# POLITECNICO DI TORINO

**Laurea Magistrale in Ingegneria Informatica**


**Tesi di Laurea Magistrale**

# Modello operativo per la valutazione e il monitoraggio della sicurezza del software in Regione Piemonte: metriche, sistemi di rendicontazione e controllo

**Relatore:**
**Prof. Cataldo Basile**

**Candidato:**
**Angelo Cimino**

**Anno Accademico 2024/2025**
**Torino**

# Abstract

La crescente digitalizzazione della Pubblica Amministrazione richiede un approccio sempre più strutturato e misurabile alla sicurezza del software. Nel contesto della Regione Piemonte, che da anni promuove iniziative a sostegno della resilienza digitale, emerge l'opportunità di consolidare e sistematizzare i processi di valutazione e controllo già in atto, favorendo una gestione della sicurezza applicativa orientata alla misurazione e al miglioramento continuo. La presente tesi propone un modello operativo per la valutazione, la rendicontazione e il monitoraggio della sicurezza del software, concepito per integrare strumenti metodologici e organizzativi nel quadro della governance ICT regionale. Il modello definisce un insieme di metriche di sicurezza, introduce un sistema di rendicontazione strutturato e prevede un meccanismo di monitoraggio e controllo, volto a garantire coerenza, trasparenza e sostenibilità nel tempo. L'approccio, pensato per adattarsi alla complessità del sistema informativo regionale, valorizza la collaborazione tra i diversi attori coinvolti e promuove una cultura della sicurezza basata su dati e responsabilità condivise. Pur sviluppato nel contesto piemontese, il modello si propone come strumento replicabile in altre realtà pubbliche, contribuendo al rafforzamento complessivo della resilienza e della governance della sicurezza digitale.

# Ringraziamenti

Desidero esprimere la mia più sincera gratitudine al Prof. Cataldo Basile per la guida attenta, il supporto costante e la disponibilità dimostrata durante la fase più significativa del mio percorso accademico.

Un ringraziamento particolare va al Dott. Luigi Citriniti, tutor aziendale, per il suo prezioso supporto, i consigli sempre puntuali e la collaborazione che ha accompagnato la realizzazione di ogni capitolo di questa tesi. Ringrazio inoltre la Regione Piemonte per avermi offerto l'opportunità di svolgere il mio lavoro di tesi in un contesto stimolante e dinamico, che mi ha permesso di mettermi alla prova e vivere un'esperienza professionale tanto formativa quanto significativa.

Un pensiero particolare va ai miei genitori, per il sostegno che mi hanno dato in questi anni e lungo tutto il percorso universitario. So che non è stato semplice affrontare il distacco, la distanza e le difficoltà di un contesto a voi distante, ma siete sempre stati il mio punto di riferimento. Vi ringrazio per tutto ciò che avete fatto per me. La vostra comprensione, il vostro affetto e il vostro amore non li ho mai dati per scontati, nonostante la vostra presenza costante. Siete sempre stati al mio fianco, con consigli, parole di conforto e un'attenzione sincera verso me e la mia vita. Conosco bene gli sforzi che avete fatto e per questo vi sarò eternamente grato. Grazie di cuore, vi voglio bene.

Desidero ringraziare anche tutta la mia famiglia. Nonostante i chilometri e il tempo passato insieme si siano ridotti da quando vivo a Torino, mi avete sempre ricordato quale sia la mia casa e il luogo in cui posso tornare per sentirmi davvero bene. I legami con voi rimarranno per me sempre forti, profondi e indelebili. La vostra presenza e la vostra importanza nella mia vita significano moltissimo. Tornare da voi spesso è stato un modo per riscoprire ciò che davvero conta. Il vostro affetto e la vostra vicinanza sono stati per me preziosi e fondamentali e per questo non potrò mai smettere di ringraziarvi.

Ringrazio poi i miei amici, vecchi e nuovi, che mi hanno fatto sentire accolto anche lontano dalla mia terra. Ho decisamente trovato una seconda famiglia qui a Torino: con voi sono cresciuto, mi sono confrontato e ho condiviso esperienze che hanno contribuito a formare la persona che sono oggi. I momenti passati insieme mi hanno riempito il cuore ed essere circondato da persone su cui posso contare veramente, è una fortuna di cui in pochi possono godere.

Un ringraziamento particolare va a Riccardo, che considero come un fratello. Abbiamo condiviso la quotidianità, i momenti belli e quelli più difficili, le giornate leggere e quelle più pesanti. Ti ringrazio per le parole, le attenzioni, l'interesse sincero per come stessi, le

confidenze e i confronti che abbiamo avuto. Tutto questo ha contribuito alla mia crescita e ai risultati che ho raggiunto e che raggiungerò. So che ci sarai sempre per me e per questo ti ringrazio dal profondo del mio cuore.

Un grazie speciale va alla mia fidanzata, Carola. Non sei qui citata per "ultima ma non per importanza", ma perché probabilmente racchiudi in te tutto ciò che ho detto finora: sei la mia famiglia, la mia amica, la mia casa. Meriti un ringraziamento particolare per tutto ciò che condividi con me e per tutto quello che fai ogni giorno. Le tue attenzioni, la tua capacità di comprendermi e di starmi accanto sono per me un tesoro immenso. So che potrò sempre contare su di te e queste parole non saranno mai sufficienti per esprimere la gratitudine e l'amore che provo nei tuoi confronti. Grazie per avermi supportato, per esserti anche spesso messa da parte ridefinendo le tue priorità, soprattutto durante questi periodi intensi verso la fine del percorso, che solo tu sai quanto siano stati impegnativi per me e per chi mi stava vicino. Ti ringrazio e ti amo, sei fondamentale per me.

Infine, ringrazio tutte le splendide persone che festeggeranno con me questo traguardo. Se siete qui è perché, in un modo o nell'altro, avete avuto un ruolo importante nel mio percorso, dai gesti più piccoli ai contributi più rilevanti, che per me significano tantissimo. Siete speciali e vi voglio bene.

Grazie a tutti.

# Indice

**Elenco delle figure** VIII

**Acronimi** XI

**Glossario** XV

**Introduzione** 1

**1 Contesto** 4
- 1.1 Contesto normativo . . . 4
  - 1.1.1 Legge 90/2024 . . . 5
  - 1.1.2 Direttiva NIS 2 . . . 7
  - 1.1.3 Linee guida AgID di sicurezza nello sviluppo delle applicazioni . . . 9
  - 1.1.4 NIST.SP.800-55 . . . 10
- 1.2 Contesto aziendale . . . 13
  - 1.2.1 Contesto organizzativo . . . 13
  - 1.2.2 Progetti correlati . . . 16

**2 Definizione del problema e obiettivi** 18
- 2.1 Sfide della sicurezza del software nella Pubblica Amministrazione . . . 18
- 2.2 Limiti degli approcci correnti alla sicurezza del software . . . 23
- 2.3 Necessità di un modello operativo scalabile . . . 27
- 2.4 Obiettivi della tesi . . . 32

**3 Progettazione e realizzazione della soluzione** 36
- 3.1 Definizione metriche di sicurezza . . . 37
  - 3.1.1 Metriche del pilastro Codice . . . 40
  - 3.1.2 Metriche del pilastro Infrastruttura . . . 43
  - 3.1.3 Metriche del pilastro Compliance tecnico-normativa . . . 47
- 3.2 Progettazione sistema di rendicontazione . . . 53
- 3.3 Progettazione del sistema di monitoraggio e controllo . . . 59

**4 Validazione** 65
4.1 Obiettivi . . . . . 66
4.2 Metodologia di validazione . . . . . 68
4.3 Risultati . . . . . 72
4.4 Limitazioni . . . . . 85

**5 Conclusioni e sviluppi futuri** 88

**Bibliografia** 94

**A Metriche del pilastro Codice** 97

**B Metriche del pilastro Infrastruttura** 106

**C Metriche del pilastro Compliance tecnico-normativa** 123

**D Prototipo Framework del Sistema di Rendicontazione** 138

**E Scheda di Validazione** 144

# Elenco delle figure


1.1 Fonti normative e documentazione tecnica di riferimento. Elaborazione dell'autore . . . . . 5

1.2 Pilastri del Cybersecurity Framework NIST. Fonte: Ermes Cybersecurity . 12

1.3 Organigramma di massima delle strutture della Regione Piemonte. Elaborazione dell'autore . . . . . 16

2.1 Principali sfide da affrontare secondo la Strategia Nazionale di Cybersicurezza 22-26. Elaborazione dell'autore . . . . . 19

2.2 Pilastri del Piano Strategico ICT 24-26 della Regione Piemonte con focus sulla cybersicurezza. Fonte: Piano Strategico pluriennale ICT 2024-2026 della Regione Piemonte . . . . . 22

2.3 Vista dei limiti degli approcci alla sicurezza del software nella Pubblica Amministrazione. Elaborazione dell'autore . . . . . 24

2.4 Stato attuale e modello auspicato di monitoraggio della sicurezza lungo il ciclo di vita del software in Regione Piemonte . . . . . 26

2.5 Rappresentazione degli attori coinvolti e dei flussi informativi distribuiti nel contesto della Regione Piemonte. Elaborazione dell'autore . . . . . 28

2.6 Le esigenze di un modello operativo scalabile per la sicurezza applicativa nel contesto regionale. Elaborazione dell'autore . . . . . 31

2.7 Elenco ed elementi chiave degli obiettivi della tesi. Elaborazione dell'autore 35

3.1 Definizione dei tre pilastri - *Codice*, *Infrastruttura* e *Compliance* tecnico-normativa - su cui si sviluppano le metriche del modello proposto dalla tesi. Elaborazione dell'autore . . . . . 39

3.2 Diagramma di flusso di massima della fase di congruità dell'offerta, prima fase delineata nel contesto del sistema di rendicontazione del modello operativo proposto nella presente tesi. Elaborazione dell'autore . . . . . 54

3.3 Diagramma di flusso di massima della fase di ciclo di vita dello sviluppo del software, seconda fase delineata nel contesto del sistema di rendicontazione del modello operativo proposto nella presente tesi. Elaborazione dell'autore 55

3.4 Diagramma di flusso di massima della fase di chiusura del progetto, terza fase delineata nel contesto del sistema di rendicontazione del modello operativo proposto nella presente tesi. Elaborazione dell'autore . . . . . 56
3.5 Diagramma di flusso di massima della fase di monitoraggio periodico, quarta fase delineata nel contesto del sistema di rendicontazione del modello operativo proposto nella presente tesi. Elaborazione dell'autore . . . . . 57
3.6 Rappresentazione delle proprietà del modello operativo verificate nel sistema di monitoraggio e controllo. Elaborazione dell'autore . . . . . 62

4.1 Rappresentazione degli step operativi che costituiscono il processo di validazione a cui è stato sottoposto il modello operativo proposto dalla presente tesi. Elaborazione dell'autore . . . . . 66
4.2 Flussi dati e relazione tra gli strumenti utilizzati nel processo di validazione dagli attori coinvolti. Elaborazione dell'autore . . . . . 71
4.3 Istogramma rappresentante l'andamento dei valori medi percentuali delle metriche per i cinque prodotti del campione della validazione, suddivise per pilastro - *Codice*: ■, *Infrastruttura*: ■, *Compliance*: ■ . Elaborazione dell'autore . . . . . 79
4.4 Rappresentazione della comparazione tra i trend relativi all'indice di conformità alle metriche nel progetto di tesi e all'indice medio generale del progetto PNRR. Elaborazione dell'autore . . . . . 81
4.5 Rappresentazione delle limitazioni del processo di validazione e del modello operativo. Elaborazione dell'autore. . . . . 86

5.1 Rappresentazione delle tre direttrici principali per gli sviluppi futuri inerenti al perfezionamento e all'implementazione del modello operativo in Regione Piemonte . . . . . 89

# Acronimi

**ACN**

Agenzia per la Cybersicurezza Nazionale

**AgID**

Agenzia per l'Italia Digitale, ente nazionale preposto all'attuazione delle politiche di innovazione tecnologica e digitalizzazione della Pubblica Amministrazione, con compiti di indirizzo, coordinamento e controllo.

**CAD**

Codice dell'Amministrazione Digitale

**CINI**

Consorzio Interuniversitario Nazionale per l'Informatica, rete nazionale che coordina attività di ricerca scientifica e trasferimento tecnologico nell'ambito dell'informatica e delle sue applicazioni, comprendendo i principali atenei italiani.

**CIS**

Centro di Ricerca in Cyber Intelligence and Information Security dell'Università di Roma La Sapienza, specializzato in ricerca e formazione sulla sicurezza informatica, la cyber intelligence e la protezione dei dati.

**CSF**

Cybersecurity Framework, modello sviluppato dal National Institute of Standards and Technology (NIST) per supportare le organizzazioni nella gestione e riduzione dei rischi informatici, attraverso un approccio strutturato basato su funzioni, categorie e controlli di sicurezza.

**CSI Piemonte**

Consorzio per il Sistema Informativo Piemontese

**CSIRT**

Computer Security Incident Response Team, gruppo specializzato nella gestione e risposta agli incidenti di sicurezza informatica, con il compito di prevenire, rilevare, analizzare e mitigare le minacce informatiche a supporto di organizzazioni o enti.

**CTE**

Configurazioni Tecnico-Economiche, documenti o schede che definiscono le caratteristiche tecniche e i costi associati a soluzioni, servizi o progetti, utilizzati per supportare la pianificazione, la valutazione e la gestione delle risorse.

**CVE**

Common Vulnerabilities and Exposures, sistema di catalogazione pubblico delle vulnerabilità note nei software, utilizzato per identificare, riferire e gestire i rischi di sicurezza in modo standardizzato a livello internazionale.

**DAST**

Dynamic Application Security Testing, metodologia di analisi della sicurezza delle applicazioni basata sul loro funzionamento in esecuzione, simulando attacchi per rilevare vulnerabilità e comportamenti non sicuri.

**ICT**

Information and Communication Technology, Tecnologie dell'Informazione e della Comunicazione

**IDS**

Intrusion Detection System, sistema progettato per monitorare le reti o i sistemi informatici al fine di rilevare attività sospette o non autorizzate, generando allarmi o segnalazioni per la gestione degli incidenti di sicurezza.

**KPI**

Key Performance Indicator, indicatore chiave di prestazione utilizzato per misurare il livello di raggiungimento di un obiettivo specifico e monitorare l'efficacia dei processi aziendali o organizzativi.

**KRI**

Key Risk Indicator, indicatore chiave di rischio utilizzato per misurare e monitorare l'esposizione al rischio di un'organizzazione, consentendo di identificare tempestivamente potenziali minacce e vulnerabilità.

**NIS**

Network and Information Security, Sicurezza delle Reti e dei Sistemi Informativi

**NIST**

National Institute of Standards and Technology, agenzia federale statunitense che sviluppa standard, linee guida e buone pratiche per la tecnologia, la sicurezza informatica e l'innovazione industriale.

**OWASP**

Open Web Application Security Project

**PA**

Pubblica Amministrazione

**PMI**

Piccole e Medie Imprese

**PNRR**

Piano Nazionale di Ripresa e Resilienza

**PTE**

Proposte Tecniche-Economiche, documenti presentati da fornitori o operatori economici per descrivere soluzioni, caratteristiche tecniche e costi associati a servizi o progetti, al fine di supportare le valutazioni di selezione e aggiudicazione

**RUP**

Responsabile Unico del Progetto

**SAL**

Stato Avanzamento Lavori

**SAST**

Static Application Security Testing, metodologia di analisi della sicurezza del software che esamina il codice sorgente o i binari senza eseguire l'applicazione, per individuare vulnerabilità e problemi di sicurezza.

**SBOM**

Software Bill of Materials, elenco dettagliato dei componenti, librerie e dipendenze presenti in un software, utilizzato per la gestione delle vulnerabilità, la conformità e la sicurezza lungo l'intero ciclo di vita dell'applicazione.

**SCA**

Software Composition Analysis, processo di identificazione e gestione delle componenti open source o di terze parti presenti in un software, volto a rilevare vulnerabilità note e garantire la conformità alle licenze.

**SIRe**

Sistema Informativo Regionale

**SP**

Special Pubblication, serie di documenti rilasciati dal NIST degli Stati Uniti che forniscono linee guida, standard e raccomandazioni sulle migliori pratiche nel campo della sicurezza informatica e delle tecnologie dell'informazione

**SQL**

Structured Query Language, linguaggio di interrogazione strutturato. È un linguaggio di programmazione standardizzato e ampiamente utilizzato per la gestione, manipolazione e interrogazione di database relazionali.

**STRIDE**

Modello di classificazione delle minacce in ambito informatico, che identifica 6 categorie di rischio: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service e Elevation of privilege.

# Glossario

**accountability**

Principio secondo cui un soggetto, un'organizzazione o un ente è responsabile delle proprie azioni, decisioni e risultati, ed è tenuto a renderne conto in modo trasparente, assumendosi le conseguenze giuridiche, etiche e organizzative.

**architetture a microservizi**

Modello architetturale per lo sviluppo di applicazioni software basato sulla suddivisione in componenti indipendenti, detti microservizi, ognuno dei quali implementa una funzionalità specifica e comunica con gli altri tramite interfacce standard (ad esempio API RESTful). Questo approccio favorisce la scalabilità, la manutenibilità e la distribuzione continua del software.

**API RESTful**

Interfaccia di programmazione che segue i principi dell'architettura REST (Representational State Transfer), consentendo la comunicazione tra sistemi tramite protocolli HTTP e l'utilizzo di risorse codificate in formato standardizzato

**assessment**

Processo di valutazione sistematica delle caratteristiche, dei rischi o delle prestazioni di un sistema, progetto o organizzazione, finalizzato a individuare punti di forza, debolezze e aree di miglioramento.

**benchmark**

Procedura di confronto sistematico delle prestazioni, dei processi o dei risultati di un'organizzazione rispetto a standard di riferimento o alle migliori pratiche del settore

**best practices**

Insieme di metodologie, procedure e approcci riconosciuti come i più efficaci e affidabili per raggiungere determinati obiettivi. Nel contesto ICT e della cybersecurity, le *best practices* rappresentano linee guida consolidate per garantire qualità, efficienza, sicurezza e conformità dei sistemi informativi e dei processi di sviluppo software.

**business continuity**

Insieme di strategie e misure volte a garantire la continuità operativa di un'organizzazione in caso di eventi avversi o interruzioni, assicurando il ripristino tempestivo dei servizi critici.

**business intelligence**

Insieme di processi, metodologie e strumenti finalizzati alla raccolta, analisi e trasformazione dei dati aziendali in informazioni strategiche, a supporto del processo decisionale e della pianificazione operativa.

**CI/CD**

Acronimo di Continuous Integration e Continuous Deployment (o Delivery). Indica un insieme di pratiche e strumenti che automatizzano il processo di sviluppo, test e rilascio del software, garantendo aggiornamenti frequenti, qualità del codice e riduzione dei tempi di distribuzione. È un elemento fondamentale nei contesti DevOps e DevSecOps.

**cloud computing**

Modello di erogazione di risorse informatiche — come server, archiviazione, database, rete, software e analisi — tramite Internet, su richiesta e con tariffazione basata sull'utilizzo. Il cloud consente scalabilità, flessibilità e riduzione dei costi infrastrutturali, supportando diversi modelli di servizio come IaaS (Infrastructure as a Service), PaaS (Platform as a Service) e SaaS (Software as a Service).

**code review**

Processo sistematico di analisi del codice sorgente di un'applicazione da parte di uno o più revisori, con l'obiettivo di individuare errori, vulnerabilità, inefficienze o violazioni delle linee guida di sviluppo sicuro, migliorando qualità, sicurezza e manutenibilità del software.

**continuous vulnerability management**

Processo sistematico e continuo di identificazione, classificazione, valutazione e mitigazione delle vulnerabilità presenti nei sistemi informatici, applicazioni e reti. L'obiettivo è ridurre il rischio di sfruttamento da parte di attaccanti e garantire un livello costante di sicurezza operativa.

**cyber maturity**

Livello di maturità di un'organizzazione nella gestione della sicurezza informatica, valutato in base alla capacità di prevenire, rilevare, rispondere e riprendersi da incidenti cibernetici.

**cybersecurity**

Insieme di tecnologie, processi e misure di protezione progettate per salvaguardare sistemi informatici, reti e dati da attacchi digitali, garantendo la confidenzialità, l'integrità e la disponibilità delle informazioni.

**cross-site scripting (XSS)**

Tipologia di vulnerabilità web in cui un'applicazione non valida o non neutralizza correttamente dati forniti dall'utente, permettendo l'iniezione di script malevoli eseguiti nel browser di altri utenti; ciò può portare al furto di cookie, sessioni, o all'esecuzione di azioni non autorizzate a nome della vittima.

**dashboard**

Interfaccia visiva che raccoglie e presenta in modo sintetico e immediato dati, metriche e indicatori chiave di prestazione (KPI/KRI), permettendo il monitoraggio, l'analisi e il supporto decisionale in ambito gestionale, tecnico o di sicurezza informatica.

**DevOps**

Approccio metodologico e culturale che integra sviluppo software (Development) e operazioni IT (Operations), con l'obiettivo di migliorare la collaborazione tra team, accelerare il rilascio di applicazioni, aumentare la qualità del software e garantire continuità e sicurezza nei processi di deployment.

**DevSecOps**

Approccio metodologico che integra le pratiche di sviluppo software (Development), operazioni IT (Operations) e sicurezza (Security) lungo l'intero ciclo di vita del software. L'obiettivo è garantire che la sicurezza sia incorporata fin dalle prime fasi dello sviluppo e sia continuamente monitorata durante il rilascio e la gestione delle applicazioni.

**filiera di automation**

Insieme integrato di tecnologie, processi e strumenti che supportano l'automazione dei flussi di lavoro e delle attività aziendali o istituzionali. La filiera comprende componenti come sistemi di orchestrazione, robotica software , piattaforme di integrazione e monitoraggio, con l'obiettivo di aumentare efficienza, ridurre errori e ottimizzare le risorse.

**firewall**

Dispositivo o software che controlla il traffico di rete in entrata e in uscita, filtrando le comunicazioni secondo regole di sicurezza prestabilite per proteggere sistemi e reti da accessi non autorizzati.

**framework**

Struttura di supporto e insieme di strumenti, metodi e linee guida che facilitano lo sviluppo, l'organizzazione e la gestione di sistemi, promuovendo riusabilità, standardizzazione e coerenza.

**governance**

Insieme di regole, processi, strutture e pratiche adottate da un'organizzazione per dirigere, gestire e controllare le proprie attività, garantendo trasparenza, responsabilità e allineamento agli obiettivi strategici.

**hardening**

Insieme di procedure e configurazioni volte a ridurre la superficie di attacco di un sistema informatico, attraverso la disattivazione di funzionalità non necessarie, l'applicazione di patch di sicurezza, la configurazione sicura dei servizi e il rafforzamento dei meccanismi di protezione.

**in house**

Società a capitale interamente pubblico che operano come braccio operativo dell'amministrazione, svolgendo attività strumentali e servizi per conto dell'ente controllante, senza logiche di mercato ma nel rispetto delle norme di evidenza pubblica.

**manifest**

File di configurazione che descrive le componenti, le dipendenze e le informazioni essenziali di un'applicazione o di un pacchetto software, utilizzato per garantirne la corretta distribuzione, esecuzione e gestione.

**measurement**

Attività di raccolta e quantificazione di dati oggettivi attraverso metriche, indicatori e criteri predefiniti, con lo scopo di monitorare e confrontare le prestazioni, l'efficacia o il livello di sicurezza di sistemi e processi.

**middleware**

Strato software che funge da intermediario tra sistema operativo, applicazioni e componenti distribuiti, facilitando la comunicazione, l'integrazione e la gestione dei dati e dei servizi in architetture complesse. Viene utilizzato per semplificare lo sviluppo e garantire interoperabilità e scalabilità dei sistemi.

**milestone**

Punto di riferimento significativo all'interno di un progetto, che segna il completamento di una fase, di un'attività o di un obiettivo intermedio. Le milestone consentono di monitorare l'avanzamento, verificare il rispetto delle scadenze e supportare il controllo della pianificazione.

**mission critical**

Termine utilizzato per indicare sistemi, applicazioni o processi la cui corretta operatività è essenziale per il funzionamento dell'organizzazione. Un guasto o una compromissione di un sistema *mission critical* può comportare gravi impatti operativi, economici o di sicurezza. Tali sistemi richiedono elevati livelli di affidabilità, disponibilità e protezione.

**open source**

Modello di sviluppo e distribuzione del software in cui il codice sorgente è reso pubblico e accessibile, permettendo a chiunque di studiarlo, modificarlo e ridistribuirlo.

Promuove la trasparenza, la collaborazione e l'innovazione condivisa, ed è alla base di molti progetti e tecnologie adottati nella Pubblica Amministrazione e nel settore privato.

**OWASP Top 10**

Classifica e documento periodico pubblicato dall'OWASP che individua e descrive le dieci principali categorie di vulnerabilità di sicurezza nelle applicazioni web. Rappresenta uno standard di riferimento internazionale per sviluppatori, auditor e responsabili della sicurezza nel ridurre i rischi più critici legati al software.

**penetration test**

Attività di valutazione della sicurezza di un sistema informatico, rete o applicazione, in cui esperti simulano attacchi reali per identificare vulnerabilità, debolezze e rischi, al fine di migliorare le contromisure e la resilienza del sistema.

**phishing**

Tecnica di attacco informatico che mira a ingannare gli utenti inducendoli a fornire informazioni sensibili, come credenziali o dati bancari, tramite comunicazioni fraudolente che simulano enti affidabili.

**privacy by design**

Principio secondo cui la protezione dei dati personali deve essere integrata sin dalla progettazione di sistemi, applicazioni e processi, garantendo la minimizzazione dei dati, la sicurezza e la riservatezza lungo tutto il ciclo di vita delle informazioni.

**ransomware**

Tipologia di malware che cifra i dati di un sistema informatico e ne limita l'accesso, richiedendo un riscatto (ransom) per ripristinare i dati o il funzionamento normale. È una delle principali minacce alla sicurezza informatica.

**release**

Versione di un software o di un'applicazione resa disponibile agli utenti o ai sistemi di produzione, comprendente nuove funzionalità, correzioni di bug e aggiornamenti di sicurezza, nell'ambito del ciclo di sviluppo e distribuzione del software.

**remediation**

Processo di correzione o mitigazione di vulnerabilità, errori o problemi identificati in sistemi informatici, applicazioni o reti, al fine di ridurre i rischi, migliorare la sicurezza e garantire la conformità agli standard e alle policy aziendali.

**reporting**

Attività di raccolta, elaborazione e presentazione di dati e informazioni, spesso attraverso report strutturati, cruscotti o dashboard, con l'obiettivo di monitorare performance, rischi e risultati, supportando il processo decisionale in ambito gestionale, tecnico o di sicurezza.

**risk assessment**

Processo di identificazione, analisi e valutazione dei rischi potenziali che possono compromettere la sicurezza, l'integrità o la disponibilità di sistemi, dati e processi aziendali.

**legacy**

Sistema, applicazione o infrastruttura tecnologica obsoleta ma ancora in uso, spesso per motivi di compatibilità o costi. I sistemi legacy possono presentare limiti in termini di sicurezza, manutenzione e integrazione con tecnologie moderne.

**security by design**

Principio di progettazione dei sistemi informatici che prevede l'integrazione delle misure di sicurezza fin dalle prime fasi di analisi e sviluppo, in modo da ridurre al minimo le vulnerabilità strutturali.

**security by default**

Approccio alla configurazione dei sistemi secondo il quale le impostazioni predefinite privilegiano la sicurezza, riducendo i rischi senza richiedere interventi manuali da parte dell'utente.

**SQL injection**

Tecnica di attacco informatico che sfrutta vulnerabilità nell'input di applicazioni che interagiscono con database SQL, permettendo a un attaccante di inserire o eseguire comandi SQL non autorizzati per visualizzare, modificare o cancellare dati, o ottenere accesso non autorizzato al sistema.

**stakeholder**

Individuo, gruppo o organizzazione che ha un interesse, diretto o indiretto, nelle attività, decisioni o risultati di un progetto, di un ente o di un'organizzazione, e il cui coinvolgimento può influenzarne il successo o l'evoluzione.

**supply chain**

Insieme dei processi, delle attività e delle risorse coinvolte nella produzione, trasformazione e distribuzione di beni e servizi, dalla materia prima fino al consumatore finale, con l'obiettivo di garantire efficienza, continuità e qualità lungo tutta la catena del valore.

**threat modeling**

Processo sistematico volto a identificare, classificare e valutare le minacce e le vulnerabilità di un sistema, applicazione o rete, al fine di definire strategie di mitigazione e rafforzare la sicurezza lungo l'intero ciclo di vita del software.

**uptime**

Periodo di tempo in cui un sistema o servizio rimane operativo e disponibile senza interruzioni, indicativo della sua affidabilità.

**vulnerabilità zero-day**

Debolezza o falla in un software sconosciuta al produttore e non ancora corretta, che può essere sfruttata dagli attaccanti immediatamente dopo la scoperta, rappresentando un rischio elevato per la sicurezza dei sistemi.

# Introduzione

Nel progressivo processo di digitalizzazione della Pubblica Amministrazione, la gestione della sicurezza informatica è diventata un elemento imprescindibile per garantire la continuità operativa, la protezione dei dati sensibili e il rispetto dei principi di trasparenza e responsabilità verso i cittadini. L'evoluzione normativa a livello europeo e nazionale ha portato all'adozione di un insieme articolato di regolamenti, direttive e linee guida che pongono le basi per una gestione sistemica e misurabile della sicurezza, imponendo nuovi obblighi, ridefinendo i requisiti minimi digitali e introducendo principi di accountability applicabili ai sistemi informativi delle amministrazioni pubbliche.

In questo scenario, la Regione Piemonte, in quanto Ente di rilevanza regionale, soggetto promotore della trasformazione digitale del territorio e soggetto *importante* secondo la NIS2 [1], è chiamata a recepire e attuare tali disposizioni non solo attraverso l'adeguamento tecnico dei propri sistemi informativi, ma anche mediante l'adozione di modelli operativi strutturati per la valutazione, il monitoraggio e il miglioramento continuo della sicurezza applicativa. La sicurezza del software assume, infatti, un ruolo strategico, poiché è proprio nelle applicazioni e nei servizi digitali che si concentra la maggiore esposizione a rischi, vulnerabilità e potenziali compromissioni.

Negli ultimi anni la Pubblica Amministrazione è diventata bersaglio privilegiato di attacchi informatici complessi e persistenti, che hanno messo in evidenza la fragilità di sistemi spesso eterogenei, stratificati e non sempre adeguatamente monitorati. Parallelamente, l'accelerazione della trasformazione digitale, unita all'adozione massiva di servizi erogati online, ha ampliato la superficie d'attacco, rendendo necessario un ripensamento delle strategie di protezione e dei meccanismi di verifica. In tale contesto, la sicurezza non può più essere concepita come adempimento residuale o funzione tecnica isolata, ma deve essere integrata nei processi di progettazione, sviluppo, gestione e governo del software, adottando logiche di misurazione, tracciabilità e standardizzazione.

La presente tesi si propone di rispondere a questa esigenza attraverso la definizione di un modello operativo per la valutazione della sicurezza del software nella Pubblica Amministrazione, con particolare applicazione al contesto della Regione Piemonte. Gli obiettivi principali consistono nel:

- identificare un insieme coerente di metriche oggettive, verificabili e ripetibili per la valutazione della sicurezza lungo tre pilastri fondamentali: *Codice* , *Infrastruttura* e *Compliance* tecnico-normativa;

- progettare un sistema di rendicontazione capace di strutturare le evidenze di sicurezza durante tutto il ciclo di affidamento, sviluppo e gestione del software;

- definire un sistema di monitoraggio e controllo in grado di assicurare la qualità valutativa, la coerenza applicativa e il miglioramento continuo del modello nel tempo;

- validare il modello attraverso la sua applicazione a un campione significativo di applicativi regionali, verificandone l'efficacia operativa e la sostenibilità organizzativa.

Per raggiungere questi obiettivi, il lavoro è stato strutturato come un percorso graduale che si sviluppa dalla cornice teorico-normativa fino alla costruzione di uno strumento pienamente operativo nel contesto regionale. La tesi si articola secondo la seguente struttura:

- Capitolo 1 – Contesto: Viene analizzato il quadro legislativo europeo e nazionale (tra cui NIS2, D.Lgs 138/2024, Legge 90/2024 ), le principali cornici metodologiche internazionali e nazionali (SP NIST e Linee Guida AgID) e il contesto organizzativo della Regione Piemonte, evidenziando i ruoli, gli attori e i sistemi informativi coinvolti nei processi di gestione della sicurezza.

- Capitolo 2 – Definizione del problema e obiettivi: Vengono delineate le principali sfide legate alla sicurezza del software nella Pubblica Amministrazione, in particolare in Regione Piemonte. Si analizzano i limiti degli approcci correnti alla gestione della sicurezza informatica, andando a definire gli elementi che rendono necessaria la progettazione di un modello operativo strutturato per la valutazione della cybersecurity. Infine gli obiettivi della tesi evidenziano come il raggiungimento degli stessi permetterà di soddisfare le necessità evidenziate e di superare i limiti presenti nell'attuale contesto regionale.

- Capitolo 3 – Progettazione e realizzazione della soluzione: Si introduce l'impianto metodologico alla base del modello, descrivendo la logica di costruzione delle metriche, il perimetro dei tre pilastri e i criteri di calcolo. Viene definito un set organico di indicatori quantitativi e qualitativi, strutturato in funzione del pilastro di appartenenza e degli obiettivi di misurazione. Viene descritto il sistema di rendicontazione, composto da flussi standardizzati, schede di fase e indicatori di conformità alle metriche, seguito dalla progettazione del sistema di monitoraggio e controllo, basato su un approccio ciclico e partecipato che coinvolge la rete dei referenti ICT regionali e garantisce la qualità e la validità del modello nel tempo.

- Capitolo 4 – Validazione: Il modello viene applicato a cinque applicativi reali del parco software regionale. La validazione permette di verificarne la robustezza metodologica, la coerenza interna, la sensibilità delle metriche e la sostenibilità operativa. Vengono presentati i risultati, le osservazioni trasversali e l'analisi delle quattro proprietà fondamentali del modello (affidabilità, applicabilità, esaustività, scalabilità), seguite dalla discussione dei limiti metodologici.

- Capitolo 5 – Conclusioni e sviluppi futuri: Il capitolo finale sintetizza i risultati raggiunti e propone possibili linee evolutive del modello, tra cui l'automatizzazione della rendicontazione, la riduzione della dipendenza da tool proprietari, l'estensione del modello a tutto il parco applicativo regionale e l'adozione di una soluzione software dedicata che recepisca il modello.

Complessivamente, la tesi si propone di offrire alla Regione Piemonte e, più in generale, alla Pubblica Amministrazione un modello pratico, metodologicamente fondato e concretamente applicabile, capace di rendere la sicurezza del software un processo misurabile, tracciabile e basato su criteri oggettivi. Il lavoro costituisce un contributo verso la costruzione di un approccio integrato e sistemico alla sicurezza applicativa, in grado di coniugare esigenze tecniche, normative e organizzative in una visione unitaria di governance del rischio informatico.

# Capitolo 1

# Contesto

Il presente capitolo si propone di delineare il quadro di riferimento entro il quale si colloca il progetto di tesi, offrendo una panoramica sia normativa sia organizzativa che permette di comprendere il contesto di riferimento e le motivazioni alla base dell'approccio metodologico adottato. L'analisi è articolata lungo due direttrici principali, strettamente interconnesse. La prima direttrice ha carattere normativo e si concentra sull'esame dei principali strumenti giuridici e regolamentari che definiscono obblighi, requisiti e linee guida relativi alla sicurezza del software nelle pubbliche amministrazioni. In questa sezione vengono quindi considerati i riferimenti legislativi, i regolamenti, le direttive europee e le linee guida che orientano la gestione sicura dei sistemi informativi, evidenziando come tali strumenti costituiscano il quadro obbligatorio e operativo entro cui le amministrazioni devono muoversi. La seconda direttrice è di natura organizzativa e mira a descrivere il contesto specifico della Regione Piemonte, con particolare attenzione ai sistemi informativi regionali. Viene illustrata la struttura operativa e strategica dell'Ente, evidenziando il contesto organizzativo di riferimento, le esigenze concrete e le sfide quotidiane che rendono necessario un approccio metodologico strutturato, in grado di integrare sicurezza, efficienza e innovazione digitale. All'interno di questo contesto vengono inoltre presentate le progettualità già in corso che insistono sullo stesso perimetro del modello descritto nella tesi, mostrando come il lavoro proposto si inserisca in un ecosistema più ampio di iniziative e interventi tecnologici e organizzativi.

## 1.1 Contesto normativo

La sezione introduce le principali fonti normative e la documentazione tecnica di riferimento per la definizione del contesto normativo su cui si sviluppa la tesi, come rappresentato in Figura 1.1.


**Figura 1.1:** Fonti normative e documentazione tecnica di riferimento. Elaborazione dell'autore

### 1.1.1 Legge 90/2024

Nel più recente sviluppo del panorama normativo italiano in materia di sicurezza informatica, la Legge del 28 giugno 2024, n. 90 [2] rappresenta un importante punto di svolta. Essa introduce disposizioni innovative e stringenti per il rafforzamento della cybersecurity nazionale, intervenendo tanto sull'organizzazione interna della Pubblica Amministrazione quanto sulla disciplina dei reati informatici. In un contesto caratterizzato da minacce cibernetiche sempre più pervasive e sofisticate, prima ancora dell'adozione della Direttiva (UE) 2022/2555 NIS 2 [1] e del suo recepimento in ambito nazionale, il legislatore ha avvertito la necessità di innalzare il livello di resilienza delle infrastrutture pubbliche e di settore strategico, delineando un quadro regolatorio che si propone di integrare efficacemente le attività di prevenzione, gestione e risposta agli incidenti informatici.

Al centro dell'impianto normativo si colloca l'introduzione di obblighi stringenti di notifica degli incidenti di cybersecurity. La legge impone infatti a una vasta platea di soggetti pubblici e para-pubblici, compresi le Regioni, i Comuni e le Aziende Sanitarie Locali, di segnalare e notificare tempestivamente qualsiasi incidente che impatti reti, sistemi informativi o servizi digitali, secondo una tassonomia specifica stabilita a livello nazionale. In particolare, è previsto che la segnalazione preliminare avvenga senza ritardo, entro 24 ore dalla conoscenza dell'evento, mentre la notifica completa deve essere trasmessa entro 72 ore. Queste disposizioni rafforzano il principio della rapidità nella comunicazione delle minacce, requisito essenziale per garantire una risposta coordinata ed efficace agli incidenti,

ed evidenziano l'importanza attribuita alla tempestività come fattore chiave della resilienza digitale.

La legge introduce inoltre un regime sanzionatorio severo per i soggetti che non rispettino gli obblighi di notifica. In parallelo, la normativa attribuisce all'Agenzia per la Cybersicurezza Nazionale (ACN) nuovi poteri di intervento, con la possibilità di imporre misure correttive specifiche volte al rafforzamento della resilienza informatica dei soggetti coinvolti. Tale rafforzamento passa anche attraverso l'adozione obbligatoria di piani di gestione del rischio, l'istituzione di strutture interne per la sicurezza delle informazioni e la nomina di un Referente per la cybersecurity dotato di comprovate competenze tecniche.

Particolare attenzione è dedicata al rafforzamento delle misure di sicurezza tramite l'uso della crittografia. Le amministrazioni pubbliche devono verificare che i sistemi e le applicazioni utilizzino soluzioni crittografiche conformi agli standard nazionali, evitando vulnerabilità note che potrebbero compromettere l'integrità o la riservatezza dei dati trattati. In tale ottica, ACN viene incaricata di sviluppare e promuovere linee guida e standard di crittografia, istituendo anche un Centro Nazionale di Crittografia, destinato a costituire il punto di riferimento per la competenza nazionale in materia.

Sul piano organizzativo, la Legge 90/2024 prevede la creazione di strutture interne deputate alla pianificazione, al monitoraggio continuo delle minacce e alla gestione operativa degli incidenti. L'integrazione del Referente per la cybersecurity regionale in queste strutture mira a rafforzare il coordinamento con l'Agenzia nazionale, favorendo la circolazione tempestiva delle informazioni e l'adozione uniforme delle misure preventive e correttive.

La nuova disciplina interviene anche sul versante contrattuale, introducendo specifiche prescrizioni per l'approvvigionamento di beni e servizi informatici destinati a contesti rilevanti per la tutela degli interessi strategici nazionali. Attraverso un decreto attuativo, saranno definiti gli *elementi essenziali di cybersecurity* che dovranno essere considerati obbligatoriamente nei procedimenti di acquisizione. La conformità a tali elementi sarà requisito fondamentale nella valutazione delle offerte, in un'ottica che privilegia la qualità e la sicurezza rispetto al mero criterio del prezzo più basso. Viene inoltre prevista una forma di premialità per le tecnologie sviluppate in ambito europeo o alleato, a sostegno dell'autonomia strategica e tecnologica nazionale nel campo della cybersecurity.

Nel complesso, la Legge 90/2024 rappresenta una svolta significativa nella strategia nazionale di cybersecurity, proponendosi di innalzare il livello di maturità complessiva della Pubblica Amministrazione, promuovere una cultura della prevenzione e rafforzare la capacità di risposta agli attacchi. In particolare, la previsione di obblighi di notifica stringenti, la valorizzazione della misurazione continua della sicurezza e l'imposizione di requisiti minimi anche nella supply chain ICT delineano un nuovo quadro in cui la semplice adozione di controlli formali non è più sufficiente. Diventa invece necessario dimostrare, attraverso evidenze oggettive e documentate, la capacità dei sistemi informativi di mantenere un adeguato livello di protezione nel tempo.

Nel contesto della tesi, la Legge 90/2024 costituisce quindi non solo un vincolo normativo da rispettare, ma anche un impulso strutturale verso l'adozione di modelli operativi più evoluti di gestione della sicurezza applicativa. Il sistema di valutazione e monitoraggio proposto, fondato sulla definizione di metriche oggettive, sull'implementazione di strumenti di raccolta e analisi dei dati di sicurezza e sulla strutturazione di processi di rendicontazione

formale, si configura come una risposta diretta ed efficace ai requisiti introdotti dal legislatore.

Attraverso l'applicazione pratica dei principi ispiratori della legge, la Regione Piemonte può non solo garantire la conformità normativa, ma anche promuovere un approccio proattivo alla gestione del rischio software, migliorando la trasparenza interna, supportando il processo decisionale strategico e rafforzando la capacità di difesa cibernetica in linea con le nuove aspettative di accountability, resilienza e misurabilità della sicurezza informatica nel settore pubblico.

### 1.1.2 Direttiva NIS 2

Con l'adozione della Direttiva (UE) 2022/2555 [1], nota come NIS 2, l'Unione Europea ha ridefinito e rafforzato il quadro normativo in materia di cybersecurity e dei sistemi informativi. L'obiettivo primario è incrementare il livello complessivo di resilienza cibernetica dei Paesi membri, promuovendo una risposta armonizzata alle minacce digitali e imponendo obblighi di sicurezza più stringenti ai soggetti pubblici e privati che forniscono servizi considerati *essenziali* e *importanti* per la società e l'economia. La nuova direttiva, che abroga la precedente NIS (UE) 2016/1148 [3], nasce dall'esigenza di colmare le lacune emerse nell'implementazione della prima normativa, spesso disomogenea tra i vari Stati membri.

Tra le principali novità della NIS 2 si segnala l'estensione dell'ambito soggettivo, che ora include non solo i gestori di infrastrutture critiche e i fornitori di servizi digitali, ma anche le pubbliche amministrazioni centrali, regionali e locali, in particolare laddove gestiscano dati rilevanti, infrastrutture ICT strategiche o affidino tali responsabilità agli enti in house. In questo scenario, la Regione Piemonte e i suoi soggetti strumentali risultano pienamente coinvolti, soprattutto in relazione all'acquisizione e alla gestione del software utilizzato per i servizi regionali. Secondo i criteri stabiliti dalla direttiva, tali soggetti possono essere qualificati come entità *essenziali* o *importanti*, rientrando così nel perimetro di applicazione della norma.

La NIS 2 introduce un insieme di obblighi di sicurezza più strutturato, fondato su un approccio di gestione del rischio. Tra i requisiti richiesti, figurano:

- l'identificazione e mitigazione delle vulnerabilità, sia note che potenziali;
- la protezione degli asset critici e dei dati sensibili;
- la gestione della supply chain ICT, con attenzione particolare ai fornitori terzi;
- l'adozione dei principi di security by design e security by default nei processi di sviluppo, approvvigionamento e manutenzione del software.

Rispetto alla precedente normativa, la NIS 2 enfatizza l'importanza della cooperazione transfrontaliera tra gli Stati membri, della standardizzazione tecnica e della promozione dell'interoperabilità. In questo contesto si inserisce un tassello fondamentale riguardante gli obblighi di notifica degli incidenti. La direttiva prevede che un incidente significativo

venga segnalato entro 24 ore dall'identificazione, venga trasmesso un aggiornamento entro 72 ore e venga prodotta una relazione conclusiva entro un mese dall'incidente.

Un'ulteriore innovazione portata dalla NIS 2 è rappresentata dalla centralità dei CSIRT nazionali e settoriali, incaricati di assistere le entità obbligate nella gestione tecnica degli incidenti e nella condivisione delle informazioni critiche. Gli Stati membri sono chiamati a garantirne l'operatività, dotandoli delle risorse necessarie e favorendo la cooperazione con gli stakeholder pubblici e privati. Questo punto si collega alla necessità, evidenziata nella tesi, di strutturare e formare figure interne alla Regione, come i referenti ICT o i componenti del gruppo di lavoro *Cybersicurezza*, per assicurare una corretta implementazione delle misure di sicurezza e una collaborazione efficace con i soggetti esterni coinvolti.

Dal punto di vista operativo, la direttiva chiede che la sicurezza informatica diventi una parte integrante della gestione digitale all'interno delle pubbliche amministrazioni. In particolare, la cybersecurity non deve essere vista come un elemento separato o accessorio, ma come un aspetto fondamentale da considerare in ogni decisione e processo organizzativo. Inoltre, la direttiva non si limita al settore pubblico: incoraggia anche le piccole e medie imprese (PMI) e i fornitori che collaborano con le amministrazioni a rafforzare le proprie misure di protezione. L'obiettivo è garantire che l'intera catena di approvvigionamento, cioè l'insieme di aziende e soggetti coinvolti nel fornire beni e servizi, sia più sicura e meno esposta a rischi informatici. Questo aspetto è particolarmente rilevante per la Regione Piemonte, che spesso acquisisce software e servizi attraverso affidamenti che coinvolgono indirettamente una catena di fornitori, talvolta complessi da monitorare in termini di compliance. La NIS 2 richiede infatti di vigilare anche su fornitori indiretti, imponendo la tracciabilità delle soluzioni adottate e delle configurazioni applicative.

In linea con quanto espresso nei considerando della direttiva, emerge la necessità per ogni ente pubblico di dotarsi di strumenti operativi e organizzativi per rendere misurabile, sostenibile e verificabile la propria postura di sicurezza, obiettivo principale della presente tesi nell'ambito del software regionale.

In Italia, la Direttiva NIS 2 è stata recepita con il Decreto Legislativo 4 settembre 2024, n. 138 [4] , che definisce il quadro nazionale per la sua attuazione. Il decreto stabilisce le competenze dell'ACN quale Autorità nazionale competente NIS, Punto di contatto unico NIS e sede operativa del CSIRT Italia. Viene inoltre introdotto un meccanismo di registrazione digitale obbligatoria per i soggetti rientranti in ambito NIS 2, che devono annualmente aggiornare i propri dati e i riferimenti organizzativi sulla piattaforma messa a disposizione da ACN . Il decreto elenca criteri dettagliati per l'identificazione dei soggetti coinvolti, comprese le pubbliche amministrazioni regionali, e rafforza il principio di cybersecurity attraverso la governance, prevedendo l'integrazione della sicurezza informatica nella pianificazione strategica e negli appalti pubblici ICT, anche con riferimento alla supply chain.

Questi elementi sono direttamente connessi agli obiettivi della tesi, che propone un modello operativo scalabile per la valutazione e il monitoraggio della sicurezza del software regionale. Il modello si basa sull'identificazione di metriche di sicurezza, processi di rendicontazione e sistemi di controllo tecnici e organizzativi, tutti ispirati ai principi di prevenzione anticipata e gestione proattiva dei rischi informatici. In particolare, il recepimento normativo italiano, il Decreto Legislativo 4 settembre 2024, n. 138[4], rappresenta il

contesto di riferimento entro cui la Regione Piemonte dovrà attuare le misure previste dalla direttiva e fornisce parte della base giuridica e organizzativa per l'adozione del modello operativo proposto.

### 1.1.3 Linee guida AgID di sicurezza nello sviluppo delle applicazioni

Nel panorama normativo nazionale, un ruolo centrale nella promozione della sicurezza informatica nella Pubblica Amministrazione è svolto dall'Agenzia per l'Italia Digitale (AgID), attraverso la pubblicazione di un insieme organico di Linee Guida sulla sicurezza nello sviluppo delle applicazioni software [5]. Queste linee guida costituiscono un riferimento tecnico e organizzativo fondamentale per le PA, delineando buone pratiche da adottare per garantire la protezione dei sistemi informativi e la resilienza delle applicazioni digitali.

L'impianto delle linee guida è fortemente ispirato al principio del security by design, che prevede l'integrazione della sicurezza fin dalle prime fasi della progettazione di un sistema. Tale approccio consente non solo di ridurre i rischi legati a vulnerabilità applicative, ma anche di costruire processi di sviluppo più robusti e verificabili nel tempo.

Le linee guida si articolano in quattro macro-aree, ciascuna delle quali affronta un aspetto specifico e complementare del ciclo di vita del software. La prima area riguarda l'adozione di un ciclo di sviluppo sicuro [6], che impone di integrare misure di sicurezza in tutte le fasi del progetto: pianificazione, progettazione, sviluppo, test, rilascio e manutenzione. Ogni fase deve essere accompagnata da attività specifiche, come l'analisi dei rischi, la definizione di standard di codifica, la formazione dei team di sviluppo e l'impiego di strumenti per l'analisi statica e dinamica del codice. L'obiettivo è ridurre il rischio di vulnerabilità già durante lo sviluppo, anziché correggerle in seguito.

Un secondo ambito riguarda più direttamente la scrittura sicura del codice [7]. Le linee guida AgID forniscono una serie di indicazioni tecniche mirate a prevenire errori comuni e vulnerabilità note, come SQL injection, cross-site scripting (XSS), errori nella gestione delle sessioni o l'utilizzo di algoritmi di crittografia deboli. Le raccomandazioni includono, tra le altre, la sanificazione e validazione degli input, l'uso di librerie di sicurezza consolidate, la gestione appropriata degli errori e l'adozione di tecniche di codifica sicura per ridurre il rischio di compromissione dei dati.

La terza area di intervento è legata alla configurazione sicura del software di base, nota anche come hardening [8]. Questo processo riguarda l'impostazione sicura degli ambienti operativi, come server, database e middleware, con l'obiettivo di ridurre la superficie di attacco. Rientrano in questa categoria attività quali la disabilitazione dei servizi non necessari, l'aggiornamento costante delle patch di sicurezza, la gestione dei permessi e dei log, l'implementazione di firewall e strumenti di rilevamento delle intrusioni (IDS) e l'applicazione di policy di sicurezza. È importante sottolineare che, anche nel caso di servizi affidati a terzi, la responsabilità della sicurezza della configurazione ricade in ultima istanza sulla Pubblica Amministrazione committente.

L'ultima area coperta dalle linee guida è quella relativa alla modellazione delle minacce

e all'adozione dei principi di security by design e privacy by design [9]. In questa fase si procede all'identificazione degli asset da proteggere, alla scomposizione logica dell'applicazione, alla rilevazione delle potenziali minacce (anche attraverso l'utilizzo di framework come STRIDE) e alla definizione e validazione delle contromisure. Questo approccio sistematico permette di anticipare scenari critici e adottare misure preventive, rafforzando la postura di sicurezza complessiva delle applicazioni.

Dal punto di vista organizzativo, le linee guida delineano anche una serie di adempimenti specifici per le pubbliche amministrazioni, con particolare attenzione alle Regioni e agli enti in house. È richiesto che ciascun ente definisca internamente ruoli e competenze dedicate alla sicurezza del software, oppure che si avvalga di fornitori esterni qualificati, mantenendo comunque un presidio attivo e consapevole. Sono inoltre indicate le figure coinvolte nel processo: il Responsabile della Transizione Digitale, il Responsabile dei Sistemi Informativi e il Referente per la cybersecurity

Un elemento trasversale a tutto il documento è l'importanza della valutazione continua della sicurezza. Tale attività può essere realizzata attraverso analisi statiche e dinamiche, penetration test, code review e altri strumenti che consentono di individuare tempestivamente le vulnerabilità e monitorare nel tempo l'efficacia delle contromisure adottate. In questo contesto, risulta fondamentale anche la definizione di metriche di sicurezza, utili per quantificare il livello di esposizione al rischio e migliorare la trasparenza nei confronti degli stakeholder.

A supporto di queste pratiche, le PA sono invitate a dotarsi di strumenti operativi adeguati: policy interne formali, linee guida aziendali per la codifica sicura, sistemi di gestione delle vulnerabilità, processi strutturati per la gestione degli incidenti e piattaforme di threat modeling. La formazione continua del personale tecnico è altresì considerata una condizione essenziale per l'efficace implementazione delle linee guida.

Nel contesto della tesi, le Linee Guida AgID costituiscono le raccomandazioni sistemiche di base per la progettazione di un modello operativo di valutazione e monitoraggio della sicurezza del software. Questo modello, pensato per essere applicato dalla Regione Piemonte e dai suoi enti in house, si propone di tradurre in pratica le raccomandazioni AgID attraverso la definizione di processi, metriche e strumenti replicabili. L'adozione di un framework operativo coerente con tali linee guida permette non solo di rafforzare la sicurezza applicativa, ma anche di garantire la conformità ai requisiti di trasparenza, rendicontazione e accountability richiesti a livello normativo.

### 1.1.4 NIST.SP.800-55

Nel panorama internazionale delle metodologie per la gestione della sicurezza informatica, un contributo di primaria importanza è offerto dalle pubblicazioni del National Institute of Standards and Technology (NIST), l'agenzia federale statunitense che sviluppa standard, linee guida e buone pratiche per la tecnologia, la sicurezza informatica e l'innovazione industriale. In particolare, le *Special Publications* 800-55v1 [10] e 800-55v2 [11] propongono un quadro metodologico organico per lo sviluppo di programmi di misurazione della sicurezza delle informazioni, con l'obiettivo di supportare decisioni basate su dati oggettivi e favorire un miglioramento continuo della postura di sicurezza organizzativa.

Nella visione proposta dal NIST, la misurazione della sicurezza non si limita alla semplice verifica della presenza di controlli, ma si configura come un'attività analitica sistematica finalizzata a descrivere, quantificare e monitorare nel tempo l'efficacia delle strategie di protezione adottate. La pubblicazione SP 800-55v1 introduce una distinzione chiara tra assessment e measurement: mentre il primo può includere valutazioni qualitative soggettive, la misurazione implica la raccolta di dati quantitativi affidabili, replicabili e significativi, attraverso l'uso di tecniche analitiche rigorose. L'approccio suggerito mira a costruire sistemi di monitoraggio basati su metriche oggettive, capaci di interpretare l'evoluzione dei rischi e di adattare dinamicamente le contromisure, superando la logica di conformità formale a favore di una reale capacità di gestione del rischio.

La pubblicazione SP 800-55v2, successiva e complementare, estende questo impianto teorico delineando un modello per la creazione di veri e propri programmi strutturati di misurazione della sicurezza. Il NIST sottolinea che un programma di misurazione efficace deve essere pienamente integrato nella governance della sicurezza informatica, supportato da una leadership consapevole e orientato al conseguimento di obiettivi strategici e operativi chiari. Non si tratta dunque di raccogliere dati in modo isolato o frammentario, ma di impostare un processo sistematico, in cui la selezione delle misure, la raccolta e l'analisi dei dati e l'utilizzo delle informazioni raccolte siano strettamente coordinati.

All'interno di questo quadro metodologico, le misure di sicurezza vengono classificate in funzione della loro finalità analitica. Alcune sono pensate per verificare la corretta implementazione dei controlli, altre per valutarne l'efficacia rispetto agli obiettivi di protezione prefissati, altre ancora per analizzare l'efficienza delle risorse impiegate o per misurare gli impatti concreti delle strategie di sicurezza sull'organizzazione. Le metriche derivate da tali misure, intese come strumenti quantitativi di monitoraggio e controllo, svolgono un ruolo centrale nella gestione dinamica del rischio e nella rendicontazione della sicurezza.

Nel contesto della Pubblica Amministrazione italiana, in particolare riferendosi alla Regione Piemonte, l'adozione di un approccio strutturato alla misurazione della sicurezza delle applicazioni software rappresenta un fattore strategico di successo. La complessità crescente dei sistemi digitali, unita all'obbligo di conformità a normative nazionali ed europee sempre più stringenti, rende indispensabile disporre di strumenti di monitoraggio che permettano non solo di verificare la presenza di requisiti minimi di sicurezza, ma anche di misurare nel tempo l'effettiva capacità delle applicazioni di resistere a minacce in evoluzione.

L'approccio NIST, fondato sulla misurazione quantitativa e sull'analisi orientata ai risultati, si integra pienamente con le esigenze di gestione della sicurezza applicativa nella Pubblica Amministrazione moderna. L'applicazione dei principi descritti nelle pubblicazioni SP 800-55v1 e SP 800-55v2 consente di superare una gestione puramente documentale della sicurezza, promuovendo invece una cultura organizzativa basata sull'evidenza, sulla valutazione continua e sull'adattamento dinamico alle minacce emergenti.

Il modello operativo proposto in questa tesi si ispira ai principi delineati dal NIST per la costruzione di un sistema di valutazione della sicurezza applicativa basato su metriche robuste e significative. L'obiettivo è quello di permettere alla Regione Piemonte di analizzare in modo oggettivo l'efficacia dei controlli implementati nei software sviluppati

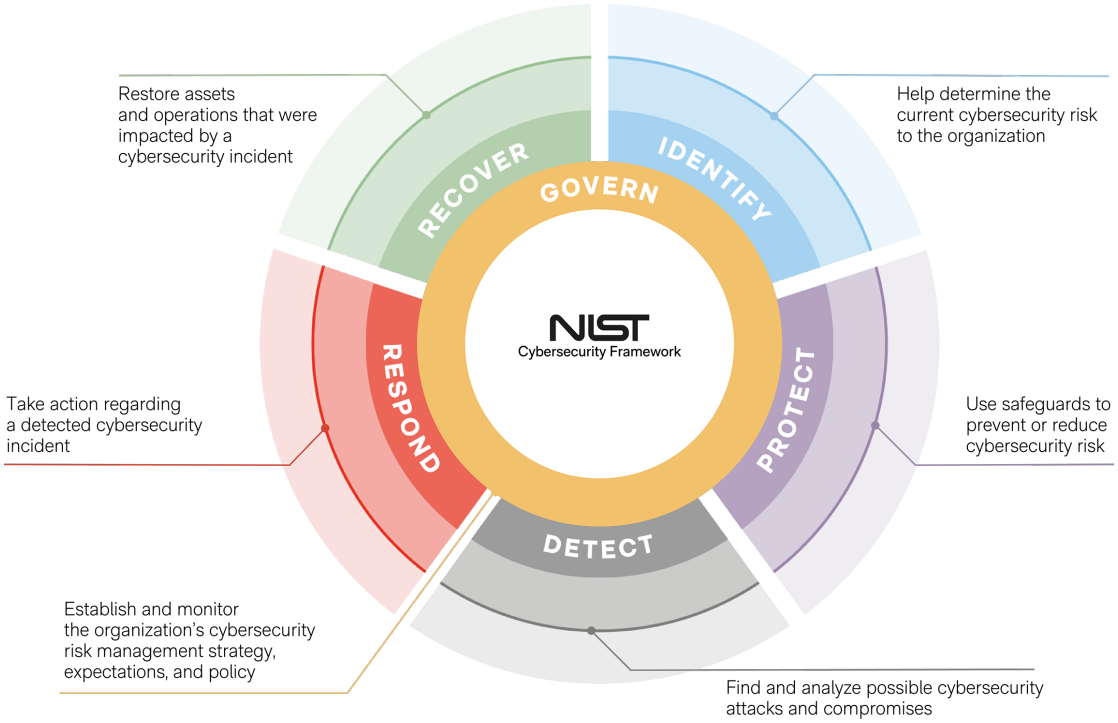


**Figura 1.2:** Pilastri del Cybersecurity Framework NIST. Fonte: Ermes Cybersecurity

o acquisiti, di individuare tempestivamente eventuali criticità, di quantificare il livello di rischio residuo e di supportare la definizione di interventi correttivi mirati. Attraverso la raccolta continua di dati e la loro interpretazione sistematica, il programma di misurazione si propone di rafforzare la capacità decisionale della governance regionale, migliorando la trasparenza interna e garantendo la rendicontazione verso gli stakeholder e gli organismi di controllo.

Come citato dagli stessi documenti, il NIST ha inoltre elaborato il Cybersecurity Framework (CSF), con il suo successivo aggiornamento CSF 2.0 , un modello ampiamente adottato a livello internazionale per la gestione strutturata del rischio informatico [12]. Il framework si basa su un approccio modulare che identifica sei funzioni principali: *Govern*, *Identify*, *Protect*, *Detect*, *Respond* e *Recover*, le quali descrivono in modo organico l'intero ciclo di gestione della sicurezza, come rappresentato in Figura 1.2. Sebbene il NIST CSF non sia stato concepito come strumento di misurazione in senso stretto, esso rappresenta una cornice metodologica fondamentale per la definizione degli obiettivi di sicurezza, per la selezione dei controlli e per la valutazione della maturità organizzativa. In particolare, il framework introduce il concetto di *Implementation Tiers* e incoraggia l'adozione di indicatori di prestazione e di rischio (KPI e KRI), strumenti indispensabili per monitorare nel tempo l'efficacia delle strategie di sicurezza. Nel prosieguo della tesi, il NIST Cybersecurity Framework sarà ripreso e approfondito come riferimento metodologico principale per la definizione dei KPI relativi alla sicurezza delle applicazioni software, in particolare considerando il suo corrispettivo documento italiano, il Framework Nazionale

per la Cybersecurity e la Data Protection [13], nato dalla collaborazione tra il Centro di Ricerca CIS di Sapienza Università di Roma e il Laboratorio Nazionale di Cybersecurity del CINI, con il supporto dell' ACN.

## 1.2 Contesto aziendale

### 1.2.1 Contesto organizzativo

L'organizzazione della Regione Piemonte è disciplinata dalla Legge Regionale 28 luglio 2008, n. 23 [14], che definisce i principi generali, i criteri e le modalità con cui si attua l'assetto degli uffici regionali, le dotazioni organiche e l'ordinamento del personale dirigente e non dirigente. Secondo tale legge, gli organi di direzione politico-amministrativa, il Consiglio regionale, investito di funzioni legislative e di indirizzo, e la Giunta regionale, con il Presidente, incaricata dell'azione esecutiva, stabiliscono programmi, linee di politica pubblica e indirizzi generali. La struttura amministrativa, invece, comprendente le direzioni e i settori, è finalizzata a tradurre queste indicazioni in atti concreti. Le direzioni regionali sono strutture organizzative stabili che assicurano un complesso organico di funzioni regionali. Esse rappresentano aree omogenee di attività dei centri di responsabilità amministrativa e , di norma, si articolano in settori. I settori sono strutture organizzative stabili preposte allo svolgimento di attività e compiti di carattere omogeneo aventi continuità operativa e autonomia organizzativa e funzionale.

In particolare, nel quadro della trasformazione digitale delle amministrazioni pubbliche, la Regione Piemonte si è dotata di un assetto organizzativo solido e articolato per la gestione dell'ICT, fondato su un modello di cooperazione istituzionale con il proprio soggetto in house, il CSI Piemonte. Questo modello, maturato nel tempo, si fonda su un'impostazione formalizzata attraverso una convenzione quadro, procedure operative condivise e ruoli ben definiti all'interno dell'organizzazione regionale.

Un ruolo cruciale viene svolto dal Settore Sistema Informativo Regionale, incardinato nella Direzione Competitività del Sistema Regionale. Esso svolge attività di governance trasversale e ha la responsabilità di programmare, guidare e controllare le azioni in ambito ICT. In particolare, gestisce la convenzione con il CSI Piemonte, valuta le configurazioni tecnico-economiche, verifica il rispetto dei livelli di servizio e delle milestone progettuali, presidia le attività di monitoraggio, congruisce il Catalogo dei Servizi annuali, conformemente a quanto richiesto dalle norme nazionali e dalle circolari AgID.

Il CSI Piemonte, costituito nel 1977 e regolato dalla legge regionale n. 48/1975 [15], agisce come soggetto esecutore della Regione in virtù della sua natura consortile. Opera in regime di controllo analogo e rappresenta un partner strategico nella realizzazione dei sistemi informativi regionali, nello sviluppo di soluzioni applicative e nella gestione di servizi ICT. La Convenzione Quadro [16], attualmente in vigore, disciplina le condizioni generali per l'affidamento di servizi, progetti e attività al CSI Piemonte. Essa costituisce la cornice giuridica e organizzativa entro cui si colloca la filiera di pianificazione, affidamento, esecuzione, monitoraggio e rendicontazione delle attività informatiche.

Gli affidamenti al CSI Piemonte si articolano in due principali modalità: da un lato, vi

sono i servizi in continuità, regolati tramite Configurazioni Tecnico-Economiche (CTE) che descrivono attività e costi ricorrenti, basati sui servizi offerti dal CSI Piemonte nel Catalogo dei Servizi annuale; dall'altro, le attività progettuali o evolutive sono definite tramite Proposte Tecnico-Economiche (PTE), documenti più articolati che prevedono uno sviluppo puntuale di requisiti, obiettivi, tempi e costi. Ogni affidamento è formalizzato attraverso specifici atti e documenti amministrativi: determina dirigenziale, disciplinare d'incarico e lettera di trasmissione. A supporto di tali atti, la convenzione e le procedure operative definiscono in dettaglio la documentazione, i ruoli, le scadenze e le modalità di controllo e verifica.

La governance dell'ICT in Regione Piemonte è strutturata secondo un modello distribuito e coordinato, nel quale ciascuna Direzione regionale è dotata di un proprio referente ICT. Questa figura, formalmente incaricata, svolge funzioni tecniche, organizzative e di raccordo tra i diversi attori del sistema informativo. Conosce in modo approfondito l'architettura dei sistemi della propria Direzione, gli applicativi in uso, i progetti in corso e le necessità evolutive ed è punto di riferimento per i colleghi interni, per il Settore Sistema Informativo Regionale e per il CSI Piemonte.

Il referente ICT affianca i RUP nella predisposizione delle richieste di servizio, nella verifica dei presupposti per il riuso o l'approvvigionamento tramite centrali di committenza, e nella definizione dei requisiti funzionali da trasmettere al fornitore. Durante la vita del progetto, partecipa alle fasi di test, verifica i documenti di congruità tecnica ed economica, monitora la qualità dei servizi resi, mantiene aggiornate le informazioni sul catalogo dei prodotti software e collabora attivamente nella promozione del riuso applicativo e nella pubblicazione dei dati sulla piattaforma Open Data. In ambito operativo, è coinvolto nella gestione dei ticket, nei contatti con il supporto tecnico CSI Piemonte e nel coordinamento delle iniziative innovative promosse a livello regionale.

Oltre alla dimensione tecnica, i referenti ICT operano anche come facilitatori e osservatori privilegiati del funzionamento del sistema. Supportano la pianificazione ICT della Direzione, promuovono la standardizzazione e l'adozione di modelli integrati, segnalano criticità e suggerimenti al Settore Sistema Informativo e svolgono un ruolo di sensibilizzazione verso colleghi e strutture sull'uso consapevole e sicuro dei servizi digitali. La loro attività si traduce in una supervisione capillare sugli applicativi e sulle soluzioni acquisite, contribuendo anche alla valutazione preliminare della sicurezza delle soluzioni, benché in assenza , ad oggi, di uno schema unificato di misurazione.

Per garantire un controllo continuo e strutturato, la Regione si è dotata di un sistema di monitoraggio tecnico-economico, che si basa su strumenti di cruscottistica per la governance dei processi informatici. Questi strumenti, alimentati con dati provenienti dal CSI Piemonte e dalle strutture regionali, permettono al Settore SIRe di verificare lo stato di avanzamento dei servizi, rilevare eventuali scostamenti o anomalie, monitorare le performance e raccogliere indicatori utili alla valutazione complessiva delle attività ICT. Il Responsabile del Monitoraggio, figura prevista dalle procedure operative, supervisiona l'intero processo, affiancato da un gruppo di supporto tecnico interno.

Nel caso di affidamenti progettuali, è prassi che i referenti ICT, insieme ai RUP, redigano una scheda tecnica con i requisiti applicativi attesi, collaborino alla stesura della PTE con il CSI Piemonte, verifichino la coerenza con il catalogo e la congruità dell'offerta e

partecipino all'accettazione dei SAL. Il Settore SIRe mantiene un ruolo centrale nel validare le PTE, assicurando omogeneità nell'applicazione delle policy e dei criteri di controllo, anche in relazione ai vincoli di bilancio e programmazione.

Il Responsabile dei Sistemi Informativi svolge anche le funzioni di Referente regionale per la cybersecurity dell'Ente, in coerenza con quanto richiesto dalla normativa nazionale, in particolare dalla Legge 90/2024 [2]. Lavora in stretta sinergia con il referente per la sicurezza del CSI Piemonte, che presidia e coordina lo CSIRT regionale, con cui condivide le attività di gestione degli incidenti, aggiornamento delle policy, verifica dei sistemi crittografici e recepimento delle indicazioni dell'ACN. Questo collegamento rafforza l'integrazione tra ente e fornitore, migliorando la capacità di reazione e coordinamento in caso di minacce o vulnerabilità.

Nel sistema ICT regionale, il monitoraggio del software rappresenta una componente cruciale per garantire la continuità operativa, la conformità contrattuale e, sempre più, la sicurezza applicativa. Sebbene non esista ancora un modello formalizzato e omogeneo di valutazione tecnica della sicurezza, la Regione Piemonte ha sviluppato nel tempo una serie di strumenti e pratiche che consentono un controllo costante sulle soluzioni software in esercizio. Il monitoraggio avviene su più livelli: da quello amministrativo, legato alla verifica dei SAL, all'osservazione della qualità del servizio resa tramite indicatori di performance (KPI), fino alla rilevazione di eventuali anomalie o regressioni funzionali, anche grazie al dialogo diretto con gli utenti finali interni alle Direzioni. I sistemi di cruscottistica e anagrafica applicativa, alimentati da dati provenienti dal CSI Piemonte e integrati con informazioni raccolte dai referenti ICT, svolgono funzioni centrali nella rappresentazione sintetica dello stato di salute dei servizi applicativi. A questo si affianca un sistema di raccolta strutturata delle non conformità, delle segnalazioni di disservizio e delle criticità emerse durante le fasi di collaudo o nella gestione operativa. Inoltre, i referenti ICT sono tenuti a monitorare l'adeguatezza delle soluzioni acquisite rispetto ai fabbisogni espressi in fase di definizione dei requisiti, contribuendo a individuare scostamenti rispetto a quanto pianificato.

In tale contesto, si delinea un ecosistema informativo pubblico fortemente interconnesso, nel quale il modello operativo si fonda sulla cooperazione continua tra i referenti ICT, il Settore Sistema Informativo Regionale, i dirigenti responsabili e il CSI Piemonte. Tale struttura ha consentito alla Regione di garantire negli anni una gestione ordinata, trasparente e tracciabile del ciclo ICT, nonostante un organigramma aziendale complesso e con una molteplicità di attori, come mostrato in Figura 1.3. Tuttavia, la crescente complessità del panorama normativo, impone oggi un ulteriore salto qualitativo verso modelli di governance incentrati non solo sull'erogazione dei servizi e l'analisi delle loro componenti funzionali, ma anche sulla misurazione continua del livello di sicurezza.

Proprio in questa direzione si muove la presente tesi, che propone un modello tecnico-organizzativo per la valutazione e il monitoraggio della sicurezza del software in uso presso la Regione Piemonte. Tale modello non si sovrappone all'esistente, ma si innesta su di esso, sfruttando le strutture operative già presenti, valorizzando le competenze dei referenti ICT, e integrandosi con le procedure di affidamento e monitoraggio già consolidate. Il contesto aziendale, con le sue articolazioni e i suoi strumenti, fornisce dunque le basi concrete su cui costruire un sistema efficace di rendicontazione della sicurezza, orientato all'evidenza,

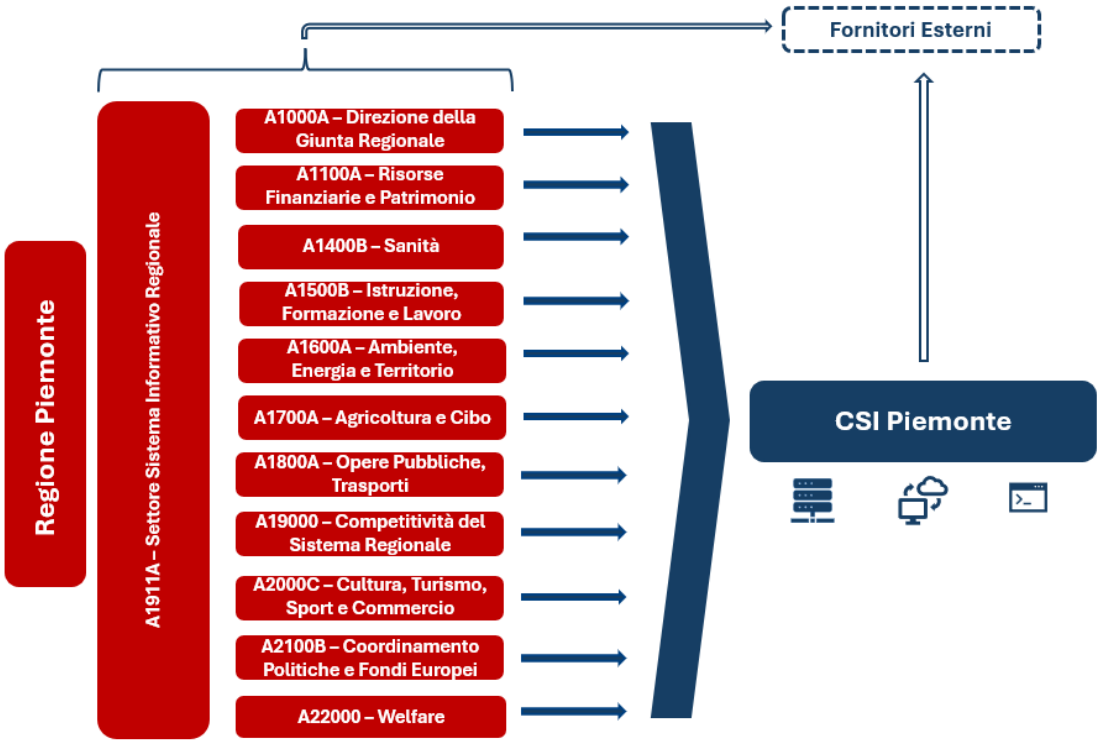


**Figura 1.3:** Organigramma di massima delle strutture della Regione Piemonte. Elaborazione dell'autore

alla trasparenza e alla gestione pro-attiva del rischio.

### 1.2.2 Progetti correlati

Un'iniziativa di particolare rilevanza nel percorso di rafforzamento della sicurezza ICT regionale è rappresentata dal programma *Transizione Digitale e Servizi Sicuri*, promosso dalla Regione Piemonte e finanziato nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR), Missione 1, Componente 1, Investimento 1.5 dedicato alla cybersecurity. Questo programma si inserisce in un quadro più ampio di strategie nazionali ed europee volte a innalzare la resilienza dei sistemi pubblici, fornendo risorse e strumenti concreti per affrontare le crescenti minacce informatiche che coinvolgono la Pubblica Amministrazione. L'obiettivo complessivo è quello di garantire che gli enti regionali possano disporre non solo di infrastrutture sicure, ma anche di modelli organizzativi e operativi capaci di prevenire, monitorare e mitigare i rischi.

All'interno del programma, un intervento di particolare interesse per il presente lavoro è quello denominato *Realizzazione di strumenti di analisi delle vulnerabilità nella filiera di automation ed interventi di mitigazione*. Esso si propone di integrare nella catena di

produzione del software regionale strumenti automatici per la verifica della qualità e della sicurezza del codice sorgente, includendo sia l'analisi statica del codice sia il controllo delle dipendenze e delle librerie esterne. L'approccio adottato è in linea con i principali standard internazionali, come le linee guida OWASP Top 10, e si inserisce nel paradigma del continuous vulnerability management, che mira a rendere la sicurezza una componente strutturale del ciclo di vita del software e non un requisito secondario.

L'elemento innovativo dell'intervento risiede proprio nella sua integrazione con la filiera DevOps regionale. L'automazione delle verifiche permette infatti di trasformare la sicurezza da controllo episodico a processo continuo, garantendo che ogni nuova release del software venga accompagnata da analisi aggiornate sulle vulnerabilità e che i risultati possano essere tempestivamente tradotti in azioni di remediation. Tale scelta non ha soltanto un valore tecnologico, ma anche organizzativo, poiché comporta un cambiamento di cultura aziendale significativo: gli sviluppatori e i referenti ICT sono chiamati a confrontarsi con strumenti che rendono visibili in tempo reale i punti di forza e le criticità del software, contribuendo a diffondere una maggiore consapevolezza sui rischi e sulle pratiche di security by design.

In questo senso, l'intervento si collega direttamente agli obiettivi della tesi. Il modello di metriche e KPI proposto nel lavoro trova infatti un naturale punto di confronto con le soluzioni introdotte dal progetto regionale. Da un lato, le dashboard e i report prodotti dagli strumenti di analisi automatica possono costituire un riferimento concreto per la misurazione di alcuni indicatori; dall'altro, il modello elaborato in questa ricerca permette di collocare tali misurazioni in un quadro più ampio, integrando i risultati tecnici con valutazioni di carattere organizzativo e normativo. Il riferimento a questo progetto assume dunque una valenza strategica poiché fornisce un termine di paragone operativo con cui validare la coerenza e la solidità delle metriche sviluppate, ma al tempo stesso offre un contesto reale in cui le proposte della tesi possono trovare applicazione.

# Capitolo 2

# Definizione del problema e obiettivi

Il presente capitolo affronta il tema della sicurezza applicativa nella Pubblica Amministrazione, con particolare riferimento al contesto operativo della Regione Piemonte. La sicurezza del software rappresenta oggi una componente essenziale della qualità e dell'affidabilità dei servizi digitali pubblici, ma la sua gestione continua a presentare limiti significativi legati alla frammentazione organizzativa, alla mancanza di metriche oggettive e alla difficoltà di garantire un monitoraggio continuo nel tempo. A partire da queste premesse, il capitolo delinea un quadro analitico volto a giustificare la necessità di un approccio più maturo e strutturato alla gestione della sicurezza applicativa. Dopo aver descritto il contesto nazionale e regionale, vengono approfondite le principali criticità del modello attuale, evidenziando come la sicurezza sia spesso trattata come un requisito accessorio piuttosto che come un elemento integrante dei processi di sviluppo e gestione del software. Da questa analisi emerge l'esigenza di un modello operativo scalabile, capace di rendere la sicurezza un processo sistematico, misurabile e sostenibile, adattabile alla complessità del sistema informativo regionale. Il capitolo esplora inoltre il ruolo dei diversi attori coinvolti, sottolineando l'importanza di una governance collaborativa basata su responsabilità condivise e flussi informativi strutturati. Infine, il capitolo introduce gli obiettivi della tesi, che costituiscono la sintesi delle necessità individuate e il punto di partenza per la costruzione del modello operativo. Tali obiettivi si concretizzano nella definizione delle metriche di sicurezza, nella progettazione del sistema di rendicontazione e nello sviluppo del sistema di monitoraggio e controllo, anticipando così il percorso di progettazione e validazione descritto nei capitoli successivi.

## 2.1 Sfide della sicurezza del software nella Pubblica Amministrazione

Negli ultimi anni, la sicurezza informatica si è affermata come una delle sfide più complesse e decisive per la Pubblica Amministrazione. L'accelerazione della trasformazione digitale,

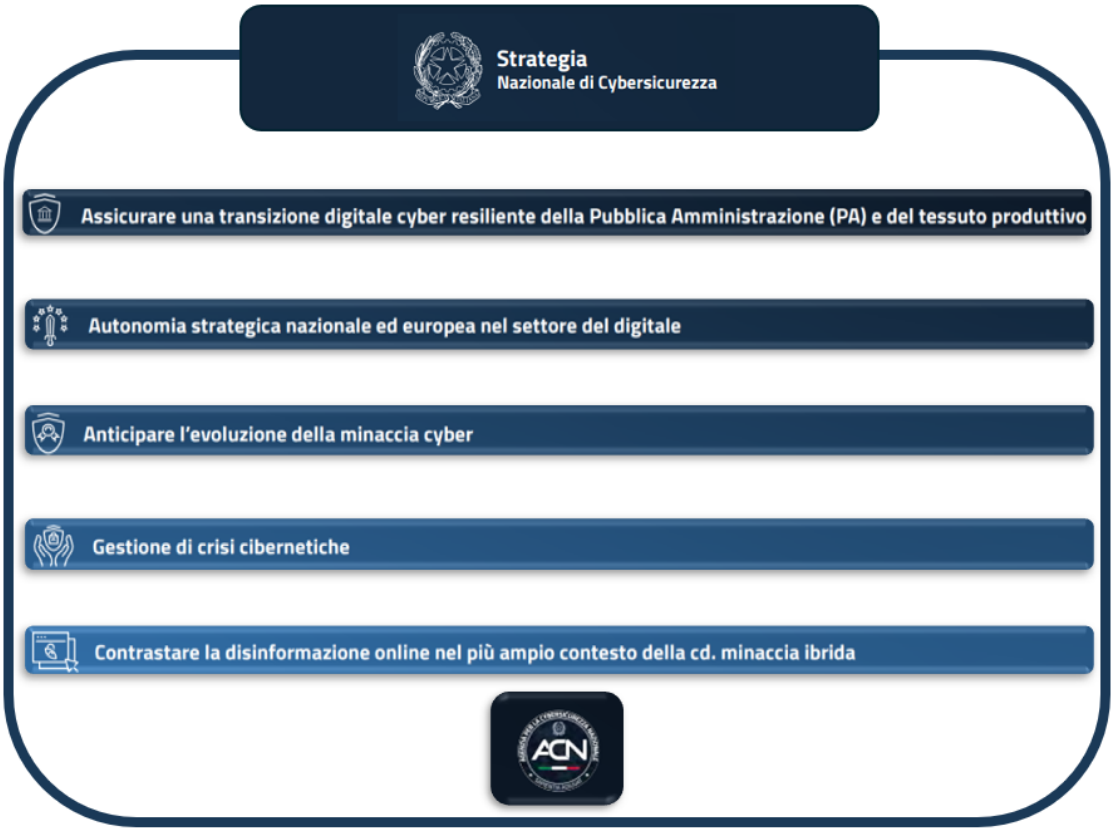


**Figura 2.1:** Principali sfide da affrontare secondo la Strategia Nazionale di Cybersicurezza 22-26. Elaborazione dell'autore

sostenuta dai programmi del PNRR e dalle strategie nazionali sulla cybersecurity, ha infatti ampliato in modo significativo la superficie d'attacco dei sistemi informativi pubblici, rendendo evidente quanto la protezione del software e dei dati sia oggi un elemento strutturale della continuità operativa e della fiducia dei cittadini verso le istituzioni. Le amministrazioni pubbliche, tradizionalmente caratterizzate da una forte eterogeneità tecnologica e da una molteplicità di fornitori, si trovano a dover affrontare minacce sempre più sofisticate in un contesto normativo e organizzativo in rapida evoluzione.

La Strategia Nazionale di Cybersicurezza 2022–2026 [17], promossa dall'ACN, sottolinea come la sicurezza non possa più essere considerata un aspetto tecnico confinato ai reparti ICT, ma debba diventare una componente trasversale della governance pubblica. Essa introduce il concetto di resilienza digitale, intesa come la capacità di un'organizzazione di anticipare, assorbire e rispondere efficacemente a incidenti informatici, garantendo nel contempo la continuità dei servizi essenziali. Il riferimento alle principali sfide da affrontare in ambito cybersecurity secondo la Strategia è rappresentato in Figura 2.1. In parallelo, il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024–2026 [18], redatto da AgID, evidenzia l'urgenza di integrare la security by design in tutte le fasi del ciclo di

vita dei servizi digitali, superando l'approccio reattivo basato su interventi post-incidente. La logica che emerge è quella di un sistema pubblico che deve essere non solo conforme alle norme, ma anche capace di misurare, monitorare e migliorare costantemente il proprio livello di sicurezza.

All'interno di questo scenario, la sicurezza del software assume una rilevanza centrale. Le applicazioni costituiscono il punto di interfaccia tra i cittadini, le imprese e le amministrazioni e rappresentano quindi uno dei principali vettori di rischio. La maggior parte delle vulnerabilità che sfociano in incidenti di sicurezza deriva, infatti, da errori di sviluppo, configurazioni errate o dipendenze da librerie di terze parti non aggiornate. La crescente diffusione di architetture a microservizi, l'utilizzo di framework open source e l'adozione massiva del cloud computing rendono la catena di fornitura del software sempre più complessa e distribuita, ponendo nuove sfide in termini di controllo, responsabilità e trasparenza. La PA si trova quindi nella necessità di dotarsi di strumenti e metodologie che permettano di valutare in modo oggettivo la sicurezza delle proprie applicazioni, sia in fase di sviluppo sia durante l'intero ciclo di vita operativo.

Nonostante i progressi compiuti negli ultimi anni, le pubbliche amministrazioni italiane continuano a scontare alcune criticità strutturali che ostacolano una gestione matura della sicurezza applicativa. In primo luogo, l'eterogeneità dei sistemi informativi e la coesistenza di sistemi legacy con soluzioni di nuova generazione generano complessità e difficoltà di integrazione. Spesso gli enti tendono a sviluppare e gestire in modo autonomo i propri applicativi, con livelli di sicurezza che possono risultare non sempre uniformi. Questa diversificazione tecnologica e organizzativa genera un ecosistema distribuito di applicazioni, infrastrutture e fornitori, all'interno del quale può essere complesso mantenere una visione unitaria del rischio informatico. Le piattaforme regionali e gli applicativi verticali operano infatti in contesti eterogenei, caratterizzati da differenti livelli di maturità, ambienti di esercizio e modelli di gestione. Tale situazione può comportare una minore coerenza nei processi di controllo e rendicontazione, con possibili effetti sulla capacità degli enti di pianificare e monitorare in modo pienamente efficace le proprie politiche di sicurezza.

In questo scenario si aggiunge una limitata integrazione dei processi di sicurezza all'interno dei flussi DevOps: la protezione del software è ancora concepita come un'attività successiva allo sviluppo e non come parte integrante del ciclo di progettazione, test e rilascio. Questo approccio a valle comporta tempi di reazione più lunghi, costi maggiori di correzione e una minore capacità predittiva. Lo stesso Piano Strategico ICT 2024–2026 della Regione Piemonte [19] evidenzia la necessità di colmare questo divario attraverso la progressiva adozione di modelli di sviluppo DevSecOps e l'introduzione di processi di analisi automatica del codice e delle dipendenze software già nelle fasi di costruzione delle applicazioni.

Un'ulteriore criticità riguarda la difficoltà di controllare in modo diretto la sicurezza del codice e delle infrastrutture sottostanti. Gran parte del software della PA è infatti sviluppato o gestito da società in house o da fornitori terzi. La gestione della supply chain del software diventa quindi un elemento chiave: è necessario garantire la tracciabilità delle componenti, la valutazione delle librerie esterne e la verifica periodica delle vulnerabilità emergenti. In questo senso, le strategie ACN e AgID insistono sulla necessità di adottare processi strutturati di Software Bill of Materials (SBOM) e di continuous vulnerability

management per assicurare una visibilità costante sul patrimonio applicativo e sulle sue dipendenze.

Altro punto debole è rappresentato dall'assenza, in molte amministrazioni, di metriche condivise per la misurazione della sicurezza. Le valutazioni avvengono spesso attraverso audit o checklist qualitative, che non consentono un confronto oggettivo tra progetti o fornitori né un monitoraggio nel tempo. L'introduzione di indicatori di performance (KPI) quantitativi e standardizzati è dunque un passaggio necessario per rendere la sicurezza un elemento misurabile, verificabile e, di conseguenza, gestibile. Tale esigenza è esplicitamente richiamata nel Piano Strategico ICT regionale, che propone di rafforzare la capacità di misurazione attraverso strumenti di governance e reporting strutturati, in linea con i modelli internazionali proposti dal NIST.

Congiuntamente alle dimensioni tecniche e organizzative, non va trascurato l'aspetto umano. La cultura della sicurezza rappresenta uno dei fattori più critici: carenza formativa da parte di sviluppatori, dirigenti e personale operativo può vanificare anche le migliori soluzioni tecnologiche. I documenti strategici più recenti nel panorama nazionale insistono sul rafforzamento delle competenze e sulla formazione continua, promuovendo la creazione di reti di esperti di materia specializzati in sicurezza, in grado di fungere da punti di raccordo tra le strutture operative e le funzioni di governance.

Parallelamente, l'evoluzione delle minacce rende lo scenario ancora più dinamico e complesso. Gli attacchi alla PA si sono moltiplicati sia in frequenza che in sofisticazione, includendo ransomware, campagne di phishing mirato, sfruttamento di vulnerabilità zero-day e compromissioni della supply chain. La pubblicazione continua di nuove *Common Vulnerabilities and Exposures* (CVE) impone un monitoraggio costante e la capacità di intervenire tempestivamente con azioni di mitigazione e aggiornamento. L'esperienza recente mostra come incidenti anche apparentemente minori possano generare effetti sistemici, mettendo fuori servizio piattaforme critiche e compromettendo la fiducia dell'utenza.

In risposta a queste sfide, le politiche di sicurezza stanno evolvendo verso modelli basati sul monitoraggio continuo e sull'automazione dei controlli. L'obiettivo non è più soltanto garantire la conformità normativa, ma costruire un ecosistema digitale resiliente e adattivo, capace di apprendere e migliorare nel tempo. L'integrazione di strumenti di analisi automatica del codice (SAST), di controllo delle dipendenze (SCA) e di testing dinamico (DAST) rappresenta oggi una delle direttrici principali della trasformazione dei processi di sviluppo nella PA. Questi strumenti, se integrati in pipeline DevSecOps, permettono di identificare vulnerabilità sin dalle prime fasi del ciclo di vita del software e di mantenere nel tempo un quadro aggiornato della sicurezza applicativa. La prospettiva è quella di implementare dei meccanismi di automazione della sicurezza che riducano l'intervento umano alle sole attività di validazione, consentendo maggiore tempestività e riducendo il rischio di errore.

Nel contesto della Regione Piemonte, tali linee evolutive trovano una declinazione concreta non solo nel Piano Strategico ICT 2024–2026 [19], che evidenzia la cybersecurity come un pilastro fondamentale del Piano, come mostrato in Figura 2.2, ma anche nel Piano Attuativo ICT 2024–2026, aggiornamento 2025 [20], che rappresenta lo strumento operativo di implementazione delle azioni previste a livello strategico dell'Ente a tema ICT. Il Piano Attuativo definisce obiettivi specifici, tempistiche e indicatori per il rafforzamento

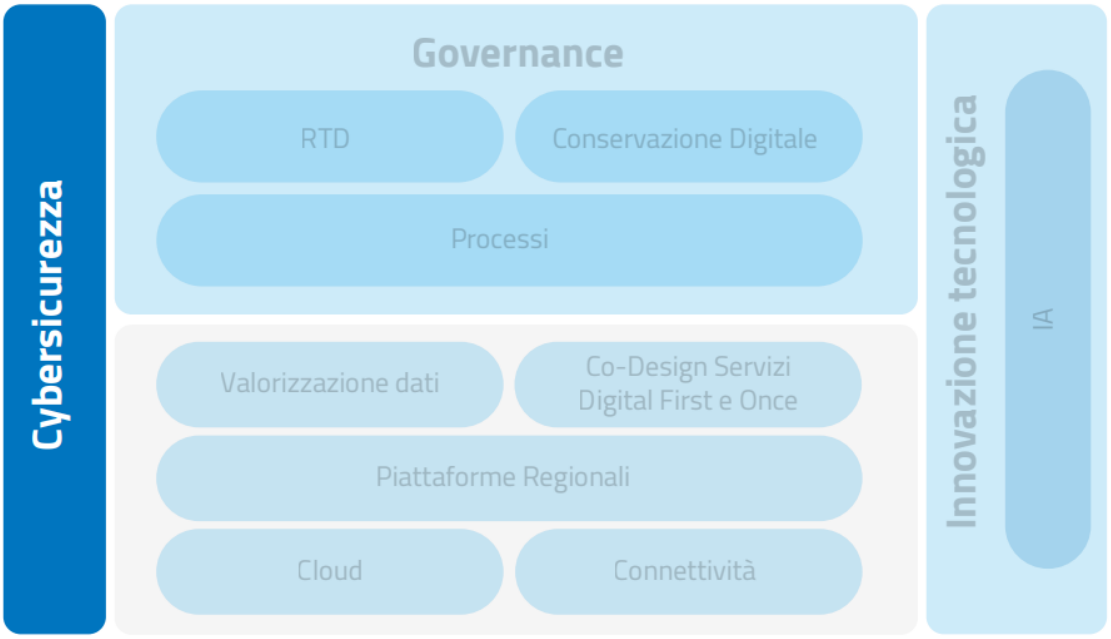


**Figura 2.2:** Pilastri del Piano Strategico ICT 24-26 della Regione Piemonte con focus sulla cybersicurezza. Fonte: Piano Strategico pluriennale ICT 2024-2026 della Regione Piemonte

della sicurezza informatica regionale, con particolare attenzione all'armonizzazione delle pratiche di gestione e monitoraggio tra le diverse direzioni. Esso mira a consolidare un modello integrato di sicurezza, fondato su tre assi principali: la gestione proattiva delle vulnerabilità, l'adozione di strumenti di analisi automatizzata e la definizione di processi di governance coordinata tra il Settore SIRe e i referenti ICT. Tale documento si pone quindi come punto di raccordo tra la dimensione strategica e quella operativa, favorendo un allineamento continuo con gli standard nazionali ed europei.

Il Piano Attuativo rafforza inoltre l'attenzione verso la coerenza architetturale e la riduzione della frammentazione applicativa, promuovendo la razionalizzazione dei sistemi e la centralizzazione di alcune funzioni di monitoraggio e controllo. Questa direzione di marcia è essenziale per superare le inefficienze legate alla dispersione delle competenze e alla mancanza di una visione unitaria sul ciclo di vita del software. In tale ottica, il modello proposto da questa tesi si inserisce come strumento complementare al Piano Attuativo, fornendo un approccio metodologico e misurabile alla valutazione della sicurezza applicativa.

In conclusione, le sfide che la Pubblica Amministrazione deve affrontare nel campo della sicurezza del software non riguardano solo la complessità tecnologica, ma anche la capacità di costruire modelli organizzativi e metodologici che traducano le strategie nazionali e regionali in pratiche operative sostenibili. La prospettiva che emerge è quella di una sicurezza misurabile, automatizzata e adattiva, in cui la valutazione delle vulnerabilità

e il controllo della qualità del software diventano parte integrante della gestione ordinaria dei sistemi informativi. È su questo terreno che si innesta il modello proposto in questa tesi, volto a fornire strumenti concreti per misurare, rendicontare e migliorare la sicurezza applicativa nel contesto pubblico regionale, in coerenza con le linee strategiche nazionali e con le migliori pratiche internazionali.

## 2.2 Limiti degli approcci correnti alla sicurezza del software

Pur avendo registrato importanti progressi, l'approccio alla sicurezza del software nella Pubblica Amministrazione italiana rimane ancora largamente reattivo, frammentato e difficilmente misurabile. Le strategie nazionali e regionali forniscono un quadro di riferimento chiaro e coerente, ma la loro piena attuazione incontra ostacoli legati a fattori tecnologici, organizzativi e culturali. La sicurezza è spesso percepita come un requisito accessorio, da gestire a valle dei processi di sviluppo e non come un elemento costitutivo della qualità del software. Tale impostazione genera disallineamenti tra indirizzi strategici e pratiche operative, con conseguenze dirette sulla capacità delle amministrazioni di prevenire e gestire in modo efficace gli incidenti di sicurezza, evidenziando dei limiti agli approcci correnti alla sicurezza del software, descritti di seguito e rappresentati graficamente in Figura 2.3.

Uno dei limiti principali risiede nella prevalenza di modelli di sicurezza basati su interventi *ex post*, fondati su verifiche occasionali, audit periodici o risposte emergenziali a incidenti già avvenuti. Questo approccio, sebbene funzionale al rispetto di requisiti di conformità normativa, si rivela insufficiente in un contesto caratterizzato da minacce dinamiche e da un'elevata velocità di rilascio del software. La mancanza di strumenti di analisi automatica e di processi di monitoraggio impedisce di individuare tempestivamente le vulnerabilità introdotte durante le fasi di sviluppo e aggiornamento. In molti casi, la sicurezza viene delegata alla fase di esercizio, quando le possibilità di intervento sono più limitate e i costi di remediation significativamente più elevati. L'assenza di una cultura della prevenzione rende inoltre difficile stabilire priorità di intervento basate su criteri di rischio e impatto reale.

Un secondo limite strutturale riguarda la scarsa integrazione tra sviluppo e sicurezza. Nei processi tradizionali, le pratiche DevOps adottate da amministrazioni e società in house non incorporano in modo sistematico controlli di sicurezza automatizzati. L'adozione del paradigma DevSecOps rimane parziale e disomogenea: solo in pochi casi strumenti di analisi statica del codice (SAST) o di analisi delle componenti software (SCA) sono integrati nei flussi CI/CD. Ciò comporta che la sicurezza del codice dipenda ancora in larga parte da competenze individuali o da verifiche manuali, con una limitata tracciabilità e una scarsa ripetibilità dei controlli. La conseguenza è una catena di fornitura del software vulnerabile, nella quale risulta difficile certificare la sicurezza delle componenti e monitorarne l'evoluzione nel tempo.

Questa situazione è riscontrabile anche nel contesto della Regione Piemonte, dove numerosi servizi in ambito informatico sono erogati dal CSI Piemonte. Pur in presenza di


**Figura 2.3:** Vista dei limiti degli approcci alla sicurezza del software nella Pubblica Amministrazione. Elaborazione dell'autore

processi consolidati per la gestione dei progetti ICT, le verifiche sulla sicurezza applicativa non risultano ancora pienamente integrate e sistematizzate all'interno delle procedure di sviluppo. I controlli di sicurezza sono condotti principalmente nelle fasi finali di collaudo o in occasione di rilasci significativi, mentre manca un sistema strutturato di analisi continua in grado di rilevare tempestivamente vulnerabilità e non conformità. Ne consegue che la valutazione del rischio si concentra su momenti puntuali, senza garantire una visione evolutiva della sicurezza nel tempo.

Un ulteriore elemento di debolezza è la disomogeneità dei requisiti di sicurezza tra fornitori e amministrazioni. Ogni ente tende a definire propri standard minimi e modalità di verifica, spesso basate su checklist qualitative o autocertificazioni. Anche a livello regionale, le modalità di controllo applicate ai progetti ICT non sono sempre uniformi. L'assenza di criteri condivisi rende difficile comparare i livelli di sicurezza dei diversi applicativi e limita la possibilità di costruire un quadro complessivo di rischio. Inoltre, la diversificazione contrattuale tra enti, società in house e fornitori esterni contribuisce a mantenere un certo grado di disomogeneità, rendendo più complessa l'adozione di metriche comuni o di livelli minimi di sicurezza condivisi.

Questo problema si riflette in modo diretto anche nella fase di valutazione della congruità delle offerte tecnico-economiche, che rappresenta il momento in cui le proposte dei fornitori vengono esaminate prima dell'affidamento. In questa fase, sebbene vengano considerati

aspetti funzionali, economici e qualitativi, la componente di sicurezza non è ancora oggetto di una valutazione pienamente strutturata e misurabile. L'analisi si basa prevalentemente su metriche qualitative o su riferimenti generici alla conformità a standard di settore, senza il supporto di metriche o indicatori quantitativi che permettano di verificare in modo oggettivo la solidità delle soluzioni proposte. Ne consegue che la sicurezza tende talvolta a essere considerata implicitamente soddisfatta, in assenza di un esplicito processo di valutazione dei parametri inerenti ai prodotti oggetto delle offerte.

Questa lacuna metodologica determina un duplice effetto: da un lato riduce la capacità della Pubblica Amministrazione di orientare i fornitori verso pratiche di sviluppo sicuro, dall'altro indebolisce le fasi di validazione, che dovrebbero costituire un presidio preventivo contro l'introduzione di vulnerabilità nella catena applicativa. L'introduzione di un sistema di metriche di sicurezza, come quello proposto nella presente tesi, si propone di rafforzare l'attuale processo di valutazione, attraverso l'impiego di strumenti oggettivi di analisi sin dalla fase di affidamento.

Il tema della misurabilità della sicurezza rappresenta un ulteriore punto debole. Sebbene gli standard internazionali, come NIST e OWASP, forniscano un repertorio consolidato di controlli e indicatori, la loro applicazione nella PA è ancora limitata e prevalentemente qualitativa. La valutazione della sicurezza avviene spesso in termini di conformità o adempimento, piuttosto che di performance o di risultato. Mancano indicatori oggettivi che permettano di quantificare il livello di esposizione o di misurare il miglioramento nel tempo. Di conseguenza, non è possibile disporre di cruscotti di controllo o di sistemi di reporting che restituiscano una visione sintetica ma accurata della postura di sicurezza complessiva dell'ente.

Sul piano organizzativo, emerge l'opportunità di rafforzare il coordinamento tra i diversi attori coinvolti nella gestione della sicurezza. Le responsabilità, oggi distribuite tra più livelli, potrebbero beneficiare di un modello di governance più chiaro e condiviso, volto a rendere più efficaci e integrati i processi di sicurezza applicativa. In assenza di un sistema di monitoraggio unificato e di canali di comunicazione strutturati, le informazioni relative alle vulnerabilità, agli incidenti o agli interventi di mitigazione tendono a rimanere confinate all'interno delle singole strutture operative. Ciò genera inefficienze, duplicazioni e ritardi nella gestione delle minacce. Il modello proposto nella tesi si colloca proprio in risposta a tale criticità, promuovendo la creazione di una rete di referenti ICT e di cybersecurity come leva per garantire una gestione coordinata e una visione condivisa della sicurezza a livello regionale.

Un altro aspetto rilevante riguarda il monitoraggio nel tempo delle applicazioni, che nella pratica corrente è limitato alla fase di rilascio dei prodotti, come evidenziato dalla Figura 2.4. Una volta completato il collaudo e messo in esercizio un software, non sono previsti controlli periodici strutturati per verificarne il mantenimento del livello di sicurezza. Le attività di verifica avvengono, nella maggior parte dei casi, solo in occasione di nuovi rilasci o aggiornamenti significativi, lasciando scoperto l'intervallo operativo tra una versione e l'altra. Questa modalità di gestione *a cicli chiusi* risulta inadeguata in un contesto in cui le vulnerabilità emergono continuamente, anche su componenti di terze parti già distribuite. La mancanza di un sistema di monitoraggio sulla sicurezza informatica riduce la capacità dell'ente di individuare tempestivamente nuove minacce e di intervenire con

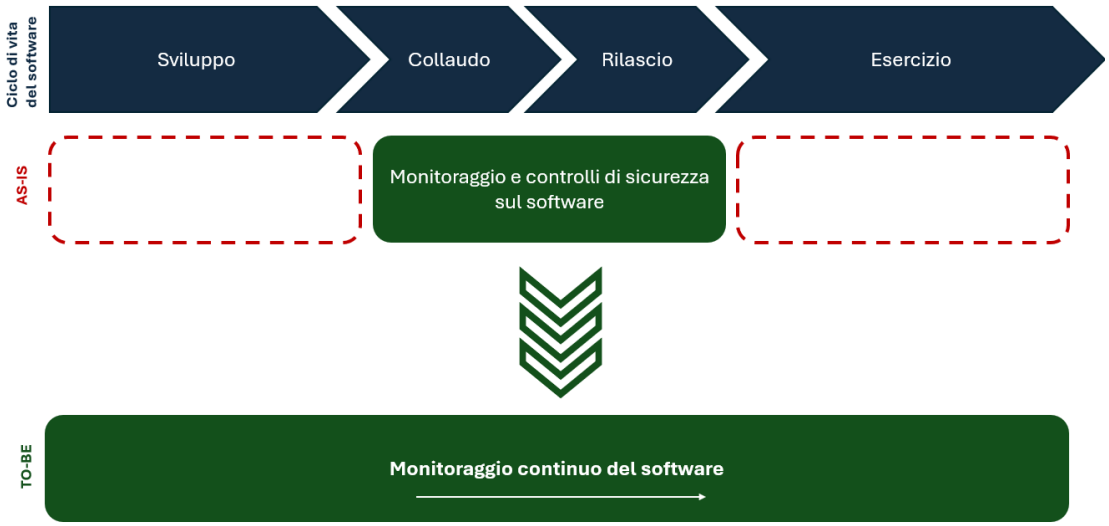


**Figura 2.4:** Stato attuale e modello auspicato di monitoraggio della sicurezza lungo il ciclo di vita del software in Regione Piemonte

azioni di mitigazione efficaci.

In questo quadro, la Regione Piemonte riconosce la necessità di passare da un modello statico di controllo a uno dinamico e automatizzato, che integri la raccolta di dati di sicurezza con meccanismi di segnalazione e risposta rapida. Tuttavia, la piena realizzazione di tale paradigma richiede la definizione di metriche standardizzate e di processi di rendicontazione strutturati, che consentano di trasformare le informazioni tecniche in evidenze misurabili e confrontabili nel tempo.

Accanto alle carenze tecniche e metodologiche, si evidenzia anche una più ampia mancanza di cultura della misurazione. Nelle amministrazioni pubbliche, la sicurezza è raramente oggetto di indicatori di performance o di rendicontazione sistematica. Mentre per ambiti come la spesa ICT o la qualità dei servizi esistono metriche consolidate e strumenti di monitoraggio, la sicurezza resta un'area scarsamente quantificata. Questa carenza genera difficoltà nel dimostrare l'efficacia delle misure adottate e nel giustificare gli investimenti necessari al loro mantenimento. Di conseguenza, la sicurezza viene spesso percepita come un costo inevitabile piuttosto che come un fattore abilitante dell'innovazione e della qualità dei servizi pubblici digitali.

Dal punto di vista metodologico, emerge infine la mancanza di modelli operativi scalabili. Le iniziative di sicurezza si concentrano frequentemente su progetti di grande impatto o di elevata criticità, trascurando applicazioni di minore complessità ma ugualmente esposte a rischio. Gli strumenti e le metodologie attualmente disponibili non sempre consentono un adattamento proporzionato alla dimensione dei progetti o alle risorse disponibili. Da questo scenario deriva una disomogeneità nella capacità di controllo e nella distribuzione

degli sforzi, con aree altamente monitorate e altre completamente prive di strumenti di valutazione. Il principio di proporzionalità fatica a tradursi in pratiche operative efficaci, soprattutto nei contesti locali e territoriali.

Nel complesso, i limiti degli approcci correnti alla sicurezza del software nella Pubblica Amministrazione derivano dalla difficoltà di tradurre gli indirizzi strategici in processi misurabili e automatizzabili. Superare tali limiti significa adottare un modello più maturo, basato su misurazione oggettiva, automazione e governance integrata. In questa prospettiva, il lavoro proposto in questa tesi intende contribuire alla costruzione di un modello operativo che renda la sicurezza applicativa un elemento strutturale, misurabile e continuamente migliorabile all'interno del ciclo di vita dei sistemi informativi pubblici.

## 2.3 Necessità di un modello operativo scalabile

L'analisi dei limiti strutturali e organizzativi che caratterizzano l'attuale gestione della sicurezza applicativa nella Pubblica Amministrazione, in particolare nel contesto della Regione Piemonte, evidenzia la necessità di un cambiamento di paradigma. Le sfide illustrate nei paragrafi precedenti, dalla frammentazione dei processi alla mancanza di metriche condivise, dalla disomogeneità delle verifiche alla difficoltà di garantire un controllo costante nel tempo, convergono verso un'unica esigenza: quella di disporre di un modello operativo che renda la sicurezza del software un processo sistematico, misurabile e adattabile. In altre parole, un modello che sia al contempo scalabile dal punto di vista tecnico, organizzativo e procedurale, capace di essere applicato in contesti differenti senza perdere coerenza metodologica né sostenibilità operativa.

Nel caso della Regione Piemonte, la complessità del sistema informativo regionale e la distribuzione delle responsabilità tra più attori, raffigurati in Figura 2.5, rendono evidente come la gestione della sicurezza non possa essere affidata a interventi puntuali o a valutazioni episodiche. L'attuale modalità di lavoro, basata su processi di verifica concentrati nella fase di rilascio delle applicazioni, non consente di garantire un livello di controllo costante e aggiornato sul parco software in esercizio. Il modello tradizionale, in cui la sicurezza è trattata come un requisito collaterale da valutare in chiusura di progetto, mostra oggi le sue potenziali criticità di fronte alla crescente dinamicità delle minacce e alla necessità di reagire in tempi rapidi.

A queste considerazioni si aggiunge la constatazione che, nelle procedure di affidamento e valutazione tecnica delle offerte, la sicurezza non viene ancora trattata come elemento oggettivamente misurabile. Le verifiche di congruità tecnico-economica effettuate sui progetti affidati al CSI Piemonte e ai fornitori terzi, sebbene precise sul piano amministrativo, non contemplano metriche strutturate di sicurezza applicativa. Ne consegue che, nella fase in cui si dovrebbero garantire le condizioni minime di qualità e conformità del software, mancano strumenti di valutazione basati su indicatori oggettivi e comparabili. Questo rappresenta un punto critico, poiché proprio in tale fase si definiscono i requisiti che influenzeranno l'intero ciclo di vita dell'applicativo.

La Regione Piemonte si trova pertanto nella necessità di disporre di un sistema capace di introdurre criteri uniformi e metodologie standardizzate per la valutazione della sicurezza,

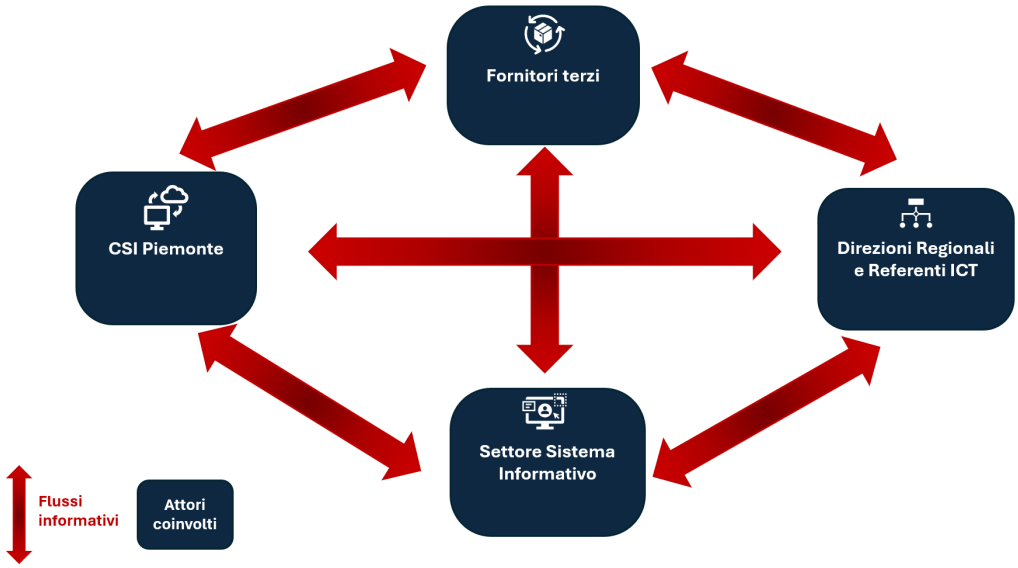


**Figura 2.5:** Rappresentazione degli attori coinvolti e dei flussi informativi distribuiti nel contesto della Regione Piemonte. Elaborazione dell'autore

integrandoli nei processi già esistenti senza introdurre discontinuità o aggravio operativo. Tale modello deve poter dialogare con le procedure di affidamento, con i processi di sviluppo e con le attività di monitoraggio, attuate tramite l'utilizzo di cruscotti e di report. L'obiettivo non è quello di sostituire strumenti o ruoli, ma di sovrapporre una struttura di misurazione trasversale, capace di collegare le dimensioni tecnologiche, organizzative e normative della sicurezza.

Un ulteriore elemento che rende necessaria l'introduzione di un modello scalabile è la varietà delle soluzioni software gestite o commissionate dalla Regione. Il sistema informativo regionale comprende infatti applicazioni con livelli di complessità molto differenti: dai portali web ai servizi a basso impatto operativo fino a sistemi mission critical che gestiscono dati sensibili o processi istituzionali fondamentali. In un contesto così eterogeneo, un modello uniforme ma rigido risulterebbe inefficace. È necessario, invece, un approccio che consenta di adattare la profondità delle verifiche e la granularità delle metriche in funzione della criticità del servizio e delle risorse disponibili. La scalabilità, in questo senso, diventa un requisito essenziale per rendere il modello applicabile a un ampio spettro di progetti, mantenendo però una coerenza metodologica di fondo.

Inoltre, la natura ibrida della governance ICT regionale richiede che il modello possa operare in modo collaborativo tra gli attori coinvolti. Il settore Sistema Informativo Regionale e il CSI Piemonte hanno ruoli differenti ma complementari: il primo attua le regole e gli standard di sicurezza; il secondo implementa e supporta la gestione dei sistemi. Un modello operativo efficace deve quindi consentire un flusso bidirezionale di informazioni tra questi livelli, fornendo strumenti di valutazione condivisi e criteri omogenei per la

rendicontazione e il monitoraggio. La creazione di un linguaggio comune basato su metriche oggettive è, in questo senso, un passo fondamentale verso una governance della sicurezza realmente integrata.

Le attività condotte nel corso del progetto hanno infatti evidenziato come, in assenza di un sistema strutturato di rendicontazione, i referenti ICT non dispongano di strumenti per valutare in modo oggettivo la sicurezza delle applicazioni di competenza. Le loro attività di monitoraggio si basano prevalentemente sull'esperienza, su segnalazioni di disservizi o su verifiche qualitative. Questo limita la possibilità di confrontare nel tempo l'evoluzione dello stato di sicurezza, di individuare pattern ricorrenti o di stimare l'efficacia delle azioni correttive adottate. Il modello proposto intende superare questa carenza, introducendo un sistema di metriche e KPI costruito per essere facilmente applicabile dai referenti ICT, senza necessità di competenze specialistiche avanzate e senza modificare radicalmente i flussi operativi già consolidati. La scelta di utilizzare strumenti e processi già noti all'organizzazione, come le fasi di validazione tecnica e di monitoraggio economico, garantisce la sostenibilità e l'integrazione del modello nel contesto esistente.

Un'altra motivazione che giustifica la necessità di un modello operativo scalabile è legata al principio della accountability istituzionale. Le recenti direttive europee e normative nazionali richiedono infatti che gli enti pubblici siano in grado di dimostrare non solo l'adozione di misure di sicurezza, ma anche la loro efficacia e il loro mantenimento nel tempo. Ciò implica la capacità di raccogliere evidenze documentali e misurabili che attestino lo stato di sicurezza del software in esercizio. Senza un modello di rendicontazione basato su metriche standardizzate, diventa difficile per la Regione Piemonte rispondere in modo puntuale alle richieste di audit o alle verifiche di conformità, sia interne sia esterne.

L'adozione di un modello scalabile rappresenta anche una leva strategica per promuovere un'evoluzione culturale all'interno dell'Amministrazione. Misurare la sicurezza significa, di fatto, renderla visibile, quindi gestibile. Quando la sicurezza è supportata da indicatori e dati misurabili, essa diventa un tema condiviso e comprensibile anche per i livelli gestionali e decisionali. In questo modo, la sicurezza smette di essere un ambito tecnico riservato agli specialisti per diventare un fattore di qualità e di accountability dell'intera organizzazione. La rete dei referenti ICT, già esistente e operativa in Regione Piemonte, insieme alla rete dei referenti di cybersecurity, costituisce in tal senso un punto di forza: essa rappresenta il canale ideale attraverso cui diffondere e consolidare pratiche comuni di valutazione e monitoraggio, garantendo al contempo la partecipazione di tutte le direzioni alla gestione della sicurezza.

La scalabilità del modello deve inoltre essere intesa anche in chiave temporale. Un sistema di misurazione e rendicontazione della sicurezza non può essere statico, ma deve poter evolvere nel tempo in funzione dei cambiamenti normativi, tecnologici e organizzativi. La continua evoluzione del panorama delle minacce e delle direttive europee, unita alla dinamicità dei processi ICT regionali, impone la necessità di un modello flessibile, capace di integrare nuovi indicatori, adattarsi a differenti livelli di maturità e recepire le evidenze operative provenienti dal campo. La previsione di cicli periodici di revisione e aggiornamento delle metriche, accompagnata da momenti di confronto tra i referenti ICT e il settore Sistema Informativo Regionale, consente di mantenere il modello allineato alle esigenze reali e di garantire un miglioramento continuo.

Oltre agli aspetti metodologici e organizzativi, la costruzione di un modello operativo scalabile assume una valenza anche formativa e culturale. L'introduzione di un sistema strutturato di valutazione e monitoraggio della sicurezza richiede infatti una progressiva maturazione delle competenze interne e una ridefinizione dei ruoli coinvolti. In questo senso, la rete dei referenti ICT e dei referenti di cybersecurity, già attiva all'interno della Regione Piemonte, diventa un elemento cardine del modello. Essa può trasformarsi da rete prevalentemente informativa , orientata alla diffusione di linee guida e alla gestione delle segnalazioni, in una rete operativa e proattiva, capace di partecipare direttamente ai processi di verifica e controllo della sicurezza applicativa.

Il modello, concepito come strumento di misurazione, rappresenta anche un potente mezzo di apprendimento organizzativo. Si realizza così un ciclo virtuoso in cui il modello non si limita a misurare la sicurezza, ma innesca processi di crescita professionale e di responsabilizzazione diffusa.

Questa evoluzione comporta una progressiva decentralizzazione del controllo. In un sistema scalabile, la sicurezza non è più gestita in modo esclusivo dal livello centrale (Settore Sistema Informativo Regionale o singoli unità operative del CSI Piemonte), ma diventa una responsabilità condivisa, in cui ciascun referente ICT contribuisce attivamente al monitoraggio e alla raccolta delle evidenze. Tale impostazione si allinea alle più recenti strategie nazionali in materia di cybersecurity, che promuovono il concetto di cyber maturity distribuita, ossia la capacità di ogni articolazione dell'organizzazione di partecipare al presidio della sicurezza secondo il principio di prossimità.

In questa prospettiva, il modello operativo assume anche una funzione di abilitazione organizzativa, poiché fornisce agli attori decentrati strumenti concreti per svolgere un ruolo attivo nel ciclo di gestione della sicurezza. Attraverso la definizione di metriche chiare, schede di valutazione standard e cruscotti di sintesi, i referenti ICT possono segnalare in modo sistematico anomalie, punti di debolezza o variazioni nello stato di sicurezza delle applicazioni, alimentando un flusso informativo continuo verso il livello centrale. Ciò favorisce una visione unificata e dinamica del rischio, superando la frammentazione informativa che oggi rappresenta uno dei principali ostacoli alla gestione efficace della sicurezza.

Parallelamente, il modello incentiva un rafforzamento delle competenze e delle strutture di cybersecurity anche sul versante dei fornitori. Le società che sviluppano o gestiscono applicazioni per conto della Regione Piemonte sono chiamate a garantire livelli minimi di sicurezza non solo in termini di conformità contrattuale, ma anche di trasparenza e collaborazione nella fornitura dei dati necessari alla misurazione. In un contesto in cui la sicurezza viene misurata attraverso KPI oggettivi, i fornitori devono essere in grado di documentare in modo puntuale le evidenze tecniche relative al codice, alle librerie di terze parti, alle configurazioni e ai processi di test. Il modello, in questo senso, funge da strumento di responsabilizzazione reciproca: la Regione definisce i parametri e le modalità di rendicontazione, mentre i fornitori sono chiamati a garantire la disponibilità delle informazioni e degli strumenti necessari alla verifica. Si realizza così un rapporto basato non solo sulla fiducia contrattuale, ma su evidenze oggettive e verificabili. Tale approccio favorisce anche una maggiore integrazione tra gli strumenti di controllo interni e quelli adottati dai fornitori, aprendo la strada a una cooperazione tecnica più matura e

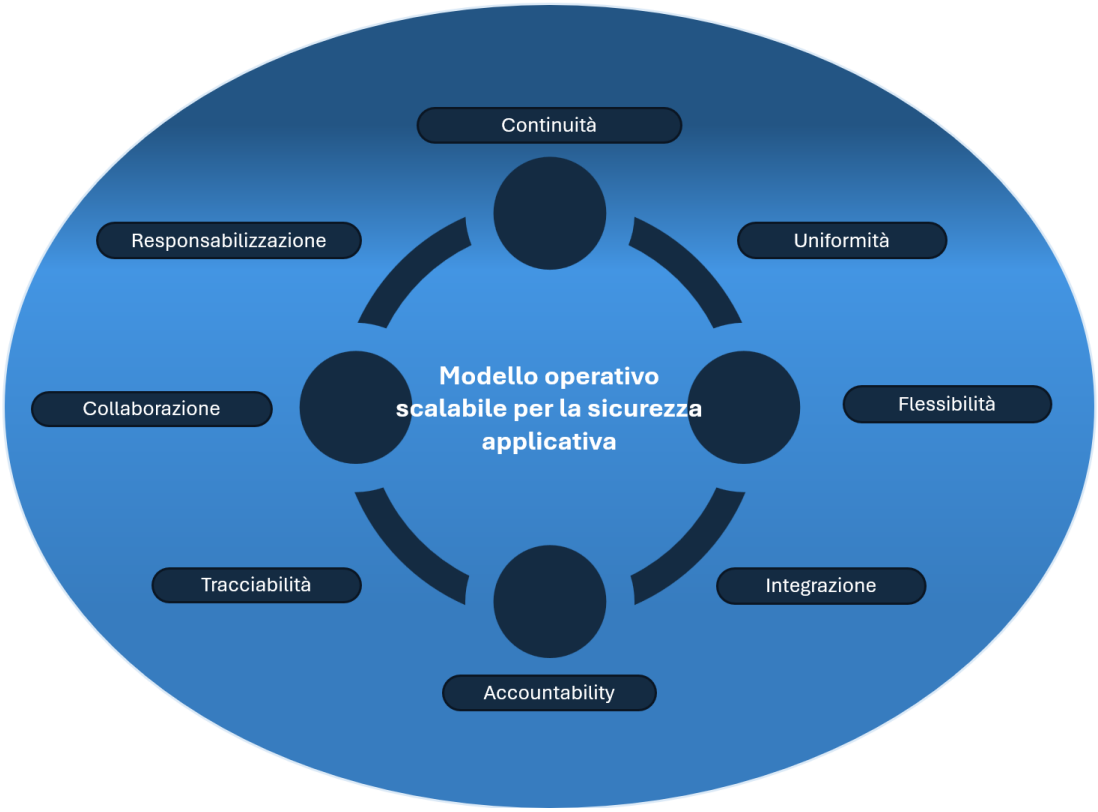


**Figura 2.6:** Le esigenze di un modello operativo scalabile per la sicurezza applicativa nel contesto regionale. Elaborazione dell'autore

orientata alla qualità complessiva del software prodotto.

Un ulteriore beneficio atteso dall'adozione del modello riguarda la tracciabilità dei processi di sicurezza. Ogni valutazione, ogni controllo e ogni aggiornamento delle metriche contribuiscono alla costruzione di una base storica di dati, utile non solo per la rendicontazione e la trasparenza, ma anche per la programmazione strategica. Analizzando le tendenze nel tempo, la Regione potrebbe individuare le aree a maggiore esposizione, le tipologie di vulnerabilità ricorrenti e le pratiche di sviluppo o gestione che determinano gli impatti più significativi sulla sicurezza. Tali informazioni diventano così la base per orientare le politiche di investimento, le scelte tecnologiche e le priorità di formazione. Inoltre, la possibilità di correlare le metriche di sicurezza con altri indicatori di performance ICT, come la qualità del servizio o la disponibilità delle piattaforme, consentirebbe inoltre di quantificare il valore della sicurezza in termini di efficienza e affidabilità del sistema informativo regionale.

L'implementazione di un modello per la valutazione della sicurezza del software interno all'Ente, porterebbe inoltre ad abbattere i costi relativi a potenziali affidamenti a fornitori esterni per la gestione della compliance normativa nell'ambito della cybersecurity; considerando comunque la cospicua necessità di risorse che sarebbero richieste qualora si

intendesse fare degli audit ai fornitori esterni per il controllo e la gestione della supply chain, senza uno strumento strutturato come quello proposto dalla presente tesi

Attraverso queste considerazioni emerge come la necessità di un modello operativo scalabile nella gestione della sicurezza del software derivi da esigenze concrete e misurabili: la mancanza di criteri uniformi di valutazione nelle fasi di affidamento, l'assenza di monitoraggio continuativo post-rilascio, la frammentazione delle responsabilità e la difficoltà di dimostrare l'efficacia delle misure di sicurezza adottate, come rappresentato sinteticamente in Figura 2.6.

## 2.4 Obiettivi della tesi

L'analisi condotta nelle sezioni precedenti ha messo in luce come la gestione della sicurezza del software nella Pubblica Amministrazione, in particolare nel contesto della Regione Piemonte, presenti ancora margini di miglioramento significativi. La frammentazione dei processi, la mancanza di metriche oggettive, l'assenza di un monitoraggio continuativo nel ciclo di vita degli applicativi e la difficoltà nel correlare la sicurezza con la qualità complessiva dei servizi informatici delineano uno scenario in cui la valutazione della sicurezza risulta complessa, disomogenea e scarsamente misurabile.

A partire da queste considerazioni, la tesi si propone di sviluppare un modello operativo per la valutazione, la rendicontazione e il monitoraggio e controllo della sicurezza del software, con l'obiettivo di trasformare la sicurezza applicativa da ambito reattivo e episodico a processo sistematico, strutturato e misurabile nel tempo.

L'obiettivo generale del progetto di tesi consiste nella definizione di un modello integrato che consenta alla Regione Piemonte di disporre di strumenti e metodologie per misurare e gestire la sicurezza del proprio patrimonio software in modo coerente, continuo e verificabile. Per raggiungere questo obiettivo, la ricerca si articola in tre principali risultati, strettamente interconnessi e coerenti con le linee guida nazionali ed europee in materia di sicurezza ICT:

1. Definizione delle metriche di sicurezza del software, attraverso l'individuazione di indicatori quantitativi e qualitativi che permettano di valutare il livello di sicurezza delle applicazioni lungo tre pilastri fondamentali: *Codice*, *Infrastruttura* e *Compliance* tecnico–normativa.

2. Progettazione di un sistema di rendicontazione, finalizzato alla raccolta, aggregazione e comunicazione strutturata delle evidenze di sicurezza, utile a supportare la governance ICT e le funzioni di controllo.

3. Progettazione di un sistema di monitoraggio e controllo, volto a garantire la continuità della valutazione nel tempo e a fornire ai referenti ICT e alle strutture competenti uno strumento operativo per il miglioramento progressivo della sicurezza applicativa.

Questi tre risultati rappresentano gli output concreti del progetto di tesi, come rappresentato in Figura 2.7, delineando gli elementi costitutivi del modello operativo descritto nel capitolo successivo.

Il primo obiettivo operativo del lavoro di tesi riguarda la definizione di un set di metriche e KPI in grado di quantificare la sicurezza del software in maniera oggettiva, ripetibile e comparabile tra progetti differenti. L'esigenza nasce dalla constatazione che, nella prassi corrente, la sicurezza applicativa viene valutata prevalentemente in modo qualitativo, mediante checklist o giudizi esperti, che non consentono di misurare l'efficacia delle misure adottate né di confrontare l'evoluzione nel tempo. L'introduzione di metriche standardizzate rappresenta quindi il primo passo per costruire una sicurezza misurabile.

Il lavoro si propone di strutturare le metriche attorno a tre dimensioni analitiche principali:

- *Codice*: analisi della qualità e della sicurezza del codice sorgente, con riferimento alla presenza di vulnerabilità note, all' uso di librerie di terze parti, alla conformità alle best practices OWASP e ai principi legati alla programmazione sicura;

- *Infrastruttura*: valutazione degli aspetti legati alla configurazione dei sistemi, alla gestione dell'ecosistema infrastrutturale sottostante agli applicativi, alla sicurezza degli ambienti di sviluppo e dei processi di rilascio;

- *Compliance* tecnico–normativa: verifica della coerenza con gli standard e le normative vigenti e della capacità dell'organizzazione di garantire la protezione dei dati e la resilienza operativa.

La definizione di queste metriche è finalizzata non solo a costruire un sistema di valutazione oggettivo, ma anche a favorire l'integrazione dei controlli di sicurezza nel ciclo di vita del software. In tal modo, la sicurezza viene misurata non come un esito, ma come un processo, con indicatori distribuiti lungo tutte le fasi, dall'analisi iniziale alla messa in esercizio. Le metriche costituiranno inoltre la base per la costruzione di un cruscotto di sicurezza regionale, uno strumento in grado di restituire una visione sintetica ma accurata dello stato di sicurezza del parco applicativo, rendendo confrontabili i risultati tra direzioni e fornitori. Tale approccio permetterà di individuare trend evolutivi, aree di rischio ricorrenti e priorità di intervento, abilitando così una gestione basata sui dati e non sulle percezioni.

Il secondo risultato atteso della tesi riguarda la progettazione di un sistema strutturato di rendicontazione della sicurezza, concepito per garantire la trasparenza, la tracciabilità e la verificabilità delle attività di valutazione. Nel contesto della Pubblica Amministrazione, la rendicontazione non rappresenta solo un adempimento tecnico, ma un principio di accountability verso la collettività e le istituzioni di controllo. Dimostrare, con evidenze oggettive, lo stato di sicurezza dei propri sistemi informativi significa infatti consolidare la fiducia dei cittadini e rafforzare la legittimità dell'azione amministrativa.

Gli strumenti proposti dovranno consentire una raccolta strutturata dei dati, preferibilmente mediante moduli standard o possibili future interfacce digitali, che riducano la discrezionalità interpretativa e assicurino la comparabilità tra progetti diversi. L'obiettivo è costruire un sistema in cui la rendicontazione non sia percepita come un mero onere burocratico, ma come un processo integrato di valutazione e miglioramento continuo. Le informazioni raccolte attraverso la rendicontazione diventeranno la base per alimentare il

sistema di monitoraggio, fornendo dati utili non solo per la compliance, ma anche per la prevenzione e la pianificazione.

Un ulteriore aspetto innovativo consiste nel coinvolgimento dei fornitori nel processo di rendicontazione. I soggetti che realizzano o gestiscono applicazioni per conto della Regione saranno chiamati a contribuire alla raccolta delle evidenze tecniche, in un'ottica di collaborazione e trasparenza. Questo approccio risponde a due esigenze: da un lato, garantire la disponibilità delle informazioni necessarie alla valutazione; dall'altro, promuovere una maggiore maturità organizzativa e tecnica nella gestione della sicurezza lungo tutta la filiera del software.

Il terzo obiettivo specifico della tesi riguarda la progettazione di un sistema di monitoraggio e controllo non limitato alla sicurezza dei singoli applicativi, ma esteso al modello stesso e alle metriche che ne costituiscono la base operativa. L'intento è quello di superare l'attuale discontinuità dei controlli e di garantire un presidio costante non solo sullo stato di sicurezza del software, ma anche sull'efficacia, sull'aggiornamento e sulla coerenza delle metriche utilizzate per valutarlo.

Attualmente, infatti, le verifiche di sicurezza avvengono prevalentemente nelle fasi di collaudo o di rilascio, senza un effettivo monitoraggio nella fase di esercizio e, ancor meno, senza una verifica periodica della tenuta del modello di valutazione stesso. Questo approccio determina una doppia criticità: da un lato, una perdita progressiva di visibilità sulle vulnerabilità e sulle configurazioni degli applicativi in esercizio; dall'altro, l'assenza di un processo strutturato di revisione e miglioramento del modello di misurazione, che rischia così di diventare statico e rapidamente obsoleto rispetto all'evoluzione tecnologica e normativa.

L'obiettivo è dunque quello di trasformare il monitoraggio da attività episodica a processo permanente e riflessivo, capace di alimentarsi attraverso flussi informativi costanti e di produrre evidenze sia operative sia metodologiche. Il sistema proposto non si limita a osservare le applicazioni, ma include la valutazione periodica della validità, pertinenza e aggiornamento delle metriche, così da garantire che gli indicatori rimangano rappresentativi del reale livello di sicurezza nel tempo.In questa prospettiva, il sistema di monitoraggio sarà concepito come una struttura scalabile e bidirezionale, in grado di adattarsi a progetti di diversa complessità e criticità e, al contempo, di raccogliere i dati necessari per misurare le prestazioni del modello stesso.

Un altro elemento chiave è l'integrazione tra il monitoraggio e il sistema di rendicontazione: le informazioni raccolte in modo continuo confluiranno nei report periodici, fornendo una base oggettiva per la valutazione delle performance e per la pianificazione degli interventi di mitigazione. In tal modo, il modello assicura una circolarità dei dati, in cui il monitoraggio alimenta la rendicontazione e quest'ultima orienta le decisioni strategiche di miglioramento.

Attraverso questi tre risultati, la tesi persegue una serie di obiettivi di impatto che travalicano la dimensione puramente tecnica. Il modello mira infatti a promuovere una cultura della sicurezza misurabile, fondata su dati e indicatori condivisi e a consolidare una governance multilivello in cui tutti gli attori partecipano attivamente alla gestione della sicurezza. La disponibilità di metriche e strumenti di monitoraggio consentirà inoltre di passare da un approccio reattivo a uno proattivo, orientato alla prevenzione e al


**Figura 2.7:** Elenco ed elementi chiave degli obiettivi della tesi. Elaborazione dell'autore

miglioramento continuo.

Dal punto di vista istituzionale, l'adozione del modello rappresenterà un passo avanti verso una maggiore accountability digitale, in linea con le raccomandazioni dell'Agenzia per la Cybersicurezza Nazionale e con gli obiettivi del Piano Strategico ICT regionale [19].In prospettiva, il modello potrà fungere da framework replicabile, adattabile ad altri contesti amministrativi e costituire la base per una metodologia diffusa di valutazione della sicurezza applicativa.

La tesi intende offrire un contributo metodologico e operativo alla costruzione di un sistema regionale per la sicurezza del software che sia trasparente, integrato e sostenibile nel tempo. L'obiettivo è trasformare la misurazione della sicurezza da attività meramente tecnica a vero e proprio strumento di governance, supporto decisionale e leva per l'innovazione organizzativa.

Il capitolo successivo sarà dedicato alla progettazione e implementazione del modello operativo, articolato nelle sue componenti fondamentali. Verranno presentate le metriche individuate, il sistema di rendicontazione e il meccanismo di monitoraggio e controllo, evidenziando come ciascun elemento contribuisca in modo sinergico alla costruzione di un approccio strutturato e misurabile alla sicurezza applicativa.

# Capitolo 3

# Progettazione e realizzazione della soluzione

Il presente capitolo descrive il percorso di progettazione e realizzazione della soluzione proposta per la valutazione della sicurezza applicativa nel contesto della Regione Piemonte. Esso costituisce il nucleo operativo della ricerca, in cui i principi teorici e normativi analizzati nei capitoli precedenti vengono tradotti in un modello concreto, strutturato e applicabile alla realtà organizzativa regionale. L'obiettivo è fornire un sistema integrato, fondato su metriche oggettive e procedure replicabili, capace di supportare la governance della sicurezza del software lungo tutto il ciclo di vita applicativo, dalla fase di acquisizione fino al monitoraggio post-rilascio. La progettazione del modello si basa sull'assunto che la sicurezza applicativa non possa essere valutata unicamente attraverso analisi tecniche, ma richieda un approccio sistemico che integri aspetti tecnologici, organizzativi e normativi. In questa prospettiva, la soluzione elaborata si configura come un modello a tre pilastri, ciascuno dei quali rappresenta una dimensione essenziale del rischio ICT e contribuisce alla definizione della postura complessiva di sicurezza dell'Ente. La seconda parte del capitolo illustra la progettazione del sistema di rendicontazione, ossia l'insieme di strumenti e processi attraverso cui le metriche vengono applicate, misurate e documentate nel ciclo di vita dei progetti ICT regionali. Tale sistema è stato pensato per integrarsi organicamente con le procedure operative già in uso nella Regione Piemonte ed è articolato in quattro fasi principali, assicurando una tracciabilità completa delle valutazioni e costituendo la base dati per le attività di controllo e miglioramento. La terza sezione è dedicata alla progettazione del sistema di monitoraggio e controllo, che rappresenta il livello di supervisione e consolidamento metodologico del modello. Esso ha la funzione di verificare nel tempo la coerenza, l'efficacia e l'attualità delle metriche, assicurando che il sistema di rendicontazione mantenga un'elevata qualità e risponda ai cambiamenti tecnologici e normativi. Nel loro insieme, le tre sezioni del capitolo traducono la dimensione teorica del modello in un framework operativo, capace di coniugare rigore metodologico e aderenza al contesto reale.

## 3.1 Definizione metriche di sicurezza

La definizione di metriche di sicurezza costituisce il punto di partenza per la costruzione di un modello operativo efficace e misurabile. Le metriche rappresentano, infatti, lo strumento attraverso cui la sicurezza può essere tradotta da principio astratto a elemento concreto e verificabile, permettendo di valutare in modo oggettivo la qualità e l'affidabilità del software lungo tutto il suo ciclo di vita. In un contesto complesso come quello della Pubblica Amministrazione, dove la pluralità di attori e tecnologie genera un'elevata eterogeneità applicativa, la misurazione standardizzata diventa condizione indispensabile per garantire coerenza, comparabilità e continuità nei processi di gestione della sicurezza.

Le metriche di sicurezza assolvono dunque a una duplice funzione: da un lato, consentono di quantificare il livello di esposizione al rischio e di identificare le aree di criticità più rilevanti; dall'altro, rappresentano la base per la rendicontazione e il monitoraggio, fornendo dati oggettivi a supporto delle decisioni strategiche e operative. Laddove la valutazione della sicurezza si fonda su giudizi qualitativi o verifiche episodiche, l'introduzione di metriche strutturate permette di instaurare un approccio sistematico, in cui le evidenze numeriche diventano il linguaggio comune attraverso cui comunicare, confrontare e migliorare le prestazioni di sicurezza nel tempo.

Per la definizione delle metriche, il modello proposto in questa tesi adotta una struttura ispirata alle linee guida del NIST, in particolare alle indicazioni contenute nella serie SP 800-55 [10, 11], che propone un quadro metodologico di riferimento riconosciuto a livello internazionale per la misurazione della sicurezza delle informazioni. Secondo l'approccio NIST, ogni metrica deve essere descritta in modo chiaro e standardizzato, così da garantirne la comprensione e l'applicabilità in contesti diversi. La struttura di riferimento adottata prevede, per ciascuna metrica, la definizione dei seguenti elementi fondamentali:

- *Unique ID*: un identificativo univoco che consente di tracciare e catalogare la metrica all'interno del modello;
- *Goal*: l'obiettivo specifico della misurazione e il valore informativo che la metrica intende fornire;
- *Scope*: l'ambito di applicazione sul quale viene considerata la metrica in oggetto;
- *Measure*: le modalità di calcolo o di valutazione della metrica, secondo i parametri definiti nella formula;
- *Type*: la categoria e natura della metrica, utile a distinguerne la finalità analitica;
- *Formula*: l'espressione utilizzata per il computo della metrica, con la descrizione dei parametri coinvolti;
- *Target*: il valore atteso o intervallo di riferimento considerato ottimale per la misurazione;
- *Implementation Evidence*: l'insieme di documenti, dati e informazioni empiriche che costituiscono le evidenze a supporto dei risultati della misurazione.

Per mantenere un raccordo metodologico completo con la struttura promossa dall'agenzia statunitense NIST, vengono inoltre richiamati i parametri non direttamente impiegati nella definizione delle metriche adottate nella tesi, ma che risultano comunque rilevanti nel quadro generale:

- *Time-based reference*: identifica i riferimenti temporali associati al computo della metrica. Nel contesto in esame, tali riferimenti sono stati integrati direttamente nella formula, per le metriche a stretto riferimento temporale, mentre per le altre sono definiti all'interno delle fasi del sistema di rendicontazione;
- *Responsible parties*: individua i ruoli e le responsabilità degli attori coinvolti nella misurazione. In questo modello, i referenti ICT sono designati come soggetti rendicontatori delle metriche, mentre i fornitori costituiscono i produttori delle informazioni necessarie al loro computo;
- *Data source*: specifica le fonti dei dati utilizzati, variabili in base al fornitore e al prodotto software oggetto di misurazione e, di conseguenza, non esplicitamente indicate nel modello;
- *Reporting format*: definisce le modalità di rappresentazione e visualizzazione dei risultati, uniformate nel presente modello attraverso il sistema di rendicontazione.

Questa struttura, applicata in modo coerente, garantisce la tracciabilità, la trasparenza e la replicabilità delle valutazioni, rendendo il modello proposto aderente ai principi di accountability e governance basati sulle evidenze, promossi dalle strategie nazionali in materia di cybersecurity.

Le metriche sono inoltre organizzate secondo tre pilastri fondamentali quali *Codice*, *Infrastruttura* e *Compliance* tecnico–normativa, che rappresentano le dimensioni complementari attraverso cui è possibile valutare in modo completo la sicurezza applicativa. Questa articolazione risponde all'esigenza di superare una visione parziale della sicurezza, concentrata esclusivamente sugli aspetti tecnici, per abbracciare una prospettiva sistemica che integri componenti tecnologiche, organizzative e di conformità normativa.

Il pilastro del *Codice* è volto a misurare la sicurezza intrinseca del software, analizzandone la qualità, la robustezza e la resilienza rispetto alle vulnerabilità note o potenziali. Il pilastro dell'*Infrastruttura* considera invece il contesto in cui il software è sviluppato, distribuito e mantenuto, valutando la sicurezza delle configurazioni, dei sistemi di rilascio e della messa in esercizio. Infine, il pilastro della *Compliance* tecnico–normativa amplia la prospettiva includendo il rispetto degli standard, delle normative e delle politiche di sicurezza, garantendo che le soluzioni sviluppate siano non solo tecnicamente sicure, ma anche coerenti con i requisiti regolamentari e organizzativi.

Questa tripartizione, rappresentata in Figura 3.1, consente di rappresentare in modo integrato la sicurezza del software, evitando che singole dimensioni siano valutate isolatamente. L'approccio adottato nella tesi intende quindi fornire una visione olistica, in cui ogni pilastro contribuisce a definire un quadro complessivo e dinamico della postura di sicurezza applicativa. Nelle sezioni che seguono, ciascun pilastro sarà analizzato nel

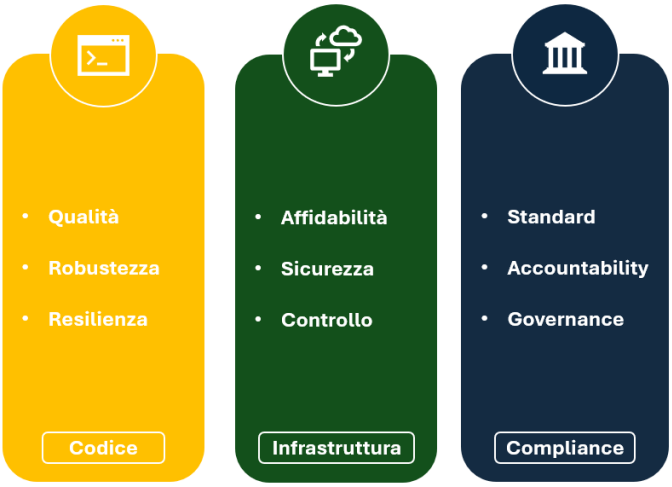


**Figura 3.1:** Definizione dei tre pilastri - *Codice*, *Infrastruttura* e *Compliance* tecnico-normativa - su cui si sviluppano le metriche del modello proposto dalla tesi. Elaborazione dell'autore

dettaglio, evidenziandone le finalità, le logiche di misurazione e le principali metriche individuate nel contesto operativo della Regione Piemonte.

I risultati che saranno raggiunti in questa sezione sono:

- la definizione di un set di metriche inerenti al codice sorgente che permetta di misurare gli aspetti principali della sicurezza del software derivanti dall'analisi statica del codice e dall'analisi delle librerie esterne;

- la definizione di un set di metriche inerenti alla componente infrastrutturale che permetta di analizzare la gestione e il monitoraggio delle risorse fisiche e virtuali, dei flussi di dati, delle postazioni di lavoro e della rete;

- la definizione di un set di metriche inerenti alla sfera tecnica-normativa che permetta di assicurare il rispetto delle linee guida nazionali e internazionali inerenti alla gestione dei processi di cybersicurezza, alla gestione del rischio, alla definizione dei ruoli e alla gestione della supply-chain;

Il risultato finale sarà un prospetto di metriche ben definite con opportune descrizioni, scopi, ambiti di applicazione, formule di calcolo e possibili evidenze documentali, che permettano di misurare quantitavamente e qualitativamente i prodotti software del parco applicativo regionale.

### 3.1.1 Metriche del pilastro Codice

Il pilastro *Codice* rappresenta il nucleo tecnico del modello operativo proposto, in quanto concentra l'attenzione sulla qualità e sulla sicurezza del software a partire dal suo elemento più essenziale, il codice sorgente. Misurare la sicurezza del codice significa valutare non soltanto la presenza di vulnerabilità o errori, ma anche la solidità complessiva del prodotto, la sua resilienza agli attacchi e la capacità dell'organizzazione di mantenere nel tempo standard di qualità coerenti con le buone pratiche di sviluppo sicuro.

La definizione delle metriche associate a questo pilastro trae origine dal lavoro già condotto nell'ambito dell'iniziativa descritta nella sezione 1.2.2, dedicata ai progetti correlati della presente tesi, da cui sono stati ripresi i principi metodologici e le logiche di analisi utilizzate per la valutazione della sicurezza applicativa nel contesto regionale. Tale progetto ha rappresentato un importante punto di partenza per la costruzione del modello, in quanto ha permesso di sperimentare un approccio integrato basato su strumenti di analisi automatica e su criteri di valutazione condivisi tra i diversi attori coinvolti. In continuità con tale esperienza, il modello proposto in questa tesi adotta un insieme di metriche che si fondano sui risultati di due strumenti già consolidati all'interno del contesto operativo della Regione Piemonte: *SonarQube* e *Meterian*.

Il primo, impiegato per attività di analisi statica del codice (SAST), consente di individuare vulnerabilità, bug e punti di debolezza nel codice sorgente, fornendo indicatori di sicurezza e affidabilità. Il secondo, dedicato alle attività di analisi della composizione del software (SCA), analizza le dipendenze esterne, identificando vulnerabilità note nelle librerie di terze parti, nonché aspetti legati alla stabilità e all'aggiornamento delle componenti software. La scelta di utilizzare questi strumenti deriva dalla volontà di garantire coerenza con le pratiche e gli strumenti già in uso presso la Regione Piemonte, assicurando al contempo la replicabilità e l'automazione delle analisi.

A partire dalle metriche già impiegate nel progetto di riferimento, il set è stato ampliato e riorganizzato in modo da garantire una copertura più completa e coerente rispetto alle esigenze del modello operativo proposto. Oltre alle metriche derivate direttamente dai report generati dai tool (come *Security Rating*, *Reliability Rating*, *Maintainability Rating* di *SonarQube* e *Library Security Rating* di *Meterian*), sono stati introdotti ulteriori indicatori con l'obiettivo di migliorare la capacità descrittiva e comparativa del sistema. In particolare, sono state aggiunte due nuove categorie di misurazione:

- le metriche di *coverage*, che misurano la percentuale effettiva di codice e di dipendenze sottoposte ad analisi, garantendo che le valutazioni siano rappresentative del reale perimetro applicativo;
- le metriche di stabilità, volte a monitorare il grado di aggiornamento e la capacità di mantenimento delle dipendenze, intese come indicatore indiretto della resilienza del software nel tempo.

L'introduzione di queste due metriche, avendo come base informativa dei valori già prodotti dai tool SAST ed SCA utilizzati, ha permesso di rendere, senza ulteriori aggravi per la misurazione, il set di metriche maggiormente esaustivo, con aspetti legati all'effettivo perimetro di applicazione delle metriche e alla stabilità delle componenti software analizzate.

I dettagli tecnici relativi a ciascuna metrica sono presenti nel documento annesso come Appendice A alla presente tesi, che costituisce parte integrante del modello proposto. L'appendice riporta in modo completo le metriche e i KPI definiti per il pilastro *Codice*, utilizzati per misurare qualità, sicurezza, affidabilità e copertura delle analisi sul software prodotto dai fornitori.

Il documento contiene innanzitutto le metriche dedicate alla sicurezza e all'affidabilità del codice sorgente. La prima di esse è la *COD-SR01*, che misura la percentuale di codice che raggiunge il livello A di *Security Rating*, calcolata in modo ponderato sulla base delle linee di codice. Questa metrica consente di valutare la presenza di vulnerabilità classificate come *Minor*, *Major*, *Critical* o *Blocker*, fornendo un valore sintetico capace di esprimere il livello di sicurezza complessiva del prodotto. Segue la metrica *COD-RR01*, che applica lo stesso metodo di valutazione alla rilevazione dei bug, attraverso il *Reliability Rating* di *SonarQube*. Anch'essa utilizza un sistema di classi che permette di confrontare facilmente diversi prodotti software o l'evoluzione di uno stesso prodotto nel tempo.

Sono inoltre presenti le metriche dedicate alla sicurezza e alla stabilità delle dipendenze software, analizzate tramite *Meterian*. La metrica COD-LSR01 valuta la percentuale di componenti che non presentano vulnerabilità di tipo *CRITICAL* nelle librerie esterne, utilizzando come riferimento il punteggio di sicurezza fornito dallo strumento. La metrica *COD-LST01* esamina invece la stabilità delle dipendenze, calcolando la percentuale di componenti che non presentano patch non applicate. Anche queste due metriche sono classificate in livelli da I a V e consentono di quantificare il rischio legato alla supply chain software, oggi particolarmente rilevante nell'ambito DevSecOps.

L'appendice include infine le metriche che dimostrano la copertura effettiva delle analisi effettuate sui prodotti software. La metrica *COD-COV01* misura la percentuale di linee di codice del prodotto effettivamente analizzate tramite *SonarQube*, con un target del 100% e una soglia minima del 95% in presenza di esclusioni motivate. La metrica *COD-COV02* valuta invece la copertura delle analisi SCA, calcolando la percentuale di dipendenze sottoposte all'analisi rispetto a quelle dichiarate nei manifest. Anch'essa prevede come valore atteso il 100%.

La presenza di queste metriche rende concreta e verificabile l'analisi descritta nel presente capitolo. Esse forniscono infatti indicatori misurabili, basati su strumenti realmente adottati, che permettono di valutare la sicurezza, l'affidabilità e la qualità del codice sviluppato, oltre alla completezza delle analisi condotte.

| ID | Ambito | Tipo di misura | Obiettivo | Formula principale | Target | Note |
|---|---|---|---|---|---|---|
| **COD-SR01** | Security Rating | Efficacia | Misurare il grado di sicurezza del codice per prevenire vulnerabilità in fase di sviluppo | % codice con Security Rating = A, ponderata per LoC | $\geq$ 100% (Classe I) | *Definizione delle Classi: I: 100%; II: 67–99%; III: 34–66%; IV: 1–33%; V: 0%* |
| **COD-RR01** | Reliability Rating | Efficacia | Valutare l'affidabilità del software tramite rilevazione di bug | % codice con Reliability Rating = A, ponderata per LoC | $\geq$ 100% (Classe I) | *Definizione delle Classi: I: 100%; II: 67–99%; III: 34–66%; IV: 1–33%; V: 0%* |
| **COD-LSR01** | Library Security | Efficacia | Valutare la sicurezza delle librerie esterne rilevando vulnerabilità CRITICAL | % componenti senza vulnerabilità CRITICAL | $\geq$ 100% (Classe I) | *Definizione delle Classi: I: 100%; II: 67–99%; III: 34–66%; IV: 1–33%; V: 0%* |
| **COD-LST01** | Library Stability | Efficacia | Valutare stabilità e affidabilità delle librerie tramite verifica patch | % componenti senza patch NON APPLICATE | $\geq$ 100% (Classe I) | *Definizione delle Classi: I: 100%; II: 67–99%; III: 34–66%; IV: 1–33%; V: 0%* |

*Continua nella pagina successiva*

| ID | Ambito | Tipo di misura | Obiettivo | Formula principale | Target | Note |
|---|---|---|---|---|---|---|
| **COD-COV01** | Coverage SAST | Implementazione | Verificare che tutto il codice sorgente sia coperto da analisi statica (SAST) | % LoC analizzate da SonarQube / totali | 100% ($\geq$ 95% con giustificazioni documentate) | |
| **COD-COV02** | Coverage SCA | Implementazione | Verificare che tutte le dipendenze siano analizzate tramite SCA (Meterian) | % dipendenze analizzate da Meterian / totali dichiarate | 100% ($\geq$ 95% con giustificazioni documentate) | |

**Tabella 3.1:** Metriche definite per il pilastro *Codice*

Le metriche individuate per il pilastro *Codice* sono rappresentate sinteticamente nella Tabella 3.1. Esse costituiscono la base per la misurazione della sicurezza del codice sorgente e delle sue dipendenze, in coerenza con gli strumenti e le metodologie descritti in questa sezione.

In conclusione, il pilastro *Codice* fornisce una base quantitativa e ripetibile per la misurazione della sicurezza intrinseca del software, trasformando i risultati delle analisi tecniche in strumenti di supporto decisionale e di miglioramento continuo. Le metriche non hanno solo una funzione diagnostica, ma rappresentano un meccanismo di apprendimento organizzativo: attraverso la loro applicazione sistematica, la Regione Piemonte potrà progressivamente consolidare pratiche di sviluppo più sicure, misurabili e orientate alla qualità.

### 3.1.2 Metriche del pilastro Infrastruttura

Il secondo pilastro del modello di valutazione della sicurezza riguarda l'infrastruttura tecnologica, ossia l'insieme delle risorse fisiche e logiche che costituiscono la base su cui vengono eseguiti e gestiti i servizi informativi. La sicurezza infrastrutturale rappresenta un elemento cardine della resilienza complessiva di un sistema informativo: garantire che i data center, le reti, i sistemi di gestione degli accessi e i meccanismi di backup siano configurati, mantenuti e monitorati in modo sicuro significa assicurare la continuità operativa e la protezione dei dati su cui si fondano i servizi digitali pubblici. Nel contesto della Regione Piemonte, tale dimensione assume un rilievo strategico, poiché la complessità del sistema informativo regionale, distribuito su più ambienti e con la partecipazione di diversi soggetti tecnici, richiede un approccio coerente e verificabile alla gestione della sicurezza infrastrutturale.

La definizione delle metriche associate al pilastro *Infrastruttura* si basa sui requisiti e sui principi contenuti nel *Regolamento per le infrastrutture digitali e per i servizi cloud per la Pubblica Amministrazione*, redatto da ACN [21]. Tale regolamento rappresenta il principale riferimento normativo per la qualificazione dei servizi di cloud computing e per la definizione dei livelli minimi di sicurezza che devono essere garantiti dalle amministrazioni e dai loro fornitori. In particolare, per la costruzione del modello proposto, si è scelto di fare riferimento ai requisiti previsti per i dati e i servizi ordinari, poiché essi costituiscono la categoria prevalente nel contesto operativo della Regione Piemonte. Questa scelta è coerente con la necessità di adottare parametri misurabili e realistici, in grado di riflettere le effettive condizioni operative della maggior parte dei servizi regionali, pur mantenendo un allineamento con gli standard nazionali e internazionali.

Il Regolamento ACN fornisce una base metodologica solida e riconosciuta, poiché integra principi di sicurezza fisica, logica e organizzativa, traducendoli in requisiti concreti e verificabili. A partire da tali requisiti, il lavoro di tesi ha individuato un insieme di metriche specifiche, adattate al contesto regionale e strutturate secondo la metodologia NIST, precedentemente illustrata nei paragrafi introduttivi della presente sezione. Per ciascuna metrica sono stati definiti gli elementi fondamentali in modo da garantire la tracciabilità, la coerenza e la riproducibilità delle valutazioni nel tempo.

Il processo di individuazione ha seguito una logica di integrazione, poiché le metriche derivano direttamente dai requisiti minimi del Regolamento ACN, che ne garantiscono la conformità ai principi di sicurezza nazionali. Su questa base, è stato svolto un ulteriore lavoro di adattamento volto a favorire la misurabilità e la rendicontabilità nel contesto operativo della Regione Piemonte, introducendo indicatori quantitativi e soglie di riferimento utili per la costruzione degli strumenti di rendicontazione e monitoraggio previsti nel modello. Questa operazione di contestualizzazione ha consentito di trasformare prescrizioni di carattere tecnico e normativo inerenti alle infrastrutture in strumenti di valutazione concreti, mantenendo la coerenza con le linee guida di cybersecurity e al tempo stesso garantendo una reale applicabilità a livello operativo.

Le metriche dettagliate per ciascuna area sono riportate nel documento allegato alla presente tesi come Appendice B. L'appendice presenta in modo strutturato le metriche e i KPI definiti per il pilastro *Infrastruttura*, con l'obiettivo di garantire continuità operativa, sicurezza fisica e logica, resilienza dei servizi digitali, corretta amministrazione degli asset e adeguate capacità di rilevamento delle minacce.

Il primo insieme di indicatori riguarda la disponibilità dell'infrastruttura, misurata attraverso la percentuale di tempo annuo in cui le risorse critiche risultano operative, sia considerando sia escludendo i fermi programmati. La metrica definita consente di valutare in modo oggettivo il livello di continuità dei servizi ICT, attraverso valori attesi molto elevati che riflettono la criticità delle infrastrutture coinvolte (*INF-A01*). Accanto a questo, l'appendice riporta le metriche riguardanti la sicurezza fisica e ambientale dei *Data Center*. Tali metriche quantificano la conformità a requisiti infrastrutturali essenziali, come la presenza di presidio continuo, la conformità agli standard tecnici di settore, la protezione antincendio, l'utilizzo di pavimenti flottanti e la connessione dei sistemi a soluzioni di continuità elettrica. È inoltre prevista una seconda metrica dedicata alla sicurezza ambientale, che valuta l'adozione di misure come procedure formalizzate per

la gestione sicura dei supporti fisici, sistemi di videosorveglianza e controlli ambientali, anch'essa espressa come percentuale di requisiti soddisfatti(*INF-DC01 e INF-DC02*).

Una parte significativa dell'appendice è dedicata all'*Asset Management*, affrontato sia dal punto di vista degli asset fisici sia da quello dei flussi informativi. Le metriche definite permettono di misurare la percentuale di dispositivi effettivamente censiti rispetto a quelli rilevati nella rete aziendale e la percentuale di flussi di dati mappati e approvati rispetto a quelli utilizzati operativamente. Tali indicatori consentono di verificare la tracciabilità delle risorse e dei flussi critici, rafforzando il controllo sugli asset e favorendo la prevenzione di accessi non autorizzati o esfiltrazioni di dati (*INF-AM01 e INF-AM02*).

L'appendice include inoltre gli indicatori dedicati all'analisi del rischio, attraverso una metrica che misura la percentuale di risorse critiche testate periodicamente contro vulnerabilità note. Questa misura consente di quantificare la copertura effettiva delle attività di risk assessment sulla componente infrastrutturale (*INF-RA01*). A essa si aggiunge un insieme articolato di metriche sulla gestione delle identità digitali e degli accessi, che valutano la conformità delle credenziali ai principi di segregazione delle funzioni e privilegio minimo, la protezione degli accessi fisici alle risorse critiche, la sicurezza degli accessi remoti e la corretta amministrazione dei privilegi. Ogni metrica è espressa come percentuale di risorse o accessi gestiti secondo precisi requisiti documentati, permettendo una valutazione oggettiva della postura di sicurezza (*INF-AC01, INF-AC02, INF-AC03 e INF-AC04*).

Arricchiscono il quadro le metriche dedicate al backup e alla manutenzione dei sistemi, che analizzano rispettivamente la regolarità dell'esecuzione dei backup, la loro verifica periodica tramite test di ripristino e la conformità della manutenzione remota alle procedure di autorizzazione previste. La presenza di indicatori su questi aspetti consente di verificare la capacità dell'infrastruttura di garantire ripristinabilità, tracciabilità degli interventi di manutenzione e protezione durante l'accesso remoto da parte di personale interno o esterno (*INF-BA01, INF-MA01 e INF-MA02*).

Infine, l'appendice riporta le metriche relative al monitoraggio continuo della sicurezza, con indicatori che misurano l'efficacia dei sistemi di rilevamento delle intrusioni, la capacità di monitorare gli eventi di sicurezza e il livello di protezione anti-malware delle postazioni terminali. Queste metriche, basate sulla percentuale di eventi di sicurezza rilevati e sulla copertura degli strumenti di protezione, consentono di valutare la maturità dell'organizzazione nel rilevamento tempestivo delle minacce e nella protezione contro i malware(*INF-DE01 e INF-DE02*).

Il set di questi KPI rende concreta l'implementazione del pilastro *Infrastruttura*, traducendo principi e requisiti teorici in strumenti misurabili applicati alla gestione reale dei sistemi. La Tabella 3.2 ne sintetizza i principali indicatori e target di riferimento, costituendo la base per la successiva fase di rendicontazione e monitoraggio.

| ID | Ambito | Tipo di misura | Obiettivo | Formula principale | Target | Note |
|---|---|---|---|---|---|---|
| **INF-A01** | Disponibilità | Efficacia | Garantire continuità e qualità dei servizi ICT | $(1 - \frac{\text{downtime}}{\text{tempo tot.}}) \times 100$ | $\geq$ 99,98% (no fermi) $\geq$ 99,6% (con fermi) | |
| **INF-DC01** | Sicurezza Data Center (fisica) | Implementazione | Conformità ai requisiti infrastrutturali e antincendio | $(\frac{\text{Req. soddisfatti}}{\text{Req. totali}}) \times 100$ | 100% dei 5 requisiti | *5 Requisiti dettagliati nel documento integrale* |
| **INF-DC02** | Sicurezza Data Center (ambientale) | Implementazione | Protezione fisica e ambientale | $(\frac{\text{Misure implem.}}{\text{Totale previste}}) \times 100$ | 100,00% | *Misure fisiche e ambientali dettagliate nel doc. integrale* |
| **INF-AM01** | Asset Management (fisico) | Implementazione + Efficacia | Tracciabilità gestione dispositivi fisici | $(\frac{\text{Dispositivi censiti}}{\text{Totale rilevati}}) \times 100$ | 100,00% | |
| **INF-AM02** | Gestione flussi dati | Implementazione + Efficacia | Tracciabilità e approvazione dei flussi informativi | $(\frac{\text{Flussi censiti}}{\text{Totale rilevati}}) \times 100$ | 100,00% | |
| **INF-RA01** | Analisi del rischio | Implementazione + Efficacia | Testing periodico delle vulnerabilità delle risorse | $(\frac{\text{Risorse testate}}{\text{Risorse totali}}) \times 100$ | 100% annualmente | |
| **INF-AC01** | Identità digitali | Implementazione + Efficacia | Gestione sicura delle credenziali di accesso | $(\frac{\text{Credenziali conformi}}{\text{Totale credenziali}}) \times 100$ | 100% conf. ai 6 requisiti | *6 requisiti dettagliati nel documento integrale* |
| **INF-AC02** | Accesso fisico | Implementazione + Efficacia | Protezione e amministrazione dell'accesso fisico | $(\frac{\text{Risorse protette}}{\text{Totale critiche}}) \times 100$ | 100,00% | *Requisiti di protezione dettagliati nel doc. integrale* |

*Continua nella pagina successiva*

| ID | Ambito | Tipo di misura | Obiettivo | Formula principale | Target | Note |
|---|---|---|---|---|---|---|
| **INF-AC03** | Accesso remoto | Implementazione + Efficacia | Sicurezza degli accessi remoti alle risorse | $(\frac{\text{Accessi sicuri}}{\text{Totale accessi}}) \times 100$ | 100,00% | *Requisiti di sicurezza dettagliati nel doc. integrale* |
| **INF-AC04** | Privilegi minimi e sep. ruoli | Implementazione + Efficacia | Accesso coerente a dati e sistemi | $(\frac{\text{Utenti sec. policy}}{\text{Totale}}) \times 100$ | 100,00% | *Policy elencate nel documento integrale* |
| **INF-BA01** | Backup | Conformità | Sicurezza e verifica dei backup | $(\frac{\text{Backup eseguiti}}{\text{Totale pianificati}}) \times 100$ | 100%, test annuale | |
| **INF-MA01** | Manutenzione remota | Conformità | Accessi remoti autorizzati e sicuri | $(\frac{\text{Manutenz. conformi}}{\text{Totale manutenz.}}) \times 100$ | 100% autoriz. preventive | *Requisiti di conformità elencati nel doc. integrale* |
| **INF-MA02** | Sicurezza perimetrale | Conformità | Configurazione e aggiornamento corretto sistemi di rete | $(\frac{\text{Firewall corretti}}{\text{Totale sistemi}}) \times 100$ | 100,00% | |
| **INF-DE01** | IDS e monitoraggio | Performance | Rilevamento eventi di sicurezza attraverso IDS | $(\frac{\text{Eventi rilevati}}{\text{Totale eventi}}) \times 100$ | 100,00% | |
| **INF-DE02** | Protezione anti-malware | Performance | Protezione endpoint e revisione policy | $(\frac{\text{Postazioni protette}}{\text{Totale}}) \times 100$ e/o $(\frac{\text{Malware rilevati}}{\text{Eventi malware}}) \times 100$ | 100% protez. postazioni | *Policy rivista annualmente* |

**Tabella 3.2:** Metriche definite per il pilastro *Infrastruttura*

### 3.1.3 Metriche del pilastro Compliance tecnico-normativa

Il terzo pilastro del modello di valutazione proposto riguarda la *Compliance* tecnico-normativa, ovvero la capacità dell'organizzazione di garantire la conformità alle disposizioni legislative, regolamentari e tecniche che disciplinano la sicurezza informatica e la protezione dei dati. In un contesto istituzionale come quello della Regione Piemonte, che rientra nella categoria dei soggetti importanti secondo la classificazione definita dall'ACN in attuazione della Direttiva NIS 2 [1], tale dimensione assume un ruolo strategico. La conformità

normativa non rappresenta soltanto un obbligo di legge, ma costituisce una componente essenziale della resilienza digitale e della accountability istituzionale, poiché garantisce che le misure di sicurezza adottate siano coerenti con gli standard nazionali e internazionali e che siano caratterizzate da elementi verificabili nel tempo.

La definizione delle metriche associate a questo pilastro si basa sul Framework Nazionale per la Cybersecurity e la Data Protection – Edizione 2025 (v2.1) [13], documento che recepisce e adatta al contesto italiano la versione 2.0 del NIST Cybersecurity Framework (CSF) [12]. Tale framework rappresenta oggi uno strumento di riferimento per la strutturazione dei programmi di sicurezza, poiché integra aspetti tecnici, organizzativi e gestionali e fornisce una visione sistemica della sicurezza basata su funzioni, categorie e sotto-categorie di controllo. In parallelo, sono stati considerati i contenuti della Determinazione ACN n. 164179/2025 [22], che definisce le misure di sicurezza di base per i soggetti pubblici e privati classificati come *essenziali* ed *importanti*. In particolare, i criteri di classificazione dei soggetti sono definiti in base alla detenzione diretta di infrastrutture informatiche, come i *data center*, che ospitano servizi considerati critici. Di conseguenza, la Regione Piemonte, delegando tale aspetto al CSI Piemonte, è classificata come soggetto *importante*, rientrando comunque nel perimetro di tale determinazione. Questa sinergia metodologica ha permesso di costruire un insieme coerente di metriche che rispondono ai requisiti minimi di sicurezza nazionale, ma al tempo stesso risultano adattabili e misurabili nel contesto operativo della Regione Piemonte.

L'obiettivo di questo pilastro è quindi quello di valutare il grado di aderenza delle pratiche e dei processi regionali ai principali standard di sicurezza e alle misure richieste dall'ACN, fornendo uno strumento di misurazione che consenta di monitorare in modo continuo l'evoluzione della maturità organizzativa. A differenza dei pilastri *Codice* e *Infrastruttura*, in cui la misurazione si focalizza su elementi prevalentemente tecnici, la *Compliance* si concentra sugli aspetti procedurali, gestionali e documentali che garantiscono la sostenibilità delle misure di sicurezza nel lungo periodo. In quest'ottica, le metriche diventano un indicatore della capacità dell'organizzazione di mantenere nel tempo un livello adeguato di controllo, consapevolezza e governance del rischio inerente alla cybersecurity.

Il processo di individuazione delle metriche è stato condotto partendo dalla mappatura tra le categorie funzionali del Framework Nazionale (*Govern*, *Identify*, *Protect*, *Detect*, *Respond*, *Recover*) e le misure previste nell'allegato tecnico ACN. Questa correlazione ha permesso di selezionare e adattare le misure più pertinenti per il contesto regionale, ponendo particolare attenzione alle aree che influenzano direttamente la gestione applicativa e infrastrutturale dei servizi ICT. Le metriche sono state di conseguenza formalizzate secondo la stessa struttura adottata per i precedenti pilastri, basata sulla metodologia del NIST, assicurando coerenza semantica e comparabilità dei risultati.

Le metriche specifiche definite per il pilastro *Compliance* sono descritte in modo esteso nel documento tecnico allegato alla presente tesi come appendice C. L'appendice presenta l'insieme delle metriche e dei KPI che permettono di valutare in modo strutturato la maturità dell'organizzazione in relazione alla gestione del rischio inerente alla cybersecurity, alla definizione delle responsabilità, alla gestione della supply chain e alla capacità di risposta e recupero dagli incidenti.

Una prima area approfondita è quella relativa alla funzione *Govern*, che include metriche orientate a verificare la chiarezza del contesto organizzativo, l'integrazione della cybersecurity nei processi di gestione del rischio e la formalizzazione dei ruoli e delle responsabilità all'interno delle diverse unità organizzative. Le metriche consentono di misurare, ad esempio, la percentuale di progetti che documentano esplicitamente gli obiettivi degli stakeholder, la presenza di processi di gestione del rischio o la completezza della definizione dei ruoli di sicurezza nelle strutture ICT. Sono inoltre presenti indicatori volti a misurare il grado di integrazione della cybersecurity nei processi delle risorse umane, così come la qualità e l'aggiornamento delle policy aziendali, attraverso misure quali l'allineamento ai requisiti strategici e l'età media delle revisioni delle policy. Una parte sostanziale delle metriche afferisce alla gestione del rischio nella supply chain ICT. L'appendice comprende infatti indicatori che valutano la presenza di strategie di sicurezza formalizzate nei contratti, la chiarezza dei ruoli e delle responsabilità tra fornitori e partner, la percentuale di fornitori classificati in base alla criticità *cyber* e il livello di inclusione delle clausole di sicurezza nei contratti. È inoltre definita una metrica che verifica la presenza di piani di gestione del rischio per i fornitori critici, indicando il livello di efficacia con cui l'organizzazione monitora e governa i rischi derivanti dalla propria catena di approvvigionamento tecnologica. Rientrano in questa area le metriche: *CTN-GV.OC01, CTN-GV.RM01 , CTN-GV.RR01, CTN-GV.RR02, CTN-GV.PO01 , CTN-GV.PO02, CTN-GV.SC01, CTN-GV.SC02, CTN-GV.SC03, CTN-GV.SC04 e CTN-GV.SC05.*

La funzione *Identify* comprende le metriche dedicate alla valutazione del rischio e ai processi di miglioramento continuo. Tali indicatori misurano la completezza delle analisi di rischio svolte, verificando l'inclusione di minacce, vulnerabilità, probabilità e impatti, nonché la qualità delle risposte pianificate per i rischi classificati come medio-alti. È inoltre prevista una metrica dedicata all'esistenza di un processo attivo di individuazione delle vulnerabilità, espressa come KPI binario. Completano questa sezione le misure relative ai piani di risposta agli incidenti, che valutano la percentuale di piani aggiornati e testati negli ultimi dodici mesi, a conferma della capacità dell'organizzazione di mantenere allineate le proprie procedure operative. Rientrano in questa area le metriche: *CTN-ID.RA, CTN-ID.RA02 , CTN-ID.RA03 e CTN-ID.IM01.*

Nell'appendice è presente anche una metrica collegata alla funzione *Protect*, dedicata alla formazione del personale in materia di cybersecurity. Essa consente di misurare la percentuale di dipendenti che hanno completato percorsi formativi negli ultimi dodici mesi, offrendo così un indicatore chiave della diffusione della consapevolezza e della cultura della sicurezza all'interno dell'organizzazione (*CTN-PR.AT01*).

Le ultime aree considerate riguardano le funzioni *Respond* e *Recover*, con metriche orientate alla gestione degli incidenti e al successivo ripristino operativo. La prima misura la percentuale di incidenti gestiti con corretto coordinamento con terze parti sulla base del piano di risposta, mentre la seconda valuta la tempestività delle comunicazioni verso gli stakeholder in caso di incidenti notificabili, verificando il rispetto delle finestre temporali richieste (24/48 ore). La metrica di recupero, infine, misura la percentuale di piani di ripristino eseguiti nei tempi previsti, fornendo un indicatore chiave dell'efficacia dell'organizzazione nel ristabilire la continuità operativa dopo un incidente. Rientrano in queste aree le metriche: *CTN-RS.MA01, CTN-RS.CO01 e CTN-RC.RP01.*

Nel complesso, l'appendice rende chiaro e misurabile il livello di aderenza dell'organizzazione ai requisiti normativi e agli standard di cybersecurity. Le metriche forniscono un insieme coerente e verificabile di criteri che permettono di valutare il grado di formalizzazione dei processi, la qualità della gestione del rischio, la robustezza delle relazioni con i fornitori e la capacità di prevenire, rilevare, gestire e recuperare da incidenti di sicurezza informatica, trasformando le prescrizioni normative in elementi concreti di valutazione e monitoraggio. Esse rappresentano un punto di raccordo tra gli aspetti tecnici misurati nei pilastri *Codice* e *Infrastruttura* e la dimensione gestionale e documentale della sicurezza, abilitando un processo di miglioramento continuo basato su evidenze oggettive. La Tabella 3.3 ne offre una sintesi complessiva, riportando i principali indicatori, obiettivi e soglie di riferimento. Tali elementi costituiranno la base operativa per le successive attività di rendicontazione, monitoraggio continuo e valutazione dell'efficacia delle misure di sicurezza nel tempo.

| **ID** | **Ambito** | **Tipo di misura** | **Obiettivo** | **Formula principale** | **Target** | **Note** |
|---|---|---|---|---|---|---|
| **CTN-GV.OC01** | GOVERN - Contesto organizzativo | Implementazione | Verificare comprensione e comunicazione obiettivi/servizi attesi degli stakeholder | $\frac{N\_prog\_DOC}{N\_prog\_TOT} \times 100$ | $\geq 95\%$ | |
| **CTN-GV.RM01** | GOVERN - Strategia di gestione del rischio | Implementazione | Integrazione gestione rischio cyber nei processi di risk management | $\frac{N\_proc\_CYBER}{N\_proc\_TOT} \times 100$ | $\geq 90\%$ | |
| **CTN-GV.RR01** | GOVERN - Ruoli e responsabilità | Implementazione | Formalizzazione e applicazione ruoli e responsabilità cyber | $\frac{N\_unit\_CYBER}{N\_unit\_TOT} \times 100$ | 100% | |
| **CTN-GV.RR02** | GOVERN - Integrazione Cybersecurity in ambito HR | Implementazione | Integrazione della cybersecurity nei processi HR | $\frac{N\_HR\_CYBER}{N\_HR\_TOT} \times 100$ | 100% | |

*Continua nella pagina successiva*

| ID | Ambito | Tipo di misura | Obiettivo | Formula principale | Target | Note |
|---|---|---|---|---|---|---|
| **CTN-GV.PO01** | GOVERN - Policy cybersecurity | Implementazione | Allineamento policy con strategia, priorità, contesto | $\frac{N\_req\_OK}{N\_req\_TOT} \times 100$ | 100% | *L'elenco dei requisiti è dettagliato nel documento integrale* |
| **CTN-GV.PO02** | GOVERN - Revisione policy di sicurezza | Qualità | Mantenimento aggiornato policy di sicurezza | media (Mesi_ultima_REV) | $\leq$ 12 mesi | |
| **CTN-GV.SC01** | GOVERN - Supply chain: strategia | Implementazione | Formalizzazione e strategia cyber nella supply chain | $\frac{N\_Contr\_CYBER}{N\_Contr\_TOT} \times 100$ | $\geq 90\%$ | |
| **CTN-GV.SC02** | GOVERN - Supply chain: ruoli e responsabilità | Implementazione | Ruoli e responsabilità cyber condivisi con i partner | $\frac{N\_Contr\_ruoli\_CYBER}{N\_Contr\_TOT} \times 100$ | 100% | |
| **CTN-GV.SC03** | GOVERN - Supply chain: classificazione fornitori | Qualità | Classificazione rischio cyber dei fornitori | $\frac{N\_Form\_CLASS}{N\_Form\_TOT} \times 100$ | $\geq 95\%$ | |
| **CTN-GV.SC04** | GOVERN - Supply chain: clausole | Implementazione | Integrazione clausole cybersecurity nei contratti | $\frac{N\_Contr\_CLAUS}{N\_Contr\_TOT} \times 100$ | $\geq 90\%$ | |
| **CTN-GV.SC05** | GOVERN - Supply chain: gestione rischio fornitori | Efficacia | Gestione attiva del rischio fornitori critici | $\frac{N\_Form\_PIANO}{N\_Form\_TOT} \times 100$ | 100% | |

*Continua nella pagina successiva*

| ID | Ambito | Tipo di misura | Obiettivo | Formula principale | Target | Note |
|---|---|---|---|---|---|---|
| **CTN-ID.RA01** | IDENTIFY - Risk Assessment: elementi | Completezza | Inclusione minacce, vulnerabilità, probabilità, impatti | $\frac{N\_RA\_completi}{N\_RA\_TOT} \times 100$ | $\geq 95\%$ | |
| **CTN-ID.RA02** | IDENTIFY - Risk Assessment: risposta | Efficacia | Documentazione e monitoraggio risposta ai rischi | $\frac{N\_rischi\_GEST}{N\_rischi\_TOT} \times 100$ | $\geq 95\%$ | |
| **CTN-ID.RA03** | IDENTIFY - Disclosure vulnerabilità | KPI binario | Esistenza processo di vulnerability disclosure | Si/No | Sì | |
| **CTN-ID.IM01** | IDENTIFY - Miglioramento: IR Plan | Qualità | Test e aggiornamento annuale piani IR | $\frac{N\_piani\_TEST}{N\_piani\_TOT} \times 100$ | 100% | |
| **CTN-PR.AT01** | PROTECT - Formazione personale | Conformità | Formazione Cybersecurity per tutto il personale | $\frac{N\_pers\_FORM}{N\_pers\_TOT} \times 100$ | $\geq 90\%$ | |
| **CTN-RS.MA01** | RESPOND - Coordinamento con terze parti | Esecuzione | Esecuzione piani IR con terze parti | $\frac{N\_inc\_COORD}{N\_inc\_TOT} \times 100$ | 100% | |
| **CTN-RS.C001** | RESPOND - Comunicazione tempestiva | Tempestività | Comunicazione agli stakeholder entro 24/48h | $\frac{N\_not\_TEMP}{N\_not\_TOT} \times 100$ | $\geq 95\%$ | |
| **CTN-RC.RP01** | RECOVER - Ripristino post-incidenti | Efficacia | Esecuzione piani di recovery nei tempi previsti | $\frac{N\_ripr\_TEMP}{N\_ripr\_TOT} \times 100$ | 100% | |

**Tabella 3.3:** Metriche definite per il pilastro *Compliance* tecnico-normativa

## 3.2 Progettazione sistema di rendicontazione

La progettazione del sistema di rendicontazione rappresenta il passaggio operativo che consente di tradurre le metriche e i principi metodologici definiti nelle sezioni precedenti in un modello applicativo concreto, capace di integrarsi nei processi amministrativi e tecnici della Regione Piemonte. Tale sistema costituisce uno degli elementi centrali del modello di sicurezza proposto, poiché consente di strutturare la raccolta, la validazione e la valutazione delle informazioni relative al livello di sicurezza delle applicazioni, garantendo coerenza e tracciabilità in ogni fase del ciclo di vita del software.

I risultati attesi della presente sezione sono:

- analisi e modellazione dei processi di affidamento software presenti in Regione Piemonte;
- progettazione di un sistema di rendicontazione innestato nei processi dell'Ente e suddiviso in fasi;
- sviluppo di un framework operativo per la rendicontazione delle metriche associate alla specifica fase del ciclo applicativo;

Nel contesto della Regione Piemonte, la progettazione è stata guidata da un principio cardine: integrare la rendicontazione della sicurezza nei processi già esistenti, evitando di introdurre sovrastrutture burocratiche o procedure parallele. Il sistema è stato pertanto concepito per innestarsi all'interno delle fasi operative previste dalla Convenzione Quadro [16] in essere con il CSI Piemonte, seguendo la logica già consolidata delle procedure di verifica di congruità tecnico-economica.

L'integrazione con i processi di acquisizione regionale si potrà concretizzare già nella fase di pre-validazione delle offerte, durante la quale i referenti ICT, in collaborazione con il Settore Sistema Informativo Regionale, effettuano la valutazione preliminare della congruità tecnico-economica delle proposte. È in questo momento che il sistema di rendicontazione trova la sua prima applicazione, consentendo di introdurre fin da subito criteri di sicurezza strutturati nella valutazione delle offerte. Successivamente, le fasi di verifica tecnica dei rilasci, di chiusura del progetto e di monitoraggio continuo diventano gli ulteriori momenti di applicazione del modello, garantendo un controllo costante e documentato lungo l'intero ciclo di vita del software.

Il sistema di rendicontazione progettato nel lavoro di tesi è articolato in quattro fasi principali, corrispondenti alle macro-fasi del ciclo di vita di una fornitura software. Questa suddivisione risponde all'esigenza di rendere il processo modulare e adattabile, mantenendo tuttavia un filo logico di continuità tra una fase e l'altra. Le fasi sono sequenziali, ma non indipendenti: ciascuna raccoglie informazioni che costituiscono la base per le successive, generando uno storico di sicurezza applicativa che consente di valutare l'evoluzione della conformità nel tempo.

La prima fase, denominata congruità dell'offerta, si colloca prima dell'affidamento e riguarda la verifica preliminare della proposta tecnico-economica (PTE) presentata dal fornitore. In questa fase il sistema di rendicontazione viene utilizzato per valutare la

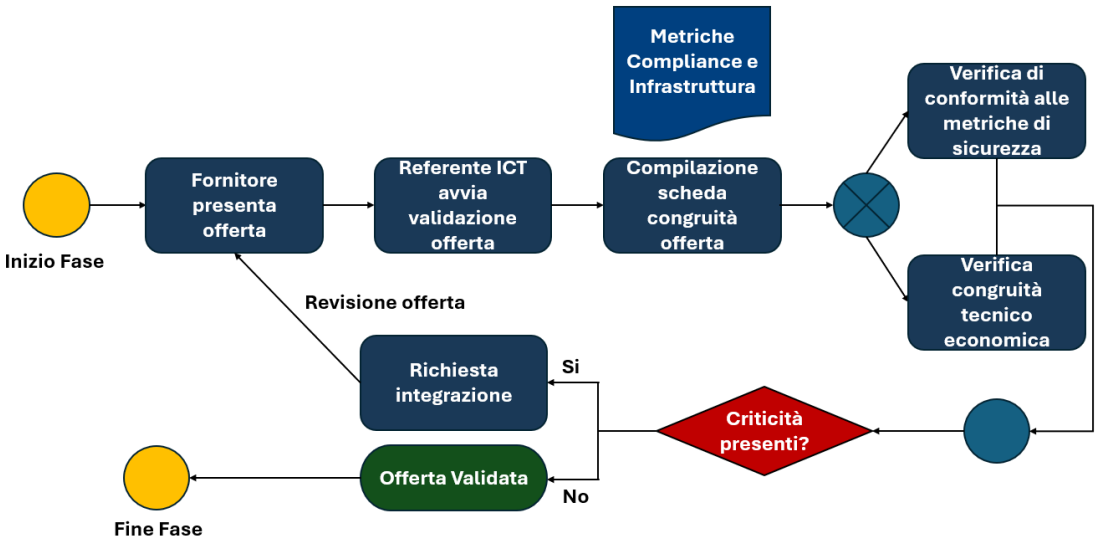


**Figura 3.2:** Diagramma di flusso di massima della fase di congruità dell'offerta, prima fase delineata nel contesto del sistema di rendicontazione del modello operativo proposto nella presente tesi. Elaborazione dell'autore

conformità iniziale dell'offerta rispetto ai requisiti minimi di sicurezza infrastrutturale e di compliance tecnico-normativa. Lo strumento principale è la *Scheda di Congruità dell'Offerta*, che consente ai referenti ICT, in collaborazione con il Settore SIRe e con il RUP, di verificare la completezza e la solidità delle misure di sicurezza dichiarate. Il processo culmina con la produzione di una checklist di valutazione, generabile a partire dal framework, che può determinare la necessità di integrazioni o modifiche alla proposta tecnica. Questa fase ha un ruolo strategico nel prevenire la successiva insorgenza di criticità, consentendo di rilevare tempestivamente eventuali carenze documentali o di sicurezza prima della stipula contrattuale.

Come rappresentato in Figura 3.2, il flusso di questa fase ha inizio con la presentazione dell'offerta da parte dei fornitori. Successivamente il referente ICT preposto avvia la validazione dell'offerta, compilando il report di congruità che, nel sistema di rendicontazione progettato, include anche le metriche dei pilastri *Infrastruttura* e *Compliance*. Dopo aver verificato la conformità alle metriche di sicurezza e i criteri di congruità generale, il referente analizza le possibili criticità: se non vengono riscontrate, l'offerta viene validata e la fase termine; di contro se vengono riscontrate criticità, viene mandata la richiesta di integrazione al fornitore, che riformulerà l'offerta, facendo ripartire il flusso associato alla fase.

La seconda fase, denominata ciclo di vita dello sviluppo del software, è applicata a ogni componente o prodotto rilasciato nel corso del progetto. Essa costituisce il cuore operativo del sistema di rendicontazione, in quanto consente di misurare in modo puntuale la qualità e la sicurezza del codice attraverso le metriche del pilastro *Codice*. Lo strumento

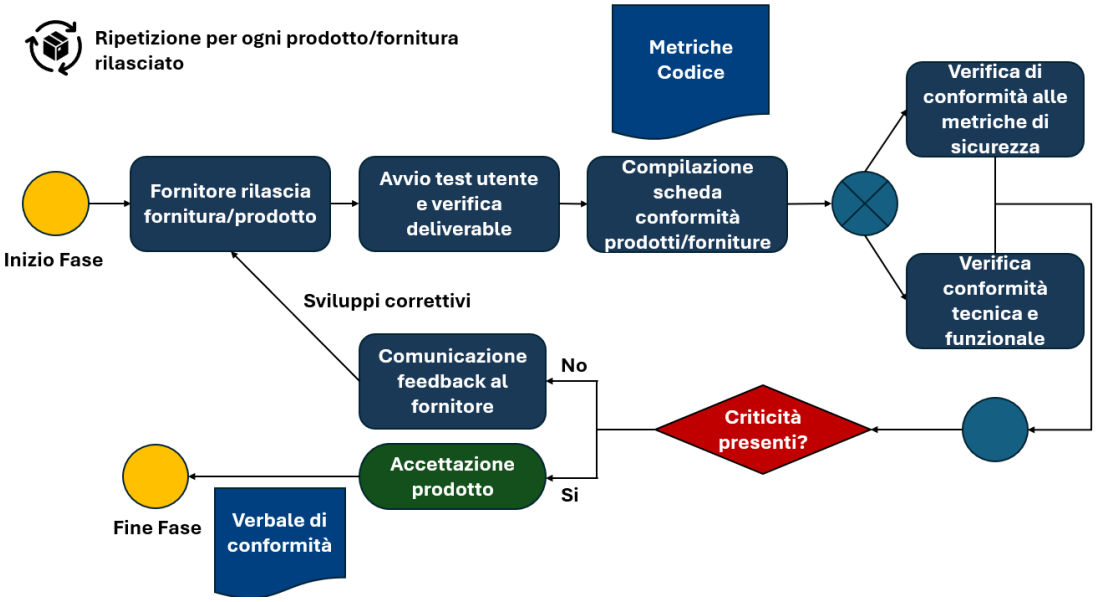


**Figura 3.3:** Diagramma di flusso di massima della fase di ciclo di vita dello sviluppo del software, seconda fase delineata nel contesto del sistema di rendicontazione del modello operativo proposto nella presente tesi. Elaborazione dell'autore

di riferimento è la *Scheda di Conformità Prodotti-Forniture*, compilata dal fornitore e verificata dal referente ICT, che registra i valori delle metriche relative al codice sorgente e ai processi di sviluppo. L'output di questa fase è un verbale di conformità, che, insieme alle analisi già svolte nel processo attualmente utilizzato in Regione Piemonte, sintetizza l'esito della verifica e stabilisce se la fornitura può essere accettata o se necessita di correzioni. La rendicontazione di questa fase è particolarmente rilevante perché consente di costruire una base dati storica sui livelli di sicurezza del software fornito e di promuovere la progressiva maturazione dei processi di sviluppo.

Come rappresentato in Figura 3.3, il flusso di questa fase ha inizio con il rilascio della fornitura/prodotto da parte dei fornitori. Successivamente il referente ICT preposto avvia il test utente e la verifica dei *deliverables* previsti, compilando la scheda di conformità che, nel sistema di rendicontazione progettato, include anche le metriche del pilastro *Codice*. Dopo aver verificato la conformità alle metriche di sicurezza e i criteri di conformità tecnica e funzionale, il referente analizza le possibili criticità: se non vengono riscontrate, il prodotto viene accettato e la fase termina; di contro se vengono riscontrate criticità, viene comunicato il *feedback* al fornitore, che correggerà le criticità del prodotto/fornitura, facendo ripartire il flusso associato alla fase. Questa fase viene ripetuta per ogni prodotto/fornitura rilasciato dal fornitore.

La terza fase, denominata chiusura del progetto, si applica al termine delle attività di sviluppo di tutte le forniture della progettualità e ha l'obiettivo di consolidare e aggiornare le metriche registrate nelle fasi precedenti. Essa prevede l'utilizzo della *Scheda di Conformità*

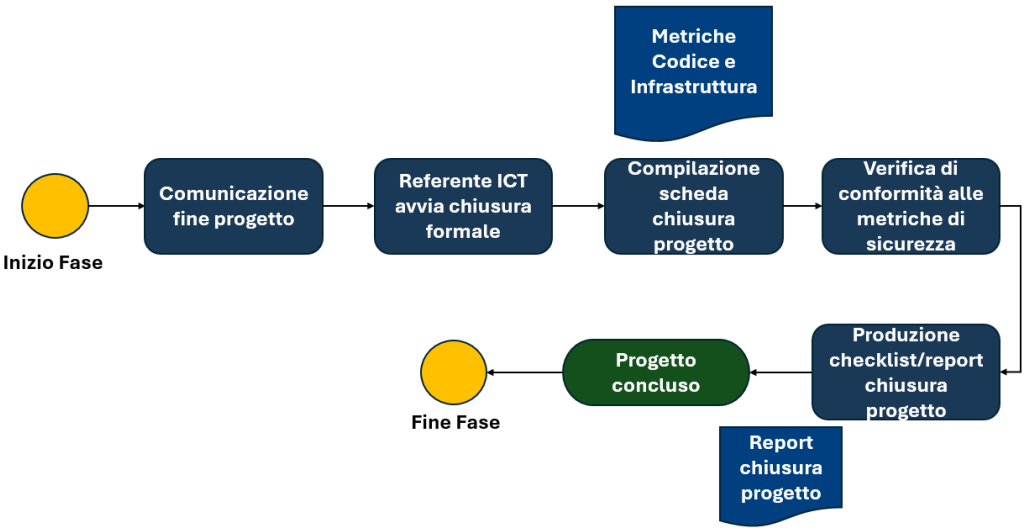


**Figura 3.4:** Diagramma di flusso di massima della fase di chiusura del progetto, terza fase delineata nel contesto del sistema di rendicontazione del modello operativo proposto nella presente tesi. Elaborazione dell'autore

*di Chiusura Progetto*, che raccoglie i dati relativi alle metriche dei pilastri *Infrastruttura* e *Codice*. In questa fase si procede a una verifica finale a cura del referente ICT, finalizzata a produrre il report conclusivo che documenta la postura di sicurezza del progetto nel suo complesso. Questo report rappresenta un documento di chiusura che potrà essere parte dell'archivio storico delle valutazioni di sicurezza applicativa della Regione. L'inclusione di questa fase di chiusura risponde all'esigenza di garantire un allineamento tra le valutazioni effettuate nel corso del progetto e lo stato effettivo della soluzione in esercizio.

Come rappresentato in Figura 3.4, il flusso di questa fase ha inizio con la comunicazione di fine progetto da parte dei fornitori. Successivamente il referente ICT preposto avvia la chiusura formale, compilando la scheda di chiusura progetto che, nel sistema di rendicontazione progettato, include anche le metriche dei pilastri *Codice* e *Infrastruttura*. Dopo aver verificato la conformità alle metriche di sicurezza, il referente produce una checklist/report di chiusura progetto e termina la formalizzazione della chiusura congiuntamente alla fase.

La quarta fase, denominata monitoraggio continuo del post-progetto, estende la rendicontazione oltre la chiusura formale, consentendo un controllo periodico e ciclico del livello di sicurezza del software nel tempo. Essa rappresenta la componente più innovativa del modello, poiché introduce la dimensione della sorveglianza costante, in linea con i principi di monitoraggio continuo promossi dal NIST. Le verifiche sono previste ad intervalli minimi di sei mesi per tutte le metriche, ridotti a tre mesi per quelle considerate e classificate critiche, sulla base delle peculiarità specifiche della progettualità, o immediatamente in seguito a eventi significativi come incidenti di sicurezza, aggiornamenti strutturali del codice e variazioni di carattere infrastrutturale. In questa fase la *Scheda di Monitoraggio*

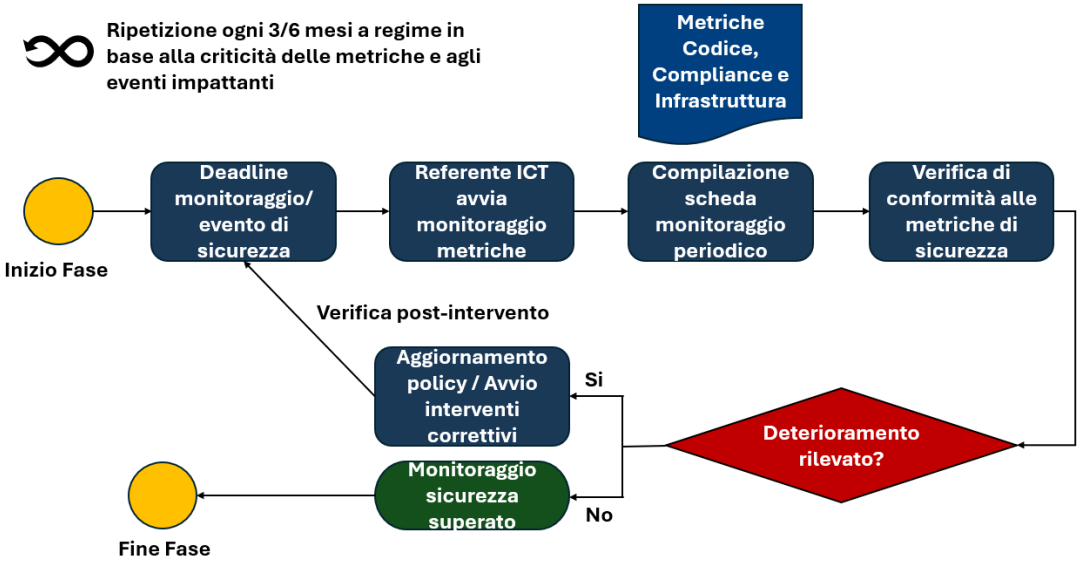


**Figura 3.5:** Diagramma di flusso di massima della fase di monitoraggio periodico, quarta fase delineata nel contesto del sistema di rendicontazione del modello operativo proposto nella presente tesi. Elaborazione dell'autore

*Periodico* permette di confrontare i valori attuali con quelli storici, individuando eventuali deterioramenti o deviazioni e attivando, se necessario, procedure di aggiornamento o interventi correttivi. Questo approccio garantisce non solo la conservazione del livello di sicurezza, ma anche la possibilità di apprendimento e miglioramento continuo del modello, rendendo la gestione della sicurezza un processo dinamico e iterativo.

Come rappresentato in Figura 3.5, il flusso di questa fase ha inizio con il raggiungimento di una *deadline* di monitoraggio o con l'avvenimento di un evento di sicurezza. Successivamente il referente ICT preposto avvia il monitoraggio delle metriche, compilando la scheda di monitoraggio periodico che, nel sistema di rendicontazione progettato, include le metriche dei pilastri *Codice*, *Infrastruttura* e *Compliance*. Dopo aver verificato la conformità alle metriche di sicurezza, il referente analizza la presenza di deterioramento nei valori delle metriche: se non vengono riscontrate, il monitoraggio viene superato con successo e la fase termine; di contro se vengono riscontrati deterioramenti, vengono aggiornate le policy di sicurezza e avviati interventi correttivi, facendo ripartire il flusso associato alla fase con delle verifiche post intervento. Le *deadline* di monitoraggio sono definite sulla base delle criticità delle metriche, ad intervalli regolari di tre/sei mesi.

Le fasi descritte trovano concreta applicazione attraverso il prototipo del framework di rendicontazione, primo risultato operativo della presente tesi, sviluppato con l'ausilio di strumenti operativi quali i fogli di calcolo. Questo strumento rappresenta l'ossatura del sistema, fornendo un insieme di schede e moduli che guidano gli attori coinvolti nella compilazione e nella verifica delle metriche. Ogni fase dispone di una propria scheda di

rendicontazione, nella quale sono elencate le metriche pertinenti con le relative formule, soglie di conformità e spazi per l'inserimento, qualora non venga raggiunto il target per la relativa metrica, di azioni di mitigazione. Il documento tecnico contentente le schede è allegato alla presente tesi ed identificato come appendice D.

Il framework implementa un indicatore sintetico di conformità, calcolato come il rapporto percentuale tra il numero di metriche che raggiungono il valore target e il numero totale di metriche previste per la fase. Questo indicatore, espresso in forma percentuale, consente di ottenere una misura immediata e comparabile del livello di conformità raggiunto in ciascuna fase del processo. L'adozione di un indicatore univoco favorisce la costruzione di una base dati coerente, che potrà essere successivamente utilizzata per generare cruscotti di controllo e confronti longitudinali tra progetti, fornitori e tipologie di software. Oltre all'indicatore di conformità, che offre una misura complessiva dell'impatto relativo alla fase analizzata, il framework prevede, per ciascuna metrica, che qualora il valore rilevato non raggiunga il target stabilito, vengano obbligatoriamente specificate le azioni di mitigazione da intraprendere per colmare le eventuali lacune emerse in sede di rendicontazione. In tal modo, il sistema guida in modo strutturato i processi connessi alla sicurezza applicativa verso il conseguimento di una piena *compliance*.

Dal punto di vista organizzativo, il sistema di rendicontazione è stato progettato per coinvolgere in modo coordinato tutti i soggetti che partecipano al processo di acquisizione e gestione del software. La responsabilità diretta della compilazione è condivisa tra i fornitori, che comunicano le informazioni volte alla rendicontazione delle metriche relative ai propri prodotti, includendo talvolta la possibilità di compilazione diretta delle metriche stesse in presenza di sub-fornitori esterni, e i referenti ICT regionali, che rendicontano le metriche e ne verificano la correttezza e la completezza. Il Settore SIRe esercita un ruolo di controllo trasversale, assicurando la coerenza metodologica e supervisionando le fasi dalla pre-validazione al monitoraggio continuo. La validazione incrociata delle rendicontazioni sarà prevista nella fase di redazione della congruità tecnico-economica, attraverso la firma congiunta del RUP del settore committente e del Dirigente dei Sistemi Informativi.

L'implementazione del sistema ha inoltre una forte valenza strategica, poiché getta le basi per la creazione di un archivio storico delle valutazioni di sicurezza delle applicazioni regionali. Questo archivio potrà essere utilizzato per condurre analisi comparative, individuare trend di rischio e definire benchmark tra soluzioni e fornitori, contribuendo alla costruzione di un ecosistema di fornitura più maturo e orientato alla qualità. In prospettiva, il sistema potrà inoltre essere collegato agli indicatori ICT presenti nei Piani Triennali ICT Regionali, costituendo un elemento di raccordo tra la dimensione operativa della sicurezza e la pianificazione strategica.

Nel complesso, la progettazione del sistema di rendicontazione rappresenta dunque il primo passo verso una gestione strutturata e basata su evidenze della sicurezza applicativa nel contesto regionale. Essa fornisce un metodo oggettivo per misurare, documentare e comunicare il livello di conformità dei progetti software ai requisiti di sicurezza, ponendosi come anello di congiunzione tra le attività operative di sviluppo e le funzioni di governance strategica della Regione Piemonte. Il valore principale del sistema risiede nella sua capacità di trasformare le verifiche di sicurezza da adempimenti episodici a processi sistematici, inseriti organicamente nel ciclo di vita dell'acquisizione e della manutenzione delle soluzioni

ICT.

La successiva sezione, dedicata alla progettazione del sistema di monitoraggio e controllo, approfondirà le analisi e il mantenimento del modello stesso, illustrando come i flussi informativi derivanti dal sistema di rendicontazione possano essere utilizzati per costruire un meccanismo di osservazione continua e predittiva della sicurezza applicativa. Verranno esaminati gli aspetti metodologici e architetturali del modello, le logiche di correlazione tra metriche, la definizione delle proprietà portanti, delineando così la transizione verso una gestione guidata dai dati della sicurezza nel sistema informativo regionale piemontese.

## 3.3 Progettazione del sistema di monitoraggio e controllo

Il sistema di monitoraggio e controllo rappresenta la componente conclusiva del modello operativo per la valutazione della sicurezza del software e costituisce l'elemento di garanzia della sua efficacia nel tempo. La sua finalità principale è quella di assicurare che le valutazioni prodotte in fase di rendicontazione trovino riscontro nella realtà operativa, accompagnando l'intero ciclo di vita degli applicativi e dei servizi informativi regionali. Nella progettazione complessiva del modello, se la rendicontazione rappresenta la fase di misurazione e documentazione della sicurezza del software, il monitoraggio e controllo costituiscono invece la fase di verifica e consolidamento, assicurando che il modello, le metriche e le procedure mantengano nel tempo coerenza, affidabilità e aggiornamento rispetto all'evoluzione tecnologica e normativa.

I risultati attesi della presente sezione, che costituiscono la progettazione del sistema di monitoraggio e controllo, sono:

- ridefinire e strutturare la figura del referente ICT per insediarla nel processo di monitoraggio e controllo del modello;
- strutturare la metodologia di monitoraggio tramite incontri periodici tra gli attori coinvolti nel processo;
- definire le proprietà fondamentali del modello per garantirne il presidio e la qualità nel tempo;
- elaborare un set strutturato di criteri di verifica operativi per il monitoraggio dello stato delle proprietà del modello nel tempo;

Il sistema nasce come meccanismo di autoregolazione del modello di sicurezza, concepito per garantire la qualità dei processi di valutazione e per stimolare un miglioramento continuo. Esso ha come obiettivo la verifica della validità del modello di misurazione stesso, attraverso un approccio strutturato, partecipato e ciclico. In tal modo, il sistema di monitoraggio agisce indirettamente anche sulla sicurezza applicativa complessiva, poiché un modello efficace e coerente nel tempo si traduce inevitabilmente in una maggiore capacità dell'Ente di individuare, prevenire e mitigare tempestivamente le vulnerabilità nei propri applicativi.

L'implementazione di tale sistema si inserisce in modo organico all'interno del modello operativo descritto nei capitoli precedenti, configurandosi come il suo livello di supervisione e miglioramento metodologico. In quanto soggetto *importante* secondo la classificazione ACN, la Regione Piemonte necessita di strumenti capaci di garantire non solo la sicurezza dei propri sistemi informativi, ma anche la solidità dei meccanismi di valutazione che ne assicurano il controllo. In questa prospettiva, il monitoraggio assume il ruolo di presidio di qualità metodologica, volto a verificare che il modello rimanga allineato agli standard nazionali e internazionali, che le metriche mantengano il loro valore descrittivo e che le procedure di rendicontazione siano applicate in modo coerente e omogeneo nei diversi contesti organizzativi.

Per garantire l'efficacia e la sostenibilità del sistema di monitoraggio e controllo, la progettazione ha previsto il consolidamento di una rete organizzativa di referenti ICT e di cybersecurity, uno per ciascuna Direzione regionale. Questa rete costituisce l'estensione funzionale e organizzativa del Settore SIRe, assicurando un presidio diffuso sulla sicurezza applicativa e sul corretto utilizzo del modello.

I referenti svolgono nel sistema progettato un duplice ruolo, strettamente interconnesso. Da un lato, operano come attuatori operativi del modello, responsabili dell'applicazione pratica delle metriche, della raccolta delle evidenze e della compilazione dei documenti di rendicontazione. In questo ambito, il loro compito consiste nel garantire che tutte le attività siano tracciate, documentate e coerenti con gli obiettivi di sicurezza stabiliti. Dall'altro lato, i referenti agiscono come osservatori qualificati del sistema, incaricati di individuare criticità, formulare proposte di miglioramento e partecipare attivamente alla revisione del modello. Questa funzione di osservazione e feedback rappresenta un elemento essenziale per mantenere il modello aggiornato, coerente e aderente al contesto operativo. La rete dei referenti diventa così un canale di apprendimento organizzativo che consente di integrare esperienze, segnalazioni e conoscenze, promuovendo una visione distribuita ma coordinata della sicurezza del software. Tale impostazione riduce il rischio di frammentazione informativa e assicura che ogni Direzione possa contribuire attivamente al miglioramento del modello, rendendo il sistema più resiliente e adattivo.

Per il consolidamento della rete dei referenti risulta necessario implementare cicli di formazione periodica, considerata condizione imprescindibile per garantirne l'efficacia nel lungo periodo. La formazione è articolata su due livelli complementari. Il primo è di tipo tematico e ha l'obiettivo di consolidare le competenze in materia di cybersecurity, sicurezza applicativa e gestione del rischio ICT, con particolare attenzione al quadro tecnico e normativo vigente. Il secondo livello è di tipo metodologico, focalizzato sull'applicazione del modello di rendicontazione e sulle procedure di monitoraggio, con il supporto di esercitazioni pratiche e simulazioni su casi reali. Questi percorsi formativi non hanno una funzione meramente didattica, ma rappresentano uno strumento di aggiornamento tecnico e normativo continuo, volto a mantenere elevato il livello di competenza dei referenti e a diffondere una cultura della sicurezza costantemente aggiornata. In tal modo, la formazione diventa parte integrante del processo di monitoraggio, contribuendo a consolidare un ecosistema di competenze condivise in cui la sicurezza viene gestita come responsabilità collettiva e non come prerogativa di pochi specialisti.

Contribuire al rafforzamento delle competenze della rete di referenti ICT, permette di

abilitare il raggiungimento del cuore del sistema di monitoraggio e controllo sviluppato. La fase principale del sistema si sviluppa in modo ciclico e continuativo, attraverso incontri trimestrali tra il Settore SIRe, i referenti ICT e della cybersecurity. Tali incontri rappresentano un'occasione di confronto e di revisione, nella quale vengono analizzati i progressi del modello, le criticità riscontrate, la qualità dei dati rendicontati e le eventuali proposte di aggiornamento. Durante queste sessioni vengono esaminati eventi significativi o casi pratici che possono evidenziare la necessità di modificare, estendere o semplificare il modello. In questo modo, il monitoraggio diventa un processo riflessivo e incrementale, in cui l'esperienza operativa alimenta costantemente l'evoluzione metodologica.

Per garantire una valutazione completa e sistematica, il sistema di monitoraggio analizza periodicamente quattro proprietà fondamentali del modello, rappresentate in Figura 3.6, considerate indicatori della sua robustezza e efficacia complessiva:

- *Affidabilità*: misura la coerenza tra i risultati del modello e la reale esposizione degli applicativi a vulnerabilità o incidenti. Durante le attività di verifica vengono analizzati i casi in cui software valutati positivamente abbiano successivamente mostrato criticità operative, al fine di ricalibrare soglie e pesi delle metriche. L'obiettivo è mantenere un legame concreto tra le valutazioni teoriche e le condizioni reali, evitando che le metriche perdano significato operativo.
- *Applicabilità*: riguarda la facilità di utilizzo e la chiarezza metodologica del modello da parte dei referenti ICT e dei fornitori. Il monitoraggio raccoglie evidenze sulle difficoltà applicative, sull'efficacia degli strumenti e sulla necessità di automatizzare alcune fasi. Tali informazioni consentono di migliorare l'usabilità del sistema e di semplificare le procedure per aumentarne l'efficienza e l'adozione corretta.
- *Esaustività*: valuta la copertura tematica e normativa del modello. Ogni ciclo di monitoraggio include un confronto sistematico con il quadro normativo vigente, verificando che le metriche siano aggiornate e pertinenti rispetto ai rischi emergenti. In questo modo, il modello rimane vivo e aderente al contesto operativo.
- *Scalabilità*: misura la capacità del modello di adattarsi a contesti e attori differenti, inclusi i fornitori ICT e la rispettiva supply chain. Attraverso il confronto e il feedback raccolto dai referenti, vengono valutate la sostenibilità tecnica ed economica del modello, nonché la sua applicabilità in progetti di diversa complessità. Questo consente di garantire una diffusione coerente e sostenibile del sistema di sicurezza applicativa in tutta l'Amministrazione.

A supporto del processo di verifica delle proprietà fondamentali, è stato definito un set strutturato di criteri operativi, sintetizzato nella Tabella 3.4. Tale strumento ha lo scopo di guidare l'attività di monitoraggio dei referenti ICT e del Settore SIRe, fornendo un quadro di riferimento univoco per la raccolta delle evidenze, la formulazione delle domande di verifica e l'individuazione delle azioni correttive da intraprendere. La tabella permette di correlare, per ciascuna proprietà del modello, gli obiettivi di valutazione, le fonti informative e gli esiti attesi, favorendo così un approccio sistematico, replicabile e trasparente al processo di controllo.


**Figura 3.6:** Rappresentazione delle proprietà del modello operativo verificate nel sistema di monitoraggio e controllo. Elaborazione dell'autore

| **Proprietà** | **Descrizione** | **Domande di verifica** | **Fonte del dato/ Evidenze** | **Esito/Azioni correttive** |
|---|---|---|---|---|
| **Affidabilità** | Il modello riflette fedelmente la sicurezza reale degli applicativi. | - Ci sono stati incidenti su software classificati *sicuri*? - Ci sono discrepanze tra punteggi e segnalazioni utenti? | Incident report, log eventi, feedback utenti, feedback Referenti, audit tecnici. | Esempio: Modificare soglia su KPI critico. |

*Continua nella pagina successiva*

| Proprietà | Descrizione | Domande di verifica | Fonte del dato/ Evidenze | Esito/Azioni correttive |
|---|---|---|---|---|
| **Applicabilità** | Il modello è concretamente utilizzabile dai Referenti ICT e Cybersicurezza. | - I Referenti riescono a raccogliere i dati richiesti? - I tempi sono compatibili con il lavoro ordinario? - Ci sono metriche poco chiare o ambigue? | Report dei referenti, richieste di supporto, tempi medi di compilazione. | Esempio: Riformulare una metrica troppo complessa. |
| **Esaustività** | Il modello copre le principali dimensioni della sicurezza in relazione alle esigenze dell'Ente. | - Sono emerse nuove minacce o requisiti normativi non coperti? - Il modello intercetta rischi rilevanti evidenziati da ACN o altre Autorità/enti? | Nuove linee guida, incidenti recenti, confronti con modelli esterni (es. NIS2, Linee Guida AgID). | Esempio: Aggiungere/modificare metriche esistenti. |
| **Scalabilità** | Il modello è applicabile anche ai fornitori esterni e si adatta a diversi contesti progettuali. | - I fornitori riescono a interpretare e rispondere ai requisiti? - Sono emerse segnalazioni di difficoltà o proposte da parte dei Fornitori o dei referenti di Direzione? | Feedback referenti, verbali incontri con fornitori, segnalazioni fornitori | Esempio: Modificare il modello adattandolo al contesto critico (rendendolo più replicabile e meno oneroso dal punto di vista della rendicontazione). |

**Tabella 3.4:** Criteri di verifica delle quattro proprietà fondamentali del modello previsti nelle procedure di monitoraggio e controllo.

Ogni ciclo di monitoraggio produce una serie di output strutturati, tra cui report di sintesi, schede di anomalia e proposte di miglioramento. Questi documenti alimentano un circuito virtuoso di miglioramento continuo, nel quale i risultati della verifica retro-agiscono sul modello, aggiornando metriche e procedure. Nel medio periodo, tali risultati costituiranno una base informativa storica per analisi longitudinali, benchmark tra fornitori e valutazioni comparative dell'evoluzione della sicurezza applicativa regionale. Sotto il profilo strategico, il sistema di monitoraggio contribuisce in modo diretto al rafforzamento della governance della sicurezza digitale della Regione Piemonte, fornendo supporto decisionale basato su dati verificabili e promuovendo una gestione condivisa della conoscenza e della responsabilità.

Il sistema di monitoraggio e controllo si configura, in definitiva, come il motore evolutivo del modello di sicurezza regionale. Attraverso la sua azione ciclica, partecipata e basata sull'evidenza, esso garantisce che il modello resti affidabile, applicabile, esaustivo e scalabile

nel tempo. La sua funzione è al contempo tecnica e strategica: assicura la qualità delle misurazioni, favorisce il miglioramento metodologico e consolida una cultura organizzativa orientata alla responsabilità condivisa e al miglioramento continuo.

Il capitolo successivo sarà dedicato alla validazione del modello, in cui il sistema sarà applicato a casi reali del portafoglio applicativo regionale, al fine di verificarne la tenuta metodologica, la capacità di misurazione e l'efficacia complessiva come strumento di supporto alla governance della sicurezza del software della Regione Piemonte.

# Capitolo 4

# Validazione

Il presente capitolo è dedicato alla fase di validazione del modello operativo per la valutazione della sicurezza del software, momento conclusivo del percorso di progettazione e realizzazione della soluzione sviluppata nel lavoro di tesi. Dopo aver definito la struttura metodologica del modello e le modalità di rendicontazione e monitoraggio, la validazione rappresenta il passaggio necessario per verificarne la solidità, la coerenza interna e l'effettiva applicabilità nel contesto organizzativo e tecnologico della Regione Piemonte. L'obiettivo generale di questa fase è dimostrare che il modello, nella sua articolazione in tre pilastri, sia in grado di misurare in modo affidabile e ripetibile il livello di sicurezza applicativa, restituendo risultati coerenti con lo stato reale dei sistemi informativi regionali.

La validazione è stata condotta su un campione di cinque applicativi che gestiscono dati riferiti ai settori ambiente, energia, trasporto pubblico locale e in parte correlati all'ambito sanitario e sono rappresentativi del parco software della Regione, selezionati in funzione della loro eterogeneità tecnologica e funzionale. L'applicazione del modello a tali casi reali ha permesso di osservare il comportamento delle metriche, di testare la chiarezza delle procedure di rendicontazione e di verificare la qualità delle informazioni prodotte dai fornitori.

Il capitolo si articola in quattro sezioni. La prima definisce le finalità e le motivazioni della validazione, illustrando il ruolo di questa fase all'interno del percorso metodologico. La seconda descrive nel dettaglio l'approccio adottato, le modalità operative di raccolta e rendicontazione dei dati, gli strumenti impiegati e i criteri di analisi applicati. La terza sezione presenta le evidenze emerse dall'applicazione del modello, analizzando le performance delle metriche per ciascun pilastro e per i diversi applicativi, nonché le valutazioni complessive del modello rispetto alle sue quattro proprietà fondamentali. Infine, l'ultima sezione discute i principali vincoli emersi sia nella sperimentazione del modello sia nel processo di validazione, evidenziando gli ambiti di miglioramento e fornendo un ponte naturale verso il capitolo successivo dedicato alle conclusioni e agli sviluppi futuri.


**Figura 4.1:** Rappresentazione degli step operativi che costituiscono il processo di validazione a cui è stato sottoposto il modello operativo proposto dalla presente tesi. Elaborazione dell'autore

## 4.1 Obiettivi

La validazione del modello operativo per la valutazione della sicurezza del software rappresenta la fase conclusiva e di verifica metodologica del lavoro di ricerca. Essa ha l'obiettivo di accertare la solidità, l'efficacia e la coerenza interna del modello elaborato, verificando che le metriche, le procedure e le logiche di funzionamento rispondano alle finalità per cui sono state progettate. La validazione costituisce dunque il passaggio necessario per trasformare una struttura teorica e metodologica in uno strumento operativo concreto, in grado di essere effettivamente applicato nel contesto organizzativo e tecnologico della Regione Piemonte. Gli step operativi che hanno costituito il processo di validazione, sono evidenziati nella Figura 4.1, mostrando le varie fasi metodologiche a cui è stato sottoposto il modello.

L'individuazione del campione precedentemente descritto ha permesso di esplorare differenti livelli di maturità tecnologica e di priorità strategica, fornendo un quadro ampio e rappresentativo su cui testare la capacità del modello di adattarsi a contesti operativi diversi. In particolare, due degli applicativi analizzati sono tecnologicamente consolidati, rappresentando casi ideali per verificare la capacità del modello di individuare correttamente un elevato livello di conformità e sicurezza.

Altri due applicativi costituiscono esempi di soluzioni intermedie, per le quali si attende

un livello di sicurezza medio, utile a verificare la sensibilità del modello nel riconoscere contesti con margini di miglioramento. Infine, un quinto applicativo è stato selezionato come caso di riferimento per le situazioni a maggiore criticità. In questo scenario, l'obiettivo era valutare la capacità del modello di restituire un punteggio coerente con la presenza di vulnerabilità e debolezze, confermando la sua attendibilità nel rilevare condizioni di rischio effettive.

La scelta di questo campione diversificato ha consentito di testare il comportamento del modello in contesti con differenti livelli di complessità tecnica, maturità infrastrutturale e priorità strategica, fornendo una validazione sia qualitativa sia quantitativa della sua efficacia.

La finalità principale della validazione è stata quella di verificare la capacità del modello di misurare in modo coerente e oggettivo la sicurezza del software, traducendo in dati misurabili le dimensioni concettuali individuate nei tre pilastri: *Codice*, *Infrastruttura* e *Compliance* tecnico-normativa. Tuttavia, l'attività non si è limitata alla sola valutazione tecnica delle metriche, ma ha assunto anche una valenza organizzativa, volta a testare la praticità e l'usabilità del modello nel contesto operativo regionale. L'obiettivo non era dunque esclusivamente quello di calcolare punteggi o produrre valutazioni numeriche, ma di osservare come il modello si comporta quando viene effettivamente applicato a casi reali: quanto è chiaro nelle sue procedure, quanto è agevole la raccolta dei dati, quanto i fornitori e i referenti ICT riescono a collaborare in modo efficace per alimentare la rendicontazione. In questo senso, la validazione si pone come banco di prova sia per la solidità metodologica del modello sia per la sua effettiva operatività.

Un aspetto fondamentale della validazione riguarda la coerenza complessiva del sistema di metriche. Poiché il modello si basa su un approccio integrato, che combina tre dimensioni interdipendenti della sicurezza applicativa, uno degli obiettivi principali è stato verificare che i risultati derivanti dai tre pilastri convergano in una valutazione complessiva coerente e interpretabile. Il modello deve infatti essere in grado di fornire una rappresentazione unitaria dello stato di sicurezza, in cui le diverse prospettive si integrano in modo armonico, evitando sovrapposizioni, contraddizioni o ridondanze. La validazione ha quindi il compito di accertare che le metriche dei tre pilastri si combinino efficacemente, restituendo un quadro fedele e bilanciato del livello di sicurezza dell'applicativo.

Sotto il profilo operativo, la validazione ha avuto anche l'obiettivo di verificare la correttezza e la consistenza del processo di raccolta e rendicontazione dei dati. Poiché la versione attuale del modello prevede un inserimento manuale delle informazioni da parte dei referenti ICT, è stato importante comprendere in che misura tale approccio sia sostenibile e accurato. La simulazione condotta, basata sulla richiesta di dati ai fornitori, ha permesso di testare le dinamiche di comunicazione, i tempi di risposta, la qualità delle evidenze fornite e la chiarezza delle procedure di compilazione. Questa componente della validazione ha quindi una funzione doppiamente utile, verificando sia l'efficacia tecnica del modello nel misurare la sicurezza che la sua capacità di inserirsi in un processo amministrativo e relazionale complesso, che coinvolge attori interni ed esterni all'Ente.

La validazione ha inoltre permesso di valutare indirettamente anche le quattro proprietà fondamentali del modello, affidabilità, applicabilità, esaustività e scalabilità, precedentemente definite come indicatori chiave della sua qualità metodologica. Attraverso l'applicazione

concreta agli applicativi selezionati, è stato possibile raccogliere informazioni utili a stimare in che misura il modello produca risultati affidabili, sia effettivamente utilizzabile dai referenti ICT, copra in modo completo le dimensioni della sicurezza rilevanti e possa adattarsi a contesti tecnologici e organizzativi diversi. In questo senso, la validazione rappresenta non solo una verifica di funzionamento, ma anche un'occasione di apprendimento e raffinamento, capace di fornire indicazioni preziose per eventuali evoluzioni future del modello.

Un altro obiettivo importante riguarda la verifica della collaborazione tra i diversi soggetti coinvolti nelle procedure previste dal modello, in particolare tra i referenti ICT, il cui ruolo nel processo di validazione è stato rappresentato dal gruppo di lavoro della tesi, e i fornitori coinvolti. La validazione ha infatti permesso di osservare concretamente come avviene lo scambio informativo necessario per alimentare la rendicontazione, verificando la chiarezza delle richieste, la disponibilità dei dati, le difficoltà operative e le modalità di interazione tra le parti. Questo aspetto, sebbene non costituisca il fulcro tecnico della validazione, è fondamentale per comprendere la reale applicabilità del modello in un contesto organizzativo complesso come quello della Regione Piemonte, dove la cooperazione tra soggetti diversi è essenziale per il buon funzionamento dei processi ICT.

Infine, la validazione si pone l'obiettivo generale di consolidare il modello come strumento stabile e affidabile per la valutazione della sicurezza del software in ambito regionale. Essa consente di verificare che il modello risulti coerente rispetto alle sue premesse teoriche, realistico nelle modalità applicative e sostenibile nel contesto operativo dell'Ente. Attraverso questa attività, si intende confermare la validità del modello non solo come esercizio accademico, ma come proposta metodologica effettivamente utilizzabile nella pratica amministrativa e gestionale. In questa prospettiva, la validazione rappresenta il momento in cui il modello passa dalla dimensione di prototipo sperimentale a quella di strumento operativo, dimostrando la propria capacità di produrre risultati significativi, misurabili e coerenti con gli obiettivi di sicurezza applicativa regionale.

## 4.2 Metodologia di validazione

La metodologia adottata per la validazione del modello operativo è stata progettata con l'obiettivo di garantire una verifica rigorosa e strutturata della sua capacità di misurare, in modo coerente e ripetibile, il livello di sicurezza applicativa degli applicativi regionali. Tale attività è stata concepita come un processo sperimentale ma metodologicamente controllato, volto a testare non solo la correttezza tecnica delle metriche e delle procedure, ma anche la loro applicabilità in un contesto organizzativo complesso come quello della Regione Piemonte. La validazione ha pertanto combinato elementi di analisi quantitativa e qualitativa, integrando momenti di interlocuzione con i fornitori, raccolta e rendicontazione dei dati, compilazione della scheda di validazione e confronto con informazioni pregresse provenienti da precedenti iniziative progettuali.

Il campione oggetto di validazione, presentato nella sezione precedente e dettagliato nella Tabella 4.1, è stato costituito da cinque applicativi selezionati dal portafoglio software regionale. Tale campione ha consentito di verificare la capacità del modello di adattarsi a

differenti situazioni operative e livelli di maturità tecnologica, in coerenza con la logica di rappresentatività che caratterizza il lavoro di ricerca. La metodologia di validazione, tuttavia, non si è limitata alla mera applicazione delle metriche a tali prodotti, ma ha previsto un articolato processo di raccolta, verifica e analisi delle informazioni, volto a valutare la solidità e la coerenza interna del modello nelle sue tre dimensioni fondamentali: *Codice*, *Infrastruttura* e *Compliance* tecnico-normativa.

| **Nome prodotto** | **Descrizione Prodotto** |
|---|---|
| **Prodotto 1** | Sistema delle scrivanie del richiedente e del funzionario per i procedimenti ambientali |
| **Prodotto 2** | Registro degli autobus del Trasporto Pubblico Locale |
| **Prodotto 3** | Sistema di gestione degli attestati del Territorio |
| **Prodotto 4** | Sistema di gestione delle esenzioni per reddito e per patologia |
| **Prodotto 5** | Sistema Informativo della Certificazione Energetica |

**Tabella 4.1:** Elenco e breve descrizione funzionale dei prodotti facenti parte del campione di validazione

Il processo di validazione è stato strutturato secondo un flusso operativo sequenziale, che riflette la logica di applicazione del modello nel contesto reale. Ogni fase si collega strettamente alla successiva, creando un ciclo di valutazione integrato che parte dalla richiesta delle informazioni, prosegue con la rendicontazione e culmina nella produzione del report finale. Tale struttura consente di mantenere la tracciabilità di ogni passaggio, garantendo che le evidenze raccolte siano sempre riferibili alle metriche e alle fasi del ciclo di vita dell'applicativo. La scelta di mantenere un approccio lineare, ma verificabile, deriva dall'esigenza di assicurare replicabilità e trasparenza metodologica, principi fondamentali per l'adozione futura del modello su larga scala.

La prima fase del processo è stata dedicata all'interlocuzione con i fornitori, in particolare con CSI Piemonte. Tale fase ha rappresentato il momento iniziale di confronto tecnico e metodologico, necessario per illustrare le finalità del modello, definire le modalità operative di rendicontazione e concordare le tempistiche di restituzione dei dati. Gli incontri preliminari, condotti in forma strutturata e supportati da scambi documentali attraverso le piattaforme collaborative regionali, hanno permesso di chiarire le modalità di compilazione dei moduli di raccolta e di condividere le informazioni necessarie per la successiva fase di analisi. Questa interlocuzione ha avuto un duplice valore: da un lato ha consentito di ottenere un accesso diretto alle informazioni tecniche relative agli applicativi oggetto di studio; dall'altro ha permesso di verificare la comprensione del modello da parte dei soggetti esterni e la loro capacità di fornire dati coerenti con le metriche definite. Tale fase è risultata particolarmente rilevante poiché ha consentito di testare, in un contesto reale, la chiarezza e la fruibilità del sistema di rendicontazione, oltre a verificare la disponibilità e la qualità delle evidenze necessarie a supportare la valutazione.

Al termine della fase di interlocuzione, è stata avviata una raccolta sistematica delle informazioni, tramite un apposito modulo per la richiesta di dati relativi ai prodotti analizzati, sviluppato in formato foglio di calcolo. Tale strumento ha rappresentato il

principale canale operativo per la raccolta dei dati tecnici e di sicurezza relativi agli applicativi oggetto di validazione. Il form è stato strutturato in modo da guidare i fornitori e il gruppo di lavoro nella compilazione delle informazioni necessarie alla rendicontazione, attraverso una suddivisione per pilastro di riferimento. Il form include una serie di domande specifiche volte alla raccolta delle informazioni, in cui ad ogni richiesta è associata la metrica di riferimento, rappresentata dal suo *Unique ID*, una sezione per la risposta alla richiesta da parte del fornitore e infine una colonna con l'elenco dei possibili documenti tecnici inerenti e utili alla raccolta e la redazione delle risposte ai quesiti. Tale impostazione ha permesso di uniformare la raccolta dei dati e di facilitare la successiva attività di rendicontazione delle metriche e validazione. Le informazioni richieste comprendono elementi di natura tecnica, organizzativa e documentale.

L'obiettivo dell'utilizzo di questo strumento è stato indicare ai fornitori una guida chiara e operativa per la raccolta delle informazioni e semplificare il lavoro dei referenti ICT e del gruppo di lavoro di tesi, garantendo la tracciabilità e la completezza delle informazioni raccolte. L'utilizzo del form, inoltre, ha consentito di identificare eventuali lacune o ambiguità nella definizione delle metriche, offrendo spunti utili per la successiva revisione del modello.

Sulla base delle informazioni ricevute, il gruppo di lavoro ha proceduto alla rendicontazione delle metriche, replicando le modalità operative previste dal modello. Tale attività ha previsto una fase di verifica incrociata dei dati condivisi dai fornitori e la richiesta di eventuali integrazioni o chiarimenti nei casi in cui le evidenze risultassero incomplete o poco significative. La rendicontazione è stata condotta per ciascun pilastro, in coerenza con la fase del ciclo di vita dell'applicativo su cui era in corso la validazione, applicando il set di metriche pertinente. Per ogni metrica, è stato attribuito il rispettivo valore e successivamente è stato calcolato l'indice di conformità complessivo per fase, secondo la formula definita nel modello operativo. Tale indicatore, espresso in forma percentuale, rappresenta la proporzione di metriche soddisfatte rispetto al totale di quelle applicabili, fornendo una misura sintetica ma significativa del livello di sicurezza e conformità dell'applicativo per quella specifica fase. La procedura di calcolo è stata condotta in modo manuale, con l'ausilio di funzioni automatizzate del foglio di calcolo, garantendo così uniformità e trasparenza nella valutazione dei risultati. Questa scelta metodologica, sebbene più onerosa, ha permesso di mantenere un controllo diretto sull'intero processo e di analizzare in modo più approfondito la relazione tra i singoli indicatori e le metriche.

La fase centrale del processo di validazione è stata la compilazione della *Scheda di Validazione*, allegata come appendice E alla presente tesi per completezza metodologica. Questo documento ha costituito lo strumento principale per la valutazione complessiva del modello applicato a ciascun applicativo. La scheda è stata compilata dal gruppo di lavoro della tesi, che ha agito in rappresentanza dei referenti ICT regionali, utilizzando i dati presentati dai fornitori e le risultanze della rendicontazione, integrate in una delle sezioni dello strumento. La scheda è articolata in più sezioni logiche, che riflettono le diverse fasi del processo di valutazione. Nella parte iniziale sono riportate le informazioni identificative dell'applicativo, quali denominazione, area funzionale, direzione di riferimento, fornitore e stato del ciclo di vita. Seguono poi sezioni descrittive che sintetizzano le caratteristiche tecniche e architetturali del sistema, le principali interfacce, le dipendenze infrastrutturali e

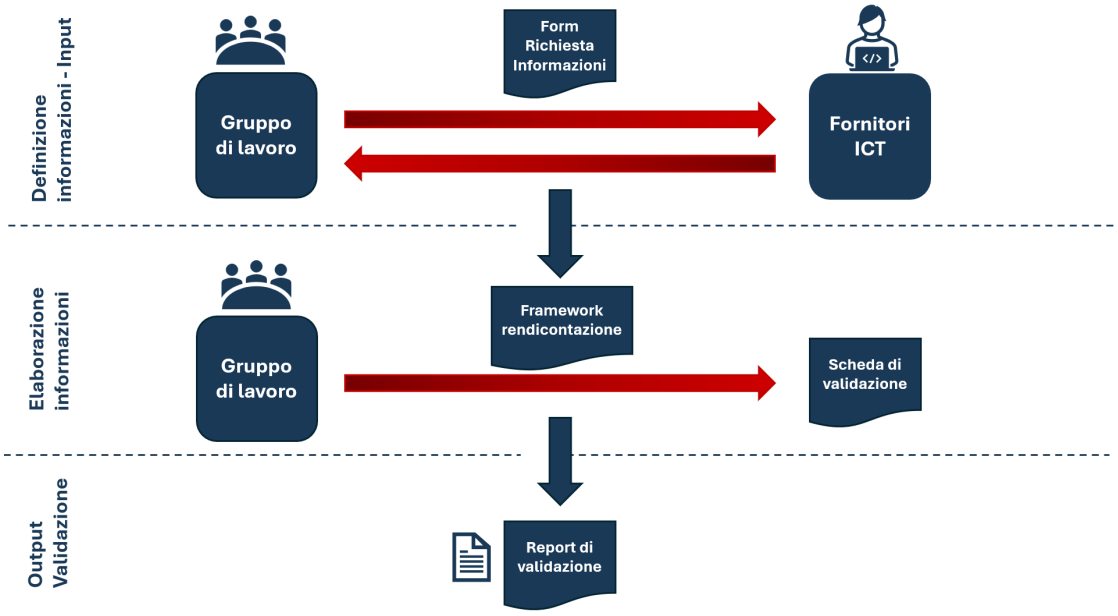


**Figura 4.2:** Flussi dati e relazione tra gli strumenti utilizzati nel processo di validazione dagli attori coinvolti. Elaborazione dell'autore

le componenti tecnologiche. La parte centrale della scheda è dedicata alla rendicontazione delle metriche, dove vengono riportati i risultati per ciascun pilastro, con indicazione dell'indice di conformità e di eventuali note esplicative. In questa sezione trovano spazio anche i riferimenti alle evidenze documentali e alle osservazioni emerse durante l'analisi, consentendo di mantenere un legame diretto tra i dati quantitativi e la loro interpretazione qualitativa. Infine, la scheda si conclude con una sezione di valutazione sintetica, in cui il gruppo di lavoro ha espresso un giudizio complessivo sull'applicabilità e sull'efficacia del modello, suddiviso secondo le quattro proprietà fondamentali già definite: affidabilità, applicabilità, esaustività e scalabilità. Tale sezione costituisce un elemento essenziale della metodologia, poiché consente di strutturare la riflessione sul funzionamento del modello in una prospettiva multidimensionale e coerente con gli obiettivi della ricerca. Gli attori coinvolti e i flussi dati scambiati tramite l'utilizzo degli strumenti sopracitati, sono rappresentati graficamente nella Figura 4.2.

Completata la fase di compilazione, i dati raccolti sono stati oggetto di un'analisi di coerenza interna e di confronto qualitativo con i risultati ottenuti in precedenti progetti, in particolare con le valutazioni condotte nell'ambito dell'iniziativa PNRR, dettagliata nella sezione 1.2.2 dedicati progetti correlati della presente tesi, che aveva come perimetro dodici applicativi regionali. Tale confronto, basato su una revisione incrociata delle informazioni, essendo il campione degli applicativi oggetto della validazione un sottoinsieme dei dodici sopracitati, ha consentito di verificare la coerenza metodologica del modello rispetto alle prassi consolidate e di evidenziare eventuali miglioramenti nella capacità di rappresentazione e nella completezza della valutazione. Anche se il confronto non aveva carattere quantitativo,

ha rappresentato una fase cruciale per la verifica della robustezza del modello, confermando la sua capacità di restituire una rappresentazione coerente delle condizioni di sicurezza, indipendentemente dal contesto applicativo specifico.

Al termine del processo, per ciascun applicativo è stato prodotto un report sintetico, coincidente con la *Scheda di Validazione* compilata, che costituisce il principale output documentale della fase di validazione. Tali report, oltre a rappresentare una testimonianza diretta dell'applicazione del modello, sono stati utilizzati come base per la successiva fase di analisi dei risultati, dove sono stati esaminati i trend, le coerenze e le aree di miglioramento. In questo modo, la metodologia di validazione ha consentito di tradurre in pratica le logiche teoriche del modello, dimostrando la fattibilità e la solidità del percorso proposto. La metodologia non si è limitata alla verifica delle singole metriche, ma ha consentito di testare l'intero ecosistema di valutazione, includendo gli aspetti relazionali, documentali e procedurali che ne garantiscono la sostenibilità. Il processo ha dimostrato che la validazione di un modello di sicurezza non può essere ridotta a una mera attività di calcolo, ma richiede un approccio integrato, capace di coniugare rigore tecnico, partecipazione organizzativa e capacità di adattamento al contesto. Questa visione sistemica rappresenta il presupposto per l'analisi dei risultati che verrà esposta nella sezione successiva, dove le evidenze raccolte saranno interpretate in relazione agli obiettivi di coerenza, affidabilità e applicabilità del modello.

## 4.3 Risultati

L'attività di validazione ha permesso di applicare concretamente il modello operativo a un insieme eterogeneo di cinque applicativi regionali, campione dettagliato nelle precedenti sezioni del presente capitolo, consentendo di verificare in che misura le metriche definite riescano a descrivere in modo coerente e ripetibile il livello di sicurezza del software nelle sue diverse dimensioni. I risultati ottenuti costituiscono la principale evidenza empirica a supporto della validità metodologica del modello e permettono di trarre considerazioni di carattere sia tecnico che interpretativo. L'analisi dei dati raccolti e delle schede di validazione, con i relativi report, ha evidenziato tendenze coerenti con le ipotesi formulate in fase di progettazione: le metriche risultano complessivamente applicabili, producono valutazioni coerenti tra i tre pilastri e restituiscono una rappresentazione equilibrata delle condizioni di sicurezza. Al tempo stesso, l'esercizio di validazione ha permesso di mettere in luce alcuni aspetti di maggiore sensibilità, in particolare nei contesti in cui le informazioni disponibili risultano più frammentate o dove la maturità tecnologica dell'applicativo è ancora in evoluzione.

Allo scopo di mostrare le evidenze che sottendono l'analisi e le considerazioni d'insieme dettagliate in seguito, si riporta la Tabella 4.2 con la rendicontazione delle metriche effettuata durante il progetto di tesi per il *Prodotto 2*, che rappresenta l'evidenza dell'attuazione delle *Schede di Rendicontazione* al caso reale, con la correlazione tra le metriche, i target, il valore attuale e le eventuali azioni di mitigazione.

| **ID Metrica** | **Target** | **Valore Attuale** | **Azioni di mitigazione** |
|---|---|---|---|
| CTN-GV.OC01 | $\geq 95\%$ | 100,00% | |
| CTN-GV.RM01 | $\geq 90\%$ | 100,00% | Per il fornitore, il processo di risk management è unico, sul perimetro del Sistema di Gestione Integrato, e comprende i rischi relativi alla cybersecurity |
| CTN-GV.RR01 | $\geq 90\%$ | 100,00% | |
| CTN-GV.RR02 | 100% | Non fornito | Il fornitore dichiara che i processi/pratiche HR riguardano soprattutto aspetti che esulano dalla cybersecurity (es. il trattamento economico, l'orario di lavoro, ecc. ); i processi di selezione tengono adeguatamente in considerazione gli aspetti di cybersecurity, il personale è adeguatamente e costantemente formato secondo le proprie mansioni, sono in atto opportune procedure di dismissione dei privilegi alla cessazione del rapporto di lavoro. Al netto Il KPI si ritiene ON TARGET |
| CTN-GV.PO01 | 100% | 100,00% | |
| CTN-GV.PO02 | $\leq 12$ mesi | 12 mesi | Le politiche di sicurezza sono adeguate al contesto e periodicamente revisionate, con cadenza almeno annuale |
| CTN-GV.SC01 | $\geq 90\%$ | 100,00% | |
| CTN-GV.SC02 | 100% | 0,00% | Il fornitore dichiara che al momento non è esplicito nei contratti, ma è in corso un piano di adeguamento, come richiesto dalla normativa vigente |
| CTN-GV.SC03 | $\geq 95\%$ | 100,00% | Il fornitore dichiara che sono identificati e classificati almeno i fornitori CRITICI; di conseguenza viene considerata la metrica ON TARGET |
| CTN-GV.SC04 | $\geq 90\%$ | 100,00% | |
| CTN-GV.SC05 | 100% | 0,00% | Al momento non è esplicito nei contratti, ma è in corso un piano di adeguamento, come richiesto dalla normativa vigente |
| CTN-ID.RA01 | $\geq 95\%$ | 100,00% | Per il fornitore, il processo di risk management è unico, sul perimetro del Sistema di Gestione Integrato, e comprende i rischi relativi alla cybersecurity |
| CTN-ID.RA02 | $\geq 95\%$ | 10,00% | Il fornitore dichiara che al momento, la percentuale è circa del 10%, ma il processo di gestione dei rischi è in continua esecuzione |
| CTN-ID.RA03 | Sì | Sì | Sì. `https://csipiemonte.it/responsible-disclosure-policy` |

*Continua nella pagina successiva*

| **Metrica** | **target** | **Valore Attuale** | **Azioni di mitigazione** |
|---|---|---|---|
| CTN-ID.IM01 | 100% | 100,00% | Sì, il CSI è certificato ISO 22301 |
| CTN-PR.AT01 | $\geq$ 90% | Non fornito | Il dato non è stato fornito dal fornitore, pertanto la metrica viene identificata come NON ON TARGET. Come azione di mitigazione si richiederà un indagine approfondita per estrarre il dato e attuare un eventuale piano di adeguamento. |
| CTN-RS.MA01 | 100% | 100,00% | |
| CTN-RS.CO01 | $\geq$ 95% | 100,00% | |
| CTN-RC.RP01 | 100% | 100,00% | |
| INF-A01 | $\geq$ 99,90% (senza fermi) e $\geq$ 99,9% (con fermi) | 99,5% - su base annuale per la disponibilità dei nodi fisici dell'infrastruttura che ospita il servizio | Il valore indicato è in maniera trascurabile al di sotto della soglia e in considerazione del fatto che l'infrastruttura Cloud Nivola su cui è ospitato l'applicativo è certificata da ACN, si considera il KPI ON TARGET |
| INF-DC01 | 100% dei 5 requisiti | 100,00% | |
| INF-DC02 | 100,00% | 100,00% | |
| INF-AM01 | 100,00% | 100,00% | |
| INF-AM02 | 100,00% | 100,00% | |
| INF-RA01 | 100% annualmente | 100,00% | |
| INF-AC01 | 100% conformità ai 6 requisiti | 100,00% | |
| INF-AC02 | 100,00% | 100,00% | |
| INF-AC03 | 100,00% | 100,00% | |
| INF-AC04 | 100,00% | 100,00% | |
| INF-BA01 | 100%, test annuale | 100,00%, al netto dei dati non ti produzione su specifica richiesta | |
| INF-MA01 | 100% autorizzazioni preventive | 100,00% | |
| INF-MA02 | 100,00% | 100,00% | |

*Continua nella pagina successiva*

| Metrica | target | Valore Attuale | Azioni di mitigazione |
|---|---|---|---|
| INF-DE01 | 100,00% | 100,00% | |
| INF-DE02 | 100% protezione postazioni, policy rivista annualmente | 100,00% | |
| COD-SR01 | $\geq$ 100% (Classe I) | 100,00% | |
| COD-RR01 | $\geq$ 100% (Classe I) | 50,00% | Il prodotto ha 4 componenti analizzate dalla soluzione SAST:<br>Componente 1 - 77.750 LOC analizzate da SAST - 46 Bugs, classe C di Reliability Rating di SonarQube su Overall Code - 0 severity Blocker - 0 severity Critical - 36 severity Major - 8 severity Minor - 2 severity Info<br>Componente 2 - 12.557 LOC analizzate da SAST - 348 Bugs, classe A di Reliability Rating di SonarQube su Overall Code - 0 severity Blocker - 0 severity Critical - 0 severity Major - 0 severity Minor - 348 severity Info<br>Componente 3 - 6.065 LOC analizzate da SAST - 96 Bugs, classe A di Reliability Rating di SonarQube su Overall Code - 0 severity Blocker - 0 severity Critical - 0 severity Major - 0 severity Minor - 96 severity Info<br>Componente 4 - 162,518 LOC analizzate da SAST - 61 Bugs, classe C di Reliability Rating di SonarQube su Overall Code - 0 severity Blocker - 0 severity Critical - 53 severity Major - 8 severity Minor - 0 severity Info<br>Nonostante la metrica sia under target, considerate le severity inerenti ai bug delle singole componenti, essendo tutte NON Blocker o Critical, si considera il KPI ON TARGET |

*Continua nella pagina successiva*

| **Metrica** | **target** | **Valore Attuale** | **Azioni di mitigazione** |
|---|---|---|---|
| COD-LSR01 | $\geq$ 100% (Classe I) | 50,00% | Situazione analisi SCA:<br>- Componente 1 - ha 7 librerie con vulnerabilità di severity CRITICAL - Componente 2 - ha 0 librerie con vulnerabilità di severity CRITICAL - Componente 3 - ha 0 librerie con vulnerabilità di severity CRITICAL - Componente 4 - ha 7 librerie con vulnerabilità di severity CRITICAL<br>Il fornitore, adesso consapevole di queste criticità, sta sviluppando insieme a Regione delle metriche per la stima dell'indice di complessità della Remediation, per poi successivamente andare a definire la priorità di intervento correttivo sui prodotti. |
| COD-LST01 | $\geq$ 100% (Classe I) | 0,00% | Nella componente Componente 1 ci sono 77 librerie open source e 46 di queste necessiterebbero di un aggiornamento quindi il 59,7% necessiterebbe di un aggiornamento di versione.<br>Nella componente Componente 2 ci sono 19 librerie open source e 1 di queste necessiterebbero di un aggiornamento quindi il 5,2% necessiterebbe di un aggiornamento di versione.<br>Nella componente Componente 3 ci sono 20 librerie open source e 15 di queste necessiterebbero di un aggiornamento quindi il 75% necessiterebbe di un aggiornamento di versione.<br>Nella componente Componente 4 ci sono 112 librerie open source e 66 di queste necessiterebbero di un aggiornamento quindi il 58,9% necessiterebbe di un aggiornamento di versione.<br>Viene evidenziato dal fornitore come il valore fornito dal report di Meterian, conta il numero assoluto di patch non applicate con base di partenza 100 e non fornisce, come da loro segnalato al Vendor, un dato veritiero sullo stato di aggiornamento percentuale delle patch sull'applicativo ( contrariamente a quanto emerge dai dati sopra riportati )<br>Il fornitore, adesso consapevole di queste criticità, sta sviluppando insieme a Regione delle metriche per la stima dell'indice di complessità della Remediation, per poi successivamente andare a definire la priorità di intervento correttivo sui prodotti. |

*Continua nella pagina successiva*

| Metrica | target | Valore Attuale | Azioni di mitigazione |
|---|---|---|---|
| COD-COV01 | $\geq$ 100% (con giustificazioni documentate) | 72,00% | In considerazione del fatto che sul SAST si possono impostare delle esclusioni per tutto il codice analizzato (come per esempio codice third party, framework, ecc.), i componenti con i quali repository sono anche dove il codice non effettivamente presente nel prodotto in esercizio (es. codice commentato, codice non più usato, ecc.) possono influenzare il risultato, si considera il KPI ON TARGET |
| COD-COV2 | $\geq$ 100% (con giustificazioni documentate) | Non fornito | Il KPI viene valutato poco significativo/-funzionante dal fornitore per la seguente motivazione: c'è sicuramente una differenza tra quanto dichiarato nei manifest e quanto rilevato dalla SCA, ma dipende da come viene effettuata la scansione. Se la scansione viene effettuata nel container, il risultato può essere distorto, pertanto viene considerata la metrica non direttamente correlata a quanto delle librerie dichiarate. Può quindi accadere che un manifest dichiari, ad esempio, 100 librerie, ma che per la configurazione della scansione solo 100 siano rilevate. Si considera il KPI NON ON TARGET. |

**Tabella 4.2:** *Scheda di Rendicontazione* redatta durante la validazione del modello, rendicontando le metriche relative al *Prodotto 2* del campione di validazione.

Nel complesso, la distribuzione dei valori medi delle singole metriche rispetto ai target e raggruppate per pilastro mostra una buona variabilità interna, utile per testare la capacità discriminante del modello. I punteggi si collocano in un intervallo con valore medio pari a circa l'83%, confermando che il modello riesce a restituire una scala graduata di valutazione, in grado di distinguere con coerenza i diversi livelli di sicurezza applicativa. Tale distribuzione suggerisce che il modello non produce risultati omogenei o uniformi, ma risponde in modo sensibile alle effettive caratteristiche dei prodotti analizzati.

L'analisi per pilastro costituisce il primo livello di interpretazione dei risultati e consente di individuare i principali trend di comportamento delle metriche. Nel pilastro del *Codice*, i valori medi delle metriche rispetto ai target si attestano su livelli intermedi, intorno al *42%*. Le metriche relative alla qualità e alla sicurezza del codice sorgente, come la gestione delle dipendenze, l'assenza di vulnerabilità note e la copertura dei test, risultano generalmente soddisfatte nei casi in cui il ciclo di sviluppo del software è ancora attivo e gestito secondo pratiche di integrazione continua. Nei prodotti meno evoluti e consolidati da tempo, si osserva una riduzione dei valori, riconducibile al minor grado di aggiornamento dei componenti e all'uso di librerie legacy. Nel complesso, le metriche del pilastro *Codice* si dimostrano efficaci nel rappresentare il livello di manutenzione e di attenzione alla sicurezza logica del software, evidenziando differenze significative tra applicativi più evoluti

e soluzioni meno aggiornate.

Il pilastro *Infrastruttura* presenta, in media, i punteggi più elevati, con valori compresi tra il 99% e il 100%. Ciò riflette il livello di maturità dell'ambiente tecnologico regionale e la presenza di pratiche consolidate di gestione della sicurezza infrastrutturale, spesso garantite da infrastrutture che implementano tecnologie di cloud computing certificate da ACN e dai sistemi di virtualizzazione e monitoraggio già consolidati. Le metriche legate alla resilienza, al backup, al controllo degli accessi e alla segregazione degli ambienti risultano pienamente soddisfatte nella maggior parte dei casi. Le lievi differenze osservate tra i vari applicativi dipendono prevalentemente dal livello di integrazione con l'infrastruttura gestita centralmente, confermando che il contesto tecnologico fornisce una base solida e omogenea per la sicurezza di sistema.

Il pilastro della *Compliance* tecnico-normativa mostra, invece, valori medi leggermente inferiori al pilastro *Infrastruttura* e maggiori del pilastro *Codice*, collocandosi intorno al 79%. Questo dato riflette la maggiore complessità delle metriche di conformità, che richiedono un allineamento costante con le normative nazionali e unionali. Nei casi in cui i processi documentali sono più strutturati e le responsabilità di compliance chiaramente definite, la conformità risulta elevata; viceversa, laddove la gestione delle evidenze è frammentata o in parte demandata ai sub-fornitori, emergono lievi scostamenti. Tale risultato conferma l'importanza del pilastro come indicatore della maturità organizzativa e della capacità di mantenere nel tempo un controllo sugli obblighi normativi che interessano l'Ente.

I risultati per ciascun applicativo permettono di apprezzare la coerenza del modello anche in termini comparativi. Il *Prodotto 1*, appartenente alla categoria degli applicativi tecnologicamente consolidati, mostra valori di conformità elevati in tutti e tre i pilastri, con un indice complessivo di conformità alle metriche pari all'85%. In particolare, le metriche infrastrutturali raggiungono quasi la piena aderenza, confermando la stabilità dell'infrastruttura e la corretta gestione degli accessi. Il *Prodotto 2*, appartenente alla medesima categoria, presenta valori leggermente inferiori, con una media dell'82%, con una lieve flessione nel pilastro *Codice*, legata all'utilizzo di componenti software non del tutto aggiornati.

Il *Prodotto 3*, appartenente alla categoria intermedia degli applicativi non prioritari ma inclini ad un'evoluzione tecnologica futura, registra un indice di conformità pari al 82%, con punteggi equilibrati ma leggermente inferiori rispetto al pilastro *Codice*, dove viene individuata la presenza di componenti con non conformità più severe. Il *Prodotto 4* presenta un andamento simile, con un indice medio di circa 79%, ma una maggiore disomogeneità tra pilastri, evidenziando una buona conformità infrastrutturale e un minore allineamento nel codice applicativo.

Infine, il *Prodotto 5*, necessitando di interventi prioritari di modernizzazione, registra i singoli valori delle metriche più bassi del campione ma con un indice di conformità complessivo anch'esso pari a circa il 79%. Le principali criticità si concentrano nel pilastro del *Codice*, coerentemente con lo stato di evoluzione del prodotto e con la presenza di vulnerabilità note.

In generale, i risultati evidenziano una progressiva diminuzione degli indici di conformità complessiva alle metriche dal *Prodotto 1* al *Prodotto 5*, coerentemente con il livello di maturità tecnologica analizzato preventivamente nel campione. Tale andamento conferma

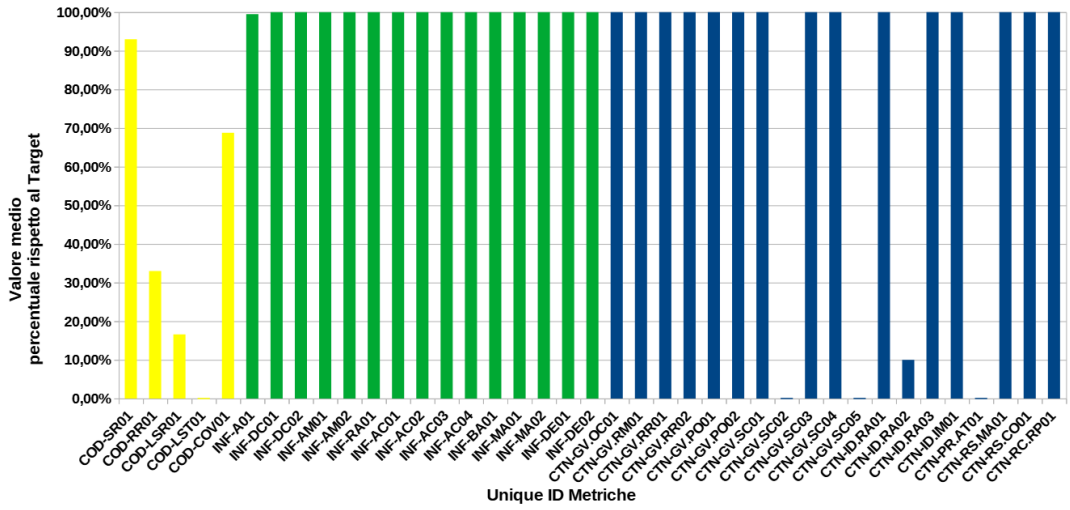


**Figura 4.3:** Istogramma rappresentante l'andamento dei valori medi percentuali delle metriche per i cinque prodotti del campione della validazione, suddivise per pilastro - *Codice*: ■, *Infrastruttura*: ■, *Compliance*: ■ . Elaborazione dell'autore

la sensibilità del modello nel discriminare correttamente situazioni di sicurezza differenti, riflettendo la reale eterogeneità del parco applicativo regionale. In Figura 4.3, viene riportato il valore medio di tutte le metriche del modello, calcolato come la media delle percentuali rispetto al target, rappresentante il 100%, dei cinque prodotti del campione. Questa rappresentazione mostra l'andamento generale e d'impatto sul campione analizzato e permette di rappresentare efficacemente il comportamento della selezione di applicativi scelti rispetto alle metriche definite, suddivise per pilastro. A supporto dei risultati evidenziati, si rappresentano, in Tabella 4.3, anche i valori medi delle metriche, rendicontati durante la validazione del modello, rispetto al campione.

| **ID Metrica** | **Valore Medio** |
|---|---|
| COD-SR01 | 93,00% |
| COD-RR01 | 33,00% |
| COD-LSR01 | 16,60% |
| COD-LST01 | 0,00% |
| COD-COV01 | 68,80% |
| INF-A01 | 99,50% |
| INF-DC01 | 100,00% |
| INF-DC02 | 100,00% |
| INF-AM01 | 100,00% |
| INF-AM02 | 100,00% |
| INF-RA01 | 100,00% |
| INF-AC01 | 100,00% |
| INF-AC02 | 100,00% |
| INF-AC03 | 100,00% |

*Continua nella pagina successiva*

| ID Metrica | Valore Medio |
|---|---|
| INF-AC04 | 100,00% |
| INF-BA01 | 100,00% |
| INF-MA01 | 100,00% |
| INF-MA02 | 100,00% |
| INF-DE01 | 100,00% |
| INF-DE02 | 100,00% |
| CTN-GV.OC01 | 100,00% |
| CTN-GV.RM01 | 100,00% |
| CTN-GV.RR01 | 100,00% |
| CTN-GV.RR02 | 100,00% |
| CTN-GV.PO01 | 100,00% |
| CTN-GV.PO02 | 100,00% |
| CTN-GV.SC01 | 100,00% |
| CTN-GV.SC02 | 0,00% |
| CTN-GV.SC03 | 100,00% |
| CTN-GV.SC04 | 100,00% |
| CTN-GV.SC05 | 0,00% |
| CTN-ID.RA01 | 10,00% |
| CTN-ID.RA02 | 10,00% |
| CTN-ID.RA03 | 100,00% |
| CTN-ID.IM01 | 100,00% |
| CTN-PR.AT01 | 0,00% |
| CTN-RS.MA01 | 100,00% |
| CTN-RS.CO01 | 100,00% |
| CTN-RS.RP01 | 100,00% |

**Tabella 4.3:** *V*alori medi di tutte le metriche calcolati sul campione selezionato durante la validazione del modello.

Il confronto dei risultati ottenuti con quelli derivanti dal progetto PNRR *Transizione Digitale e Servizi Sicuri*, già descritto nella sezione 1.2.2, ha evidenziato una coerenza significativa nei trend delle metriche, soprattutto per quanto riguarda la componente di sicurezza del codice, essendo anche l'unico aspetto analizzato dal progetto pregresso. Gli applicativi oggetto di validazione, essendo un sottoinsieme dei dodici analizzati in tale progetto, mostrano andamenti analoghi rispetto ai punteggi di sicurezza registrati in precedenza: i prodotti più maturi e consolidati mantengono valori elevati, mentre quelli oggetto di prossimi interventi di evoluzione tecnologica presentano livelli inferiori, confermando la correlazione tra maturità applicativa e grado di conformità alle metriche.

L'unico valore che non rispetta il trend analizzato è associato al *Prodotto 3*, per il quale viene dato un indicatore medio generale, calcolato sulla base dei valori delle metriche estratte dai tool utilizzati nell'iniziativa PNRR, migliore rispetto al *Prodotto 2* e uguale al *Prodotto 1*. Questo perché la metrica individuata nel progetto di tesi e l'analisi effettuata considerano in maniera più dettagliata le singole componenti del software, discriminando non solo sul numero di linee di codice impattate, ma anche sulla criticità delle non conformità riscontrate. Questo aspetto, a parità di punteggio sulla metrica relativa al *Reliability Rating*, determina un non raggiungimento del target per il *Prodotto 3*, andando a determinare un indice di conformità alle metriche del modello inferiore a quello del *Prodotto*

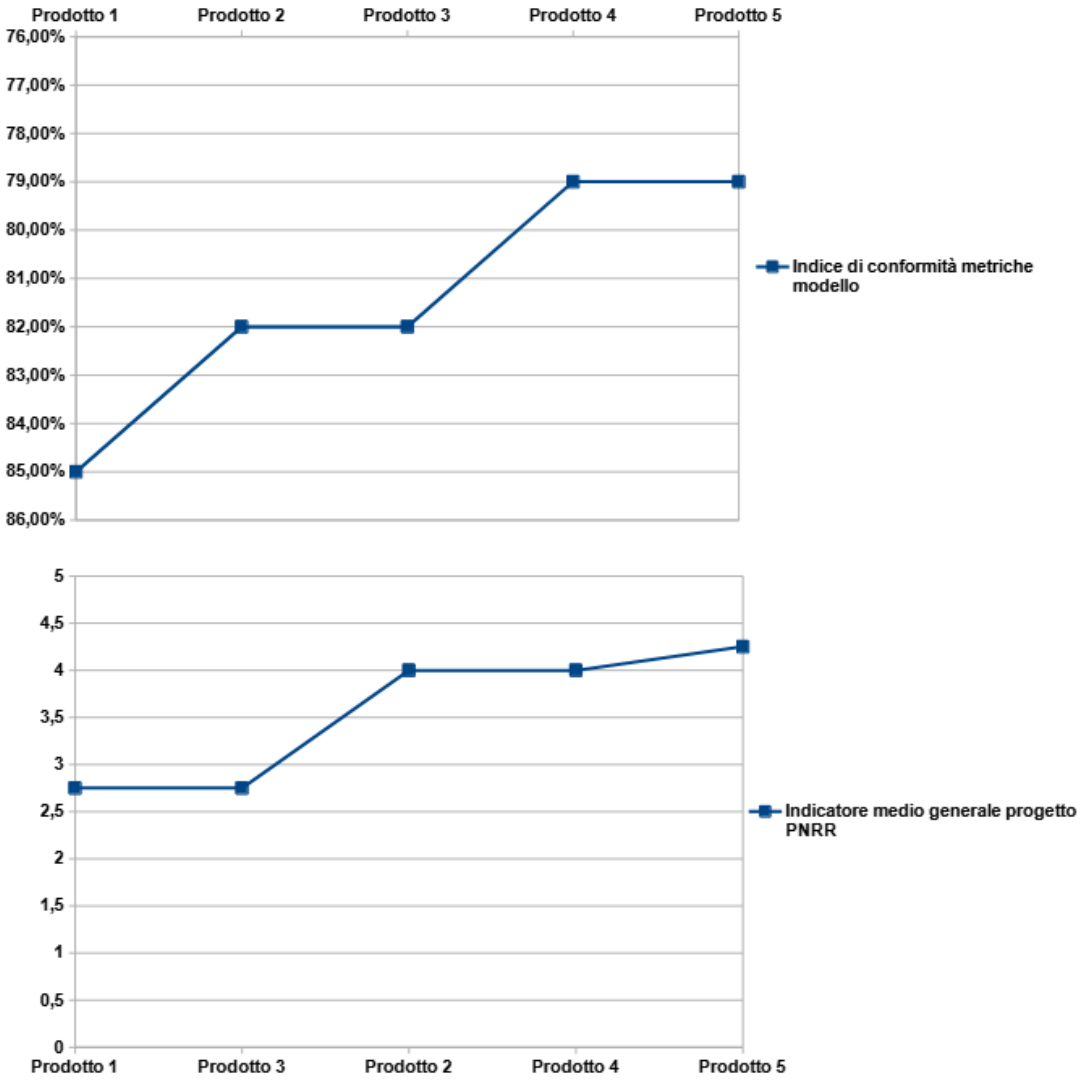


**Figura 4.4:** Rappresentazione della comparazione tra i trend relativi all'indice di conformità alle metriche nel progetto di tesi e all'indice medio generale del progetto PNRR. Elaborazione dell'autore

*1* e pari a quello del *Prodotto 2*. Nei grafici riportati in Figura 4.4 è riportato il confronto tra i due trend analizzati, con una scala delle ordinate impostata in modo speculare per consentire una valutazione diretta dell'andamento complessivo. Tale configurazione riflette la diversa natura degli indicatori: l'indice di conformità alle metriche presenta valutazioni migliori al crescere della percentuale, mentre l'indicatore medio generale derivante dal progetto PNRR assume valori più favorevoli al diminuire del proprio valore.

Tuttavia, rispetto all'esperienza PNRR, il modello sviluppato nell'ambito del lavoro

di tesi arricchisce la prospettiva di analisi, integrando la dimensione puramente tecnica con due ulteriori assi di valutazione, *Infrastruttura* e *Compliance* tecnico-normativa, che consentono una lettura più completa del livello di sicurezza applicativa. Se nel progetto PNRR l'attenzione era concentrata principalmente sull'analisi statica del codice sorgente, il modello validato amplia il campo di osservazione includendo aspetti organizzativi, gestionali e infrastrutturali. Tale ampliamento ha reso la valutazione più sensibile e multidimensionale, capace di cogliere non solo le vulnerabilità tecniche, ma anche la qualità dei processi, l'adeguatezza delle configurazioni e il grado di conformità normativa.

In questo senso, la coerenza tra i risultati dei due approcci rappresenta un elemento di conferma della solidità metodologica del modello: pur introducendo nuove dimensioni e una maggiore articolazione metrica, esso mantiene una continuità di lettura con le valutazioni pregresse, assicurando comparabilità e tracciabilità dei risultati nel tempo. Ciò dimostra la capacità del modello di integrare efficacemente esperienze precedenti e di evolvere verso uno strumento di misurazione più completo e coerente con gli obiettivi di governance della sicurezza applicativa regionale.

Sul piano metodologico, la validazione ha consentito anche di verificare il comportamento del modello rispetto alle quattro proprietà fondamentali che ne definiscono la qualità complessiva. Come riportato nella Tabella 4.4 e nella relativa legenda in Tabella 4.5, i valori medi ottenuti mostrano un quadro equilibrato, con una valutazione media pari a 3,75 punti su un valore massimo di 5 nelle diverse proprietà e con i criteri di valutazione dettagliati nella legenda. L'*Affidabilità* risulta elevata, con valutazione pari a 4 su 5, confermando che i risultati delle metriche sono coerenti con lo stato reale di sicurezza degli applicativi e che il modello mantiene una buona stabilità di valutazione. L'*Applicabilità*, con una valutazione pari a 4 su 5, risulta soddisfacente: le metriche si sono dimostrate comprensibili e gestibili nel processo di rendicontazione, soprattutto grazie all'introduzione, dopo le prime fasi di confronto con i fornitori, del form strutturato per la raccolta delle informazioni. L'*Esaustività* si attesta attorno al valore di 4 su 5, evidenziando che la copertura tematica e normativa è ampia, nonostante possa essere ulteriormente estesa per tenere conto delle evoluzioni regolamentari. Infine, la *Scalabilità*, con una valutazione pari a 3 su 5, rappresenta la dimensione più sfidante: il modello si dimostra potenzialmente adattabile ma richiede ulteriori verifiche per garantire la piena trasferibilità a contesti applicativi di diversa complessità e natura.

| Proprietà | Score (0-5) | Osservazioni e suggerimenti operativi | Evidenze Raccolte |
|---|---|---|---|
| **Affidabilità** | 4 | Al momento la valutazione risulta in linea con le precedenti analisi con metriche di sicurezza svolte sull'applicativo | Analisi e metriche derivanti dall'iniziativa regionale "ICT_O_07 transizione Digitale e Servizi Sicuri"- NextGenerationEU - PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" |
| **Applicabilità** | 4 | Sono state evidenziate delle difficoltà preventive, risolte con la trasposizione delle informazioni richieste sotto forma di domande mirate ai fornitori che hanno ristabilito la facilità di applicazione delle metriche | Riscontro dei fornitori durante la raccolta delle informazioni, documento prodotto per la raccolta informazioni mirata. Buon indice di conformità alle metriche. |
| **Esaustività** | 4 | Al momento, il modello sembrerebbe coprire tutti gli aspetti principalmente rilevanti sul software | Analisi componenti funzionali e schede di panoramica sul software (deploy, FP del software, analisi tool SCA/-SAST). Buon indice di conformità alle metriche. |
| **Scalabilità** | 3 | Facilitazione della rendicontazione tramite tool automatico, classificazione delle metriche su livelli di mandatarità differenti, per permettere l'applicabilità del modello a sotto-fornitori esterni in modalità più semplificate e immediate | Riscontro dei fornitori durante la raccolta delle informazioni ma comunque buon indice di conformità alle metriche |

**Tabella 4.4:** Scheda riepilogativa per la valutazione delle proprietà fondamentali del modello. Elaborazione dell'autore.

| Score | Descrizione |
|---|---|
| 0 | La proprietà non è in alcun modo soddisfatta |
| 1 | La proprietà è in minima parte soddisfatta; gravi carenze |

*Continua nella pagina successiva*

| Score | Descrizione |
|---|---|
| 2 | La proprietà è parzialmente soddisfatta, ma con evidenti limiti |
| 3 | La proprietà è mediamente soddisfatta, ma richiede miglioramenti |
| 4 | La proprietà è quasi completamente soddisfatta, con marginali criticità |
| 5 | La proprietà è pienamente soddisfatta; situazione ideale |

**Tabella 4.5:** Legenda dei punteggi relativi alle proprietà del modello assegnati in Tabella 4.4

Nel complesso, i risultati confermano che il modello operativo è in grado di rappresentare in modo fedele e coerente la condizione di sicurezza del software e di integrarsi efficacemente nei processi di valutazione e controllo dell'Ente. La coerenza tra i tre pilastri e la consistenza interna delle metriche attestano la robustezza metodologica della soluzione proposta, mentre le differenze riscontrate tra gli applicativi dimostrano la sua capacità di adattarsi a contesti eterogenei senza perdere significatività o capacità descrittiva. Oltre alla solidità analitica, la validazione ha messo in luce anche la flessibilità e la scalabilità del modello, che si è dimostrato applicabile a sistemi caratterizzati da diversi livelli di maturità tecnologica e gestionale. La possibilità di utilizzare lo stesso framework valutativo per applicativi con natura e funzionalità differenti tra loro, rappresenta uno degli elementi di maggiore valore, poiché consente all'Ente di mantenere nel tempo una visione unitaria e comparabile della sicurezza del proprio patrimonio software.

Dal punto di vista metodologico, la validazione ha dimostrato la coerenza del modello anche rispetto ai principi di trasparenza, tracciabilità e ripetibilità della misurazione, requisiti essenziali per un suo impiego continuativo nel contesto pubblico. Il modello, infatti, consente di documentare in modo chiaro ogni fase del processo di valutazione, fornendo indicatori sintetici ma fondati su evidenze verificabili. Ciò lo rende non solo uno strumento di controllo, ma anche un dispositivo di apprendimento organizzativo, capace di restituire valore informativo e orientare il miglioramento continuo.

In sintesi, la validazione ha quindi pienamente raggiunto gli obiettivi prefissati, consolidando la proposta metodologica e dimostrando che il modello possiede le caratteristiche per essere adottato in modo strutturato nell'ambito della governance regionale della sicurezza applicativa. La sua solidità, la capacità di adattamento e la trasparenza del processo valutativo lo rendono un riferimento operativo affidabile per la gestione della sicurezza del software in ambito pubblico, ponendo le basi per successive evoluzioni orientate al monitoraggio continuo e all'automazione dei processi di rendicontazione.

## 4.4 Limitazioni

L'attività di validazione, pur confermando la solidità e l'applicabilità del modello operativo per la valutazione della sicurezza del software, ha permesso di evidenziare alcune limitazioni, sia di natura metodologica, legate alle condizioni in cui la validazione è stata condotta, sia di carattere strutturale, proprie del modello stesso, come rappresentato sinteticamente in Figura 4.5. Queste limitazioni non riducono la validità complessiva dell'approccio, ma rappresentano elementi di riflessione utili per la sua futura evoluzione e per un suo impiego più esteso e automatizzato all'interno dell'ecosistema digitale regionale.

Le limitazioni riconducibili alla fase di validazione riguardano innanzitutto la dimensione e la composizione del campione. La verifica è stata infatti condotta su un numero limitato di applicativi, cinque in totale, selezionati in modo da rappresentare diverse condizioni di maturità tecnologica e priorità strategica, ma comunque non sufficienti a coprire l'intera eterogeneità del parco applicativo regionale. Sebbene tale scelta sia coerente con la natura sperimentale della ricerca, essa riduce la generalizzabilità dei risultati e impone cautela nell'estrapolare conclusioni di carattere universale. Inoltre, gli applicativi inclusi nel campione presentano stati di ciclo di vita relativamente omogenei: tutti si trovano infatti in una fase a regime, corrispondente alla piena operatività e alla stabilizzazione funzionale del software. Nessuno dei prodotti analizzati si collocava invece nelle fasi iniziali del ciclo di vita, come pre-rilascio o immediato post-rilascio, dove le dinamiche di sviluppo e di gestione della sicurezza risultano più instabili e soggette a variazioni. Questa circostanza ha limitato la possibilità di osservare il comportamento del modello in condizioni di maggiore variabilità, riducendo la capacità di testarne la sensibilità alle modifiche di stato dell'applicativo nel tempo.

Un'ulteriore limitazione riguarda la verifica delle metriche, considerato che questa è strettamente legata alla disponibilità e all'affidabilità dei dati forniti, nonché alla capacità di interpretare correttamente le evidenze tecniche trasmesse. Questa dipendenza è ulteriormente accentuata dal fatto che la validazione è stata condotta in un contesto simulato, dove il gruppo di lavoro della tesi ha agito in rappresentanza dei referenti ICT, applicando le logiche del modello senza il coinvolgimento diretto dei soggetti che avranno la responsabilità della rendicontazione. Tale impostazione, pur necessaria per garantire coerenza metodologica e controllo dei processi, ha inevitabilmente ridotto la rappresentatività organizzativa del test, limitando la possibilità di valutare appieno le dinamiche collaborative e i flussi informativi reali tra i diversi attori del modello.

Accanto a questi elementi, la validazione ha permesso di evidenziare anche alcune limitazioni intrinseche al modello operativo. La prima riguarda l'assenza di automatismi nella rendicontazione, che nella versione attuale del modello si basa su un processo manuale di raccolta, verifica e compilazione dei dati. Tale approccio, sebbene funzionale alla sperimentazione, comporta tempi di esecuzione più lunghi, una maggiore possibilità di errore umano e un livello di scalabilità limitato. Il modello è stato concepito in modo da poter essere integrato in futuro con strumenti di automazione e interfacce dirette verso piattaforme già in uso nell'Ente, ma questa integrazione costituisce un'evoluzione prevista e non ancora implementata. Il tema verrà infatti ripreso nel capitolo successivo, dedicato alle conclusioni e agli sviluppi futuri, dove sono proposte soluzioni tecniche per

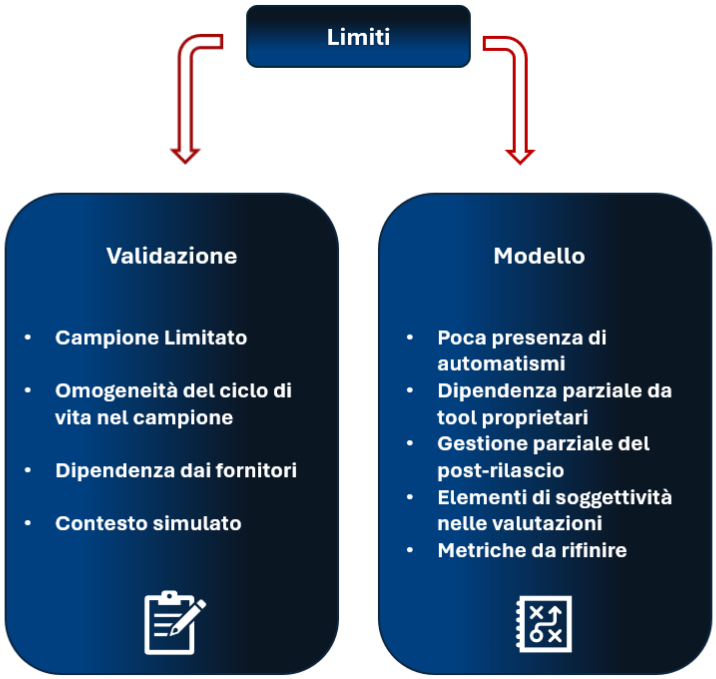


**Figura 4.5:** Rappresentazione delle limitazioni del processo di validazione e del modello operativo. Elaborazione dell'autore.

l'automatizzazione del processo di rendicontazione e monitoraggio.

Un ulteriore limite strutturale riguarda la dipendenza del modello da soluzioni proprietarie. L'utilizzo di *SonarQube* e *Meterian* come strumenti di riferimento per l'analisi del codice deriva dall'attuale assetto tecnologico regionale, ma vincola il modello a un ecosistema di strumenti specifici. Tale scelta, se da un lato garantisce continuità con le pratiche operative già in uso, dall'altro limita la portabilità e la replicabilità del modello in contesti che adottano strumenti diversi. In prospettiva, sarà pertanto utile prevedere la possibilità di parametrizzare le metriche in modo indipendente dai tool utilizzati, introducendo una logica di interoperabilità con altre piattaforme di analisi.

Altri limiti emergono con riferimento alla gestione delle fasi post-rilascio nel ciclo di vita del software. Sebbene il modello preveda un monitoraggio continuo nella quarta fase di rendicontazione, la sua implementazione è ancora poco strutturata e non completamente automatizzata. Ciò riduce la capacità di catturare tempestivamente variazioni significative nelle condizioni di sicurezza degli applicativi, in particolare dopo gli aggiornamenti o le modifiche infrastrutturali. La futura integrazione con strumenti di monitoraggio dinamico e segnalazione degli incidenti potrebbe colmare questa lacuna, garantendo una tracciabilità più costante nel tempo.

Un aspetto di rilievo metodologico riguarda la presenza di componenti soggettive nella valutazione di alcune metriche. In diversi casi, la determinazione del livello di conformità

dipende da informazioni qualitative fornite dai fornitori o da valutazioni interpretative legate alle azioni di mitigazione che verranno intraprese per colmare il non raggiungimento del target. Questa dimensione soggettiva, pur inevitabile in contesti complessi come quello della sicurezza applicativa, può introdurre margini di variabilità nei risultati e richiede, per il futuro, una maggiore strutturazione dei criteri di verifica e dei meccanismi di evidenza documentale.

In alcuni casi specifici, alcune metriche non sono state valutate o hanno evidenziato limiti di applicabilità. È il caso, ad esempio, della metrica *COD-COV02*, relativa al confronto tra le librerie dichiarate nel manifest e quelle rilevate tramite strumenti SCA. Il fornitore ha segnalato come tale indicatore possa risultare poco significativo o potenzialmente fuorviante, poiché la differenza tra librerie dichiarate e librerie effettivamente analizzate dipende dalla logica di dipendenza transitiva: uno stesso manifest con poche librerie può comportare l'inclusione di numerose dipendenze indirette, che varierebbero il perimetro ideale di analisi, andando a invalidare in parte il riferimento. In altri casi, come per la metrica *COD-LST01*, è emersa una sensibilità eccessiva della formula: il valore tende a ridursi drasticamente a zero anche in presenza di una sola libreria che necessiti di aggiornamento per componente. Tale configurazione, pur utile per rilevare tempestivamente vulnerabilità, potrebbe risultare troppo rigida e andrebbe calibrata per riflettere meglio le differenze tra componenti. Queste osservazioni forniscono indicazioni operative preziose per la revisione futura delle metriche, al fine di migliorarne la granularità e la capacità descrittiva.

Nel complesso, le limitazioni riscontrate non compromettono la validità del modello, ma ne delineano il perimetro di applicabilità e le aree di potenziale miglioramento. Esse riflettono in parte la natura sperimentale della validazione e in parte la complessità intrinseca di un sistema di misurazione che mira a integrare dimensioni tecniche, organizzative e normative. La consapevolezza di tali limiti costituisce un valore aggiunto per la ricerca, poiché consente di definire con maggiore precisione le direttrici di sviluppo del modello e di predisporre interventi mirati al suo consolidamento.

In prospettiva, le riflessioni emerse dalla fase di validazione e dall'analisi dei limiti rappresentano la base per le proposte di miglioramento che saranno presentate nel capitolo successivo, dedicato alle conclusioni e agli sviluppi futuri. In tale sede verranno delineate le possibili evoluzioni tecnologiche e metodologiche del modello, con particolare attenzione all'automatizzazione dei processi, all'ampliamento e consolidamento delle metriche e al rafforzamento della capacità predittiva e adattiva del sistema nel tempo.

# Capitolo 5

# Conclusioni e sviluppi futuri

Il percorso del progetto presentato in questa tesi ha avuto come obiettivo principale la definizione, progettazione e validazione di un modello operativo per la valutazione della sicurezza del software nel contesto della Regione Piemonte. Tale obiettivo nasce dall'esigenza concreta di dotare l'Ente di uno strumento metodologicamente valido, coerente con le direttive europee e nazionali sulla sicurezza informatica e capace di integrarsi nei processi di governance ICT già esistenti. L'intero lavoro si è sviluppato secondo una logica progressiva, che ha combinato una riflessione teorica sui principi della sicurezza applicativa con la costruzione di un framework operativo, fino alla sua verifica empirica su casi reali. In questo percorso, si è cercato di coniugare rigore metodologico e aderenza al contesto organizzativo, affinché il modello risultasse non solo concettualmente coerente, ma anche realmente utilizzabile.

Sotto il profilo dei risultati, la ricerca ha raggiunto gli obiettivi prefissati: il modello si è dimostrato affidabile, applicabile e coerente con il contesto regionale. La verifica delle quattro proprietà fondamentali, affidabilità, applicabilità, esaustività e scalabilità, ha confermato la robustezza dell'impianto metodologico, evidenziando al contempo gli ambiti su cui sarà opportuno concentrare i futuri perfezionamenti. La coerenza con le valutazioni precedenti condotte nell'ambito dei progetti correlati, rafforza ulteriormente la credibilità del modello e ne attesta la compatibilità con le prassi e gli strumenti già adottati a livello regionale.

Nel complesso, il lavoro svolto dimostra come sia possibile tradurre principi teorici, normativi e le linee guida di sicurezza in un sistema operativo concreto, capace di fornire risultati misurabili e di valore per l'organizzazione. Il modello non si limita a valutare la sicurezza del software, ma promuove una visione evolutiva della gestione ICT, in cui la sicurezza diventa una dimensione intrinseca e continua del ciclo di vita applicativo. La validazione empirica e i risultati ottenuti costituiscono dunque non solo una conferma della coerenza metodologica del modello, ma anche un punto di partenza per la sua futura evoluzione, verso forme di automazione, integrazione e scalabilità più avanzate. In questa prospettiva, il lavoro di tesi ha dunque completato un ciclo metodologico completo: dalla definizione concettuale del modello, alla sua progettazione tecnica, fino alla verifica sperimentale e alla proiezione verso l'implementazione operativa.

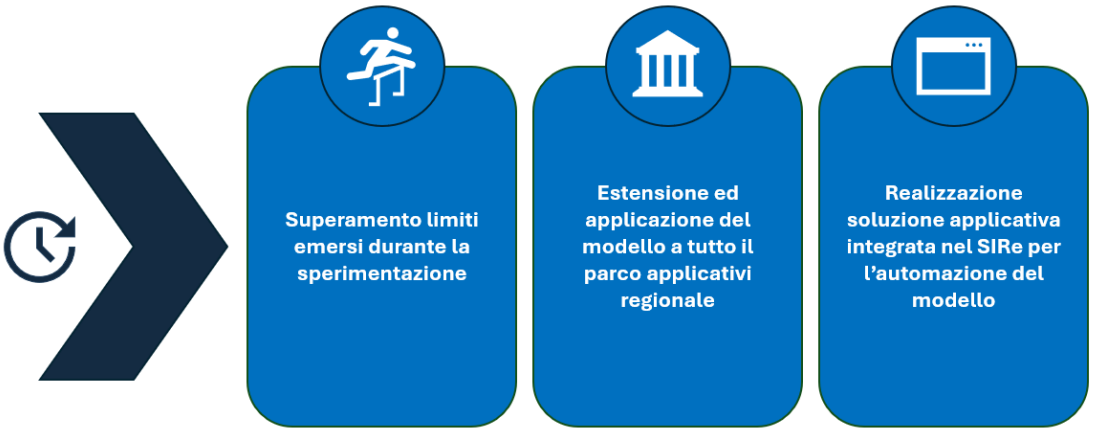


**Figura 5.1:** Rappresentazione delle tre direttrici principali per gli sviluppi futuri inerenti al perfezionamento e all'implementazione del modello operativo in Regione Piemonte

Il modello operativo sviluppato e validato nel corso di questo lavoro rappresenta quindi un punto di partenza solido ma non definitivo. La sua validazione ne ha dimostrato la robustezza metodologica e l'efficacia applicativa, ma al tempo stesso ha evidenziato margini di evoluzione che potranno essere colmati attraverso un percorso di consolidamento e progressiva integrazione tecnologica. Gli sviluppi futuri, in quest'ottica, si articolano lungo tre direttrici principali: il superamento dei limiti emersi durante la sperimentazione, l'estensione del modello a un perimetro più ampio di applicazioni regionali e l'implementazione di una soluzione applicativa dedicata, in grado di automatizzare la rendicontazione e integrarsi con l'architettura dei sistemi informativi regionali. La rappresentazione visiva delle direttrici principali degli sviluppi futuri del modello è mostrata in Figura 5.1.

Il primo ambito di evoluzione riguarda il superamento dei limiti del modello. La validazione ha evidenziato la necessità di automatizzare, almeno parzialmente, le attività di rendicontazione e monitoraggio, attualmente basate su processi manuali e compilazioni in fogli di calcolo. In prospettiva, il modello potrà essere implementato all'interno di un sistema informativo capace di interfacciarsi in modo diretto con gli strumenti di analisi statica e dinamica del codice già in uso presso l'Ente. Attraverso l'integrazione di API RESTful esposte da tali tool, sarà possibile estrarre automaticamente i dati di sicurezza e i report di analisi, alimentando in modo trasparente le metriche del pilastro *Codice*. La componente automatizzata dovrà essere in grado di precompilare le schede di rendicontazione, lasciando ai referenti ICT la sola attività di validazione e integrazione delle evidenze documentali.

Parallelamente, si prevede di ridurre la dipendenza da soluzioni proprietarie adottando progressivamente strumenti *open source* equivalenti, in grado di fornire analisi di sicurezza

comparabili e interoperabili. In questa prospettiva, le formule di calcolo delle metriche dovranno essere generalizzate per garantire coerenza indipendentemente dal tool impiegato, favorendo la portabilità del modello e la neutralità tecnologica. Tale approccio consentirà, inoltre, di rafforzare la sostenibilità a lungo termine del modello, riducendo i vincoli di licenza e ampliando la platea di soluzioni integrabili

Un'ulteriore area di miglioramento riguarda la standardizzazione delle procedure di compilazione. L'esperienza della validazione ha mostrato come alcuni indicatori presentino margini di soggettività interpretativa, spesso dipendenti dalla qualità e dalla completezza delle informazioni fornite dai fornitori. Per superare questa criticità, sarà necessario definire policy e linee guida di rendicontazione univoche, corredate da esempi pratici e da checklist operative, che consentano ai referenti ICT di applicare le metriche in modo coerente. Gli incontri periodici di formazione e confronto, già previsti nel sistema di monitoraggio e controllo, potranno essere estesi a questa finalità, contribuendo alla costruzione di un linguaggio tecnico condiviso e alla riduzione della variabilità nelle valutazioni.

La prospettiva di evoluzione del modello include anche la raffinazione di alcune metriche specifiche emerse come critiche. In particolare, la metrica *COD-LST01*, relativa all'aggiornamento delle librerie, potrà essere riformulata per evitare che la presenza di una sola libreria obsoleta azzeri il punteggio complessivo della componente, rendendo l'indicatore più sensibile alle differenze di gravità e distribuzione delle vulnerabilità. Analogamente, la metrica *COD-COV02*, attualmente esclusa per scarsa significatività, potrà essere ripensata integrando strumenti di analisi che valutino la profondità reale delle dipendenze, andando ad esempio a lavorare sullo SBOM, restituendo così una misura più coerente della complessità del software.

In prospettiva operativa, il modello potrà essere esteso a tutto il parco applicativo regionale, consentendo di costruire una *baseline* di sicurezza che rappresenti la fotografia complessiva dello stato dei sistemi informativi dell'Ente. Tale estensione permetterà di analizzare la distribuzione dei livelli di maturità, individuare pattern ricorrenti e definire priorità di intervento strategiche. Sarà inoltre l'occasione per testare il modello su applicativi in differenti fasi del ciclo di vita , dal pre-rilascio alla gestione a regime, ampliando così la base empirica e migliorando la capacità del modello di adattarsi a contesti dinamici.

Un ulteriore passaggio previsto consiste nell'introduzione del modello all'interno dei processi reali della Regione Piemonte, con il coinvolgimento diretto dei referenti ICT. Attraverso un percorso di sperimentazione progressiva, sarà possibile validare il modello in situazioni operative concrete, superando la dimensione simulata della validazione iniziale. In questa fase, il confronto costante con i fornitori permetterà di raffinare ulteriormente le metriche e di consolidare le modalità di raccolta delle evidenze.

Queste azioni di miglioramento trovano naturale continuità nella prospettiva di una soluzione applicativa dedicata, che costituisce la traduzione tecnologica del modello stesso. Lo sviluppo più significativo riguarda la progettazione e realizzazione di una soluzione che implementi il modello operativo e ne automatizzi le principali funzioni. Tale sistema potrà essere concepito come un modulo integrato nella piattaforma regionale di gestione dell'asset applicativo, già in uso per la catalogazione e il tracciamento del parco software dell'Ente. In questa architettura, la valutazione di sicurezza diventerà una proprietà nativa

di ciascun applicativo, sintetizzata da indicatori aggregati e dettagliata da schede specifiche compilabili in funzione della fase del ciclo di vita.

La soluzione sarà basata su un'architettura modulare a microservizi, con un database centralizzato per la persistenza delle informazioni e un *layer* di integrazione tramite API RESTful per l'interoperabilità con i sistemi regionali e i tool esterni. Il sistema di *backend* gestirà il motore di calcolo delle metriche, la generazione dei punteggi di conformità e la logica di aggiornamento periodico. La parte *frontend*, accessibile tramite interfaccia web, consentirà ai referenti ICT di visualizzare la situazione di sicurezza complessiva, compilare o aggiornare le schede, allegare evidenze e generare report di sintesi.

Un sistema di gestione eventi permetterà di attivare automaticamente notifiche e avvisi ai referenti ICT in caso di variazioni significative: ad esempio, una modifica del codice sorgente che innesca una nuova *build*, un alert di vulnerabilità rilevato dai tool SAST/SCA o la registrazione di un incidente di sicurezza. In tali casi, il sistema potrà richiedere la ricompilazione della scheda di rendicontazione o aggiornare automaticamente i valori delle metriche interessate. Tutte le versioni delle schede e dei punteggi saranno archiviate, consentendo analisi storiche e confronti longitudinali.

La dashboard di sicurezza applicativa, integrata nella sezione dedicata della piattaforma di gestione dell'asset o in un modulo applicativo di reporting esterno, rappresenterà il punto di accesso principale per la consultazione dei risultati. Essa mostrerà indicatori sintetici per pilastro, trend temporali, confronti tra applicativi e report esportabili in formato standard. I dati alimenteranno anche le attività di monitoraggio e controllo già descritte nei capitoli precedenti, permettendo un'integrazione diretta tra valutazione, rendicontazione e miglioramento continuo.

L'introduzione di tale sistema produrrà inevitabilmente impatti organizzativi significativi. Da un lato, la standardizzazione delle procedure di valutazione e la disponibilità di dati oggettivi contribuiranno a consolidare la cultura della sicurezza e la consapevolezza del rischio all'interno dell'Ente. Dall'altro, la digitalizzazione del processo permetterà di ridurre i tempi di raccolta, aumentare la tracciabilità delle evidenze e supportare decisioni più informate nella pianificazione delle attività ICT. L'adozione del modello in un contesto reale consentirà inoltre di promuovere un linguaggio tecnico condiviso tra referenti, fornitori e strutture regionali, favorendo la nascita di una comunità di pratica interna alla Regione Piemonte.

In prospettiva più ampia, il modello e la sua implementazione applicativa potranno essere riutilizzati come buona pratica anche da altre pubbliche amministrazioni, fungendo da riferimento per la definizione di metodologie di valutazione della sicurezza del software coerenti con le normative e le linee guida nazionali ed europee. Tale potenzialità di riuso rappresenta un'occasione di valorizzazione del lavoro svolto, che si traduce in un contributo concreto alla diffusione di approcci standardizzati alla governance della sicurezza applicativa nel settore pubblico, nonché all'adempimento agli obblighi di legge dell'art. 69 del Codice dell'Amministrazione Digitale (CAD) [23], a cui si potrà ottemperare pubblicando il codice sorgente della soluzione in formato *open source* sulla piattaforma nazionale di *Developers Italia*.

In conclusione, l'evoluzione del modello operativo non si limita a un miglioramento tecnico, ma si configura come un vero e proprio percorso di crescita organizzativa e culturale.

L'obiettivo non è soltanto misurare la sicurezza, ma renderla un elemento costitutivo dei processi di sviluppo, gestione e governo del software regionale. In definitiva, il modello rappresenta un patrimonio metodologico e operativo per la Regione Piemonte, in grado di orientare le scelte future in materia di sicurezza applicativa e di rafforzare la capacità dell'Ente di governare la propria trasformazione digitale in modo consapevole, misurabile e sicuro.

# Bibliografia


[1] *Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure elevate per un livello comune elevato di cibersicurezza nell'Unione (direttiva NIS2)*. Dic. 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[2] *Legge 28 giugno 2024, n. 90, disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*. Giu. 2024. URL: https://www.gazzettaufficiale.it/eli/id/2024/07/02/24G00108/SG.

[3] *Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS)*. Lug. 2016. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[4] *Decreto Legislativo 4 settembre 2024, n. 138, di recepimento della Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifiche al regolamento (UE) n. 910/2014 e alla direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148*. Set. 2024. URL: https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG.

[5] Agenzia per l'Italia Digitale (AgID). *Linee Guida di sicurezza nello sviluppo delle applicazioni*. Documento principale. 2022. URL: https://www.agid.gov.it/sites/agid/files/2024-07/Linee-guida_di_sicurezza_sviluppo-applicazioni.pdf.

[6] Agenzia per l'Italia Digitale (AgID). *Allegato A – Linee guida per l'adozione di un ciclo di sviluppo di software sicuro*. 2022. URL: https://www.agid.gov.it/sites/agid/files/2024-06/Linee_guida_per_ladozione_di_un_ciclo_di_sviluppo_di_software_sicuro.pdf.

[7] Agenzia per l'Italia Digitale (AgID). *Allegato B – Linee Guida per lo sviluppo sicuro di codice*. 2022. URL: https://www.agid.gov.it/sites/agid/files/2024-06/Linee_guida_per_lo_sviluppo_sicuro_di_codice.pdf.

[8] Agenzia per l'Italia Digitale (AgID). *Allegato C – Linee Guida per la configurazione per adeguare la sicurezza del software di base*. 2022. URL: https://www.agid.gov.it/sites/agid/files/2024-06/Linee_guida_per_la_configurazione_per_adeguare_la_sicurezza_del_software_di_base.pdf.

[9] Agenzia per l'Italia Digitale (AgID). *Allegato D – Linee Guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design*. 2022. URL: https://www.agid.gov.it/sites/agid/files/2024-06/Linee_guida_per_la_modellazione_delle_minacce-e-individuazione-azioni-di-mitigazione.pdf.

[10] Katherine Schroeder, Hung Trinh e Victoria Pillitteri. *Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures*. Special Publication (NIST SP 800-55 v1). Volume 1, guida per la selezione di misure di sicurezza. National Institute of Standards e Technology (NIST), 2024. URL: https://doi.org/10.6028/NIST.SP.800-55v1.

[11] Katherine Schroeder, Hung Trinh e Victoria Pillitteri. *Measurement Guide for Information Security: Volume 2 — Developing an Information Security Measurement Program*. Special Publication (NIST SP 800-55 v2). Volume 2, guida per lo sviluppo di un programma sistematico di misurazione della sicurezza. National Institute of Standards e Technology (NIST), 2024. URL: https://doi.org/10.6028/NIST.SP.800-55v2.

[12] Cherilyn Pascoe, Stephen Quinn e Karen Scarfone. *The NIST Cybersecurity Framework (CSF) 2.0*. Framework aggiornato per la gestione del rischio informatico. 2024. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[13] CIS–Sapienza Research / CINI Cybersecurity National Lab. *Framework Nazionale per la Cybersecurity e la Data Protection*. Versione aggiornata. 2025. URL: https://www.cybersecurityframework.it/sites/default/files/framework2/FNCDP_-_Edizione_2025_v2.1_-_Core.xlsx.

[14] *Legge regionale 28 luglio 2008, n. 23 — Disciplina dell'organizzazione degli uffici regionali e disposizioni concernenti la dirigenza ed il personale*. Bollettino Ufficiale 29 luglio 2008, suppl. ord. n. 2. Lug. 2008. URL: https://arianna.consiglioregionale.piemonte.it/base/coord/c2008023.html.

[15] *Legge regionale 4 settembre 1975, n. 48, Regione Piemonte — Costituzione del Consorzio per il trattamento automatico dell'informazione e del Comitato provvisorio per la progettazione di un sistema regionale integrato dell'informazione*. Pubblicata nel Bollettino Ufficiale n. 37 del 16 settembre 1975; testo coordinato. Set. 1975. URL: https://arianna.consiglioregionale.piemonte.it/base/coord/c1975048.html.

[16] *Convenzione Quadro tra Regione Piemonte e CSI Piemonte*. Deliberazione della Giunta Regionale n. 21-4474 del 29 dicembre 2021. Regolamenta la collaborazione e l'erogazione di servizi informatici e tecnologici nell'ambito della Pubblica Amministrazione regionale. 2021. URL: https://www.regione.piemonte.it/governo/bollettino/abbonati/2022/03/attach/dgr_04474_1050_29122021.pdf.

[17] Agenzia per la Cybersicurezza Nazionale. *Strategia Nazionale di Cybersicurezza 2022–2026*. Documento di indirizzo strategico per il rafforzamento della resilienza cibernetica nazionale. Mag. 2022. URL: https://www.acn.gov.it/portale/documents/20119/531899/ACN_Strategia.pdf/81644476-f547-6a63-dda6-3356f4d1b2f6?t=1719931791748.

[18] Agenzia per l'Italia Digitale (AgID) e Dipartimento per la Trasformazione Digitale (DTD). *Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024–2026*. Documento di programmazione strategica per la trasformazione digitale della Pubblica Amministrazione italiana. 2024. URL: https://www.agid.gov.it/it/agenzia/piano-triennale.

[19] Regione Piemonte. *Piano Strategico pluriennale ICT 2024–2026 della Regione Piemonte*. Approvato con DGR n. 7-8093 del 22 gennaio 2024. Gen. 2024. URL: https://www.regione.piemonte.it/web/temi/sviluppo/transizione-al-digitale/piano-strategico-pluriennale-ict-2024-2026.

[20] Regione Piemonte. *Piano Attuativo pluriennale ICT 2024–2026*. Approfondisce le iniziative operative annuali del Piano Strategico ICT 2024–2026 e viene aggiornato annualmente ( ultimo Aggiornamento 2025 ). Mag. 2025. URL: https://www.regione.piemonte.it/web/temi/sviluppo/transizione-al-digitale/piano-attuativo-pluriennale-ict-2024-2026.

[21] Agenzia per la Cybersicurezza Nazionale (ACN). *Regolamento per le infrastrutture digitali e per i servizi cloud per la Pubblica Amministrazione, ai sensi dell'articolo 33-septies, comma 4, del Decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla Legge 17 dicembre 2012, n. 221*. Pubblicato dall'Agenzia per la Cybersicurezza Nazionale (ACN). Giu. 2024. URL: https://www.acn.gov.it/portale/documents/d/guest/regolamentocloud.

[22] Agenzia per la Cybersicurezza Nazionale (ACN). *Determinazione n. 164179/2025*. Determinazione dell'Agenzia per la Cybersicurezza Nazionale - Specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto NIS. 2025. URL: https://www.acn.gov.it/portale/documents/d/guest/detacn_nis_specifiche_2025_164179_signed.

[23] *Codice dell'Amministrazione Digitale. D.Lgs. 7 marzo 2005, n. 82 e successive modifiche*. Gazzetta Ufficiale della Repubblica Italiana. 2005. URL: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82#.

# Appendice A

# Metriche del pilastro Codice

In questa appendice è riportato il documento elaborato durante il progetto di tesi, relativo alla fase di definizione delle metriche del pilastro *Codice*. Il documento fornisce una descrizione dettagliata di ciascuna metrica, con la relativa definizione, struttura e modalità di calcolo, secondo l'organizzazione e i criteri illustrati nel corpo della tesi. Tale appendice consente di avere una visione completa e strutturata degli output generati durante la definizione delle metriche di sicurezza inerenti al codice.

**Metriche e KPI – Pilastro Codice**

*Le metriche e i KPI sotto elencati sono basati sugli indicatori dell'analisi SAST ( Static Application Secutity Testing ), in particolare effettuata dal tool SonarQube, e dall'analisi SCA ( Software Composition Analysis ), effettuata con il tool Meterian. Sono state definite le metriche sulla base di questi due tool essendo gli strumenti attualmente utilizzati in Regione Piemonte.*

**COD-SR – Valutazione di Sicurezza ( Security Rating )**

L'insieme delle metriche "security", "security review" e "security hotspot" utilizzate in SonarQube. Nello specifico la metrica generale "Security Rating" misura il grado di sicurezza del codice sorgente. Essa ha il seguente significato rispetto alla scala di valori del tool:

A = 0 Vulnerabilità (o solo vulnerabilità di tipo "Informativa")
B = almeno 1 vulnerabilità di tipo "Minor" (minore)
C = almeno 1 vulnerabilità di tipo "Major" (maggiore)
D = almeno 1 vulnerabilità di tipo "Critical" (critica)
E = almeno 1 vulnerabilità di tipo "Blocker" (bloccante)

L'indicatore sarà alla base delle metriche di questa sezione

- **Unique ID:** COD-SR01
- **Goal:** Misurare il grado di sicurezza del prodotto software attraverso l'analisi statica del codice sorgente, per identificare e prevenire vulnerabilità in fase di sviluppo.
- **Scope:** Tutti i prodotti software sviluppati ( e/o manutenuti ) dai fornitori e analizzati tramite SonarQube.
- **Measure:** Percentuale di codice sorgente che rispetta la condizione "Security Rating su Overall Code pari ad A" secondo il quality gate di SonarQube, ponderata sul peso in Linee di Codice (LoC).
- **Type:** Metrica di efficacia
- **Formula:**

$$Security\ \ Compliance\ \ (\%) = \left( \frac{\sum LoC_{i \in A}}{\sum LoC_{i=1\ldots n}} \right) \times 100$$

  Dove:

  - A è l'insieme delle componenti che rispettano il rating A.
  - $LoC_i$ sono le Linee di Codice della componente i-esima.
  - n è il numero totale di componenti del prodotto.
- **Target:**
  ≥ 100% (Classe I), raccomandato come stato desiderato.

- **Implementation Evidence:**
  - Sintesi report generato automaticamente da SonarQube a ogni commit o build.
  - Classificazione del prodotto secondo le seguenti soglie:

| Classe | % codice conforme (Security Rating = A) |
|---|---|
| I | 100% |
| II | 67% – 99% |
| III | 34% – 66% |
| IV | 1% – 33% |
| V | 0% |

  - Evidenza documentata nel sistema CI/CD e disponibile nella dashboard SonarQube o equivalenti.

**COD-RR – Valutazione di Affidabilità ( Reliability Rating )**

L’insieme delle metriche di “relaibility” utilizzate in SonarQube. Nello specifico la metrica generale “Reliability Rating” misura il grado di affidabilità del codice sorgente. Essa ha il seguente significato rispetto alla scala di valori del tool:

A = 0 bug (o solo bug di tipo "Informativo")
B = almeno 1 bug di tipo "Minor" (minore)
C = almeno 1 bug di tipo "Major" (maggiore)
D = almeno 1 bug di tipo "Critical" (critico)
E = almeno 1 bug di tipo "Blocker" (bloccante)

L’indicatore sarà alla base delle metriche di questa sezione

- **Unique ID:** COD-RR01
- **Goal:** Valutare l'affidabilità del prodotto software in base alla presenza di bug rilevati tramite analisi statica, al fine di assicurare un comportamento corretto e prevedibile in fase di esecuzione.
- **Scope:** Tutti i prodotti software sviluppati (e/o manutenuti) dai fornitori, sottoposti ad analisi con SonarQube.
- **Measure:** Percentuale del codice sorgente del prodotto che non presenta bug secondo SonarQube e che rispetta la condizione “Reliability Rating su Overall Code pari ad A”, ponderata in base alle Linee di Codice (LoC).
- **Type:** Misura di efficacia
- **Formula:**

$$\textit{Reliability Compliance}\ (\%) = \left( \frac{\sum LoC_{i \in A}}{\sum LoC_{i=1..n}} \right) \times 100$$

Dove:

- A è l'insieme delle componenti che rispettano il rating A.
- $LoC_i$ sono le Linee di Codice della componente i-esima.
- n è il numero totale di componenti del prodotto.

- **Target:**
  ≥ 100% (Classe I) consigliato come stato ottimale.
- **Implementation Evidence:**
  - Sintesi report SonarQube generati ad ogni commit o build.
  - Aggregazione ponderata per LoC delle componenti con Reliability Rating = A.
  - Classificazione:

| Classe | % codice conforme (Reliability Rating = A) |
|---|---|
| I | 100% |
| II | 67% – 99% |
| III | 34% – 66% |
| IV | 1% – 33% |
| V | 0% |

  - Evidenza verificabile in SonarQube o dashboard CI/CD equivalente.

**COD-LSR – Valutazione di Sicurezza delle librerie ( Library Security Rating )**

La metrica è definita sulla base dell' *assessment report* di Meterian. In particolare è uno dei punteggi etichettato come *Security:* esso misura se la *codebase* è affetta da vulnerabilità di sicurezza. Viene dato da Meterian un punteggio da 0 – alta probabilità di insicurezza - a un punteggio di 100 – molto sicuro sulla base delle analisi del tool, sopratutto sulla base della presenza o meno di vulnerabilità di tipo *critical*

Questo riferimento è alla base delle metriche successive.

- **Unique ID:** COD-LSR01
- **Goal:** Valutare il livello di sicurezza del prodotto relativamente all'utilizzo di librerie di terze parti, identificando la presenza di vulnerabilità critiche nelle dipendenze software.
- **Scope:** Tutte le componenti di prodotto sviluppati (e/o manutenuti) dai fornitori, analizzate tramite tool Meterian, che includono dipendenze da librerie esterne.
- **Measure:** Percentuale di componenti software del prodotto che non presentano vulnerabilità CRITICAL sulle dipendenze secondo l'analisi Meterian.
- **Type:** Misura di efficacia
- **Formula:**

$$\textit{Library Security Compliance}\ (\%) = \left(\frac{N_{safe}}{N_{total}}\right) \times 100$$

  Dove:

  - N_{safe} = numero di componenti senza vulnerabilità CRITICAL.
  - N_{total} = numero totale di componenti analizzate.

- **Target:**
  ≥ 100% (Classe I) consigliato come livello ottimale.
- **Implementation Evidence:**
  - Report di analisi delle dipendenze generati da Meterian o tool SCA equivalenti.
  - Classificazione delle componenti in base alla presenza o assenza di vulnerabilità di tipo **CRITICAL**.
  - Classificazione secondo soglie percentuali:

| Classe | % componenti senza vulnerabilità CRITICAL |
|---|---|
| I | 100% |
| II | 67% – 99% |
| III | 34% – 66% |
| IV | 1% – 33% |
| V | 0% |

  - Evidenza tracciata in dashboard del sistema CI/CD o report Meterian esportabili.

**COD-LST – Valutazione della Stabilità delle librerie ( Library Stability)**

La metrica  è definita sulla base dell' *assessment report* di Meterian. In particolare è uno dei punteggi etichettato come *Stability:* nonostante possa essere non solo determinato dagli aspetti di sicurezza, analizza la presenza di difetti nella codebase che possano causare crash, comportamenti non previsti o basse prestazioni, parametri quindi che inficiano comunque l'affidabilità del codice. L'indicatore di stabilità viene calcolato da Meterian tutte le componenti che possano essere patchate: per ogni patch non applicata, viene sottratto 1 punto dal punteggio iniziale di 100.

Questo riferimento è alla base delle metriche successive.

- **Unique ID:** COD-LST01
- **Goal:** Valutare il livello di affidabilità e stabilità del prodotto relativamente all'utilizzo di librerie di terze parti, identificando la presenza di patch non applicate nelle dipendenze software.
- **Scope:** Tutte le componenti di prodotto sviluppati (e/o manutenuti) dai fornitori, analizzate tramite tool Meterian, che includono dipendenze da librerie esterne.
- **Measure:** Percentuale di componenti software del prodotto che non presentano patch NON APPLICATE sulle dipendenze secondo l'analisi Meterian.
- **Type:** Misura di efficacia
- **Formula:**

$$Library\ \ Stability\ \ Compliance\ \ (\%) = \left( \frac{N_{stable}}{N_{total}} \right) \times 100$$

  Dove:

  - N_{stable} = numero di componenti senza patch NON APPLICATE.
  - N_{total} = numero totale di componenti analizzate.

- **Target:**
  ≥ 100% (Classe I) consigliato come livello ottimale.
- **Implementation Evidence:**
  - Report di analisi delle dipendenze generati da Meterian o tool SCA equivalenti.
  - Classificazione delle componenti in base alla presenza o assenza di patch da applicare.

- Classificazione secondo soglie percentuali:

| Classe | % componenti senza patch NON APPLICATE |
|---|---|
| I | 100% |
| II | 67% – 99% |
| III | 34% – 66% |
| IV | 1% – 33% |
| V | 0% |

- Evidenza tracciata in dashboard del sistema CI/CD o report Meterian esportabili.

**COD-COV – Copertura Codice Sorgente ( Coverage )**

Le metriche si pongono l'obiettivo di verificare la quasi totale copertura delle analisi SAST e SCA sul codice sorgente.

- **Unique ID:** COD-COV01
- **Goal:** Verificare che la totalità del codice sorgente del prodotto sia effettivamente sottoposta ad analisi statica tramite SonarQube, garantendo così una copertura completa nel monitoraggio di bug e vulnerabilità.
- **Scope:** Tutto il codice sorgente sviluppato internamente o integrato nel prodotto (inclusi moduli core, microservizi, API, frontend/backend, ecc.).
- **Measure:** Percentuale di linee di codice (LoC) del prodotto che risultano analizzate da SonarQube rispetto al totale del codice presente nel repository.
- **Type:** Metrica di implementazione
- **Formula:**

$$SAST \;\; Coverage \;\; (\%) = \left( \frac{LoC_{SAST}}{LoC_{total}} \right) \times 100$$

  Dove:

  - LoC_{SAST} = linee di codice effettivamente analizzate da SonarQube.
  - LoC_{total} = linee di codice presenti nel repository/version control.

- **Target:**
  100% (analisi completa)
  Soglia minima accettabile: ≥ 95% per copertura quasi totale, con giustificazioni documentate per le esclusioni.

- **Implementation Evidence:**
    - Confronto tra:
        - Numero totale di LoC (misurabile tramite script CI, plugin Git ).
        - Numero di LoC analizzate da SonarQube (presente nei report SonarQube).
    - Evidenza documentata nei pipeline log, nei report build, e nella dashboard SonarQube.

- **Unique ID:** COD-COV02
- **Goal:** Verificare che tutte le librerie di terze parti e dipendenze esterne siano effettivamente sottoposte ad analisi di sicurezza tramite strumenti di SCA (es. Meterian), per garantire che eventuali vulnerabilità note vengano individuate tempestivamente.
- **Scope:** Tutte le dipendenze (librerie, pacchetti, moduli) incluse nei progetti software del prodotto, indipendentemente dal linguaggio (Java, JS, Python, ecc.) o dallo strumento di package management (es. Maven, npm, pip, ecc.).
- **Measure:** Percentuale di librerie/dipendenze effettivamente analizzate tramite Meterian rispetto al numero totale di librerie dichiarate nei manifest file.
- **Type:** Metrica di implementazione
- **Formula:**

  $$SCA\ \ Coverage\ \ (\%)=\left(\frac{N_{analizzate}}{N_{totali}}\right)\times 100$$

  Dove:
    - N_{analizzate} = numero di dipendenze effettivamente sottoposte ad analisi da Meterian.
    - N_{totali} = numero totale di dipendenze dichiarate nei file di configurazione.
- **Target:**
  100% (tutte le dipendenze analizzate )
  Soglia minima accettabile: ≥ 95% per copertura quasi totale, con motivazioni documentate per le esclusioni (es. dipendenze locali o non supportate)
- **Implementation Evidence:**
    - Report generato da Meterian che elenca le dipendenze analizzate.
    - Confronto con il numero totale di dipendenze presenti nei manifest file
    - Log CI/CD o script di scansione che mostrino la presenza dell'analisi Meterian in pipeline.

**Tabella Riepilogo Metriche e KPI – Pilastro Codice**

| ID | Ambito | Tipo di misura | Obiettivo | Formula principale | Target | Note |
|---|---|---|---|---|---|---|
| **COD-SR01** | Security Rating | Efficacia | Misurare il grado di sicurezza del codice per prevenire vulnerabilità in fase di sviluppo | % codice con Security Rating = A, ponderata per LoC | ≥ 100% (Classe I) | *Definizione delle Classi: I: 100%, II: 67–99%, III: 34–66%, IV: 1–33%, V: 0%* |
| **COD-RR01** | Reliability Rating | Efficacia | Valutare l'affidabilità del software tramite rilevazione di bug | % codice con Reliability Rating = A, ponderata per LoC | ≥ 100% (Classe I) | *Definizione delle Classi: I: 100%, II: 67–99%, III: 34–66%, IV: 1–33%, V: 0%* |
| **COD-LSR01** | Library Security | Efficacia | Valutare la sicurezza delle librerie esterne rilevando vulnerabilità CRITICAL | % componenti senza vulnerabilità CRITICAL | ≥ 100% (Classe I) | *Definizione delle Classi: I: 100%, II: 67–99%, III: 34–66%, IV: 1–33%, V: 0%* |
| **COD-LST01** | Library Stability | Efficacia | Valutare stabilità e affidabilità delle librerie tramite verifica patch | % componenti senza patch NON APPLICATE | ≥ 100% (Classe I) | *Definizione delle Classi: I: 100%, II: 67–99%, III: 34–66%, IV: 1–33%, V: 0%* |
| **COD-COV01** | Coverage SAST | Implementazione | Verificare che tutto il codice sorgente sia coperto da analisi statica (SAST) | % LoC analizzate da SonarQube / totali | 100% (≥ 95% con giustificazioni documentate) | |
| **COD-COV02** | Coverage SCA | Implementazione | Verificare che tutte le dipendenze siano analizzate tramite SCA (Meterian) | % dipendenze analizzate da Meterian / totali dichiarate | 100% (≥ 95% con giustificazioni documentate) | |

# Appendice B

# Metriche del pilastro Infrastruttura

In questa appendice è riportato il documento elaborato durante il progetto di tesi, relativo alla fase di definizione delle metriche del pilastro *Infrastruttura*. Il documento fornisce una descrizione dettagliata di ciascuna metrica, con la relativa definizione, struttura e modalità di calcolo, secondo l'organizzazione e i criteri illustrati nel corpo della tesi. Tale appendice consente di avere una visione completa e strutturata degli output generati durante la definizione delle metriche di sicurezza inerenti all'infrastruttura digitale.

**Metriche e KPI – Pilastro Infrastruttura**

*L'elenco delle seguenti metriche è stato redatto sulla base dei livelli minimi previsti nel caso di dati e servizi ordinari indicati nel Regolamento per le infrastrutture digitali e per i servizi cloud per la Pubblica Amministrazione, redatto dall'Agenzia per la Cybersicurezza Nazionale ( ACN* ).

**INF-A– Disponibilità**

Livelli di disponibilità dell'infrastruttura fisica e digitale

- **Unique ID:** INF-A01
- **Goal:** Garantire la continuità operativa e la qualità dei servizi digitali tramite un'infrastruttura ICT altamente affidabile. L'obiettivo di sicurezza è assicurare la disponibilità delle risorse critiche e non riducendo al minimo i disservizi.
- **Scope:** Infrastruttura digitale a supporto dei servizi istituzionali (es. rete, server, storage, virtualizzazione).
- **Measure:** Percentuale di tempo annuo in cui l'infrastruttura è disponibile, calcolata sia al netto sia includendo i fermi programmati.
- **Type:** Misura di efficacia.
- **Formula:**
  - Disponibilità = (1 - [tempo di inattività non pianificato] / [tempo totale annuo]) × 100
  - Disponibilità totale = (1 - [tempo di inattività totale, inclusi fermi pianificati] / [tempo totale annuo]) × 100
- **Target:**
  - ≥ 99,98% senza fermi programmati
  - ≥ 99,6% includendo i fermi programmati
- **Implementation Evidence:** Log di sistema, report da strumenti di monitoraggio, registro fermi pianificati, report incident management, dati SLA.

**INF-DC – Sicurezza Data Center**

Conformità dei Data Center a requisiti minimi di sicurezza fisica e infrastrutturale

- **Unique ID:** INF-DC01
- **Goal:** Garantire la protezione fisica e infrastrutturale dei sistemi critici per assicurare la disponibilità, l'integrità e la resilienza dei servizi digitali erogati attraverso il Data Center.
- **Scope:** Tutti i Data Center (CED) di proprietà o gestiti dal soggetto fornitore, inclusi locali, impianti, infrastrutture elettriche e antincendio. Esclusi ambienti temporanei, laboratori e uffici tecnici non utilizzati per l'elaborazione dati.

- **Measure:** Numero di requisiti minimi di sicurezza fisica e infrastrutturale soddisfatti sul totale previsto (5 su 5):
    - R1. Il soggetto garantisce il presidio operativo all'interno del Data Center per 24 ore al giorno, 7 giorni a settimana per tutto l'anno.
    - R2. Il Data Center è stato progettato e realizzato secondo standard di riferimento infrastrutturali, ad esempio ANSI/BICSI 002, TIA-942, EN 50600, Uptime Institute Tier Certification o analoghi.
    - R3. Il soggetto garantisce le caratteristiche antincendio del Data Center in conformità alle norme antincendio vigenti.
    - R4. Nei locali ospitanti i Data Center sono presenti pavimenti flottanti qualora la distribuzione dell'alimentazione elettrica e del cablaggio non avvenga per via aerea.
    - R5 -Il soggetto garantisce che tutti i server dei Data Center sono connessi ad apparati per la continuità elettrica (UPS).
- **Type:** Misura di implementazione.
- **Formula:**
    - Conformità = (Numero di requisiti soddisfatti / Numero totale di requisiti previsti) × 100
- **Target:**
    - 100% di conformità ai 5 requisiti fondamentali specificati.
- **Implementation Evidence:**
    - Registro delle certificazioni di progettazione e costruzione (es. TIA-942, EN 50600)
    - Contratti o turni di servizio per presidio 24/7
    - Documentazione impianti antincendio (conformità normativa)
    - Planimetrie tecniche che evidenziano la presenza di pavimenti flottanti
    - Inventario server con indicazione connessione a UPS

- **Unique ID:** INF-DC02
- **Goal:** Ridurre il rischio di accessi non autorizzati e danni ambientali ai sistemi critici attraverso l’adozione di misure di sicurezza fisica e ambientale.
- **Scope:** Tutti i locali Data Center, incluse le aree perimetrali, punti di accesso, zone di carico/scarico, impianti di controllo ambientale e supporti fisici.
- **Measure:** Numero di misure fisiche e ambientali implementate e mantenute sul totale di quelle previste (3 su 3):

    - R1. Esiste un documento di dettaglio che definisce politiche e procedure inerenti allo spostamento sicuro di supporti fisici. Queste policy e procedure dovranno essere riviste su base almeno annuale.
    - R2. Sono implementati, manutenuti e adottati sistemi di sorveglianza all'esterno dei data center e in tutti i punti di ingresso e uscita al fine di rilevare ogni tentativo di ingresso non autorizzato.
    - R3. Sono implementati, mantenuti e adottati, all'interno dei Data Center, i sistemi di controllo ambientale al fine di monitorare e testare l'adeguatezza delle temperature e le condizioni di umidità all'interno dell'area, nel rispetto dei principali standard di settore.
- **Type:** Misura di implementazione.
- **Formula:**
    - Conformità = (Numero di controlli implementati / Totale controlli previsti) × 100
- **Target:**
    - 100% di adozione e mantenimento delle misure previste
- **Implementation Evidence:**
    - Documento ufficiale delle policy per la gestione sicura dei supporti fisici, con firma e data di revisione
    - Log di manutenzione e verifica dei sistemi di videosorveglianza (esterni e accessi)
    - Report di monitoraggio ambientale (temperature e umidità), registro degli allarmi ambientali, documentazione di conformità agli standard

**INF-AM – Asset Management**

I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio.

- **Unique ID:** INF-AM01
- **Goal:** Garantire la visibilità completa e il controllo sugli asset fisici dell'organizzazione ( e/o fornitore ) per prevenire accessi non autorizzati e migliorare la gestione delle risorse ICT.
- **Scope:** Tutti i sistemi e gli apparati fisici connessi o connettibili alla rete interna dell'organizzazione ( e/o fornitore ), inclusi server, dispositivi di rete, workstation, stampanti e dispositivi mobili aziendali.
- **Measure:** Percentuale di sistemi e apparati fisici effettivamente censiti sul totale di quelli rilevati in rete o presenti fisicamente.
- **Type:** Misura di implementazione ed efficacia.
- **Formula:**

    - Conformità = (Numero dispositivi censiti e approvati / Numero totale dispositivi presenti o rilevati in rete interna aziendale ) × 100
- **Target:**
    - 100% dei dispositivi fisici devono essere censiti e approvati; 0% di accessi da dispositivi non autorizzati
- **Implementation Evidence:**
    - Elenco aggiornato degli asset fisici
    - Log e report dei sistemi di discovery e controllo accessi
    - Policy che definisce il processo di approvazione e inserimento di nuovi asset

- **Unique ID:** INF-AM02
- **Goal:** Garantire la tracciabilità, la sicurezza e il controllo dei flussi informativi all'interno e all'esterno dell'organizzazione, riducendo i rischi di perdita o esfiltrazione di dati.
- **Scope:** Tutti i flussi di dati strutturati e non strutturati, interni ed esterni, relativi all'infrastruttura digitale, ai servizi ICT e ai sistemi informativi dell'organizzazione.
- **Measure:** Percentuale di flussi identificati, censiti e approvati sul totale dei flussi rilevati o utilizzati operativamente.
- **Type:** Misura di implementazione ed efficacia.
- **Formula:**
    - Conformità = (Numero di flussi identificati, mappati e approvati / Numero totale flussi rilevati o utilizzati) × 100
- **Target:**
    - 100% dei flussi di dati devono essere censiti e formalmente approvati
- **Implementation Evidence:**
    - Registro ufficiale dei flussi di dati (data flow inventory o data flow map)
    - Documentazione di approvazione da parte dei responsabili di processo o ICT
    - Report di strumenti di network monitoring, DLP o data flow analysis
    - Policy per la gestione dei flussi di dati

**INF-RA – Analisi del rischio**

L’assessment comprende il rischio di cybersecurity inerente all'operatività dell'organizzazione , degli asset e degli individui.

- **Unique ID:** INF-RA01
- **Goal:** Assicurare che tutte le risorse infrastrutturali critiche dell’organizzazione ( e/o fornitore ) siano periodicamente verificate e testate per identificare e documentare le vulnerabilità, con il fine di migliorare la sicurezza complessiva e mitigare i rischi cibernetici.
- **Scope:** Tutte le risorse, inclusi sistemi, dispositivi, locali, infrastrutture critiche, sia gestite internamente che in outsourcing.
- **Measure:** Percentuale di risorse critiche testate e verificate per le vulnerabilità, rispetto al totale delle risorse individuate.
- **Type:** Misura di implementazione ed efficacia.
- **Formula:**
    - Conformità = (Numero di risorse testate per vulnerabilità / Numero totale di risorse identificate) × 100

  Può essere applicata ad una categoria di risorse specifiche ( ad es. risorse per la sicurezza perimetrale )
- **Target:**
    - 100% delle risorse *critiche* devono essere testate e verificate annualmente per vulnerabilità
- **Implementation Evidence:**
    - Piano aggiornato di verifica e test di sicurezza
    - Documentazione delle attività di scansione delle vulnerabilità e dei test di sicurezza
    - Report di audit sui sistemi in outsourcing

**INF-AC – Gestione delle identità digitali e dell’accesso alle risorse**

L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate.

- **Unique ID:** INF-AC01
- **Goal:** Garantire che le credenziali di accesso per utenti, dispositivi e processi siano gestite in modo sicuro, con adeguate politiche di aggiornamento, verifica, revoca e audit, rispettando i principi di segregazione delle funzioni e minimizzazione dei privilegi.
- **Scope:** Gestione delle identità digitali, credenziali di accesso per personale interno ed esterno, dispositivi e processi aziendali.

- **Measure:** Percentuale di credenziali gestite in conformità con le politiche aziendali di accesso e sicurezza.
- **Type:** Misura di implementazione ed efficacia.
- **Formula:**
    - Conformità = (Numero di credenziali gestite in conformità con i requisiti elencati / Numero totale di credenziali) × 100

  Requisiti:

- R1. Le credenziali di accesso sono individuali per il personale del soggetto e per il personale esterno che ha accesso all'infrastruttura e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza.
- R2. Esistono politiche e procedure per la gestione delle credenziali di cui al requisiti R1, le quali dovranno essere aggiornate almeno su base annuale e rese disponibili, per la consultazione, all'Amministrazione.
- R3. Sono definiti meccanismi di gestione, memorizzazione e revisione delle informazioni in materia di credenziali, identità di sistema e livello di accesso.
- R4. Le credenziali sono aggiornate tempestivamente e senza ingiustificato ritardo qualora vi siano variazioni dell'utenza .
- R5. Le identità di sistema sono gestite impiegando certificati digitali o tecniche alternative che assicurano un livello equivalente di sicurezza.
- R6. Esiste una pianificazione aggiornata degli audit di sicurezza per verificare il rispetto di quanto previsto nei requisiti precedenti ed esiste un registro degli audit effettuati con la relativa documentazione.

- **Target:**
    - 100% delle credenziali devono essere conformi ai requisiti elencati
- **Implementation Evidence:**
    - Documentazione delle politiche e procedure di gestione delle credenziali, incluse le revisioni annuali
    - Registro di accesso e aggiornamento delle credenziali, con evidenza della segregazione delle funzioni
    - Report degli audit di sicurezza periodici e documentazione di revisione delle credenziali
    - Registro delle variazioni dell'utenza  e aggiornamento tempestivo delle credenziali
    - Certificati digitali o tecniche di sicurezza equivalenti utilizzati per la gestione delle identità di sistema

- **Unique ID:** INF-AC02
- **Goal:** Garantire che l'accesso fisico alle risorse critiche sia protetto attraverso politiche di sicurezza, processi, metodologie e tecnologie adeguate, nonché definire un perimetro di sicurezza fisico per proteggere il personale, i dati e i sistemi informativi.
- **Scope:** Accesso fisico a tutte le risorse critiche e infrastrutture, in particolare ai Data Center, sistemi informatici sensibili e aree protette.
- **Measure:** Percentuale di risorse fisiche protette e amministrate secondo le politiche di accesso fisico.
- **Type:** Misura di implementazione ed efficacia.
- **Formula:**
    - Conformità = (Numero di risorse fisiche protette conformemente ai requisiti / Numero totale di risorse fisiche) × 100

  Requisiti:
    - R1. Esistenza di un documento aggiornato con le politiche di sicurezza adottate per la protezione e l'amministrazione degli accessi fisici e processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
    - R2. È definito un perimetro di sicurezza fisico al fine di salvaguardare il personale, i dati e i sistemi informativi.
- **Target:**
    - 100% delle risorse fisiche critiche devono essere protette e amministrate in conformità con le politiche di sicurezza fisica adottate.
- **Implementation Evidence:**
    - Documentazione aggiornata delle politiche di sicurezza per l'accesso fisico, inclusi i censimenti delle risorse
    - Descrizione dei processi, metodologie e tecnologie impiegate per garantire la protezione e l'amministrazione dell'accesso fisico
    - Piano e report sulla definizione del perimetro di sicurezza fisico, che includa misure di protezione per il personale, i dati e i sistemi

- **Unique ID:** INF-AC03
- **Goal:** Garantire che l'accesso remoto alle risorse sia amministrato con misure di controllo adeguate, che includano il monitoraggio, la registrazione, l'autenticazione sicura e la gestione centralizzata degli accessi, in modo da proteggere i dati e le risorse dell'amministrazione.
- **Scope:** Accessi remoti a tutte le risorse e infrastrutture aziendali, comprese le risorse dati e sistemi informativi sensibili.

- **Measure:** Percentuale di accessi remoti amministrati in conformità con le politiche di sicurezza aziendale.
- **Type:** Misura di implementazione ed efficacia.
- **Formula:**
    - Conformità = (Numero di accessi remoti gestiti con adeguate misure di sicurezza conformemente ai requisiti elencati / Numero totale di accessi remoti) × 100

  Requisiti:

    - R1. Gli accessi da remoto effettuati sono monitorati da parte di un team preposto di cybersecurity
    - R2. Fatti salvi documentati limiti tecnici, sono implementate adeguate misure di controllo dell'accesso, adottando sistemi di autenticazione, autorizzazione e registrazione/contabilizzazione centralizzata degli accessi, coadiuvati da sistemi di autenticazione, la cui sicurezza è proporzionale al rischio
    - R3. definito e implementato un modello di gestione degli accessi centralizzato volto ai processi di autorizzazione, logging e comunicazione degli accessi alle risorse e ai dati dell'Amministrazione.
    - R4. Esiste un log degli accessi eseguiti da remoto
    - R5.Per gli accessi da remoto, sono impiegati modalità di autenticazione a fattore multiplo.
- **Target:**
    - 100% degli accessi remoti devono essere monitorati, registrati e protetti da adeguate misure di autenticazione e autorizzazione centralizzate, conformemente ai requisiti elencati.
- **Implementation Evidence:**
    - Documentazione delle politiche di gestione dell'accesso remoto
    - Sistema di monitoraggio centralizzato degli accessi remoti, con evidenza di logging e registrazione degli accessi
    - Report di auditing degli accessi remoti e dei sistemi di autenticazione impiegati
    - Descrizione dei sistemi di autenticazione a fattore multiplo e loro applicazione agli accessi remoti

- **Unique ID:** INF-AC04
- **Goal:** Garantire che i diritti di accesso alle risorse siano amministrati in conformità con i principi di privilegio minimo e separazione delle funzioni, per minimizzare i rischi di accesso non autorizzato e per proteggere i dati e le risorse sensibili.

- **Scope:** Tutte le risorse dell'organizzazione, inclusi dati, applicazioni, sistemi e infrastrutture, nonché i gruppi di utenti e le loro autorizzazioni.
- **Measure:** Percentuale di risorse e accessi correttamente gestiti secondo il principio del privilegio minimo e separazione delle funzioni.
- **Type:** Misura di implementazione ed efficacia.
- **Formula:**
    - Conformità = (Numero di risorse e gruppi di utenti gestiti secondo i requisiti elencati / Numero totale di risorse e gruppi di utenti) × 100

  Requisiti:

    - R1. Sono le risorse censite a cui è necessario accedere, per quali funzioni e con quali autorizzazioni, i gruppi di utenti e i loro privilegi in relazione alle risorse a cui possono accedere e con quali autorizzazioni e l'assegnazione degli utenti censiti a gruppi di utenti.
    - R2. Nell'ambito di implementazione dell'accesso al sistema informativo, vengono osservati principi di separazione delle funzioni e del privilegio minimo in relazione al rischio organizzativo.
    - R3. Sono definite e implementate politiche, procedure e misure tecniche per la segregazione dei ruoli di accesso privilegiato in modo che l'accesso amministrativo ai dati, le capacità di crittografia e gestione delle chiavi e le capacità di registrazione siano distinte e separate.
- **Target:**
    - 100% delle risorse e degli utenti devono rispettare le politiche di privilegio minimo e separazione delle funzioni, con una gestione corretta e documentata dei gruppi e delle autorizzazioni di accesso.
- **Implementation Evidence:**
    - Documentazione dei censimenti delle risorse e delle relative autorizzazioni di accesso
    - Report sui gruppi di utenti e sui privilegi associati alle risorse
    - Politiche e procedure per la separazione delle funzioni e per l'assegnazione dei privilegi minimi
    - Evidenze delle misure tecniche adottate per la segregazione dei ruoli di accesso privilegiato, inclusi l'accesso amministrativo ai dati, la gestione delle chiavi di crittografia e la registrazione

**INF-BA – Backup delle informazioni**

- **Unique ID:** INF-BA01
- **Goal:** Assicurarsi che i backup dei dati vengano eseguiti periodicamente, siano amministrati in modo sicuro e siano verificati regolarmente per garantire la disponibilità e la ripristinabilità delle informazioni in caso di incidenti.
- **Scope:** Dati memorizzati su sistemi locali, nel cloud e relativi all'Amministrazione, inclusi backup necessari per il completo ripristino dei sistemi e dei servizi.
- **Measure:** Percentuale di backup eseguiti regolarmente e con successo verificati (test di ripristino).
- **Type:** Misura di conformità, che valuta l'esecuzione, la gestione e la verifica dei backup, inclusi quelli nel cloud.
- **Formula:**
    - Percentuale di backup con successo = (Numero di backup eseguiti e verificati regolarmente / Numero totale di backup pianificati) × 100, con i seguenti requisiti:
        - R1. Il 100% dati devono essere coperti da backup
        - R2. I backup devono essere eseguiti con frequenza ragionevole sulla base della criticità del dato
        - R3. I backup devono essere protetti in termini di riservatezza, integrità e disponibilità.
- **Target:**
    - 100% dei dati devono essere sottoposti a backup periodici.
    - I backup devono essere verificati tramite test di ripristino almeno una volta all'anno.
    - I backup devono essere protetti in termini di riservatezza, integrità e disponibilità.
- **Implementation Evidence:**
    - Documentazione dei backup eseguiti (compresi backup locali e nel cloud).
    - Report dei test di ripristino annuali.
    - Registri che documentano la protezione dei backup e le misure di sicurezza per garantire che non siano accessibili in modo permanente ai sistemi.

**INF-MA – Manutenzione**

La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti

- **Unique ID:** INF-MA01
- **Goal:** Garantire che la manutenzione remota delle risorse e dei sistemi avvenga in modo sicuro, con accessi controllati e autorizzati, per evitare accessi non autorizzati e potenziali rischi per la sicurezza.
- **Scope:** Manutenzione remota delle risorse IT e dei sistemi, comprese le funzioni di sicurezza, effettuata sia da personale interno che da terze parti.
- **Measure:** Percentuale di manutenzione remota eseguita in conformità alle politiche di autorizzazione e sicurezza definite.
- **Type:** Misura di conformità, che verifica se gli accessi remoti per la manutenzione sono stati adeguatamente approvati e documentati.
- **Formula:**
    - Percentuale di manutenzione remota conforme = (Numero di manutenzioni remote conformi ai requisiti elencati / Numero totale di manutenzioni remote) × 100

      Requsiti:

        - R1. Conformi ai requisiti di INF-AC03 ( Target Metrica soddisfatta)
        - R2. Tutti di accessi eseguiti da remoto da personale di terze parti siano autorizzati dall’organizzazione  di cybersecurity
- **Target:**
    - 100% degli accessi remoti di manutenzione devono essere autorizzati dal team di cybersecurity.
    - Accessi remoti limitati ai soli casi essenziali, con adeguata documentazione e approvazione.
- **Implementation Evidence:**
    - Registri di approvazione per la manutenzione remota.
    - Documentazione dei processi e delle procedure di autorizzazione per la manutenzione remota.
    - Log di accesso remoto contenenti i dettagli su chi ha effettuato l'accesso, quando e per quale motivo.

- **Unique ID:** INF-MA02
- **Goal:** Garantire che le reti di comunicazione e controllo siano protette attraverso l'uso di sistemi perimetrali adeguatamente configurati, aggiornati e manutenuti, inclusi firewall e altri sistemi di sicurezza di rete.

- **Scope:** Reti di comunicazione e controllo che gestiscono il flusso di informazioni sensibili e vitali per l'organizzazione, comprese le soluzioni di sicurezza come i firewall (sia di rete che applicativi).
- **Measure:** Percentuale di sistemi perimetrali (firewall e dispositivi simili) che sono aggiornati, configurati e manutenuti correttamente.
- **Type:** Misura di conformità, che verifica se i sistemi di protezione delle reti sono mantenuti e configurati correttamente.
- **Formula:**
    - Percentuale di sistemi di protezione correttamente configurati = (Numero di sistemi perimetrali correttamente configurati e aggiornati / Numero totale di sistemi perimetrali) × 100
- **Target:**
    - 100% dei sistemi perimetrali (firewall e simili) devono essere aggiornati, configurati e manutenuti correttamente.
    - I sistemi perimetrali devono essere regolarmente testati e configurati per proteggere adeguatamente le reti di comunicazione e controllo.
- **Implementation Evidence:**
    - Registri di configurazione e manutenzione dei sistemi perimetrali (firewall, dispositivi di rete sicuri).
    - Report di aggiornamenti e modifiche dei firewall e di altri dispositivi di sicurezza di rete.
    - Documentazione delle politiche e delle procedure di gestione e protezione dei sistemi perimetrali.

**INF-DE – Monitoraggio continuo di sicurezza**

I sistemi informativi e gli asset sono monitorati per identificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.

- **Unique ID:** INF-DE01
- **Goal:** Garantire che l'organizzazione monitori costantemente la rete informatica per rilevare eventi di cybersecurity e potenziali minacce, utilizzando sistemi di rilevamento delle intrusioni e processi di monitoraggio degli eventi di sicurezza.
- **Scope:** Monitoraggio in tempo reale delle reti e dei sistemi informatici per identificare tempestivamente potenziali attacchi o anomalie legate alla sicurezza, utilizzando IDS e altre tecnologie di monitoraggio.
- **Measure:** Percentuale di eventi di sicurezza monitorati e rilevati tramite sistemi di rilevamento delle intrusioni (IDS) e processi di monitoraggio continuo degli eventi di sicurezza.

- **Type:** Misura di performance, che verifica l'efficacia e l'efficienza del monitoraggio continuo degli eventi di sicurezza sulla rete.
- **Formula:**
    - Percentuale di eventi rilevati correttamente = (Numero di eventi di cybersecurity monitorati / Numero totale di eventi relativi alle infrastrutture ) × 100
    - Presenza di IDS - Intrusion Detection Systems: Si/No
- **Target:**
    - 100% dei sistemi di monitoraggio devono rilevare correttamente gli eventi di cybersecurity sulla rete.
    - I processi di monitoraggio devono essere in grado di rilevare eventi legati alla sicurezza delle applicazioni e dell'infrastruttura sottostante.
- **Implementation Evidence:**
    - Configurazioni e log dei sistemi di rilevamento delle intrusioni (IDS).
    - Report di analisi degli eventi di sicurezza monitorati, che mostrano la rilevazione e la risposta agli incidenti di cybersecurity.
    - Documentazione delle politiche e delle procedure di monitoraggio della rete e delle applicazioni.

- **Unique ID:** INF-DE02
- **Goal:** Garantire che l'organizzazione implementi e utilizzi strumenti efficaci per la prevenzione e il rilevamento di malware, compresi sistemi di protezione per le postazioni terminali (Endpoint Protection System - EPS). Inoltre, le politiche di protezione anti-malware devono essere definite e riviste periodicamente per garantire la loro efficacia.
- **Scope:** Monitoraggio delle risorse IT per identificare e neutralizzare il codice malevolo, attraverso l'uso di software di protezione endpoint e strumenti anti-malware, assicurando la protezione continua contro minacce esterne.
- **Measure:**
    - Percentuale di postazioni protette da soluzioni anti-malware attive e aggiornate.
    - Percentuale di rilevamento di malware su base periodica.
    - Frequenza di revisione delle politiche anti-malware.
- **Type:** Misura di performance che verifica l'efficacia dei sistemi di protezione anti-malware e la loro implementazione attraverso le postazioni terminali.
- **Formula:**
    - Percentuale di postazioni protette da anti-malware = (Numero di postazioni protette / Numero totale di postazioni) × 100

    - Percentuale di malware rilevato = (Numero di malware rilevati / Numero totale di eventi di malware monitorati) × 100

- **Target:**
    - 100% delle postazioni terminali devono essere protette da Endpoint Protection Systems (EPS).
    - Politiche di protezione anti-malware devono essere riviste almeno annualmente.
    - Il tasso di rilevamento di malware deve essere elevato, con una percentuale di rilevamento che si avvicina al 100%.
- **Implementation Evidence:**
    - Log e report generati dagli strumenti di protezione (EPS).
    - Documentazione delle politiche anti-malware aggiornate.
    - Certificazioni e rapporti sui test di malware effettuati.

**Tabella Riepilogo Metriche e KPI – Pilastro Infrastrutture**

| ID | Ambito | Obiettivo | Tipo di misura | Formula principale | Target | Note |
|---|---|---|---|---|---|---|
| **INF-A01** | Disponibilità | Garantire continuità e qualità dei servizi ICT | Efficacia | (1 - downtime / tempo totale) × 100 | ≥99,98% (senza fermi), ≥99,6% (con fermi) | |
| **INF-DC01** | Sicurezza Data Center (fisica) | Conformità ai requisiti infrastrutturali e antincendio | Implementazione | (Requisiti soddisfatti / Requisiti totali) × 100 | 100% dei 5 requisiti | *5 Requisiti dettagliati nel documento integrale* |
| **INF-DC02** | Sicurezza Data Center (ambientale) | Protezione fisica e ambientale | Implementazione | (Misure implementate / Totale previste) × 100 | 100,00% | *Misure fisiche e ambientali dettagliate nel documento integrale* |
| **INF-AM01** | Asset Management (fisico) | Tracciabilità e gestione dispositivi fisici | Implementazione + Efficacia | (Dispositivi censiti / Totale rilevati) × 100 | 100,00% | |
| **INF-AM02** | Gestione flussi dati | Tracciabilità e approvazione dei flussi informativi | Implementazione + Efficacia | (Flussi censiti / Totale rilevati) × 100 | 100,00% | |
| **INF-RA01** | Analisi del rischio | Testing periodico delle vulnerabilità delle risorse | Implementazione + Efficacia | (Risorse testate / Risorse totali) × 100 | 100% annualmente | |
| **INF-AC01** | Identità digitali | Gestione sicura delle credenziali di accesso | Implementazione + Efficacia | (Credenziali conformi / Totale credenziali) × 100 | 100% conformità ai 6 requisiti | *6 requisiti dettagliati nel documento integrale* |
| **INF-AC02** | Accesso fisico | Protezione e amministrazione dell'accesso fisico | Implementazione + Efficacia | (Risorse protette / Totale risorse critiche) × 100 | 100,00% | *Requisiti di protezione dettagliati nel documento integrale* |
| **INF-AC03** | Accesso remoto | Sicurezza degli accessi remoti alle risorse | Implementazione + Efficacia | (Accessi sicuri / Totale accessi remoti) × 100 | 100,00% | *Requisiti di sicurezza dettagliati nel documento integrale* |
| **INF-AC04** | Privilegi minimi e separazione ruoli | Accesso coerente a dati e sistemi | Implementazione + Efficacia | (Utenti e risorse gestiti secondo policy / Totale | 100,00% | *Policy elencate nel documento integrale* |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | secondo privilegi minimi | | utenti e risorse) × 100 | | |
| **INF-BA01** | Backup | Sicurezza e verifica dei backup | Conformità | (Backup eseguiti e verificati / Totale backup pianificati) × 100 | 100%, test annuale | |
| **INF-MA01** | Manutenzione remota | Accessi remoti autorizzati e sicuri | Conformità | (Manutenzioni conformi / Totale manutenzioni remote) × 100 | 100% autorizzazioni preventive | *Requisiti di conformità elencati nel documento integrale* |
| **INF-MA02** | Sicurezza perimetrale | Configurazione e aggiornamento corretto dei sistemi di rete | Conformità | (Firewall e simili corretti / Totale sistemi perimetrali) × 100 | 100,00% | |
| **INF-DE01** | IDS e monitoraggio | Rilevamento eventi di sicurezza attraverso IDS | Performance | (Eventi rilevati / Totale eventi infrastruttura) × 100 | 100,00% | |
| **INF-DE02** | Protezione anti-malware | Protezione endpoint e revisione policy | Performance | (Postazioni protette / Totale postazioni) × 100 e/o (Malware rilevati / Eventi malware) × 100 | 100% protezione postazioni, policy rivista annualmente | |

# Appendice C

# Metriche del pilastro Compliance tecnico-normativa

In questa appendice è riportato il documento elaborato durante il progetto di tesi, relativo alla fase di definizione delle metriche del pilastro *Compliance* tecnico-normativa. Il documento fornisce una descrizione dettagliata di ciascuna metrica, con la relativa definizione, struttura e modalità di calcolo, secondo l'organizzazione e i criteri illustrati nel corpo della tesi. Tale appendice consente di avere una visione completa e strutturata degli output generati durante la definizione delle metriche di sicurezza inerenti all'infrastruttura digitale.

**Metriche e KPI – Pilastro Compliance tecnico-normativa**

*Le metriche e i KPI sotto elencati sono basati sul Framewok Nazione per la Cybersecurity e la Data Protection Edizione 2025 – v2.1.0, con una selezione di metriche sulla base dei requisiti per i Soggetti Importanti, come Regione Piemonte, definiti da ACN con la delibera n. 164179/2025 Allegato 1.*

**CTN-GV – GOVERN**

La strategia di gestione del rischio di cybersecurity dell'organizzazione, i suoi obiettivi e le relative policy sono stabilite, comunicate e monitorate.

**CTN-GV.OC - Contesto organizzativo**
Il contesto - missione, aspettative degli stakeholder, dipendenze e requisiti legali, normativi e contrattuali - che influisce sulle decisioni di gestione del rischio di cybersecurity dell'organizzazione è compreso.

- **Unique ID**: CTN-GV.OC01
- **Goal**: Verificare che gli obiettivi, le capacità e i servizi critici attesi dagli stakeholder siano chiaramente compresi e comunicati.
- **Scope**: Tutti i progetti digitali che coinvolgono stakeholder interni o esterni.
- **Measure**: Percentuale di progetti con documentazione esplicita degli obiettivi e dei servizi attesi dagli stakeholder.
- **Type**: Metrica di implementazione
- **Formula**:
  $\left(\frac{N_{prog\,DOC}}{N_{prog\,TOT}}\right)\times 100$

  Dove:

  - *N_prog_DOC* = Numero di progetti e servizi inerenti agli stakeholder documentati
  - *N_prog_TOT* = Numero di progetti inerenti agli stakeholder totale
- **Target**: ≥ 95%
- **Implementation Evidence**: Analisi dei documenti di progetto, verbali di incontri con stakeholder, repository documentali.

**CTN-GV.RM - Strategia di gestione del rischio**
Le priorità, i vincoli, le dichiarazioni sulla tolleranza e la propensione al rischio, e le assunzioni dell'organizzazione sono stabilite, comunicate e utilizzate per supportare le decisioni sul rischio operativo.

- **Unique ID**: CTN-GV.RM01
- **Goal**: Verificare l'integrazione tra gestione del rischio di cybersecurity e i processi di risk management dell'organizzazione.
- **Scope**: Tutti i processi di risk management formalizzati.
- **Measure**: Percentuale dei processi di risk management che includono considerazioni di cybersecurity.
- **Type**: Metrica di implementazione
- **Formula**:
  $\left(\frac{N_{proc\,CYBER}}{N_{proc\,TOT}}\right)\times 100$

  Dove:

  - *N_proc_CYBER* = Numero di processi formalizzati con considerazioni di cybersecurity
  - *N_proc_TOT* = Numero di processi formalizzati totale
- **Target**: ≥ 90%
- **Implementation Evidence**: Risk register, piani di mitigazione, politiche di gestione rischio aggiornate.

**CTN- GV.RR - Ruoli, responsabilità e correlati poteri**
Sono stabiliti e comunicati i ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo.

- **Unique ID**: CTN-GV.RR01
- **Goal**: Verificare che i ruoli e le responsabilità in materia di cybersecurity siano chiari e attuati.
- **Scope**: Tutte le unità organizzative coinvolte nella gestione ICT.
- **Measure**: Percentuale di unità con ruoli cybersecurity formalizzati.
- **Type**: Metrica di implementazione
- **Formula**:
  $\left(\frac{N_{unit\,CYBER}}{N_{unit\,TOT}}\right)\times 100$

  Dove:

  - *N_unit_CYBER* = Numero di unità organizzative con ruoli di cybersecurity formalizzati
  - *N_unit_TOT* = Numero di unità totali

- **Target**: 100%
- **Implementation Evidence**: Organigrammi, job description, policy di responsabilità.

- **Unique ID**: CTN-GV.RR02
- **Goal**: Misurare il grado di inclusione della cybersecurity nei processi HR.
- **Scope**: Tutte le fasi del ciclo di vita del personale (assunzione, formazione, valutazione).
- **Measure**: Presenza di requisiti o contenuti relativi alla cybersecurity nei processi HR.
- **Type**: Misura di implementazione
- **Formula**:

  $$\left(\frac{N_{HR\,CYBER}}{N_{HR\,TOT}}\right)\times 100$$

  Dove:

  - *N_HR_CYBER* = Numero di processi/pratiche del ciclo di vita del personale ( HR ) dove ci sono requisiti e/o contenuti relativi alla cybersecurity
  - *N_HR_TOT* = Numero di processi/pratiche del ciclo di vita del personale ( HR ) totale
- **Target**: Tutti i processi HR mappati devono includere riferimenti alla cybersecurity, 100%
- **Implementation Evidence**: Documenti HR, moduli di onboarding, programmi di formazione.

**CTN-GV.PO - Politica**
La politica di cybersecurity dell'organizzazione è stabilita, comunicata e applicata.

- **Unique ID**: CTN-GV.PO01
- **Goal**: Verificare l’allineamento della policy di cybersecurity con strategia, priorità e contesto.
- **Scope**: Tutta la documentazione policy in vigore.
- **Measure**: Stato di approvazione e comunicazione della policy.
- **Type**: Metrica di implementazione
- **Formula**:

  $$\left(\frac{N_{Req\,OK}}{N_{Req\,TOT}}\right)\times 100$$

Dove:

- *N_req_OK* = numero di requisiti sulle politiche ( policy ) di cybersecurity soddisfatti
- *N_req_TOT* = numero totale di requisiti sulle politiche ( policy ) di cybersecurity

Requisiti:

1. Le politiche ( policy ) di cybersecurity sono in linea con il contesto organizzativo aziendale
2. Le politiche ( policy ) di cybersecurity sono il linea con la strategia di cybersecurity e con le priorità aziendali
3. Le politiche ( policy ) di cybersecurity sono correttamente comunicate e applicate

- **Target**: Tutti i documenti policy attivi allineati ai requisiti elencati.
- **Implementation Evidence**: Policy firmate, atti formali, verbali di presentazione.

- **Unique ID**: CTN-GV.PO02
- **Goal**: Assicurare il mantenimento aggiornato della policy cybersecurity.
- **Scope**: Tutte le versioni della policy pubblicate.
- **Measure**: Età media (in mesi) della policy di sicurezza rispetto alla revisione prevista.
- **Type**: Metrica di qualità
- **Formula**:

$$\left( \frac{\sum Mesi\,da\,ultima\,REV_{i=1\ a\ n}}{n} \right)$$

Dove:

- *Mesi_da_ultima_REV* = Mesi tra l'ultima revisione della policy e il momento del calcolo della metrica
- *n* = Numero totale delle policy di cybersicurezza

- **Target**: ≤ 12 mesi
- **Implementation Evidence**: Cronologia delle versioni, sistema di gestione documentale.

**CTN-GV.SC - Gestione del rischio di cybersecurity della catena di approvvigionamento**
I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione.

- **Unique ID**: CTN-GV.SC01
- **Goal**: Assicurare che strategia, politiche e processi di gestione del rischio nella supply chain siano formalizzati e condivisi.
- **Scope**: Tutti gli stakeholder coinvolti nella supply chain IT/ICT.
- **Measure**: % di contratti/framework di fornitura che includono esplicitamente una strategia cybersecurity in linea con l'organizzazione il programma, la strategia, gli obiettivi, le politiche e i processi di gestione del rischio aziendali .
- **Type**: Metrica di implementazione
- **Formula**:

  $$\left(\frac{N_{Contr\ CYBER}}{N_{Contr\ TOT}}\right)\times 100$$

  Dove:

  - *N_Contr_CYBER* = Numero di contratti/framework di fornitura che includono esplicitamente una strategia cybersecurity in linea con l' organizzazione il programma, la strategia, gli obiettivi, le politiche e i processi di gestione del rischio aziendali. La strategia deve essere stabilita e accettata dagli stakeholder.
  - *N_Contr_TOT* = Numero di contratti/framework di fornitura totale
- **Target**: ≥ 90%
- **Implementation Evidence**: Contratti, documentazione strategica approvata, verbali.

- **Unique ID**: CTN-GV.SC02
- **Goal**: Verificare che i ruoli e le responsabilità in ambito cybersecurity siano condivisi con fornitori e partner.
- **Scope**: Tutti i contratti con fornitori e accordi con partner IT/ICT.
- **Measure**: % dei documenti che specificano ruoli e responsabilità cyber.
- **Type**: Metrica di implementazione
- **Formula**:

  $$\left(\frac{N_{Contr\ ruoli\ CYBER}}{N_{Contr\ TOT}}\right)\times 100$$

  Dove:

  - *N_Contr_ruoli_CYBER* = Numero di contratti/framework di fornitura che hanno dei documenti che specificano ruoli e responsabilità cyber dei fornitori
  - *N_Contr_TOT* = Numero di contratti/framework di fornitura totale
- **Target**: 100%
- **Implementation Evidence**: Contratti, MoU, SLA, RACI condivisi.

- **Unique ID**: CTN-GV.SC03
- **Goal**: Misurare il livello di classificazione dei fornitori in base alla criticità cybersecurity.
- **Scope**: Tutti i fornitori IT/ICT attivi.
- **Measure**: % di fornitori  IT/ICT classificati in categorie di rischio .
- **Type**: Metrica di qualità
- **Formula**:

  $$\left(\frac{N_{Forn\,CLASS}}{N_{Forn\,TOT}}\right)\times 100$$

  Dove:
  - *N_Forn_CLASS* = Numero di fornitori IT/ICT classificati in base alla criticità in temrini di cybersicurezza.
  - *N_Forn_TOT* = Numero di fornitori IT/ICT totale.
- **Target**: ≥ 95%
- **Implementation Evidence**: Matrice di rischio fornitori, registro vendor.

- **Unique ID**: CTN-GV.SC04
- **Goal**: Assicurare l'inclusione di requisiti di sicurezza nei contratti di fornitura.
- **Scope**: Tutti i contratti e accordi con terze parti IT/ICT.
- **Measure**: % contratti/accordi IT/ICT contenenti clausole cybersecurity.
- **Type**: Metrica di implementazione
- **Formula**:

  $$\left(\frac{N_{Contr\,CLAUS}}{N_{Contr\,TOT}}\right)\times 100$$

  Dove:

  - *N_Contr_CLAUS* = Numero di contratti o accordi IT/ICT contenenti clausole di cybersecurity.
  - *N_Contr_TOT* = Numero di contratti/accordi IT/ICT totale.
- **Target**: ≥ 90%
- **Implementation Evidence**: Contratti , checklist di revisione e controllo delle clausole.

- **Unique ID**: CTN-GV.SC05
- **Goal**: Monitorare e gestire attivamente i rischi derivanti da fornitori IT/ICT.
- **Scope**: Tutti i fornitori IT/ICT classificati come critici.
- **Measure**: % di fornitori critici con piano di gestione rischio attivo.
- **Type**: Metrica di efficacia
- **Formula**:

  $$\left(\frac{N_{Forn\,PIANO}}{N_{Forn\,TOT}}\right)\times 100$$

  Dove:
  - *N_Forn_PIANO* = Numero di fornitori IT/ICT classificati come critici con un piano di gestione del rischio informativo attivo.
  - *N_Forn_TOT* = Numero di fornitori IT/ICT totale.
- **Target**: 100%
- **Implementation Evidence**: Piani di mitigazione, report audit, documenti di classificazione rischio dei fornitori.

**CTN-ID – IDENTIFY**

I rischi attuali di cybersecurity dell'organizzazione sono compresi.

**CTN-ID.RA - Valutazione del rischio (Risk Assessment)**
È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.

- **Unique ID**: CTN-ID.RA01
- **Goal**: Garantire che l’analisi del rischio includa minacce, vulnerabilità, probabilità e impatti.
- **Scope**: Tutti i processi di risk assessment.
- **Measure**: % dei processi di valutazione del rischio che includono minacce, vulnerabilità, probabilità e impatti.

- **Type**: Metrica di completezza
- **Formula**:

  $$\left(\frac{N_{RA\ completi}}{N_{RA\ TOT}}\right)\times 100$$

  Dove:

  - *N_RA_completi* = Numero di processi di risk assesment che includono valutazioni su minacce, vulnerabilità, probabilità e impatti.
  - *N_RA_TOT* = Numero di processi di risk assessment totale.
- **Target**: ≥ 95%
- **Implementation Evidence**: Report di risk assessment.

- **Unique ID**: CTN-ID.RA02
- **Goal**: Misurare la qualità della risposta al rischio (prioritizzazione, pianificazione, comunicazione).
- **Scope**: Tutti i rischi classificati medio-alti.
- **Measure**: % dei rischi con risposta documentata e monitorata.
- **Type**: Metrica di efficacia
- **Formula**:

  $$\left(\frac{N_{rischi\ GEST}}{N_{rischi\ TOT}}\right)\times 100$$

  Dove:

  - *N_rischi_GEST* = Numero di rischi classificati come medio-alti, con risposte al rischio prioritizzate, pianificate, monitorate e comunicate, con documentazione.
  - *N_rischi_TOT* = Numero di rischi con classificazione medio-alta totale
- **Target**: ≥ 95%
- **Implementation Evidence**: Registro rischi, piani di risposta, tracciamento follow-up.

- **Unique ID**: CTN-ID.RA03
- **Goal**: Garantire la presenza di un processo per ricezione, analisi e risposta a disclosure di vulnerabilità.
- **Scope**: Tutti i sistemi e servizi ICT esposti.
- **Measure**: Presenza di processo di vulnerability disclosure attivo.
- **Type**: KPI binario
- **Formula**:

  Si/No
- **Target**: Sì (implementato)
- **Implementation Evidence**: Vulnerability Disclosure Policy (VDP), canali di contatto pubblico tracciati e definiti.

**CTN-ID.IM - Miglioramento**
I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity dell'organizzazione sono identificati in tutte le funzioni del framework.

- **Unique ID**: CTN-ID.IM01
- **Goal**: Verificare che i piani di risposta agli incidenti siano aggiornati e testati.
- **Scope**: Tutti i piani IR (Incident Response).
- **Measure**: % dei piani aggiornati e con test effettuato negli ultimi 12 mesi.
- **Type**: Metrica di qualità
- **Formula**:

  $$\left(\frac{N_{piani\,TEST}}{N_{piani\,TOT}}\right)\times 100$$

  Dove:

  - *N_piani_TEST* = Numero di piani di IR ( Incident Response ) aggiornati e testati negli ultimi 12 mesi.
  - *N_piani_TOT* = Numero totale di piani di IR ( Incident Response ).
- **Target**: 100 %
- **Implementation Evidence**: Report di test dei piani di IR, cronologia versioni, report audit.

**CTN-PR - PROTECT**
Sono adottate misure di protezione per gestire i rischi di cybersecurity dell'organizzazione.

**CTN-PR.AT - Consapevolezza e formazione**
Il personale dell'organizzazione è sensibilizzato e formato sulla cybersecurity in modo da poter svolgere i propri compiti inerenti alla cybersecurity.

- **Unique ID**: CTN-PR.AT01
- **Goal**: Garantire la formazione continua del personale su rischi e policy cybersecurity.
- **Scope**: Tutto il personale in forza all'azienda.
- **Measure**: % di personale formato su temi di sicurezza negli ultimi 12 mesi.
- **Type**: Metrica di conformità.
- **Formula**:

  $$\left(\frac{N_{persFORM}}{N_{persTOT}}\right)\times 100$$

  Dove:

  - *N_pers_FORM* = Numero del personale formato sui rischi e sulle policy di cybersecurity dell'azienda
  - *N_pers_TOT* = Numero totale del personale in forza all'azienda.
- **Target**: ≥ 90%
- **Implementation Evidence**: Registro formazione, report test di apprendimento.

**CTN.RS - RESPOND**
Sono intraprese azioni in risposta a un incidente di cybersecurity rilevato.

**CTN-RS.MA - Gestione degli incidenti**
Le risposte agli incidenti di cybersecurity rilevati sono gestite.

- **Unique ID**: CTN-RS.MA01
- **Goal**: Verificare l'esecuzione coordinata dei piani di risposta con terze parti.
- **Scope**: Tutti gli incidenti dichiarati.
- **Measure**: % incidenti con coinvolgimento delle terze parti gestiti secondo il Piano.
- **Type**: Metrica di esecuzione.
- **Formula**:

$$\left(\frac{N_{inc\,COORD}}{N_{inc\,TOT}}\right)\times 100$$

Dove:

- *N_inc_COORD* = Numero di incidenti svolti con corretto coordinamento con terze parti coinvolte, secondo Piano di risposta agli incidenti.
- *N_inc_TOT* = Numero totale di incidenti rilevati.

- **Target**: 100%
- **Implementation Evidence**: Report IR, verbali di incident review.

**CTN-RS.CO - Segnalazione e comunicazione della risposta agli incidenti**
Le attività di risposta sono coordinate con gli stakeholder interni ed esterni come richiesto da leggi, regolamenti o politiche.

- **Unique ID**: CTN-RS.CO01
- **Goal**: Misurare la tempestività della comunicazione agli stakeholder.
- **Scope**: Tutti gli incidenti notificabili.
- **Measure**: % incidenti comunicati entro 24/48h
- **Type**: Metrica di tempestività
- **Formula**:

  $$\left(\frac{N_{not\,TEMP}}{N_{not\,TOT}}\right)\times 100$$

  Dove:

  - *N_not_TEMP* = Numero totale di incidenti notificati e comunicati entro 24/48h.
  - *N_not_TOT* = Numero totale di incidenti notificati
- **Target**: ≥ 95%
- **Implementation Evidence**: Report di comunicazioni ( per vario mezzo ), Registro ricevute PEC, cronologia ticket.

**CTN-RC - RECOVER**
Gli asset e le operazioni interessati da un incidente di cybersecurity sono ripristinati.

**CTN-RC.RP - Esecuzione del piano di ripristino dagli incidenti**
Le attività di ripristino sono eseguite per garantire la disponibilità operativa dei sistemi e dei servizi interessati da incidenti di cybersecurity.

- **Unique ID**: CTN-RC.RP01
- **Goal**: Misurare l'esecuzione effettiva dei piani di ripristino post-incidente.
- **Scope**: Tutti i sistemi IT colpiti da incidente.
- **Measure**: % di piani di recovery completati entro la finestra prevista.
- **Type**: Metrica di efficacia.
- **Formula**:

  $$\left(\frac{N_{ripr\,TEMP}}{N_{ripr\,TOT}}\right)\times 100$$

  Dove:

  - *N_ripr_TEMP* = Numero di ripristini eseguiti entro la finestra prevista/stabilita da Piano.
  - *N_ripr_TOT* = Numero totale ripristini effettuati a fronte di un incidente
- **Target**: 100%
- **Implementation Evidence**: Log recovery, cronologia ripristini, report post-incident

**Tabella Riepilogo Metriche e KPI – Pilastro Compliance Tecnico-Normativa**

| ID | Ambito | Obiettivo | Tipo di misura | Formula principale | Target | Note |
|---|---|---|---|---|---|---|
| **CTN-GV.OC01** | GOVERN - Contesto organizzativo | Verificare comprensione e comunicazione obiettivi/servizi attesi stakeholder | Implementazione | N_prog_DOC / N_prog_TOT * 100 | ≥ 95% | |
| **CTN-GV.RM01** | GOVERN - Strategia di gestione del rischio | Integrazione gestione rischio cyber nei processi di risk management | Implementazione | N_proc_CYBER / N_proc_TOT * 100 | ≥ 90% | |
| **CTN-GV.RR01** | GOVERN - Ruoli e responsabilità | Formalizzazione e applicazione ruoli e responsabilità cyber | Implementazione | N_unit_CYBER / N_unit_TOT * 100 | 100% | |
| **CTN-GV.RR02** | GOVERN - Cybersecurity in ambito HR | Integrazione della cybersecurity nei processi HR | Implementazione | N_HR_CYBER / N_HR_TOT * 100 | 100% | |
| **CTN-GV.PO01** | GOVERN - Policy cybersecurity | Allineamento policy con strategia, priorità, contesto | Implementazione | N_req_OK / N_req_TOT * 100 | 100% | *L'elenco dei requisiti è dettagliato nel documento integrale* |
| **CTN-GV.PO02** | GOVERN - Revisione policy | Mantenimento aggiornato policy di sicurezza | Qualità | media(Mesi_da_ultima_REV) | ≤ 12 mesi | |
| **CTN-GV.SC01** | GOVERN - Supply chain: strategia | Formalizzazione e strategia cyber nella supply chain | Implementazione | N_Contr_CYBER / N_Contr_TOT * 100 | ≥ 90% | |
| **CTN-GV.SC02** | GOVERN - Supply chain: ruoli e responsabilità | Ruoli e responsabilità cyber condivisi con i partner | Implementazione | N_Contr_ruoli_CYBER / N_Contr_TOT * 100 | 100% | |
| **CTN-GV.SC03** | GOVERN - Supply chain: classificazione fornitori | Classificazione rischio cyber dei fornitori | Qualità | N_Forn_CLASS / N_Forn_TOT * 100 | ≥ 95% | |
| **CTN-GV.SC04** | GOVERN - Supply chain: clausole | Integrazione clausole cybersecurity nei contratti | Implementazione | N_Contr_CLAUS / N_Contr_TOT * 100 | ≥ 90% | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | cyber | | | | | |
| **CTN-GV.SC05** | GOVERN - Supply chain: gestione rischio fornitori | Gestione attiva del rischio fornitori critici | Efficacia | N_Forn_PIANO / N_Forn_TOT * 100 | 100% | |
| **CTN-ID.RA01** | IDENTIFY - Risk Assessment: elementi | Inclusione minacce, vulnerabilità, probabilità, impatti | Completezza | N_RA_completi / N_RA_TOT * 100 | ≥ 95% | |
| **CTN-ID.RA02** | IDENTIFY - Risk Assessment: risposta | Documentazione e monitoraggio risposta ai rischi | Efficacia | N_rischi_GEST / N_rischi_TOT * 100 | ≥ 95% | |
| **CTN-ID.RA03** | IDENTIFY - Disclosure vulnerabilità | Esistenza processo di vulnerability disclosure | KPI binario | Sì/No | Sì | |
| **CTN-ID.IM01** | IDENTIFY - Miglioramento: IR Plan | Test e aggiornamento annuale piani IR | Qualità | N_piani_TEST / N_piani_TOT * 100 | 100% | |
| **CTN-PR.AT01** | PROTECT - Formazione personale | Formazione cybersecurity per tutto il personale | Conformità | N_pers_FORM / N_pers_TOT * 100 | ≥ 90% | |
| **CTN-RS.MA01** | RESPOND - Coordinamento con terze parti | Esecuzione piani IR con terze parti | Esecuzione | N_inc_COORD / N_inc_TOT * 100 | 100% | |
| **CTN-RS.CO01** | RESPOND - Comunicazione tempestiva | Comunicazione agli stakeholder entro 24/48h | Tempestività | N_not_TEMP / N_not_TOT * 100 | ≥ 95% | |
| **CTN-RC.RP01** | RECOVER - Ripristino post-incidenti | Esecuzione piani di recovery nei tempi previsti | Efficacia | N_ripr_TEMP / N_ripr_TOT * 100 | 100% | |

# Appendice D

# Prototipo Framework del Sistema di Rendicontazione

In questa appendice è riportato il documento elaborato durante il progetto di tesi, relativo alla fase di progettazione del sistema di rendicontazione. Il documento illustra le metriche previste per ognuna delle fasi facenti parte del sistema di rendicontazione del modello, indicando, per ogni fase, i razionali per il calcolo dell'indice di conformità alle metriche. Tale appendice consente di avere una visione completa e strutturata degli output generati durante la progettazione del sistema di rendicontazione.

Congruità Offerta

| Compliance Tecnico-Normativa | Target | Valore Attuale | Azioni di mitigazione |
|---|---|---|---|
| **CTN-GV.OC01** | ≥ 95% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.RM01** | ≥ 90% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.RR01** | 100% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.RR02** | 100% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.PO01** | 100% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.PO02** | ≤ 12 mesi | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.SC01** | ≥ 90% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.SC02** | 100% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.SC03** | ≥ 95% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.SC04** | ≥ 90% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.SC05** | 100% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-ID.RA01** | ≥ 95% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-ID.RA02** | ≥ 95% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-ID.RA03** | Sì | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-ID.IM01** | 100% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-PR.AT01** | ≥ 90% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-RS.MA01** | 100% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-RS.CO01** | ≥ 95% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-RC.RP01** | 100% | - | Obbligatorio nel caso il target non sia rispettato |

| Infrastrutture | Target | Valore Attuale | Azioni di mitigazione |
|---|---|---|---|
| **INF-A01** | ≥99,98% (senza fermi), ≥99,6% (con fermi) | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-DC01** | 100% dei 5 requisiti | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-DC02** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AM01** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AM02** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-RA01** | 100% annualmente | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AC01** | 100% conformità ai 6 requisiti | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AC02** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AC03** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AC04** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-BA01** | 100%, test annuale | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-MA01** | 100% autorizzazioni preventive | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-MA02** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-DE01** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-DE02** | 100% protezione postazioni, policy rivista annualmente | - | Obbligatorio nel caso il target non sia rispettato |

| | |
|---|---|
| **Indicatore di conformità alle metriche** | N° di metriche che raggiungono il Target/Numero di metriche della Fase di Rendicontazione * 100% |

Conformità Prodotti-Forniture

*Nota: Verifica da ripetere per ogni fornitura/prodotto del progetto*

| Codice | Target | Valore Attuale | Azioni di mitigazione |
|---|---|---|---|
| **COD-SR01** | ≥ 100% (Classe I) | - | Obbligatorio nel caso il target non sia rispettato |
| **COD-RR01** | ≥ 100% (Classe I) | - | Obbligatorio nel caso il target non sia rispettato |
| **COD-LSR01** | ≥ 100% (Classe I) | - | Obbligatorio nel caso il target non sia rispettato |
| **COD-LST01** | ≥ 100% (Classe I) | - | Obbligatorio nel caso il target non sia rispettato |
| **COD-COV01** | 100% (≥ 95% con giustificazioni documentate) | - | Obbligatorio nel caso il target non sia rispettato |
| **COD-COV02** | 100% (≥ 95% con giustificazioni documentate) | - | Obbligatorio nel caso il target non sia rispettato |

| | |
|---|---|
| **Indicatore di conformità alle metriche** | N° di metriche che raggiungono il Target/Numero di metriche della Fase di Rendicontazione del Prodotto * 100% |

Chiusura Progetto

| Infrastrutture | Target | Valore Attuale | Azioni di mitigazione |
|---|---|---|---|
| **INF-A01** | ≥99,98% (senza fermi), ≥99,6% (con fermi) | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-DC01** | 100% dei 5 requisiti | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-DC02** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AM01** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AM02** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-RA01** | 100% annualmente | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AC01** | 100% conformità ai 6 requisiti | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AC02** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AC03** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AC04** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-BA01** | 100%, test annuale | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-MA01** | 100% autorizzazioni preventive | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-MA02** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-DE01** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-DE02** | 100% protezione postazioni, policy rivista annualmente | - | Obbligatorio nel caso il target non sia rispettato |

| Codice | Target | Valore Attuale | Azioni di mitigazione |
|---|---|---|---|
| **COD-SR01** | ≥ 100% (Classe I) | - | Obbligatorio nel caso il target non sia rispettato |
| **COD-RR01** | ≥ 100% (Classe I) | - | Obbligatorio nel caso il target non sia rispettato |
| **COD-LSR01** | ≥ 100% (Classe I) | - | Obbligatorio nel caso il target non sia rispettato |
| **COD-LST01** | ≥ 100% (Classe I) | - | Obbligatorio nel caso il target non sia rispettato |
| **COD-COV01** | 100% (≥ 95% con giustificazioni documentate) | - | Obbligatorio nel caso il target non sia rispettato |
| **COD-COV02** | 100% (≥ 95% con giustificazioni documentate) | - | Obbligatorio nel caso il target non sia rispettato |

| | |
|---|---|
| **Indicatore di conformità alle metriche** | N° di metriche che raggiungono il Target/Numero di metriche della Fase di Rendicontazione * 100% |

Monitoraggio Periodico

*Nota: Ripetere con intervallo minimo di 6 mesi. 3 mesi in casi di KPI critici e di particolare Eventi che richiedono una misurazione aggiornata delle metriche.*

| Compliance Tecnico-Normativa | Target | Valore Attuale | Azioni di mitigazione |
|---|---|---|---|
| **CTN-GV.OC01** | ≥ 95% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.RM01** | ≥ 90% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.RR01** | 100% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.RR02** | 100% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.PO01** | 100% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.PO02** | ≤ 12 mesi | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.SC01** | ≥ 90% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.SC02** | 100% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.SC03** | ≥ 95% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.SC04** | ≥ 90% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-GV.SC05** | 100% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-ID.RA01** | ≥ 95% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-ID.RA02** | ≥ 95% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-ID.RA03** | Sì | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-ID.IM01** | 100% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-PR.AT01** | ≥ 90% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-RS.MA01** | 100% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-RS.CO01** | ≥ 95% | - | Obbligatorio nel caso il target non sia rispettato |
| **CTN-RC.RP01** | 100% | - | Obbligatorio nel caso il target non sia rispettato |

| Infrastrutture | Target | Valore Attuale | Azioni di mitigazione |
|---|---|---|---|
| **INF-A01** | ≥99,98% (senza fermi), ≥99,6% (con fermi) | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-DC01** | 100% dei 5 requisiti | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-DC02** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AM01** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AM02** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-RA01** | 100% annualmente | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AC01** | 100% conformità ai 6 requisiti | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AC02** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AC03** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-AC04** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-BA01** | 100%, test annuale | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-MA01** | 100% autorizzazioni preventive | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-MA02** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-DE01** | 100,00% | - | Obbligatorio nel caso il target non sia rispettato |
| **INF-DE02** | 100% protezione postazioni, policy rivista annualmente | - | Obbligatorio nel caso il target non sia rispettato |

| Codice | Target | Valore Attuale | Azioni di mitigazione |
|---|---|---|---|
| **COD-SR01** | ≥ 100% (Classe I) | - | Obbligatorio nel caso il target non sia rispettato |
| **COD-RR01** | ≥ 100% (Classe I) | - | Obbligatorio nel caso il target non sia rispettato |
| **COD-LSR01** | ≥ 100% (Classe I) | - | Obbligatorio nel caso il target non sia rispettato |
| **COD-LST01** | ≥ 100% (Classe I) | - | Obbligatorio nel caso il target non sia rispettato |

Monitoraggio Periodico

| | | | |
|---|---|---|---|
| **COD-COV01** | 100% (≥ 95% con giustificazioni documentate) | - | Obbligatorio nel caso il target non sia rispettato |
| **COD-COV02** | 100% (≥ 95% con giustificazioni documentate) | - | Obbligatorio nel caso il target non sia rispettato |

| | |
|---|---|
| **Indicatore di conformità alle metriche** | N° di metriche che raggiungono il Target/Numero di metriche della Fase di Rendicontazione * 100% |

# Appendice E

# Scheda di Validazione

In questa appendice è riportato il documento elaborato durante il progetto di tesi e utilizzato come strumento per la validazione del modello operativo. Il documento illustra la struttura delle informazioni raccolte per la caratterizzazione degli applicativi valutati e per l'analisi delle proprietà del modello. Tale appendice consente di avere una panoramica delle informazioni raccolte volte alla validazione e all'analisi dei dati.

Dati Identificativi Software

| | |
|---|---|
| **Nome Prodotto Software** | |
| **Direzione Titolare** | |
| **Fornitore** | |
| **RUP** | |
| **Referente ICT Riferimento** | |

Descrizione Software

| | |
|---|---|
| **Funzionalità principali** | |
| **Utenti target** | |
| **Ambiente Tecnologico** | |
| **Interfacce e integrazioni principali** | |
| **Contesto progettuale / Fase attuale** | |
| **Valutazione Sicurezza Preliminare** | |

Rendicontazione Metriche

*Nota*
*Inserire tabelle checklist in base alla fase progettuale in cui si applica il modello seguendo la struttura del file* ***Prototipo Framework Sistema Rendicontazione***

***INSERIRE TABELLA***

Valutazioni Finali

| **Valutazione Software** |
|---|

| | |
|---|---|
| **Valutazione Cumulativa Sicurezza del Software sulla base dei risultati del modello** | |
| **Note e Osservazioni Finali** | |

| **Valutazione Modello** |
|---|

| **Proprietà** | **Score (0-5)** | **Osservazioni e suggerimenti operativi** | **Evidenze Raccolte** |
|---|---|---|---|
| Affidabilità | | | |
| Applicabilità | | | |
| Esaustività | | | |
| Scalabilità | | | |

| **Legenda Score** | **Descrizione** |
|---|---|
| 0 | La proprietà non è in alcun modo soddisfatta |
| 1 | La proprietà è in minima parte soddisfatta; gravi carenze |
| 2 | La proprietà è parzialmente soddisfatta, ma con evidenti limiti |
| 3 | La proprietà è mediamente soddisfatta, ma richiede miglioramenti |
| 4 | La proprietà è quasi completamente soddisfatta, con marginali criticità |
| 5 | La proprietà è pienamente soddisfatta; situazione ideale |