlet e SOA
- 2.9.1. Introduzione alle applicazioni Internet II
- 2.9.2. Applets
- 2.9.3. Introduzione ai Servlet
- 2.9.4. Servlet HTTP e loro funzionamento
- 2.9.5. Mantenimento delle informazioni di stato nelle Servlet
  - 2.9.5.1. Campi modulo nascosti
  - 2.9.5.2. *Cookie*
  - 2.9.5.3. Variabili del Servlet
  - 2.9.5.4. Oggetto Sessione
- 2.9.6. Servizi Web
- 2.9.7. Protocollo SOAP
- 2.9.8. Breve panoramica dell'architettura REST

2.10. Paradigmi avanzati
- 2.10.1. Introduzione ai paradigmi avanzati
- 2.10.2. Paradigma MOM
- 2.10.3. Paradigma dell'agente software mobile
- 2.10.4. Paradigma dello spazio degli oggetti
- 2.10.5. Informatica collaborativa
- 2.10.6. Tendenze future dell'informatica distribuita

Sicurezza nei sistemi e nelle reti di comunicazione

3.1. Panoramica sulla sicurezza, la crittografia e le crittoanalisi classiche
- 3.1.1. Sicurezza informatica: prospettiva storica
- 3.1.2. Ma cos'è esattamente la sicurezza?
- 3.1.3. Storia della crittografia
- 3.1.4. Cifrari sostitutivi
- 3.1.5. Caso di studio: la macchina Enigma

3.2. Crittografia simmetrica
- 3.2.1. Introduzione e terminologia base
- 3.2.2. Crittografia simmetrica
- 3.2.3. Modalità di funzionamento
- 3.2.4. DES
- 3.2.5. Il nuovo standard DES
- 3.2.6. Crittografia del flusso
- 3.2.7. Crittoanalisi

3.3. Crittografia asimmetrica
- 3.3.1. Origini della crittografia a chiave pubblica
- 3.3.2. Concetti di base e funzionamento
- 3.3.3. L'algoritmo RSA
- 3.3.4. Certificati digitali
- 3.3.5. Conservazione e gestione delle chiavi

3.4. Attacchi in rete
- 3.4.1. Minacce e attacchi alla rete
- 3.4.2. Enumerazione
- 3.4.3. Intercettazione del traffico: *Sniffers*
- 3.4.4. Attacchi di negazione del servizio
- 3.4.5. Attacchi ARP poisoning

3.5. Architetture di sicurezza
- 3.5.1. Architetture di sicurezza tradizionali
- 3.5.2. Secure Socket Layer: SSL
- 3.5.3. Protocollo SSH
- 3.5.4. Reti Private Virtuali (VPN)
- 3.5.5. Meccanismi di protezione dell'unità di archiviazione esterna
- 3.5.6. Meccanismi di protezione hardware

3.6. Tecniche di protezione del sistema e sviluppo sicuro del codice
- 3.6.1. Sicurezza operativa
- 3.6.2. Risorse e controlli
- 3.6.3. Monitoraggio
- 3.6.4. Sistemi di rilevamento delle intrusioni
- 3.6.5. IDS di *Host*
- 3.6.6. IDS di rete
- 3.6.7. IDS basati sulla firma
- 3.6.8. Sistemi di esche
- 3.6.9. Principi di sicurezza di base nello sviluppo del codice
- 3.6.10. Gestione dei guasti
- 3.6.11. Nemico pubblico numero 1: buffer overflow
- 3.6.12. Botch crittografici

3.7. Botnet e *Spam*
- 3.7.1. Origine del problema
- 3.7.2. Processo di spam
- 3.7.3. Invio di spam
- 3.7.4. Affinamento della mailing list

3.7.5. Tecniche di protezione
3.7.6. Servizi *Antispam* offerti da terzi
3.7.7. Casi di studio
3.7.8. Spam esotico
3.8. Audit e attacchi web
3.8.1. Raccolta di informazioni
3.8.2. Tecniche di attacco
3.8.3. Strumenti
3.9. Malware e codice maligno
3.9.1. Che cos'è il malware?
3.9.2. Tipi di malware
3.9.3. Virus
3.9.4. Criptovirus
3.9.5. Worm
3.9.6. *Adware*
3.9.7. *Spyware*
3.9.8. *Hoaxes*
3.9.9. *Pishing*
3.9.10. Trojan
3.9.11. L'economia del malware
3.9.12. Possibili soluzioni
3.10. Analisi forense
3.10.1. Raccolta di evidenze
3.10.2. Analisi delle evidenze
3.10.3. Tecniche anti-forensi
3.10.4. Caso di studio pratico

Reti e infrastrutture aziendali

4.1. Reti di trasporto
4.1.1. Architettura funzionale delle reti di trasporto
4.1.2. Interfaccia del nodo di rete in SDH
4.1.3. Elemento di rete
4.1.4. Qualità e disponibilità della rete
4.1.5. Gestione della rete di trasmissione
4.1.6. Evoluzione delle reti di trasmissione
4.2. Architetture WAN classiche
4.2.1. Reti WAN Wide Area
4.2.2. Standard WAN
4.2.3. Incapsulamento WAN
4.2.4. Dispositivi WAN
4.2.4.1. Router
4.2.4.2. Modem
4.2.4.3. *Switch*
4.2.4.4. Server di comunicazione
4.2.4.5. *Gateway*
4.2.4.6. *Firewall*
4.2.4.7. *Proxy*
4.2.4.8. NAT
4.2.5. Tipi di connessione
4.2.5.1. Collegamenti punto-punto
4.2.5.2. Commutazione di circuito
4.2.5.3. Commutazione di pacchetto
4.2.5.4. Circuiti virtuali WAN
4.3. Reti basate su ATM
4.3.1. Introduzione, caratteristiche e modello di livello
4.3.2. Livello di accesso fisico ATM
4.3.2.1. Sottolivello dipendente dal mezzo fisico PM
4.3.2.2. Sottostrato di convergenza della trasmissione, TC

4.3.3. Cella ATM
4.3.3.1. Intestazione
4.3.3.2. Connessione virtuale
4.3.3.3. Nodo di commutazione ATM
4.3.3.4. Controllo di flusso (caricamento del collegamento)
4.3.4. Adattamento delle celle AAL
4.3.4.1. Tipi di servizi AAL
4.4. Modelli di accodamento avanzati
4.4.1. Introduzione
4.4.2. Fondamenti di teoria delle code
4.4.3. Sistemi di base della teoria delle code
4.4.3.1. Sistemi M/M/1, M/M/m e M/M/∞
4.4.3.2. Sistemi M/M/1/k e M/M/m/m
4.4.4. Teoria delle code dei sistemi avanzati
4.4.4.1. Sistema M/G/1
4.4.4.2. Sistema M/G/1 con priorità
4.4.4.3. Reti di accodamento
4.4.4.4. Modellazione di reti di comunicazione
4.5. Qualità del servizio nelle reti aziendali
4.5.1. Fondamenti
4.5.2. Fattori di QoS nelle reti convergenti
4.5.3. Concetti di QoS
4.5.4. Politiche QoS
4.5.5. Metodi di implementazione della QoS
4.5.6. Modelli di QoS
4.5.7. Meccanismi per l'implementazione della QoS DiffServ
4.5.8. Esempi di applicazione
4.6. Reti aziendali e infrastrutture All-Ethernet
4.6.1. Topologie di Rete Ethernet
4.6.1.1. Topologia a Bus
4.6.1.2. Topologia a stella
4.6.2. Formato del frame Ethernet e IEEE

4.6.3. Rete Ethernet commutata
4.6.3.1. Reti Virtuali VLAN
4.6.3.2. Aggregazione di porte
4.6.3.3. Ridondanza delle connessioni
4.6.3.4. Gestione delle QoS
4.6.3.5. Funzioni di sicurezza
4.6.4. Fast Ethernet
4.6.5. Gigabit Ethernet
4.7. Infrastrutture MPLS
4.7.1. Introduzione
4.7.2. MPLS
4.7.2.1. Background di MPLS ed evoluzione
4.7.2.2. Architettura MPLS
4.7.2.3. Rispedizione di pacchetti etichettati
4.7.2.4. Protocollo di distribuzione delle etichette (LDP)
4.7.3. VPN MPLS
4.7.3.1. Definizione di una VPN
4.7.3.2. Modelli VPN
4.7.3.3. Modello di VPN MPLS
4.7.3.4. Architettura di VPN MPLS
4.7.3.5. *Virtual Routing Forwarding* (VRF)
4.7.3.6. RD
4.7.3.7. Route Target (RT)
4.7.3.8. Propagazione del percorso VPNv4 in una VPN MPLS
4.7.3.9. Inoltro dei pacchetti in una rete VPN MPLS
4.7.3.10. BGP
4.7.3.11. Comunità estesa BGP: RT
4.7.3.12. Trasporto di etichette BGP
4.7.3.13. Riflettore di rotta (RR)
4.7.3.14. Gruppo RR
4.7.3.15. Selezione del percorso BGP
4.7.3.16. Spedizione di pacchi

4.7.4. Protocolli di *Routing* comuni in ambienti MPLS
4.7.4.1. Protocolli di instradamento a Distanza Vettoriale
4.7.4.2. Protocolli di instradamento di tipo Link State
4.7.4.3. OSPF
4.7.4.4. ISIS
4.8. Servizi di vettore e VPN
4.8.1. Introduzione
4.8.2. Requisiti di base della VPN
4.8.3. Tipologie di VPN
4.8.3.1. Accesso remoto VPN
4.8.3.2. VPN punto a punto
4.8.3.3. VPN interna (su LAN)
4.8.4. Protocolli utilizzati nelle VPN
4.8.5. Implementazioni e tipi di connessione
4.9. NGN (Next Generation Networks)
4.9.1. Introduzione
4.9.2. Antecedenti
4.9.2.1. Definizione e caratteristiche della rete NGN
4.9.2.2. Migrazione alle reti di nuova generazione
4.9.3. Architettura NGN
4.9.3.1. Livello primario di connettività
4.9.3.2. Livello di accesso
4.9.3.3. Livello di servizio
4.9.3.4. Livello di gestione
4.9.4. IMS
4.9.5. Organizzazioni di standardizzazione
4.9.6. Tendenze normative
4.10. Revisione degli standard ITU e IETF
4.10.1. Introduzione
4.10.2. Standardizzazione
4.10.3. Alcune organizzazioni standard
4.10.4. Protocolli e standard del livello fisico della WAN
4.10.5. Esempi di protocolli orientati al mezzo

Architetture di sicurezza

5.1. Principi di base della sicurezza informatica
5.1.1. Cosa si intende per sicurezza informatica?
5.1.2. Obiettivi della sicurezza informatica
5.1.3. Servizi di sicurezza informatica
5.1.4. Conseguenze della mancanza di sicurezza
5.1.5. Principio di difesa della sicurezza
5.1.6. Politiche, piani e procedure di sicurezza
5.1.6.1. Gestione degli account utente
5.1.6.2. Identificazione e autenticazione degli utenti
5.1.6.3. Autorizzazione e controllo dell'accesso logico
5.1.6.4. Monitoraggio del server
5.1.6.5. Protezione dei dati
5.1.6.6. Sicurezza delle connessioni remote
5.1.7. L'importanza del fattore umano
5.2. Standardizzazione e certificazione della sicurezza informatica
5.2.1. Standard di sicurezza
5.2.1.1. Scopo degli standard
5.2.1.2. Organi responsabili
5.2.2. Norme negli Stati Uniti
5.2.2.1. TCSEC
5.2.2.2. Criteri Federali
5.2.2.3. FISCAM
5.2.2.4. NIST SP 800
5.2.3. Standard europei
5.2.3.1. ITSEC
5.2.3.2. ITSEM
5.2.3.3. Agenzia Europea per la Sicurezza delle Reti e dell'Informazione
5.2.4. Standard internazionali
5.2.5. Processo di certificazione

5.3. Minacce alla sicurezza informatica: vulnerabilità e malware
- 5.3.1. Introduzione
- 5.3.2. Vulnerabilità dei sistemi
  - 5.3.2.1. Incidenti di sicurezza della rete
  - 5.3.2.2. Cause di vulnerabilità dei sistemi informatici
  - 5.3.2.3. Tipi di vulnerabilità
  - 5.3.2.4. Responsabilità dei produttori di software
  - 5.3.2.5. Strumenti di valutazione delle vulnerabilità
- 5.3.3. Minacce alla sicurezza informatica
  - 5.3.3.1. Classificazione degli intrusi in rete
  - 5.3.3.2. Motivazioni degli aggressori
  - 5.3.3.3. Fasi di un attacco
  - 5.3.3.4. Tipi di attacco
- 5.3.4. Virus informatici
  - 5.3.4.1. Caratteristiche generali
  - 5.3.4.2. Tipi di virus
  - 5.3.4.3. Danni da virus
  - 5.3.4.4. Come combattere i virus

5.4. Terrorismo informatico e risposta agli incidenti
- 5.4.1. Introduzione
- 5.4.2. La minaccia del terrorismo informatico e della guerra informatica
- 5.4.3. Conseguenze dei fallimenti e degli attacchi alle imprese
- 5.4.4. Spionaggio nelle reti informatiche

5.5. Identificazione degli utenti e sistemi biometrici
- 5.5.1. Introduzione all'autenticazione, all'autorizzazione e alla registrazione degli utenti
- 5.5.2. Modello di sicurezza AAA
- 5.5.3. Controllo degli accessi
- 5.5.4. Identificazione dell'utente
- 5.5.5. Verifica della password
- 5.5.6. Autenticazione con certificati digitali
- 5.5.7. Identificazione dell'utente remoto
- 5.5.8. Accesso singolo
- 5.5.9. Gestire le password
- 5.5.10. Sistemi biometrici
  - 5.5.10.1. Caratteristiche generali
  - 5.5.10.2. Tipi di sistemi biometrici
  - 5.5.10.3. Implementazione dei sistemi

5.6. Fondamenti di crittografia e protocolli crittografici
- 5.6.1. Introduzione alla crittografia
  - 5.6.1.1. Crittografia, crittoanalisi e crittologia
  - 5.6.1.2. Funzionamento di un sistema crittografico
  - 5.6.1.3. Storia dei sistemi crittografici
- 5.6.2. Crittoanalisi
- 5.6.3. Classificazione dei sistemi crittografici
- 5.6.4. Sistemi crittografici simmetrici e asimmetrici
- 5.6.5. Autenticazione con sistemi crittografici
- 5.6.6. Firma elettronica
  - 5.6.6.1. Che cos'è una firma elettronica?
  - 5.6.6.2. Caratteristiche della firma elettronica
  - 5.6.6.3. Autorità di certificazione
  - 5.6.6.4. Certificati digitali
  - 5.6.6.5. Sistemi affidabili basati su terze parti
  - 5.6.6.6. Uso della firma elettronica
  - 5.6.6.7. ID elettronico
  - 5.6.6.8. Fattura elettronica

5.7. Strumenti di sicurezza della rete
- 5.7.1. Il problema della sicurezza delle connessioni Internet
- 5.7.2. Sicurezza della rete esterna
- 5.7.3. Il ruolo dei server *Proxy*
- 5.7.4. Il ruolo dei firewall
- 5.7.5. Server di autenticazione per le connessioni remote
- 5.7.6. L'analisi dei registri di attività
- 5.7.7. Sistemi di rilevamento delle intrusioni
- 5.7.8. Esche

5.8. Sicurezza nelle reti private virtuali e wireless
- 5.8.1. Sicurezza di rete reti private virtuali
  - 5.8.1.1 Il ruolo delle VPN
  - 5.8.1.2 Protocolli per le VPN
- 5.8.2. Sicurezza tradizionale nelle reti wireless
- 5.8.3. Possibili attacchi alle reti wireless
- 5.8.4. Il protocollo WEP
- 5.8.5. Standard per la sicurezza nelle reti wireless
- 5.8.6. Raccomandazioni per il rafforzamento della sicurezza

5.9. Sicurezza nell'uso dei servizi Internet
- 5.9.1. Navigazione sicura sul web
  - 5.9.1.1. Il servizio www
  - 5.9.1.2. Problemi di sicurezza su www
  - 5.9.1.3. Raccomandazioni sulla sicurezza
  - 5.9.1.4. Protezione della privacy su Internet
- 5.9.2. Sicurezza della posta elettronica
  - 5.9.2.1. Caratteristiche della posta elettronica
  - 5.9.2.2. Problemi di sicurezza nella posta elettronica
  - 5.9.2.3. Raccomandazioni per la sicurezza della posta elettronica
  - 5.9.2.4. Servizi avanzati di posta elettronica
  - 5.9.2.5. Uso della posta elettronica da parte dei dipendenti
- 5.9.3. SPAM
- 5.9.4. Il *Phising*

5.10. Controllo dei contenuti
- 5.10.1. La distribuzione di contenuti via Internet
- 5.10.2. Misure legali per combattere i contenuti illegali
- 5.10.3. Filtraggio, catalogazione e blocco dei contenuti
- 5.10.4. Danni all'immagine e alla reputazione

Centri dati, funzionamento della rete e servizi

6.1. Data center: concetti e componenti di base
- 6.1.1. Introduzione
- 6.1.2. Concetti di base
  - 6.1.2.1. Definizione di un DC
  - 6.1.2.2. Classificazione e importanza
  - 6.1.2.3. Disastri e perdite
  - 6.1.2.4. Tendenza evolutiva
  - 6.1.2.5. Costi della complessità
  - 6.1.2.6. Pilastri e strati di ridondanza
- 6.1.3. Filosofia di progettazione
  - 6.1.3.1. Obiettivi
  - 6.1.3.2. Selezione della posizione
  - 6.1.3.3. Disponibilità
  - 6.1.3.4. Elementi critici
  - 6.1.3.5. Valutazione e analisi dei costi
  - 6.1.3.6. Bilancio informatico
- 6.1.4. Componenti di base
  - 6.1.4.1. Piano tecnico
  - 6.1.4.2. Tipi di piastrelle
  - 6.1.4.3. Considerazioni generali
  - 6.1.4.4. Dimensione DC
  - 6.1.4.5. *Rack*
  - 6.1.4.6. Server e apparecchiature di comunicazione
  - 6.1.4.7. Monitoraggio

6.2. Data Center: sistemi di controllo
- 6.2.1. Introduzione
- 6.2.2. Alimentazione elettrica
  - 6.2.2.1. Rete elettrica
  - 6.2.2.2. Potenza elettrica
  - 6.2.2.3. Strategie di distribuzione elettrica

6.2.2.4. UPS
6.2.2.5. Generatori
6.2.2.6. Problemi elettrici
6.2.3. Controllo ambientale
6.2.3.1. Temperatura
6.2.3.2. Umidità
6.2.3.3. Condizionamento dell'aria
6.2.3.4. Stima delle calorie
6.2.3.5. Strategie di raffreddamento
6.2.3.6. Progettazione dei corridoi. Circolazione dell'aria
6.2.3.7. Sensori e manutenzione
6.2.4. Sicurezza e prevenzione degli incendi
6.2.4.1. Sicurezza fisica
6.2.4.2. Incendio e sua classificazione
6.2.4.3. Classificazione e tipi di sistemi di estinzione
6.3. Data Center: progettazione e organizzazione
6.3.1. Introduzione
6.3.2. Progettazione della rete
6.3.2.1. Tipologie
6.3.2.2. Cablaggio strutturato
6.3.2.3. Backbone
6.3.2.4. Cavi di rete UTP e STP
6.3.2.5. Cavi per telefonia
6.3.2.6. Elementi terminali
6.3.2.7. Cavi in fibra ottica
6.3.2.8. Cavo coassiale
6.3.2.9. Trasmissione senza fili
6.3.2.10. Raccomandazioni ed etichettatura
6.3.3. Organizzazione
6.3.3.1. Introduzione
6.3.3.2. Misure di base
6.3.3.3. Strategie per la gestione dei cavi
6.3.3.4. Politiche e procedure
6.3.4. Gestione dei CD
6.3.5. Standard nel *Data Center*
6.4. *Data Center*: modelli di business e continuità
6.4.1. Introduzione
6.4.2. Ottimizzazione
6.4.2.1. Tecniche di ottimizzazione
6.4.2.2. *Data Centers* ecologici
6.4.2.3. Sfide attuali
6.4.2.4. *Data Centers* modulari
6.4.2.5. Housing
6.4.2.6. Consolidamento dei *Data Centers*
6.4.2.7. Monitoraggio
6.4.3. Continuità aziendale
6.4.3.1. BCP. Piano di continuità operativa. Punti chiave
6.4.3.2. DR. Piano di disaster recovery
6.4.3.3. Implementazione di un DR
6.4.3.4. *Backup* e strategie
6.4.3.5. *Data Center* di backup
6.4.4. Le migliori prassi
6.4.4.1. Raccomandazioni
6.4.4.2. Utilizzo della metodologia ITIL
6.4.4.3. Metriche di disponibilità
6.4.4.4. Controllo ambientale
6.4.4.5. Gestione dei rischi
6.4.4.6. Responsabile per CD
6.4.4.7. Strumenti
6.4.4.8. Suggerimenti per l'implementazione
6.4.4.9. Caratterizzazione

6.5. *Cloud Computing*: introduzione e nozioni di base
- 6.5.1. Introduzione
- 6.5.2. Concetti e terminologia di base
- 6.5.3. Obiettivi e benefici
  - 6.5.3.1. Disponibilità
  - 6.5.3.2. Affidabilità
  - 6.5.3.3. Scalabilità
- 6.5.4. Rischi e sfide
- 6.5.5. Ruoli. Provider. Consumer
- 6.5.6. Caratteristiche del Cloud
- 6.5.7. Modelli di erogazione del servizio
  - 6.5.7.1. IaaS
  - 6.5.7.2. PaaS
  - 6.5.7.3. SaaS
- 6.5.8. Tipi di Cloud
  - 6.5.8.1. Pubblico
  - 6.5.8.2. Privato
  - 6.5.9.3. Ibrido
- 6.5.9. Tecnologie abilitanti del cloud
  - 6.5.9.1. Architetture di rete
  - 6.5.9.2. Reti a banda larga. Interconnettività
  - 6.5.9.3. Tecnologie di Data Center
    - 6.5.9.3.1. *Computing*
    - 6.5.9.3.2. *Storage*
    - 6.5.9.3.3. *Networking*
    - 6.5.9.3.4. Alta disponibilità
    - 6.5.9.3.5. Sistemi d *Backup*
    - 6.5.9.3.6. Bilanciatori
  - 6.5.9.4. Virtualizzazione
  - 6.5.9.5. Tecnologie web
  - 6.5.9.6. Tecnologia multitenant

6.5.9.7. Tecnologia di servizio
6.5.9.8. Sicurezza Cloud
6.5.9.8.1. Termini e concetti
6.5.9.8.2. Integrità e autenticazione
6.5.9.8.3. Meccanismi di sicurezza
6.5.9.8.4. Minacce alla sicurezza
6.5.9.8.5. Attacchi alla sicurezza del cloud
6.5.9.8.6. Caso di studio

6.6. *Cloud Computing*: tecnologia e sicurezza nel cloud
6.6.1. Introduzione
6.6.2. Meccanismi di Infrastruttura Cloud
6.6.2.1. Perimetro della rete
6.6.2.2. Conservazione
6.6.2.3. Ambiente server
6.6.2.4. Monitoraggio del cloud
6.6.2.5. Alta Disponibilità
6.6.3. Meccanismi di Sicurezza del Cloud (parte I)
6.6.3.1. Automatizzazione
6.6.3.2. Bilanciatori di carico
6.6.3.3. Monitoraggio SLA
6.6.3.4. Meccanismi di pagamento per uso
6.6.4. Meccanismi di Sicurezza del Cloud (parte II)
6.6.4.1. Sistemi di tracciabilità e audit
6.6.4.2. Sistemi di Failover
6.6.4.3. Hypervisor
6.6.4.4. Clustering
6.6.4.5. Sistemi Multitenant

6.7. *Cloud Computing*: Infrastruttura. Meccanismi di controllo e sicurezza
6.7.1. Introduzione ai meccanismi di gestione del cloud
6.7.2. Sistemi di amministrazione remota
6.7.3. Sistemi di gestione delle risorse
6.7.4. Sistemi di gestione degli accordi sul livello di servizio
6.7.5. Sistemi di gestione della fatturazione
6.7.6. Meccanismi di Sicurezza Cloud
6.7.6.1. Crittografia
6.7.6.2. *Hashing*
6.7.6.3. Firma digitale
6.7.6.4. PKI
6.7.6.5. Gestione dell'identità e degli accessi
6.7.6.6. SSO
6.7.6.7. Gruppi di sicurezza basati sul cloud
6.7.6.8. Sistemi di bastionatura

6.8. *Cloud Computing*: architettura Cloud
6.8.1. Introduzione
6.8.2. Architettura Cloud di base
6.8.2.1. Architetture di distribuzione del carico di lavoro
6.8.2.2. Architetture di utilizzo delle risorse
6.8.2.3. Architetture scalabili
6.8.2.4. Architetture di bilanciamento del carico
6.8.2.5. Architetture ridondanti
6.8.2.6. Esempi
6.8.3. Architettura Cloud avanzate
6.8.3.1. Architetture di cluster di hypervisor
6.8.3.2. Architetture di bilanciamento del carico virtuale
6.8.3.3. Architetture *non-stop*
6.8.3.4. Architettura ad alta disponibilità
6.8.3.5. Architetture Bare metal
6.8.3.6. Architetture ridondanti
6.8.3.7. Architetture ibride

6.8.4. Architetture cloud specializzate
6.8.4.1. Architetture ad accesso diretto I/O
6.8.4.2. Architetture ad accesso diretto LUN
6.8.4.3. Architetture di rete elastiche
6.8.4.4. Architetture SDDC
6.8.4.5. Architetture speciali
6.8.4.6. Esempi
6.9. *Cloud Computing*: modelli di fornitura dei servizi
6.9.1. Introduzione
6.9.2. Fornitura di servizi Cloud
6.9.3. La prospettiva del fornitore di servizi
6.9.4. Prospettiva del consumatore di questi servizi
6.9.5. Casi di studio
6.10. *Cloud Computing*: modelli contrattuali, metriche e fornitori di servizi
6.10.1. Introduzione ai modelli di fatturazione e alle metriche
6.10.2. Modelli di fatturazione
6.10.3. Metriche di pagamento per uso
6.10.4. Considerazioni sulla gestione dei costi
6.10.5. Introduzione alle metriche QoS e agli SLA
6.10.6. Metriche di qualità del servizio
6.10.7. Metriche di prestazione del servizio
6.10.8. Metriche di scalabilità del servizio
6.10.9. Modello di servizio SLA
6.10.10. Casi di studio

Programmazione avanzata

7.1. Introduzione alla programmazione orientata agli oggetti
7.1.1. Introduzione alla programmazione orientata agli oggetti
7.1.2. Progettazione delle lezioni
7.1.3. Introduzione a UML per la modellazione dei problemi
7.2. Relazioni tra lezioni
7.2.1. Astrazione ed ereditarietà
7.2.2. Concetti avanzati di ereditarietà
7.2.3. Polimorfismo
7.2.4. Composizione e aggregazione
7.3. Introduzione ai design pattern per i problemi orientati agli oggetti
7.3.1. Cosa sono i design pattern?
7.3.2. Pattern Factory
7.3.3. Pattern Singleton
7.3.4. Pattern Observer
7.3.5. Pattern Composite
7.4. Eccezioni
7.4.1. Quali sono le eccezioni?
7.4.2. Gestione e acquisizione delle eccezioni
7.4.3. Avvio delle eccezioni
7.4.4. Creazione di eccezioni
7.5. Interfacce utente
7.5.1. Introduzione a Qt
7.5.2. Posizionamento
7.5.3. Cosa sono gli eventi?
7.5.4. Eventi: definizione e acquisizione
7.5.5. Sviluppo di interfacce utente
7.6. Introduzione alla programmazione concorrente
7.6.1. Introduzione alla programmazione concorrente
7.6.2. Il concetto di processo e di thread
7.6.3. Interazione tra processi o thread
7.6.4. Thread in C++
7.6.5. Vantaggi e svantaggi della programmazione concorrente
7.7. Gestione e sincronizzazione dei thread
7.7.1. Ciclo di vita di un thread
7.7.2. La classe Thread
7.7.3. Pianificazione del thread
7.7.4. Gruppi di thread
7.7.5. Thread di tipo demoniaco
7.7.6. Sincronizzazione
7.7.7. Meccanismi di bloccaggio
7.7.8. Meccanismi di comunicazione
7.7.9. Monitor

7.8. Problemi comuni nella programmazione concorrente
- 7.8.1. Il problema dei produttori-consumatori
- 7.8.2. Il problema dei lettori e degli scrittori
- 7.8.3. Il problema della cena dei filosofi

7.9. Documentazione e test del software
- 7.9.1. Perché è importante documentare il software?
- 7.9.2. Documentazione di progettazione
- 7.9.3. Utilizzo di strumenti per la documentazione

7.10. Test di software
- 7.10.1. Introduzione al test del software
- 7.10.2. Tipi di test
- 7.10.3. Test dell'unità
- 7.10.4. Test di integrità
- 7.10.5. Test di convalida
- 7.10.6. Test del sistema

Ingegneria dei sistemi e dei servizi di rete

8.1. Introduzione all'ingegneria dei sistemi e dei servizi di rete
- 8.1.1. Concetto di sistema informatico e ingegneria informatica
- 8.1.2. Il software e le sue caratteristiche
  - 8.1.2.1. Caratteristiche del software
- 8.1.3. L'evoluzione del software
  - 8.1.3.1. Gli albori dello sviluppo del software
  - 8.1.3.2. La crisi del software
  - 8.1.3.3. L'Ingegneria del software
  - 8.1.3.4. La tragedia del software
  - 8.1.3.5. L'attualità del software
- 8.1.4. I miti del software
- 8.1.5. Le nuove sfide del software
- 8.1.6. Etica professionale nell'ingegneria del software
- 8.1.7. SWEBOK. Il corpo di conoscenze dell'ingegneria del software

8.2. Il processo di sviluppo
- 8.2.1. Processo di risoluzione dei problemi
- 8.2.2. Il processo di sviluppo del software
- 8.2.3. Processo del software e ciclo di vita
- 8.2.4. Cicli di vita. Modelli di processo (tradizionali)
  - 8.2.4.1. Modello a cascata
  - 8.2.4.2. Modelli basati su prototipi
  - 8.2.4.3. Modello di sviluppo incrementale
  - 8.2.4.4. Sviluppo rapido delle applicazioni (RAD)
  - 8.2.4.5. Modello a spirale
  - 8.2.4.6. Processo di sviluppo unificato o Rational Unified Process (RUP)
  - 8.2.4.7. Sviluppo del software basato sui componenti
- 8.2.5. Il manifesto agile. Metodi agili
  - 8.2.5.1. Extreme Programming (XP)
  - 8.2.5.2. Scrum
  - 8.2.5.3. Feature Driven Development (FDD)
- 8.2.6. Standard di processo del software
- 8.2.7. Definizione di processo software
- 8.2.8. Maturità del processo software

8.3. Pianificazione e gestione di progetti agili
- 8.3.1. Che cos'è Agile?
  - 8.3.1.1. Storia di Agile
  - 8.3.1.2. Manifesto Agile
- 8.3.2. Fondamenti di Agile
  - 8.3.2.1. La mentalità agile
  - 8.3.2.2. L'adattamento ad Agile
  - 8.3.2.3. Il ciclo di vita dello sviluppo del prodotto
  - 8.3.2.4. Il triangolo di ferro
  - 8.3.2.5. Lavorare con l'incertezza e la volatilità
  - 8.3.2.6. Processi definiti e processi empirici
  - 8.3.2.7. I miti di Agile

8.3.3. L'ambiente Agile
8.3.3.1. Il modello operativo
8.3.3.2. Ruoli Agile
8.3.3.3. Tecniche Agile
8.3.3.4. Pratiche Agile
8.3.4. Quadri di lavoro Agile
8.3.4.1. e-Xtreme Programming (XP)
8.3.4.2. Scrum
8.3.4.3. Dynamic Systems Development Method (DSDM)
8.3.4.4. Agile Project Management
8.3.4.5. Kanban
8.3.4.6. Lean software Development
8.3.4.7. Lean Start-up
8.3.4.8. Scaled Agile Framework (SAFe)
8.4. Gestione della configurazione e repository collaborativi
8.4.1. Nozioni di base sulla gestione della configurazione del software
8.4.1.1. Che cos'è la gestione della configurazione del software?
8.4.1.2. Configurazione del software ed elementi di configurazione del software
8.4.1.3. Linee di base
8.4.1.4. Versioni, revisioni, varianti e *Releases*
8.4.2. Attività di gestione della configurazione
8.4.2.1. Identificazione della configurazione
8.4.2.2. Controllo delle modifiche alla configurazione
8.4.2.3. Generazione di rapporti di stato
8.4.2.4. Verifica della configurazione
8.4.3. Il piano di gestione della configurazione
8.4.4. Strumenti di gestione della configurazione
8.4.5. La gestione della configurazione nella metodologia Metrica v.3
8.4.6. La gestione della configurazione nello SWEBOK

8.5. Test di sistemi e servizi
- 8.5.1. Concetti generali di test
  - 8.5.1.1. Verifica e convalida
  - 8.5.1.2. Definizione di test
  - 8.5.1.3. Principi del test
- 8.5.2. Approcci ai test
  - 8.5.2.1. Test scatola bianca
  - 8.5.2.2. Modello black box
- 8.5.3. Prove statiche o revisioni
  - 8.5.3.1. Revisioni tecniche formali
  - 8.5.3.2. *Passaggi a piedi*
  - 8.5.3.3. Ispezioni del codice
- 8.5.4. Test dinamici
  - 8.5.4.1. Test unitari
  - 8.5.4.2. Test di integrazione
  - 8.5.4.3. Test di sistema
  - 8.5.4.4. Test di accettazione
  - 8.5.4.5. Test di regressione
- 8.5.5. Alpha test e beta test
- 8.5.6. Il processo di testing
- 8.5.7. Errore, difetto e fallimento
- 8.5.8. Strumenti di test automatizzati
  - 8.5.8.1. Junit
  - 8.5.8.2. LoadRunner

8.6. Modellazione e progettazione di architetture di rete
- 8.6.1. Introduzione
- 8.6.2. Caratteristiche dei sistemi
  - 8.6.2.1. Descrizione dei sistemi
  - 8.6.2.2. Descrizione e caratteristiche dei servizi
  - 8.6.2.3. Requisiti di operatività

8.6.3. Analisi dei requisiti
8.6.3.1. Requisiti dell'utente
8.6.3.2. Requisiti dell'applicazione
8.6.3.3. Requisiti di rete
8.6.4. Progettazione di architetture di rete
8.6.4.1. Architettura di riferimento e componenti
8.6.4.2. Modelli di architettura
8.6.4.3. Architetture di sistema e di rete
8.7. Modellazione e progettazione di sistemi distribuiti
8.7.1. Introduzione
8.7.2. Architettura di routing e *Routing*
8.7.2.1. Strategia di indirizzamento
8.7.2.2. Strategia di instradamento
8.7.2.3. Considerazioni del disegno
8.7.3. Considerazioni sulla progettazione
8.7.4. Processo di progettazione
8.8. Piattaforme e ambienti di distribuzione
8.8.1. Introduzione
8.8.2. Sistemi informatici distribuiti
8.8.2.1. Concetti di base
8.8.2.2. Modelli informatici
8.8.2.3. Vantaggi, svantaggi e sfide
8.8.2.4. Fondamenti del sistema operativo
8.8.3. Implementazioni di reti virtualizzate
8.8.3.1. Necessità del cambiamento
8.8.3.2. Trasformazione delle reti: da "all-IP" al cloud
8.8.3.3. Implementazione della rete nel cloud
8.8.4. Esempio: architettura di rete in Azure
8.9. Prestazioni E2E: ritardo e larghezza di banda. QoS
8.9.1. Introduzione
8.9.2. Analisi del rendimento
8.9.3. QoS
8.9.4. Gestione e prioritizzazione del traffico
8.9.5. Accordi sul livello di servizio
8.9.6. Considerazioni del disegno
8.9.6.1. Valutazione delle prestazioni
8.9.6.2. Relazioni e interazioni
8.10. Automazione e ottimizzazione della rete
8.10.1. Introduzione
8.10.2. Gestione della rete
8.10.2.1. Protocolli di gestione e configurazione
8.10.2.2. Architetture di gestione della rete
8.10.3. Orchestrazione e automazione
8.10.3.1. Architettura ONAP
8.10.3.2. Controllori e funzioni
8.10.3.3. Politiche
8.10.3.4. Inventario di rete
8.10.4. Ottimizzazione

Audit dei Sistemi Informativi

9.1. Audit dei sistemi informativi. Norme di buona pratica
9.1.1. Introduzione
9.1.2. Audit e COBIT
9.1.3. L'audit dei sistemi di gestione ICT
9.1.4. Certificazioni
9.2. Concetti e metodologie di audit dei sistemi
9.2.1. Introduzione
9.2.2. Metodologie di valutazione del sistema: quantitative e qualitative
9.2.3. Metodologia di audit informatico
9.2.4. Il piano di audit
9.3. Il contratto di audit
9.3.1. Natura giuridica dell'incarico
9.3.2. Le parti di un incarico di revisione
9.3.3. Oggetto dell'incarico di revisione
9.3.4. Il rapporto di audit

9.4. Elementi organizzativi della revisione contabile
- 9.4.1. Introduzione
- 9.4.2. Missione del dipartimento di audit
- 9.4.3. Pianificazione dell'audit
- 9.4.4. Metodologia di audit IS

9.5. Quadro giuridico per gli audit
- 9.5.1. Protezione dei dati personali
- 9.5.2. Protezione legale del software
- 9.5.3. Reati tecnologici
- 9.5.4. Contratti, firma e identità elettronica

9.6. Audit e quadri di outsourcing
- 9.6.1. Introduzione
- 9.6.2. Concetti di base dell'outsourcing
- 9.6.3. La verifica dell'outsourcing informatico
- 9.6.4. Quadri di riferimento: CMMI, ISO27001, ITIL

9.7. Audit di sicurezza
- 9.7.1. Introduzione
- 9.7.2. Sicurezza fisica e logica
- 9.7.3. Sicurezza dell'ambiente
- 9.7.4. Pianificazione ed esecuzione dell'audit di sicurezza fisica

9.8. Audit della rete e di Internet
- 9.8.1. Introduzione
- 9.8.2. Vulnerabilità della rete
- 9.8.3. Principi e diritti in Internet
- 9.8.4. Controlli ed elaborazione dei dati

9.9. Audit delle applicazioni e dei sistemi informatici
- 9.9.1. Introduzione
- 9.9.2. Modelli di riferimento
- 9.9.3. Valutazione della qualità delle domande
- 9.9.4. Verifica dell'organizzazione e della gestione dell'area di sviluppo e manutenzione

9.10. Audit dei dati personali
- 9.10.1. Introduzione
- 9.10.2. Leggi e regolamenti sulla protezione dei dati
- 9.10.3. Sviluppo dell'audit
- 9.10.4. Infrazioni e sanzioni

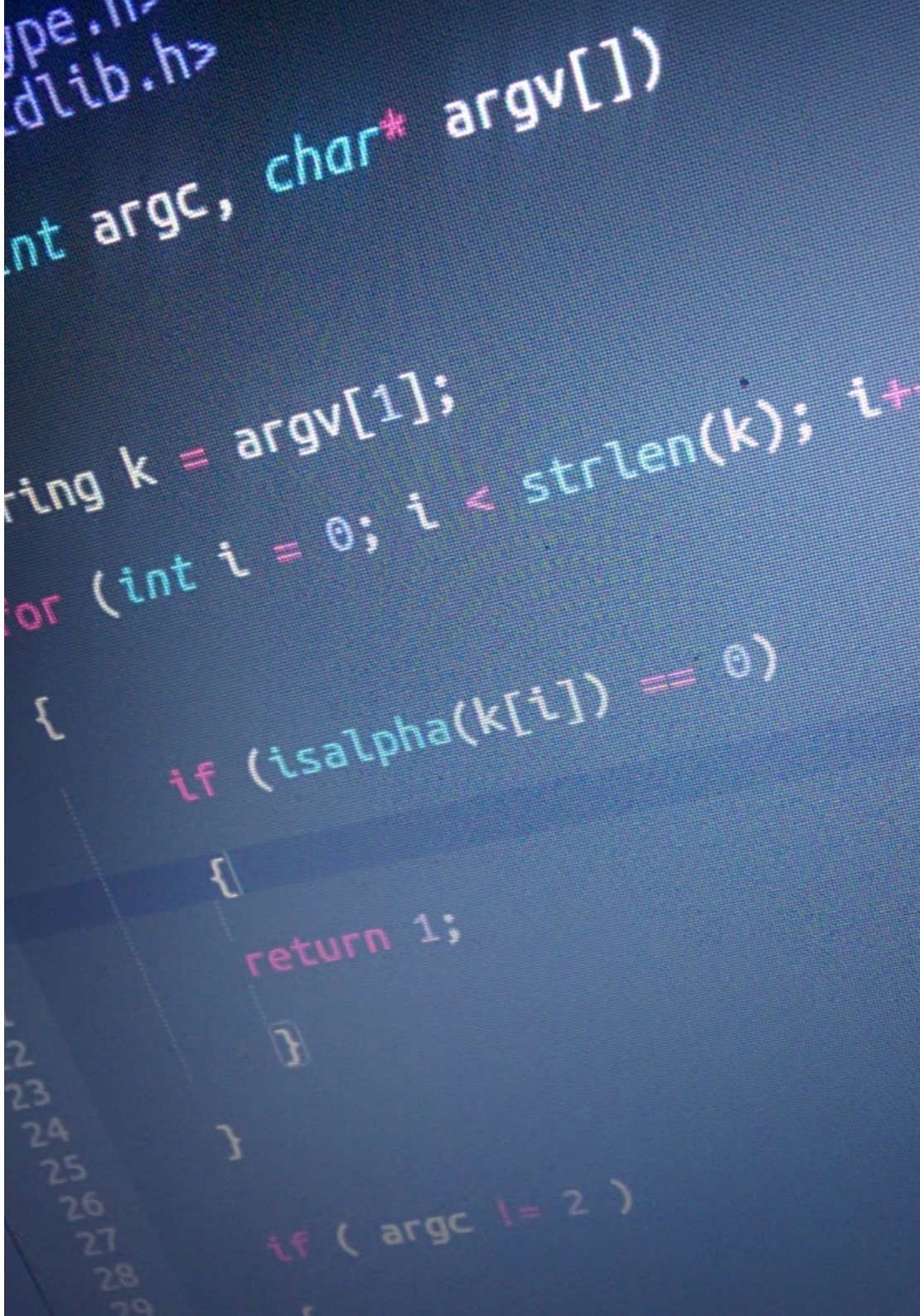
Gestione dei progetti

10.1. Concetti fondamentali del project management e del ciclo di vita della gestione del progetto
- 10.1.1. Cos'è un progetto?
- 10.1.2. Metodologia comune
- 10.1.3. Che cos'è la gestione dei progetti?
- 10.1.4. Che cos'è un piano di progetto?
- 10.1.5. Benefici
- 10.1.6. Ciclo di vita del progetto
- 10.1.7. Gruppi di processo o ciclo di vita della gestione del progetto
- 10.1.8. Il rapporto tra gruppi di processo e aree di conoscenza
- 10.1.9. Relazioni tra ciclo di vita del prodotto e del progetto

10.2. Avvio e pianificazione
- 10.2.1. Dall'idea al progetto
- 10.2.2. Sviluppo della carta del progetto
- 10.2.3. Riunione di avvio del progetto
- 10.2.4. Compiti, nozioni e competenze nel processo di start-up
- 10.2.5. Il piano di progetto
- 10.2.6. Sviluppo del piano base: Passaggi
- 10.2.7. Compiti, nozioni e competenze nel processo di pianificazione

10.3. La gestione degli *Stakeholders* e del percorso
- 10.3.1. Identificare le parti interessate
- 10.3.2. Sviluppare un piano per la gestione delle parti interessate
- 10.3.3. Gestire il coinvolgimento delle parti interessate
- 10.3.4. Controllare il coinvolgimento delle parti interessate

10.3.5. L'obiettivo del progetto
10.3.6. La gestione e il piano relativo al campo di applicazione
10.3.7. Riunire i requisiti
10.3.8. Definire l'ambito di applicazione
10.3.9. Creare la WBS
10.3.10. Verificare e controllare il campo di applicazione
10.4. L'ideazione della tabella di marcia
10.4.1. La gestione del tempo e il relativo piano
10.4.2. Definire le attività
10.4.3. Sequenza delle attività
10.4.4. Stima delle risorse delle attività
10.4.5. Stimare la durata delle attività
10.4.6. Sviluppo della tabella di marcia e calcolo del percorso critico
10.4.7. Controllo della tabella di marcia
10.5. Sviluppo del budget e risposta ai rischi
10.5.1. Fare una stima dei costi
10.5.2. Definire il budget e la curva a S
10.5.3. Controllo dei costi e metodo earned value
10.5.4. I concetti di rischio
10.5.5. Come fare un'analisi dei rischi
10.5.6. Lo sviluppo del piano di risposta
10.6. Gestione qualità
10.6.1. Pianificazione della qualità
10.6.2. Garanzia della qualità
10.6.3. Controllo della qualità
10.6.4. Concetti statistici di base
10.6.5. Strumenti per la gestione della qualità



10.7. Comunicazione e risorse umane
- 10.7.1. Pianificare la gestione delle comunicazioni
- 10.7.2. Analisi dei requisiti di comunicazione
- 10.7.3. Tecnologia delle comunicazioni
- 10.7.4. Modelli di comunicazione
- 10.7.5. Metodi di comunicazione
- 10.7.6. Piano di gestione delle comunicazioni
- 10.7.7. Gestire le comunicazioni
- 10.7.8. La gestione delle risorse umane
- 10.7.9. Soggetti principali e il loro ruolo nei progetti
- 10.7.10. Tipi di organizzazione
- 10.7.11. Organizzazione del progetto
- 10.7.12. Squadre di lavoro

10.8. Approvvigionamento
- 10.8.1. Il processo di acquisto
- 10.8.2. Pianificazione
- 10.8.3. Ricerca di fornitori e presentazione di offerte
- 10.8.4. Assegnazione del contratto
- 10.8.5. Gestione del contratto
- 10.8.6. I contratti
- 10.8.7. Tipi di contratto
- 10.8.8. Negoziazione del contratto

10.9. Attuazione, monitoraggio, controllo e chiusura
- 10.9.1. I gruppi dei processi
- 10.9.2. Attuazione del progetto
- 10.9.3. Monitoraggio e controllo del progetto
- 10.9.4. Chiusura del progetto

10.10. Responsabilità professionale
- 10.10.1. Responsabilità professionale
- 10.10.2. Caratteristiche della responsabilità sociale e professionale
- 10.10.3. Codice etico del leader di progetto
- 10.10.4. Responsabilità vs. PMP®
- 10.10.5. Esempi di responsabilità
- 10.10.6. Vantaggi della professionalizzazione

Un processo di crescita professionale e personale che diventerà un'enorme spinta alla tua competitività”

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.***

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

Caso di Studio per contestualizzare tutti i contenuti

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

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

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

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

Un metodo di apprendimento innovativo e differente

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

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

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

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

Metodologia Relearning

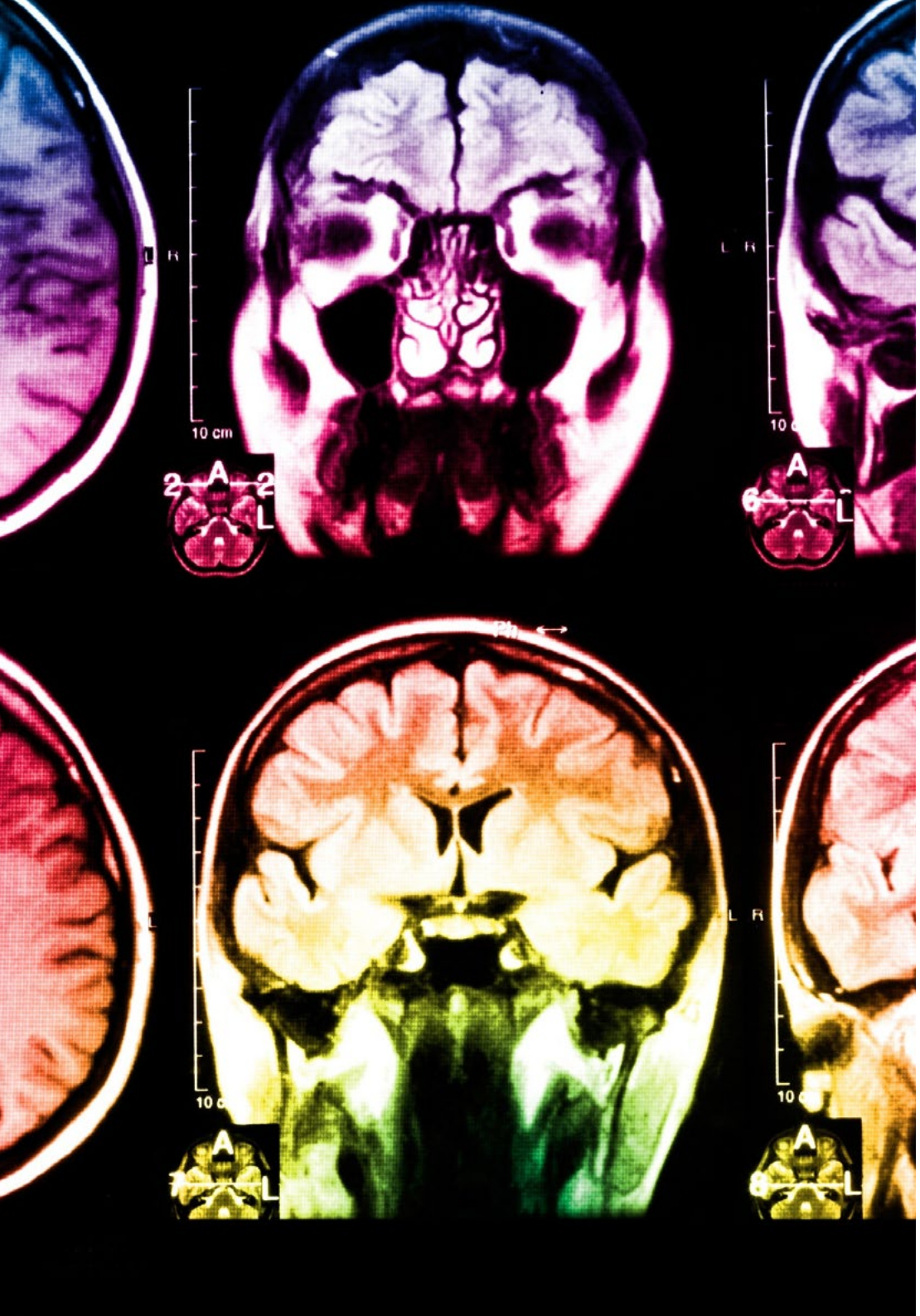
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

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

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

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

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



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

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

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

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

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

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.

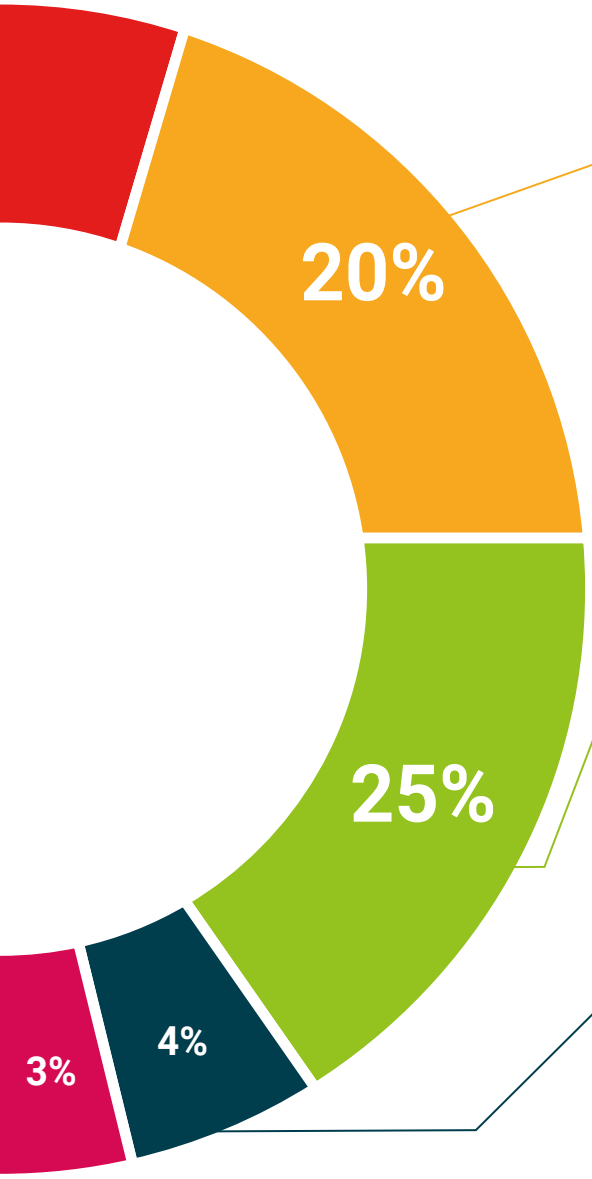
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

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.



Casi di Studio

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

Riepiloghi interattivi

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

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

Testing & Retesting

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

07

Titolo

Questo programma ti consentirà di ottenere il titolo di studio di Master in Telematica rilasciato da TECH Global University, la più grande università digitale del mondo.

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

Questo programma ti consentirà di ottenere il titolo di studio privato di **Master in Telematica** 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 Universtity** 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 in Telematica**

Modalità: **online**

Durata: **12 mesi**

Accreditamento: **60 ECTS**


tech global university

Dott. Cristian David Velasquez Granada, con documento d'identità 31914606J ha superato con successo e ottenuto il titolo di:

Master in Telematica

Si tratta di un titolo di studio privato corrispondente a 1800 horas di durata equivalente a # ECTS, con data di inizio dd/mm/aaaa e data di fine dd/mm/aaaa.

TECH Global University è un'università riconosciuta ufficialmente dal Governo di Andorra il 31 de gennaio 2024, appartenente allo Spazio Europeo dell'Istruzione Superiore (EHEA).

In Andorra la Vella, 28 febbraio 2024

Dott. Pedro Navarro Illana
Rector

código único TECH: AFWOR23S techtitute.com/titulos


Master in Telematica

Tipo di insegnamento	ECTS
Obbligatorio (OB)	60
Opzionale (OP)	0
Tirocinio Esterno (TE)	0
Tesi di Master (TM)	0
	Totale 60

Distribuzione generale del Programma

Corso	Insegnamento	ECTS	Codice
1°	Reti di computer	6	OB
1°	Sistemi distribuiti	6	OB
1°	Sicurezza nei sistemi e nelle reti di comunicazione	6	OB
1°	Reti e infrastrutture aziendali	6	OB
1°	Architetture di sicurezza	6	OB
1°	Centri dati, funzionamento della rete e servizi	6	OB
1°	Programmazione avanzata	6	OB
1°	Ingegneria dei sistemi e dei servizi di rete	6	OB
1°	Audit dei Sistemi Informativi	6	OB
1°	Gestione di Progetti	6	OB

Dott. Pedro Navarro Illana
Rector

tech global university

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

tech global university

Master

Telematica

- Modalità: **online**
- Durata: **12 mesi**
- Titolo: **TECH Global University**
- Accreditamento: **60 ECTS**
- Orario: **a scelta**
- Esami: **online**

Master
Telematica

tech global university