# Master Privato

## Gestione delle Politiche di Cybersecurity in Azienda

tech università tecnologica

tech università tecnologica

# Master Privato

## Gestione delle Politiche di Cybersecurity in Azienda

- Modalità: **online**
- Durata: **12 mesi**
- Titolo: **TECH Università Tecnologica**
- Dedizione: **16 ore/settimana**
- Orario: **a scelta**
- Esami: **online**

Acceso web: www.techtitute.com/it/informatica/master/master-gestione-politiche-cybersecurity-azienda

# Indice

01

# Presentazione

La crescente dipendenza di molte aziende e industrie da ambienti virtuali ha portato alla proliferazione di crimini e attacchi informatici a danno di ogni tipo di organizzazione. Indipendentemente dalle dimensioni o dalla sede, le minacce alla cybersecurity rappresentano un pericolo reale che può comportare numerose perdite di tempo, denaro e dati. Per questo motivo, la figura dell'informatico con conoscenze specifiche in Gestione delle Politiche di Cybersecurity sta diventando sempre più importante nel settore aziendale e offre ampie opportunità di crescita sia professionale che personale. Questa qualifica offre ai professionisti dell'IT un'eccellente opportunità per dare un impulso alla loro carriera, giacché è stata ideata da un team di professionisti con una vasta esperienza nel settore. Il formato 100% online della qualifica, inoltre, la rende un'opzione pienamente compatibile con qualsiasi tipo di attività o responsabilità.

*Iscriviti ora e accedi ai contenuti specializzati in Politiche di Gestione degli Incidenti, Sicurezza del Software e Disaster Recovery"*

Migliaia di criminali informatici attaccano ogni giorno le aziende di tutto il mondo, anche a distanza di migliaia di chilometri, il che ha reso la cybersecurity una delle principali preoccupazioni del panorama aziendale moderno. Le vulnerabilità delle organizzazioni che si affidano ad ambienti virtuali possono essere sfruttate da criminali di ogni tipo, che rubano dati sensibili o ne impediscono l'accesso in cambio di un riscatto.

Ecco perché una corretta Gestione delle Politiche di Cybersecurity in Azienda comporta una grande responsabilità, giacché si tratta di una posizione lavorativa di grande prestigio e proiezione economica, oltre che di responsabilità, per l'informatico specializzato. Pertanto, fare un passo avanti e approfondire questioni come i sistemi di controllo per individuare le minacce o i protocolli di comunicazione sicuri, rappresenta una spinta diretta verso una posizione chiave in qualsiasi organizzazione.

Un personale docente accuratamente selezionato da TECH ha preparato contenuti didattici di prim'ordine per questo Master Privato. Nel corso di 10 moduli completi, l'informatico amplierà le proprie competenze nell'implementazione di politiche di sicurezza fisica e ambientale, sistemi di gestione della sicurezza delle informazioni, strumenti di monitoraggio e molte altre competenze che lo renderanno una risorsa preziosa in qualsiasi istituzione.

Tutto questo con l'innegabile vantaggio di non dover frequentare lezioni frontali o orari fissi, poiché l'intero programma viene impartito online. I contenuti didattici sono scaricabili da qualsiasi dispositivo dotato di connessione a Internet e possono essere utilizzati come guida di riferimento anche al termine della qualifica. L'informatico avrà la libertà di adattare il carico di studio al proprio ritmo e di conciliarlo con la propria attività professionale abituale o con le proprie responsabilità.

Questo **Master Privato in Gestione delle Politiche di Cybersecurity in Azienda** possiede il programma educativo più completo e aggiornato del mercato. Le caratteristiche principali del corso sono:

- Lo sviluppo di casi di studio presentati da esperti in Cybersecurity Informatica
- Contenuti grafici, schematici ed eminentemente pratici forniscono informazioni scientifiche e pratiche sulle discipline mediche essenziali per l'esercizio della professione
- Esercizi pratici che offrono un processo di autovalutazione per migliorare l'apprendimento
- La sua speciale enfasi sulle metodologie innovative
- Lezioni teoriche, domande all'esperto, forum di discussione su questioni controverse e lavoro di riflessione individuale
- La disponibilità di accesso ai contenuti da qualsiasi dispositivo fisso o portatile con una connessione internet

*Posizionati come responsabile delle Politiche di Cybersecurity, adattandoti a tutti i tipi di situazioni e di eventi imprevisti in termini di Sicurezza Informatica"*

*Incorpora nel tuo lavoro quotidiano le più efficaci pratiche di sicurezza contro gli attacchi, perfezionate da un team di docenti specializzati nel settore"*

*Accedi a un programma ricco di contenuti multimediali, rafforzato da temi specifici sulle politiche di sicurezza gestionale, sulla classificazione del rischio informatico e sull'Hijacking.*

*Potrai scegliere quando, dove e come seguire l'intero corso, con la totale libertà di progredire nel programma di studio secondo i tuoi ritmi.*

Il personale docente del programma comprende prestigiosi professionisti che apportano la propria esperienza, così come specialisti riconosciuti e appartenenti a società scientifiche di primo piano.

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 progettazione 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. Sarai supportato da un innovativo sistema video interattivo sviluppato da esperti rinomati.

02

# Obiettivi

Poiché la cybersecurity è un tema così importante nel mondo imprenditoriale attuale, il presente corso posiziona l'informatico come parte centrale nella gestione di questi problemi. Per questo motivo, gli obiettivi perseguiti nel corso del programma sono molteplici, ma si darà priorità all'offerta di contenuti teorici aggiornati e basati sugli ultimi progressi nel campo della sicurezza informatica.

*Avrai a disposizione una guida di riferimento sulla Gestione delle Politiche di Cybersecurity che ti aiuterà a rafforzare la tua carriera di esperto di sicurezza digitale"*

## Obiettivi generali

- Approfondire la comprensione dei concetti chiave della sicurezza informatica
- Sviluppare le misure necessarie per garantire buone pratiche di sicurezza delle informazioni
- Sviluppare le diverse metodologie per effettuare un'analisi esaustiva delle minacce
- Installare e conoscere i diversi strumenti utilizzati nel trattamento e nella prevenzione degli incidenti

*La metodologia pedagogica di TECH ti permetterà di raggiungere i tuoi obiettivi più ambiziosi anche prima di quanto ti aspetti"*

## Obiettivi specifici

### Modulo 1. Sistema di Gestione della Sicurezza Informatica (SGSI)

- Analizzare le normative e gli standard attualmente applicabili ai SGSI
- Sviluppare le fasi necessarie per implementare un SGSI in un'entità
- Analizzare le procedure di gestione e implementazione degli incidenti di sicurezza delle informazioni

### Modulo 2. Aspetti organizzativi della Politica di Sicurezza Informatica

- Implementare un SGSI in azienda
- Determinare quali dipartimenti devono essere coperti dall'implementazione del sistema di gestione della sicurezza
- Implementare le necessarie contromisure di sicurezza nelle operazioni

### Modulo 3. Politiche di sicurezza per l'analisi delle minacce nei sistemi informatici

- Analizzare il significato delle minacce
- Determinare le fasi della gestione preventiva delle minacce
- Confronto tra diverse metodologie di gestione delle minacce

### Modulo 4. Implementazione Pratica delle Politiche di Sicurezza del Software e dell'Hardware

- Determinare cosa sono Autenticazione e Identificazione
- Analizzare i diversi metodi di Autenticazione esistenti e la loro implementazione pratica
- Implementare la corretta politica di controllo degli accessi per il software e i sistemi
- Stabilire le principali tecnologie di identificazione attuali
- Generare conoscenze specialistiche sulle diverse metodologie esistenti per il bastioning dei sistemi

### Modulo 5. Politiche di Gestione degli Incidenti di Sicurezza

- Sviluppare conoscenze specialistiche su come gestire gli incidenti causati da eventi di sicurezza informatica
- Determinare il funzionamento di un team di gestione degli incidenti di sicurezza
- Analizzare le diverse fasi della gestione degli eventi di sicurezza informatica
- Esaminare i protocolli standardizzati per la gestione degli incidenti di sicurezza

### Modulo 6. Implementazione di Politiche di Sicurezza Fisica e Ambientale in Azienda

- Analizzare i termini Area Sicura e Perimetro Sicuro
- Esaminare la Biometria e i sistemi biometrici
- Implementare le corrette politiche di sicurezza per la sicurezza fisica
- Definire le normative vigenti sulle aree sicure dei sistemi informatici

### Modulo 7. Politiche di Comunicazione Sicura in Azienda

- Proteggere una rete di comunicazione suddividendola in partizioni
- Analizzare i diversi algoritmi di crittografia utilizzati nelle reti di comunicazione
- Implementare diverse tecniche di crittografia nella rete, come TLS, VPN o SSH
- Modulo 8. Implementazione pratica delle Politiche di Sicurezza in caso di Attacchi
- Determinare i diversi attacchi reali al sistema informatico
- Valutare le diverse politiche di sicurezza per mitigare gli attacchi
- Attuare tecnicamente le misure per mitigare le principali minacce

### Modulo 9. Strumenti di Monitoraggio nelle Politiche di Sicurezza dei Sistemi Informatici

- Sviluppare il concetto di Monitoraggio e Implementazione delle Metriche
- Configurare i registri di controllo sui sistemi e monitorare le reti
- Presentare i migliori strumenti di monitoraggio del sistema attualmente disponibili sul mercato

### Modulo 10. Politica di Disaster Recovery pratica

- Generare conoscenze specialistiche sul concetto di continuità della sicurezza delle informazioni
- Sviluppare un piano di continuità aziendale
- Sviluppare un piano di continuità aziendale
- Analizzare un piano di continuità ICT

03

# Competenze

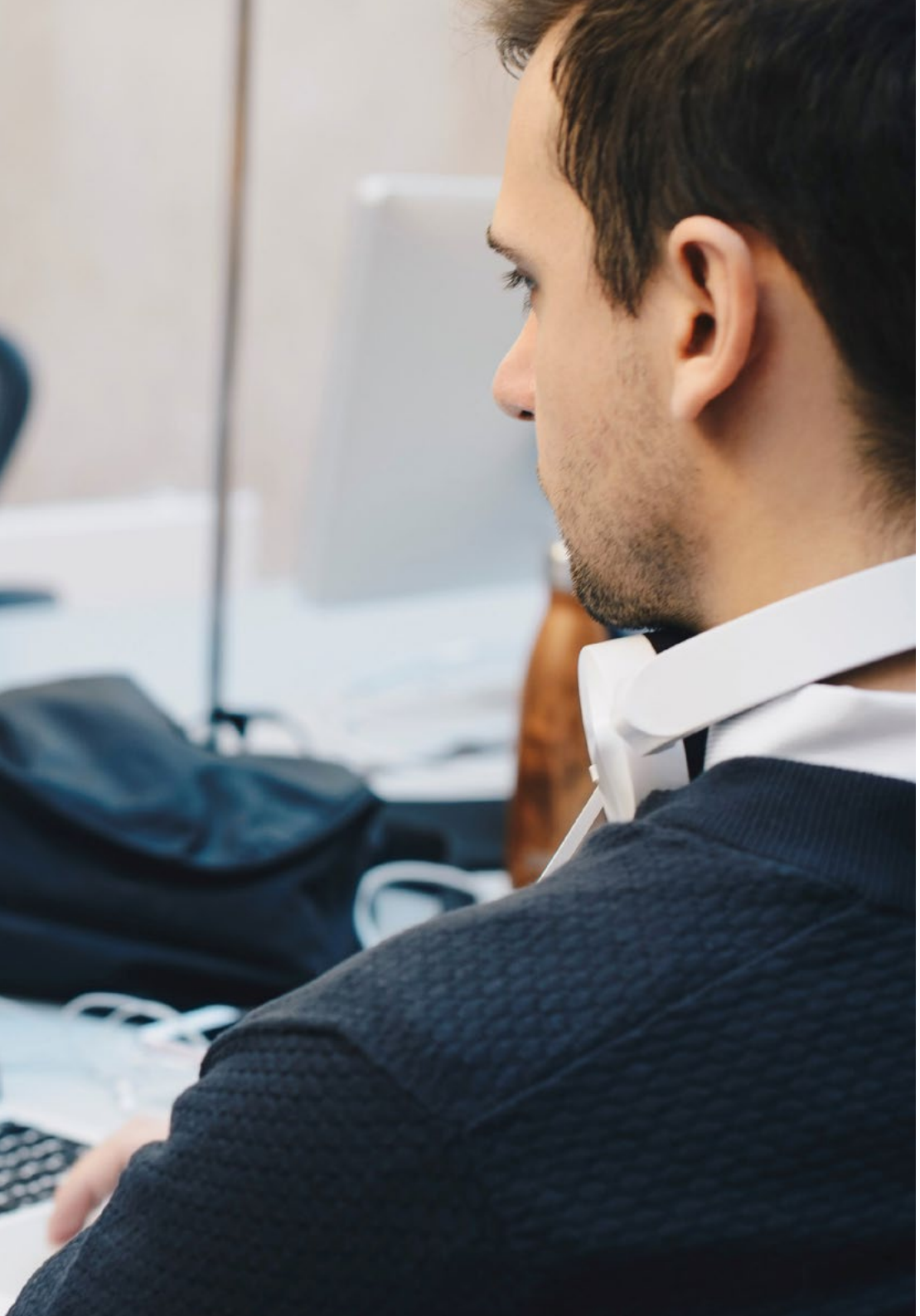
Per sviluppare le competenze avanzate e specializzate che deve possedere un informatico esperto in Politiche di Cybersecurity, TECH si è avvalsa di un personale docente di alto livello. Grazie alla combinazione pratica della loro esperienza professionale e degli ultimi sviluppi nel campo della sicurezza digitale, l'informatico otterrà una maggiore contestualizzazione di ogni argomento trattato, con numerosi esempi e risorse multimediali a supporto.

*Otterrai una serie di competenze che ti renderanno fondamentale in qualsiasi piano di strategia informatica della tua organizzazione"*

## Competenze generali

- Implementare e sviluppare un piano di continuità operativa a seconda dell'entità e alle sue esigenze
- Sviluppare un'Analisi dei Processi Aziendali
- Analizzare le metodologie di controllo
- Valutare la necessità di un'analisi informatica forense per lo studio approfondito degli incidenti registrati

*Aumenterai le tue prospettive lavorative e salariali grazie a una specializzazione nella materia che attualmente desta grande preoccupazione, la cybersecurity"*





## Competenze specifiche

- Determinare il coinvolgimento di un SGSI nell'organizzazione interna dell'ente, nonché il suo status
- Stabilire le politiche di sicurezza dell'azienda
- Determinare le misure da attuare nei confronti dei fornitori e della manutenzione dei sistemi informativi
- Generare conoscenze specialistiche sul controllo delle minacce
- Determinare le fasi della gestione preventiva delle minacce
- Sviluppare metodologie per l'analisi delle minacce informatiche
- Classificare le minacce in base all'impatto e alla gravità
- Progettare la propria metodologia per l'analisi e il controllo preventivo delle minacce
- Implementare una corretta politica di controllo degli accessi per reti e servizi
- Analizzare l'importanza di una corretta gestione degli incidenti di sicurezza
- Catalogare i diversi sistemi biometrici in vigore
- Esaminare la Biometria e i sistemi biometrici
- Implementare corrette politiche di sicurezza fisica e sistemi di controllo degli accessi fisici nei CED
- Implementare una rete sicura
- Esaminare le vulnerabilità delle piattaforme mobili e IoT e come evitarle
- Stabilire i tipi di Ingegneria Sociale e imparare a mitigarli
- Analizzare il concetto di Monitoraggio e Implementazione delle Metriche
- Determinare la necessità di continuità della sicurezza delle informazioni

04

# Direzione del corso

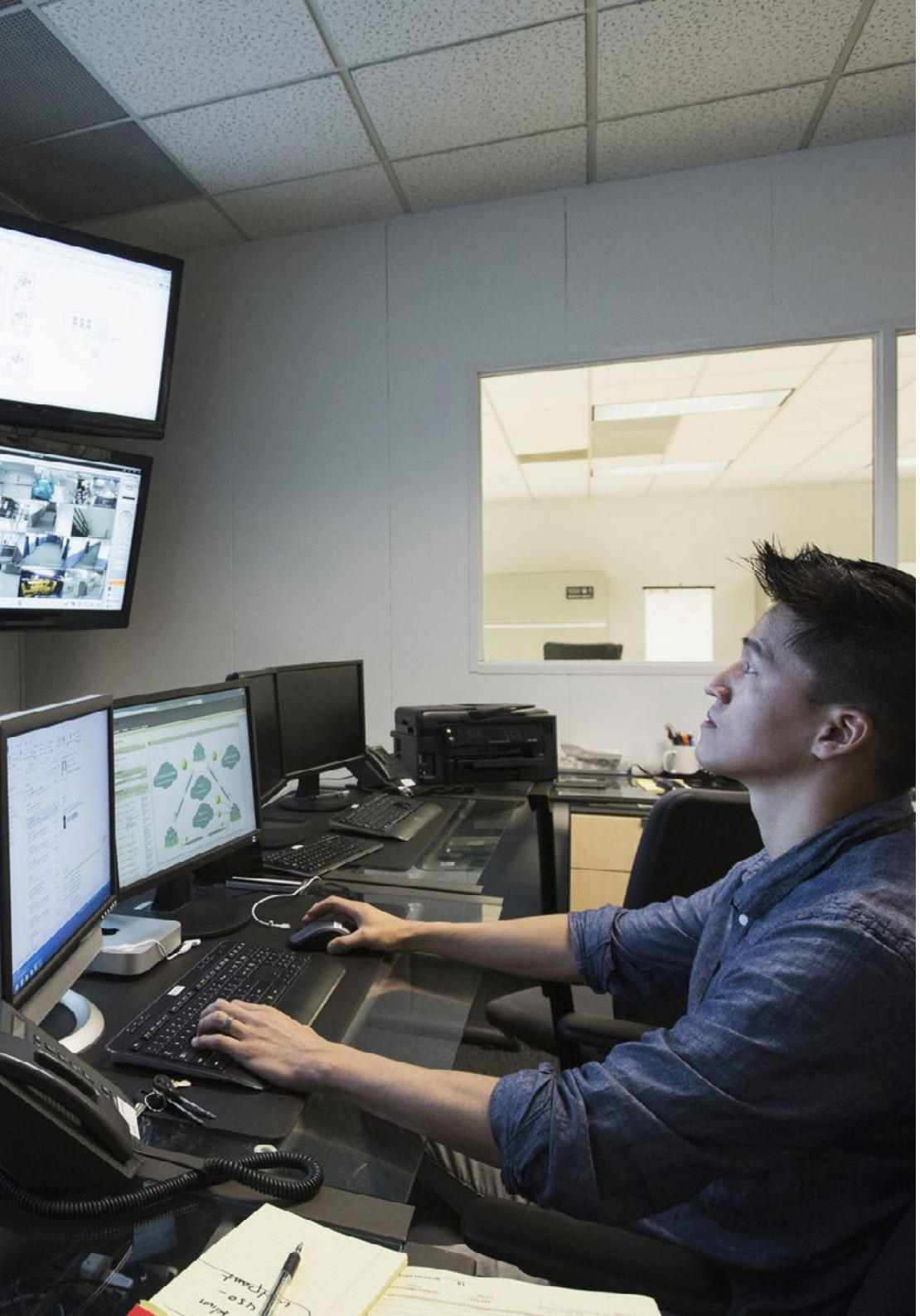
Tutti i professionisti selezionati da TECH per questo Master Privato vantano una vasta esperienza nel campo della gestione dei servizi informatici ma sempre con un occhio di riguardo alla cybersecurity e alla corretta esecuzione dei protocolli. È proprio questa esperienza a conferire una qualità superiore all'intero programma di studio, in quanto la sua natura eminentemente pratica fa sì che l'informatico possa adottare immediatamente tutte le nuove conoscenze, migliorando le proprie competenze anche prima del completamento della qualifica.

*Riceverai il supporto e l'aiuto di un gruppo di docenti impegnati al massimo nel tuo miglioramento professionale in Gestione delle Politiche di Cybersecurity"*

## Direzione

### Dott.ssa Fernández Sapena, Sonia

- Chief Security Officer presso l'Università delle Isole Baleari
- Senior Security Architect presso diverse università
- Responsabile della Sicurezza Informatica presso Sufi e Campus Extens dell'UIB
- Laurea in Ingegneria Informatica presso l'Università di Alcalá de Henares
- Master in DevOps: Docker and Kubernetes presso il Cyber Business Center





## Personale docente

### Dott. Oropesiano Carrizosa, Francisco

- Gestore dei servizi Web/Mail/DNS/Gestori di contenuti
- Tecnico della Sicurezza di Rete e dei Sistemi Server
- Progettazione e realizzazione di siti Web
- Laurea in Ingegneria Informatica presso l'Università di Alcalá de Henares
- Master in DevOps: Docker and Kubernetes presso il Cyber Business Center
- Master Esperto in Reti e Telecomunicazioni

### Dott. Peralta Alonso, Jon

- Avvocato / DPO presso Altia Consultores S.A.
- Avvocato / Consulente legale presso Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Direttore Commerciale presso Kutxabank
- Laurea in Giurisprudenza presso l'Università Pubblica dei Paesi Baschi
- Master in Protezione dei Dati presso la EIS Innovative School
- Laurea in Master Universitario in Legge presso l'Università Pubblica dei Paesi Baschi

### Dott. Ortega López, Florencio

- Consulente di ICT e Sicurezza in aziende private e pubbliche
- Laurea in Ingegneria Tecnica Industriale presso l'Università di Alcalá de Henares
- Master Universitario per il personale docente dell'Unir
- MBA in Gestione e Amministrazione Aziendale presso IDE-CESEM
- Master in Direzione e Gestione delle Tecnologie dell'Informazione presso IDE-CESEM

05

# Struttura e contenuti

TECH ha utilizzato la metodologia del *Relearning* per sviluppare tutti i contenuti di questo programma. Ciò significa che i concetti più importanti nel campo della Gestione delle Politiche di Cybersecurity vengono forniti progressivamente nel corso dell'intero programma, garantendo un insegnamento molto più efficace e rapido. L'informatico avrà accesso a numerosi video di approfondimento, esercizi di autoconsapevolezza e letture complementari specificamente selezionate per ogni argomento del programma.


*Tutto il materiale multimediale contenuto in questo Master Privato ti aiuterà a specializzarti in modo molto più approfondito, veloce ed esaustivo"*

## **Modulo 1.** Sistema di Gestione della Sicurezza Informatica

1.1. Sicurezza delle informazioni. Aspetti chiave
  1.1.1. Sicurezza delle informazioni
    1.1.1.1. Riservatezza
    1.1.1.2. Integrità
    1.1.1.3. Disponibilità
    1.1.1.4. Misure di sicurezza informatica
1.2. Sistema di gestione della sicurezza informatica
  1.2.1. Modelli di gestione della sicurezza informatica
  1.2.2. Documenti per l'implementazione di un SGSI
  1.2.3. Livelli e controlli del SGSI
1.3. Norme e standard internazionali
  1.3.1. Standard internazionali di sicurezza informatica
  1.3.2. Origine ed evoluzione dello standard
  1.3.3. Standard Internazionali di Gestione della Sicurezza Informatica
  1.3.4. Altri standard di riferimento
1.4. Norme ISO/IEC 27.000
  1.4.1. Oggetto e ambito di applicazione
  1.4.2. Struttura della norma
  1.4.3. Certificazione
  1.4.4. Fasi dell'accreditamento
  1.4.5. Vantaggi degli standard ISO/IEC 27.000
1.5. Progettazione e implementazione di un Sistema Generale di Sicurezza Informatica
  1.5.1. Progettazione e implementazione di un Sistema Generale di Sicurezza Informatica
  1.5.2. Fasi di implementazione di un sistema Generale di Sicurezza Informatica
  1.5.3. Piano di continuità aziendale
1.6. Fase I: diagnosi
  1.6.1. Diagnosi preliminare
  1.6.2. Identificazione del livello di stratificazione
  1.6.3. Livello di conformità agli standard/norme
1.7. Fase II: preparazione
  1.7.1. Contesto organizzativo
  1.7.2. Analisi delle norme di sicurezza applicabili
  1.7.3. Ambito di applicazione del Sistema di Sicurezza Generale Informatico
  1.7.4. Politica del Sistema Generale di Sicurezza Informatico
  1.7.5. Obiettivi del Sistema Generale di Sicurezza Informatico
1.8. Fase III: pianificazione
  1.8.1. Classificazione degli attivi
  1.8.2. Valutazione del rischio
  1.8.3. Identificazione di minacce e rischi
1.9. Fase IV: attuazione e monitoraggio
  1.9.1. Analisi dei risultati
  1.9.2. Assegnazione di responsabilità
  1.9.3. Tempistica del piano d'azione
  1.9.4. Monitoraggio e controlli
1.10. Politiche di sicurezza per la gestione degli incidenti
  1.10.1. Fasi
  1.10.2. Categorizzazione degli incidenti
  1.10.3. Procedure e gestione degli incidenti

## **Modulo 2.** Aspetti organizzativi della Politica di Sicurezza Informatica

2.1. Organizzazione interna
  2.1.1. Assegnazione di responsabilità
  2.1.2. Separazione dei compiti
  2.1.3. Contatti con le autorità
  2.1.4. La sicurezza informatica nella gestione dei progetti
2.2. Gestione delle attività
  2.2.1. Responsabilità sui beni
  2.2.2. Classificazione delle informazioni
  2.2.3. Gestione dei supporti di memorizzazione

2.3. Politiche di sicurezza nei processi aziendali
  2.3.1. Analisi dei processi aziendali vulnerabili
  2.3.2. Analisi dell'impatto aziendale
  2.3.3. Classificazione dei processi rispetto all'impatto aziendale
2.4. Politiche di sicurezza legate alle Risorse Umane
  2.4.1. Pre-assunzione
  2.4.2. Durante il reclutamento
  2.4.3. Cessazione o cambio di incarico
2.5. Politiche di sicurezza a livello di gestione
  2.5.1. Linee guida per la gestione della sicurezza delle informazioni
  2.5.2. BIA - analisi dell'impatto
  2.5.3. Piano di recupero come politica di sicurezza
2.6. Acquisizione e manutenzione di sistemi informatici
  2.6.1. Requisiti di sicurezza dei sistemi informatici
  2.6.2. Sicurezza dei dati di sviluppo e di supporto
  2.6.3. Dati di prova
2.7. Sicurezza con i fornitori
  2.7.1. Sicurezza informatica con i fornitori
  2.7.2. Gestione della fornitura del servizio con garanzia
  2.7.3. Sicurezza della catena di approvvigionamento
2.8. Sicurezza operativa
  2.8.1. Responsabilità operative
  2.8.2. Protezione contro il codice maligno
  2.8.3. Copie di backup
  2.8.4. Registri delle attività e monitoraggio
2.9. Gestione della sicurezza e normative
  2.9.1. Gestione della sicurezza e normative
  2.9.2. Conformità ai requisiti legali
  2.9.3. Revisioni di sicurezza informatica
2.10. Sicurezza nella gestione della continuità operativa
  2.10.1. Sicurezza nella gestione della continuità operativa
  2.10.2. Continuità della sicurezza informatica
  2.10.3. Licenziamenti

## **Modulo 3.** Politiche di Sicurezza per l'Analisi delle Minacce nei Sistemi Informatici

3.1. Gestione delle minacce nelle politiche di sicurezza
  3.1.1. Gestione dei rischi
  3.1.2. Rischio di sicurezza
  3.1.3. Metodologie di gestione delle minacce
  3.1.4. Implementazione delle metodologie
3.2. Fasi della gestione delle minacce
  3.2.1. Identificazione
  3.2.2. Analisi
  3.2.3. Localizzazione
  3.2.4. Misure di salvaguardia
3.3. Sistemi di controllo per la localizzazione delle minacce
  3.3.1. Sistemi di controllo per la localizzazione delle minacce
  3.3.2. Classificazione e flusso di informazioni
  3.3.3. Analisi dei processi vulnerabili
3.4. Classificazione del rischio
  3.4.1. Tipi di rischio
  3.4.2. Calcolo della probabilità di pericolo
  3.4.3. Rischio residuale
3.5. Trattamento dei rischi
  3.5.1. Trattamento dei rischi
  3.5.2. Implementazione delle misure di salvaguardia
  3.5.3. Trasferire o assumere

3.6. Controllo del rischio
- 3.6.1. Processo continuo di gestione del rischio
- 3.6.2. Implementazione delle metriche di sicurezza
- 3.6.3. Modello strategico delle metriche di sicurezza informatica

3.7. Metodologie pratiche per l'analisi e il controllo delle minacce
- 3.7.1. Catalogo delle minacce
- 3.7.2. Catalogo delle misure di controllo
- 3.7.3. Catalogo delle salvaguardie

3.8. Norma ISO 27005
- 3.8.1. Identificazione dei rischi
- 3.8.2. Analisi dei rischi
- 3.8.3. Valutazione dei rischi

3.9. Matrice di rischio, impatto e minaccia
- 3.9.1. Dati, sistemi e personale
- 3.9.2. Probabilità di minaccia
- 3.9.3. Entità del danno

3.10. Progettazione di fasi e processi nell'analisi dei rischi
- 3.10.1. Identificazione degli elementi critici dell'organizzazione
- 3.10.2. Determinazione delle minacce e degli impatti
- 3.10.3. Analisi dell'impatto e del rischio
- 3.10.4. Metodologie

## **Modulo 4.** Implementazione pratica delle politiche di sicurezza del software e dell'hardware

4.1. Implementazione pratica delle politiche di sicurezza del software e dell'hardware
- 4.1.1. Implementazione dell'identificazione e dell'autorizzazione
- 4.1.2. Implementazione di tecniche di identificazione
- 4.1.3. Misure tecniche per l'autorizzazione

4.2. Tecnologie di identificazione e autorizzazione
- 4.2.1. Identificatore e OTP
- 4.2.2. *Token USB* o smart card PKI
- 4.2.3. Chiave "Difesa Confidenziale"
- 4.2.4. RFID attivo

4.3. Politiche di sicurezza per l'accesso a software e sistemi
- 4.3.1. Implementazione delle politiche di controllo degli accessi
- 4.3.2. Implementazione di politiche di accesso alle comunicazioni
- 4.3.3. Tipi di strumenti di sicurezza per il controllo degli accessi

4.4. Gestione dell'accesso degli utenti
- 4.4.1. Gestione dei diritti di accesso
- 4.4.2. Separazione dei ruoli e delle funzioni di accesso
- 4.4.3. Implementazione dei diritti di accesso nei sistemi

4.5. Controllo dell'accesso a sistemi e applicazioni
- 4.5.1. Regola dell'accesso minimo
- 4.5.2. Tecnologie di accesso sicuro
- 4.5.3. Politiche di sicurezza nelle password

4.6. Tecnologie dei sistemi di identificazione
- 4.6.1. Active Directory
- 4.6.2. OTP
- 4.6.3. PAP, CHAP
- 4.6.4. KERBEROS, DIAMETER, NTLM

4.7. Controlli CIS per i sistemi di difesa bastion
- 4.7.1. Controlli CIS di base
- 4.7.2. Controlli CIS fondamentali
- 4.7.3. Controlli organizzativi CIS

4.8. Sicurezza operativa
- 4.8.1. Protezione contro il codice maligno
- 4.8.2. Copie di backup
- 4.8.3. Registri delle attività e monitoraggio

4.9. Gestione delle vulnerabilità tecniche
- 4.9.1. Vulnerabilità tecniche
- 4.9.2. Gestione delle vulnerabilità tecniche
- 4.9.3. Restrizioni all'installazione del software

4.10. Implementazione delle pratiche della politica di sicurezza
- 4.10.1. Implementazione delle pratiche della politica di sicurezza
- 4.10.2. Vulnerabilità logiche
- 4.10.3. Implementazione delle politiche di difesa

## **Modulo 5.** Politiche di gestione degli incidenti di sicurezza

5.1. Politiche e miglioramenti per la gestione degli incidenti di sicurezza delle informazioni
- 5.1.1. Gestione degli incidenti
- 5.1.2. Responsabilità e procedure
- 5.1.3. Notifica di eventi

5.2. Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)
- 5.2.1. Dati di funzionamento del sistema
- 5.2.2. Tipi di sistemi di rilevamento delle intrusioni
- 5.2.3. Criteri per la collocazione di IDS/IPS

5.3. Risposta agli incidenti di sicurezza
- 5.3.1. Procedura di raccolta delle informazioni
- 5.3.2. Processo di verifica delle intrusioni
- 5.3.3. Organi del CERT

5.4. Processo di notifica e gestione dei tentativi di intrusione
- 5.4.1. Responsabilità nel processo di notifica
- 5.4.2. Classificazione degli incidenti
- 5.4.3. Processo di risoluzione e recupero

5.5. Analisi forense come politica di sicurezza
- 5.5.1. Prove volatili e non volatili
- 5.5.2. Analisi e raccolta di prove elettroniche
  - 5.5.2.1. Analisi delle prove elettroniche
  - 5.5.2.2. Raccolta di prove elettroniche

5.6. Strumenti per i Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)
- 5.6.1. *Snort*
- 5.6.2. Suricata
- 5.6.3. Solar-Winds

5.7. Strumenti di centralizzazione degli eventi
- 5.7.1. SIM
- 5.7.2. SEM
- 5.7.3. SIEM

5.8. Guida di sicurezza CCN-STIC 817
- 5.8.1. Guida di sicurezza CCN-STIC 817
- 5.8.2. Gestione degli incidenti informatici
- 5.8.3. Metriche e indicatori

5.9. NIST SP800-61
- 5.9.1. Capacità di risposta agli incidenti di sicurezza informatica
- 5.9.2. Gestione degli incidenti
- 5.9.3. Coordinamento e condivisione delle informazioni

5.10. Norma ISO 27035
- 5.10.1. Norma ISO 27035. Principi di gestione degli incidenti
- 5.10.2. Linee guida per lo sviluppo di un piano di gestione degli incidenti
- 5.10.3. Linee guida per le operazioni di risposta agli incidenti

## **Modulo 6.** Implementazione di politiche di sicurezza fisica e ambientale in azienda

6.1. Aree sicure
- 6.1.1. Perimetro di sicurezza fisica
- 6.1.2. Lavorare in aree sicure
- 6.1.3. Sicurezza di uffici, sedi e risorse

6.2. Controlli fisici all'ingresso
- 6.2.1. Controlli fisici all'ingresso
- 6.2.2. Politiche di controllo degli accessi fisici
- 6.2.3. Sistemi di controllo dell'ingresso fisico

6.3. Vulnerabilità dell'accesso fisico
- 6.3.1. Vulnerabilità dell'accesso fisico
- 6.3.2. Principali vulnerabilità fisiche
- 6.3.3. Implementazione delle misure di salvaguardia

6.4. Sistemi biometrici fisiologici
- 6.4.1. Impronta digitale
- 6.4.2. Riconoscimento facciale
- 6.4.3. Riconoscimento dell'iride e della retina
- 6.4.4. Altri sistemi biometrici fisiologici

6.5. Sistemi biometrici comportamentali
- 6.5.1. Riconoscimento della firma
- 6.5.2. Riconoscimento dello scrittore
- 6.5.3. Riconoscimento vocale
- 6.5.4. Altri sistemi biometrici comportamentali

6.6. Gestione del rischio nella biometria
- 6.6.1. Gestione del rischio nella biometria
- 6.6.2. Implementazione di sistemi biometrici
- 6.6.3. Vulnerabilità dei sistemi biometrici

6.7. Implementazione delle politiche in *hosts*
- 6.7.1. Installazione della rete e sicurezza di cablaggio
- 6.7.2. Ubicazione dell'apparecchiatura
- 6.7.3. Uscita delle apparecchiature all'esterno dei locali
- 6.7.4. Apparecchiature informatiche incustodite e politica dei posti liberi

6.8. Protezione ambientale
- 6.8.1. Sistemi di protezione antincendio
- 6.8.2. Sistemi di protezione antisismica
- 6.8.3. Sistemi di protezione antisismica

6.9. Sicurezza del centro di elaborazione dati
- 6.9.1. Porte di sicurezza
- 6.9.2. Sistemi di videosorveglianza (CCTV)
- 6.9.3. Controllo di sicurezza

6.10. Normative internazionali sulla sicurezza fisica
- 6.10.1. IEC 62443-2-1 (europea)
- 6.10.2. NERC CIP-005-5 (U.S.A.)
- 6.10.3. NERC CIP-014-2 (U.S.A.)

## **Modulo 7.** Politiche di comunicazione sicura in azienda

7.1. Gestione della sicurezza di rete
- 7.1.1. Controllo e monitoraggio della rete
- 7.1.2. Separazione della rete
- 7.1.3. Sistemi di sicurezza di rete

7.2. Protocolli di comunicazione sicuri
- 7.2.1. Modello TCP/IP
- 7.2.2. Protocollo IPSEC
- 7.2.3. Protocollo TLS

7.3. Protocollo TLS 1,3
- 7.3.1. Fasi di un processo TLS1.3
- 7.3.2. Protocollo *Handshake*
- 7.3.3. Protocollo di registrazione
- 7.3.4. Differenze con TLS 1.2

7.4. Algoritmi crittografici
- 7.4.1. Algoritmi crittografici utilizzati nelle comunicazioni
- 7.4.2. *Cipher-suites*
- 7.4.3. Algoritmi crittografici consentiti per TLS 1.3

7.5. Funzioni *Digest*
- 7.5.1. Funzioni *Digest*
- 7.5.2. MD6
- 7.5.3. SHA

7.6. PKI. Infrastruttura a chiave pubblica
- 7.6.1. PKI e le sue entità
- 7.6.2. Certificato digitale
- 7.6.3. Tipi di certificati digitali

7.7. Comunicazioni tunneling e trasporto
- 7.7.1. Comunicazioni tunneling
- 7.7.2. Comunicazioni di trasporto
- 7.7.3. Implementazione del tunneling crittografato

7.8. SSH. *Secure Shell*
- 7.8.1. SSH. Shell sicura
- 7.8.2. Funzionamento SSH
- 7.8.3. Strumenti SSH

7.9. Verifica dei sistemi crittografici
- 7.9.1. Verifica dei sistemi crittografici
- 7.9.2. Test di integrità
- 7.9.3. Test del sistema crittografico

7.10. Sistemi crittografici
- 7.10.1. Sistemi crittografici
- 7.10.2. Vulnerabilità dei sistemi crittografici
- 7.10.3. Salvaguardie crittografiche

## **Modulo 8.** Implementazione pratica delle politiche di sicurezza in caso di attacchi

8.1. *System Hacking*
- 8.1.1. *System Hacking*
- 8.1.2. Rischi e vulnerabilità
- 8.1.3. Contromisure

8.2. DoS nei servizi
- 8.2.1. DoS nei servizi
- 8.2.2. Rischi e vulnerabilità
- 8.2.3. Contromisure

8.3. *Session Hijacking*
- 8.3.1. *Session Hijacking*
- 8.3.2. Il processo di *Hijacking*
- 8.3.3. Contromisure di *Hijacking*

8.4. Evasione di IDS, *Firewalls and Honeypots*
- 8.4.1. Evasione di IDS, *Firewalls and Honeypots*
- 8.4.2. Tecniche di evasione
- 8.4.3. Implementazione delle contromisure

8.5. *Hacking Web Servers*
- 8.5.1. *Hacking Web Servers*
- 8.5.2. Attacchi ai server web
- 8.5.3. Implementazione delle misure di difesa

8.6. *Hacking Web Applications*
- 8.6.1. *Hacking Web Applications*
- 8.6.2. Attacchi alle applicazioni web
- 8.6.3. Implementazione delle misure di difesa

8.7. *Hacking Wireless Networks*
- 8.7.1. *Hacking Wireless Networks*
- 8.7.2. Vulnerabilità delle reti wi-fi
- 8.7.3. Implementazione delle misure di difesa

8.8. *Hacking Mobile Platforms*
- 8.8.1. *Hacking Mobile Platforms*
- 8.8.2. Vulnerabilità di piattaforme mobili
- 8.8.3. Implementazione delle contromisure

8.9. *Ramsonware*
- 8.9.1. *Ramsonware*
- 8.9.2. Vulnerabilità che causano *Ramsonware*
- 8.9.3. Implementazione delle contromisure

8.10. Ingegneria Sociale
- 8.10.1. Ingegneria Sociale
- 8.10.2. Tipi di ingegneria Sociale
- 8.10.3. Contromisure per l'ingegneria Sociale

## **Modulo 9.** Strumenti di Monitoraggio nelle Politiche di Sicurezza dei Sistemi Informatici

9.1. Politiche di monitoraggio dei sistemi informatici
- 9.1.1. Monitoraggio dei Sistemi
- 9.1.2. Metriche
- 9.1.3. Tipi di metriche

9.2. Controllo e registrazione dei Sistemi
- 9.2.1. Audit e Registrazione dei Sistemi
- 9.2.2. Controllo e registrazione di Windows
- 9.2.3. Controllo e registrazione di Linux

9.3. Protocollo SNMP. *Simple Network Management Protocol*
- 9.3.1. Protocollo SNMP
- 9.3.2. Funzionamento SNMP
- 9.3.3. Strumenti SNMP

9.4. Monitoraggio delle reti
- 9.4.1. Monitoraggio delle reti
- 9.4.2. Monitoraggio della rete nei sistemi di controllo
- 9.4.3. Strumenti di monitoraggio per i sistemi di controllo

9.5. Nagios. Sistema di monitoraggio delle reti
- 9.5.1. Nagios
- 9.5.2. Funzionamento di Nagios
- 9.5.3. Installazione di Nagios

9.6. Zabbix. Sistema di monitoraggio delle reti
- 9.6.1. Zabbix
- 9.6.2. Funzionamento di Zabbix
- 9.6.3. Installazione di Zabbix

9.7. Cacti. Sistema di monitoraggio delle reti
- 9.7.1. Cacti
- 9.7.2. Funzionamento di Cacti
- 9.7.3. Installazione di Cacti

9.8. Pandora. Sistema di monitoraggio delle reti
- 9.8.1. Pandora
- 9.8.2. Funzionamento di Pandora
- 9.8.3. Installazione di Pandora

9.9. *SolarWinds*. Sistema di monitoraggio delle reti
- 9.9.1. *SolarWinds*
- 9.9.2. Funzionamento di *SolarWinds*
- 9.9.3. Installazione di *SolarWinds*

9.10. Normativa di Monitoraggio
- 9.10.1. Normativa di Monitoraggio
- 9.10.2. Controlli CIS su controllo e registrazione
- 9.10.3. NIST 800-123 (U.S.A.)

## **Modulo 10.** Politica di Disaster Recovery Pratica di Sicurezza

10.1. DRP. Piano di Disaster Recovery
- 10.1.1. Scopo di un DRP
- 10.1.2. Vantaggi di un DRP
- 10.1.3. Conseguenze della mancanza di un DRP e del suo mancato aggiornamento

10.2. Guida alla definizione di un DRP (Disaster Recovery Plan)
- 10.2.1. Portata e obiettivi
- 10.2.2. Progettazione della strategia di recupero
- 10.2.3. Assegnazione di ruoli e responsabilità
- 10.2.4. Realizzazione di un inventario di hardware, software e servizi
- 10.2.5. Tolleranza ai tempi di inattività e alla perdita di dati
- 10.2.6. Definizione dei tipi specifici di DRP richiesti
- 10.2.7. Attuazione di un piano di formazione, sensibilizzazione e comunicazione

10.3. Portata e obiettivi di un DRP (Disaster Recovery Plan)
- 10.3.1. Garanzia di risposta
- 10.3.2. Componenti tecnologici
- 10.3.3. Portata della politica di continuità

10.4. Progettazione di una Strategia DRP (Disaster Recovery)
- 10.4.1. Strategia di Disaster Recovery
- 10.4.2. Budget
- 10.4.3. Risorse Umane e Fisiche
- 10.4.4. Posizioni dirigenziali a rischio
- 10.4.5. Tecnologia
- 10.4.6. Dati

10.5. Continuità dei processi informatici
- 10.5.1. Pianificazione della continuità
- 10.5.2. Implementazione della continuità
- 10.5.3. Verifica e valutazione della continuità

10.6. Portata di un BCP (Business Continuity Plan)
- 10.6.1. Determinazione dei processi più critici
- 10.6.2. Approccio basato sugli attivi
- 10.6.3. Approccio al processo

10.7. Implementazione di processi aziendali garantiti
- 10.7.1. Attività prioritarie (PA)
- 10.7.2. Tempi di recupero ideali (IRT)
- 10.7.3. Strategie di sopravvivenza

10.8. Analisi organizzativa
- 10.8.1. Ottenimento di informazioni
- 10.8.2. Analisi dell'impatto aziendale (BIA)
- 10.8.3. Analisi del rischio organizzativo

10.9. Risposta di emergenza
- 10.9.1. Piano di crisi
- 10.9.2. Piani di ripristino dell'ambiente operativo
- 10.9.3. Procedure tecniche di lavoro o di incidente

10.10. Norma internazionale ISO 27031 BCP
- 10.10.1. Obiettivi
- 10.10.2. Termini e definizioni
- 10.10.3. Operazione

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

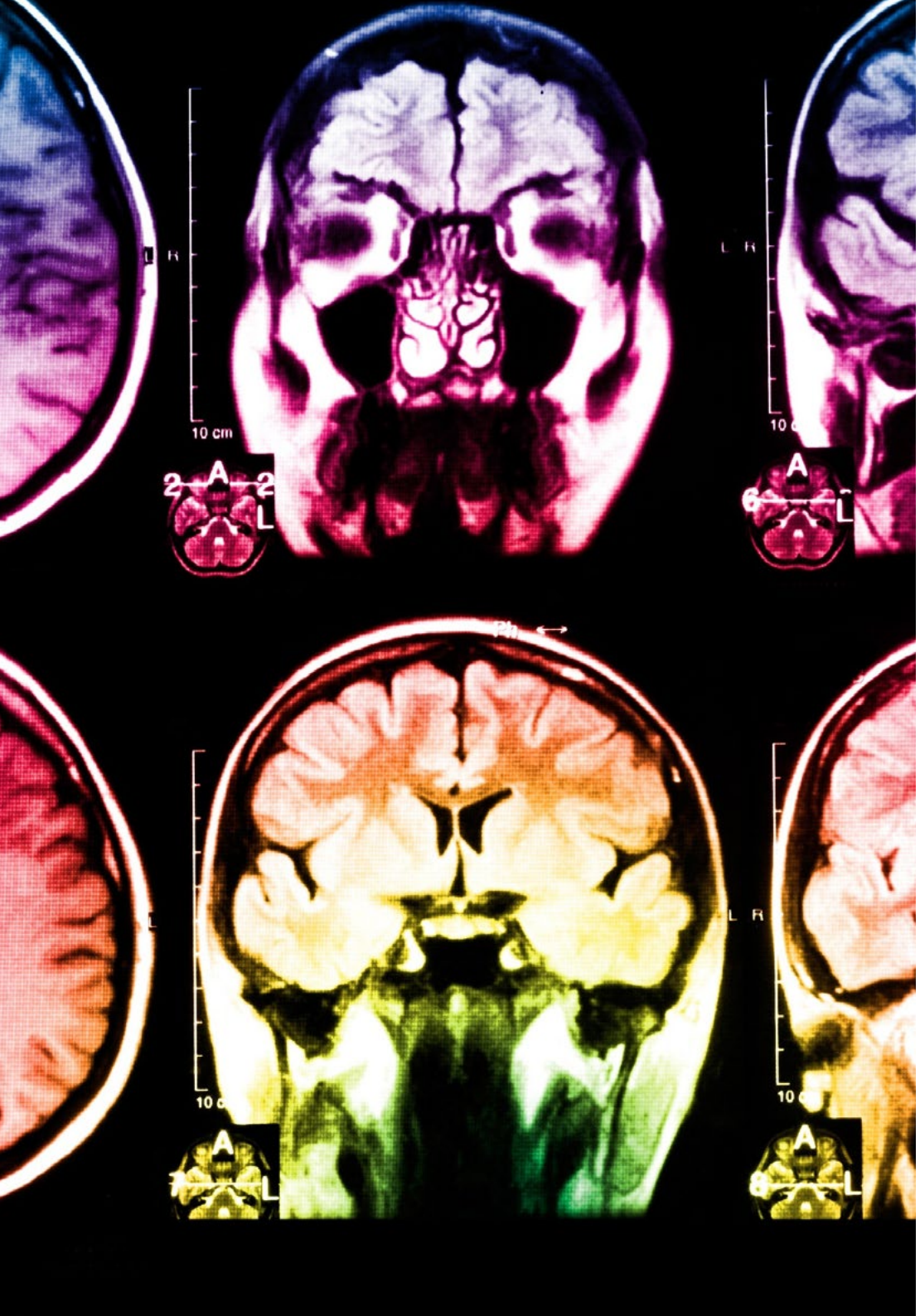
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

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.

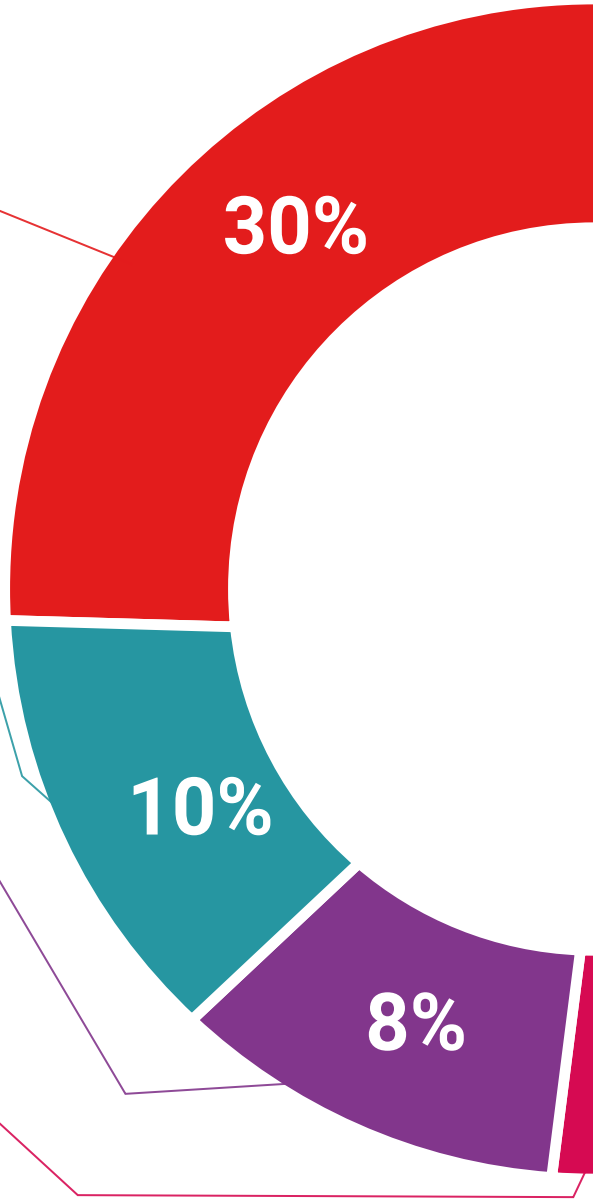
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

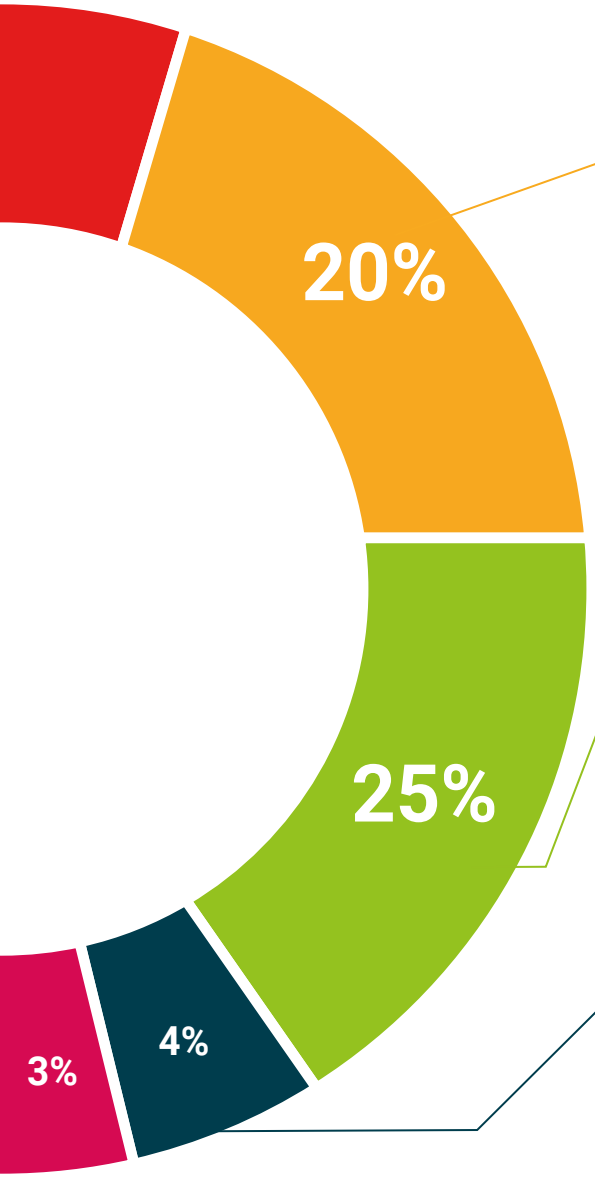
### Pratiche di competenze e competenze

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

Il Master Privato in Gestione delle Politiche di Cybersecurity in Azienda, oltre alla preparazione più rigorosa e aggiornata, l'accesso a una qualifica di Master Privato rilasciata da TECH Università Tecnologica.

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

Questo **Master Privato in Gestione delle Politiche di Cybersecurity in Azienda** possiede il programma più completo e aggiornato del mercato.

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

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

Titolo: **Master Privato in Gestione delle Politiche di Cybersecurity in Azienda**

N. Ore Ufficiali: **1.500 O.**

tech università tecnologica

Conferisce il presente

DIPLOMA

a

Dott./Dott.ssa _____, con documento d'identità n°_____

Per aver completato con esito positivo e accreditato il programma di

MASTER PRIVATO

in

Gestione delle Politiche di Cybersecurity in Azienda

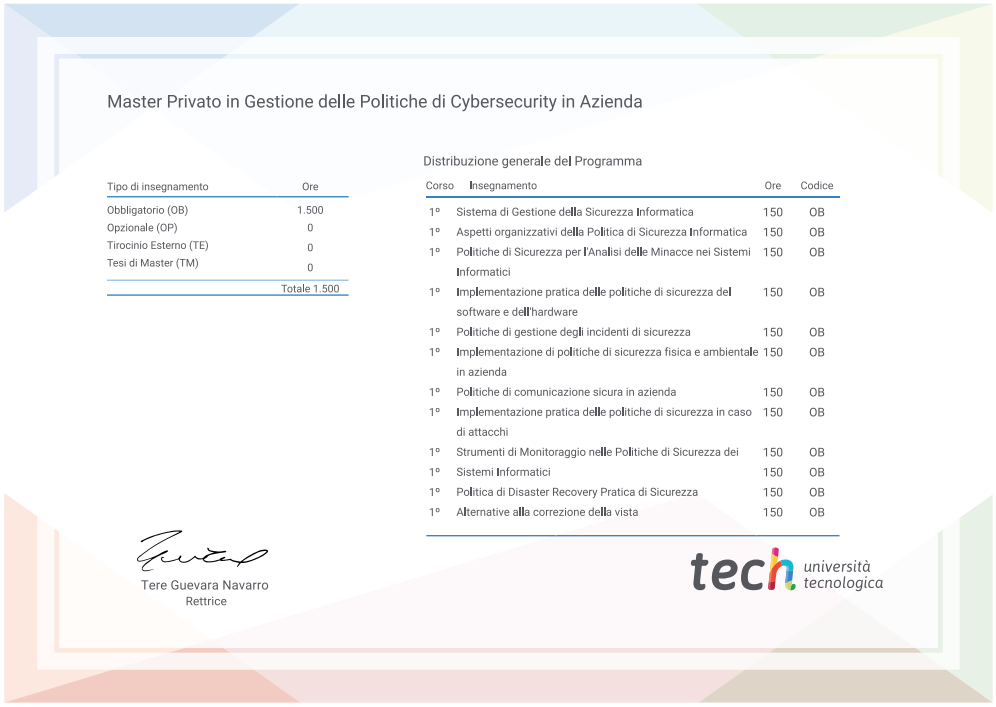
Si tratta di un titolo rilasciato da questa Università ed equivalente a 1.500 ore, con data di inizio gg/mm/aaaa e con data di fine gg/mm/aaaa.

TECH è un Istituto Privato di Istruzione Superiore riconosciuto dal Ministero della Pubblica Istruzione a partire dal 28 giugno 2018.

In data 17 Giugno 2020

Tere Guevara Navarro
Rettrice

Questo titolo deve essere sempre accompagnato da un titolo universitario rilasciato dall'autorità competente per l'esercizio della pratica professionale in ogni paese. codice unico TECH: AFWORD23S techtitute.com/titulos



Master Privato in Gestione delle Politiche di Cybersecurity in Azienda

| Tipo di insegnamento | Ore |
|---|---|
| Obbligatorio (OB) | 1.500 |
| Opzionale (OP) | 0 |
| Tirocinio Esterno (TE) | 0 |
| Tesi di Master (TM) | 0 |
| | Totale 1.500 |

Distribuzione generale del Programma

| Corso | Insegnamento | Ore | Codice |
|---|---|---|---|
| 1° | Sistema di Gestione della Sicurezza Informatica | 150 | OB |
| 1° | Aspetti organizzativi della Politica di Sicurezza Informatica | 150 | OB |
| 1° | Politiche di Sicurezza per l'Analisi delle Minacce nei Sistemi Informatici | 150 | OB |
| 1° | Implementazione pratica delle politiche di sicurezza del software e dell'hardware | 150 | OB |
| 1° | Politiche di gestione degli incidenti di sicurezza | 150 | OB |
| 1° | Implementazione di politiche di sicurezza fisica e ambientale in azienda | 150 | OB |
| 1° | Politiche di comunicazione sicura in azienda | 150 | OB |
| 1° | Implementazione pratica delle politiche di sicurezza in caso di attacchi | 150 | OB |
| 1° | Strumenti di Monitoraggio nelle Politiche di Sicurezza dei Sistemi Informatici | 150 | OB |
| 1° | Politica di Disaster Recovery Pratica di Sicurezza | 150 | OB |
| 1° | Alternative alla correzione della vista | 150 | OB |

Tere Guevara Navarro
Rettrice

tech università tecnologica

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

tech università tecnologica

# Master Privato

## Gestione delle Politiche di Cybersecurity in Azienda

- Modalità: **online**
- Durata: **12 mesi**
- Titolo: **TECH Università Tecnologica**
- Dedizione: **16 ore/settimana**
- Orario: **a scelta**
- Esami: **online**

# Master Privato

## Gestione delle Politiche di Cybersecurity in Azienda

tech università tecnologica