Politecnico di Torino

Politecnico di Torino

Corso di Laurea
a.a. 2022/2023
Sessione di Laurea dicembre 2023

Valutazione di un caso di riuso di soluzione software nella Pubblica Amministrazione e suo rilascio in modalità open source

Relatori:
Prof. Vetrò Antonio
Prof. Torchiano Marco

Candidato:
Braia Gerardo

Indice

1 Introduzione

Nel contesto dell'evoluzione tecnologica e della crescente importanza dell'open source nella Pubblica Amministrazione, la tesi si propone di esaminare in dettaglio un caso di riuso di soluzione software e il suo processo di rilascio in modalità open source attraverso la piattaforma di Developers Italia. L'obiettivo è valutare l'efficacia di questa strategia di riuso e condivisione di software nell'ambito governativo, esaminando i vantaggi, le sfide e le implicazioni pratiche di tale approccio. In particolare, verrà realizzata un'analisi qualitativa del software coinvolto, concentrandosi sulla valutazione delle sue caratteristiche tecniche da parte di strumenti di analisi statica del codice, come SonarCloud. L'obiettivo di questa analisi è comprendere a quali categorie di "warning" dare priorità, al fine di definire strategie di miglioramento. Confrontando il software oggetto di tesi con soluzioni simili già presenti nel catalogo di Developers Italia, è possibile stabilire quanto sia necessario ridurre il debito tecnico e quali aree richiedano un intervento immediato per migliorare la qualità del software.
La tesi si struttura in tre sezioni: la prima fornisce un'analisi dello stato dell'arte riguardo l'utilizzo di licenze aperte per il riuso di soluzioni software all'interno della Pubblica Amministrazione. La seconda sezione si focalizza sull'applicazione pratica delle procedure tecniche relative al rilascio in modalità open source di un software, includendo anche una valutazione degli interventi effettuati sul codice per ridurre il debito tecnico dell'applicativo. La terza sezione comprende un confronto tra il tempo di riparazione del debito tecnico stimato da strumenti di analisi statica del codice e quello effettivo, al fine di valutare l'accuratezza delle predizioni fornite.

2 La trasformazione digitale

La trasformazione digitale è l'insieme di cambiamenti che si verificano in tutti gli aspetti della società umana, principalmente in termini di tecnologia, cultura, organizzazione, creatività e gestione che sono legati principalmente alla tecnologia digitale. La trasformazione digitale, agendo in modo organico e combinato su questi aspetti, va oltre la semplice adozione di nuove tecnologie e consente di trovare, elaborare e rendere accessibili grandi quantità di contenuti indipendentemente dalla reale disponibilità di risorse (umane, materiali, intellettuali, economiche, ecc.), creando nuove connessioni tra persone, luoghi e cose. Le tecnologie digitali nei sistemi organizzativi pubblici e privati possono aumentare l'efficienza generale, migliorare le interazioni con i cittadini, promuovere l'innovazione, migliorare il processo decisionale e aumentare gli standard di servizio. Questo processo è consentito dallo sviluppo di nuove tecnologie, ma non si limita alla loro adozione: promuove la trasparenza, la condivisione e l'inclusione di tutti i partecipanti, integrando e coinvolgendo l'intero ecosistema coinvolto. Grazie a questo nuovo approccio il destinatario finale del valore creato dalla trasformazione digitale è di fatto al centro dello sviluppo o addirittura partecipe dello stesso, accedendo così in maniera efficace e consapevole al servizio stesso indipendentemente dal fatto che si tratti di beni materiali, immateriali o dati. Le organizzazioni pubbliche, a differenza del settore privato, hanno regolamenti rigidi, gerarchie e strutture burocratiche, mentre le leadership sono spesso impreparate a comprendere e assimilare le nuove tecnologie, lasciando a dipartimenti più piccoli senza personale e risorse finanziarie la responsabilità di guidare l'innovazione. Un'altra considerazione interessante deriva dall'obiettivo principale delle strategie digitali implementate. L'avanzamento nel processo di digitalizzazione è meno probabile per le organizzazioni che utilizzano strategie orientate ai costi e che si concentrano quindi sulla riduzione dei costi di fornitura dei servizi. Al contrario, le organizzazioni che si basano sulla soddisfazione dei propri clienti e dei propri utenti registrano vantaggi duraturi. La trasformazione digitale nel settore pubblico italiano sembra aver trovato l'opportunità di crescere durante la pandemia di COVID-19. Il Dipartimento per l'Innovazione ha organizzato un forum di discussione su diffusione e attuazione del Piano Triennale al quale cittadini sono stati invitati a partecipare attivamente per aiutare a realizzare il Piano 2020-2022. Questo processo di consultazione aperta è quasi unico nella storia della politica italiana e ha consentito ai giornalisti, ai cittadini interessati, ai membri del settore privato di partecipare direttamente alla creazione della prima bozza del Piano, permettendo loro di fornire suggerimenti al documento originale e aprendo la discussione sulle priorità che la politica doveva affrontare. Per decenni, il settore privato ha spinto l'"agenda digitale" in Italia, ma l'instabilità politica del paese, con un tempo medio di esecuzione di 500 giorni, ha impedito lo spostamento delle politiche. Nel corso degli ultimi due decenni, un numero crescente di agenzie governative che si occupano dell'agenda dell'innovazione digitale della nazione ha seguito i cambiamenti nell'esecutivo, il che ha

certamente rallentato l'avanzamento tecnologico della nazione: a volte portando a responsabilità sovrapposte per più agenzie, altre volte lasciando anni in cui nessuna agenzia ha avuto potere delegato sulla questione. Il “Piano di innovazione digitale 2022-2024” più recente si concentra sulla definizione del lavoro agile e sull'implementazione del concetto di “digital first” nella pubblica amministrazione. La transizione digitale in Italia è stata significativamente accelerata nell'ultimo anno grazie alle enormi risorse stanziate dal Pnrr e agli sforzi profusi per realizzare interventi profondi che agiscano su molti componenti essenziali del nostro sistema economico, come la connettività per cittadini, imprese e pubbliche amministrazioni, una PA moderna e alleata dei cittadini e del sistema produttivo e la digitalizzazione del sistema sanitario. Sono stati avviati programmi ambiziosi che potrebbero rivitalizzare la competitività e l'immagine internazionale della nostra nazione, con l'obiettivo di assegnare all'Italia un ruolo di leadership nella strategia europea per il decennio digitale.
Il piano nazionale per la transizione digitale si fonda su cinque pilastri:

- connettività ultraveloce
- digitalizzazione della Pubblica Amministrazione
- digitalizzazione delle imprese
- digitalizzazione del sistema sanitario
- innalzamento sostanziale delle competenze digitali della popolazione.

Connettività ultraveloce

Il rapporto DESI 2022 (Digital Economy and Society Index) afferma che, sebbene l'Italia sia passata dal 23° al 7° posto in un anno nella classifica della connettività, i suoi risultati sono inferiori alla media dell'UE, in particolare per quanto riguarda l'adozione complessiva della banda larga fissa (66% in Italia contro il 78% nell'UE). Inoltre, rispetto all'obiettivo del decennio digitale di una copertura universale entro il 2030, persistono carenze nella copertura del territorio con connessioni a banda ultra larga, in particolare FTTH (Fiber to the Home), che è molto al di sotto della media europea. La copertura delle reti ad altissima capacità è anche molto inferiore alla media Ue, con un 44% contro il 70%. La diffusione del 5G, invece, è cresciuta significativamente, passando dall’ 8% al 99,7% delle aree popolate. Sono stati stanziati 6,7 miliardi da fondi pubblici e 2,2 miliardi di investimenti privati e ciò consentirà a tutti, dalle scuole agli ospedali, ai privati cittadini come agli uffici dell'amministrazione pubblica, di accedere an Internet ad alta velocità.

Digitalizzazione della Pubblica Amministrazione

La rapida trasformazione digitale della Pubblica Amministrazione è il tema del secondo punto. A gennaio 2021 erano state assegnate 16 milioni di identità Spid, ma i dati più recenti del 24 luglio 2022 mostrano che le identità digitali sono quasi raddoppiate da allora. Nello stesso periodo, anche il numero di cittadini iscritti all'Anagrafe Nazionale della Popolazione Residente (ANPR) è aumentato significativamente, passando da 55,9 milioni a 61,8 milioni. Il numero di transazioni che sono state effettuate attraverso PagoPA, il portale dei pagamenti verso la Pubblica Amministrazione, è più che triplicato in appena 14 mesi. È passato da circa 185 milioni di euro nel gennaio 2021 a circa 559 milioni di euro nel luglio 2022. L'app Io è stata un grade successo, ottenendo più di 30 milioni di download. Essa permette di gestire i servizi pubblici locali e nazionali digitalmente, direttamente dal proprio smartphone, racchiudendo in un unico posto tutti i documenti del proprio domicilio digitale, insieme alle notifiche e alla possibilità di effettuare i pagamenti. Dal 2024 l'applicazione dovrebbe aggiornarsi, introducendo il Digital Wallet, che consente di caricare documenti riconosciuti in tutta Europa con un riconoscimento identico a quello dei documenti cartacei. Anche la patente di guida, la tessera elettorale digitale e tessera sanitaria dovranno essere immesse all'interno del wallet utilizzando un QR code simile al Green Pass.

Digitalizzazione Imprese

Secondo uno studio dell'Istat, la quota di piccole e medie imprese italiane che hanno raggiunto un livello base di digitalizzazione si attesta al 60,3% al 2021, a fronte della media dell'Unione Europea del 56%. Il tasso di digitalizzazione delle imprese in Italia è in linea con la media dei 27 Paesi dell'Unione Europea, se si considerano i livelli di digitalizzazione delle imprese in base al numero di lavoratori. Solo il 19% circa delle piccole e medie imprese ha ancora un livello basso o molto basso di adozione dell'ICT. Il 38% delle grandi imprese ha una bassa adozione delle tecnologie digitali, mentre il 62% ha una alta o molto alta digitalizzazione. L'obiettivo europeo di digitalizzazione da raggiungere entro il 2030 si attesta al 90%, e ciò significa che l'Italia e l'Unione nel suo complesso hanno ancora molto da fare per raggiungere il traguardo designato. L'impatto della dimensione delle imprese sull'adozione delle tecnologie ICT è un altro tema evidente. I servizi cloud, l'Internet of Things (IoT) e le applicazioni di intelligenza artificiale sono tra queste le più diffuse tra le aziende italiane. L'Italia sembra avere un buon posizionamento a livello europeo per quanto riguarda l'adozione di queste tecnologie, registrando livelli superiori alla media dei 27 Paesi dell'UE nell'implementazione di processi produttivi intelligenti basati sull' IoT e nell'acquisto di servizi Cloud. Solo il 24% delle grandi imprese italiane ha adottato strumenti di IA, rispetto al 28% europeo. Invece, le tecnologie cloud vengono adottate rapidamente: Nel 2021, il 60% delle PMI italiane (contro il 40% europeo) ha acquistato servizi Cloud, aumentando fino all'83% delle grandi imprese (contro il 72% europeo). Il 32% delle PMI italiane e il 59% delle grandi imprese nostrane hanno utilizzato devices interconnessi, più di 10 punti percentuali sopra la media europea del 48%.

Sanità Digitale

La sanità digitale è il quarto pilastro del piano, con l'obiettivo di fornire le stesse garanzie e stesso livello di efficienza di funzionamento in ogni parte della nazione. Pertanto, è necessario garantire un accesso facile a tutte le prestazioni specialistiche e ai dati sanitari. Il fascicolo sanitario elettronico (FSE) e le piattaforme di telemedicina sono i due obiettivi principali del piano sanitario digitale. Il FSE fornisce uno strumento per tracciare e consultare lo storico sanitario di ciascun cittadino, condividendolo con i professionisti per garantire un servizio sanitario più efficiente. Il FSE ha un orizzonte temporale che copre l'intera vita del paziente, includendo l'intera storia clinica generata da più strutture sanitarie, nonché tutti i documenti caricati online dall'utente o dall'assistito stesso. Il FSE è oggi presente in tutte le regioni italiane, ma ha livelli diversi di operatività, partecipazione e utilizzo. Lo scenario completo dei dati, accessibile sul sito istituzionale dell'AgiD e del Ministero della Salute, consente di valutare l'andamento e lo stato di diffusione sul territorio nazionale. I dati mostrano che la Lombardia e l'Emilia-Romagna sono le regioni in cui il FSE viene utilizzato più frequentemente da cittadini, medici e aziende sanitarie. Inoltre, la strategia nazionale del PNRR mira a promuovere e finanziare lo sviluppo di una piattaforma nazionale di telemedicina, che consentirà agli operatori sanitari di fornire un'assistenza migliore ai pazienti, anche a distanza, grazie a dati sicuri e accessibili.

Competenze Digitali

Nonostante l'aumento delle competenze di base negli ultimi anni, il rapporto DESI 2022 sottolinea una situazione cruciale, in particolare per quanto riguarda le competenze digitali avanzate e specialistiche: la percentuale di specialisti digitali nella forza lavoro italiana è inferiore alla media dell'UE ed è ostacolata dai tassi molto bassi di iscrizione e laurea in discipline scientifiche in generale, in particolare in quelle relative all'informatica. Per quanto riguarda l'uso della tecnologia, più della metà della popolazione italiana rimane sprovvista di capacità quantomeno basilari (solo il 46% della popolazione raggiunge competenze digitali di base) e, sebbene il divario con i principali Paesi stia diminuendo (nel 2019 la distanza dalla media Ue era di oltre il 16%, nel 2021 è di circa l'8%), l'Italia rimane comunque alla terzultima posizione della classifica complessiva relativa alle competenze. Per assicurare il processo di trasformazione digitale della nazione, è necessario agire sia sull'offerta che sulla domanda. Sono state prese varie misure per aiutare la popolazione ad acquisire competenze digitali, poiché l'incapacità della stessa di usufruire appieno dei servizi offerti potrebbe comportare gravi lacune nel processo di digitalizzazione dell'Italia. A tal fine, la Conferenza delle Regioni ha approvato il piano del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri sulla misura 1.7.2 del Pnrr che mira allo sviluppo della Rete dei servizi di facilitazione digitale. L'obiettivo è realizzare 3.000 punti di facilitazione in tutto il paese per migliorare le competenze e l'inclusione digitale di 2 milioni di persone. Al progetto è stato assegnato un finanziamento di 135 milioni, che sarà ripartito attraverso vari accordi con le regioni. Il rafforzamento e la digitalizzazione dell'offerta formativa e degli ambienti scolastici, secondo il Piano Scuola 4.0, rimangono le principali sfide per quanto riguarda le nuove generazioni.

2.1 Digitalizzazione nella pubblica amministrazione

La digitalizzazione nella pubblica amministrazione italiana è un processo in evoluzione che mira a migliorare l'efficienza, la trasparenza e l'accessibilità dei servizi pubblici e a semplificare le procedure amministrative per i cittadini e le aziende. Per raggiungere questo obiettivo, è necessario agire sull' "infrastruttura digitale", tramite la migrazione delle amministrazioni al cloud, l'accelerazione dell'interoperabilità tra gli enti pubblici, lo snellimento delle procedure secondo il principio "once only" (le pubbliche amministrazioni non devono chiedere informazioni a imprese e cittadini già fornite in precedenza) e il rafforzamento della cybersecurity. Contemporaneamente, i processi prioritari delle Amministrazioni Centrali vengono adeguati agli standard condivisi da tutti gli Stati Membri dell'UE, i servizi vengono ampliati e l'accessibilità viene migliorata. Questi interventi devono essere accompagnati da iniziative che supportano l'acquisizione e l'arricchimento delle competenze digitali per rendere tutto questo funzionale alla transizione digitale della nazione.

In particolare, sono previsti sette investimenti principali:

- Infrastrutture digitali (900 mln)
- Abilitazione e facilitazione migrazione al cloud (1 mld)
- Dati e interoperabilità (650 mln)
- Servizi digitali e cittadinanza digitale (2,01 mld)
- Cybersecurity (620 mln)
- Digitalizzazione delle grandi amministrazioni centrali (610 mln)
- Competenze digitali di base (200 mln)

Infrastrutture digitali

La trasformazione digitale della Pubblica Amministrazione (PA) si concentra sulla migrazione dei dati e degli applicativi informatici delle singole amministrazioni verso il cloud, secondo un approccio "cloud first", una modifica che porterà a servizi più sicuri e integrati. A partire da quelli meno efficienti e sicuri, il processo consentirà di razionalizzare e consolidare numerosi data center presenti sul territorio. Ad oggi, circa il 95% degli undicimila data center utilizzati dagli enti pubblici in Italia non soddisfa i requisiti minimi di sicurezza, affidabilità, capacità elaborativa ed efficienza. Ciò significa che le amministrazioni centrali dovrebbero scegliere tra questi due modelli: migrare sul Polo Strategico Nazionale (PSN), una nuova infrastruttura dedicata al cloud (completamente "privata" o "ibrida"), situata sul territorio nazionale e all'avanguardia in termini di prestazioni e sicurezza, oppure migrare sul cloud "pubblico" di uno degli operatori di mercato opportunamente certificati.

Abilitazione e facilitazione migrazione al cloud

È previsto un programma di supporto e incentivi per il trasferimento di basi dati e applicazioni, in particolare rivolto alle amministrazioni locali, per accompagnare la migrazione delle PA centrali e locali al cloud. Le amministrazioni potranno scegliere tra una lista di fornitori certificati basata su requisiti di sicurezza e protezione e standard di performance. Le amministrazioni che parteciperanno al programma di trasformazione riceveranno “pacchetti” completi di risorse tecniche e finanziarie per aiutarle. In una logica vera e propria di “migration as a service”, verranno fornite alle amministrazioni risorse specializzate nella gestione amministrativa, saranno aiutate nella fase di analisi tecnica e di definizione delle priorità, nella contrattazione del supporto tecnico esterno necessario all'attuazione e nell'attività complessiva di project management. Per l'esecuzione dell'attività di migrazione, le PA locali minori che non possono gestirla individualmente dovranno aggregarsi in raggruppamenti creati ad hoc. La transizione al cloud è anche utile per lo sviluppo di un ecosistema di startup e imprese che può integrare e migliorare l'offerta e la qualità dei software per la PA.

Dati e interoperabilità

Il divario digitale presente nella pubblica amministrazione italiana oggi si riflette in una diminuzione della produttività e spesso si traduce in un carico insostenibile per cittadini e imprese, che devono affrontare l'accesso a diverse amministrazioni come se fossero compartimenti stagni, senza alcuna interconnessione tra di loro. La trasformazione digitale della pubblica amministrazione mira a rivoluzionare l'architettura e le modalità di connessione tra le basi di dati delle varie amministrazioni. L'obiettivo è creare una rete di banche dati pubbliche che possano comunicare tra di loro, portando a un significativo risparmio economico per le amministrazioni e a un notevole risparmio di tempo per i cittadini. La creazione di un unico profilo digitale consente alle amministrazioni di accedere alle informazioni sui cittadini in modo rapido, semplice ed efficace. La piena interoperabilità dei dataset della pubblica amministrazione consentirà un ampio utilizzo dell'identità digitale e dell'indirizzo di residenza digitale, scelti liberamente dai cittadini. In particolare, l'investimento lavora su due fronti:

- Creare una Piattaforma Digitale Nazionale Dati (PDND), garantendo l'interoperabilità dei dati pubblici, consentendo agli enti di fornire servizi in modo sicuro, più veloce ed efficace ed evitando ai cittadini di fornire ripetutamente informazioni che la PA ha già acquisito.
- Facilitare l'attuazione dello “Sportello Digitale Unico”, un progetto europeo che mira a uniformare l'accesso ai servizi digitali in tutte le nazioni membri dell'UE.

Servizi digitali e cittadinanza digitale

La trasformazione dell'architettura digitale della PA, che passa dal cloud all'interoperabilità dei dati, è accompagnata da investimenti mirati a rendere la vita digitale dei cittadini più semplice attraverso il miglioramento dei servizi pubblici.
L'investimento si suddivide in sei punti:

- Migliorare l'esperienza dei servizi pubblici digitali definendo e sostenendo l'adozione di modelli affidabili e riutilizzabili per la creazione e l'erogazione di siti web.
- Migliorare l'accessibilità dei servizi pubblici digitali mediante la promozione di strumenti e strategie condivise, che comprendono test di usabilità, iniziative di comunicazione e diffusione, nonché la creazione di kit specializzati e altre iniziative.
- Velocizzare ed espandere l'adozione di pagoPA, piattaforma tramite la quale è possibile effettuare pagamenti verso le Pubbliche Amministrazioni, e dell'app IO come punto di contatto primario tra cittadini ed Enti per usufruire dei servizi pubblici digitali.
- Incoraggiare l'adozione dell'Anagrafe nazionale della popolazione residente (ANPR) e dell'identità digitale (Sistema Pubblico di Identità Digitale, SPID e Carta d'Identità Elettronica, CIE).
- Sviluppare e implementare la piattaforma di notifiche digitali degli atti pubblici, che consentirà alle PA di ridurre i costi e il tempo per cittadini ed enti notificando atti amministrativi a valore legale a persone fisiche e giuridiche.
- Promuovere nei comuni l'adozione di Mobility as a Service (MaaS) al fine di digitalizzare il trasporto locale e offrire ai cittadini un'esperienza integrata di mobilità che parte dalla pianificazione del viaggio ai pagamenti.

Cybersecurity

La digitalizzazione rende la società più vulnerabile alle minacce cyber su tutti i fronti, come frodi, ricatti informatici e attacchi terroristici. Italia digitale 2026 include misure significative per migliorare la sicurezza cibernetica, come la piena implementazione del "Perimetro di sicurezza nazionale cibernetica". Gli investimenti sono suddivisi in quattro principali aree di intervento. Per cominciare, sono rafforzati i presidi di front-line per gestire gli alert e gli eventi a rischio intercettati con la PA e le aziende di interesse nazionale. In secondo luogo, sono state sviluppate o consolidate le capacità tecniche di valutazione e audit continuo della sicurezza di apparati elettronici e applicazioni utilizzati per fornire servizi vitali a soggetti che svolgono funzioni essenziali. Si progettano investimenti nell'assunzione di nuovo personale nelle aree di pubblica sicurezza e nella polizia giudiziaria, incaricate di prevenire e investigare il crimine informatico diretto contro i cittadini. Inoltre, si investe nel personale dei dipartimenti responsabili della difesa della nazione dalle minacce cibernetiche. Infine, sono stati irrobustiti gli asset e le unità responsabili della sicurezza nazionale e della risposta alle minacce cyber.

Digitalizzazione delle grandi amministrazioni centrali

I processi utilizzati per fornire i servizi pubblici sono spesso inefficaci e non digitali. Gli sforzi per digitalizzare le grandi amministrazioni centrali sono, quindi, il primo passo verso la trasformazione digitale della Pubblica Amministrazione.
In particolare, sono coinvolte le seguenti amministrazioni:

- INPS (180 milioni): miglioramento dei sistemi e delle procedure interne e sviluppo dei punti di contatto digitali.
- Ministero della Giustizia (133,2 milioni): digitalizzazione degli archivi relativi ai procedimenti civili dei tribunali ordinari, delle corti d'appello e degli atti giudiziari di Cassazione, creazione di un Data Lake per l'estrazione e l'organizzazione degli orientamenti giurisprudenziali, analisi statistiche avanzate, anche sulla base di dati non strutturati contenuti nei documenti, con l'obiettivo di monitorare l'efficienza e l'efficacia del sistema giudiziario, ottimizzando la gestione dei tempi di istruttoria.
- INAIL (116 milioni): digitalizzazione di tutti i processi e dei servizi istituzionali, adottando un digital workplace: un ambiente di lavoro digitale, con un vasto ecosistema di tecnologie a disposizione dei dipendenti.
- Ministero dell'Interno (107 milioni): digitalizzazione dei processi interni e dei servizi al cittadino, creazione di applicazioni e sistemi gestionali interni e formazione del personale migliorandone le capacità digitali.
- Ministero della Difesa (42,5 milioni): consolidare l'infrastruttura digitale, aumentare la sicurezza delle informazioni e passare ad un paradigma open source per le applicazioni relative alla gestione del personale.
- Guardia di Finanza (25 milioni): utilizzare la data science per prevenire e combattere gli illeciti economici finanziari mediante l'implementazione di algoritmi di intelligenza artificiale e modelli di analisi predittiva e prescrittiva.
- Consiglio di Stato (7,5 milioni): potenziamento del sistema informativo della Giustizia Amministrativa mediante l'implementazione di un sistema di conservazione dei documenti giurisdizionali, la creazione di un Data Warehouse con nuove funzionalità di Business Intelligence che consentono l'analisi e la previsione di statistiche georeferenziate e predittive, l'implementazione di applicazioni di Intelligenza Artificiale per il miglioramento dell'efficienza dei processi di lavoro e l'aumento della sicurezza informatica.

Competenze digitali di base

L'Italia digitale 2026 prevede iniziative per supportare le competenze digitali dei cittadini, con l'obiettivo di assicurarsi che tutti abbiano le stesse opportunità e completare il percorso verso un Paese completamente digitale. L'obiettivo è garantire un sostegno consistente e diffuso al completamento del percorso di alfabetizzazione digitale. Il Piano

nazionale di ripresa e resilienza prevede una serie di misure che coprono tutti gli aspetti del percorso educativo.

L'investimento contempla due misure:

- sviluppare l'iniziativa “Servizio civile digitale”, con l'obiettivo di formare circa 9.700 volontari e coinvolgere un milione di cittadini in attività di facilitazione e educazione digitale.
- ampliare l'esperienza dei “Centri di facilitazione digitale”, che sono punti di accesso fisici, tipicamente situati in biblioteche, scuole e centri sociali, che forniscono ai cittadini formazione sulle competenze digitali sia di persona che online per supportare l'inclusione digitale.

2.2 Il Codice per l’amministrazione digitale

Il Codice dell'amministrazione digitale (CAD) è un testo unico che organizza e riunisce le regole per l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese. È stato istituito con il decreto legislativo 7 marzo 2005, n. 82, ed è stato successivamente modificato più volte nel corso degli anni per rispondere alle sfide sempre più complesse del mondo digitale. Il CAD si propone di promuovere l'efficienza, la trasparenza e la modernizzazione dell'amministrazione pubblica italiana, fungendo da pilastro per la trasformazione digitale del Paese.

Analisi contenuti più significativi Codice dell’amministrazione digitale

L'aggiunta di un vasto elenco di diritti per cittadini e imprese è forse la componente più importante del CAD. I principali diritti di cui dispone il cittadino in seguito all’entrata in vigore del CAD sono:

- diritto alla propria identità digitale
- diritto a comunicare e partecipare digitalmente
- diritto al proprio domicilio digitale
- diritto a servizi on-line semplici e integrati
- diritto alla alfabetizzazione informatica
- diritto a non esibire certificati alla PA
- diritto alla trasparenza amministrativa digitale
- diritto alla protezione dei propri dati digitali
- diritto all’accessibilità e usabilità

Organizzazione delle pubbliche amministrazioni

Secondo il CAD, le pubbliche amministrazioni devono utilizzare le tecnologie dell'informazione e della comunicazione per raggiungere obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione. Devono anche rispettare i principi di uguaglianza e non discriminazione e riconoscere i diritti dei cittadini e delle imprese in conformità agli obiettivi presenti nel Piano triennale per l’informatica nella pubblica amministrazione. Secondo il CAD, le PA devono tradurre il principio fondamentale del “digital first” creando un modello e definendo processi, metodologie e regole allo scopo di conservare dati, informazioni e documenti digitali rilevanti per l'ente pubblico, fondendo e coordinando in modo digitale i principi essenziali del diritto e dell’archivistica. In particolare, il CAD definisce e specifica che tutti i documenti amministrativi devono nascere informatici e che le PA devono gestire i documenti in un sistema di gestione documentale affidabile, come specificato nelle regole tecniche, che oggi sono basate sulle Linee Guida AgID.

Documento informatico

Nel Contesto dell'Articolo 20 del Codice dell'Amministrazione Digitale (CAD), troviamo una definizione chiara del documento informatico. Quest'ultimo è descritto come un “documento elettronico che contiene rappresentazioni digitali di atti, fatti o dati giuridicamente rilevanti”. Questa definizione è contrapposta a quella del documento analogico, che è definito come un documento non informatico. Secondo l'Articolo 20 del CAD, un documento informatico soddisfa il requisito della forma scritta e ottiene il valore probatorio, come stabilito dall'Articolo 2702 del Codice Civile (in altre parole, diventa equivalente a una scrittura privata), quando presenta una firma digitale, una firma elettronica qualificata o una firma elettronica avanzata. Inoltre, può soddisfare questi requisiti se è stato formato attraverso un processo che ha coinvolto l'identificazione informatica del suo autore e rispetta i criteri fissati dall'Agenzia per l'Italia Digitale (AgID), garantendo sicurezza, integrità e immodificabilità del documento e rendendo manifesta e inequivocabile la sua riconducibilità all'autore. Va notato che l'Articolo 20 del CAD conferisce validità giuridica anche a documenti informatici che, in generale, rispettano i criteri di sicurezza, integrità e immodificabilità e che presentano qualsiasi tipo di firma elettronica, anche una firma elettronica semplice, a condizione che la riconducibilità all'autore sia “manifesta e inequivocabile”. Queste disposizioni dell'Articolo 20 del CAD sono in linea con l'attuale concetto di documento informatico e con la definizione di documento elettronico stabilita dal Regolamento eIDAS (Regolamento (UE) n. 910/2014). In questo contesto, un documento informatico è un "contenuto" che può adattarsi a vari "contenitori" per essere creato, gestito e conservato. Può assumere molteplici formati e firme, nonché essere trasmesso attraverso diversi mezzi, ma deve comunque garantire la sicurezza, l'immodificabilità e l'integrità. In particolare, un documento non deve necessariamente consistere in un testo scritto, può essere costituito da qualsiasi flusso di dati in forma elettronica, a condizione che il suo contenuto sia archiviato in modo statico e preservato nella sua integrità nel corso del tempo.

Firme elettroniche e certificati

In passato, era necessario che i documenti fossero fisicamente firmati e sottoscritti. Tuttavia, grazie al Regolamento eIDAS (Reg. 910/2014/UE), che riguarda l'identificazione elettronica e i servizi fiduciari, si è verificata una significativa evoluzione. Ora, anziché “segnare” un documento, ci concentriamo su “consegnare” documenti in formato elettronico. Questo passaggio cruciale coinvolge partner fidati che, previa verifica di affidabilità da parte delle autorità competenti per i soggetti qualificati, partecipano alla creazione, gestione, firma, trasmissione e conservazione dei documenti informatici. In questa prospettiva, le firme elettroniche non agiscono più come una semplice apposizione sul documento per attribuirne l'imputabilità giuridica. Piuttosto, sono associate a un determinato contenuto giuridicamente rilevante, con un valore giuridico e probatorio variabile in base alla sicurezza e all'affidabilità del processo. In altre parole, le firme

elettroniche attribuiscono quel contenuto a un soggetto specifico nell'ambito dell'ordinamento giuridico.

Linee guida siti web pubblica amministrazione

Secondo il CAD, le pubbliche amministrazioni devono creare siti istituzionali su reti telematiche che rispettino i principi di accessibilità, usabilità, affidabilità, chiarezza di linguaggio, semplicità di consultazione, qualità, omogeneità ed interoperabilità. Le linee guida fissano le procedure per la costruzione e l'aggiornamento dei siti web delle amministrazioni. Pertanto, le linee guida di design AgID per i siti della pubblica amministrazione includono una serie di elementi condivisi, visivi ed estetici, nonché regole di struttura e usabilità, con l'obiettivo di rendere più semplice l'accesso ai servizi e la fruizione delle informazioni online. Hanno l'obiettivo di migliorare l'esperienza dei cittadini quando utilizzano il sito web di una pubblica amministrazione e migliorare il rapporto e la comunicazione tra cittadini e pubblica amministrazione. Di fatto, queste linee guida aiutano a realizzare alcuni dei diritti fondamentali della cittadinanza digitale elencati precedentemente.

2.3 Linee guida AgID

L'Agenzia per l'Italia digitale (AgID) è un'agenzia pubblica italiana fondata nel 2012. Sotto la direzione e la vigilanza del presidente del Consiglio dei ministri o del ministro da lui delegato, ha come obiettivo perseguire il massimo livello di innovazione tecnologica nell'organizzazione e nello sviluppo della pubblica amministrazione e nel servizio dei cittadini e delle imprese, nel rispetto dei principi di legalità, imparzialità e trasparenza e secondo criteri di efficienza, economicità ed efficacia. Essa incorpora ed eredita le competenze precedentemente assegnate alla DigitPA, all'Agenzia per la diffusione delle tecnologie per l'innovazione e al Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei ministri.
Le finalità dell'Agenzia per l'Italia digitale, secondo lo Statuto approvato a febbraio 2014, sono le seguenti:

- Garantire il coordinamento informatico delle amministrazioni statali, regionali e locali allo scopo di progettare e monitorare l'evoluzione strategica del sistema informativo della pubblica amministrazione, promuovendo l'adozione di infrastrutture e standard che riducano i costi sostenuti dalle singole amministrazioni e migliorino i servizi erogati.
- Accreditare i "Certification Authority", i soggetti certificatori digitali, a rilasciare certificati digitali, SPID, conservazione sostitutiva, marca temporale, ecc., svolgendo quindi la funzione di "registration authority".
- Perseguire l'ottimizzazione della spesa informatica delle pubbliche amministrazioni monitorando le spese e assistendo le amministrazioni pubbliche nazionali e locali nel raggiungimento degli obiettivi di standardizzazione e revisione dei processi interni e di ottimizzazione della spesa informatica complessiva.
- Eseguire le attività richieste per adempiere agli impegni internazionali presi dallo Stato nelle aree di sua competenza.
- Promuovere l'innovazione digitale nella nazione e contribuire alla creazione di nuove conoscenze e alla diffusione di nuove opportunità di sviluppo economico, culturale e sociale, collaborando con istituzioni e organismi europei, nazionali e regionali aventi finalità analoghe, anche attraverso la stipula di accordi strategici.
- La formulazione di direttive, normative e criteri.
- La promozione di programmi di alfabetizzazione informatica destinati alla cittadinanza

2.3.1 Linee guida di design

Le linee guida di design per i servizi web della PA sono un insieme di linee guida che descrivono come dovrebbero essere progettati i siti e i servizi della Pubblica Amministrazione. Il loro obiettivo è quello di stabilire e fornire linee guida per la progettazione e la costruzione di siti web e servizi digitali erogati dalle Pubbliche Amministrazioni, conformemente a quanto stabilito dall'articolo 53 del D. Lgs. 7 marzo 2005, n. 82 e s.m.i. recante il Codice dell'Amministrazione Digitale.

Le precedenti “Linee guida per i siti web delle pubbliche amministrazioni”, stabilite all'articolo 4 della Direttiva del Ministro per la Pubblica Amministrazione, avevano lo scopo di indicare alle PA:

- metodi e strumenti per l'ottimizzazione dei siti web pubblici obsoleti.
- strumenti per potenziare i siti web attivi.
- approcci per gestire e mantenere i contenuti web aggiornati.
- i contenuti minimi.

A tal fine, le linee guida sono state progettate per delineare gli elementi essenziali del processo di sviluppo progressivo di siti web e servizi online con l'obiettivo di fornire informazioni di qualità ai cittadini. La progettazione, la costruzione, la gestione e il monitoraggio dei servizi pubblici digitali richiedono un adeguamento delle metodologie e degli strumenti a causa dei cambiamenti nel contesto normativo e tecnologico a livello nazionale ed europeo.

Le presenti linee guida:

- Annullano e sostituiscono le “Linee guida per i siti web delle PA” contenute nell'articolo 4 della Direttiva del Ministro per la Pubblica Amministrazione e l'innovazione 26 novembre 2009, n. 8 e tutte le relative disposizioni.
- Sono emesse ai sensi dell'articolo 71 del CAD e della Determinazione AGID n. 160 del 17 maggio 2018, che contiene il “Regolamento per l'adozione di linee guida per l'attuazione del Codice dell'amministrazione digitale”.
- Forniscono un elenco di linee guida tecniche che dovrebbero essere eseguite in modo dettagliato utilizzando le linee guida, gli strumenti, i modelli e i kit disponibili su https://designers.italia.it.

Elenco dei requisiti:

- Accessibilità: rendere il contenuto, la struttura e il comportamento degli strumenti informatici accessibili a tutti, secondo i requisiti di legge.
- Affidabilità, trasparenza e sicurezza: progettare e creare servizi digitali che garantiscano la sicurezza e la trasparenza delle informazioni in conformità con le leggi unionali e nazionali in materia di protezione dei dati personali.
- Semplicità di consultazione ed esperienza d'uso: progettare, realizzare e mantenere siti web e servizi digitali utili e facili da usare utilizzando una metodologia di progettazione centrata sull'utente.
- Monitoraggio dei servizi: analizzare e migliorare l'esperienza di utilizzo dei siti web e dei servizi digitali attraverso la rilevazione quantitativa e qualitativa dei dati di fruizione
- Interfaccia utente: rendere disponibili interfacce utenti intuitive.
- Integrazione delle piattaforme abilitanti: prevedere un'esperienza d'uso comune nell'utilizzo delle varie procedure online.
- Licenze: dare la priorità all'utilizzo di una licenza aperta ai contenuti.
- Attuazione: garantire che le attività relative alla progettazione, allo sviluppo e alla manutenzione di siti Web e servizi digitali soddisfino le presenti linee guida.

2.3.2 Linee guida sull’interoperabilità

Il Piano Triennale per l'informatica della Pubblica Amministrazione include il nuovo Modello di Interoperabilità, che è essenziale per il corretto funzionamento dell'intero Sistema informativo della PA. Per mezzo di soluzioni tecnologiche che garantiscono l'interazione e lo scambio di informazioni senza vincoli di implementazione, evitando integrazioni ad hoc, il modello rende possibile la collaborazione tra pubbliche amministrazioni e tra queste e soggetti terzi, in particolare:

- Consente lo sviluppo di nuove applicazioni per gli utenti della PA.
- Garantisce che anche terzi possano accedere ai dati dell'amministrazione nel rispetto del diritto alla privacy.
- È sviluppato in conformità con i principi indicati nel nuovo European Interoperability Framework (EIF), approvato nella Comunicazione COM(2017) 134 della Commissione Europea del 23 marzo 2017.

Tutte le amministrazioni devono seguire gli standard tecnologici e utilizzare i pattern e i profili del nuovo Modello di interoperabilità. Ciò consentirà alle amministrazioni di creare e esporre Application Programming Interface (API) in conformità con gli standard consolidati esistenti anche all'interno dell'Unione europea. In particolare, le API costruite secondo il nuovo Modello di Interoperabilità garantiscono:

- la possibilità di monitorare le varie versioni delle API per consentire evoluzioni non distruttive (versioning)
- documentazione associata alla versione delle API (documentation)
- limitazioni sull'utilizzo derivanti dalle caratteristiche delle API e della classe di utilizzatori stesse (throttling)
- tracciabilità di tutte le richieste ricevute e del loro esito (logging e accounting)
- un livello di servizio adeguato in base al tipo di servizio fornito (SLA)
- configurazione delle risorse in maniera scalabile

Nello specifico:

- le “Linee guida sull’interoperabilità tecnica delle Pubbliche Amministrazioni” descrivono e aggiornano le tecnologie che consentono l'interoperabilità tra PA, cittadini e imprese, nonché i pattern di interoperabilità (interazione e sicurezza), i profili di interoperabilità e il modello di governance utilizzato dall'Agenzia per l'Italia Digitale
- le “Linee guida Tecnologie e standard per la sicurezza dell’interoperabilità tramite API dei sistemi informatici” descrivono come utilizzare le API per proteggere, mantenere l'integrità e la riservatezza dei dati scambiati mentre i sistemi informatici pubblici e privati interagiscono tra loro

- le “Linee Guida sull’infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l’interoperabilità dei sistemi informativi e delle basi di dati” definiscono i processi di approvazione, identificazione e autorizzazione gestiti dall'infrastruttura tecnologica per l'interoperabilità dei sistemi informativi e delle basi di dati (PDND). Inoltre, specificano le procedure attraverso le quali le parti coinvolte conducono le loro interazioni utilizzando l'Infrastruttura interoperabilità PDND e stabiliscono i metodi per raccogliere e conservare le informazioni relative agli accessi e alle transazioni effettuate tramite l'Infrastruttura stessa.
- le “Linee guida sul punto di accesso telematico ai servizi della Pubblica Amministrazione” delineano i principi adottati sia dal gestore che dai soggetti che mettono a disposizione uno o più servizi tramite il punto di accesso telematico per la creazione di servizi online attraverso questo punto. Queste linee guida comprendono l'architettura logica del punto di accesso telematico, le funzionalità offerte da questo punto per supportare la creazione dei servizi online, le integrazioni con le piattaforme previste dal CAD, i gestori di identità digitali e i prestatori di servizi fiduciari qualificati. Inoltre, le linee guida includono il modello di governance applicato dal gestore del punto di accesso telematico per soddisfare le richieste dei soggetti erogatori in merito alla creazione e messa in funzione dei servizi online tramite il punto di accesso telematico, così come le disposizioni sulla sicurezza e la protezione dei dati personali garantite dal gestore e dai soggetti erogatori durante la realizzazione e l'esecuzione dei servizi online tramite il punto di accesso telematico.

2.3.3 Misure minime di sicurezza ICT per le pubbliche amministrazioni

Le misure minime di sicurezza ICT emanate dall'AgID forniscono un riferimento pratico per valutare e migliorare la sicurezza informatica delle amministrazioni per combattere le minacce informatiche più comuni. Consistono in controlli organizzativi, tecnologici e procedurali che sono utili alle amministrazioni per valutare il loro livello di sicurezza informatica. Le misure minime sono suddivise in tre livelli di attuazione, a seconda della complessità del sistema informativo a cui si riferiscono e della situazione organizzativa dell'amministrazione:

- **Minimo:** livello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua dimensione o forma, deve essere o rendersi conforme.
- **Standard:** rappresenta la maggior parte delle realtà della PA italiana e costituisce il livello di sicurezza superiore al livello minimo che ogni amministrazione deve considerare come base di riferimento.
- **Avanzato:** questo approccio dovrebbe essere implementato principalmente da organizzazioni con una maggiore esposizione ai rischi, come quelle che gestiscono informazioni altamente critiche o forniscono servizi di grande rilevanza. Tuttavia, dovrebbe anche essere considerato come un obiettivo di miglioramento per tutte le altre organizzazioni.

Obiettivi delle misure minime

Le misure minime forniscono un importante supporto metodologico e sono anche un mezzo attraverso il quale le amministrazioni, in particolare quelle più piccole e con meno possibilità di avvalersi di professionisti specifici, possono verificare autonomamente la propria situazione e iniziare un percorso di monitoraggio e miglioramento.
Le misure minime:

- fanno da punto di riferimento operativo utilizzabile immediatamente
- definiscono una base comune di misure tecniche e organizzative essenziali
- forniscono uno strumento utile per verificare lo stato di protezione contro le minacce informatiche e identificare modi per migliorarla
- sottolineano la responsabilità delle amministrazioni nell'ottimizzazione e nella costante manutenzione del proprio livello di sicurezza cibernetica.

L'adeguamento alle misure minime è di competenza del responsabile dell'unità dedicata all'organizzazione, all'innovazione e alle tecnologie, come stabilito nel CAD (articolo 17) o, in mancanza di tale figura, del dirigente designato.

2.3.4 Il Regolamento generale sulla protezione dei dati (GDPR)

Il Regolamento Generale sulla Protezione dei Dati è un regolamento fondamentale che ha cambiato il modo in cui i dati personali vengono trattati e protetti in tutta l'UE. Entrato in vigore il 25 maggio 2018, il GDPR è stato progettato per adattare le normative alla crescente digitalizzazione delle informazioni personali e per rafforzare la privacy e la sicurezza dei dati per i cittadini europei. Questo regolamento ha introdotto una serie di nuovi standard e requisiti che impattano su aziende, fornitori di servizi e privati.

Obiettivi e Scopo del GDPR

Uno degli obiettivi principali del GDPR è stato quello di armonizzare le leggi sulla privacy dei paesi membri dell'UE e dare ai cittadini un maggiore controllo sui loro dati personali. Le leggi sulla protezione dei dati dell'UE non erano tutte uniformi prima dell'entrata in vigore del GDPR, il che poteva causare confusione e incertezza. Il GDPR ha cercato di risolvere questo problema creando standard comuni per la gestione dei dati personali, imponendo sanzioni per le violazioni. La protezione dei dati personali è un altro degli obiettivi chiave del GDPR. Tramite questo regolamento, sono stati introdotti requisiti rigorosi per garantire la sicurezza e la riservatezza dei dati personali a causa della crescente quantità di dati digitali in circolazione e delle minacce cibernetiche. Le organizzazioni sono tenute ad adottare le misure necessarie per proteggere i propri dati dai tentativi di accesso non autorizzato, divulgazione, perdita, danneggiamento.

Principali Principi del GDPR

Il GDPR si fonda su una serie di principi che orientano la gestione delle informazioni personali. Questi principi evidenziano la centralità della chiarezza, del potere decisionale individuale e della responsabilità delle organizzazioni che si occupano di dati personali. Tra i principali pilastri del GDPR troviamo:

- **Legittimità, Equità e Trasparenza:** i dati personali devono essere trattati in modo legale, equo e trasparente nei confronti delle parti interessate. Le organizzazioni devono chiarire come saranno utilizzati i dati.
- **Finalità Limitate:** i dati personali devono essere raccolti e trattati solo per scopi specifici, chiari e legittimi.
- **Minimizzazione dei Dati:** solo i dati personali necessari per raggiungere gli scopi dichiarati devono essere raccolti e trattati dalle organizzazioni. I dati non dovrebbero essere conservati più a lungo del necessario.
- **Esattezza dei Dati:** le informazioni personali devono essere precise e, quando richiesto, mantenute aggiornate. Le organizzazioni devono implementare procedure per rettificare o rimuovere dati errati o non più rilevanti.

- **Limitazione della Conservazione:** i dati devono essere conservati in modo che le persone interessate possano essere identificate solo per il tempo necessario agli scopi per i quali sono stati prelevati.
- **Integrità e Riservatezza:** è responsabilità delle organizzazioni assicurare la protezione e la riservatezza delle informazioni personali attraverso adeguate misure tecniche e organizzative.

Diritti delle Persone Interessate

Il GDPR potenzia i diritti dei cittadini dell'UE in merito ai loro dati personali. Alcuni dei principali diritti delle persone interessate secondo il GDPR includono:

- **Diritto all'Informazione:** le persone interessate devono essere informate in modo chiaro e trasparente su come verranno trattati i loro dati personali.
- **Diritto di Accesso:** le persone interessate hanno il diritto di accedere ai propri dati personali che vengono trattati da un'organizzazione.
- **Diritto di Rettifica:** le persone interessate possono richiedere la correzione di dati personali inesatti o incompleti.
- **Diritto alla Cancellazione (Diritto all'Oblio):** le persone interessate possono richiedere la cancellazione dei propri dati personali in determinate circostanze, ad esempio se i dati non sono più necessari per gli scopi per cui sono stati raccolti.
- **Diritto di Opposizione al Trattamento:** le persone interessate hanno il diritto di opporsi al trattamento dei propri dati personali in alcuni casi, come nel caso di marketing diretto.
- **Diritto alla Portabilità dei Dati:** le persone interessate hanno il diritto di ricevere i propri dati personali in un formato strutturato, comunemente usato e leggibile da dispositivo automatico, e di trasmettere tali dati a un'altra organizzazione.

Implicazioni per le Organizzazioni

Il GDPR ha avuto un impatto significativo sulle organizzazioni che trattano dati personali, inclusi enti governativi, aziende, organizzazioni non profit e fornitori di servizi online. Le implicazioni principali includono:

- **Consapevolezza e Formazione:** Le organizzazioni devono essere consapevoli dei requisiti del GDPR e formare il personale che tratta dati personali.
- **Consenso esplicito:** Le organizzazioni devono ottenere un consenso esplicito dalle persone interessate per trattare i loro dati personali, e tale consenso deve essere revocabile in qualsiasi momento.

- **Responsabile della Protezione dei Dati (DPO):** Alcune organizzazioni devono nominare un DPO, che è responsabile di sorvegliare il rispetto delle normative sulla protezione dei dati all'interno dell'organizzazione.
- **Valutazione dell'Impatto sulla Protezione dei Dati (DPIA):** Le organizzazioni devono condurre una DPIA per valutare e mitigare i rischi per la privacy quando il trattamento dei dati può comportare rischi elevati per i diritti e le libertà delle persone interessate.
- **Notifica di Violazioni dei Dati:** In caso di violazione dei dati personali, le organizzazioni devono notificare le autorità competenti e, in alcuni casi, le persone interessate entro 72 ore dalla scoperta della violazione.

Sanzioni e Conformità

Il GDPR ha introdotto sanzioni significative per le organizzazioni che non rispettano le norme sulla protezione dei dati. Le sanzioni possono variare in base alla gravità della violazione e possono raggiungere importi fino al 4% del fatturato annuo globale dell'organizzazione o 20 milioni di euro, a seconda di quale importo sia più elevato. Per evitare tali sanzioni, le organizzazioni devono assicurarsi di essere conformi al GDPR. Ciò include la revisione e l'aggiornamento delle politiche sulla protezione dei dati, l'adozione di misure di sicurezza adeguate e la collaborazione con le autorità di controllo della protezione dei dati.

2.3.5 Linee guida su acquisizione e riuso di software per le pubbliche amministrazioni

Le Linee guida sull'acquisizione e il riuso di software da parte delle pubbliche amministrazioni forniscono orientamenti alle amministrazioni nel processo decisionale riguardo all'acquisto di software, alla condivisione e al riuso delle soluzioni open source. Esse sostituiscono la precedente circolare AgID 63/2013 intitolata “Linee guida per la valutazione comparativa prevista dall'art. 68 del D.Lgs. 7 marzo 2005, n. 82 Codice dell'Amministrazione digitale” e relativi allegati, sono state adottate con la determinazione n. 115 del 9 maggio 2019 e sono state pubblicate nella Gazzetta Ufficiale, serie generale n. 119 del 23 maggio 2019.
Queste linee guida promuovono un cambiamento culturale, spingendo verso una maggiore adozione di software open source. Ciò significa che qualsiasi investimento fatto da un'Amministrazione Pubblica può essere condiviso con altre amministrazioni e la comunità nel suo complesso, semplificando così le decisioni di acquisto e gli investimenti nei servizi digitali. Le Linee Guida, adottate in conformità agli articoli 68 (Analisi comparativa delle soluzioni) e 69 (Riuso delle soluzioni e standard aperti) del Codice dell'amministrazione digitale, introducono significative innovazioni. In esse si stabilisce che le Pubbliche Amministrazioni dovrebbero sviluppare il codice sempre con licenza aperta ed effettuare una valutazione comparativa tecnico-economica durante l'acquisto di software, motivando le loro scelte e dando priorità alle soluzioni open source, incluse quelle offerte da altre amministrazioni. Inoltre, queste Linee Guida stabiliscono che le soluzioni rese riutilizzabili dalle Pubbliche Amministrazioni dovrebbero essere pubblicate con licenza open source in un repository pubblicamente accessibile e inserite nel catalogo Developers Italia. Per sostenere le amministrazioni in questi piani di approvvigionamento, vengono fornite guide tecniche in allegato, che possono essere incluse nei contratti o nei documenti di gare d'appalto:

- Guida alla pubblicazione open source di software realizzato per la PA.
- Guida alla manutenzione di software open source.
- Guida alla modifica di software open source preso in riuso o di terzi.

2.3.5.1 Valutazione comparativa del software

L'articolo 68 comma 1 del CAD elenca le categorie di soluzioni che sono oggetto di un'analisi comparativa tecnica ed economica tra i seguenti tipi di software:

- **Software sviluppato per conto della pubblica amministrazione:** la soluzione, nota anche come “opzione make”, implica che la Pubblica Amministrazione assegni al fornitore lo sviluppo del software, che sia una creazione completamente nuova o una modifica di un software preesistente. In questo contesto, il fornitore si impegna a fornire alla P.A. il software sviluppato in base ai requisiti stabiliti da quest'ultima. Ad esempio, nel ciclo di vita del software, che comprende le fasi di analisi, progettazione, sviluppo, collaudo, rilascio e manutenzione, la P.A. può assumersi la responsabilità delle fasi di analisi e progettazione, definendo i requisiti del software, e successivamente delegare lo sviluppo al fornitore.
- **Riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione:** la soluzione di “riuso” riguarda l'utilizzo di un software già esistente e disponibile all'interno della Pubblica Amministrazione, compreso anche l'impiego dei suoi componenti.
- **software libero o a codice sorgente aperto:** software open source, comprendente tutti i programmi informatici distribuiti in conformità con una licenza certificata dall'Open Source Initiative (OSI), come dettagliato nel documento sulle “Licenze per il software aperto”.
- **software fruibile in modalità cloud computing:** soluzione in cui la Pubblica Amministrazione acquisisce il software come un servizio, escludendo le opzioni di Hardware as a Service (HaaS) e Infrastructure as a Service (IaaS).
- **software di tipo proprietario mediante ricorso a licenza d’uso**: software con licenza d'uso di tipo proprietario da installare in loco (on premise).
- **software combinazione delle precedenti soluzioni:** software formato da componenti appartenenti a più di una delle categorie sopra menzionate. Ad esempio, software in cui una soluzione in riuso utilizza un middleware Open Source e ha accesso an un database proprietario, con componenti create appositamente per conto dell'amministrazione destinataria della soluzione. È la forma più adottata tra quelle utilizzate nelle pubbliche amministrazioni.

I criteri per la valutazione comparativa tra le soluzioni, come specificati nell'articolo 1-bis dell'articolo 68 del Codice dell'Amministrazione Digitale (CAD), includono:

- **Costo complessivo:** è da intendersi come il Total Cost of Ownership (TCO) della soluzione, che è calcolato su una finestra temporale appropriata per il contesto della valutazione e include il costo di migrazione verso altra soluzione.

- **Utilizzo di formati di dati aperti:** utilizzo di formati standard e aperti per la rappresentazione di dati, metadati e documenti da parte della soluzione da valutare al fine di garantire che i sistemi informatici delle pubbliche amministrazioni e/o dei gestori di pubblici servizi siano interoperabili tra loro.
- **Utilizzo di interfacce aperte:** l'utilizzo di interfacce aperte da parte della soluzione in fase di valutazione implica l'impiego di Application Programming Interfaces (API) e altre interfacce pubbliche che sono documentate e consentono l'implementazione e l'estensione libera. Questo è fatto con l'obiettivo di garantire la compatibilità e l'interoperabilità tra i sistemi informatici utilizzati dalle pubbliche amministrazioni e/o dai gestori di servizi pubblici.
- **Utilizzo di standard per l'interoperabilità:** valutazione dell'adeguatezza della soluzione per garantire l'interoperabilità dei sistemi informatici delle pubbliche amministrazioni e/o dei gestori di pubblici servizi.
- **Livelli di sicurezza:** è relativo alla presenza di garanzie adeguate riguardo ai livelli di sicurezza della soluzione, indipendentemente dalla natura giuridica del titolare del software e/o dell'erogatore del servizio in modalità cloud computing.
- **Conformità alla normativa in materia di protezione dei dati personali:** conformità dei processi e delle procedure alle leggi sulla protezione dei dati personali, senza considerare la natura giuridica del proprietario del software o del provider di servizi cloud computing.
- **Livelli di servizio del fornitore:** è la capacità del fornitore di fornire i servizi in conformità alle metriche precedentemente stabilite dalla pubblica amministrazione in un Service Level Agreement (SLA).

2.3.5.2 Fasi del processo decisionale

Dato che le soluzioni sono molto diverse e la realizzazione di confronti quantitativi uniformi può essere complessa, specialmente quando si confronta una soluzione con costi definiti (come una soluzione proprietaria in modalità on premise o in modalità cloud computing) con una soluzione da sviluppare da zero, per la quale è disponibile solo uno studio di fattibilità, si è scelto di delineare un processo decisionale attraverso la descrizione di Fasi e la loro organizzazione in Macro fasi. L'immagine successiva illustra le Macro fasi che caratterizzano il processo decisionale per condurre la valutazione comparativa come previsto dall'articolo 68 del CAD.

Figura 1 - Fasi del processo decisionale

Macro fase 1: Questa fase è finalizzata a definire le necessità specifiche dell'amministrazione, identificando i requisiti e i vincoli (sia organizzativi che finanziari) che influenzeranno le decisioni per individuare una soluzione adatta alle esigenze dell'ente pubblico.

Macro fase 2: In questa fase, l'amministrazione pubblica verifica la possibilità di soddisfare le proprie esigenze mediante l'utilizzo di soluzioni già adoperate da altre amministrazioni (denominate “soluzioni riutilizzate dalle PA”) o mediante l'impiego di software open source o con codice sorgente aperto (conosciuti come “soluzioni Open Source”).

Macro fase 3: Se la Macro Fase 2 non consente di soddisfare le esigenze dell'amministrazione pubblica, si procede a cercare una soluzione tramite software di tipo proprietario, utilizzando licenze d'uso esistenti o sviluppando nuove soluzioni da zero.

2.3.5.2.1 Macro fase 1: Individuazione delle esigenze

In questa Macro Fase, l'amministrazione pubblica delineerà le sue esigenze, compresi bisogni e vincoli, che saranno determinanti nella scelta di una soluzione. Si consiglia di preparare un documento descrittivo delle esigenze individuate, senza restrizioni particolari sulla forma, che sarà utilizzato nelle fasi successive per la comparazione e la valutazione delle soluzioni.

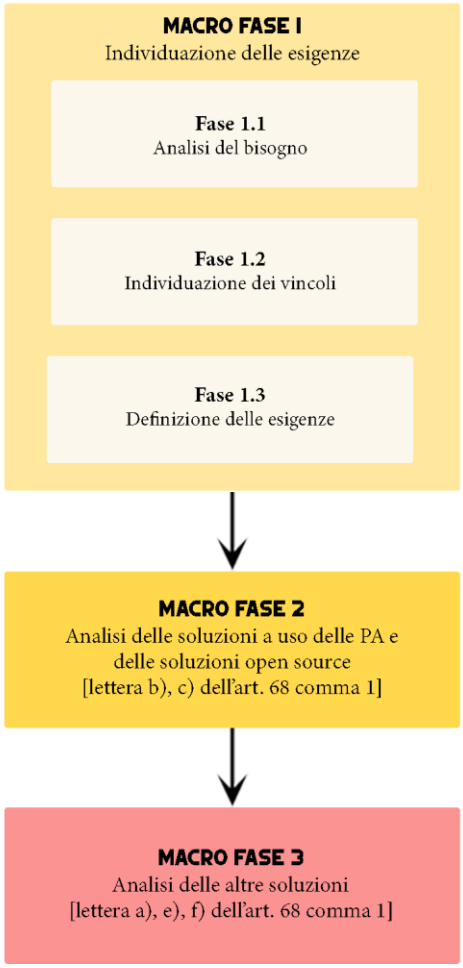

Figura 2 - Macro fase 1

Fase 1.1: Analisi del fabbisogno

L'amministrazione definisce le sue esigenze per individuare la soluzione software. In questo processo, tiene in considerazione quanto stabilito nel Programma degli acquisti e nella Programmazione dei lavori pubblici, come stabilito dall'articolo 21 del D.Lgs. n. 50 del 18/04/2016. Le attività pianificate in questa fase includono:

- Un'analisi del contesto che comprende la descrizione delle caratteristiche dell'amministrazione, tra cui le sue finalità, struttura e organizzazione.

- La documentazione dei flussi operativi che sono influenzati dal software da acquisire e che l'amministrazione utilizza per condurre le procedure amministrative.
- L'identificazione delle possibili ottimizzazioni dei flussi operativi in relazione al software da acquisire.
- La determinazione degli strumenti necessari per attuare i processi operativi individuati.
- La formulazione dei requisiti, inclusi i bisogni che il software deve soddisfare, con una distinzione tra requisiti essenziali e requisiti opzionali.

Questa fase si conclude con l'individuazione delle esigenze specifiche dell'amministrazione pubblica.

2.4.2 Fase 1.2: Individuazione dei vincoli

L'amministrazione espone i limiti che influenzano l'acquisizione della soluzione software. Le attività previste in questa fase includono:

- La determinazione della disponibilità di budget per garantire la disponibilità e l'implementazione della soluzione da acquisire, che potrebbe includere la pulizia dei dati, la migrazione da sistemi esistenti, l'installazione, la personalizzazione, l'integrazione con sistemi preesistenti, la formazione, il supporto all'avvio, le attività operative, e il pagamento di potenziali costi aggiuntivi, ecc.
- La stima dei tempi necessari per implementare la soluzione che la Pubblica Amministrazione può gestire.
- L'identificazione delle norme e delle linee guida tecniche che il software dovrà seguire durante la sua implementazione, ad esempio, le Linee Guida AgID sul Design, le Linee Guida AgID sull'Interoperabilità e le Linee Guida AgiD per lo sviluppo di software sicuro.
- L'identificazione di eventuali altri vincoli di interesse dell'amministrazione.

Questa fase si conclude con l'individuazione dei limiti, sia economici che temporali, che influenzano le decisioni dell'amministrazione.

2.4.3 Fase 1.3: Redazione del documento descrittivo delle esigenze

L'amministrazione elabora il documento che descrive le esigenze, il quale sarà utilizzato nelle fasi successive del processo di valutazione comparativa. Le attività previste in questa fase includono:

- La creazione del documento descrittivo delle esigenze, che comprende le informazioni raccolte nelle fasi precedenti 1.1 e 1.2.

Questa fase si conclude con la disponibilità del documento descrittivo delle esigenze.

2.3.5.2.2 Macro fase 2: Analisi delle soluzioni a riuso delle PA e delle soluzioni Open Source

Basandosi sulla disponibilità di “soluzioni a riuso delle PA” e “soluzioni Open Source”, è compito della pubblica amministrazione accertare se queste risorse sono in grado di adeguarsi alle sue esigenze. Con l'obiettivo di ottimizzare la spesa complessiva delle pubbliche amministrazioni, la valutazione delle esigenze dovrebbe inizialmente focalizzarsi sulle "soluzioni a riuso delle PA" e, in un secondo momento, sulle “soluzioni Open Source”. L'implementazione dell'articolo 69 del CAD garantisce che le “soluzioni a riuso delle PA” mettano a disposizione il loro codice sorgente, completo di documentazione, in un repository pubblico con licenza aperta.

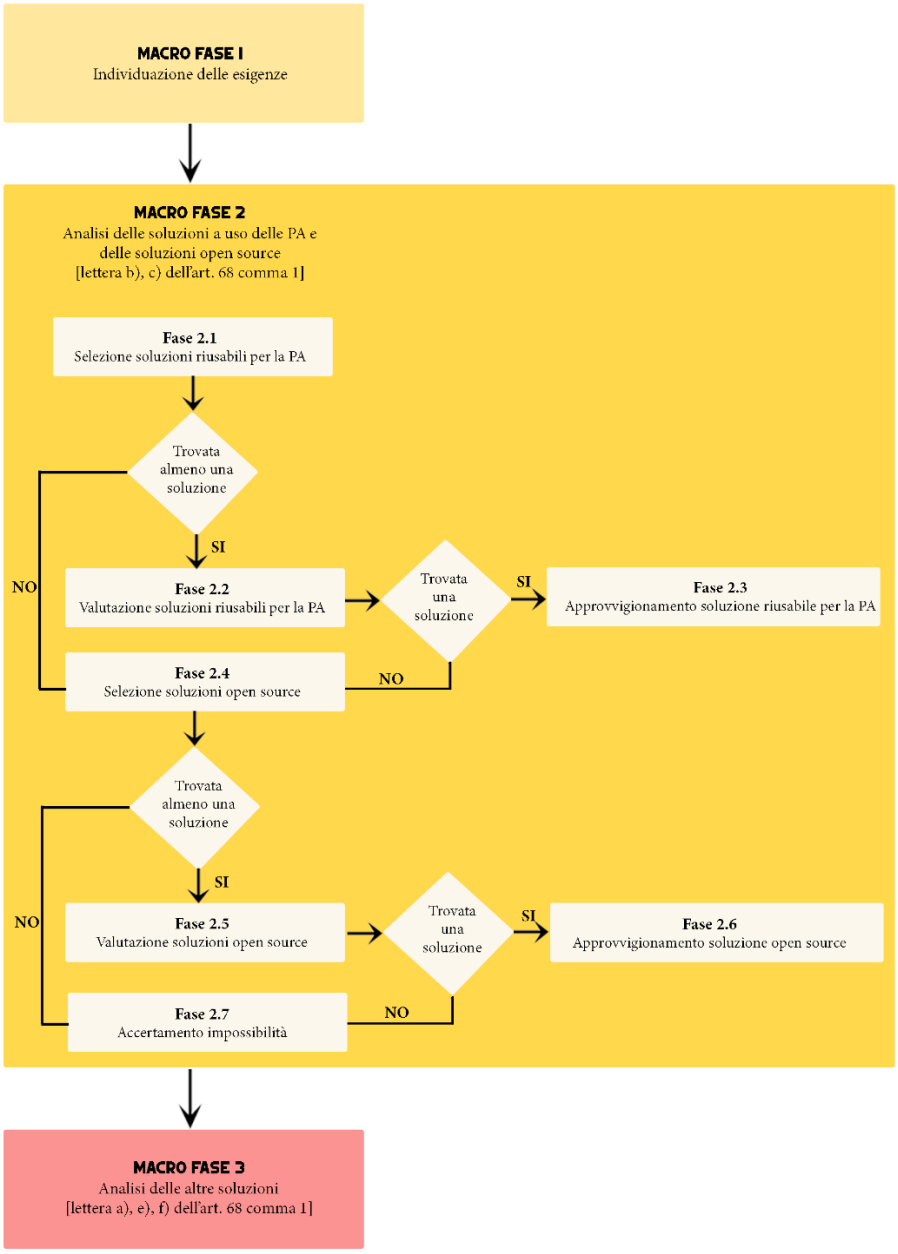

Figura 3 - Macro fase 2

Fase 2.1: Ricerca soluzioni riusabili per la PA

L'amministrazione seleziona le potenziali “soluzioni a riuso delle PA” che possono rispondere alle sue necessità. Le attività previste in questa fase comprendono:

- La ricerca delle “soluzioni a riuso delle PA” disponibili sulla piattaforma Developers Italia.

Questa fase si conclude con l'individuazione delle “soluzioni a riuso delle PA” che sono rilevanti per la Pubblica Amministrazione.

Fase 2.2: Valutazione soluzioni riusabili per la PA

Se nella fase precedente 2.1 è stata individuata almeno una delle “soluzioni a riuso delle PA” che potrebbe interessare alla Pubblica Amministrazione, la fase di valutazione attuale si concentra sulla selezione della miglior “soluzione a riuso della PA”. In questa fase, sono ammissibili anche soluzioni che soddisfano la maggior parte dei requisiti ma richiedono modifiche o personalizzazioni. Per ciascuna delle “soluzioni a riuso delle PA” potenzialmente interessanti, vengono eseguite le seguenti attività:

- Verifica iniziale della conformità alle normative vigenti, come indicato nella scheda del software disponibile su Developers Italia, con particolare attenzione alla conformità alle regole sull'interoperabilità, alle normative sulla protezione dei dati personali, ai requisiti minimi di sicurezza e all'accessibilità.
- Valutazione della qualità della soluzione attraverso vari parametri, alcuni dei quali possono essere reperiti nella scheda del software su Developers Italia, come la copertura dei requisiti funzionali e non funzionali, la presenza di un fornitore di manutenzione, la disponibilità di accordi con terze parti stipulati dall'amministrazione titolare, vincoli e dipendenze con altri software open source o proprietari, competenze interne alla PA per la gestione dell'ambiente e dei linguaggi utilizzati nella soluzione, numero e tipologia di altre pubbliche amministrazioni che utilizzano il progetto open source, vitalità del progetto open source.
- Calcolo del Total Cost of Ownership, con particolare attenzione ai costi di installazione del software nel Cloud della PA o i costi per l'utilizzo del software come servizio (SaaS) se presente nel Marketplace Cloud di AgID, i costi di formazione del personale, i costi di integrazione con i sistemi esistenti, i costi di personalizzazione per soddisfare requisiti specifici, e i costi per verificare la conformità alle normative vigenti.
- Stima dei tempi per la messa in produzione della soluzione.
- Altre stime specifiche dell'amministrazione, se necessarie.

Per valutare quanto sopra, la pubblica amministrazione deve raccogliere tutte le informazioni necessarie secondo le norme stabilite:

- Il costo (TCO) rientra nei limiti di bilancio stabiliti
- I tempi di messa in produzione sono compatibili con i tempi stimati
- Il rispetto di eventuali altri vincoli impedenti

L'amministrazione individuerà la soluzione più adatta alle sue esigenze in base alla valutazione effettuata. Questa fase si conclude con la selezione della migliore “soluzione a riuso delle PA”, o con l'eventuale constatazione dell'assenza di una soluzione adeguata.

Fase 2.3: Approvvigionamento della soluzione riusabile per la PA

Se, dopo la fase precedente 2.2, l'amministrazione ha individuato una “soluzione a riuso della PA” che corrisponde alle sue esigenze, procederà con l'acquisizione e la fase di valutazione comparativa si considera conclusa. Nel caso in cui la Pubblica Amministrazione debba sostenere costi durante la fase di acquisizione, come personalizzazione, installazione o formazione, seguirà le procedure previste dal D.Lgs. 50/2016 e sue modifiche (noto come Codice dei contratti pubblici).

Fase 2.4: Ricerca soluzioni Open Source

Se non è possibile individuare una “soluzione a riuso della PA”, l'amministrazione deve estendere la ricerca per identificare soluzioni potenzialmente adatte alle sue esigenze tra le “soluzioni Open Source”. Questi sono software rilasciati sotto una licenza aperta, ma non di proprietà di una Pubblica Amministrazione e quindi non pubblicati per il riutilizzo. In questa fase, sono ammissibili anche soluzioni che soddisfano la maggior parte dei requisiti ma richiedono modifiche o personalizzazioni. Le attività previste in questa fase includono:

- La ricerca di progetti di software Open Source la cui proprietà non appartiene a enti pubblici. Questa ricerca dovrebbe almeno essere condotta utilizzando gli strumenti disponibili su Developers Italia e potrebbe essere estesa ad altre piattaforme internazionali che gestiscono progetti di software Open Source.

La ricerca condotta dalla pubblica amministrazione deve verificare:

- Se la licenza del software rientra tra quelle suggerite nel presente documento o è certificata da OSI (lista completa).
- Se la licenza è compatibile con le licenze di altri software con cui si intende integrare o con l'uso previsto per il software.

Questa fase si conclude con l'individuazione delle “soluzioni Open Source” di interesse per la pubblica amministrazione.

Fase 2.5: Valutazione soluzioni Open Source

Se nella fase precedente 2.4 è stata identificata almeno una delle “soluzioni Open Source” potenzialmente interessanti, la fase di valutazione successiva ha l'obiettivo di selezionare la miglior “soluzione Open Source” per soddisfare le esigenze della Pubblica Amministrazione. La valutazione del software open source in questa fase deve seguire gli stessi criteri di valutazione descritti nella fase 2.2. Si può considerare la fase 2.5 come una replica della fase 2.2, ma applicata a un diverso insieme di software (open source di terzi invece che software a riuso).
Questa fase si conclude con la determinazione della migliore “soluzione Open Source”, oppure con la constatazione dell'assenza di una soluzione adatta.

Fase 2.6: Approvvigionamento della soluzione Open Source

Se, a seguito della fase precedente 2.5, l'amministrazione ha identificato una “soluzione Open Source” che risponde alle sue esigenze, procederà all'acquisizione. Il processo di acquisizione è descritto nel documento “Riuso di un software”. La fase di valutazione comparativa si considera conclusa. Nel caso in cui la Pubblica Amministrazione debba sostenere spese durante la fase di approvvigionamento (come personalizzazione, installazione o formazione), seguirà le procedure previste dal Codice dei contratti pubblici.

Fase 2.7: Accertamento impossibilità

Se si accerta l'impossibilità di individuare una soluzione che soddisfi almeno in larga misura le esigenze dell'amministrazione tra le “soluzioni a riuso della PA” e le “soluzioni Open Source”, si procederà alla stesura di un documento (senza restrizioni di forma) che espliciti le ragioni di questa impossibilità. Questo documento verrà archiviato come parte del procedimento.
La pubblica amministrazione continuerà la valutazione comparativa seguendo le fasi previste nelle successive fasi del processo.

2.3.5.2.3 Macro fase 3: Analisi delle altre soluzioni

Per soddisfare le proprie esigenze, la pubblica amministrazione DEVE esaminare simultaneamente le possibilità offerte sia dalle soluzioni proprietarie sia da una realizzazione ex novo.

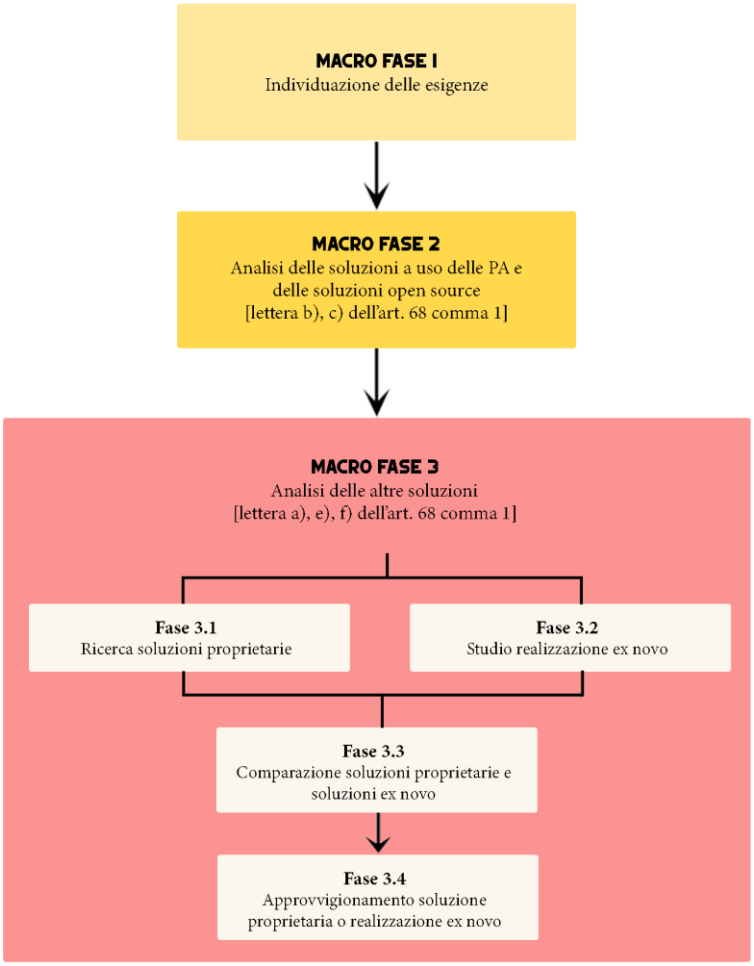

Figura 4 - Macro fase 3

Fase 3.1: Ricerca soluzioni proprietarie

La pubblica amministrazione deve valutare le soluzioni proprietarie disponibili sul mercato. Questa valutazione deve comprendere una ricerca di soluzioni con licenza d'uso proprietaria e un'analisi delle offerte in conformità con quanto previsto dal Codice dei contratti pubblici. L'amministrazione deve anche assicurarsi che il software con licenza rispetti i seguenti requisiti, poiché la mancanza di uno solo di questi requisiti rende la soluzione non idonea:

- Conformità alle regole sull'interoperabilità prescritte dalle linee guida emanate in attuazione dell'articolo 73 del CAD.
- Conformità alle normative sulla protezione dei dati personali.
- Conformità ai livelli minimi di sicurezza previsti per le pubbliche amministrazioni.
- Conformità ai requisiti di accessibilità (Legge 4/2004).
- Possibilità di esportare gratuitamente, in qualsiasi momento, l'intera base di dati, inclusi tutti i tipi di indici o metadati utilizzati per implementare le funzionalità del software, in un formato standard, aperto e documentato per evitare il rischio di lock-in.

Tra i software che soddisfano questi requisiti, l'amministrazione deve condurre un'analisi comparativa che tenga conto dei seguenti criteri:

- Garantire la soddisfazione dei requisiti funzionali e non funzionali definiti nella Macro Fase 1 insieme a quelli indicati nella documentazione.
- Verificare la capacità della soluzione di interoperare con i sistemi già in uso presso l'amministrazione.
- Valutare eventuali costi per l'installazione del software nel Cloud della PA o per l'utilizzo del software tramite modalità SaaS, se disponibili nel Marketplace Cloud di AgID.
- Considerare i costi necessari per integrare la soluzione con i sistemi esistenti presso l'amministrazione.
- Valutare i costi relativi alla formazione del personale responsabile della gestione e amministrazione della soluzione esaminata.
- Calcolare il Total Cost of Ownership e verificarne la congruità rispetto alla disponibilità di bilancio stabilita nella fase precedente della Macro Fase 1.

Questa fase si conclude con l'individuazione delle soluzioni con licenza d'uso proprietaria che soddisfano le esigenze dell'amministrazione.

Fase 3.2: Studio realizzazione ex novo

Dopo aver determinato se esiste o meno una soluzione proprietaria adatta alle proprie esigenze, la Pubblica Amministrazione elabora un documento di progetto di fattibilità. Questo documento deve includere una stima delle attività, dei costi e dei tempi necessari per la creazione di una nuova soluzione che soddisfi integralmente le esigenze delineate nel documento sull'analisi dei fabbisogni, come descritto nella Fase 1.1: Analisi del fabbisogno.

Fase 3.3: Comparazione soluzioni proprietarie e realizzazione ex novo

Nella valutazione tra lo sviluppo di una soluzione ex novo e l'acquisto di una soluzione proprietaria (comunemente chiamata valutazione “make or buy”), l'amministrazione esamina attentamente i vantaggi e gli svantaggi di entrambe le opzioni, prendendo in considerazione i seguenti aspetti:

Vantaggi dell'acquisto di una soluzione proprietaria:

- Rapida implementazione.
- Garanzia totale e responsabilità applicativa a carico del fornitore.
- Servizio di manutenzione fornito dal fornitore.
- Costi iniziali di acquisto o abbonamento generalmente inferiori rispetto allo sviluppo completo.

Vantaggi dello sviluppo di una soluzione ex novo:

- Adattamento completo alle esigenze e agli obiettivi specifici.
- Facilità nella gestione dei dati, inclusa l'importazione ed esportazione.
- Costo totale di proprietà (TCO) più vantaggioso a medio/lungo termine.
- Possibilità di condividere la soluzione con altre entità, consentendo ottimizzazioni dei costi di gestione.
- Scalabilità e possibilità di aggiornamenti futuri.
- Potenziale per il riuso da parte di altre amministrazioni.

Svantaggi di una soluzione proprietaria:

- Spese ricorrenti come licenze periodiche (abbonamenti mensili o annuali) o costi per aggiornamenti a pagamento.
- Limitazioni nella flessibilità del flusso operativo, che potrebbe non adattarsi perfettamente all'organizzazione operativa della Pubblica Amministrazione.
- Possibilità di essere bloccati (lock-in) in futuro, con costi elevati per cambiare soluzione.
- Dipendenza dalla stabilità economica del fornitore.

Svantaggi di una soluzione sviluppata ex novo:

- Maggiore complessità delle attività da svolgere.
- Necessità di coordinamento più esteso.
- Tempi di implementazione più lunghi rispetto all'acquisto di una soluzione pronta all'uso.

Fase 3.4: Approvvigionamento soluzione proprietaria o realizzazione ex Novo

In seguito alla fase precedente, la Pubblica Amministrazione ha individuato una soluzione, che può essere con licenza proprietaria o da sviluppare ex novo, che soddisfa le sue esigenze. Successivamente, procede all'approvvigionamento della soluzione seguendo le procedure previste dal Codice dei contratti pubblici. Se si opta per l'acquisizione di software proprietario sotto licenza, è importante ricordare che l'Amministrazione deve, se possibile, cercare di acquisire la titolarità del codice sviluppato al fine di renderlo disponibile per il riuso. Con questa fase, la valutazione comparativa è considerata conclusa.

2.4 Developers Italia

Developers Italia è una piattaforma nata in collaborazione tra AgID e il Team per la Trasformazione Digitale del Governo al fine di migliorare la qualità e l'efficienza dei servizi pubblici attraverso la collaborazione e l'innovazione tecnologica. La piattaforma è stata progettata per facilitare la condivisione di soluzioni, conoscenze e strumenti tra sviluppatori e amministrazioni pubbliche, con l'obiettivo di semplificare i processi amministrativi, aumentare la trasparenza e migliorare l'esperienza dei cittadini.
Developers Italia è stata ideata con diversi obiettivi in mente, tra cui:

- **Collaborazione tra Settori:** l'obiettivo della piattaforma è promuovere la collaborazione tra aziende pubbliche e private. Il contributo degli sviluppatori alle iniziative pubbliche può aumentare l'efficienza, l'innovazione e la trasparenza nella fornitura dei servizi.
- **Riutilizzo delle Soluzioni:** Sviluppatori ed enti governativi possono collaborare su progetti e soluzioni che possono essere riutilizzati da altri enti, aiutando così a risparmiare tempo e risorse. Questa collaborazione promuove l'uso di software open source, incoraggia lo sviluppo collaborativo di soluzioni e permette di creare applicazioni più sicure e affidabili.
- **Innovazione:** l'apertura all'innovazione della piattaforma consente agli sviluppatori di sperimentare nuove soluzioni e approcci, promuovendo un ciclo di miglioramento continuo nei servizi pubblici.
- **Trasparenza e Partecipazione dei Cittadini:** attraverso soluzioni tecnologiche trasparenti e accessibili, Developers Italia promuove la partecipazione attiva dei cittadini nei processi decisionali e nell'accesso alle informazioni pubbliche.

2.4.1 Vantaggi e svantaggi dell'adozione di software a riuso nella pubblica amministrazione

Nell'era digitale in cui la tecnologia è divenuta il motore trainante dei processi amministrativi e dei servizi erogati alla collettività, la pubblica amministrazione è chiamata a rimodellare costantemente i propri approcci operativi. In questo scenario di cambiamenti rapidi e richieste crescenti da parte dei cittadini, l'adozione di soluzioni software gioca un ruolo fondamentale nel miglioramento dell'efficienza e dell'efficacia dell'apparato pubblico. In questo contesto, l'adozione di software a riuso presenta un potenziale promettente, avendo costi complessivi ridotti e una rapida implementazione. Tuttavia, come qualsiasi decisione che coinvolge tecnologie e processi complessi, il riuso del software comporta una serie di vantaggi e svantaggi che meritano considerazione.

Vantaggi:

- **Efficienza nell'implementazione:** L'adozione di software già esistente accelera notevolmente il processo di implementazione delle soluzioni tecnologiche, risparmiando tempo, risorse e sforzi. In contrasto, lo sviluppo di software personalizzato richiede un impegno significativo in termini di tempo, personale altamente qualificato e risorse finanziarie considerevoli.
- **Ottimizzazione dei costi:** L'utilizzo di software a riuso spesso comporta costi inferiori rispetto allo sviluppo da zero. Questo aspetto è particolarmente rilevante per le amministrazioni con budget limitati, poiché gran parte del lavoro necessario è già stato completato.
- **Riduzione dei rischi:** L'adozione di software a riuso riduce in modo sostanziale i rischi associati all'implementazione di nuove soluzioni. I software già testati e utilizzati con successo in altre situazioni sono più affidabili in nuovi contesti, contribuendo a ridurre al minimo i rischi di errori critici, problemi di sicurezza e malfunzionamenti durante lo sviluppo.
- **Aggiornamenti costanti:** Gli sviluppatori di software a riuso sono costantemente impegnati nell'ottimizzazione delle loro soluzioni. L'adozione di tali software garantisce l'accesso a miglioramenti e nuove funzionalità senza necessità di investimenti aggiuntivi. Questo è fondamentale per mantenere i servizi della pubblica amministrazione allineati con gli sviluppi tecnologici più recenti.
- **Scalabilità:** Le amministrazioni devono essere in grado di gestire volumi di dati in crescita e carichi di lavoro in aumento senza intoppi. Le soluzioni a riuso sono progettate con un'architettura scalabile, consentendo un'espansione flessibile per soddisfare le crescenti esigenze, evitando la necessità di ridisegnare completamente il software.

- **Promozione della standardizzazione:** L'utilizzo di software a riuso aiuta a stabilire standard e linee guida comuni per la pubblica amministrazione, migliorando la coerenza e l'interoperabilità tra diversi settori e organizzazioni governative.
- **Manutenzione agevolata:** Il software a riuso è spesso supportato da una comunità di sviluppatori o da organizzazioni che forniscono aggiornamenti e manutenzione costante. Ciò garantisce che il software rimanga sempre aggiornato, sicuro e funzionale nel tempo.
- **Facilitazione della condivisione delle best practice:** L'adozione di software a riuso consente alle amministrazioni di condividere best practice e conoscenze con altre entità governative, promuovendo una collaborazione più efficace.
- **Accesso a funzionalità avanzate:** Molto software a riuso è stato sviluppato per fornire funzionalità avanzate o specializzate, rendendo disponibili queste capacità senza la necessità di affrontare costi o complessità elevati durante lo sviluppo interno.
- **Massima flessibilità:** L'uso di software a riuso offre un'ampia flessibilità nella selezione delle soluzioni. Le amministrazioni possono valutare diverse opzioni e adottare quelle che meglio soddisfano le loro esigenze specifiche.

Svantaggi:

- **Adattamento e personalizzazione:** Alcuni software preesistenti potrebbero necessitare di modifiche significative per adattarsi alle specifiche esigenze dell'amministrazione pubblica. Questo può comportare costi aggiuntivi e complessità nell'implementazione.
- **Dipendenza da terze parti:** L'adozione di software già esistente può comportare una dipendenza dagli sviluppatori o dai fornitori originali per eventuali modifiche o supporto tecnico. Questa dipendenza potrebbe generare problemi se i fornitori originali non sono in grado o non sono disponibili per fornire assistenza.
- **Problematiche di sicurezza:** L'uso di software a riuso potrebbe comportare il rischio di ereditare vulnerabilità o problemi di sicurezza presenti nel codice sorgente originale. È fondamentale eseguire una rigorosa revisione della sicurezza per garantire che il software sia adeguatamente protetto.
- **Vincoli di licenza:** Alcuni software a riuso possono essere soggetti a licenze che impongono limitazioni sull'uso o richiedono la condivisione delle modifiche apportate. È importante comprendere e rispettare queste licenze per evitare controversie legali.
- **Controllo e personalizzazione limitati:** L'adozione di software a riuso potrebbe limitare il controllo e la personalizzazione del software stesso. Questo potrebbe non essere ideale quando sono necessarie soluzioni altamente specifiche o personalizzate.

Senza dubbio, i vantaggi derivanti dall'adozione di software a riuso nella pubblica amministrazione superano considerevolmente gli svantaggi. I vantaggi sopracitati sono fattori che sottolineano chiaramente il valore di questa pratica, traducendosi in un miglioramento dell'efficienza, della scalabilità e della qualità delle operazioni nell'ambito della pubblica amministrazione.

2.4.2 Confronto dei costi tra software a riuso e soluzioni proprietarie

Nell'analizzare i costi legati all'adozione di software a riuso, come librerie open-source o componenti preesistenti, rispetto all'impiego di soluzioni proprietarie, ci sono alcune considerazioni da tenere presente:

Per l'adozione di software a riuso:

- **Costi Iniziali:** le librerie open-source o i componenti preesistenti sono generalmente disponibili gratuitamente o con costi di licenza notevolmente ridotti rispetto alle soluzioni proprietarie. Questo può ridurre significativamente i costi iniziali di implementazione.
- **Sviluppo e Personalizzazione:** l'uso di software a riuso offre l'opportunità di risparmiare tempo durante la fase iniziale dello sviluppo, poiché si parte da una base già esistente. Tuttavia, è importante notare che potrebbe essere necessario apportare modifiche e personalizzazioni per adattare il software alle esigenze specifiche del progetto. Questo processo di personalizzazione potrebbe richiedere risorse aggiuntive, come tempo e competenze di sviluppo.
- **Manutenzione e Aggiornamenti:** le librerie open-source possono essere mantenute dalla comunità di sviluppatori o dalle organizzazioni che le supportano. Tuttavia, è importante riconoscere che la manutenzione continua è necessaria per garantire la sicurezza e la stabilità del software. Gli aggiornamenti per affrontare le vulnerabilità di sicurezza o migliorare le funzionalità possono richiedere un impegno costante da parte del team di sviluppo.
- **Sicurezza:** mentre le librerie open-source offrono vantaggi in termini di accessibilità e personalizzazione, possono anche presentare potenziali vulnerabilità di sicurezza. Pertanto, è fondamentale monitorare attentamente gli aggiornamenti delle librerie e applicare correzioni quando necessario per mitigare i rischi. La sicurezza è un aspetto critico da considerare quando si fa affidamento al riuso del software.
- **Integrazione:** l'integrazione di librerie open-source può richiedere uno sforzo significativo per assicurarsi che funzionino in modo ottimale all'interno del sistema esistente. Questo può comportare la necessità di sviluppare connessioni personalizzate, risolvere problemi di compatibilità e assicurarsi che le librerie si integrino senza problemi con altri componenti del sistema.
- **Lock-in del fornitore:** Utilizzando il software a riuso, si riduce il rischio di essere vincolati a un unico fornitore o a una piattaforma specifica. Questo offre una maggiore flessibilità e indipendenza nella gestione del software nel lungo termine.

Per l’adozione di soluzioni proprietarie:

- **Costi Iniziali:** le soluzioni proprietarie di solito comportano un costo significativo per l'acquisizione delle licenze d'uso. Questi costi iniziali possono essere considerevoli e devono essere inclusi nel budget del progetto.
- **Sviluppo e Personalizzazione:** le soluzioni proprietarie sono sviluppate per adattarsi alle esigenze specifiche dell'utente. Tuttavia, la personalizzazione di queste soluzioni può richiedere più tempo e risorse rispetto all'utilizzo di software a riuso. Il processo di sviluppo personalizzato potrebbe coinvolgere la collaborazione con il fornitore per definire i requisiti esatti.
- **Manutenzione e Aggiornamenti:** le soluzioni proprietarie spesso includono supporto e servizi di aggiornamento forniti dal fornitore. Tuttavia, è importante considerare che questi servizi possono comportare costi aggiuntivi nel tempo. La manutenzione e gli aggiornamenti sono gestiti in gran parte dal fornitore, ma è essenziale comprendere i costi associati a tali servizi.
- **Sicurezza:** le soluzioni proprietarie tendono a offrire un maggiore controllo sulla sicurezza, ma questo dipende dalla qualità e dalla prontezza del supporto fornito dal fornitore. È importante valutare attentamente le politiche di sicurezza e i protocolli di gestione dei dati dell'offerta proprietaria per garantire la protezione dei dati sensibili.
- **Integrazione:** le soluzioni proprietarie sono spesso progettate per funzionare insieme in modo più fluido. Ciò semplifica l'integrazione con altri sistemi e componenti, riducendo il tempo e gli sforzi necessari per far funzionare il software all'interno dell'ecosistema esistente.
- **Lock-in del Fornitore:** con le soluzioni proprietarie, c'è un rischio maggiore di dipendenza da un unico fornitore, poiché le personalizzazioni e le integrazioni possono essere strettamente legate alle tecnologie e ai protocolli specifici offerti dal fornitore. Questo potrebbe limitare l'agilità e la flessibilità nell'adozione di soluzioni alternative in futuro. Pertanto, è importante valutare attentamente il rischio di lock-in del fornitore quando si opta per soluzioni proprietarie.

3 Caso concreto di riuso

L'obiettivo principale del lavoro di tesi è la pubblicazione in riuso di un applicativo già esistente, migliorandone però la qualità, abbassandone quindi il debito tecnico fino a raggiungere gli standard della piattaforma di Developers Italia. Prima di iniziare il lavoro effettivo sul codice, sono state eseguite una serie di attività preliminari per definire un piano chiaro che guidasse il processo di miglioramento. Queste attività includono:

- **Esame del Codice dell'Amministrazione Digitale e delle Linee Guida AGID:** In questa fase, è stata condotta un'analisi del Codice dell'Amministrazione Digitale, insieme alle linee guida fornite dall'AGID relative al riuso. L'obiettivo era comprendere appieno il contesto in cui operare e identificare i requisiti tecnico-legali che dovevano essere rispettati.
- **Analisi Qualitativa del Software:** È stata condotta un'analisi dettagliata del software esistente, valutando la sua qualità complessiva. Inoltre, è stata effettuata una comparazione tra il livello di debito tecnico identificato tramite piattaforme esterne come SonarCloud nel software oggetto di tesi e quello rilevato in software analoghi già presenti nel catalogo. Questo confronto ha permesso di identificare quali categorie di warning prioritizzare durante il processo di miglioramento.

Il processo preliminare è fondamentale per stabilire una base solida prima di procedere con il lavoro effettivo sul codice. Consente di comprendere appieno il contesto, i requisiti e le aree critiche da affrontare per portare l'applicativo al livello desiderato di qualità e conformità con gli standard di Developers Italia. Una volta completate queste attività, è possibile definire in modo più preciso le strategie e le priorità per il miglioramento del software, garantendo un processo efficiente e ben strutturato.

3.1 Introduzione al progetto Calamità Naturali

L'applicativo offre un modulo di assegnazione di indennizzi per i danni causati da calamità naturali. Tramite esso è possibile inviare richieste di indennizzo entro 45 giorni dalla pubblicazione del decreto ministeriale che riconosce lo stato di calamità naturale, emesso dal MiPAAF. Queste richieste mirano a fornire sostegno alle imprese agricole colpite da eventi come alluvioni, terremoti, valanghe e avversità atmosferiche come gelo, grandine, ghiaccio, siccità, piogge e altre. Le domande possono essere immediatamente elaborate dai funzionari competenti, che avviano il procedimento. Attraverso questo servizio, è possibile monitorare l'andamento della pratica e compilare e inviare tutte le successive comunicazioni via web. Gli indennizzi possono essere richiesti dalle aziende agricole e dalle cooperative di raccolta, lavorazione, trasformazione e commercializzazione di prodotti agricoli che risiedono nelle zone designate da un decreto ministeriale. Conformemente al D.Lgs. 29 marzo 2004, n. 102, gli indennizzi sono concessi esclusivamente per danni a produzioni, strutture e impianti produttivi non coperti da un Piano assicurativo agricolo annuale, purché il danno rappresenti almeno il 30% del valore della produzione lorda vendibile. Inoltre, sono previsti interventi di ripristino delle infrastrutture legate all'attività agricola, inclusi quelli riguardanti l'irrigazione e la bonifica, compatibilmente con le esigenze delle imprese agricole.
La sezione "Calamità Naturali" del SIA-RB comprende due moduli applicativi:

- **Calamità Naturali (Pratiche):** Questo modulo consente agli utenti di compilare online le domande di indennizzo. Le richieste vengono protocollate e inoltrate agli uffici competenti per avviare il procedimento amministrativo. Gli utenti possono monitorare lo stato della pratica e inviare la documentazione richiesta nei tempi previsti.
- **Calamità Naturali (Configurazione):** Questo modulo è riservato ai funzionari della Pubblica Amministrazione e serve per configurare i bandi di assegnazione degli indennizzi da calamità naturali che saranno successivamente pubblicati e gestiti sul servizio Calamità Naturali (Pratiche).

Gli utenti di questo servizio includono:

- I consorzi irrigui che possono presentare richieste di finanziamento per il ripristino delle infrastrutture irrigue.
- I titolari o rappresentanti legali delle aziende agricole, che possono presentare richieste di contributo e verificare lo stato di avanzamento delle pratiche.
- I Centri di Assistenza Agricola (CAA) che possono presentare domande di aiuto per conto delle aziende agricole a cui prestano assistenza.
- La Pubblica Amministrazione competente per l'ammissione al finanziamento.

3.2 Sonarcloud

Nel mondo dell'ingegneria del software, la qualità del codice è un aspetto cruciale per garantire che un'applicazione o un sistema funzioni correttamente, sia robusto, mantenibile e privo di bug critici. La gestione della qualità del codice è diventata sempre più importante a causa della crescente complessità dei progetti software e della necessità di rispettare standard elevati. SonarCloud è un servizio cloud offerto da SonarSource, un'azienda specializzata nell'analisi statica del codice e nella gestione della qualità del software. Questo strumento si è guadagnato una reputazione eccellente nel campo dello sviluppo software grazie alla sua capacità di identificare e risolvere problemi nel codice sorgente, contribuendo così a migliorare la qualità del software stesso. Ci sono diversi elementi fondamentali di SonarCloud che contribuiscono a renderlo un prezioso alleato per gli sviluppatori, tra cui:

- **Analisi Statica del Codice:** il processo automatizzato di analisi statica esamina il codice sorgente alla ricerca di una vasta gamma di problemi, tra cui bug, vulnerabilità di sicurezza, duplicazione del codice, e violazioni delle best practice di programmazione. Questa analisi è fondamentale per identificare potenziali errori nel codice prima che possano causare problemi nel software in produzione. Inoltre, permette di risparmiare tempo e risorse che altrimenti sarebbero stati spesi nella risoluzione di problemi dopo il rilascio.
- **Integrazione Semplice nei Processi di Sviluppo:** grazie a plugin e integrazioni con strumenti di integrazione continua come Jenkins, Travis CI, CircleCI e molti altri, è possibile eseguire l'analisi statica del codice in modo automatico durante il processo di build e rilascio. Ciò significa che è possibile identificare e risolvere problemi di codice in modo continuo, riducendo il rischio di accumulo di debiti tecnici.
- **Segnalazione Dettagliata dei Problemi:** quando il sistema rileva un problema nel codice, fornisce un dettagliato insieme di informazioni al riguardo. Questo feedback non si limita a indicare la posizione del problema, ma esplica le ragioni per cui è stato identificato come tale e offre suggerimenti per risolverlo. Questa chiarezza è di importanza vitale per gli sviluppatori, poiché semplifica la comprensione delle modifiche necessarie.
- **Misurazione della Qualità del Codice:** questo strumento offre una serie di metriche e indicatori chiave di performance che consentono di valutare la qualità generale del codice. Tra questi indicatori ci sono la copertura del codice, la complessità ciclomatica, il numero di bug e vulnerabilità, il debito tecnico e molti altri. Queste metriche permettono di avere una panoramica completa sulla salute del progetto e di monitorare i progressi nel migliorare la qualità del software nel tempo.
- **Supporto per Diversi Linguaggi di Programmazione:** indipendentemente dal linguaggio utilizzato per lo sviluppo del software, è probabile che SonarCloud sia in grado di analizzare il codice e fornire feedback dettagliato. Tra i linguaggi supportati figurano

Java, JavaScript, C#, Python, Ruby e molti altri. Questa flessibilità lo rende adatto a una vasta gamma di progetti software.

- **Regole personalizzabili:** tramite questo strumento è possibile definire regole personalizzate per l'analisi del codice. Gli sviluppatori possono creare regole su misura che rispecchiano le particolari linee guida e gli standard di codifica del progetto o dell'azienda. Questo livello di personalizzazione consente di affrontare in modo mirato le sfide specifiche del progetto, garantendo che SonarCloud fornisca feedback rilevanti e utili per migliorare la qualità del codice. Inoltre, questa caratteristica rende SonarCloud adatto a una vasta gamma di contesti, da piccoli progetti open source a grandi applicazioni aziendali complesse, dove le esigenze di analisi del codice possono variare notevolmente.

È importante notare che SonarCloud è una versione cloud-based del prodotto SonarQube. Quest'ultimo è una soluzione on-premises per l'analisi della qualità del codice. L'adozione di SonarCloud offre ai team di sviluppo il vantaggio di accedere a queste potenti funzionalità senza la necessità di gestire e mantenere un'infrastruttura locale. Questo è particolarmente vantaggioso per i progetti open source e i team di sviluppo che desiderano migliorare la qualità del loro codice in modo efficiente, senza il peso delle complesse operazioni di gestione dei server. In aggiunta, SonarCloud offre una serie di ulteriori vantaggi. Per esempio, elimina la necessità di dedicare risorse all'installazione e alla configurazione iniziale di SonarQube, risparmiando tempo prezioso che può essere impiegato direttamente nell'analisi del codice e nell'implementazione di miglioramenti. SonarCloud offre inoltre una maggiore scalabilità, consentendo ai team di espandere facilmente le risorse di analisi in base alle esigenze del progetto. Questa flessibilità è particolarmente utile per i progetti soggetti a picchi di attività o che richiedono una distribuzione geografica.

3.3 Definizione e calcolo dei requisiti qualitativi

La prima fase del processo di definizione dei requisiti qualitativi consiste nello stabilire quali applicativi già presenti sulla piattaforma di Developers Italia analizzare. Questa selezione attenta ha creato una base solida e coerente per la definizione dei requisiti qualitativi che l'applicativo oggetto di tesi deve soddisfare. Sono stati analizzati quindi solo i progetti che soddisfano le seguenti caratteristiche:

- stato del progetto impostato a "stabile". Questo criterio di selezione ha contribuito a garantire che gli applicativi considerati avessero già raggiunto un grado di maturità significativo, offrendo quindi un solido punto di partenza per l'analisi dei requisiti qualitativi.
- applicativi sviluppati per dispositivi desktop, escludendo dalla ricerca tutti i progetti sviluppati per dispositivi mobili come telefoni e tablet. La scelta è determinata dalla necessità di garantire che i risultati dell'analisi fossero immediatamente applicabili all'applicativo oggetto di tesi, senza influenze o complessità legate alle peculiarità dei dispositivi stessi.
- selezionati solo i progetti relativi ad applicazioni standalone con un'interfaccia indipendente, escludendo i progetti che corrispondono a estensioni di altri applicativi, librerie, addon o file di configurazione.

Sono stati analizzati i seguenti applicativi:

- **Conam:** gestione del procedimento amministrativo sanzionatorio per le materie di competenza regionale.
- **Gestione Autorizzazioni:** gestione web-based delle richieste di manutenzione stradale e trasloco effettuate dalle aziende competenti
- **Rebus:** gestione delle anagrafiche degli autobus, dei contratti e dei soggetti del Trasporto Pubblico Locale
- **Sportello Paesaggio e trasmissioni provvedimenti:** gestione dei procedimenti di Autorizzazioni e accertamenti di compatibilità paesaggistica con localizzazione dell'intervento su sistemi GIS.
- **Sigea:** gestione degli eventi delle attività turistiche
- **Iuffi:** gestione del monitoraggio fitosanitario per la lotta agli organismi nocivi
- **Preference Center:** gestione e invio di comunicazioni personalizzate per affiancare il lavoro quotidiano di diffusione di contenuti di una redazione.
- **Portale Allerta Meteo:** portale della Pubblica Amministrazione per le funzioni di allertamento meteo
- **Nova:** Market place realizzato dal Comune di Genova per rendere accessibili i servizi necessari alla creazione ed innovazione d'impresa.
- **Esenzione:** gestione delle esenzioni per patologia della Regione Piemonte.

Ogni progetto è stato sottoposto ad un'analisi completa da parte di SonarCloud, che ha consentito di raccogliere dati fondamentali relativi all'affidabilità, alla manutenibilità e alla sicurezza degli applicativi stessi. Questo processo di analisi ha incluso il calcolo del numero di bug, di code smell e di vulnerabilità di sicurezza presenti all'interno dei progetti. I dati così ottenuti sono stati poi normalizzati rispetto alla dimensione degli applicativi (espressa in termini di linee di codice). Sulla base di questi dati normalizzati, è stato stabilito un obiettivo da raggiungere per ciascuna delle categorie di analisi. Il valore di questo obiettivo corrisponde al numero di problemi che SonarCloud dovrebbe segnalare nel progetto per far sì che la categoria analizzata rientri nel primo quartile della distribuzione di dati. Le categorie, raggiungendo questo obiettivo avanzato, dimostrano una qualità notevolmente superiore rispetto alla media, alzando quindi il livello di affidabilità, manutenibilità e sicurezza, promuovendo una migliore esperienza per gli utenti finali e una maggiore sostenibilità nel tempo. Per evitare di abbattere il debito tecnico in modo completamente casuale o puramente opportunistico (come, ad esempio, eliminando solo le soluzioni più facili e rapide), è stato seguito un approccio basato sul marcatore di gravità assegnato dal SonarCloud, correggendo prima i problemi più gravi segnalati come bloccanti, poi i critici e così via, fino al raggiungimento dell'obiettivo stabilito.
Di seguito la tabella riassuntiva dei tre indici di qualità considerati:

Progetto	Righe di codice (k)	Security	Security normalizzato	Bug	Bug normalizzati	Code smell (k)	Code smell (k) normalizzati
Conam	137	0	0	62	0,453	4,7	0,034
Gestione Autorizzazioni	50	2	0,04	135	2,7	6,1	0,122
Rebus	220	0	0	282	1,282	6,7	0,030
Sportello Paesaggio	325	0	0	557	1,714	14	0,043
Sigea	123	0	0	707	5,748	8	0,065
Iuffi	276	2	0,007	292	1,058	17	0,062
Preference Center	66	1	0,015	315	4,773	18	0,273
Portale Allerta Meteo	406	10	0,025	345	0,850	21	0,052
Nova	32	2	0,062	118	3,688	4,3	0,134
Esenzione	77	1	0,013	108	1,403	6,3	0,082
Calamità Naturali	210	3	0,014	623	2,967	13,7	0,065

3.4 Vulnerabilità di sicurezza

La sicurezza è un tema di cruciale importanza nell'era digitale in cui viviamo. Con l'aumento esponenziale dell'uso di dispositivi mobili, applicazioni web e software in generale, è fondamentale garantire che le informazioni sensibili degli utenti siano protette da minacce e attacchi informatici. È possibile migliorare significativamente la sicurezza dei propri applicativi e proteggere gli utenti da potenziali minacce seguendo alcune buone pratiche durante il processo di sviluppo, come ad esempio:

- **Validazione dei dati in ingresso:** assicurarsi che tutti i dati provenienti dall'utente siano validati e sanificati correttamente per prevenire attacchi come SQL injection, XSS (Cross-Site Scripting) e CSRF (Cross-Site Request Forgery).
- **Utilizzo di librerie e framework sicuri:** utilizzare librerie e framework affidabili e mantenuti regolarmente per ridurre il rischio di vulnerabilità di sicurezza.
- **Autenticazione e autorizzazione:** implementare una robusta autenticazione degli utenti per garantire che solo gli utenti autorizzati possano accedere alle funzionalità riservate. Utilizzare un sistema di autorizzazione per garantire che gli utenti accedano solo alle risorse che sono autorizzati a visualizzare o modificare.
- **Protezione delle password:** memorizzare le password in modo sicuro utilizzando algoritmi di hash crittograficamente sicuri e un sale (salt) unico per ciascuna password. Inoltre, incoraggiare gli utenti a utilizzare password complesse.
- **Gestione delle sessioni:** utilizzare token di sessione sicuri e implementare timeout di sessione per proteggere contro attacchi di session hijacking.
- **Validazione lato server:** non fidarsi solo della validazione lato client, ma eseguire anche la validazione lato server per prevenire attacchi che potrebbero bypassare la validazione client-side.
- **Protezione contro attacchi di injection:** sanificare e parametrizzare le query SQL per prevenire SQL injection. Utilizzare anche l'output encoding per prevenire XSS.
- **Gestione degli errori sicura:** non mostrare informazioni sensibili sugli errori agli utenti finali. Registrare i dettagli degli errori in modo sicuro e notificare gli amministratori del sistema in caso di errori critici.
- **Aggiornamenti regolari:** mantenere il software aggiornato con le ultime patch di sicurezza per tutti i componenti e le librerie utilizzate.
- **Riservatezza e protezione dei dati:** assicurarsi che i dati sensibili siano adeguatamente cifrati in transito e a riposo e che venga applicato un adeguato controllo degli accessi.

Di seguito sono riportati i risultati relativi all'elaborazione dei dati estratti dagli applicativi analizzati, come mostrato nel capitolo 3.3, riferiti solo alla categoria della sicurezza:

Progetto	Righe di codice (k)	Security	Security normalizzato
Conam	137	0	0
Gestione Autorizzazioni	50	2	0,040
Rebus	220	0	0
Sportello Paesaggio	325	0	0
Sigea	123	0	0
Iuffi	276	2	0,007
Preference Center	66	1	0,015
Portale Allerta Meteo	406	10	0,025
Nova	32	2	0,062
Esenzione	77	1	0,013
Calamità Naturali	210	3	0,014

Elaborando questi dati, si evidenzia che l'obiettivo da raggiungere, fissato al primo quartile, corrisponde alla correzione di tutte le vulnerabilità di sicurezza. È importante sottolineare che, data la natura critica della categoria in questione, l'obiettivo dovrebbe essere la risoluzione di tutte le vulnerabilità, indipendentemente dal valore ottenuto come risultato dell'analisi dei dati. Tutti e tre i problemi segnalati sono relativi alla stampa del dettaglio della stack trace sulla console di log. In generale, la stampa di informazioni di debug su una console di un'applicazione in produzione può comportare diversi rischi per la sicurezza. Questi rischi includono:

- La possibile esposizione di informazioni sensibili, come nomi di classi, metodi o percorsi di file, presenti nella stack trace. Tali informazioni potrebbero essere sfruttate da un potenziale attaccante per acquisire dettagli sul funzionamento interno dell'applicazione o per individuare potenziali vulnerabilità.
- Il rischio di esposizione di informazioni relative agli utenti qualora fossero contenuti nella stack trace. Questo potrebbe comportare violazioni della privacy degli utenti e problemi di conformità con le leggi sulla protezione dei dati.
- Quando le informazioni di debug vengono registrate in file di log, è fondamentale garantire che questi file siano adeguatamente protetti e che le informazioni sensibili siano crittografate o rimosse dai log.

La soluzione attuata, nonché la più semplice e ovvia possibile, è stata quella di eliminare le istruzioni di stampa.

3.5 Reliability

La “reliability” o “affidabilità” si riferisce alla capacità di un sistema, dispositivo, processo o prodotto di funzionare in modo coerente, costante e senza guasti o problemi in un determinato contesto o periodo di tempo. SonarCloud considera il numero di problemi segnalati come bug come indice della reliability del progetto. Avere un codice senza bug è fondamentale per garantire la stabilità, l'affidabilità e l'efficienza di un software. I bug possono causare malfunzionamenti e rallentamenti, mettendo a rischio la soddisfazione degli utenti e l'integrità dei dati. Un codice privo di bug non solo migliora l'esperienza dell'utente, ma contribuisce anche alla reputazione del software e dell'azienda, promuovendo la fiducia dei clienti e facilitando il successo sul mercato. Pertanto, investire nella scrittura di un codice di alta qualità e nella sua continua manutenzione è un passo cruciale per il successo a lungo termine di qualsiasi progetto software. Di seguito sono riportati i risultati relativi all’elaborazione dei dati estratti dagli applicativi analizzati, come mostrato nel capitolo 3.3, riferiti solo alla categoria reliability:

Progetto	Righe di codice (k)	Bug	Bug normalizzati
Conam	137	62	0,453
Gestione Autorizzazioni	50	135	2,7
Rebus	220	282	1,282
Sportello Paesaggio	325	557	1,714
Sigea	123	707	5,748
Iuffi	276	292	1,058
Preference Center	66	315	4,773
Portale Allerta Meteo	406	345	0,850
Nova	32	118	3,688
Esenzione	77	108	1,403
Calamità Naturali	210	623	2,967

Elaborando questi dati, si evidenzia che l'obiettivo da raggiungere, fissato al primo quartile, corrisponde a un numero di bug rimanenti associati al progetto pari a 234.
È essenziale sottolineare che SonarCloud classifica come "bug" anche le carenze del software legate all'accessibilità. Per accessibilità nel software si intende la progettazione e lo sviluppo di applicazioni, siti web, programmi e altri prodotti software in modo che possano essere utilizzati in modo efficace e comprensibile da parte di persone con diverse abilità e disabilità.
Di seguito vengono descritti alcuni dei bug corretti:

- In alcuni punti dell’applicativo poteva essere lanciata una “NullPointerException”, un'eccezione di runtime che si verifica quando si tenta di accedere o manipolare un oggetto che è attualmente impostato su “null”. Questa eccezione è il risultato di un

errore di programmazione e indica tipicamente che si sta cercando di eseguire un'operazione su un riferimento a un oggetto che in realtà non punta a un oggetto in memoria. È stata gestita verificando se l'oggetto è null prima di accedere ai suoi metodi o proprietà.

- In alcune strutture condizionali erano presenti le stesse istruzioni in entrambi i rami. Problema risolto spostando le istruzioni comuni fuori dal blocco condizionale.
- Alcuni cicli venivano gestiti in modo non condizionale attraverso l'uso dell'istruzione “break”. Il codice è stato riscritto in modo tale da non richiedere più l'utilizzo di questa istruzione.
- Alcune funzioni avevano multiple istruzioni di “return”. Sono state riscritte in modo tale da richiedere l'utilizzo di questa istruzione solo una volta.
- Molte delle tabelle presenti nell’applicativo non avevano l’attributo “summary” valorizzato. Per questioni di accessibilità verso gli utenti con disabilità visiva, è importante che le tabelle forniscano una descrizione dei loro contenuti prima che i dati siano accessibili. Problema risolto valorizzando l’attributo.
- Alcune delle tabelle non avevano l’header “<th>”. Le tecnologie assistive, come i lettori di schermo, utilizzano questi header per aiutare l’utente nella consultazione delle tabelle. Senza di essi, l'utente si perde rapidamente nel flusso dei dati. Problema risolto valorizzando l’attributo.

3.6 Maintainability

La “maintainability” o “manutenibilità” si riferisce alla misura in cui un sistema, un prodotto, un software o un componente possono essere facilmente mantenuti, riparati o modificati nel corso del tempo con un costo e uno sforzo ragionevoli. SonarCloud considera il numero di problemi segnalati come “code smell” come indice della maintainability del progetto. Di seguito alcuni aspetti chiave che contribuiscono alla manutenibilità del codice:

- **Chiarezza e leggibilità:** il codice dovrebbe essere scritto in modo chiaro e leggibile in modo che sia facile da comprendere. L'uso di nomi di variabili e funzioni descrittivi, la formattazione coerente e i commenti appropriati possono contribuire a rendere il codice più leggibile.
- **Modularità:** suddividere il codice in moduli o componenti separati, ognuno dei quali ha una funzione ben definita, semplifica la gestione delle modifiche e delle correzioni. Questo principio è spesso chiamato "scomposizione" o "decomposizione" del codice.
- **Documentazione:** fornire documentazione chiara e aggiornata, inclusi commenti nel codice e documentazione esterna, può aiutare gli sviluppatori a comprendere il comportamento del software e come modificarlo correttamente.
- **Evitare complessità inutile:** mantenere il codice semplice ed evitare l'uso di strutture o tecniche complesse quando non sono necessarie può contribuire a migliorare la manutenibilità.
- **Gestione degli errori:** implementare una gestione degli errori efficace e coerente può rendere più semplice individuare e risolvere problemi nel software.
- **Versionamento del codice:** utilizzare sistemi di controllo del versionamento come Git per tenere traccia delle modifiche al codice e consentire il ripristino a versioni precedenti in caso di problemi.
- **Adeguata pianificazione e documentazione delle modifiche:** prima di apportare modifiche significative al codice, pianificare attentamente e documentare le modifiche in modo da evitare confusione e garantire che il team sia allineato sulle modifiche da apportare.

La manutenibilità del codice è un aspetto critico dello sviluppo software e richiede uno sforzo continuo da parte del team di sviluppo per mantenerla nel tempo. Investire tempo ed energie nella scrittura di codice mantenibile può risultare vantaggioso nel lungo termine, riducendo i costi e i rischi associati alla manutenzione del software.

Di seguito sono riportati i risultati relativi all'elaborazione dei dati estratti dagli applicativi analizzati, come mostrato nel capitolo 3.3, riferiti solo alla categoria maintainability:

Progetto	Righe di codice (k)	Code smell (k)	Code smell (k) normalizzati
Conam	137	4,7	0,034
Gestione Autorizzazioni	50	6,1	0,122
Rebus	220	6,7	0,030
Sportello Paesaggio	325	14	0,043
Sigea	123	8	0,065
Iuffi	276	17	0,062
Preference Center	66	18	0,273
Portale Allerta Meteo	406	21	0,052
Nova	32	4,3	0,134
Esenzione	77	6,3	0,082
Calamità Naturali	210	13,7	0,065

Elaborando questi dati, si evidenzia che l'obiettivo da raggiungere, fissato al primo quartile, corrisponde a un numero di code smell rimanenti associati al progetto pari a 9500. Di seguito vengono descritti alcune delle soluzioni attuate a risolvere i problemi segnalati:

- È stata ridotta la complessità di molti metodi. Per calcolare la complessità ciclomatica si utilizza il numero di cammini linearmente indipendenti nel codice. Diminuire la complessità di un metodo serve a migliorarne la comprensibilità, facilitarne il testing e il refactoring, riducendo inoltre il rischio di errori.
- Aggiunta la parola chiave "let", "const" o "var" alla dichiarazione di alcune variabili in javascript. L'omissione di queste keyword può portare alla creazione accidentale di variabili globali, il che può causare comportamenti inattesi e difficili da debuggare. Esplicitando le dichiarazioni, si riducono notevolmente le possibilità di errori di questo tipo. Inoltre, impedendo alle variabili di fuoriuscire dallo scope in cui sono state dichiarate, si evitano collisioni di nomi di variabili in contesti diversi all'interno dello stesso programma.
- Fusi tra loro due blocchi condizionali, migliorandone la leggibilità.
- Esplicitate le parentesi graffe nell' else. Non sempre è facile e immediato capire a che codice si riferisce l'else, quando più blocchi if/else sono annidati tra loro. Esplicitare le parentesi graffe rende il codice più chiaro.
- Sostituito il metodo size() con il metodo isEmpty() per testare se la collezione è vuota o meno. Entrambe le modalità sono funzionanti, tuttavia la complessità del metodo isEmpty() è O(1) mentre quella di size() è O(n), quindi meno performante.
- Riordinati i modificatori delle classi java, secondo le linee guida della documentazione di java. Non seguire questa convenzione non ha impatti tecnici, ma riduce la leggibilità del codice.

- Aggiunto il caso di default allo switch, fornendo un comportamento predefinito per situazioni impreviste o valori non attesi.
- Eliminato il metodo toString() utilizzato su una variabile già String.
- Eliminati dei blocchi di codice commentati.
- Eliminati alcuni parametri inutilizzati all'interno di metodi.
- Eliminate alcune variabili inutilizzate all'interno di metodi.
- Eliminati i blocchi di codice vuoti ({ }).
- Eliminato il cast non necessario da alcune variabili.
- Eliminato il commento contrassegnato con il TOFIX, perché il relativo codice era già stato corretto.
- Eliminato il commento contrassegnato con il TODO, perché il relativo codice era già stato scritto.

3.7 Pubblicazione del software sulla piattaforma

Pubblicare software su Developers Italia richiede il rispetto di determinate procedure e requisiti. Il processo è suddiviso in più fasi:

- Individuazione dello strumento di code hosting
- Scelta della licenza
- Individuazione e rilascio del materiale
- Rilascio del codice e organizzazione del repository
- File readme
- Documentazione
- Sicurezza
- Registrazione del repository su Developers Italia

Individuazione dello strumento di code hosting

L'Amministrazione titolare del software deve selezionare uno strumento di code hosting che soddisfi i seguenti requisiti tecnici minimi:

- Accesso al codice sorgente libero e senza autenticazione in lettura
- Registrazione libera e gratuita
- Interfaccia web per la navigazione e lettura sia del codice sia della relativa documentazione
- Utilizzo di un sistema di gestione delle versioni che supporti la creazione e la gestione di rami di sviluppo in parallelo.
- Un sistema di segnalazioni che consente la lettura pubblica senza richiedere autenticazione e l'invio di segnalazioni dietro autenticazione
- Disponibile al pubblico almeno un processo per l'invio di modifiche, la revisione del codice e l'integrazione delle modifiche, il tutto gestito completamente dalla piattaforma
- Sistema di gestione dei rilasci
- Disponibilità di API per la comunicazione e l'estrazione di dati e metadati dai repository

I seguenti strumenti di hosting del codice sono consigliati in quanto soddisfano questi requisiti e sono raccomandati a causa della loro ampia diffusione internazionale:

- GitHub
- BitBucket
- GitLab
- Phabricator/Phacility
- Gitea
- Gogs

Se il software rappresenta un lavoro derivato da un altro software open source già esistente, è consigliabile utilizzare la stessa piattaforma per sfruttare le sue funzionalità di collaborazione. Nel caso del progetto “Calamità Naturali” è stato utilizzato il repository GitHub preesistente appartenente alla regione Basilicata.

Scelta della licenza

La licenza da adottare deve essere specificata dall'Amministrazione nel capitolato o concordata successivamente, in conformità con le Linee Guida. L'Incaricato deve assicurare che questa licenza sia compatibile con quelle eventualmente utilizzate per componenti riutilizzati o incorporati, con o senza modifiche, per i quali non si detengono i diritti (ad esempio: librerie, asset grafici), compresi quelli di proprietà dell'Incaricato stesso. Se i componenti si trovano in file separati, è ammissibile conservare la licenza distinta, a condizione che ciò sia consentito dalle licenze e che i file stessi riportino in modo esplicito l'indicazione della licenza diversa e dei titolari dei diritti economici di sfruttamento. Per applicare la licenza selezionata al materiale da rilasciare, è necessario creare un file chiamato "LICENSE" nella radice del repository, contenente il testo integrale della licenza scelta, senza apportare alcuna modifica. Inoltre, è obbligatorio indicare la licenza applicata all'inizio di ciascun file sorgente tramite espressione (o codice) SPDX, al fine di consentire una facile automatizzazione della metadatazione delle licenze utilizzate. In conformità con l'articolo 69, comma 2 del Codice dell'Amministrazione Digitale, il detentore dei diritti da indicare nel codice sorgente è l'Amministrazione committente, che ne ha acquisito la titolarità. Una licenza di software libero consente l'utilizzo del codice sorgente correlato senza costi, ma impone determinati vincoli da rispettare. Di conseguenza, quando si desidera integrare più componenti di software libero rilasciati con licenze diverse, è necessario effettuare un'analisi per valutarne la compatibilità. Questa analisi può diventare particolarmente complessa se coinvolge diverse licenze, comportando costi aggiuntivi. In altre parole, l'uso di un'ampia varietà di licenze complica e rende più dispendioso il processo di riutilizzo del software, andando contro gli obiettivi stabiliti nell'articolo 69 del CAD. Di conseguenza, le linee guida su acquisizione e riuso del software per le pubbliche amministrazioni propongono il seguente albero decisionale per la selezione di una licenza aperta:

- Nel caso in cui il software venga rilasciato come una modifica di un software Open Source preesistente (cioè un software precedentemente utilizzato da un'altra amministrazione o di proprietà di terze parti), l'amministrazione adotterà la stessa licenza con cui il software è stato inizialmente distribuito. Questa scelta mira a promuovere l'interoperabilità ottimale e il riuso del software da parte di altri utenti che utilizzano la stessa soluzione.
- Nel caso di un software nuovo, l'amministrazione dovrebbe adottare la licenza EUPL v1.2. Questa licenza, sviluppata dalla Commissione europea, è stata selezionata perché

è una licenza “copyleft” che promuove l'interoperabilità a livello europeo ed è disponibile anche in italiano. Tuttavia, esistono alcune eccezioni a questa raccomandazione generale:
    - Nel caso in cui il software fosse principalmente utilizzato tramite rete, si dovrebbe adottare la licenza “GNU Affero General Public License” versione 3 e successive. Questa scelta è giustificata dal fatto che questa licenza, oltre ad essere compatibile con la maggior parte delle licenze Open Source, impone che chiunque modifichi il codice debba rilasciare tali miglioramenti, anche nel caso in cui il software venga utilizzato come parte di un servizio SaaS.
- Nel caso in cui vengano rilasciati componenti software isolati con un ampio campo di applicazione (ad esempio, librerie software o SDK), è consigliabile utilizzare la licenza “BSD 3-Clause”. Questa scelta è motivata dalla volontà di garantire un utilizzo il più libero possibile da parte di tutti gli attori, consentendo la creazione di applicazioni basate su queste librerie, che possono essere rilasciate sotto qualsiasi altra licenza. Questo tipo di componenti software è spesso utilizzato per favorire l'interoperabilità con le Pubbliche Amministrazioni e può contribuire alla creazione di ecosistemi che includono applicazioni di terze parti, compresi software proprietari.
- Per quanto riguarda la documentazione tecnica del software, si raccomanda l'utilizzo della licenza Creative Commons CC-BY 4.0. Questa licenza è stata selezionata per la sua capacità di agevolare il riutilizzo della documentazione e degli esempi di codice contenuti in essa, garantendo una maggiore accessibilità e condivisione delle informazioni.

Nel caso del progetto “Calamità Naturali” è stata utilizzata la licenza EUPL v1.2, in concordanza con l’albero decisionale.

Individuazione e rilascio del materiale

Sono soggetti all’obbligo di rilascio in open source i seguenti materiali:

- il codice sorgente
- la struttura del database
- gli script o altri materiali necessari per l'installazione in un ambiente di sviluppo o di produzione
- gli asset grafici generici, come bottoni e elementi grafici
- la documentazione destinata all'installazione delle dipendenze, alla compilazione e alla messa in funzione

Sono invece esclusi dall'obbligo di rilascio i seguenti elementi:

- i dati utilizzati in produzione o trattati con il software sviluppato
- gli asset grafici specifici, come i loghi delle aziende, su cui non si applica la licenza scelta

Rilascio del codice e organizzazione del repository

l codice sorgente deve essere distribuito integralmente in modo che chiunque, seguendo la documentazione, possa compilarlo e metterlo in funzione senza apportare modifiche. È essenziale mantenere i nomi delle variabili, delle funzioni, delle classi e degli altri simboli chiari e comprensibili. Inoltre, è vietata qualsiasi forma di compressione che possa compromettere la leggibilità del codice. Qualsiasi tentativo di offuscare il codice costituirà una violazione degli obblighi di distribuzione. Si consiglia l'adozione di un'architettura modulare, basata sulla suddivisione della logica in librerie specializzate e singolarmente riutilizzabili. È importante definire e documentare le API interne all'interno dei commenti del codice. Nel caso di integrazione di librerie esterne, si suggerisce di utilizzare un gestore di pacchetti al fine di semplificare la manutenzione e gli aggiornamenti. Il rilascio in open source non dovrebbe essere considerato solo come un adempimento da eseguire alla fine del processo di sviluppo. Dovrebbe essere pianificato sin dalla fase iniziale, ad esempio progettando il software in modo che tutte le informazioni specifiche dell'Amministrazione committente (come nomi, indirizzi e server) siano facilmente configurabili tramite file di configurazione. Inoltre, il software dovrebbe essere progettato in modo da essere riutilizzabile da altre parti interessate. Il repository dovrebbe essere organizzato con una struttura di directory chiara e intuitiva. Ad esempio, è consigliabile separare documentazione, librerie, eseguibili, script di servizio, test suite e così via in directory distinte.

File readme

È necessario includere nel repository un file denominato "README.md" che contenga:

- il titolo del repository ed un sottotitolo descrittivo
- la descrizione estesa del repository in un linguaggio comprensibile anche dai professionisti, specificando il contesto di utilizzo, le finalità del software, screenshot, link a pagine istituzionali del progetto, se presenti
- i link alla documentazione aggiuntiva non inclusa nel repository, se disponibile
- la spiegazione della struttura del repository
- l’elenco di tutti i prerequisiti e delle dipendenze come sistemi operativi, librerie, framework, con indicazione esplicita di possibili dipendenze da software commerciali
- le istruzioni per l’installazione, come la procedura per l’installazione di requisiti e dipendenze, build system, comandi per la compilazione o il deployment
- le indicazioni sullo status del progetto
- i link a eventuali sistemi di Continuous Integration (come TravisCI o CircleCI), copertura del codice e altre metriche correlate al repository
- la documentazione riguardante l'eventuale impiego di sistemi finalizzati ad agevolare e velocizzare il deployment in ambienti di sviluppo, test e produzione, come ad esempio

l'uso di immagini Docker o altri strumenti di virtualizzazione con immagini preconfigurate
- il nome dell’amministrazione detentrice di copyright
- il nome dell’azienda incaricata del mantenimento del progetto e, facoltativamente, è possibile aggiungere i nomi delle persone incaricate
- l’indirizzo e-mail al quale inviare le segnalazioni di sicurezza

Documentazione

- È indispensabile includere nella documentazione del software tutte le istruzioni necessarie a:
- installare le dipendenze
- creare un ambiente di sviluppo da zero, preferibilmente con l'aggiunta di script, immagini di container, Makefile o altri strumenti per semplificare il processo
- eseguire la compilazione del software, quando applicabile
- effettuare l'installazione del software in un ambiente di produzione
- fornire una chiara comprensione dell'architettura del software, a beneficio di terze parti interessate che desiderino riutilizzarlo o integrarlo

La documentazione allegata deve, inoltre, conformarsi alle direttive riguardanti la pubblicazione di documentazione tecnica delineate nelle Linee Guida di design per i servizi web della Pubblica Amministrazione e nella Guida a Docs Italia, entrambe pubblicate da AgID. Tale documentazione deve essere redatta in un formato testuale che consenta il controllo delle versioni a livello di riga (per esempio, sono accettati formati come HTML, Markdown, reStructuredText e LaTeX). Non saranno accettati documenti in formato ODT, DOCX o PDF, in quanto tali formati non permettono di gestire le diverse versioni a livello di riga. Nel caso in cui il capitolato richieda anche la creazione di documentazione destinata agli utenti finali, come un "manuale utente" o un documento simile, l'obbligo di rilascio si applica allo stesso modo. Per questo tipo di documentazione sono ammessi anche formati binari, a condizione che siano aperti, modificabili e compatibili con più piattaforme. Si precisa, quindi, che il formato PDF non è consentito.

Sicurezza

Considerando che la sicurezza del software rappresenta un aspetto di estrema importanza che va preso in considerazione durante l'intero ciclo di sviluppo, è opportuno sottolineare che questo documento non affronterà in dettaglio tali questioni. Tuttavia, verranno di seguito elencati alcuni principi basilari relativi a specifiche precauzioni da adottare nel processo di rilascio. È obbligatorio rimuovere dal codice sorgente qualsiasi riferimento a password, certificati o altre credenziali legate a sistemi reali, inclusi quelli di test. Per raggiungere questo obiettivo, è necessario utilizzare file di configurazione separati o

implementare una blacklist nel sistema di controllo di versione, come ad esempio il file .gitignore o .hgignore. Nel caso si desideri integrare il repository con un sistema di deployment automatico che richieda la conservazione di credenziali, è consentito l'utilizzo dei metodi di cifratura sicuri forniti dalla piattaforma di hosting del codice e dai sistemi di Continuous Integration adottati. È fondamentale assicurarsi che tali credenziali (come chiavi API, segreti, password, ecc.) non siano state accidentalmente caricate nel repository, sia nella versione attuale che nelle revisioni precedenti. È consigliabile evitare di riscrivere algoritmi che siano già presenti in librerie open source esterne. Questi algoritmi possono riguardare aree come la crittografia, la sanitizzazione dell'input, i protocolli di rete, il parsing di XML o altri formati, nonché la gestione della memoria, tra le altre cose. Inoltre, è obbligatorio rimuovere tutto il codice che non viene utilizzato, poiché la sua presenza potrebbe causare confusione o farlo erroneamente apparire come manutenuto, con il rischio di essere reintegrato senza i necessari controlli. Se il software è un'applicazione web accessibile tramite una rete pubblica o include applicazioni web, è altamente raccomandato rendere accessibile a ogni installazione un file situato all'indirizzo https://<nome-host>/.well-known/security.txt, con una formattazione conforme alle direttive reperibili sul sito https://securitytxt.org. Questo file è progettato per fornire informazioni rilevanti agli individui che scoprono vulnerabilità e intendono segnalare problemi di sicurezza.

Registrazione del repository su Developers Italia

Una volta che il repository pubblico è stato aperto, è essenziale procedere con la registrazione su Developers Italia. Questo passo assicura l'indicizzazione e la visibilità del repository nel motore di ricerca presente sul sito. La registrazione si completa in due semplici passaggi:

- Pubblicazione di un file denominato “publiccode.yml” nella directory principale del repository. Questo file è uno standard che identifica il progetto come “software utile per la Pubblica Amministrazione” e fornisce informazioni fondamentali per la valutazione e il potenziale riuso del software. L'indicizzatore (crawler) di Developers Italia rileverà automaticamente questo file e utilizzerà le informazioni al suo interno per generare una scheda dedicata nel catalogo.
- Aggiunta dello strumento di code-hosting al motore di ricerca. La prima volta che si utilizza questo strumento (o, più precisamente, quando si crea un'organizzazione all'interno dello stesso), è necessario registrarla e associarla alla Pubblica Amministrazione.

4 Studio dei tempi di refactoring

L'efficace gestione del debito tecnico è cruciale per garantire la salute a lungo termine dei progetti software. Nel contesto di questa sfida, strumenti come SonarCloud sono diventati un pilastro fondamentale per aiutare le aziende a identificare e affrontare i problemi, tuttavia un aspetto che spesso rimane in secondo piano è la precisione nella stima del tempo necessario per la loro correzione. L'obiettivo di questo studio è confrontare il tempo di riparazione effettivo con quello stimato per valutare l'accuratezza dei tempi di riparazione del debito tecnico forniti da SonarCloud.
In quest'analisi si è fatto uso di diverse metriche:

- Mean(RE) o errore relativo medio, definito nel seguente modo:

$$Mean(RE) = \frac{1}{n}\sum_{i=1}^{n} RE_i$$

  dove n indica il numero di problemi risolti mentre RE_i si riferisce all'errore relativo associato alla stima dei tempi di risoluzione dell'i-esimo problema ed è definito come:

$$RE_i = \frac{tempo\_misurato - tempo\_stimato}{tempo\_misurato}$$

  Buone stime sono caratterizzate da un valore basso di Mean(RE), tuttavia può succedere che i valori positivi di RE_i siano bilanciati da valori negativi. Quando ciò accade, un valore basso di Mean(RE) potrebbe non implicare buone stime. Valori positivi di Mean(RE) indicano che, in media, il tempo di riparazione suggerito da SonarCloud è sottostimato. D'altra parte, valori negativi di Mean(RE) indicano che, in media, tale tempo di riparazione è sovrastimato.
- MMRE o media del valore assoluto degli errori relativi, definito nel seguente modo:

$$MMRE = \frac{1}{n}\sum_{i=1}^{n} MRE_i$$

  dove n indica il numero di problemi risolti mentre MRE_i si riferisce al modulo dell'errore relativo associato alla stima dei tempi di risoluzione dell'i-esimo problema ed è definito come:

$$MRE_i = \frac{|tempo\_misurato - tempo\_stimato|}{tempo\_misurato}$$

  Se il valore di MMRE è piccolo, allora SonarCloud dovrebbe produrre, in media, buone stime. Vale la pena notare che MMRE può essere influenzato da casi con picchi molto elevati di MRE_i.
- MdMRE, definita come la mediana del valore assoluto degli errori relativi. Metrica utilizzata per limitare l'impatto dei valori molto alti di MRE. Minore è questo valore, migliori sono le stime.

- PRED25, definita come percentuale delle stime con $MRE_i < 0.25$. In altre parole, questa metrica misura la percentuale di stime che hanno un errore relativo minore del 25%. Maggiore questo valore, migliori sono le stime.
- PRED50, definita come percentuale delle stime con $MRE_i < 0.50$. In altre parole, questa metrica misura la percentuale di stime che hanno un errore relativo minore del 50%. Maggiore questo valore, migliori sono le stime.

Queste metriche misurano diverse proprietà del modello predittivo. Utilizzarle per valutare la precisione delle stime del tempo di riparazione dovrebbe permetterci di ottenere una comprensione più approfondita e accurata dell'attendibilità delle stime stesse, mitigando il rischio di un bias legato all'utilizzo di una singola metrica.
L'analisi è stata condotta sui tempi di correzione dei bug associati agli indicatori "bug" e "code smell". Non è stata effettuata sull'indicatore "security" poiché sono presenti solamente tre vulnerabilità di sicurezza, numero troppo limitato per condurre un'analisi significativa.

Tipo di vulnerabilità	Mean(RE)	MMRE	MdMRE	PRED25	PRED50
Bug	-0.81	0.83	0.67	23%	28%
Code smell	-1.09	1.11	0.67	41%	43%

I risultati associati ad entrambi gli indicatori sembrano convergere e indicano che le stime fornite da SonarCloud non sono accurate. Il tempo di risoluzione del debito tecnico stimato è, in generale, sopravvalutato. Questo è possibile dedurlo dal segno negativo di Mean(RE). Inoltre, il valore di MMRE è molto simile a quello di Mean(RE), suggerendo che la presenza di casi in cui il tempo di riparazione è stato sovrastimato è molto maggiore dei casi in cui il tempo di riparazione è stato sottostimato. L'analisi della MdMRE conferma che le stime presentano errori significativi. È interessante notare che i code smell mostrano dei picchi di valore più altri rispetto ai bug, il cui impatto viene limitato dal calcolo della mediana. Infine, esaminando le metriche PRED25 e PRED50, emerge che le stime dei tempi relativi ai code smell sono più precise rispetto a quelle relative ai bug. La prossimità tra questi due valori suggerisce che le stime dei tempi siano abbastanza accurate in una parte dei casi (23%per i bug e 41% per i code smell) e decisamente inaccurate in una parte più grande, senza la presenza di una zona mediamente accurata.
In prospettiva futura, sarebbe estremamente interessante condurre una replica dello studio, ampliando il campione di applicativi considerati come riferimento e utilizzando una varietà più ampia di strumenti di analisi statica del codice. Questo approccio consentirebbe di effettuare un confronto approfondito dei risultati ottenuti da ciascun tool utilizzato, contribuendo così a migliorare la comprensione delle differenze e delle similitudini tra le diverse metodologie di analisi e fornendo una visione più completa e rappresentativa delle tendenze.

5 Conclusioni

La trasformazione digitale rappresenta una delle più significative prospettive del terzo millennio per la nostra società. Nonostante siano stati già compiuti notevoli progressi, vi è ancora molto lavoro da svolgere. Nel prossimo futuro il digitale potrebbe effettivamente trasformare l'Italia in un paese notevolmente migliorato, caratterizzato da infrastrutture solide, una pubblica amministrazione più digitalizzata e interconnessa, un settore produttivo più competitivo e appetibile per gli investitori nazionali ed internazionali, un sistema sanitario più resistente ed un sistema educativo moderno, sostenitore di una vera Repubblica Digitale. Tuttavia, nonostante i considerevoli progressi compiuti grazie al Codice dell'Amministrazione Digitale, restano alcune sfide aperte. La digitalizzazione ha introdotto nuove questioni relative alla sicurezza informatica e alla tutela della privacy, pertanto è di fondamentale importanza che l'amministrazione pubblica continui a investire in misure di sicurezza e monitori attentamente l'uso dei dati. La protezione dei dati personali e la prevenzione delle minacce cibernetiche devono rimanere al centro dell'agenda digitale italiana.
L'accelerata evoluzione tecnologica richiede un costante aggiornamento del CAD per adattarlo alle nuove sfide e opportunità. La collaborazione tra il settore pubblico, il settore privato e la società civile è essenziale per sviluppare politiche e normative in grado di guidare l'innovazione e la modernizzazione dell'amministrazione pubblica italiana. Solo attraverso la cooperazione sinergica sarà possibile proseguire lungo questo percorso che richiede impegno e una visione a lungo termine.

Sitografia

https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rules_it

https://developers.italia.it/it/come-lo-uso

https://developers.italia.it/it/riuso/pubblicazione

https://innovazione.gov.it/italia-digitale-2026/il-piano/digitalizzazione-della-pa/

https://innovazione.gov.it/progetti/developers-italia

https://it.wikipedia.org/wiki/Agenzia_per_l%27Italia_digitale

https://it.wikipedia.org/wiki/Digital_transformation

https://it.wikipedia.org/wiki/Regolamento_generale_sulla_protezione_dei_dati

https://protezionedatipersonali.it/regolamento-generale-protezione-dati

https://www.agendadigitale.eu/documenti/codice-dellamministrazione-digitale-cose-e-quali-sono-i-punti-principali-da-conoscere/

https://www.agid.gov.it/it/agenzia/chi-siamo

https://www.agid.gov.it/it/agenzia/strategia-quadro-normativo/codice-amministrazione-digitale

https://www.agid.gov.it/it/design-servizi/linee-guida-design-servizi-digitali-pa

https://www.agid.gov.it/it/design-servizi/riuso-open-source/linee-guida-acquisizione-riuso-software-pa

https://www.agid.gov.it/it/infrastrutture/sistema-pubblico-connettivita/il-nuovo-modello-interoperabilita

https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

https://www.agid.gov.it/sites/default/files/repository_files/design-linee-guida-docs.pdf

https://www.agid.gov.it/sites/default/files/repository_files/documentazione/misure_minime_di_sicurezza_v.1.0.pdf

https://www.agid.gov.it/sites/default/files/repository_files/lg_infrastruttura_interoperabilita_pdnd.pdf

https://www.agid.gov.it/sites/default/files/repository_files/lg_punto_accesso_telematico_servizi_pa_3112021.pdf

https://www.agid.gov.it/sites/default/files/repository_files/lg-acquisizione-e-riuso-software-per-pa-docs_pubblicata.pdf

https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_interoperabilit_tecnica_pa.pdf

https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_tecnologie_e_standard_sicurezza_interoperabilit_api_sistemi_informatici.pdf

https://www.astrid-online.it/static/upload/protected/cnip/cnipa_quad_38_int.pdf

https://www.docenti.unina.it/webdocenti-be/allegati/materiale-didattico/270191

https://www.forumpa.it/pa-digitale/riuso-di-buone-pratiche-e-di-software-come-e-perche-usarlo-per-rinnovare-la-pa/

https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Considerando+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale++dell%27Unione+europea+127+del+23+maggio+2018

https://www.i-com.it/2022/08/26/transizione-digitale-litalia-accelera-ma-resta-il-nodo-delle-competenze