
Università degli Studi di Milano
Facoltà di Scienze e Tecnologie
*Corso di Laurea in Sicurezza dei Sistemi e delle Reti Informatiche*

# SICUREZZA DELL'INFRASTRUTTURA AWS IN UNA STARTUP FINTECH

**Relatore:** Prof. Claudio Agostino Ardagna

**Correlatore:** Lorenzo Perotta, Andrea Pasini, Simone Cortese

Tesi di:
Andrea Ferraboli
Matricola: 09985A

Anno Accademico 2024-2025

*dedicato a chi mi vuole bene, a chi mi stima e ai miei compagni di viaggio, vi voglio bene*

# Indice

# Capitolo 1

# Introduzione

## La Cybersecurity nelle Startup Fintech: Sfide, Vulnerabilità e Strategie di Protezione in un Ecosistema in Rapida Evoluzione

Il settore fintech rappresenta oggi una delle aree più dinamiche e innovative dell'ecosistema startup, con investimenti globali che hanno raggiunto i 115 miliardi di dollari, in crescita esponenziale rispetto ai 53.2 miliardi del 2018 [1]. Questo rapido sviluppo, caratterizzato dall'implementazione di tecnologie emergenti per i servizi finanziari, porta con sé non solo opportunità senza precedenti ma anche significative sfide in termini di sicurezza informatica. Le startup fintech, che si trovano all'intersezione tra finanza tradizionale e innovazione tecnologica, gestiscono dati estremamente sensibili diventando bersagli privilegiati per i cybercriminali. Questa tesi esplora le vulnerabilità specifiche di queste realtà, analizza le principali minacce che affrontano e propone strategie di sicurezza efficaci anche in contesti di risorse limitate, evidenziando come un approccio proattivo alla cybersecurity non rappresenti un costo ma un investimento strategico fondamentale per il successo a lungo termine di una startup fintech.

### Il Contesto delle Startup Fintech: Un Ecosistema Dinamico e Sfidante

Le startup fintech operano in un ambiente caratterizzato da elevata incertezza, risorse limitate e necessità di crescita rapida, fattori che influenzano profondamente le decisioni in ambito IT e sicurezza informatica [2]. A differenza delle istituzioni finanziarie tradizionali, queste realtà innovative non dispongono generalmente di strutture gerarchiche complesse o budget consistenti dedicati alla sicurezza, dovendo

invece adottare approcci agili e flessibili. Secondo Gartner, un'impresa per essere considerata fintech deve possedere quattro caratteristiche fondamentali: utilizzare la tecnologia come veicolo, generare la maggior parte dei ricavi dal settore dei servizi finanziari, differenziarsi attraverso l'innovazione dirompente e adottare un modello di business orientato alla trasformazione digitale [1].

Il contesto finanziario in cui operano le startup fintech impone pressioni significative sulle decisioni di spesa. Ogni investimento, compreso quello per l'infrastruttura IT e la sicurezza, deve essere attentamente valutato in termini di ritorno immediato e benefici a lungo termine [2]. Questa ottimizzazione dei costi rappresenta una sfida continua, poiché la sicurezza informatica richiede investimenti costanti che spesso non producono risultati immediatamente visibili, ma la cui assenza può comportare conseguenze catastrofiche. In questo equilibrio delicato, le startup fintech devono trovare il giusto compromesso tra la necessità di scalare rapidamente e l'implementazione di solide misure di protezione.

La cultura del lavoro nelle startup fintech è caratterizzata da ritmi serrati e team multifunzionali in cui le competenze sono trasversali e i confini tra ruoli spesso sfumati [2]. Questa agilità, se da un lato rappresenta un vantaggio competitivo, dall'altro può tradursi in vulnerabilità quando le competenze in materia di sicurezza non sono adeguatamente distribuite o considerate prioritarie. La pressione per la velocità di sviluppo e il rapido accesso al mercato può portare a trascurare aspetti fondamentali della sicurezza, creando quello che in gergo tecnico viene definito "security debt" – un debito tecnico in ambito sicurezza che, come un mutuo a tassi elevati, diventa sempre più oneroso da ripagare con il passare del tempo.

### La Distinzione tra Cybersecurity Bancaria e Fintech

Un aspetto fondamentale da considerare è la sostanziale differenza tra l'approccio alla cybersecurity nel settore bancario tradizionale e nelle startup fintech. Mentre le banche operano in un contesto fortemente regolamentato, con obblighi legali precisi in materia di sicurezza e protezione dei dati, le fintech hanno tradizionalmente goduto di una maggiore flessibilità normativa [3]. Le grandi istituzioni bancarie investono ingenti risorse nel testare costantemente le proprie misure di sicurezza, consapevoli che anche il minimo incidente può comportare la perdita di migliaia di clienti e sanzioni finanziarie significative.

Le fintech, spesso costituite da piccole startup in rapida espansione, possono fungere da "overlay" per le banche, facilitando la fornitura di servizi finanziari innovativi ma operando inizialmente con regolamentazioni meno stringenti [3]. Questa differenza normativa sta tuttavia diminuendo, soprattutto per quelle fintech che si trasformano gradualmente in vere e proprie banche, sottoponendosi così a un maggiore scrutinio

regolamentare. La sfida per le startup fintech consiste quindi nel bilanciare l'agilità operativa con l'adozione di standard di sicurezza elevati, anticipando l'evoluzione normativa del settore.

## Sfide Principali per le Startup Fintech in Ambito Cybersecurity

Le startup fintech affrontano sfide specifiche nel campo della sicurezza informatica, che derivano dalla loro natura innovativa e dalle caratteristiche distintive del loro modello di business [2]. La prima e più evidente sfida è rappresentata dal budget limitato per la sicurezza, che spesso costringe a difficili compromessi tra lo sviluppo di nuove funzionalità e l'implementazione di adeguate misure protettive. Questa limitazione finanziaria si riflette anche nella difficoltà di attrarre e mantenere personale specializzato in cybersecurity, un ambito in cui la domanda supera ampiamente l'offerta e le grandi aziende possono offrire compensi difficilmente pareggiabili da una startup.

La pressione per un rapido accesso al mercato rappresenta un'ulteriore sfida significativa. Nel settore fintech, essere i primi a offrire un servizio innovativo può fare la differenza tra il successo e il fallimento, ma questa corsa contro il tempo spesso porta a sottovalutare gli aspetti legati alla sicurezza [2]. Inoltre, la scalabilità dell'infrastruttura IT rappresenta una sfida tecnica considerevole: progettare sistemi che siano non solo sicuri ma anche in grado di crescere rapidamente al crescere dell'azienda richiede competenze specifiche e una pianificazione accurata.

L'adozione di tecnologie emergenti, caratteristica distintiva delle fintech, introduce nuove superfici di attacco e vulnerabilità potenziali [2]. Cloud computing, intelligenza artificiale, blockchain e API aperte offrono opportunità straordinarie ma richiedono approcci di sicurezza specifici e aggiornati. Allo stesso tempo, la crescente interconnessione con partner, fornitori e piattaforme di terze parti amplia ulteriormente la superficie di attacco, rendendo la gestione del rischio ancora più complessa.

Non va sottovalutato, infine, il rischio rappresentato dalle minacce interne (insider threats). Nelle fasi iniziali di una startup, quando i controlli sono meno rigidi e le procedure di sicurezza meno formalizzate, il rischio legato a dipendenti negligenti o, in casi più rari, malintenzionati, aumenta considerevolmente [2]. La cultura della condivisione e dell'apertura, tipica delle startup, deve quindi essere bilanciata con adeguate politiche di accesso e controllo.

## Minacce e Attacchi Informatici nel Settore Fintech

Il settore fintech, per la sua natura altamente tecnologica e la gestione di dati finanziari sensibili, è diventato uno dei bersagli preferiti dei cybercriminali [4]. Tra le minacce più diffuse e pericolose figurano gli attacchi di phishing, attraverso i quali

i malintenzionati cercano di ottenere credenziali di accesso, dati personali o informazioni finanziarie utilizzando email, messaggi e siti web fraudolenti che imitano comunicazioni ufficiali [4]. Queste tecniche di social engineering sfruttano la fiducia degli utenti e le loro abitudini digitali per compromettere account e sistemi aziendali.

I malware e i ransomware rappresentano un'altra categoria di minacce particolarmente grave per le startup fintech. Questi software malevoli possono infiltrarsi nei sistemi attraverso vari vettori, bloccare l'accesso ai dati e richiedere un riscatto per ripristinarlo, causando danni finanziari diretti e interruzioni operative significative [4]. Le conseguenze di un attacco ransomware possono essere devastanti per una startup con risorse limitate, sia in termini economici che reputazionali.

Gli attacchi alle API (Application Programming Interfaces), sempre più utilizzate nel settore fintech per l'integrazione con servizi terzi, costituiscono un vettore di attacco in crescita [2]. Le API mal configurate o non adeguatamente protette possono diventare punti di ingresso privilegiati per i cybercriminali, consentendo l'accesso non autorizzato a dati sensibili e funzionalità critiche del sistema. Simile criticità presentano le configurazioni errate dei servizi cloud, che possono esporre involontariamente dati riservati o creare vulnerabilità sfruttabili.

Le startup fintech devono inoltre considerare il rischio di attacchi DDoS (Distributed Denial of Service), che mirano a rendere inaccessibili i servizi sovraccaricando i server con richieste fraudolente [2]. Questi attacchi, relativamente semplici da orchestrare ma potenzialmente molto dannosi, possono essere utilizzati sia come attacco diretto che come diversivo per mascherare altre attività malevoli più sofisticate.

### Conseguenze degli Attacchi e Impatto sulle Startup Fintech

L'impatto di un attacco informatico su una startup fintech può essere multidimensionale e, in molti casi, esistenziale. A livello finanziario, oltre ai costi diretti per il ripristino dei sistemi e la gestione dell'incidente, vanno considerati i potenziali risarcimenti a clienti danneggiati, le sanzioni normative e l'aumento dei premi assicurativi [2]. Ma è forse l'impatto reputazionale a rappresentare la minaccia più grave: in un settore basato sulla fiducia come quello finanziario, una violazione dei dati può comprometterne irreparabilmente l'immagine, portando alla perdita di clienti attuali e potenziali.

L'interruzione operativa conseguente a un attacco può avere effetti a catena, influenzando non solo i clienti diretti ma anche partner commerciali e fornitori [2]. In un ecosistema interconnesso come quello fintech, l'interdipendenza tra diverse piattaforme e servizi amplifica ulteriormente l'impatto di un incidente di sicurezza, con effetti che possono estendersi ben oltre il perimetro aziendale immediato.

## Problemi Comuni e Cause Principali degli Attacchi

Analizzando gli attacchi informatici che colpiscono le startup fintech, emergono alcuni problemi ricorrenti che ne costituiscono le cause principali [2]. Spesso non si tratta di attacchi particolarmente sofisticati, ma dello sfruttamento di vulnerabilità note o di errori di configurazione basilari. La mancanza di controlli di sicurezza fondamentali, come firewall correttamente configurati, politiche di password robuste e autenticazione a due fattori, rappresenta una delle criticità più diffuse.

Gli errori di configurazione nei servizi cloud, come storage S3 esposti pubblicamente o API non adeguatamente protette, costituiscono un'altra fonte significativa di vulnerabilità [2]. La rapida adozione di servizi cloud da parte delle startup fintech, spesso senza le necessarie competenze interne o senza una valutazione approfondita delle implicazioni di sicurezza, aumenta considerevolmente il rischio di esposizione di dati sensibili.

Le vulnerabilità nel codice applicativo rappresentano un altro punto di debolezza comune. Problematiche come SQL injection, cross-site scripting e altre vulnerabilità OWASP Top 10 possono persistere nel codice quando i processi di sviluppo non includono adeguate pratiche di secure coding e test di sicurezza [2]. In un contesto di sviluppo rapido, tipico delle startup, la pressione per rilasciare nuove funzionalità può portare a trascurare questi aspetti fondamentali.

La mancanza di monitoraggio continuo e di logging efficace rappresenta un ulteriore problema critico. Senza adeguati sistemi di rilevamento e risposta, gli attacchi possono rimanere non rilevati per lunghi periodi, aumentando significativamente i danni potenziali [2]. L'assenza di processi strutturati per la gestione degli incidenti può inoltre rallentare la risposta quando un attacco viene effettivamente rilevato, esponendo l'organizzazione a rischi maggiori.

Infine, l'affidamento eccessivo a consulenti tecnici non adeguatamente verificati o a personale IT con limitata esperienza in sicurezza informatica può introdurre vulnerabilità significative nei sistemi [2]. La scelta di partner tecnologici e risorse umane deve quindi includere una valutazione attenta delle competenze specifiche in materia di cybersecurity.

## Importanza di un Approccio Proattivo alla Cybersecurity

Implementare una solida strategia di cybersecurity fin dalle prime fasi di sviluppo di una startup fintech non rappresenta un costo ma un investimento strategico fondamentale [2]. L'approccio "security by design" consente di integrare la sicurezza nei processi aziendali e nello sviluppo del prodotto, riducendo significativamente i costi a lungo termine e minimizzando i rischi. Trascurare la sicurezza nelle fasi iniziali,

infatti, porta all'accumulo di quello che viene definito "security debt", un debito tecnico in ambito sicurezza che diventa sempre più oneroso da ripagare con il passare del tempo.

Un approccio preventivo alla sicurezza risulta sempre più efficace ed economico rispetto a uno reattivo [2]. I costi per implementare misure di sicurezza di base sono generalmente inferiori rispetto a quelli necessari per rispondere a un incidente, che possono includere non solo il ripristino dei sistemi ma anche sanzioni, risarcimenti e danni reputazionali. La cybersecurity deve quindi essere considerata come parte integrante della strategia aziendale, non come un elemento accessorio o un costo da minimizzare.

Le startup fintech devono inoltre considerare che adeguati livelli di sicurezza rappresentano spesso un requisito fondamentale per attrarre investitori e partner commerciali [2]. Durante le fasi di due diligence, l'analisi delle misure di sicurezza implementate è diventata una componente standard, e lacune significative in questo ambito possono compromettere opportunità di finanziamento o collaborazioni strategiche.

## Approccio Metodologico della Tesi

Questa tesi si propone di affrontare le sfide della cybersecurity nelle startup fintech attraverso un approccio metodologico strutturato ma flessibile [2]. Pur concentrandosi su un caso studio pratico specifico, l'obiettivo è fornire principi e best practice di sicurezza generici e applicabili a qualsiasi startup fintech, indipendentemente dalla piattaforma tecnologica specifica utilizzata. L'approccio adottato riconosce le limitazioni di risorse tipiche delle startup e propone soluzioni scalabili che possono evolvere con la crescita dell'organizzazione.

La metodologia si basa su tre pilastri fondamentali: l'identificazione delle minacce specifiche per il modello di business fintech, la prioritizzazione degli interventi in base al rapporto rischio/beneficio e l'implementazione di controlli di sicurezza essenziali ma efficaci [2]. Questo approccio pragmatico consente di ottenere un livello di protezione adeguato anche con risorse limitate, concentrando gli sforzi sugli aspetti più critici.

La tesi analizzerà inoltre come integrare la cybersecurity nel ciclo di vita dello sviluppo software, un aspetto particolarmente rilevante per le startup fintech che spesso si differenziano attraverso piattaforme tecnologiche proprietarie [2]. L'adozione di metodologie DevSecOps, che integrano la sicurezza nei processi di sviluppo e operations, rappresenta infatti una delle strategie più efficaci per bilanciare velocità di innovazione e robustezza della sicurezza.

## Conclusione

La cybersecurity rappresenta una sfida fondamentale per le startup fintech, che devono bilanciare innovazione, crescita rapida e protezione di dati altamente sensibili. In un contesto caratterizzato da risorse limitate e pressione competitiva, l'adozione di un approccio strategico alla sicurezza informatica diventa un fattore critico di successo, non solo per proteggere l'azienda da minacce immediate ma anche per costruire basi solide per una crescita sostenibile.

Attraverso l'analisi delle specifiche vulnerabilità del settore fintech, la comprensione delle minacce più rilevanti e l'implementazione di strategie di sicurezza appropriate, le startup possono trasformare la cybersecurity da potenziale ostacolo a vantaggio competitivo [2], [3]. Questa tesi si propone di fornire una guida pratica e accessibile per raggiungere questo obiettivo, dimostrando come sia possibile costruire un'infrastruttura IT sicura ed efficiente anche con risorse limitate, adottando un approccio incentrato sul rischio e sulla protezione degli asset più critici.

La cybersecurity nelle startup fintech non è solo una questione tecnica ma un elemento strategico che influenza la fiducia dei clienti, le relazioni con i partner, la conformità normativa e, in ultima analisi, la sostenibilità del business stesso [4]. Investire nella sicurezza fin dalle prime fasi di sviluppo rappresenta quindi una scelta non solo prudente ma strategicamente vantaggiosa, che può fare la differenza tra il successo e il fallimento in un mercato sempre più competitivo e attento agli aspetti di protezione dei dati.

# Capitolo 2

# Principi di Sicurezza in un'infrastruttura Cloud

Nel settore fintech, la cybersecurity è una pietra angolare fondamentale per proteggere i dati sensibili e mantenere la fiducia degli utenti [5]. Le startup fintech operano in un contesto altamente digitale – con pagamenti elettronici, mobile banking, criptovalute e API aperte – che offre efficienze senza precedenti ma introduce anche rischi significativi [5]. Tra le minacce più comuni vi sono violazioni di dati finanziari, furti di identità, frodi sulle transazioni e attacchi informatici mirati ai sistemi di pagamento [5]. A differenza delle banche tradizionali, le fintech nascono spesso con minori vincoli normativi iniziali e un time-to-market aggressivo; ciò porta talvolta a trascurare gli aspetti di sicurezza nelle prime fasi di sviluppo [5]. Release frequenti e rapide possono indurre queste aziende a **omettere o posticipare misure di sicurezza** non ritenute immediatamente essenziali al business [5]. Ne risulta che molte soluzioni fintech, sebbene innovative, possono presentare controlli di sicurezza parziali o deboli, aumentando la probabilità di violazioni rispetto a istituzioni finanziarie più regolamentate.

Oltre alle minacce tecniche, le fintech affrontano rigorose sfide di **compliance normativa**. Se operano in ambito pagamenti, devono soddisfare standard come il **PCI DSS** (Payment Card Industry Data Security Standard) per la protezione dei dati delle carte, nonché normative sulla protezione dei dati personali come il **GDPR**. Studi di settore mostrano come molte fintech siano ancora in ritardo su questi fronti: ad esempio, il 62% dei siti web principali di aziende fintech esaminati non era conforme agli standard PCI DSS e il 64% non rispettava i requisiti GDPR [6]. Allo stesso tempo, regolamentazioni finanziarie come la PSD2 (Payment Services Directive 2) impongono requisiti di sicurezza (es. autenticazione forte del cliente) e le fintech che offrono servizi analoghi a quelli bancari possono trovarsi sottoposte a verifiche di **sicurezza informatica e continuità operativa** tipiche del settore finanziario

tradizionale.

In questo contesto complesso, diventa cruciale adottare **principi di cybersecurity strutturati** e basati su framework riconosciuti a livello internazionale. Questi framework forniscono un approccio sistematico per identificare i rischi, implementare controlli adeguati e garantire la resilienza dei sistemi. Nel seguito del capitolo verranno analizzati i principali framework e standard di sicurezza informatica – dal **NIST Cybersecurity Framework** all'ISO/IEC 27001, da linee guida NIST specifiche (SP 800-53, SP 800-82 per l'OT e SP 800-63B per le password) ai modelli di **Zero Trust** – illustrando come possano essere applicati nella pratica alla protezione dell'infrastruttura cloud di una startup fintech, con particolare riferimento ai server e ai dati ospitati su **Amazon Web Services (AWS)**. Verranno inoltre discusse **best practice e strategie di mitigazione** delle minacce più comuni, considerando le peculiarità degli ambienti cloud-native come AWS e l'importanza di un approccio di "difesa in profondità" integrato con i requisiti normativi di settore.

Prima di addentrarci nei framework, è fondamentale richiamare il modello di responsabilità condivisa nel cloud: **AWS è responsabile della sicurezza "of the cloud"**, ovvero della protezione dell'infrastruttura fisica e dei servizi di base (data center, hardware, rete, virtualizzazione), mentre **al cliente spetta la sicurezza "in the cloud"**, cioè la configurazione sicura dei propri ambienti virtuali, la gestione di accessi, rete, dati e applicazioni [7]. In altri termini, una fintech su AWS deve comunque implementare adeguati controlli di rete, cifratura, identity management, monitoring e così via, costruendo su un foundation sicuro fornito dal cloud provider ma senza delegare totalmente la responsabilità. Tenendo presente questo principio, esaminiamo ora i framework di sicurezza e come essi guidano l'implementazione di misure difensive su AWS.

## 2.1 NIST Cybersecurity Framework (CSF)

Il **NIST Cybersecurity Framework (CSF)**, sviluppato dal National Institute of Standards and Technology statunitense, è un framework di riferimento ampiamente adottato a livello globale come base per la gestione del rischio cyber in organizzazioni di qualsiasi settore o dimensione [8]. Nato per proteggere le infrastrutture critiche, il CSF è strutturato in cinque funzioni fondamentali – **Identify, Protect, Detect, Respond, Recover** – che rappresentano il ciclo continuo di gestione della sicurezza. Recentemente, con la versione 2.0 del 2024, è stata aggiunta una sesta funzione **"Govern"**, a sottolineare l'importanza delle attività organizzative e di governance nella gestione del rischio cyber [9]. Ciascuna funzione si articola in categorie e sottocategorie di controlli di sicurezza, fornendo così una tassonomia delle capacità di cybersecurity che un'azienda dovrebbe sviluppare. Ad esempio, il CSF include categorie che coprono l'identificazione degli asset critici, la protezione tramite controlli

di accesso e cifratura, il monitoraggio continuo degli eventi di sicurezza, la gestione degli incidenti e la resilienza operativa post-attacco.

Per una fintech che opera su AWS, il NIST CSF fornisce una **mappa concettuale** per implementare misure di sicurezza cloud in modo coerente e completo. AWS stessa riconosce il CSF come framework di riferimento e mette a disposizione linee guida su come allineare i servizi AWS alle diverse funzioni del CSF [9]. In pratica:

### 2.1.1 Identify (Identifica)

riguarda l'inventario e la classificazione di risorse, dati, software e flussi critici. Su AWS ciò implica mappare tutti i servizi in uso (istanze EC2, database RDS, bucket S3, ecc.), identificare i dati sensibili (es. dati finanziari dei clienti) e valutarne l'impatto in caso di compromissione. Strumenti come AWS Config e AWS Resource Explorer aiutano a mantenere la visibilità sugli asset cloud. È importante anche identificare le dipendenze da terze parti (ad es. API bancarie, servizi di pagamento) e i rischi di supply chain, in linea con l'enfasi posta dal CSF 2.0 sulla sicurezza della catena di fornitura [9].

### 2.1.2 Protect (Proteggi)

comprende tutte le misure volte a salvaguardare servizi e dati. In un'infrastruttura AWS, ciò include la **protezione della rete cloud** tramite VPC ben progettati e segmentati (suddividendo ambienti di produzione, staging, test in subnet isolate), l'uso di **security group** e **ACL di rete** per filtrare il traffico, e l'adozione di firewall applicativi e servizi come AWS WAF per difendersi da attacchi web. Possono essere integrate soluzioni di terze parti per rafforzare il perimetro, come vedremo con Check Point Quantum. La funzione Protect copre anche la **sicurezza dei dati**: su AWS è fondamentale cifrare i dati sia **a riposo** (es. tramite AWS KMS per chiavi di cifratura gestite e abilitando la crittografia su EBS, S3, RDS, etc.) sia **in transito** (usando protocolli TLS per API ed endpoint, e VPN/IPSec per connessioni private). Il controllo degli accessi ai dati va implementato con rigidi permessi IAM e politiche di bucket S3 che limitino l'accesso solo ai ruoli o servizi autorizzati. Un altro aspetto chiave è la **gestione delle identità e degli accessi (IAM)**: il CSF prescrive di implementare il principio del minimo privilegio e misure di robusta autenticazione. AWS IAM consente di definire ruoli e policy granulari, abilitare l'MFA sugli account (compreso l'account root) e centralizzare la gestione identitaria (ad esempio integrando provider SAML/SSO per gli utenti). L'uso di IAM Roles con credenziali temporanee per servizi e applicazioni riduce il rischio di credenziali statiche esposte. Queste misure rispecchiano i **principi Zero Trust** di non fidarsi mai implicitamente di un'entità e di verificare ogni richiesta (vedi sezione 2.4). Infine, Protect include la **protezione**

**dei sistemi e delle applicazioni**: ciò si traduce in hardening delle istanze (patching sistematico di sistemi operativi e middleware, disabilitazione di servizi inutili), utilizzo di servizi gestiti AWS (es. RDS, Lambda) che sollevano dall'onere di gestire direttamente server e riducono la superficie d'attacco, e impostazione di backup regolari e meccanismi di disaster recovery (snapshots, replicazione tra region, etc.) per garantire resilienza (quest'ultimo aspetto sconfina con la funzione Recover).

### 2.1.3 Detect (Individua)

il framework enfatizza la capacità di rilevare tempestivamente eventi anomali e possibili incidenti. Su AWS, **logging e monitoring** sono fondamentali. Ogni risorsa cloud dovrebbe generare log appropriati: AWS CloudTrail per tracciare tutte le chiamate API e attività nell'account, AWS CloudWatch per metriche di sistema e applicative con allarmi in caso di valori fuori soglia, AWS Config per cambiamenti di configurazione. Servizi avanzati come Amazon GuardDuty forniscono un monitoraggio continuo delle minacce analizzando pattern di traffico e log (identificando ad esempio comportamenti anomali indicativi di credenziali compromesse o istanze malevoli). Analogamente, Amazon Macie può rilevare eventuali esposizioni di dati sensibili su S3. L'aggregazione centralizzata dei log (magari in un servizio come Amazon S3 o CloudWatch Logs) e la loro correlazione tramite un SIEM (AWS offre AWS Security Hub per correlare avvisi da vari servizi) consente di **abilitare alerting in tempo reale** verso il team di sicurezza. Queste capacità rispondono all'esigenza di *traceability*: ogni azione o modifica nell'ambiente cloud deve essere tracciata e monitorata [10].

### 2.1.4 Respond (Rispondi)

definisce le attività di **gestione degli incidenti** nel momento in cui si verifica un problema di sicurezza. Una startup fintech dovrebbe avere un piano di incident response anche se piccola: procedure per analizzare gli eventi, contenere l'incidente (ad esempio isolando istanze compromesse, ruotando chiavi/API key esposte), eliminare la minaccia e ripristinare i servizi. AWS mette a disposizione strumenti che aiutano nella risposta: ad esempio, AWS CloudTrail facilita le indagini forensi permettendo di ricostruire le azioni compiute da un aggressore nell'account; servizi come AWS IAM Access Analyzer possono essere usati per verificare e chiudere eventuali accessi non intenzionali; AWS Systems Manager Incident Manager aiuta a orchestrare la risoluzione coordinando notifiche e runbook automatici. È buona prassi effettuare simulazioni di incidenti e game-day per allenare il team a rispondere efficacemente, come raccomandato anche dal Well-Architected Framework [10]. Inoltre, bisogna considerare gli

adempimenti di notifica: in caso di violazione di dati personali, ad esempio, il GDPR impone la comunicazione al Garante entro 72 ore, quindi il processo di incident response deve includere escalation manageriali e legali.

### 2.1.5 Recover (Recupera)

riguarda la **resilienza operativa** e la capacità di ripristinare rapidamente i servizi dopo un incidente o un guasto, minimizzando l'impatto sugli utenti e sui partner. In AWS, questo significa disporre di backup offline e piani di **disaster recovery** testati. Una fintech potrebbe mantenere backup crittografati dei database finanziari (ad esempio usando AWS Backup per centralizzare e automatizzare i backup di RDS, EBS, DynamoDB, etc.) e predisporre infrastrutture di ripristino in una regione secondaria per far fronte a eventi catastrofici sulla regione primaria. Servizi come Amazon S3 garantiscono durabilità elevatissima per i dati (11 9's) e possono versionare gli oggetti in modo da recuperare dati alterati o cancellati per errore. Il recover include anche comunicazioni post-incidente e miglioramento continuo: dopo il ripristino è importante condurre un post-mortem, capire le lezioni apprese e aggiornare i controlli di sicurezza per prevenire il ripetersi dell'incidente [9].

## 2.2 ISO/IEC 27001 e Sistemi di Gestione della Sicurezza (ISMS)

L'**ISO/IEC 27001** è lo standard internazionale di riferimento per stabilire, implementare e mantenere un *Information Security Management System* (**ISMS**), ovvero un sistema di gestione della sicurezza delle informazioni a 360 gradi. Si tratta di un framework gestionale che adotta un approccio basato sul rischio per garantire **riservatezza, integrità e disponibilità** delle informazioni aziendali attraverso un insieme di controlli di sicurezza organizzativi, fisici e tecnici. ISO 27001 è riconosciuto globalmente ed è applicato da organizzazioni in tutti i settori come **benchmark** di best practice per la sicurezza [11].

Cuore della norma è il ciclo PDCA (Plan-Do-Check-Act) applicato alla sicurezza: l'azienda deve condurre una valutazione dei rischi (identificando asset informativi, minacce, vulnerabilità e impatti), quindi adottare controlli adeguati (selezionati da una lista di riferimento nell'Annex A dello standard, che contiene 93 controlli suddivisi per tematiche nella versione 2022, tra cui politiche di sicurezza, sicurezza delle risorse umane, controllo accessi, criptografia, sicurezza fisica, sicurezza operativa, sicurezza delle comunicazioni, controllo fornitori, gestione incidenti, continuità operativa, compliance, ecc.), monitorare e riesaminare periodicamente l'efficacia di tali controlli, e migliorare continuamente il sistema. La certificazione ISO 27001, rilasciata da un

ente terzo accreditato, attesta che l'organizzazione segue questo processo e rispetta tutti i requisiti dello standard.

Per una startup fintech, ottenere la certificazione ISO 27001 può rappresentare un fattore abilitante di fiducia sul mercato – specialmente se si rivolge a clientela enterprise o bancaria – ma anche una sfida data la mole di processi e misure da implementare. L'adozione di servizi cloud AWS può tuttavia facilitare il raggiungimento della conformità ISO 27001. Innanzitutto, AWS stesso è certificato ISO/IEC 27001 per la propria infrastruttura globale di servizi cloud (oltre che per altri standard come ISO 27017 per i controlli cloud-specific e ISO 27018 per la privacy nel cloud), il che significa che i data center e i servizi AWS sono gestiti secondo controlli di sicurezza riconosciuti. Questo aiuta la fintech a concentrarsi sui controlli applicativi e organizzativi, sapendo che molti requisiti di base – ad esempio sulla protezione fisica dei server, il controllo degli accessi ai locali, la continuità elettrica e di rete – sono già coperti e attestati dalla piattaforma AWS. Tuttavia, la **responsabilità dell'implementazione** rimane al cliente per tutti i controlli relativi ai propri dati e configurazioni nel cloud (cfr. modello di responsabilità condivisa). Ad esempio, ISO 27001 richiede di controllare gli accessi logici: la fintech dovrà definire policy IAM, regole di password e uso di MFA in AWS per soddisfare tale controllo. Richiede di tenere registri degli eventi: la fintech dovrà configurare logging (CloudTrail, etc.) e conservarne le evidenze. Richiede di cifrare informazioni sensibili: la fintech dovrà abilitare la crittografia nei servizi AWS dove risiedono dati critici.

## 2.3 NIST SP 800-53 – Catalogo di Controlli di Sicurezza

Il framework NIST SP 800-53 fornisce un **catalogo completo di controlli di sicurezza e privacy** per sistemi informativi, originariamente sviluppato per le agenzie federali USA ma ormai adottato come riferimento anche da molte organizzazioni nel settore privato [11]. Si tratta quindi di uno standard più **prescrittivo e tecnico**, che copre aspetti di sicurezza logica, fisica, procedurale e del personale, organizzati in diverse famiglie di controlli. L'ultima revisione (Rev. 5) del NIST 800-53 contiene **20 famiglie di controlli** principali [11], tra cui ad esempio:

1. **AC – Access Control** (controllo degli accessi)
2. **IA – Identification and Authentication** (identificazione e autenticazione)
3. **SC – System and Communications Protection** (protezione dei sistemi e delle comunicazioni, es. cifratura, segregazione di rete)

4. **SI – System and Information Integrity** (integrità dei sistemi e delle informazioni, es. anti-malware, gestione vulnerabilità, monitoraggio)
5. **AU – Audit and Accountability** (audit e tracciabilità, es. logging)
6. **IR – Incident Response** (risposta agli incidenti)
7. **CP – Contingency Planning** (piani di emergenza e DR)
8. **PE – Physical and Environmental Protection** (sicurezza fisica)
9. **PS – Personnel Security** (sicurezza del personale, background check, ecc.)
10. **...** (oltre a **Risk Assessment**, **Security Assessment**, **Configuration Management**, **Training**, **Maintenance**, **Supply Chain Risk Management**, ecc.)

In totale, l'800-53 Rev.5 cataloga circa 1000 controlli di sicurezza, da cui vengono derivati dei **controlli di baseline** (Low, Moderate, High) in base al livello di impatto del sistema [11]. Ad esempio, un sistema *Moderate* (come potrebbe essere un sistema fintech con dati sensibili ma non classificati) deve implementare tutti i controlli del baseline Moderate, che sono un sottoinsieme di quelli totali, selezionati in base a un'analisi del rischio. Le organizzazioni possono poi *personalizzare* (tailor) il baseline aggiungendo o escludendo controlli a seconda delle esigenze specifiche e dei requisiti normativi applicabili [11].

Dal punto di vista di AWS, è importante notare che **l'infrastruttura AWS è già stata validata rispetto ai controlli NIST 800-53** (Rev.4) nell'ambito delle certificazioni FedRAMP Moderate/High per i servizi AWS [8]. Ciò significa che AWS ha superato audit di terza parte che attestano la presenza di controlli di sicurezza allineati a 800-53 per quanto riguarda la piattaforma cloud sottostante [8]. AWS ha ottenuto "Authority to Operate" FedRAMP per molte region (inclusa GovCloud) proprio in base a questi controlli [8]. Per la fintech cliente, questo non significa automaticamente essere conforme a 800-53, ma fornisce una base solida: ad esempio, i controlli di sicurezza fisica (PE) e ambientale, molti controlli di rete (SC), e parte di quelli di monitoraggio (SI) sono già soddisfatti dall'ambiente AWS stesso. Rimane al cliente implementare i controlli a livello di applicazione e configurazione cloud (ad es., definire ruoli IAM – controllo AC-2, o abilitare il versioning su S3 – parte di SC e SI, ecc.). AWS fornisce anche strumenti come **AWS Audit Manager** con regole predefinite per NIST 800-53, che consentono di valutare l'account AWS rispetto ai controlli di tale framework e collezionare evidenze in caso di audit [12].

## 2.4 Architettura Zero Trust (ZTA)

Tradizionalmente, la sicurezza informatica aziendale si basava su un modello di **difesa perimetrale**: si creava una rete aziendale considerata "fidata" all'interno, separata dall'esterno non fidato tramite firewall e altre barriere (il cosiddetto modello "castle and moat"). Tuttavia, con l'evoluzione delle minacce e soprattutto con la distribuzione di sistemi su cloud, utenti mobili, telelavoro e dispositivi personali, questo paradigma è diventato inefficace. Nasce così il concetto di **Zero Trust**, formalizzato anche dal NIST nel documento SP 800-207, che rivoluziona l'approccio: *non si deve mai implicitamente fidare di nulla, sia all'interno che all'esterno del perimetro, ma verificare esplicitamente ogni richiesta di accesso a risorse aziendali* [13]. In un'Architettura Zero Trust (**ZTA**), le difese non sono più incentrate su una rete interna considerata sicura, ma **sull'identità degli utenti e dei dispositivi, e sul contesto delle richieste**, indipendentemente dalla loro provenienza.

I principi cardine della Zero Trust, come delineati dal NIST, includono: **nessuna fiducia implicita basata su posizione di rete** (essere su una rete interna non concede privilegi di per sé) [13]; **autenticazione e autorizzazione continue** per ogni accesso, convalidando sia l'utente che il dispositivo prima di consentire comunicazioni [13]; **micro-segmentazione** delle risorse per minimizzare il movimento laterale – ovvero, anche all'interno dell'infrastruttura, segmentare applicazioni, servizi e database in piccole zone con regole di accesso rigorose; **principio del privilegio minimo dinamico**, adattando i permessi in base al contesto (orario, geolocalizzazione, integrità del dispositivo, comportamento anomalo); **monitoraggio e verifica costante** del traffico e dei comportamenti per rilevare eventuali compromissioni. In sintesi, Zero Trust "sposta" il confine di fiducia dal network all'entità che richiede l'accesso, in un modello in cui **ogni transazione è autenticata, criptata e validata** in modo robusto, come se provenisse da un ambiente non fidato, anche se in realtà avviene all'interno del sistema.

## 2.5 Sicurezza OT (Tecnologie Operative) – NIST SP 800-82

Nel dominio della cybersecurity aziendale, oltre all'IT tradizionale (server, applicazioni, dati), acquista importanza la protezione delle **tecnologie operative (OT)**, ossia quei sistemi digitali che interagiscono con il mondo fisico. Le aziende fintech, essendo principalmente nel settore finanziario digitale, generalmente non operano impianti industriali o infrastrutture OT su larga scala come farebbe una utility o una fabbrica. Tuttavia, è possibile che alcune componenti fisiche rientrino nel perimetro di una fintech: si pensi ad esempio agli **ATM/Bancomat**, ai dispositivi POS smart,

ai data center on-premises con sistemi di building automation, o a eventuali sensori IoT impiegati per servizi innovativi [14]. Il **NIST SP 800-82** fornisce linee guida specifiche per migliorare la sicurezza dei sistemi OT, tenendo conto dei loro requisiti unici di prestazioni, affidabilità e sicurezza fisica [14]. Tali sistemi presentano sfide peculiari: spesso operano in tempo reale, non possono subire interruzioni (disponibilità e sicurezza fisica prevalgono su confidenzialità), utilizzano protocolli proprietari o legacy, e possono avere cicli di vita molto lunghi con componenti non facilmente aggiornabili.

Per mettere in sicurezza ambienti OT, il framework NIST OT Security raccomanda di: **segmentare rigorosamente le reti OT dalle reti IT**, inserendo gateway e firewall industriali che limitino il traffico; **implementare controlli di accesso e monitoraggio specifici** per i protocolli OT; assicurare l'**integrità e l'affidabilità** dei comandi inviati ai dispositivi fisici; gestire patch e vulnerabilità OT in modo pianificato, compensando quando necessario; e predisporre piani di incident response OT che considerino anche scenari di sicurezza fisica e safety [14].

## 2.6 Sicurezza delle Password e Gestione delle Identità – NIST SP 800-63B

Le **password** rimangono tutt'oggi uno dei principali meccanismi di autenticazione, ma anche un punto debole sfruttato di frequente dagli attaccanti (tramite phishing, attacchi a dizionario, credential stuffing, ecc.). Per questo motivo, il NIST ha pubblicato il documento **NIST SP 800-63B** (Digital Identity Guidelines) che fornisce raccomandazioni aggiornate su come gestire in modo sicuro le password, ovvero i "memorized secrets" [15]. Le linee guida più recenti ribaltano alcuni concetti tradizionali a favore di un approccio più user-friendly e sicuro. In sintesi, il NIST suggerisce di privilegiare la lunghezza e la complessità "naturale" delle password rispetto a regole forzate e reset frequenti, integrando tali misure con verifiche di qualità e fattori aggiuntivi [15].

## 2.7 Difesa Perimetrale Avanzata e Soluzioni di Next-Gen Firewall – Check Point Quantum

Oltre ai framework e alle linee guida generali, è utile considerare l'adozione di **tecnologie specifiche** per potenziare la sicurezza dell'infrastruttura cloud. Nel panorama attuale, i firewall di nuova generazione e le piattaforme integrate di threat prevention giocano un ruolo chiave nel proteggere reti e workload, specialmente in scenari ibridi o multi-cloud. **Check Point Quantum** è un esempio di suite di sicurezza

che una fintech potrebbe adottare per migliorare la propria postura difensiva [16]. In particolare, Check Point Quantum Network Security offre una protezione scalabile e multi-livello contro minacce informatiche evolute, integrando moduli come SandBlast Threat Prevention e una console di gestione unificata [16].

## 2.8 Best practice e strategie di mitigazione

Attraverso l'analisi dei framework e delle soluzioni sopra esposte, emergono alcuni **principi trasversali di sicurezza** che dovrebbero guidare ogni fintech nella protezione della propria infrastruttura su AWS. Di seguito, le migliori pratiche e strategie di mitigazione più efficaci:

- **Identità solida e minimo privilegio**: Utilizzare account separati, applicare il principio del minimo privilegio e adottare MFA, come suggerito dal Well-Architected Framework [10].
- **Segmentazione e difesa in profondità**: Implementare controlli multipli a vari livelli, segmentando reti e isolando applicazioni, come indicato dal Well-Architected Framework [10].
- **Protezione dei dati critica**: Cifrare i dati a riposo e in transito, classificare le informazioni e implementare DLP, in accordo con le linee guida AWS [10].
- **Monitoraggio continuo e traceability**: Abilitare logging e correlare i dati tramite SIEM, come raccomandato dal Well-Architected Framework [10].
- **Automatizzare la sicurezza e l'infrastruttura come codice**: Utilizzare IaC e automatizzare controlli di sicurezza per ridurre errori umani [10].
- **Preparazione agli incidenti e resilienza**: Disporre di piani di incident response e di continuità operativa, testandoli regolarmente [10].
- **Formazione e cultura della sicurezza**: Investire nella formazione continua e adottare un approccio "Secure by Design" e "Shift Left" [5].
- **Compliance proattiva**: Integrare controlli normativi (es. PCI DSS, GDPR) nel ciclo di sicurezza per rafforzare l'ambiente [5].

# Capitolo 3

# Fondamenti di Sicurezza su AWS

## 3.1 Modello di responsabilità condivisa di AWS

## 3.2 Best practice di sicurezza specifiche per startup fintech

## 3.3 Panoramica dei principali servizi di sicurezza di AWS

### 3.3.1 AWS Identity and Access Management (IAM)

### 3.3.2 AWS Key Management Service (KMS)

### 3.3.3 AWS CloudTrail e Amazon CloudWatch (servizi concorrenti)

### 3.3.4 AWS GuardDuty, Amazon Inspector e Amazon Macie (alternativa valida)

### 3.3.5 Altri servizi rilevanti (es. AWS WAF, VPC)

# Capitolo 4

# Gestione delle Identità e degli Accessi (IAM)

## 4.1 Implementazione del principio del minimo privilegio

## 4.2 Creazione e gestione di utenti, gruppi e ruoli IAM

## 4.3 Utilizzo di policy IAM per concedere permessi granulari

## 4.4 Configurazione dell'autenticazione a più fattori (MFA)

## 4.5 Gestione delle credenziali (es. utilizzo di IAM Roles per EC2)

## 4.6 Audit e monitoraggio degli accessi IAM

# Capitolo 5

# Monitoraggio e Logging della Sicurezza

## 5.1 Configurazione di AWS CloudTrail per tracciare le attività degli utenti

## 5.2 Implementazione di Amazon CloudWatch per monitorare le metriche di sistema

## 5.3 Creazione di allarmi per eventi specifici e attività sospette

## 5.4 Utilizzo di AWS GuardDuty per il rilevamento automatico di minacce

## 5.5 Integrazione con sistemi SIEM (Security Information and Event Management)

## 5.6 Gestione e analisi dei log

# Capitolo 6

# Protezione dei Dati Sensibili e Conformità Normativa

## 6.1 Crittografia dei dati a riposo e in transito

## 6.2 Gestione delle chiavi di crittografia con AWS KMS o CloudHSM

## 6.3 Implementazione di meccanismi per la protezione dei dati in S3

## 6.4 Misure per la conformità a PCI DSS (se rilevante)

## 6.5 Misure per la conformità al GDPR e protezione dei dati personali

## 6.6 Valutazione e gestione del rischio di perdita di dati

# Capitolo 7

# Casi Studio e Implementazione Pratica

**7.1 Esempio di architettura di sicurezza AWS per una startup fintech (proposta)**

**7.2 Implementazione delle best practice descritte nei capitoli precedenti**

**7.3 Test di penetrazione e valutazione della sicurezza dell'ambiente**

**7.4 Analisi dei risultati e confronto con le best practice**

**7.5 Integrazione di strumenti di sicurezza terzi (es. SentinelOne)**

**7.6 Infrastruttura di base AWS, integrazione codice e infrastruttura di un sistema honeypot**

**7.7 Deadcode per confondere malware (Capitolo 7)**

**7.8 Autenticazione con chiavi pubbliche (Capitolo 8)**



**7.9 Progettazione e implementazione di una Virtual Private Cloud (VPC) isolata**

# Capitolo 8

# Discussione e Conclusioni

## 8.1 Rielaborazione delle domande di ricerca iniziali e discussione dei risultati

## 8.2 Riflessioni sulle sfide e opportunità per la sicurezza di AWS nelle startup fintech

## 8.3 Prospettive future per la ricerca e l'innovazione

## 8.4 Raccomandazioni per la creazione di un modello di cybersecurity resiliente per startup fintech

# Bibliografia


[1] Gartner, *Rapporto sugli investimenti globali Fintech*, Investimenti globali in Fintech: crescita e trend, 2018.

[2] Anonimo, *Le sfide della cybersecurity nelle startup Fintech*, Rapporto sul rischio e le vulnerabilità in ambito Fintech, 2023.

[3] Anonimo, *Differenze tra Cybersecurity Bancaria e Fintech*, Analisi comparativa degli approcci di sicurezza, 2023.

[4] Anonimo, *Minacce informatiche nel settore Fintech*, Analisi delle tipologie di attacchi e delle vulnerabilità in ambito Fintech, 2023.

[5] Netguru. "Cybersecurity in Fintech. Why Is It Important? [2023 Update]". Accessed: 2025-03-10. indirizzo: `https://www.netguru.com/blog/cybersecurity-in-fintech`.

[6] S-PRO. "Fintech security and regulatory compliance best practices and checklists". Accessed: 2025-03-10. indirizzo: `https://s-pro.io/whitepapers/fintech-security-best-practices`.

[7] A. W. Services. "AWS Shared Responsibility Model". Accessed: 2025-03-10. indirizzo: `https://aws.amazon.com/marketplace/pp/prodview-noe2gzebdrqog`.

[8] A. W. Services. "NIST - Amazon Web Services (AWS)". Accessed: 2025-03-10. indirizzo: `https://aws.amazon.com/compliance/nist/`.

[9] A. W. Services. "Updated whitepaper available: Aligning to the NIST Cybersecurity Framework in the AWS Cloud". Accessed: 2025-03-10. indirizzo: `https://aws.amazon.com/blogs/security/updated-whitepaper-available-aligning-to-the-nist-cybersecurity-framework-in-the-aws-cloud/`.

[10] A. W. Services. "Security - AWS Well-Architected Framework". Accessed: 2025-03-10. indirizzo: `https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.pillar.security.en.html`.

[11] Hyperproof. "NIST SP 800-53 Compliance — Improve Your Security System". Accessed: 2025-03-10. indirizzo: `https://hyperproof.io/nist-800-53/`.

[12] A. W. Services. “AWS Audit Manager: Automate Evidence Collection for Compliance”. Accessed: 2025-03-10. indirizzo: https://docs.aws.amazon.com/audit-manager/latest/userguide/NIST-Cybersecurity-Framework-v1-1.html.

[13] N. I. of Standards e Technology. “Zero Trust Architecture”. Accessed: 2025-03-10. indirizzo: https://www.nist.gov/publications/zero-trust-architecture.

[14] N. I. of Standards e Technology. “SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security”. Accessed: 2025-03-10. indirizzo: https://csrc.nist.gov/pubs/sp/800/82/r3/ipd.

[15] JumpCloud. “NIST 800-63 Password Guidelines at a Glance”. Accessed: 2025-03-10. indirizzo: https://jumpcloud.com/blog/nist-800-63-password-guidelines.

[16] A. W. Services. “AWS Marketplace: Check Point Quantum Network Security”. Accessed: 2025-03-10. indirizzo: https://aws.amazon.com/marketplace/pp/prodview-eu5dbipshnzkq.