

# Indice Ufficiale della Tesi

---

## "Dall'Alimentazione alla Cybersecurity: Fondamenti di un'Infrastruttura IT Sicura nel Contesto della Grande Distribuzione"

---

### 1. Introduzione (8-10 pagine)

- **Contesto e sfide specifiche della GDO:** Operatività H24, architetture distribuite, volumi transazionali, dati sensibili.
- **Framework di analisi:** Criteri di valutazione (sicurezza, scalabilità, compliance, TCO, resilienza).
- **Obiettivo:** Analisi critica dell'evoluzione da infrastrutture tradizionali a modelli cloud-ibridi nella GDO, con focus su sicurezza e compliance.
- **Struttura della tesi:** Roadmap dal fisico al digitale.

### 2. Threat Landscape e Sicurezza Distribuita nella GDO (18-20 pagine)

- **Minacce specifiche alla GDO:**
  - Attacchi ai sistemi POS e di pagamento.
  - Compromissione di architetture distribuite (sede centrale ↔ punti vendita).
  - Minacce cloud-native: misconfigurazioni, lateral movement.
- **Architetture di sicurezza per ambienti distribuiti:**
  - Segmentazione avanzata: micro-segmentazione e Zero Trust principles.
  - Protezione endpoint in contesti retail (POS, IoT, mobile).
  - SIEM e SOC per monitoring centralizzato multi-sito.
- **Focus: Secure by Design per la GDO.**

### 3. Evoluzione Infrastrutturale: Da Data Center a Cloud-First (20-22 pagine)

- **Infrastruttura fisica critica:**
  - Alimentazione ridondante e continuità operativa nei punti vendita.
  - Cooling e vincoli ambientali in retail environments.
- **Architetture di rete moderne:**
  - SD-WAN per collegamenti sede-filiali.
  - Edge computing: elaborazione locale vs centralizzata.
  - Connectivity patterns per architetture ibride.
- **Cloud adoption nella GDO:**
  - Migration patterns: lift-and-shift vs cloud-native.
  - Multi-cloud strategy per disaster recovery geografico.
  - Performance optimization: latenza critica per POS e inventory management.

### 4. Compliance Integrata e Governance (20-22 pagine)

- **Regulatory landscape per la GDO:**
  - **PCI-DSS:** Implementazione in architetture distribuite e cloud.
  - **Direttiva NIS2:** Supply chain security e incident management.
  - **GDPR:** Data governance in ambienti ibridi.

- **Governance frameworks:**
  - Risk management per infrastrutture critiche.
  - Business Continuity Planning: on-premise, cloud, hybrid scenarios.
  - Vendor management e supply chain security.
- **Caso di Studio: Cyber-Physical Attack:**
  - Scenario: compromissione sistemi di refrigerazione via IoT.
  - Impact analysis: operational, financial, reputational.
  - Response and mitigation strategies.

## 5. Sintesi e Direzioni Strategiche (8-10 pagine)

- **Best practices identificate:** Framework integrato per la sicurezza GDO.
  - **Trade-off analysis:** Sicurezza vs performance, controllo vs flessibilità, costi vs resilienza.
  - **Strategic roadmap:** AI-powered security, sustainable IT, supply chain resilience.
- 

## Riferimenti Essenziali

- **Standards:** ISO 27001, PCI-DSS v4.0, NIST Cybersecurity Framework
  - **Regulatory:** GDPR, NIS2 Directive, ENISA Guidelines
  - **Industry:** Retail industry reports (Gartner, Forrester), CSP security documentation
  - **Academic:** IEEE, ACM proceedings su retail cybersecurity
- 

**Target:** 75-80 pagine | **Approccio:** Analisi critica e best practices | **Focus:** 3 pilastri strategici