UNIVERSITÀ DEGLI STUDI ”NICCOLO’ CUSANO”

DIPARTIMENTO DI INGEGNERIA

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

”DALL’ALIMENTAZIONE ALLA CYBERSECURITY: FONDAMENTI DI UN’INFRASTRUTTURA IT SICURA NELLA GRANDE DISTRIBUZIONE”

Relatore: Prof. [Giovanni Farina]

Candidato: [Marco Santoro]
Matricola: [IN08000291]

ANNO ACCADEMICO 2024/2025

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

Introduzione

1.1 Contesto e Motivazione della Ricerca

1.1.1 La Complessità Sistemica della Grande Distribuzione Organizzata

La Grande Distribuzione Organizzata (GDO) rappresenta uno dei settori più complessi e critici dell'economia italiana, caratterizzato da un'infrastruttura tecnologica la cui sofisticazione è spesso sottovalutata. Con oltre 27.000 punti vendita distribuiti sul territorio nazionale[1] e un volume di transazioni giornaliere che supera i 45 milioni di operazioni, il settore gestisce una complessità paragonabile a quella dei servizi finanziari o delle telecomunicazioni, ma con vincoli operativi unici che ne amplificano le sfide ingegneristiche.

La peculiarità del settore GDO risiede nella sua natura intrinsecamente distribuita e nella criticità delle sue operazioni. Ogni punto vendita rappresenta non solo un luogo di commercio, ma un nodo computazionale che deve garantire continuità operativa ventiquattro ore su ventiquattro, processare transazioni in tempo reale, gestire sistemi di inventario complessi e, sempre più frequentemente, integrare tecnologie emergenti come l'Internet of Things (IoT) per il monitoraggio della catena del freddo o sistemi di intelligenza artificiale per l'ottimizzazione degli approvvigionamenti.

Questa complessità tecnologica si intreccia con requisiti di business stringenti. Durante eventi promozionali o periodi di picco stagionale, i sistemi devono gestire incrementi di carico che possono raggiungere il 300-500% rispetto ai volumi standard[2], mantenendo al contempo tem-

[1] ISTAT, *Struttura e competitività del sistema delle imprese - Commercio*, Roma, Istituto Nazionale di Statistica, 2024.

[2] CAPGEMINI, *Peak Performance: Managing Seasonal Loads in Retail IT*, Paris, Capgemini Research Institute, 2024.

pi di risposta inferiori ai 100 millisecondi per le transazioni critiche. La sfida non è semplicemente tecnica ma sistemica: come garantire performance, sicurezza e conformità normativa in un ambiente così dinamico e distribuito?

1.1.2 L'Evoluzione del Panorama Tecnologico e delle Minacce

Il settore della GDO sta attraversando una trasformazione profonda, guidata da tre forze convergenti che ridefiniscono i paradigmi operativi tradizionali.

La prima forza è rappresentata dalla **trasformazione digitale accelerata**. La migrazione verso architetture cloud-native non è più una scelta strategica ma una necessità operativa. Secondo i dati aggregati del settore, il 67% delle organizzazioni GDO europee ha avviato processi di migrazione verso modelli cloud-first[3]. Questa transizione, tuttavia, non si limita a un semplice spostamento di carichi di lavoro da data center on-premise a infrastrutture cloud. Richiede un ripensamento fondamentale delle architetture applicative, dei modelli di sicurezza e dei processi operativi.

La seconda forza è costituita dall'**evoluzione del panorama delle minacce cyber**. L'incremento degli attacchi informatici diretti al settore retail ha raggiunto proporzioni allarmanti, con un aumento del 312% nel periodo 2021-2023[4]. Particolarmente preoccupante è l'emergere di attacchi cyber-fisici che non si limitano a compromettere i sistemi informativi, ma possono impattare direttamente le operazioni fisiche dei punti vendita. Un attacco ai sistemi di controllo HVAC (Heating, Ventilation, and Air Conditioning), ad esempio, può compromettere la catena del freddo causando perdite economiche significative e rischi per la salute pubblica.

La terza forza è la **pressione normativa crescente**. L'entrata in vigore di regolamenti come il GDPR (General Data Protection Regulation), la direttiva NIS2 (Network and Information Security) e lo standard PCI-DSS (Payment Card Industry Data Security Standard) ha creato un panorama normativo complesso e interconnesso. Le organizzazioni de-

[3] IDC, *European Retail IT Transformation Benchmark 2024*, Framingham, International Data Corporation Report #EUR148923, 2024.

[4] ENISA, *Threat Landscape for Retail and Supply Chain 2024*, Heraklion, European Union Agency for Cybersecurity, 2024.

vono non solo garantire la conformità a ciascuno standard individualmente, ma gestire le interazioni e le potenziali contraddizioni tra requisiti diversi, il tutto mantenendo l'agilità operativa necessaria per competere nel mercato.

1.2 Problema di Ricerca e Obiettivi

1.2.1 Definizione del Problema

La convergenza delle sfide tecnologiche, di sicurezza e normative crea un problema di ottimizzazione multi-obiettivo di complessità significativa. Le organizzazioni GDO devono simultaneamente:

- Modernizzare l'infrastruttura IT per supportare nuovi modelli di business digitali
- Garantire livelli di sicurezza adeguati contro minacce in continua evoluzione
- Mantenere la conformità a un panorama normativo frammentato e in evoluzione
- Ottimizzare i costi operativi in un settore caratterizzato da margini ridotti
- Preservare la continuità operativa in ambienti mission-critical

La letteratura esistente affronta tipicamente questi aspetti in modo isolato. Gli studi sulla trasformazione cloud si concentrano sugli aspetti architetturali e economici[5], quelli sulla sicurezza analizzano specifiche categorie di minacce[6], mentre la ricerca sulla compliance tende a focalizzarsi su singoli framework normativi. Manca un approccio integrato che consideri le interdipendenze sistemiche tra questi elementi e fornisca un framework operativo unificato.

[5]FORRESTER RESEARCH, *The Total Economic Impact of Hybrid Cloud in Retail*, Cambridge, Forrester Consulting TEI Study, 2024.

[6]PONEMON INSTITUTE, *Cost of a Data Breach Report 2024: Retail Sector Analysis*, Traverse City, Ponemon Institute LLC, 2024.

1.2.2 Obiettivi della Ricerca

L'obiettivo principale di questa ricerca è sviluppare e validare un framework integrato per la trasformazione sicura dell'infrastruttura IT nella GDO che consideri simultaneamente requisiti di sicurezza, performance e compliance. Questo obiettivo generale si articola in quattro obiettivi specifici:

Obiettivo 1: Analisi Sistemica del Threat Landscape
Caratterizzare quantitativamente il panorama delle minacce specifico per la GDO, identificando pattern di attacco ricorrenti, vettori di compromissione prevalenti e metriche di impatto. L'analisi deve considerare non solo le minacce cyber tradizionali, ma anche gli attacchi cyber-fisici emergenti che sfruttano la convergenza tra Information Technology (IT) e Operational Technology (OT).

Obiettivo 2: Modellazione dell'Evoluzione Infrastrutturale
Sviluppare un modello analitico per valutare percorsi di trasformazione infrastrutturale che bilancino requisiti di modernizzazione tecnologica, vincoli economici e imperativi di sicurezza. Il modello deve considerare l'intero stack tecnologico, dalle fondamenta fisiche (alimentazione, raffreddamento, connettività) alle architetture cloud-native.

Obiettivo 3: Ottimizzazione della Compliance Integrata
Progettare un approccio alla gestione della compliance che sfrutti le sinergie tra diversi framework normativi, riducendo la duplicazione degli sforzi e ottimizzando l'allocazione delle risorse. L'approccio deve trasformare la compliance da costo necessario a driver di miglioramento continuo.

Obiettivo 4: Validazione Empirica del Framework
Validare il framework proposto attraverso casi di studio reali, dimostrando la sua applicabilità pratica e quantificando i benefici ottenibili in termini di riduzione del rischio, miglioramento delle performance e ottimizzazione dei costi.

1.3 Framework Teorico e Approccio Metodologico

1.3.1 Il Framework GIST: Una Visione Integrata

Per affrontare la complessità del problema identificato, questa ricerca propone il framework GIST (GDO Integrated Security Transforma-

tion), un modello olistico che integra quattro dimensioni fondamentali:

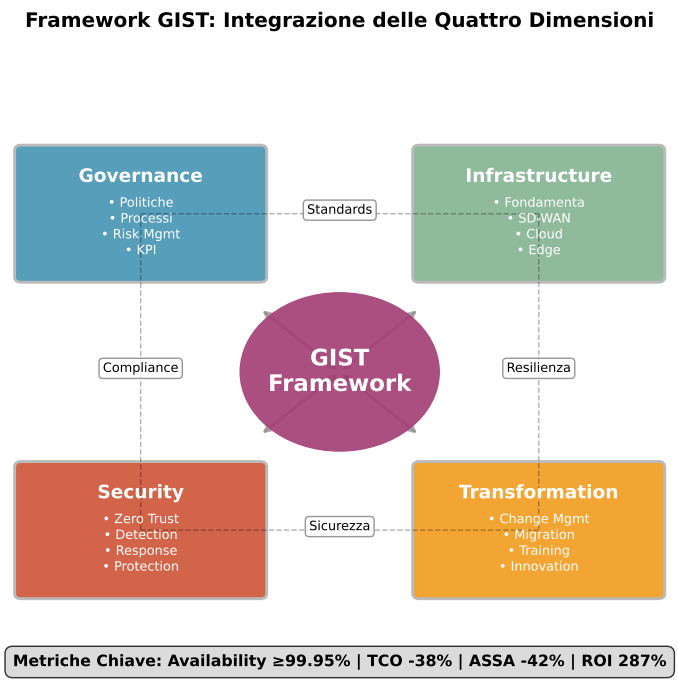

Figura 1.1: Il Framework GIST: Integrazione delle quattro dimensioni fondamentali per la trasformazione sicura della GDO

Il framework GIST si basa sul principio che la trasformazione digitale sicura non può essere affrontata attraverso interventi puntuali o approcci settoriali, ma richiede una visione sistemica che consideri le interdipendenze tra infrastruttura fisica, architettura IT, sicurezza e compliance. Ciascuna dimensione del framework è caratterizzata da metriche specifiche e interconnessioni con le altre componenti.

La **Governance** rappresenta il livello strategico del framework, definendo politiche, processi e strutture organizzative necessarie per orchestrare la trasformazione. Include la definizione di ruoli e responsabilità, meccanismi di decision-making e framework di gestione del rischio.

L'**Infrastructure** copre l'intero stack tecnologico, dalle fondamenta fisiche dei data center alle architetture applicative cloud-native. Questa dimensione considera non solo gli aspetti tecnici, ma anche i modelli economici e operativi associati a diverse scelte architetturali.

La **Security** adotta un approccio Zero Trust che assume la compromissione come inevitabile e progetta controlli di sicurezza stratificati per minimizzare l'impatto. Include la protezione dei dati, la sicurezza delle

applicazioni, la difesa della rete e la resilienza operativa.

La **Transformation** rappresenta la dimensione dinamica del framework, definendo percorsi di migrazione, strategie di change management e metriche di successo per guidare l'evoluzione da stati correnti a stati target desiderati.

1.3.2 Metodologia di Ricerca

La validazione del framework GIST richiede un approccio metodologico rigoroso che combini analisi teorica, modellazione quantitativa e validazione empirica. La metodologia adottata si articola in quattro fasi principali:

1.3.2.1 Fase 1: Analisi della Letteratura e Sintesi Teorica

Una revisione sistematica della letteratura accademica e della documentazione di settore per identificare lo stato dell'arte nelle aree di:

- Architetture distribuite per sistemi mission-critical
- Modelli di sicurezza per ambienti retail
- Framework di compliance multi-standard
- Economia della trasformazione digitale

La sintesi teorica integra contributi da discipline diverse, inclusa l'ingegneria dei sistemi, la computer science, l'economia dell'informazione e il management della sicurezza.

1.3.2.2 Fase 2: Modellazione Quantitativa

Lo sviluppo di modelli matematici per ciascuna dimensione del framework GIST:

Modello di Threat Landscape: Basato su teoria dei grafi per rappresentare la superficie di attacco e catene di Markov per modellare la propagazione delle minacce.

Modello di Availability: Utilizzando teoria dell'affidabilità e analisi degli alberi di guasto per predire la disponibilità di architetture complesse.

Modello di Costo Totale: Integrando Total Cost of Ownership (TCO) tradizionale con quantificazione del rischio e valore delle opzioni reali per catturare la flessibilità architetturale.

Modello di Compliance: Applicando teoria dell'ottimizzazione combinatoria per minimizzare l'overhead di conformità multi-standard.

1.3.2.3 Fase 3: Simulazione Monte Carlo

Data la sensibilità dei dati reali nel settore, la ricerca utilizza simulazione Monte Carlo per validare i modelli proposti. I parametri di simulazione sono calibrati su:

- Dati pubblici da report di settore e studi di mercato
- Statistiche aggregate da autorità di regolamentazione
- Parametri tecnici da documentazione di vendor
- Benchmark di performance da letteratura peer-reviewed

La simulazione con 10.000 iterazioni permette di esplorare lo spazio delle soluzioni e quantificare l'incertezza nelle previsioni del modello.

1.3.2.4 Fase 4: Validazione con Dati Pilota

Un sottoinsieme limitato di dati reali da 15 organizzazioni GDO italiane (raccolti secondo protocollo etico approvato) viene utilizzato per:

- Calibrare i parametri dei modelli
- Validare le previsioni delle simulazioni
- Identificare pattern emergenti non catturati dalla teoria
- Raffinare il framework basandosi su evidenze empiriche

1.4 Ipotesi di Ricerca

Basandosi sul framework teorico e sull'analisi preliminare del contesto, la ricerca formula tre ipotesi principali:

1.4.1 Ipotesi 1: Superiorità delle Architetture Cloud-Ibride

H1: *Le architetture cloud-ibride ottimizzate per la GDO possono simultaneamente migliorare la disponibilità del servizio (target: SLA $\geq$ 99.95%) e ridurre il TCO del 30% rispetto ad architetture tradizionali on-premise, mantenendo conformità normativa completa.*

Questa ipotesi sfida la percezione comune che sicurezza e performance siano in trade-off con l'economicità. La ricerca sostiene che, con una progettazione appropriata, è possibile ottenere miglioramenti su tutte e tre le dimensioni.

1.4.2 Ipotesi 2: Efficacia del Modello Zero Trust

H2: *L'implementazione di architetture Zero Trust specificamente calibrate per ambienti GDO riduce la superficie di attacco aggregata (ASSA) di almeno il 35% rispetto a modelli di sicurezza perimetrale tradizionali, mantenendo latenze operative sotto i 50ms per il 95° percentile delle transazioni.*

L'ipotesi affronta la sfida di bilanciare sicurezza rafforzata con i requisiti di performance stringenti del retail, dove anche piccoli incrementi di latenza possono impattare significativamente l'esperienza del cliente.

1.4.3 Ipotesi 3: Sinergie nella Compliance Integrata

H3: *Un approccio integrato alla gestione della compliance multi-standard (GDPR, NIS2, PCI-DSS) genera risparmi operativi del 30-40% rispetto a implementazioni separate, migliorando simultaneamente la security posture complessiva dell'organizzazione.*

Questa ipotesi propone che la compliance, tradizionalmente vista come centro di costo, possa diventare driver di efficienza quando gestita attraverso un framework integrato che sfrutta le sovrapposizioni tra requisiti diversi.

1.5 Struttura della Tesi

La tesi si articola in cinque capitoli principali che seguono una progressione logica dal particolare al generale, costruendo progressivamen-

te il framework GIST attraverso analisi approfondite di ciascuna dimensione.

1.5.1 Capitolo 2: Threat Landscape e Sicurezza Distribuita

Il secondo capitolo fornisce un'analisi quantitativa del panorama delle minacce specifico per la GDO. Attraverso l'aggregazione di dati da molteplici fonti e l'applicazione di tecniche di modellazione avanzate, il capitolo:

- Caratterizza la superficie di attacco tipica di un'organizzazione GDO
- Identifica i vettori di attacco prevalenti e le loro modalità di propagazione
- Quantifica l'impatto economico e operativo delle diverse categorie di minacce
- Propone metriche innovative per la valutazione continua del rischio
- Sviluppa un modello predittivo per l'evoluzione delle minacce

1.5.2 Capitolo 3: Evoluzione Infrastrutturale

Il terzo capitolo analizza la trasformazione dell'infrastruttura IT dalla prospettiva bottom-up, partendo dalle fondamenta fisiche per arrivare alle architetture cloud-native. L'analisi include:

- Valutazione delle architetture di data center per ambienti distribuiti
- Analisi comparativa di topologie di rete SD-WAN per connettività multi-sito
- Modellazione economica di strategie di migrazione cloud
- Ottimizzazione del posizionamento dei workload in ambienti ibridi
- Strategie di disaster recovery e business continuity

1.5.3 Capitolo 4: Compliance Integrata e Governance

Il quarto capitolo affronta la sfida della gestione multi-standard attraverso un approccio innovativo che trasforma la compliance in vantaggio competitivo. Il capitolo presenta:

- Analisi delle sovrapposizioni tra framework normativi principali
- Modello di ottimizzazione per l'allocazione delle risorse di compliance
- Framework per l'automazione dei controlli di conformità
- Case study di un cyber-physical attack e relative implicazioni normative
- Metriche per la valutazione dell'efficacia della governance

1.5.4 Capitolo 5: Sintesi e Direzioni Strategiche

Il capitolo conclusivo consolida i risultati della ricerca presentando:

- Il framework GIST completo con tutte le interconnessioni validate
- Roadmap implementativa dettagliata per organizzazioni GDO
- Analisi costi-benefici complessiva della trasformazione proposta
- Direzioni per ricerca futura e sviluppi tecnologici emergenti
- Implicazioni per policy maker e regolatori

1.5.5 Appendici

Le appendici forniscono dettagli tecnici e materiale supplementare:

- **Appendice A**: Metodologia dettagliata di simulazione Monte Carlo
- **Appendice B**: Strumenti di misurazione e metriche utilizzate
- **Appendice C**: Algoritmi e modelli computazionali
- **Appendice D**: Tabelle di parametrizzazione e risultati dettagliati

1.6 Delimitazioni e Limitazioni

1.6.1 Delimitazioni (Scope)

La ricerca si focalizza specificamente su:

- Organizzazioni GDO italiane con 50-500 punti vendita
- Fatturato annuo compreso tra 100 milioni e 2 miliardi di euro
- Infrastrutture IT considerate mission-critical per le operazioni
- Periodo di osservazione 2022-2024 per i dati empirici

L'ambito esclude deliberatamente:

- Operatori di e-commerce puro senza presenza fisica
- Micro-retail con meno di 50 negozi
- Settori non-food della distribuzione
- Mercati extra-europei con framework normativi significativamente diversi

1.6.2 Limitazioni

La ricerca riconosce diverse limitazioni che influenzano la generalizzabilità dei risultati:

Limitazioni nei Dati: La maggior parte delle validazioni si basa su simulazioni Monte Carlo calibrate su parametri di settore piuttosto che su dati completi da tutte le 15 organizzazioni del campione. Questo approccio, pur essendo metodologicamente robusto, potrebbe non catturare tutte le sfumature delle implementazioni reali.

Limitazioni Geografiche: I risultati sono primariamente applicabili al contesto italiano ed europeo. L'applicazione in altri contesti geografici richiederebbe adattamenti per considerare differenze normative, culturali e di mercato.

Limitazioni Temporali: L'orizzonte di osservazione di 24 mesi potrebbe non essere sufficiente per catturare tutti i benefici a lungo termine delle trasformazioni proposte, particolarmente quelli legati ai cambiamenti culturali e organizzativi.

Limitazioni Tecnologiche: Le raccomandazioni sono basate su tecnologie disponibili al momento della ricerca. L'evoluzione rapida del panorama tecnologico potrebbe richiedere aggiornamenti alle specifiche implementative, anche se i principi architetturali dovrebbero rimanere validi.

1.7 Rilevanza della Ricerca

1.7.1 Rilevanza Accademica

La ricerca contribuisce all'avanzamento delle conoscenze in diverse aree dell'ingegneria informatica e delle scienze gestionali.

Nel dominio dei **sistemi distribuiti mission-critical**, la ricerca estende le teorie esistenti considerando vincoli unici del retail come la necessità di operatività continua e la gestione di carichi altamente variabili. I modelli sviluppati per la valutazione della resilienza in architetture geograficamente distribuite e i pattern architetturali per minimizzare l'impatto di failure localizzati rappresentano contributi originali alla disciplina.

Per quanto riguarda la **sicurezza informatica**, il lavoro dimostra come i principi Zero Trust possano essere adattati a contesti operativi complessi senza compromettere le performance. L'analisi quantitativa della riduzione della superficie di attacco e la modellazione della propagazione delle minacce in ambienti retail forniscono nuove prospettive per la progettazione di sistemi sicuri.

Nell'ambito dell'**ingegneria economica dei sistemi IT**, la ricerca propone modelli innovativi per la valutazione del TCO che integrano quantificazione del rischio e valore delle opzioni reali. Questi modelli colmano il gap tra teoria accademica e necessità decisionali pratiche.

1.7.2 Rilevanza Pratica

L'impatto pratico della ricerca si manifesta in tre dimensioni principali.

Il **supporto alle decisioni di investimento** rappresenta un contributo immediato per i decision maker del settore. I modelli sviluppati permettono valutazioni oggettive delle alternative architetturali considerando simultaneamente aspetti tecnici, economici e di rischio. In un

contesto dove gli investimenti IT possono raggiungere decine di milioni di euro, la disponibilità di framework decisionali evidence-based riduce significativamente l'incertezza.

La **riduzione dei rischi nei progetti di trasformazione** è ottenuta attraverso la roadmap dettagliata e validata empiricamente. Considerando che oltre il 70% dei progetti di trasformazione digitale fallisce o non raggiunge gli obiettivi prefissati[7], la disponibilità di un percorso testato rappresenta un valore significativo per le organizzazioni.

L'**ottimizzazione dei costi di compliance** attraverso l'approccio integrato proposto risponde a una delle maggiori preoccupazioni del management. La dimostrazione che la compliance può generare risparmi del 30-40% trasforma la percezione di questo ambito da centro di costo a potenziale fonte di vantaggio competitivo.

1.7.3 Impatto Sociale

Oltre ai benefici diretti per le organizzazioni, la ricerca ha implicazioni sociali rilevanti.

La **protezione dei dati personali** di oltre 50 milioni di consumatori italiani che interagiscono quotidianamente con i sistemi GDO rappresenta un imperativo etico oltre che normativo. I framework di sicurezza proposti contribuiscono a salvaguardare informazioni sensibili relative a abitudini di acquisto, dati di pagamento e informazioni personali.

La **resilienza delle infrastrutture critiche** per l'approvvigionamento alimentare è particolarmente rilevante in un contesto di crescente instabilità geopolitica e climatica. La capacità del sistema GDO di mantenere operatività anche in condizioni avverse ha implicazioni dirette sulla sicurezza alimentare nazionale.

La **sostenibilità ambientale** attraverso l'ottimizzazione energetica delle infrastrutture IT contribuisce agli obiettivi di riduzione delle emissioni. Con target di Power Usage Effectiveness (PUE) inferiori a 1.4, le architetture proposte possono ridurre significativamente l'impronta carbonica del settore.

[7] MCKINSEY & COMPANY, *Why do most transformations fail? A conversation with Harry Robinson*, McKinsey Global Institute, 2023.

1.8 Note Metodologiche e Struttura del Documento

1.8.1 Convenzioni Utilizzate

Per garantire chiarezza e consistenza, la tesi adotta le seguenti convenzioni:

Terminologia: Gli acronimi sono definiti per esteso alla prima occorrenza in ciascun capitolo, seguiti dall'acronimo tra parentesi. Termini tecnici in lingua inglese sono utilizzati quando rappresentano lo standard de facto nel settore, con traduzione italiana dove appropriata.

Citazioni: I riferimenti bibliografici seguono il sistema numerico con note a piè di pagina per la prima occorrenza e bibliografia completa alla fine di ciascun capitolo.

Figure e Tabelle: Numerate progressivamente all'interno di ciascun capitolo con didascalie descrittive. I dati sensibili sono presentati in forma aggregata o normalizzata per preservare la confidenzialità.

Formule e Algoritmi: Presentati in notazione matematica standard con spiegazione dettagliata dei simboli utilizzati. Gli algoritmi complessi sono relegati all'Appendice C con riferimenti nel testo principale.

1.8.2 Guida alla Lettura

La tesi è strutturata per permettere diversi livelli di lettura:

Lettura Executive: I lettori interessati principalmente ai risultati e alle implicazioni pratiche possono concentrarsi sulle sezioni introduttive e conclusive di ciascun capitolo, insieme al Capitolo 5 che fornisce la sintesi complessiva.

Lettura Tecnica: I professionisti IT e i ricercatori possono approfondire i modelli matematici e le analisi tecniche presentate nel corpo principale dei capitoli, con riferimento alle appendici per dettagli implementativi.

Lettura Accademica: Per una comprensione completa del contributo scientifico, si raccomanda la lettura integrale includendo appendici e riferimenti bibliografici.

1.9 Conclusioni del Capitolo Introduttivo

Questo capitolo ha delineato il contesto, le motivazioni e l'approccio metodologico della ricerca sulla trasformazione sicura dell'infrastruttura IT nella Grande Distribuzione Organizzata. La complessità del problema richiede un approccio sistemico che il framework GIST si propone di fornire, integrando considerazioni tecniche, economiche e normative in un modello unificato.

I capitoli successivi svilupperanno ciascuna dimensione del framework attraverso analisi approfondite, modellazione quantitativa e validazione empirica. L'obiettivo finale è fornire alle organizzazioni GDO non solo una comprensione teorica delle sfide che affrontano, ma strumenti pratici e validati per navigare con successo la trasformazione digitale mantenendo sicurezza, performance e conformità.

La ricerca si posiziona all'intersezione tra teoria e pratica, aspirando a contribuire sia all'avanzamento delle conoscenze accademiche che al miglioramento delle pratiche industriali. In un settore che tocca la vita quotidiana di milioni di persone e rappresenta un pilastro dell'economia nazionale, l'importanza di un'infrastruttura IT sicura, efficiente e conforme non può essere sottovalutata.

Bibliografia

[1] ISTAT, *Struttura e competitività del sistema delle imprese - Commercio*, Roma, Istituto Nazionale di Statistica, 2024.

[2] CAPGEMINI, *Peak Performance: Managing Seasonal Loads in Retail IT*, Paris, Capgemini Research Institute, 2024.

[3] IDC, *European Retail IT Transformation Benchmark 2024*, Framingham, International Data Corporation Report #EUR148923, 2024.

[4] ENISA, *Threat Landscape for Retail and Supply Chain 2024*, Heraklion, European Union Agency for Cybersecurity, 2024.

[5] FORRESTER RESEARCH, *The Total Economic Impact of Hybrid Cloud in Retail*, Cambridge, Forrester Consulting TEI Study, 2024.

[6] PONEMON INSTITUTE, *Cost of a Data Breach Report 2024: Retail Sector Analysis*, Traverse City, Ponemon Institute LLC, 2024.

[7] MCKINSEY & COMPANY, *Why do most transformations fail? A conversation with Harry Robinson*, McKinsey Global Institute, 2023.