



Comune di SAN SPERATE

Città Metropolitana di Cagliari

Piano triennale per l'Informatica 2024-2026 del Comune di San Sperate

Riferimento al Piano triennale per l'informatica 2024-2026 pubblicato da AGID
a cura del Servizio Informatico Comunale e del Responsabile della transizione digitale

San Sperate, maggio 2026

Sommario

INTRODUZIONE AL PIANO TRIENNALE.....	5
Struttura e articolazione del Piano Triennale	5
Obiettivi del Piano Triennale.....	6
Principi guida	8
Contesto Nazionale.....	9
PARTE I^a – COMPONENTI STRATEGICHE	12
Capitolo 1 - Organizzazione e gestione del cambiamento	12
Struttura e organizzazione dell'Ente.....	12
Resoconto dei finanziamenti PNRR.....	14
Ruolo del Responsabile e dell'Ufficio per la Transizione Digitale	18
Obiettivo 1.1 – Migliorare i processi di trasformazione digitale della PA.....	21
Competenze digitali per il Paese e per la PA	22
Obiettivo 1.2 – Diffusione competenze digitali nel Paese e nella PA.....	25
Monitoraggio	26
Obiettivo 1.3 – Monitorare e analizzare lo stato di digitalizzazione del paese	28
Capitolo 2 - Il procurement per la trasformazione digitale.....	29
Il procurement per la trasformazione digitale.....	29
Gli acquisti di beni e servizi standardizzati	29
Gli acquisti di innovazione per la trasformazione digitale.....	30
L'ecosistema digitale degli acquisti pubblici	30
Organizzazione della stazione appaltante nel nuovo Codice dei Contratti Pubblici.....	31
La qualificazione della Stazione appaltante	32
L'organizzazione della Stazione appaltante e il ruolo del RUP	32
La collaborazione tra stazioni appaltanti	33
Obiettivo 2.1 – Rafforzare l'ecosistema nazionale di approvvigionamento digitale	34
Obiettivo 2.2 – Diffondere l'utilizzo degli appalti innovativi.....	35
Le gare strategiche per la trasformazione digitale	35
Obiettivo 2.3 – Favorire e monitorare l'utilizzo dei servizi previsti dalle Gare strategiche	37
PARTE II^a – LE COMPONENTI TECNOLOGICHE	38
Descrizione PARTE SECONDA.....	38
Capitolo 3 - Servizi	38
Introduzione al Capitolo.....	38
E-Service in interoperabilità tramite PDND	39
Obiettivo 3.1 – Migliorare la capacità di erogare e-service	42

Progettazione dei servizi: accessibilità e design	43
Obiettivo 3.2 – Migliorare la capacità di generare e erogare e-service	45
Formazione, gestione e conservazione dei documenti informatici	46
Obiettivo 3.3 – Consolidare l'applicazione delle Linee guida per la formazione, gestione e conservazione documentale	48
Single Digital Gateway	49
Obiettivo 3.4 – SDG (Single Digital Gateway) - Monitorare e migliorare la qualità e l'accesso ai servizi digitali offerti dallo Sportello per l'Italia	50
Capitolo 4 - Piattaforme	52
Introduzione al Capitolo.....	52
Piattaforme nazionali che erogano servizi a cittadini/imprese o ad altre PA.....	52
Obiettivo 4.1 – Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA	61
Piattaforme che attestano attributi.....	65
Obiettivo 4.2 – Ottenere la piena interoperabilità tra le piattaforme	69
Basi dati interesse nazionale.....	70
Obiettivo 4.3 – Migliorare la sicurezza, accessibilità e l'interoperabilità delle basi dati di interesse nazionale	70
Capitolo 5 – Dati e Intelligenza Artificiale	72
Open data e data governance.....	72
Obiettivo 5.1 – Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese	77
Obiettivo 5.2 – Aumentare la qualità dei dati e dei metadati	78
Obiettivo 5.3 – Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati	79
Intelligenza artificiale per la Pubblica Amministrazione.....	80
Ambienti di sperimentazione e sviluppo	82
Principi generali per l'utilizzo dell'intelligenza artificiale nella Pubblica Amministrazione	82
Dati per l'intelligenza artificiale	84
Obiettivo 5.4 – Aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale	85
Obiettivo 5.5 – Dati per l'intelligenza artificiale	86
Capitolo 6 – Infrastrutture	87
Infrastrutture digitali e Cloud	87
Punti di attenzione e azioni essenziali per tutti gli enti	92
Approfondimento tecnologico per gli RTD	92

Obiettivo 6.1 – Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la strategia «Cloud Italia» e migrando verso infrastrutture e servizi cloud qualificati (incluso PSN)	95
Il sistema pubblico di connettività	97
Obiettivo 6.2 – Garantire alle amministrazioni la disponibilità della connettività SPC	97
Capitolo 7 – Sicurezza informatica	98
Sicurezza informatica	98
Obiettivo 7.1 – Adottare una governance della cybersicurezza diffusa nella PA	100
Obiettivo 7.2 – Gestire i processi di approvvigionamento IT coerentemente con i requisiti di sicurezza definiti	101
Obiettivo 7.3 – Gestione e mitigazione del rischio cyber	101
Obiettivo 7.4 – Potenziare le modalità di prevenzione e gestione degli incidenti informatici	102
Obiettivo 7.5 – Implementare attività strutturate di sensibilizzazione cyber del personale	103
Obiettivo 7.6 – Contrastare il rischio cyber attraverso attività di supporto proattivo alla PA	104
APPENDICE 1. Definizioni e Acronimi	105
APPENDICE 2. Crediti e versioni	106

INTRODUZIONE AL PIANO TRIENNALE

Struttura e articolazione del Piano Triennale

Il Piano Triennale, sia esso alla sua prima stesura o un aggiornamento, è strutturato in tre parti principali:

- **Introduzione** – struttura, obiettivi, riferimenti e contesto nazionale.
- Parte Prima - **Componenti strategiche per la trasformazione digitale**: è articolata in due capitoli che descrivono le leve strategiche su cui investire per accelerare il processo di trasformazione digitale delle PA, focalizzando l'attenzione su un approccio innovativo che affronti, in maniera sistematica, tutti gli aspetti legati a organizzazione, processi, regole, dati e tecnologie.
- Parte seconda – **Componenti tecnologiche**: le componenti tecnologiche del modello strategico sono riportate nei capitoli su Servizi, Piattaforme, Dati e intelligenza artificiale, Infrastrutture, Sicurezza. Il tema dell'interoperabilità diventa trasversale a tutti i capitoli ed è evidenziato in particolare nel capitolo dedicato ai Servizi. Il capitolo "Dati" è integrato da una sezione nuova dedicata all'intelligenza artificiale. Sono riportati alcuni principi generali che dovranno essere adottati e declinati in fase di applicazione, tenendo in considerazione lo scenario in veloce evoluzione.

Per ogni macrosezione sopra descritta verrà replicato il modello del Piano Triennale proposto da AGID, ovvero per ogni componente verranno evidenziati:

- lo Scenario introduce brevemente i temi affrontati nel capitolo, illustra lo stato dell'arte in raccordo con i Piani precedenti e offre un'anteprima delle traiettorie future, evidenziando anche i relativi punti di attenzione ed azioni essenziali utili a tutti gli enti;
- il Contesto normativo e strategico elenca i riferimenti, eventualmente aggiornati, a cui le amministrazioni devono attenersi, in termini di fonti normative con link a documenti e/o siti ufficiali e riferimenti ad attività progettuali finanziate, compresi i riferimenti agli specifici investimenti del PNRR;
- le sezioni Obiettivi e Risultati attesi descrivono i macro-obiettivi del Piano sul tema specifico e, per ciascun obiettivo individuano i risultati attesi (RA) e relativi target annuali per il triennio 2024-2026;
- le Linee di Azione ovvero le attività a carico dell'Ente

Obiettivi del Piano Triennale

L'AGID, nelle more di emanare le linee guida necessarie, e supportare gli Enti nella stesura del proprio piano Triennale, ha catalogato e ottimizzato gli **obiettivi** del Piano Triennale attraverso un sistema di tassonomie condiviso. Tali obiettivi sono a loro volta classificati e inseriti in macro-categorie chiamate "capitoli". Essi guideranno l'azione amministrativa di digitalizzazione del nostro Ente:

Capitolo 1 - Organizzazione e gestione del cambiamento

- Obiettivo 1.1 - Migliorare i processi di trasformazione digitale della PA
- Obiettivo 1.2 - Diffusione competenze digitali nel Paese e nella PA
- Obiettivo 1.3 - Monitorare e analizzare lo stato di digitalizzazione del paese

Capitolo 2 - Il procurement per la trasformazione digitale

- Obiettivo 2.1 - Rafforzare l'ecosistema nazionale di approvvigionamento digitale
- Obiettivo 2.2 - Diffondere l'utilizzo degli appalti innovativi
- Obiettivo 2.3 - Favorire e monitorare l'utilizzo dei servizi previsti dalle Gare strategiche

Capitolo 3 – Servizi

- Obiettivo 3.1 - Migliorare la capacità di erogare e-service
- Obiettivo 3.2 - Migliorare la capacità di generare ed erogare servizi digitali
- Obiettivo 3.3 - Consolidare l'applicazione delle Linee guida per la formazione, gestione e conservazione documentale
- Obiettivo 3.4 - SDG (Single Digital Gateway) - Monitorare e migliorare la qualità e l'accesso ai servizi digitali offerti dallo Sportello per l'Italia

Capitolo 4 – Piattaforme

- Obiettivo 4.1 - Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA
- Obiettivo 4.2 - Ottenere la piena interoperabilità tra le piattaforme
- Obiettivo 4.3 - Migliorare la sicurezza, accessibilità e l'interoperabilità delle basi dati di interesse nazionale

Capitolo 5 - Dati e Intelligenza Artificiale

- Obiettivo 5.1 - Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese
- Obiettivo 5.2 - Aumentare la qualità dei dati e dei metadati
- Obiettivo 5.3 - Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati
- Obiettivo 5.4 - Aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale
- Obiettivo 5.5 - Dati per l'intelligenza artificiale

Capitolo 6 – Infrastrutture

- Obiettivo 6.1 - Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la strategia “Cloud Italia” e migrando verso infrastrutture e servizi Cloud qualificati (incluso PSN)
- Obiettivo 6.2 - Garantire alle amministrazioni la disponibilità della connettività SPC

Capitolo 7 - Sicurezza informatica

- Obiettivo 7.1 - Adottare una governance della cybersicurezza diffusa nella PA
- Obiettivo 7.2 - Gestire i processi di approvvigionamento IT coerentemente con i requisiti di sicurezza definiti
- Obiettivo 7.3 - Gestione e mitigazione del rischio cyber
- Obiettivo 7.4 - Potenziare le modalità di prevenzione e gestione degli incidenti informatici
- Obiettivo 7.5 - Implementare attività strutturate di sensibilizzazione cyber del personale
- Obiettivo 7.6 - Contrastare il rischio cyber attraverso attività di supporto proattivo alla PA

Il Comune di San Sperate, nelle more di redigere una propria versione del Piano Triennale per l'informatica che sia aderente a quanto indicato dall'AGID, provvederà ad affrontare quanti più obiettivi possibili del presente schema. Non tutti gli obiettivi possono essere perseguiti dal nostro Ente, in quanto alcuni riguardano altre tipologie di AOO.

Principi guida

I seguenti principi guida emergono dal quadro normativo e sono da tenere presenti ad ogni livello decisionale e in ogni fase di implementazione, naturalmente declinandoli nello specifico della missione istituzionale di ogni ente pubblico.

- **Digital & mobile first** (digitale e mobile come prima opzione): le pubbliche amministrazioni devono erogare i propri servizi pubblici in digitale e fruibili su dispositivi mobili, considerando alternative solo in via residuale e motivata, attraverso la «riorganizzazione strutturale e gestionale» dell'ente ed anche con una «costante semplificazione e reingegnerizzazione dei processi»;
- **Digital Identity only** (accesso esclusivo mediante identità digitale): le PA devono adottare in via esclusiva sistemi di identità digitale definiti dalla normativa assicurando l'accesso tramite SPID/CIE/CNS;
- **Once only e transfrontaliero**: le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite, devono dare accesso ai loro fascicoli digitali e devono rendere disponibili a livello transfrontaliero i servizi pubblici rilevanti;
- **Cloud first**: le pubbliche amministrazioni, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano primariamente il paradigma cloud, e utilizzano esclusivamente infrastrutture digitali adeguate e servizi cloud qualificati secondo i criteri fissati da ACN e nel quadro del SPC;
- **Servizi inclusivi e accessibili**: le pubbliche amministrazioni devono progettare servizi pubblici digitali che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori;
- **dati pubblici un bene comune** (open data by design e by default): il patrimonio informativo della pubblica amministrazione è un bene fondamentale per lo sviluppo del Paese e deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile;
- **interoperabile by design**: i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e attraverso processi digitali collettivi a prescindere dai canali di erogazione del servizio che sono individuati logicamente e cronologicamente dopo la progettazione dell'interfaccia API;
- **sicurezza e privacy by design**: i servizi digitali devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali;
- **user-centric, data driven e agile**: le pubbliche amministrazioni devono progettare servizi pubblici che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo;
- **open source**: le pubbliche amministrazioni devono tenere conto della necessità di prevenire il rischio di lock-in nei propri servizi, prediligere l'utilizzo di software con

codice aperto o di e-service e, nel caso di software sviluppato per loro conto, deve essere reso disponibile il codice sorgente, nonché promuovere l'amministrazione aperta e la condivisione di buone pratiche sia amministrative che tecnologiche;

- **sostenibilità digitale:** le pubbliche amministrazioni devono considerare l'intero ciclo di vita dei propri servizi e la relativa sostenibilità economica, territoriale, ambientale e sociale, anche ricorrendo a forme di aggregazione;
- **sussidiarietà, proporzionalità e appropriatezza della digitalizzazione:** I processi di digitalizzazione dell'azione amministrativa coordinati e condivisi sono portati avanti secondo i principi di sussidiarietà, proporzionalità e appropriatezza della digitalizzazione, ovvero lo Stato deve intraprendere iniziative di digitalizzazione solo se sono più efficaci di quelle a livello regionale e locale, e in base alle esigenze espresse dalle amministrazioni stesse, limitandosi negli altri casi a quanto necessario per il coordinamento informatico dei dati, e al tempo stesso le singole amministrazioni devono garantire l'appropriatezza delle iniziative di digitalizzazione portate avanti autonomamente, cioè in forma non condivisa con altri enti al livello territoriale ottimale rispetto alle esigenze preminenti dell'azione amministrativa e degli utenti dei servizi pubblici.

Contesto Nazionale

Le sfide che aspettano il sistema Paese nei prossimi anni sono di sicuro rilievo e riguarderanno sicuramente la trasformazione del Paese verso nuovi orizzonti in termini di digitalizzazione, transizione ecologica, mobilità sostenibile, istruzione, inclusione e coesione sociale e salute, tutti obiettivi delle linee di sviluppo e investimento individuate dall'UE per il rilancio dell'economia e della vita in Europa. Resta infatti centrale la necessità di rivedere l'organizzazione dei processi confermando come i servizi digitali e l'informatizzazione siano un perno della trasformazione digitale del Paese.

I cambiamenti da attuare sono accompagnati da nuove normative e nuove opportunità che aiuteranno il Paese a proseguire nella direzione di trasformazione digitale già iniziata. Il Piano Triennale si pone infatti come sintesi tra le varie linee di trasformazione digitale della Pubblica Amministrazione.

In particolare, il **Piano Nazionale di Ripresa e Resilienza (PNRR)** è lo strumento che, grazie ai fondi del **Next Generation Europe EU**, si sviluppa intorno a tre assi strategici condivisi a livello europeo tra cui quello della digitalizzazione e innovazione. Il PNRR prevede in particolare nella componente denominata "Digitalizzazione, innovazione e sicurezza nella PA" grandi investimenti pubblici. Questa misura contribuirà in maniera determinante a supportare la strategia di digitalizzazione in corso, erogando finanziamenti per progetti specifici che dovranno necessariamente essere concepiti in armonia con le disposizioni del CAD e di tutte le altre normative e linee guida pubblicate.

A livello nazionale, la **Strategia Italia digitale 2026**, si concentra da un lato sulle infrastrutture digitali e la connettività a banda ultra-larga e, dall'altro su quegli interventi volti a trasformare la Pubblica Amministrazione in chiave digitale. Come specificato nella Strategia, i due assi sono necessari per garantire a tutti i cittadini un accesso a connessioni veloci e per migliorare il rapporto tra cittadino e pubblica amministrazione. Gli interventi hanno come traguardo:

- la diffusione dell'identità digitale
- la riduzione del gap di competenze digitali
- l'incremento dell'uso dei servizi in cloud da parte della PA
- la crescita dell'erogazione dei servizi digitali essenziali erogati online
- il completamento delle reti a banda ultra- larga su tutto il territorio nazionale.

Gli scopi del Piano Triennale sono definiti principalmente da:

Decreto legislativo 7 marzo 2005, n. 82 (**Codice dell'Amministrazione Digitale - CAD**):

- Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di uguaglianza e di non discriminazione, nonché per l'effettivo riconoscimento dei diritti dei cittadini e delle imprese di cui al presente Codice in conformità agli obiettivi indicati nel Piano triennale per l'informatica nella Pubblica Amministrazione di cui all'articolo 14-bis, comma 2, lett. b) (..)
- Le pubbliche amministrazioni utilizzano, nei rapporti interni, in quelli con altre amministrazioni e con i privati, le tecnologie dell'informazione e della comunicazione, garantendo l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni nel rispetto delle Linee guida.
- Le pubbliche amministrazioni operano per assicurare l'uniformità e la graduale integrazione delle modalità di interazione degli utenti con i servizi informatici (..) da esse erogati, qualunque sia il canale di erogazione, nel rispetto dell'autonomia e della specificità di ciascun erogatore di servizi. (..)

Agenzia per l'Italia digitale, come definito nell'art. 14-bis del CAD, essa svolge funzioni di:

- emanazione di Linee guida contenenti regole, standard e guide tecniche, nonché di indirizzo, vigilanza e controllo sull'attuazione e sul rispetto delle norme di cui al presente Codice, anche attraverso l'adozione di atti amministrativi generali, in materia di agenda digitale, digitalizzazione della Pubblica Amministrazione, sicurezza informatica, interoperabilità e cooperazione applicativa tra sistemi informatici pubblici e quelli dell'Unione europea;
- programmazione e coordinamento delle attività delle amministrazioni per l'uso delle tecnologie dell'informazione e della comunicazione, mediante la redazione e la successiva verifica dell'attuazione del Piano triennale per l'informatica nella Pubblica

Amministrazione contenente la fissazione degli obiettivi e l'individuazione dei principali interventi di sviluppo e gestione dei sistemi informativi delle amministrazioni pubbliche. Il predetto Piano è elaborato dall'AGID, anche sulla base dei dati e delle informazioni acquisiti dai soggetti di cui all'articolo 2, comma 2, ed è approvato dal Presidente del Consiglio dei ministri o dal Ministro delegato entro il 30 settembre di ogni anno (...)

Legge 28 dicembre 2015, n. 208 (**legge di stabilità 2016**) Art. 1.:

- Comma 512. Al fine di garantire l'ottimizzazione e la razionalizzazione degli acquisti di beni e servizi informatici e di connettività, fermi restando gli obblighi di acquisizione centralizzata previsti per i beni e servizi dalla normativa vigente, le amministrazioni pubbliche e le società inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1 della legge 31 dicembre 2009, n. 196, provvedono ai propri approvvigionamenti esclusivamente tramite Consip SpA o i soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi soggetti. (..)
- Comma 513. L'Agenzia per l'Italia digitale (AGID) predispone il Piano triennale per l'informatica nella Pubblica Amministrazione che è approvato dal Presidente del Consiglio dei Ministri o dal Ministro delegato. Il Piano contiene, per ciascuna amministrazione o categoria di amministrazioni, l'elenco dei beni e servizi informatici e di connettività e dei relativi costi, suddivisi in spese da sostenere per innovazione e spese per la gestione corrente, individuando altresì i beni e servizi la cui acquisizione riveste particolare rilevanza strategica.
- Comma 514. Ai fini di cui al comma 512, Consip SpA o il soggetto aggregatore interessato, sentita l'AGID per l'acquisizione dei beni e servizi strategici indicati nel Piano triennale per l'informatica nella Pubblica Amministrazione di cui al comma 513, programma gli acquisti di beni e servizi informatici e di connettività, in coerenza con la domanda aggregata di cui al predetto Piano. (..) Consip SpA e gli altri soggetti aggregatori promuovono l'aggregazione della domanda funzionale all'utilizzo degli strumenti messi a disposizione delle pubbliche amministrazioni su base nazionale, regionale o comune a più amministrazioni.

PARTE I^a – COMPONENTI STRATEGICHE

Capitolo 1 - Organizzazione e gestione del cambiamento

Struttura e organizzazione dell'Ente

Il Comune di SAN SPERATE è l'Ente Locale che amministra il territorio urbano della Città di San Sperate. La struttura amministrativa del Comune è articolata su 5 aree così suddivise:

- Area 1 - Amministrativa, Servizi Generici e alla Persona
- Area 2 - Finanziaria Contabile ed Economica
- Area 3 - Vigilanza e Demografici
- Area 4 - Tecnica e Assetto del Territorio
- Area 5 - Manutentiva e Lavori Pubblici

Il servizio Informatico Comunale, ovvero il servizio che tra l'altro si occupa anche della stesura del presente piano triennale, si trova inquadrato all'interno dell'Area 1 ed è composto da due sole figure: il Responsabile – Dott.ssa Iride Atzori – e l'istruttore informatico, Alberto Mameli.

Il comune di San Sperate ha una dotazione organica pari a 39 dipendenti di ruolo oltre il Segretario Comunale. Tutti i dipendenti, il Segretario e gli organi politici utilizzano delle postazioni di lavoro con le quali si interfacciano agli strumenti applicativi (con diversi profili di accesso e privilegi in base al proprio ruolo nell'Ente).

Il presente Piano Triennale per l'Informatica è stato sviluppato per rispondere alle esigenze specifiche del comune di San Sperate, al fine di migliorare l'efficienza e l'efficacia dell'amministrazione pubblica locale attraverso l'uso delle tecnologie dell'informazione e della comunicazione.

Il Piano Triennale ICT per il triennio riprende quanto previsto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione di **AGID** 2022-2024 e lo integra con le linee programmatiche di mandato dell'attuale Amministrazione Comunale, e con gli indirizzi strategici e le aree di intervento, delle diverse missioni del bilancio e del DUP che individuano la digitalizzazione quale missione strategica.

La redazione del documento risponde al compito individuato nella Circolare 3/2018 del Ministero della Pubblica Amministrazione, al punto e) *“competenza del U-RTD in materia di predisposizione del Piano triennale per l'informatica della singola amministrazione, nelle forme e secondo le modalità definite dall'Agenzia per l'Italia digitale”*.

Il presente Piano Triennale per l'Informatica 2024-2026 per il Comune di San Sperate si propone di promuovere la modernizzazione, l'efficienza e la trasparenza dell'amministrazione pubblica locale attraverso l'uso delle tecnologie dell'informazione e della comunicazione. L'adozione di soluzioni digitali consentirà al comune di offrire servizi più accessibili e convenienti per i cittadini, migliorando complessivamente la qualità della vita all'interno della comunità.

Gli obiettivi strategici da raggiungere con il Piano comprendono:

1. Modernizzazione dell'amministrazione pubblica: Promuovere l'adozione di strumenti digitali per semplificare e automatizzare i processi amministrativi, migliorando l'accessibilità e la qualità dei servizi offerti ai cittadini.
2. Digitalizzazione dei servizi: Offrire servizi pubblici online, consentendo ai cittadini di interagire con l'amministrazione comunale in modo rapido e conveniente, riducendo la necessità di spostamenti fisici e di conseguenza generando valore pubblico.
3. Sicurezza dei dati: Garantire la protezione dei dati sensibili dei cittadini e dell'amministrazione comunale attraverso l'implementazione di misure di sicurezza informatica adeguate.
4. Partecipazione e trasparenza: Favorire la partecipazione dei cittadini alla vita amministrativa, fornendo strumenti per la consultazione e la condivisione di informazioni sui progetti e le decisioni del comune.
5. Sviluppo dell'innovazione: Promuovere la cultura dell'innovazione all'interno dell'amministrazione comunale, incoraggiando la sperimentazione di nuove tecnologie e soluzioni digitali per migliorare i servizi offerti.

Scopo dell'Amministrazione è quello di dare seguito al potenziamento digitale ottenuto grazie alle risorse PNRR sotto indicate, prevedendo budget di spesa sufficienti per il mantenimento delle soluzioni tecnologiche avviate e l'attivazione di nuove soluzioni digitali atte alla semplificazione e al miglioramento dell'attività amministrativa.

La situazione attuale relativa ai finanziamenti PNRR ottenuti è riassunto nella seguente tabella in cui viene indicata la misura, il finanziamento ottenuto e lo stato di applicazione e realizzazione della misura stessa.

Codice	Misura PNRR	Finanziamento	Stato attuale
1.2	Abilitazione al Cloud	€ 83.044,00	CONCLUSO
1.4.1	Esperienza del Cittadino	€ 51.654,00	CONCLUSO
1.4.3	pagoPA	€ 4.285,00	CONCLUSO
1.4.3	app IO	€ 6.860,00	CONCLUSO
1.4.4	SPID CIE	€ 14.000,00	CONCLUSO
1.4.4	ANPR ANSC	€ 8.979,20	CONCLUSO
1.4.5	Notifiche Digitali	€ 32.589,00	CONCLUSO
1.3.1	PDND - ANNCSU	€ 9.506,14	IN FASE DI VERIFICA

Nei successivi paragrafi verranno approfondite tali informazioni.

Resoconto dei finanziamenti PNRR

Come indicato nei paragrafi precedenti il PNRR prevede in particolare nella componente denominata “**Digitalizzazione, innovazione e sicurezza nella PA**” diverse misure di finanziamento dedicate alla digitalizzazione dell’Ente. Il comune di San Sperate ha correttamente richiesto ed utilizzato tali somme secondo la seguente tabella riassuntiva.

MISURA	1.2 - ABILITAZIONE AL CLOUD PER LE PA LOCALI COMUNI (APRILE 2022)' - M1C1 PNRR FINANZIATO DALL'UNIONE EUROPEA
Descrizione	L’investimento è collegato all’obbligo, introdotto dall’art. 35 del D.L. 76/2020, per la PA di migrare i propri CED verso ambienti cloud. Viene favorita la migrazione di sistemi, dati e applicazioni digitali verso servizi cloud qualificati, in modo da migliorare la qualità dei servizi digitali per i cittadini e la loro sicurezza, dismettendo i data center meno efficienti e migliorando l’efficienza energetica delle infrastrutture della PA e la sostenibilità ambientale.
Stato attuale	CONCLUSO - Tutte le operazioni sono concluse, compresa la contrattualizzazione del fornitore, la messa in opera e l’attivazione delle operazioni necessarie, rendicontazione, asseverazione e liquidazione finale del fornitore.
Importo ottenuto	€ 83.044,00
Fornitore	Arionline Srl, C.F. /P.IVA 02161330929, sede legale via Filoteo Alberini, 25 00139 Roma (RM)
Lavori svolti	- Migrazione di tutta la suite attiva verso la piattaforma in cloud certificato AGID raggiungibile dall’indirizzo web https://sic-comunesansperate.arionline.cloud/ - Mantenimento piattaforma in cloud per anni 2024, 2025 e 2026

MISURA	1.4.1 - ESPERIENZA DEL CITTADINO NEI SERVIZI PUBBLICI - COMUNI (SETTEMBRE 2022)” - M1C1 PNRR 1.4 “SERVIZI E CITTADINANZA DIGITALE”
Descrizione	L’investimento è relativo all’adesione da parte di tutte le pubbliche amministrazioni all’implementazione di un modello standard di siti web dedicato alla PAL e PAC che tengano conto della personalizzazione, integrazione CMS e migrazione dei contenuti secondo modelli sistemi progettuali aderenti alle linee guida emanate dall’AGID. Il modello suddivide il nuovo sito web istituzionale in 4 diverse interfacce di pubblicazione: amministrazione locale, servizi al cittadino, notizie e documenti pubblici dell'amministrazione.
Stato attuale	CONCLUSO - Tutte le operazioni sono concluse, compresa la contrattualizzazione del fornitore, la messa in opera e l’attivazione delle operazioni necessarie, rendicontazione, asseverazione e liquidazione finale del fornitore.
Importo ottenuto	€ 51.654,00
Fornitore	DigitalPA Srl, C.F. /P.IVA 03553050927, sede legale via San Tommaso d'Aquino, 18/a 09134 Cagliari
Lavori svolti	- Aggiornamento del portale istituzionale secondo le linee guida AGID, raggiungibile dall’indirizzo web https://www.comune.sansperate.ca.it/ - Mantenimento piattaforma in cloud per anni 2024, 2025

MISURA	1.4.3 - PagoPA' COMUNI (settembre 2022) - Missione 1 Componente 1 del PNRR, finanziato dall'Unione europea nel contesto dell'iniziativa Next Generation EU - Investimento 1.4 "SERVIZI E CITTADINANZA DIGITALE"
Descrizione	La misura è collegata all'articolo 5 del decreto legislativo 7 marzo 2005, n. 82 recante il codice dell'amministrazione digitale (nel seguito "CAD") che ha previsto in capo alle pubbliche amministrazioni, ai gestori di pubblici servizi e alle società a controllo pubblico come individuati dall'art. 2 del CAD, l'obbligo di accettare, tramite la piattaforma pagoPA, i pagamenti spettanti a qualsiasi titolo attraverso sistemi di pagamento elettronico.
Stato attuale	CONCLUSO - Tutte le operazioni sono concluse, compresa la contrattualizzazione del fornitore, la messa in opera e l'attivazione delle operazioni necessarie, rendicontazione, asseverazione e liquidazione finale del fornitore.
Importo ottenuto	€ 4.285,00
Fornitore	Arionline Srl, C.F. /P.IVA 02161330929, sede legale via Filoteo Alberini, 25 00139 Roma (RM)
Lavori svolti	Attivazione del nodo di pagamento PagoPA per il Comune di San Sperate, raggiungibile dal Cittadino all'indirizzo: https://www.cittadinodigitale.it/ (selezionando poi il nostro comune tra la lista delle PA)

MISURA	1.4.3 - APP IO" - Comuni (Settembre 2022) - Missione 1 Componente 1 del PNRR - Investimento 1.4 "SERVIZI E CITTADINANZA DIGITALE"
Descrizione	La Misura è collegata all'articolo 64-bis del CAD che prevede che le pubbliche amministrazioni, tramite il punto di accesso telematico attivato presso la Presidenza del Consiglio dei ministri, rendano fruibili digitalmente i propri servizi. Inoltre, l'articolo 3-bis, comma 1, del CAD, al fine di semplificare e favorire l'accesso ai servizi in rete della pubblica amministrazione da parte di cittadini e imprese e l'effettivo esercizio del diritto all'uso delle tecnologie digitali, ha introdotto il diritto di accedere ai servizi on-line della pubblica amministrazione "tramite la propria identità digitale e anche attraverso il punto di accesso telematico di cui all'articolo 64-bis". In particolare, l'App IO mette a disposizione di tutte le pubbliche amministrazioni e gli altri soggetti di cui all'art. 2 del CAD una piattaforma comune e semplice da usare, con la quale relazionarsi in modo personalizzato, rapido e sicuro, consentendo l'accesso ai servizi e alle comunicazioni delle amministrazioni direttamente dal proprio smartphone. Inoltre, la sua implementazione determina una maggiore fruibilità dei servizi online, permettendo di accedere, attraverso l'App, che si basa sull'utilizzo di altre piattaforme abilitanti previste dalla legge, ad una pluralità di servizi e informazioni.
Stato attuale	CONCLUSO - Tutte le operazioni sono concluse, compresa la contrattualizzazione del fornitore, la messa in opera e l'attivazione delle operazioni necessarie, rendicontazione, asseverazione e liquidazione finale del fornitore.
Importo ottenuto	€ 6.860,00
Fornitore	Arionline Srl, C.F. /P.IVA 02161330929, sede legale via Filoteo Alberini, 25 00139 Roma (RM)
Lavori svolti	Attivazione e mantenimento di oltre 14 servizi sull'applicazione AppIO relativi al Comune di San Sperate, fruibili da applicazione mobile (alcuni sono in consultazione).

MISURA	1.4.4 - SPID CIE - Comuni (Settembre 2022)' Missione 1 Componente 1 del PNRR, finanziato dall'Unione europea nel contesto dell'iniziativa Next Generation EU - Investimento 1.4 "SERVIZI E CITTADINANZA DIGITALE"
Descrizione	La Misura è atta a favorire l'adozione dell'identità digitale (Sistema Pubblico di Identità Digitale, SPID e Carta d'Identità Elettronica, CIE) e dell'Anagrafe nazionale della popolazione residente (ANPR), consentendo l'accesso ai servizi online dell'Ente tramite CIE, CNS e SPID. Oltre questo, alle amministrazioni aderenti, è richiesto l'utilizzo dello standard <i>OpenID Connect</i> , o, in alternativa, l'erogazione di un piano formativo idoneo a costruire le basi per un successivo passaggio tecnologico.
Stato attuale	CONCLUSO - Tutte le operazioni sono concluse, compresa la contrattualizzazione del fornitore, la messa in opera e l'attivazione delle operazioni necessarie, rendicontazione, asseverazione e liquidazione finale del fornitore.
Importo ottenuto	€ 14.000,00
Fornitore	Arionline Srl, C.F. /P.IVA 02161330929, sede legale via Filoteo Alberini, 25 00139 Roma (RM)
Lavori svolti	attivazione e mantenimento dell'interfaccia di accesso ai servizi online dell'Ente, tramite uno dei suddetti sistemi pubblici di identità digitale, raggiungibile attraverso il seguente link: https://www.cittadinodigitale.it/apkauthgatewayui/AuthService/index

MISURA	1.4.4 - Estensione dell'utilizzo dell'anagrafe nazionale digitale (ANPR) – Adesione allo Stato Civile digitale (ANSC) - COMUNI (LUGLIO 2024) - M1C1 PNRR FINANZIATO DALL'UNIONE EUROPEA - Next Generation EU.
Descrizione	L'investimento prevede la realizzazione dell'adeguamento e dell'evoluzione delle caratteristiche tecniche della piattaforma di funzionamento dell'ANPR per l'erogazione dei servizi resi disponibili ai comuni per l'utilizzo dell'Archivio Nazionale informatizzato dei registri dello Stato Civile (ANSC). Lo scopo è quello di creare un Archivio nazionale informatizzato dei registri dello Stato Civile in un'unica piattaforma centralizzata, accessibile a tutti i Comuni, che permette di gestire digitalmente tutte le operazioni relative all'iscrizione, trascrizione, annotazione e conservazione degli atti nei registri dello Stato Civile e offre l'opportunità di generare digitalmente certificati con piena valenza legale.
Stato attuale	CONCLUSO - Tutte le operazioni sono concluse, compresa la contrattualizzazione del fornitore, la messa in opera e l'attivazione delle operazioni necessarie, rendicontazione, asseverazione e liquidazione finale del fornitore.
Importo ottenuto	€ 8.979,20
Fornitore	Arionline Srl, C.F. /P.IVA 02161330929, sede legale via Filoteo Alberini, 25 00139 Roma (RM)
Lavori svolti	Attivazione del nodo di interoperabilità tra gli applicativi in uso presso il Comune di San Sperate e la piattaforma ANPR (anagrafe nazionale popolazione residente) per le funzionalità legato allo stato civile

MISURA	1.4.5 - Piattaforma Notifiche Digitali - Comuni (Settembre 2022)" - PNRR M1C1 Investimento 1.4 "SERVIZI E CITTADINANZA DIGITALE"
Descrizione	Lo scopo della misura 1.4.5 del PNRR è di adottare un'unica piattaforma per l'invio e la ricezione delle notifiche a valore legale, semplificando il processo per tutti: gli enti che le inviano e i destinatari che le ricevono: SEND è il servizio di Notifiche Digitali. Le notifiche SEND sono comunicazioni a valore legale emesse in via ufficiale da un'amministrazione come multe, avvisi di accertamento di tributi o rimborsi. Le notifiche SEND sono quindi diverse dalle "notifiche push", cioè quei brevi messaggi che ricevi sullo schermo del tuo dispositivo. Per valore legale si intende che l'invio e la ricezione di queste comunicazioni producono degli effetti giuridici sia nei confronti di chi le invia sia di chi le riceve. Per esempio, se ricevi una multa per violazione del codice stradale, la data in cui la ricevi incide sull'importo che dovrai pagare o sulla tua facoltà di contestarla. Servizio Notifiche Digitali offre agli enti pubblici un sistema più efficiente e sicuro di invio delle comunicazioni, sollevando le amministrazioni dalla gestione dell'intero processo di notificazione. Gli enti mittenti devono solo depositare l'atto da notificare sulla piattaforma che si occuperà dell'invio, per via digitale o analogica. Con SEND, diminuisce l'incertezza della reperibilità dei destinatari e si riducono i tempi e i costi di gestione.
Stato attuale	CONCLUSO - Tutte le operazioni sono concluse, compresa la contrattualizzazione del fornitore, la messa in opera e l'attivazione delle operazioni necessarie, rendicontazione, asseverazione e liquidazione finale del fornitore.
Importo ottenuto	€ 32.589,00
Fornitore	Arionline Srl, C.F. /P.IVA 02161330929, sede legale via Filoteo Alberini, 25 00139 Roma (RM)
Lavori svolti	- attivazione e mantenimento dell'interfaccia di gestione della piattaforma SEND relativa al Comune di San Sperate, raggiungibile dal link https://selfcare.pagopa.it/auth/login - attivazione e configurazione tecnica dei protocolli di interscambio e di interoperabilità

MISURA	1.3.1 - "Piattaforma Digitale Nazionale Dati - ARCHIVIO NAZIONALE DEI NUMERI CIVICI DELLE STRADE URBANE (ANNCSU) – COMUNI (MAGGIO 2025)" - PNRR M1C1 Investimento 1.3 "DATI E INTEROPERABILITÀ"
Descrizione	L'investimento prevede la realizzazione del sistema di interoperabilità tra i sistemi locale e le piattaforme nazionali al fine di garantire a tutti i Comuni italiani il conferimento dei dati georeferenziati relativi a tutti i numeri civici di propria competenza all'interno dell'Archivio Nazionale dei Numeri Civici e delle Strade Urbane (ANNCSU).
Stato attuale	IN VERIFICA – Richiesta di finanziamento andata a buon fine, lavori eseguiti e richiesta l'asseverazione inoltrata, si attende la convalida.
Importo ottenuto	€ 8.979,20
Fornitore	Arionline Srl, C.F. /P.IVA 02161330929, sede legale via Filoteo Alberini, 25 00139 Roma (RM)
Lavori svolti	Attività ancora in fase di verifica tecnica

Ruolo del Responsabile e dell'Ufficio per la Transizione Digitale

Scenario

In questo quadro, occorre consolidare e potenziare i Responsabili e gli Uffici per la transizione al digitale, tenendo conto dei nuovi profili professionali necessari e, in particolare, del fabbisogno urgente nelle PA di specialisti ICT dedicati a sicurezza e trasformazione digitale.

A novembre 2023, analizzando i dati disponibili sull'Indice dei domicili digitali della Pubblica Amministrazione e dei Gestori di Pubblici Servizi, risultano ancora da nominare circa 2.400 RTD nelle pubbliche amministrazioni e negli enti pubblici con tale obbligo di nomina.

Circa la metà risultano essere amministrazioni comunali, in particolare di piccole dimensioni, o loro aggregazioni; ma il trend di nomina degli RTD presso tali tipologie di PA risulta essere in costante aumento e si rileva che alcune PA locali, sulla base delle proprie esigenze, hanno colto l'opportunità di procedere alla nomina del RTD e alla costituzione dell'Ufficio per la transizione digitale in forma associata, in aderenza a quanto previsto dal comma 1-septies dell'art. 17 del CAD. La collaborazione tra amministrazioni è infatti una delle leve a disposizione degli Enti per mettere a fattor comune risorse e competenze per raggiungere gli obiettivi di trasformazione digitale, attraverso la nomina del RTD e dell'UTD in forma associata, che permette di individuare un unico ufficio dirigenziale generale a cui affidare la transizione alla modalità operativa digitale e i conseguenti processi di digitalizzazione.

Per quanto concerne gli ambiti di approfondimento per l'UTD si sottolinea che:

- i criteri di progettazione dei processi digitali, sia semplici che collettivi, sono riportati nelle Linee guida sull'interoperabilità tecnica approvate con Determinazione AGID 547/2021. I processi digitali possono essere semplici (quando riguardano l'esposizione di e-service da parte di un singolo ente, per procedimenti/procedure utili ad una generalità indistinta di enti destinatari, ad es. il calcolo dell'ISEE, la verifica di dati in ANPR o nel Registro imprese, ecc.) oppure possono essere processi digitali collettivi quando coinvolgono più enti.
- è compito dell'Ufficio del RTD curare sia gli aspetti di interoperabilità tecnica che quelli di interoperabilità organizzativa, semantica e giuridica, ricercando la collaborazione con gli altri enti autonomamente o attraverso gli spazi di interoperabilità e cooperazione applicativa (facendo riferimento al relativo coordinatore);
- la gestione del ciclo di vita degli e-service dell'amministrazione richiede la strutturazione di opportuni presidi organizzativi e strumenti tecnologici per l'API-management, in forma singola o associata.

Il processo di collaborazione tra enti va incoraggiato e viene agevolato dalla condivisione di pratiche e soluzioni tra gli enti stessi e dalla disponibilità di modelli attuativi da sperimentare e adattare alla singola realtà territoriale o tematica. La costituzione di un UTD in forma associata, prevista per le PA diverse da quelle centrali dall'art. 17 comma 1-septies, è diversa

dalla gestione associata della funzione ICT che spesso caratterizza le Unioni di Comuni. Come chiarito dalla Circolare 3 del 2018 del Ministro per la Pubblica Amministrazione, può «avvenire in forza di convenzioni o, per i Comuni, anche mediante l'Unione di Comuni» e quindi può rappresentare un'opportunità per le Amministrazioni e gli enti pubblici di mettere a fattor comune risorse per favorire la transizione digitale.

Con decreto del Sindaco nr. 04 del 04/03/2021, ai sensi del Codice dell'Amministrazione Digitale e ss.mm.ii., è stato istituito l'**ufficio responsabile della transizione digitale** (d'ora in avanti U-RTD).

L'**AGID** ricorda che possono essere individuate alcune azioni, utili per tutte le amministrazioni, al fine di accelerare il processo di digitalizzazione ovvero:

1. occorre istituire, ove non sia stato già fatto, l'Ufficio per la transizione digitale, in forma singola o associata, con conseguente nomina del Responsabile per la transizione digitale (RTD). Nell'ottica di creare un ecosistema digitale all'interno dell'Ente, la struttura organizzativa va potenziata;
2. per strutturare l'ente come ecosistema digitale amministrativo è essenziale il potenziamento del ruolo e della dotazione di risorse umane e strumentali dell'UTD e la definizione, con appositi atti, di schemi organizzativi chiari rispetto al raccordo e all'attribuzione di competenze tra RTD ed altre figure dirigenziali dell'ente. L'erogazione dei servizi pubblici passa sempre più da strumenti digitali; quindi, è fondamentale la progettazione di sistemi informativi e servizi digitali e sicuri by design, affinché siano moderni, accessibili, di qualità e di facile fruizione;
3. la mappatura dei processi dell'ente, e la loro revisione in chiave digitale, può prendere le mosse da quanto già fatto nell'ente per la valutazione del rischio corruttivo, integrando opportunamente la mappatura già realizzata con altre informazioni presenti nell'ente come, ad esempio, il Catalogo dei procedimenti dell'ente e il Catalogo dei servizi erogati dall'ente;
4. all'interno del PIAO previsto dall'articolo 6 del decreto-legge n. 80 del 9 giugno 2021, occorre ricomprendere gli obiettivi specifici di digitalizzazione, semplificazione e reingegnerizzazione, a partire dalla mappatura di cui sopra e dalle priorità del singolo ente.

A sostegno del rafforzamento dei RTD e degli UTD continua, inoltre, ad essere strategica la disponibilità di strumenti utili ed iniziative per favorire l'aggiornamento sulle materie di competenza e per condividere soluzioni e pratiche, nonché di occasioni di incontro e tavoli di confronto interistituzionali. È in quest'ottica che AGID mette a disposizione la piattaforma di community ReTeDigitale dedicata ai RTD e al personale degli UTD, le comunità digitali tematiche/ territoriali al suo interno e le iniziative laboratoriali con l'obiettivo di supportare i processi di trasformazione digitale nelle Amministrazioni centrali, locali e negli Enti presenti nell'Indice dei domicili digitali della Pubblica Amministrazione e dei Gestori di pubblici servizi.

Risulta fondamentale inoltre sfruttare al massimo i tavoli di incontro istituzionale e favorire le occasioni di scambio e condivisione tra amministrazioni e tra RTD anche attraverso il rilancio della Conferenza dei RTD con incontri periodici e iniziative di prossimità sul territorio per favorire la più ampia partecipazione anche da parte dei piccoli enti. Inoltre, va incentivato l'approccio proattivo delle amministrazioni e degli enti pubblici nel condividere dati, esperienze, proposte; sono in primis da valorizzare e promuovere le iniziative a livello territoriale che vedono la partecipazione congiunta di RTD e UTD di enti diversi, che attraverso attività di scouting e condivisione favoriscono la diffusione delle eccellenze e l'individuazione di soluzioni ai problemi più diffusi.

Situazione attuale del Comune di San Sperate (scenario locale)

Il Comune perciò, per individuare e dare attuazione alla propria strategia in merito al digitale, si è strutturato dal punto di vista organizzativo individuando le seguenti figure che dovranno intervenire attivamente nel processo di digitalizzazione:

- il **Responsabile U-RTD** dottoressa **Iride Atzori** dipendente dalle comprovate competenze manageriali e di gestione delle risorse umane, già responsabile di posizione organizzativa per l'Area 1, che comprende i servizi ICT dell'Ente;
- l'istruttore informatico **Alberto Mameli**, dalle comprovate competenze tecnologiche, d'informatica giuridica e manageriali, come richieste dall'art. 17 del CAD vigente, soggetto vicario al Responsabile U-RTD. Svolge il ruolo operativo all'interno dell'ufficio indicando al Responsabile le migliori scelte e strategie da applicare per ottemperare a quanto richiesto dalla normativa su transizione digitale, cyber security, pubblicità legale, amministrazione del sistema, della rete e delle piattaforme informatiche a disposizione dell'Ente;
- i **Responsabili di Settore**, i quali collaborano con il Responsabile della transazione al digitale (RTD) sia nella definizione della strategia dell'ente, fornendo annualmente i fabbisogni e lo stato dell'arte dell'area in termini di digitale, che nell'attuazione della strategia stessa, ciascuno per quanto di propria competenza;

Oltre a queste figure interne, l'U-RTD viene supportato da:

- il **Responsabile della Protezione Dati** (Data Protection Officer - DPO): assicura la coerenza con quanto indicato nel GDPR (Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016). Attualmente tale figura è ricoperta dall'avvocato **Ivan Orrù**, DPO dell'Ente;
- il **Responsabile della Conservazione dei documenti amministrativi** il quale verifica e analizza il corretto andamento del processo di digitalizzazione sia in termini di open data che in termini operativi (ovvero la verifica dello standard utilizzato per la conservazione e la sicurezza dei dati stessi);
- **Sindaco e Giunta** che approvano il Piano Triennale con atto formale (Delibera di giunta) e possono richiedere modifiche al Piano Triennale.

La scelta dei componenti è stata determinata dalla necessità di creare un ufficio con le competenze tecniche, informatiche, legali, manageriali e comunicative necessarie. Inserendo quindi l'istruttore informatico, che ha il ruolo di soggetto vicario al Responsabile U-RTD, e tutti i responsabili delle altre aree: quest'ultima scelta è appunto mirata a creare un servizio "trasversale" che coinvolga tutti gli uffici dell'Ente e che non rileghi la transizione al digitale al solo ufficio ICT.

Contesto normativo e strategico

Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" art. 17.
- Circolare n. 3 del 1° ottobre 2018 del Ministro per la Pubblica Amministrazione sul Responsabile per la transizione al digitale.

Obiettivo 1.1 – Migliorare i processi di trasformazione digitale della PA

Risultati attesi:

- RA1.1.1 - Rafforzare la collaborazione e lo scambio di pratiche e soluzioni tra Amministrazioni
- RA1.1.2 - Individuazione e diffusione di modelli organizzativi/operativi degli Uffici Transizione digitale, anche in forma associata

CAP1.PA.01

Le Amministrazioni e gli Enti in IndicePA interessati possono proporre ad AgID l'attivazione di una comunità digitale tematica/territoriale su retedigitale.gov.it

Azioni previste/eseguite: il Comune di San Sperate attualmente non partecipa direttamente ad alcuna comunità digitale tematica/territoriale su retedigitale.gov.it.

CAP1.PA.02

Le Amministrazioni e gli Enti in IndicePA interessati utilizzano i format presenti nel kit per proporre nuove comunità digitali ed effettuano monitoraggi semestrali delle attività in esse svolte

Azioni previste/eseguite: il Comune di San Sperate attualmente non partecipa direttamente ad alcuna comunità digitale tematica/territoriale su retedigitale.gov.it.

CAP1.PA.03

Le PA partecipanti alle iniziative laboratoriali forniscono contributi e proposte di modifica e integrazione al Vademecum sulla nomina del Responsabile per la transizione al digitale e sulla costituzione dell'Ufficio per la transizione al digitale in forma associata.

Azioni previste/eseguite: il Comune di San Sperate attualmente non partecipa direttamente ad alcuna comunità digitale tematica/territoriale su retedigitale.gov.it.

CAP1.PA.04

Le PA partecipanti alle iniziative laboratoriali e che hanno adottato modelli organizzativi/operativi per l'Ufficio per la transizione al digitale condividono le esperienze, gli strumenti sviluppati e i processi implementati.

Azioni previste/eseguite: il Comune di San Sperate attualmente non partecipa direttamente ad alcuna comunità digitale tematica/territoriale su retedigitale.gov.it.

CAP1.PA.05

Le PA partecipanti alle iniziative laboratoriali sperimentano i modelli proposti e forniscono ad AGID il feedback delle esperienze di nomina RTD e UTD in forma associata realizzate.

Azioni previste/eseguite: il Comune di San Sperate attualmente non partecipa direttamente ad alcuna comunità digitale tematica/territoriale su retedigitale.gov.it.

CAP1.PA.06

Le PA partecipanti alle iniziative laboratoriali sperimentano i modelli proposti e forniscono ad AGID il feedback sui nuovi modelli organizzativi/operativi dell'UTD adottati.

Azioni previste/eseguite: il Comune di San Sperate attualmente non partecipa direttamente ad alcuna comunità digitale tematica/territoriale su retedigitale.gov.it.

Competenze digitali per il Paese e per la PA

Scenario

Tra i fattori abilitanti dei processi di trasformazione digitale un ruolo imprescindibile è esercitato dalle competenze digitali, ovvero il complesso di conoscenze, attitudini e abilità funzionali a orientarsi, interagire e operare nell'ambiente digitale, sia per la vita che per il lavoro. La strategia UE ragiona infatti su due dimensioni:

- La sfera personale, nella quale si inquadrano una serie di attività comuni nel quotidiano - comprese le interazioni con i servizi pubblici - che richiedono il possesso di competenze digitali di base; il Decennio Digitale Europeo ha fissato per il 2030 l'obiettivo dell'80% della popolazione in possesso di queste competenze;
- La sfera professionale, in cui, oltre alle medesime competenze digitali di base (per esempio, per l'accesso a servizi pubblici per le imprese) sono richieste, in particolare per alcuni settori, sempre più competenze specialistiche nel campo ICT; in questo caso, l'obiettivo fissato per il Decennio Digitale Europeo è pari a 20 milioni di specialisti ICT, rispettando l'equilibrio di genere.

Il tema delle competenze digitali acquista un particolare rilievo nel contesto della vita pubblica, che vede confrontarsi gli utenti di servizi pubblici digitali e la Pubblica Amministrazione, erogatrice dei medesimi servizi. LA PA, in particolare, necessita di competenze digitali per i propri dipendenti (a tutti i livelli, dirigenziali e non dirigenziali), e di

competenze digitali specifiche del settore professionale e di intervento (come, ad esempio, nella Sanità e nella Giustizia), ma soprattutto esprime un fabbisogno crescente di competenze ICT specialistiche.

Come già indicato nelle precedenti edizioni del Piano triennale per l'informatica nella PA, l'Italia ha definito una propria «Strategia nazionale per le competenze digitali» con un Piano operativo di attuazione, verificato e aggiornato sulla base di un ciclo annuale di monitoraggio, nell'ambito dell'iniziativa strategica nazionale «Repubblica Digitale». La maggior parte delle azioni presenti nel Piano operativo è finanziata e inclusa nel PNRR. Per quanto riguarda in particolare i cittadini, nel 2023 hanno preso avvio le attività correlate all'investimento 1.7 del PNRR, «Competenze digitali di base», che si pone l'obiettivo di ridurre la quota di cittadini a rischio di esclusione digitale tramite:

- il potenziamento della Rete dei Centri di facilitazione digitale
- la creazione di una rete di giovani volontari per lo sviluppo e il miglioramento delle competenze digitali nell'ambito del «Servizio Civile Digitale (sub-investimento 1.7.1).

Con riferimento alle competenze digitali della Pubblica Amministrazione, la Strategia nazionale per le competenze digitali prevede il potenziamento e lo sviluppo delle competenze digitali della forza lavoro e delle competenze di e-leadership di coloro che ricoprono ruoli di responsabilità di unità organizzative e di progetti, con il coordinamento del Dipartimento della Funzione Pubblica.

Il fabbisogno di competenze digitali nella Pubblica Amministrazione riguarda tutta la popolazione dei pubblici dipendenti: tanto dei dirigenti, chiamati a esercitare la propria funzione pubblica in un contesto essenzialmente trasformato dalla tecnologia, che del personale di livello non dirigenziale, Esempi di iniziative in risposta a tale fabbisogno sono:

- l'iniziativa «Syllabus per la formazione digitale», che mira a consentire a tutti i dipendenti delle amministrazioni aderenti l'accesso, attraverso la piattaforma online del Dipartimento della Funzione Pubblica;
- le proposte formative della Scuola Nazionale dell'Amministrazione su tematiche quali la cybersicurezza e i sistemi in cloud, le tecnologie abilitanti per l'organizzazione, la digitalizzazione nel PNRR, la progettazione della trasformazione digitale e la gestione dell'innovazione, fino al ruolo di intelligenza artificiale (IA) e dati nei sistemi decisionali di supporto alla PA.;
- a livello territoriale, nell'ambito dell'accordo stipulato tra ANCI e il Dipartimento per la Trasformazione Digitale, è stata costituita l'Academy ANCI, specificamente dedicata alla formazione di funzionari e dirigenti comunali. L'Academy realizzerà iniziative volte ad accrescere le competenze degli operatori comunali a fornire un'informazione costante, attraverso incontri online e in presenza, mirati sia all'attuazione degli Avvisi emanati dal Dipartimento nell'ambito della Misura 1 Componente 1 del PNRR, sia - di più ampio respiro - alle priorità legate al processo di digitalizzazione della PA.

La Strategia nazionale per le competenze digitali prevede inoltre lo sviluppo di competenze specialistiche ICT per fronteggiare le sfide legate alle tecnologie emergenti e al possesso delle competenze chiave per i lavori del futuro con il coordinamento di Ministero dell'Università e Ricerca e Ministero dell'Impresa e del Made in Italy. In particolare, le azioni di formazione e divulgazione hanno l'obiettivo di ridurre il divario di genere presente in ambito ICT, incentivando la partecipazione della popolazione femminile ai corsi di laurea e alle professioni ICT ed eliminando gli stereotipi che alimentano il divario nelle STEM e in ICT. Le azioni rispondono alla necessità di costituire strutture di supporto per il genere femminile, non solo per l'orientamento e la scelta di percorsi di studio, ma anche in termini di reskilling e upskilling, oltre che di supporto nel progresso di carriera.

Le azioni inserite nel Piano operativo dedicate all'incremento degli specialisti ICT sono volte ad incentivare l'accesso alle discipline e alle professioni scientifico - tecnologiche, con particolare attenzione ai corsi di laurea ICT e all'impiego di risorse ICT nel settore pubblico e privato e anche ad alcuni target specifici a rischio di esclusione sociale ed espulsione dal mercato del lavoro, come nel caso delle azioni del Fondo per la Repubblica Digitale.

Queste azioni sono in linea con quelle proposte dalle Associazioni di categoria ICT: i) il potenziamento dei Licei Scientifici e gli ITIS con indirizzo tecnologico aumentando il numero di classi del 50% rispetto all'attuale programmazione, ii) l'aumento del numero degli Istituti Tecnologici Superiori (ITS), iii) il monitoraggio del proseguimento degli studenti nei percorsi post-diploma e nel mondo del lavoro, premiando le scuole superiori e i docenti il cui tasso di giovani NEET (Non in Educazione, Occupazione o Formazione) nei 12 mesi successivi al diploma sia inferiore a una percentuale prefissata, iv) la creazione di un fondo per lo sviluppo di programmi formativi in collaborazione con le aziende, v) l'adattamento rapido dei programmi alle richieste del mercato vi) la riduzione del gap di competenze tecnologiche da parte dei docenti.

Il PNRR sostiene le azioni del Piano volte a favorire l'incremento di specialisti ICT e l'occupazione di queste risorse nei settori considerati strategici per la crescita del Paese, con particolare riferimento agli investimenti dedicati al potenziamento delle condizioni di supporto alla ricerca e all'innovazione (M4C2 Investimento 3). Lo sviluppo di una rete di formazione digitale per le amministrazioni locali, al fine di supportare la trasformazione tecnologica e dei processi, è l'auspicio anche delle Associazioni di impresa ICT. Le micro e piccole imprese digitali locali, che costituiscono oltre il 90% delle imprese ICT italiane, possono creare una rete di piccoli fornitori qualificati che siano punto di riferimento sul territorio.

Collaborare con queste realtà locali offre vantaggi duplici per le pubbliche amministrazioni: evitare la dipendenza unicamente da grandi aziende e favorire la presenza locale, contribuendo all'occupazione nelle aree periferiche. Per ciò che concerne il ruolo degli specialisti ICT all'interno delle PA occorre quindi promuovere strumenti per la definizione della «famiglia professionale» degli specialisti ICT nella PA, e per il loro corretto

inquadramento all'interno del CCNL e per strutturare dei chiari percorsi di carriera, anche perché oggi, per queste figure professionali, le PA non sono concorrenziali rispetto al mercato. Inoltre, nell'ambito del PNRR, e in particolare dell'investimento 2.3 M1C1, è prevista l'attivazione di almeno 20 «comunità di competenze» (community of Practice), trasversali alle amministrazioni, tra le quali si annoverano anche quelle dedicate alla digital transformation: l'intervento, a titolarità della Scuola Nazionale dell'Amministrazione, è destinato a sviluppare e contaminare best practice all'interno della PA.

Contesto normativo e strategico

Riferimenti normativi italiani:

- Direttiva del Ministro per la Pubblica Amministrazione del 23 marzo 2023 "Pianificazione della formazione e sviluppo delle competenze funzionali alla transizione digitale, ecologica e amministrativa promosse dal Piano Nazionale di Ripresa e Resilienza"

Riferimenti normativi europei:

- Raccomandazione del Consiglio del 22 maggio 2018 relativa alle competenze chiave per l'apprendimento permanente (GU 2018/C 189/01)
- Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni COM (2020) 67 final del 19 febbraio 2020 - Plasmare il futuro digitale dell'Europa
- Decisione (EU) 2022/2481 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 che istituisce il programma strategico per il Decennio Digitale 2030
- Decisione del Parlamento Europeo e del Consiglio relativa a un Anno Europeo delle Competenze 2023 COM (2022) 526 final 2022/0326

Obiettivo 1.2 – Diffusione competenze digitali nel Paese e nella PA

Risultati attesi:

- RA1.2.1 - Diffusione competenze digitali di base per cittadini e imprese
- RA1.2.2 - Diffusione competenze digitali di base nella PA
- RA1.2.3 - Diffusione delle competenze specialistiche ICT

CAP1.PA.07

Le PA, in funzione delle proprie necessità, partecipano alle iniziative pilota, alle iniziative di sensibilizzazione e a quelle di formazione di base e specialistica per il proprio personale, come previsto dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali

Azioni previste/eseguite: il Comune di San Sperate partecipa alle iniziative di sensibilizzazione e a quelle di formazione di base e specialistica per il proprio personale, anche attraverso l'adesione alla piattaforma Syllabus, alla quale sono stati iscritti tutti i dipendenti dell'ente.

Inoltre l'Amministrazione fruisce di una seconda piattaforma di formazione, attivata a livello di Unione dei Comuni, specifica su temi prioritari e strategici.

CAP1.PA.08

Le PA aderiscono all'iniziativa "Syllabus per la formazione digitale" e promuovono la partecipazione alle iniziative formative sulle competenze di base da parte dei dipendenti pubblici, concorrendo al conseguimento dei target del PNRR in tema di sviluppo del capitale umano della PA e in linea con il Piano strategico nazionale per le competenze digitali.

Azioni previste/eseguite: il Comune di San Sperate ha aderito all'iniziativa "Syllabus per la formazione digitale" a partire dall'anno 2023 con l'iscrizione di tutti i dipendenti. Nel corso degli ultimi anni il personale dipendente ha proseguito con la formazione su tale piattaforma.

CAP1.PA.09

Le PA, in funzione della propria missione istituzionale, realizzano iniziative per lo sviluppo delle competenze digitali dei cittadini previste dal PNRR e in linea con il Piano operativo della Strategia Nazionale per le Competenze Digitali.

Azioni previste/eseguite: il Comune di San Sperate, durante l'anno 2025, ha aderito alla "Rete dei facilitatori digitali" promossa dal Ministero e realizzata a livello di Unione dei Comuni. Si prevede di avviare nuovamente il servizio durante l'anno 2026. Oltre questo l'Ente sta provvedendo, attraverso i volontari del Servizio Civile Nazionali, all'attivazione di percorsi di facilitazione digitale per i Cittadini, sulla linea dell'esperienza precedente.

Monitoraggio

Scenario

Il Codice dell'Amministrazione Digitale, all'art.14-bis lettera c), ha attribuito ad AGID il compito di realizzare il monitoraggio delle attività e la verifica dei risultati delle amministrazioni, in termini sia di coerenza con il Piano triennale e sia di costi/benefici dei sistemi informativi delle singole PA. Allo stesso tempo, tali azioni di monitoraggio e verifica hanno l'obiettivo di supportare l'attuazione fisica, finanziaria e procedurale del Piano triennale nel suo complesso. Il monitoraggio della trasformazione digitale del Paese si articola su più livelli:

1. la misurazione dei risultati attesi (RA) e delle linee di azione (LA) conseguiti dal sistema PA per ciascuna componente tecnologica e non tecnologica del Piano triennale;
2. il monitoraggio dell'andamento della spesa e degli investimenti ICT, misurati attraverso la una rilevazione periodica della spesa ICT.

Queste attività vengono condotte in coerenza con gli indicatori del Programma europeo Decennio Digitale, che prevede un sistema di monitoraggio strutturato, trasparente e condiviso, basato sull'indice di digitalizzazione dell'economia e della società (DESI), e

integrato con nuovi indicatori, per misurare i progressi compiuti verso ciascuno degli obiettivi per il 2030.

A fronte degli ingenti investimenti previsti dal Piano nazionale di ripresa e resilienza (PNRR) per la digitalizzazione della Pubblica Amministrazione, il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri ha avviato la costituzione di un Osservatorio sulla trasformazione digitale nel territorio italiano: una raccolta sistematica di dati sulle risorse previste per la digitalizzazione della PA, sui progetti finanziati e sulle amministrazioni coinvolte in questo processo, anche attraverso l'integrazione con altre banche dati pertinenti. L'intento è di accompagnare alle scelte di policy un'attività di monitoraggio e di misurazione degli impatti, fornendo elementi oggettivi di valutazione delle politiche pubbliche, che possano contribuire a orientare le iniziative future in materia di semplificazione e digitalizzazione dei processi. A tale scopo è prevista la realizzazione di una serie di prodotti di analisi, tra cui indicatori originali e questionari di monitoraggio che contribuiranno alla stesura di un report sull'avanzamento della digitalizzazione nel Paese. L'Osservatorio si pone quindi come strumento di analisi istituzionale che ha il potenziale di diventare un asset strategico per il monitoraggio del Piano triennale per l'informatica nella Pubblica Amministrazione.

Le attività dell'Osservatorio prevedono un importante lavoro sul territorio, attraverso attività di informazione e coinvolgimento degli enti. In aggiunta gli accordi firmati tra il Dipartimento e le principali rappresentanze istituzionali territoriali prevedono, tra le diverse linee di attività, anche la raccolta sistematica di dati al fine di migliorare le politiche e meglio pianificare futuri interventi. Si tratta di raccolte da sistematizzare nel tempo di carattere quantitativo e qualitativo. Al netto di quelli in corso di definizione, si citano i primi accordi firmati, nello specifico con la Conferenza delle Regioni e delle Province Autonome, con l'Associazione Nazionale Comuni Italiani (ANCI) e con l'Unione Province Italiane (UPI). Per gli scopi dell'Osservatorio, ai fini del monitoraggio del Piano triennale e per le caratteristiche stesse del PNRR, particolare attenzione è stata posta sui Comuni. È previsto infatti l'utilizzo di informazioni primarie fornite direttamente dai Comuni e dalle città metropolitane attraverso lo svolgimento di cicli di raccolta dati.

Contesto normativo e strategico

Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 «Codice dell'amministrazione digitale» (in breve CAD) art. 14-bis lettera c)

Riferimenti normativi europei:

- Ministerial Declaration on eGovernment - Tallinn declaration - 6 ottobre 2017
Regolamento (UE) 2018/1724 del 2 ottobre 2018 che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE) 1024/2012 Berlin Declaration on Digital Society and Value-based Digital Government - 8 dicembre 2020

- Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al comitato delle regioni Bussola per il digitale 2030: il modello europeo per il decennio digitale
- Decisione di esecuzione (ue) della Commissione Europea del 30 giugno 2023 che definisce gli indicatori chiave di prestazione per misurare i progressi compiuti verso il conseguimento degli obiettivi digitali di cui all'articolo 4, paragrafo 1, della decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio

Obiettivo 1.3 – Monitorare e analizzare lo stato di digitalizzazione del paese

Risultati attesi:

- RA1.3.1 - Definizione di un indice di digitalizzazione della PA italiana
- RA1.3.2 - Acquisizione ed elaborazione di informazioni analitiche da Enti Locali
- RA1.3.3 - Aumento delle tipologie e delle fonti dati integrate all'interno dell'Osservatorio

CAP1.PA.10

Le PA che fanno parte del campione alimentano l'indice di digitalizzazione secondo la metodologia definita dal Gruppo di lavoro AgID-ISTAT-DTD

Azioni previste/eseguite: il Comune di San Sperate non fa parte del campione che alimenta l'indice di digitalizzazione secondo la metodologia definita dal Gruppo di lavoro.

CAP1.PA.11

Gli Enti locali partecipano alla prima fase della raccolta dati, garantendo l'accuratezza e la completezza delle informazioni.

Azioni previste/eseguite: il Comune di San Sperate non fa parte del campione che alimenta l'indice di digitalizzazione, ma garantisce la partecipazione alla fase di raccolta dati se e quando riceverà indicazioni precise in merito.

CAP1.PA.12

Gli Enti locali partecipano alla seconda fase della raccolta dati, garantendo l'accuratezza e la completezza delle informazioni.

Azioni previste/eseguite: il Comune di San Sperate non fa parte del campione che alimenta l'indice di digitalizzazione, ma garantisce la partecipazione alla fase di raccolta dati se e quando riceverà indicazioni precise in merito.

Capitolo 2 - Il procurement per la trasformazione digitale

Il procurement per la trasformazione digitale

Scenario

La trasformazione digitale della Pubblica Amministrazione si basa sull'innovazione dei suoi processi, finalizzati al miglioramento dell'efficienza e della qualità dei servizi a partire dalle aree di interesse pubblico ad alto impatto per il benessere dei cittadini come la salute, la giustizia, la protezione dei consumatori, la mobilità, il monitoraggio ambientale, l'istruzione e la cultura, con l'obiettivo di stimolare la diffusione di modelli organizzativi di open innovation.

La concreta attuazione del processo di trasformazione digitale richiede la disponibilità di risorse professionali e strumentali, disponibili in parte all'interno dell'amministrazione pubblica e in parte e all'esterno. Ne consegue che grande attenzione va prestata affinché l'acquisizione di risorse dal mercato (procurement) sia realizzata con efficacia ed efficienza. La stessa riforma nazionale del procurement pubblico, milestone del Piano Nazionale di Ripresa e Resilienza – PNRR (M1C1-70), introdotta dal Codice dei Contratti pubblici (Decreto lgs. N. 36 del 31 marzo 2023) soprattutto con riferimento alla Parte II, "Della digitalizzazione del ciclo di vita dei contratti", introduce un profondo percorso di trasformazione digitale degli acquisti della Pubblica Amministrazione volto alla semplificazione, velocizzazione delle procedure e maggiore trasparenza.

Ciò è tanto più importante se si tiene conto che nel decennio 2013-2022 la Pubblica Amministrazione italiana ha effettuato acquisti per un valore complessivo di oltre 2.900 Miliardi di euro e ha stipulato contratti con oltre 35.000 fornitori. Con un valore che si avvicina al 10% del PIL, la spesa pubblica in appalti è anche uno strumento di politica industriale per il Paese. Di questa grande massa di risorse, la spesa in ICT è valutata in oltre 7 miliardi di euro per l'anno 2022, in aumento rispetto al 2021. Le progettualità in essere e prospettiche si focalizzano principalmente sull'aggiornamento dell'esistente, mentre ancora limitati sono gli investimenti verso l'introduzione di soluzioni digitali che puntino su tecnologie innovative data-driven o verso le nuove frontiere definite dall'adozione di sistemi di intelligenza artificiale.

Gli acquisti di beni e servizi standardizzati

A partire dall'anno 2000 il nostro Paese ha realizzato un programma di "Razionalizzazione degli acquisti", che si basa su strategie di aggregazione e centralizzazione degli acquisti pubblici, in tutti i settori, compreso l'ICT, la digitalizzazione e la trasformazione digitale. L'attuazione del programma di razionalizzazione ha portato negli anni alla costruzione di un sistema di governance incentrato su ANAC, il rafforzamento di Consip quale centrale nazionale di acquisto, la costituzione del sistema dei soggetti aggregatori regionali e del relativo Tavolo tecnico coordinato dal Ministero dell'Economia e delle Finanze, un'imponente digitalizzazione del sistema appalti con la costituzione della Banca dati nazionale dei contratti pubblici (BDNCP).

Gli strumenti di acquisto basati sulle Convenzioni, gli Accordi quadro, il Mercato Elettronico e il Sistema dinamico di acquisizione sono ampiamente disponibili e facilitano l'acquisto di beni e servizi standard per l'ICT, la digitalizzazione e la trasformazione digitale.

Gli acquisti di innovazione per la trasformazione digitale

Già nel 2012 l'obiettivo strategico dell'Agenda Digitale Italiana era quello della modernizzazione dei rapporti tra Pubblica Amministrazione, cittadini e imprese, attraverso azioni dirette a favorire lo sviluppo di domanda e offerta di servizi digitali innovativi e a promuovere la crescita di capacità industriali adeguate a sostenere lo sviluppo di tali servizi.

Subito dopo, con il D.L. 179/2012 (anche noto come Decreto sviluppo 2.0 o Startup Act), l'Italia si è dotata di norme specifiche per promuovere gli appalti che hanno ad oggetto servizi di ricerca e innovazione. Il nuovo Codice dei contratti pubblici ha confermato la disciplina delle procedure per gli acquisti di innovazione: il dialogo competitivo, il partenariato per l'innovazione e l'appalto pre-commerciale. Tali norme definiscono un quadro di strumenti amministrativi e di coordinamento istituzionale tra i livelli ministeriali di governo, i soggetti finanziatori e le agenzie che attuano gli acquisti.

Gli acquisti di innovazione, nel prossimo triennio, sono indirizzati prioritariamente alla sperimentazione di modelli di commercializzazione ed acquisto di soluzioni di intelligenza artificiale ed alla crescita di capacità industriali nel settore, anche attraverso collaborazioni internazionali. Allo stato attuale, Smarter Italy è il principale programma di sperimentazione di appalti di innovazione nella Pubblica Amministrazione. In parallelo, in coerenza con questo programma, diverse amministrazioni hanno svolto, in collaborazione con AGID e utilizzando la Piattaforma per gli appalti di innovazione, consultazioni preliminari di mercato cui hanno partecipato, nel complesso, migliaia di operatori economici. La fase della consultazione è molto importante per l'emersione dei fabbisogni di innovazione e consente alla stazione appaltante di avere gli elementi, in primis, per individuare la procedura da utilizzare per dare avvio all'acquisto di innovazione. Le consultazioni hanno riguardato differenti tematiche, tra cui, la cybersecurity e i sistemi anticontraffazione, lo sviluppo digitale nei paesi ad economia emergente, l'Intelligenza artificiale per i medici di base, i concorsi digitali, la produzione delle materie prime seconde, il comunicare il Made in Italy.

L'ecosistema digitale degli acquisti pubblici

Nelle disposizioni della Parte II del Libro I artt. 19-36 "Digitalizzazione del ciclo di vita dei contratti pubblici" del Codice dei contratti pubblici, è stabilito che dal 1° gennaio 2024 tutte le procedure di acquisto della Pubblica Amministrazione siano svolte in modalità digitale attraverso piattaforme di approvvigionamento digitale (art. 25). Le stazioni appaltanti devono mettere a disposizione degli operatori economici i servizi digitali per partecipare alle procedure di acquisto e gli operatori economici sono obbligati ad utilizzare tali servizi per partecipare alle medesime. Le citate piattaforme devono essere interoperabili, tramite Piattaforma Digitale Nazionale dei Dati (PDND), con la Banca dati nazionale dei contratti pubblici (BDNCP) (art. 23) di ANAC, l'infrastruttura tecnologica abilitante la gestione in digitale

del ciclo di vita dei contratti pubblici. Tale sistema informativo distribuito è definito dal Codice dei contratti pubblici “Ecosistema nazionale di approvvigionamento digitale” (art. 22).

L'Agenzia per l'Italia digitale, con l'adozione delle Regole tecniche e dello Schema Operativo nel rispetto di quanto previsto dal Codice dei contratti pubblici, ha definito i requisiti tecnici delle piattaforme e le modalità di certificazione per il loro funzionamento, per il raggiungimento dei previsti obiettivi di digitalizzazione. La regolazione tecnica dovrà includere, per la fase di “post-award”, l'introduzione del formato UBL per gli ordini elettronici e il documento di trasporto elettronico (DDT), nonché delle modalità di trasmissione attraverso l'infrastruttura di rete PEPPOL che consente lo scambio, in modalità sicura, dei suddetti documenti in formato standard, oltre la previsione di un'evoluzione del Sistema d'Interscambio (SDI) per la conformità del formato domestico della fattura elettronica (FatturaPA) a quello europeo definito con la norma europea EN16931 e l'integrazione con la richiamata infrastruttura di rete PEPPOL.

La digitalizzazione dei contratti pubblici rappresenta un esempio virtuoso di infrastruttura pubblica al servizio di un complesso ecosistema composto da amministrazioni centrali, stazioni appaltanti, operatori economici e molti altri attori. In tale contesto, la PDND assume un ruolo centrale, non solo ai fini della messa in interoperabilità delle banche dati degli enti certificanti (oltre 10 amministrazioni centrali) che devono proseguire nel rendere disponibili i loro dati ai fini della piena operatività del Fascicolo Virtuale dell'Operatore Economico (FVOE, art. 24, Delibera ANAC n. 262 del 20 giugno 2023), ma anche in quanto consente l'accesso agli e-service di ANAC che abilitano l'operatività del ciclo di vita del procurement.

La digitalizzazione degli acquisti pubblici è parte fondamentale del percorso di trasformazione digitale della PA contribuendo a snellire e ad accelerare le procedure amministrative di acquisto, ad allargare la partecipazione dei soggetti che operano nel mercato e a rendere il ciclo di vita degli appalti ancora più trasparente, rendendo semplici e puntuali i necessari controlli. Lo sviluppo dell'ecosistema digitale degli acquisti pubblici, nel prossimo triennio, è indirizzato prioritariamente ad incrementarne la robustezza, attraverso un processo diffuso di certificazione delle piattaforme di approvvigionamento digitale, e a porre le basi per un radicale efficientamento, anche attraverso l'utilizzo di sistemi di intelligenza artificiale.

Organizzazione della stazione appaltante nel nuovo Codice dei Contratti Pubblici

La efficace realizzazione di un processo di acquisto, dalla programmazione alla esecuzione, necessita risorse professionali e organizzazione. Il nuovo Codice prevede che le stazioni appaltanti, per condurre acquisti complessi, siano dotate di risorse umane, risorse strumentali, adeguata esperienza. Pertanto, introduce il sistema di qualificazione delle stazioni appaltanti. Il principio del risultato costituisce criterio prioritario per l'esercizio del potere discrezionale e per l'individuazione della regola del caso concreto, nonché per valutare la responsabilità del personale che svolge funzioni amministrative o tecniche nelle fasi di programmazione, progettazione, affidamento ed esecuzione dei contratti e attribuire gli incentivi al personale coinvolto negli appalti. Nell'attuazione delle procedure di acquisto si richiede quel passaggio da un approccio puramente amministrativo a uno orientato al soddisfacimento delle esigenze concrete, la cui necessità è stata già individuata negli orientamenti della Commissione Europea.

La qualificazione della Stazione appaltante

La qualificazione delle Stazioni appaltanti è uno strumento per attestare la capacità di gestire direttamente, secondo criteri di qualità, efficienza e professionalizzazione, e nel rispetto dei principi di economicità, efficacia, tempestività e correttezza, le attività che caratterizzano il processo di acquisizione e riguarda almeno una delle fasi di progettazione, affidamento o esecuzione del contratto. Il Codice dei contratti pubblici individua tre livelli di qualificazione, base (per servizi e forniture fino alla soglia di 750.000 euro), intermedia (fino a 5 milioni di euro) e avanzata (senza limiti di importo).

Si precisa che il Codice, all'art. 114 comma 8, stabilisce che per i contratti di servizi e forniture di particolare importanza il Direttore dell'esecuzione deve essere diverso dal Responsabile Unico di Progetto (RUP). L'allegato II.14 del suddetto Codice, all'art. 32, stabilisce che sono considerati servizi di particolare importanza, indipendentemente dall'importo, gli interventi particolarmente complessi sotto il profilo tecnologico, le prestazioni che richiedono l'apporto di una pluralità di competenze, gli interventi caratterizzati dall'utilizzo di componenti o di processi produttivi innovativi o dalla necessità di elevate prestazioni per quanto riguarda la loro funzionalità. In via di prima applicazione del Codice sono individuati, tra i servizi di particolare importanza, quelli di telecomunicazione e i servizi informatici. Sono, inoltre, considerate forniture di particolare importanza le prestazioni di importo superiore a 500.000 euro.

L'organizzazione della Stazione appaltante e il ruolo del RUP

Il "nuovo RUP", nel Codice è stato ridenominato Responsabile Unico di Progetto (art. 15 D.lgs. 36/2023), al posto di Responsabile Unico del Procedimento, avvicinandolo alla figura di un project manager, con capacità di gestione delle risorse finanziarie, strumentali ed umane di cui può disporre. Il nuovo Codice riconosce la complessità di una procedura che va dalla pianificazione all'esecuzione e consente alle amministrazioni di definire modelli organizzativi che sembrano più efficaci per la gestione dell'intero ciclo di vita dell'acquisto. Per ogni acquisto, si prevede la nomina di un responsabile di (sub)procedimento per le fasi di programmazione, progettazione, affidamento ed esecuzione. Le relative responsabilità sono ripartite in base ai compiti svolti in ciascuna fase, ferme restando le funzioni di supervisione, indirizzo e coordinamento del RUP. Le stazioni appaltanti possono inoltre istituire una struttura di supporto al RUP e affidare incarichi di assistenza al medesimo. Il Direttore dell'esecuzione è la figura professionale che va a potenziare il RUP negli acquisti di particolare importanza. Fermo restando il rispetto delle disposizioni di servizio eventualmente impartite dal RUP, il Direttore dell'esecuzione opera in autonomia in ordine al coordinamento, alla direzione e al controllo tecnico-contabile nell'esclusivo interesse all'efficiente e sollecita esecuzione del contratto.

Nelle amministrazioni complesse, il processo di approvvigionamento nel settore ICT coinvolge molteplici unità funzionali, tipicamente la funzione Sistema informativo, la funzione Acquisti, la funzione Legale, la funzione Innovazione ove esistente. È fortemente auspicato che il Responsabile per la transizione digitale venga coinvolto negli acquisti ICT.

La collaborazione tra stazioni appaltanti

L'articolo 62 del Codice abilita le stazioni appaltanti a collaborare tra loro, secondo i modelli dell'aggregazione e della centralizzazione. Inoltre, è sempre possibile per le pubbliche amministrazioni attivare collaborazioni con altre amministrazioni e richiedere aiuto nello svolgimento delle procedure di acquisto.

È auspicabile che la collaborazione ricomprenda la fase di progettazione dell'acquisto, con lo scopo di condividere e dare valore alle esperienze pregresse di altre amministrazioni. Lo strumento Analytics della BDNCP, la pubblicazione dei dati aperti della BDNCP e la comunità dei Responsabili per la transizione digitale facilitano la ricerca e la individuazione di quelle amministrazioni che hanno effettuato acquisti ritenuti di interesse.

Il nuovo Codice contratti prevede che la progettazione di servizi e forniture sia articolata in un unico livello, ma l'amministrazione può definire preliminarmente un approfondito "quadro esigenziale", che indirizzi la successiva fase di progettazione nel settore ICT. Tale fase è predisposta dai dipendenti in servizio, i quali ne assumono la responsabilità finale ma, ove sia necessario, rimane la possibilità di ricorrere alla consulenza di professionisti abilitati ed esperti, in particolare per la definizione delle specifiche tecniche o di altri apporti specialistici.

Per la collaborazione tra enti nei progetti ICT sono interessanti anche le nuove opportunità offerte dagli "appalti congiunti" ex art.62 comma 14 del nuovo Codice che stabilisce che due o più stazioni appaltanti possano decidere di svolgere congiuntamente "una o più fasi della procedura di affidamento o di esecuzione di un appalto o di un accordo quadro di lavori, servizi e forniture, purché almeno una di esse sia qualificata allo svolgimento delle fasi stesse in rapporto al valore del contratto. Le stazioni appaltanti sono responsabili in solido dell'adempimento degli obblighi derivanti dal codice. Esse nominano un unico RUP in comune tra le stesse in capo alla stazione appaltante delegata (...). Ciascuna stazione appaltante è responsabile dell'adempimento degli obblighi derivanti dal codice unicamente per quanto riguarda le parti da essa svolte a proprio nome e per proprio conto".

Contesto normativo e strategico

Riferimenti normativi italiani:

- Legge 24 dicembre 2007, n. 244 "Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato" (legge finanziaria 2008) art. 1 co. 209 -214
- Decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla Legge 17 dicembre 2012, n. 221 "Ulteriori misure urgenti per la crescita del Paese", art. 19
- Legge 27 dicembre 2017, n. 205 "Bilancio di previsione dello Stato per l'anno finanziario 2018 e bilancio pluriennale per il triennio 2018-2020", art. 1 co. 411-415
- Decreto Legislativo 27 dicembre 2018, n. 148 - Attuazione della direttiva (UE) 2014/55 del Parlamento europeo e del Consiglio del 16 aprile 2014, relativa alla fatturazione elettronica negli appalti pubblici
- Decreto del Ministero dell'Economia e delle Finanze del 27 dicembre 2019 "Modifica del decreto 7 dicembre 2018 recante: Modalità e tempi per l'attuazione delle disposizioni in materia di emissione e trasmissione dei documenti attestanti

l'ordinazione degli acquisti di beni e servizi effettuata in forma elettronica da applicarsi agli enti del Servizio sanitario nazionale”

- Decreto legislativo 31 marzo 2023, n. 36 “Codice dei contratti pubblici”, artt. 19-26
- Circolare AGID n. 3 del 6 dicembre 2016 “Regole Tecniche aggiuntive per garantire il colloquio e la condivisione dei dati tra sistemi telematici di acquisto e di negoziazione”
- Determinazione AGID n. 137 del 1° giugno 2023 “Requisiti tecnici e modalità di certificazione delle Piattaforme di approvvigionamento digitale”
- Determinazione AGID n. 218 del 25 settembre 2023 “Schema operativo a supporto della Certificazione delle Piattaforme di approvvigionamento digitale”
- Decisione di esecuzione del Consiglio del 13 luglio 2021, che approva il Piano Nazionale di ripresa e resilienza (Allegato)
- Riforma 1.10 - M1C1-70 “Recovery procurement platform” per la modernizzazione del sistema nazionale degli appalti pubblici e il sostegno delle politiche di sviluppo attraverso la digitalizzazione e il rafforzamento della capacità amministrativa delle amministrazioni aggiudicatrici

Riferimenti normativi europei:

- Regolamento (UE) n. 910/2014 del 23 luglio 2014 - eIDAS
- Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni COM (2020) 67 final del 19 febbraio 2020 - Plasmare il futuro digitale dell'Europa
- Comunicazione della Commissione Europea "Orientamenti in materia di appalti per l'innovazione" (2021) 4320 del 18 giugno 2021 - (2021/C 267/01)
- Comunicazione del Consiglio Europeo «Joint Declaration on Innovation Procurement in EU - Information by the Greek and Italian Delegations» del 20 settembre 2021

Obiettivo 2.1 – Rafforzare l’ecosistema nazionale di approvvigionamento digitale

Risultati attesi:

- RA2.1.1 - Diffusione del processo di certificazione delle piattaforme di approvvigionamento digitale

CAP2.PA.01

I soggetti aggregatori devono dotarsi di piattaforme di approvvigionamento che digitalizzano la fase di esecuzione dell’appalto.

Azioni previste/eseguite: il Comune di San Sperate non è un soggetto aggregatore, ma usufruisce delle piattaforme di e-procurement quali il MePA (www.acquistiinretepa.it) e il CAT Sardegna.

CAP2.PA.02

Le stazioni appaltanti devono digitalizzare la fase di esecuzione dell'appalto.

Azioni previste/eseguite: il Comune di San Sperate Dal 1° gennaio 2024, a seguito dell'introduzione del nuovo Codice dei contratti pubblici, approvato con decreto legislativo 31 marzo 2023 n. 36, l'Ente si è adeguato alle nuove indicazioni normative che prevedono la digitalizzazione dell'intero ciclo di vita dei contratti pubblici, ricorrendo all'utilizzo di piattaforme di approvvigionamento digitale certificate quali MePA (www.acquistiinretepa.it) e il CAT Sardegna.

Obiettivo 2.2 – Diffondere l'utilizzo degli appalti innovativi

Risultati attesi:

- RA2.2.1 - Incremento della partecipazione di PMI e start up agli appalti di Innovazione
- RA2.2.3 - Incremento della diffusione degli appalti di innovazione nelle PA

CAP2.PA.03

Le amministrazioni entrano nel programma delle consultazioni di mercato.

Azioni previste/eseguite: il Comune di San Sperate attualmente non partecipa a questo tipo di consultazioni.

CAP2.PA.04

Le amministrazioni che hanno avviato appalti di innovazione completano la fase di aggiudicazione e di esecuzione

Azioni previste/eseguite: il Comune di San Sperate attualmente non ha avviato appalti simili.

Le gare strategiche per la trasformazione digitale

Scenario

Le gare strategiche ICT sono strumenti che consentono alle Amministrazioni di acquisire servizi necessari ad implementare le strategie per la trasformazione digitale della Pubblica Amministrazione. In generale, quindi, sono disponibili servizi per operare sulla definizione di processi e sull'erogazione di servizi digitali, sulla analisi e realizzazione delle componenti applicative e infrastrutturali, con specifico riferimento al paradigma cloud. In sinergia con le previsioni del Piano triennale e al fine di indirizzare e governare la trasformazione digitale della PA italiana, AGID opera una funzione di indirizzo strategico e governance centralizzata di tutte le iniziative, anche mediante la costituzione di organismi di coordinamento e controllo, finalizzati alla direzione strategica e tecnica delle stesse.

In particolare, l'Agenzia per l'Italia digitale svolge le seguenti funzioni, tutte volte a garantire alle amministrazioni strumenti efficaci ed efficienti per il raggiungimento degli obiettivi del Piano triennale:

- fornisce ai soggetti aggregatori gli indirizzi strategici delle nuove iniziative da pubblicare;
- monitora il rispetto dei vincoli contrattuali e la qualità della fornitura;
- monitora lo stato di avanzamento degli Accordi quadro;
- analizza i progetti implementati dalle Amministrazioni per monitorare la coerenza delle iniziative e l'andamento degli indicatori di digitalizzazione e gli obiettivi del Piano triennale perseguibili con l'iniziativa, oltre a favorire modalità di co-working o co-partecipazione finanziaria tra le amministrazioni;
- analizza le proposte di standardizzazione di processi, modelli, soluzioni, metriche, metodologie di stima dei servizi e, nella sua componente pubblica, ne valuta l'adozione;
- valuta le eventuali proposte di evoluzione e/o adeguamento dei servizi da parte del fornitore.

È inoltre in corso l'implementazione di ulteriori azioni concrete volte ad accompagnare le pubbliche amministrazioni per una acquisizione sempre più consapevole degli strumenti disponibili all'interno del paniere delle gare strategiche, al fine di garantire contratti di elevata standardizzazione e qualità. Le gare strategiche ICT si pongono pertanto il duplice obiettivo di:

- creare il "sistema operativo" del Paese, ovvero una serie di componenti fondamentali sui quali definire ed erogare servizi più semplici ed efficaci per i cittadini, le imprese e la stessa Pubblica Amministrazione;
- incentivare l'utilizzo e supportare le amministrazioni nella definizione di contratti coerenti con gli obiettivi definiti dal Piano triennale.

Le iniziative strategiche ICT sono realizzate attraverso appalti aggiudicati da Consip nella forma dell'Accordo quadro, che consentono a tutte le Amministrazioni di acquistare rapidamente i servizi necessari per attuare il percorso di transizione al digitale secondo il paradigma dell'ordine diretto, ove l'Amministrazione non abbia esigenze progettuali peculiari ovvero attraverso lo strumento dell'appalto specifico tra i fornitori selezionati da Consip, con garanzie di qualità e prezzi vantaggiosi. In particolare, le Amministrazioni possono accedere, ad oggi, a un piano molto ricco di gare strategiche che nell'ultimo anno è stato ampliato con le seconde edizioni di alcune iniziative sulla base dell'andamento di adesione registrato per le prime edizioni. In particolare, a luglio 2024 risultavano attive 18 gare, con un massimale di circa 10 miliardi. Sono in corso di attivazione 7 gare, per un massimale di circa 5 miliardi. Le attività di monitoraggio di AGID sulle Gare strategiche hanno carattere di continuità e pertanto periodicamente sul sito, nella sezione del Piano triennale dedicata agli Strumenti, è possibile trovare informazioni aggiornate.

Contesto normativo

Riferimenti normativi italiani:

- Decreto legislativo 31 marzo 2023, n. 36 «Codice dei contratti pubblici»;
- CAD, art.14-bis comma 2 lettera d).

Obiettivo 2.3 – Favorire e monitorare l'utilizzo dei servizi previsti dalle Gare strategiche

Risultati attesi:

- RA2.3.1 - Incremento del livello di trasformazione digitale mediante la disponibilità di Gare strategiche allo scopo definite

CAP2.PA.05

Le PA, nel proprio piano acquisti, programmano i fabbisogni di adesione alle iniziative strategiche disponibili per il perseguimento degli obiettivi del Piano triennale

Azioni previste/eseguite: il Comune di San Sperate ha pianificato nel proprio programma triennale ICT i fabbisogni relativi alla digitalizzazione e trasformazione digitale, in termini di infrastrutture, piattaforme, processi, software applicativi, hardware, connettività e realizzazione di progetti innovativi. Lo strumento d'acquisto più idoneo per il raggiungimento degli obiettivi prefissati verrà stabilito in prossimità dell'avvio dell'iter procedurale a seconda delle iniziative Consip disponibili.

CAP2.PA.06

Le PA, nel proprio piano acquisti, programmano i fabbisogni di adesione alle iniziative strategiche disponibili per il perseguimento degli obiettivi del Piano triennale anni 2026/2027

Azioni previste/eseguite: il Comune di San Sperate ha pianificato nel proprio programma triennale ICT i fabbisogni relativi alla digitalizzazione e trasformazione digitale, in termini di infrastrutture, piattaforme, processi, software applicativi, hardware, connettività e realizzazione di progetti innovativi. Lo strumento d'acquisto più idoneo per il raggiungimento degli obiettivi prefissati verrà stabilito in prossimità dell'avvio dell'iter procedurale a seconda delle iniziative Consip disponibili.

PARTE IIa – LE COMPONENTI TECNOLOGICHE

Descrizione PARTE SECONDA

Componenti tecnologiche: le componenti tecnologiche del modello strategico sono riportate nei capitoli (numerati da 3 a 7) su Servizi, Piattaforme, Dati e intelligenza artificiale, Infrastrutture, Sicurezza. Il tema dell'interoperabilità diventa trasversale a tutti i capitoli ed è evidenziato in particolare nel capitolo dedicato ai Servizi. Il capitolo «Dati» è integrato da una sezione nuova dedicata all'intelligenza artificiale. Sono riportati alcuni principi generali che dovranno essere adottati dalle pubbliche amministrazioni e declinati in fase di applicazione, tenendo in considerazione lo scenario in veloce evoluzione.

Capitolo 3 - Servizi

Introduzione al Capitolo

Negli ultimi anni, la digitalizzazione è diventata una forza trainante per l'innovazione nei servizi pubblici, con gli enti locali al centro di questo cambiamento. L'adozione di tecnologie digitali è essenziale per migliorare l'efficienza, aumentare la trasparenza e garantire la qualità dei servizi offerti ai cittadini. In questo processo di trasformazione è indispensabile anche definire un framework di riferimento per guidare ed uniformare le scelte tecnologiche. In particolare, l'architettura a microservizi può esser considerata come una soluzione agile e scalabile, che permette di standardizzare i processi digitali e di facilitare anche il processo di *change-management* nelle organizzazioni governative locali. Per garantire la possibilità a tutti gli Enti di poter cogliere questa enorme opportunità, anche a coloro che si trovano in condizioni di carenze di know-how e risorse, il presente Piano propone e promuove un'evoluzione del Modello di interoperabilità passando dalla sola condivisione dei dati a quella della condivisione dei servizi.

I vantaggi dell'utilizzo di un'architettura basata su microservizi sono:

- Flessibilità e scalabilità
- Agilità nello sviluppo
- Integrazione semplificata
- Resilienza e affidabilità

La transizione verso un'architettura a microservizi richiede la consapevolezza che non sia necessario solo un intervento tecnologico ma che richiede soprattutto un controllo per la gestione del cambiamento che, come abbiamo visto nel cap. 1 coinvolge diverse fasi chiave, quali la formazione continua, il coinvolgimento attivo degli stakeholder, il monitoraggio dell'impatto del cambiamento e naturalmente anche una comunicazione efficace. Per gli enti che potrebbero non avere un know-how interno sufficiente, l'architettura a microservizi offre l'opportunità di sfruttare le soluzioni e i servizi già sviluppati da altri enti innovando profondamente il concetto di riuso. Questo approccio non solo consente di colmare il gap

strutturale interno, ma fornisce anche un vantaggio significativo in termini di risparmio di tempo e ottimizzazione delle risorse.

L'architettura a microservizi, attraverso la condivisione di processi e lo sviluppo once only riduce la duplicazione degli sforzi e dei costi. La condivisione di e-service vede nella Piattaforma Digitale Nazionale Dati Interoperabilità (PDND Interoperabilità) il layer focale per la condivisione di dati e processi. La sostenibilità e la crescita collaborativa nell'ambito dell'architettura a microservizi non si limita al singolo ente. In molte situazioni, possono entrare in gioco altre istituzioni a supporto, come Regioni, Unioni o Enti capofila (HUB nazionali e/o regionali), che possono agire svolgendo un ruolo fondamentale nello sviluppo fornendo soluzioni tecnologiche e/o amministrative, per facilitare l'integrazione e l'implementazione del processo di innovazione. Questo approccio consente agli enti più piccoli di beneficiare delle risorse condivise e delle soluzioni già implementate, accelerando così il processo di digitalizzazione. Come già accennato nel capitolo 2, il Codice dei contratti pubblici, offre in tal senso nuove opportunità, come ad esempio la strutturazione di "appalti congiunti" ex art.62 comma 14 del D. Lgs. 36/2023.

Il coinvolgimento attivo delle istituzioni aggregate come facilitatori tecnologici è essenziale per garantire una transizione armoniosa verso l'architettura a microservizi. Guardando al futuro, la sinergia tra enti locali, Regioni e altre istituzioni aggregate pone le basi per un ecosistema digitale coeso, capace di affrontare sfide complesse e di offrire servizi pubblici sempre più efficienti. La collaborazione istituzionale diventa così un elemento fondamentale per plasmare un futuro digitale condiviso e orientato all'innovazione.

E-Service in interoperabilità tramite PDND

Scenario

L'interoperabilità facilita l'interazione digitale tra Pubbliche Amministrazioni, cittadini e imprese, recependo le indicazioni dell'European Interoperability Framework e, favorendo l'attuazione del principio once only secondo il quale la PA non deve chiedere a cittadini e imprese dati che già possiede.

A fine di raggiungere la completa interoperabilità dei dataset e dei servizi chiave tra le PA centrali e locali e di valorizzare il capitale informativo delle pubbliche amministrazioni, nell'ambito del Sub- Investimento M1C1_1.3.1 «Piattaforma nazionale digitale dei dati» del Piano Nazionale di Ripresa e Resilienza, è stata realizzata la Piattaforma Digitale Nazionale Dati (PDND). La PDND è lo strumento per gestire l'autenticazione, l'autorizzazione e la raccolta e conservazione delle informazioni relative agli accessi e alle transazioni effettuate suo tramite. La Piattaforma fornisce un insieme di regole condivise per semplificare gli accordi di interoperabilità snellendo i processi di istruttoria, riducendo oneri e procedure amministrative. Un ente può aderire alla Infrastruttura interoperabilità PDND siglando un accordo di adesione, attraverso le funzionalità messe a disposizione dell'infrastruttura.

La PDND permette alle amministrazioni di pubblicare e-service, ovvero servizi digitali conformi alle Linee Guida realizzati ed erogati attraverso l'implementazione di API (Application Programming Interface) REST o SOAP (per retrocompatibilità) cui vengono associati degli attributi minimi necessari alla fruizione. Le API esposte vengono registrate e popolano il Catalogo pubblico degli e-service.

La Piattaforma dovrà evolvere recependo le indicazioni pervenute dalle varie amministrazioni e nel triennio a venire dovrà anche:

1. consentire la condivisione di dati di grandi dimensioni (bulk) prodotti dalle amministrazioni e l'elaborazione di politiche data-driven;
2. offrire alle amministrazioni la possibilità di accedere ai dati di enti o imprese di natura privata non amministrativa e di integrarsi con i processi di questi ultimi;
3. permettere alle amministrazioni di essere informate, in maniera asincrona, su eventuali variazioni a dati precedentemente fruiti, abilitando anche una gestione intelligente dei meccanismi di caching locale delle informazioni;
4. attivare modelli di erogazione inversa, con i quali un ente, potrà erogare e-service, abilitati a ricevere dati da altri soggetti;
5. abilitare lo scambio dato sia in modalità sincrona che asincrona, permettendo anche il trasferimento di grosse moli di dati, o di pacchetti dati che necessitano di elevati tempi di elaborazione per il confezionamento;
6. consentire ad una amministrazione di delegare un altro aderente alla piattaforma ad utilizzare per suo conto le funzionalità dell'infrastruttura medesima per la registrazione, la modifica degli e-service sul Catalogo API e la gestione delle richieste di fruizione degli e-service, ivi compresa la compilazione dell'analisi dei rischi;
7. pubblicare i propri dati aperti attraverso API che siano catalogate secondo le norme pertinenti (DCAT_AP-IT, INSPIRE, ...) e che possano essere raccolte nei portali nazionali ed europei.

Al fine di sviluppare servizi integrati sempre più efficienti ed efficaci e di fornire a cittadini e imprese servizi rispondenti alle rispettive esigenze, il Dipartimento per la Trasformazione Digitale supporta e PA nell'adozione del Modello di interoperabilità, pianificando e coordinando iniziative di condivisione, anche attraverso protocolli d'intesa e accordi finalizzati a:

- costituzione di tavoli e gruppi di lavoro;
- avvio di progettualità congiunte;
- capitalizzazione di soluzioni realizzate dalla PA in open source o su siti o forum per condividere la conoscenza

Maggiori dettagli sulla **Piattaforma Digitale Nazionale Dati** sono disponibili sul portale di progetto.

Contesto normativo

Riferimenti normativi italiani:

- Decreto legislativo 30 giugno 2003, n. 196 «Codice in materia di protezione dei dati personali»
- Decreto legislativo 7 marzo 2005, n. 82 «Codice dell'amministrazione digitale» in breve CAD), artt. 12, 15, 50, 50-ter, 73, 75
- Decreto del Presidente della Repubblica 7 settembre 2010, n. 160 «Regolamento per la semplificazione ed il riordino della disciplina sullo sportello unico per le attività produttive, ai sensi dell'articolo 38, comma 3, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133»
- Decreto-legge 14 dicembre 2018, n. 135, convertito con modificazioni dalla Legge 11 febbraio 2019, n. 12 «Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la Pubblica Amministrazione», art. 8, comma 3
- Decreto-legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 «Misure urgenti per la semplificazione e l'innovazione digitale», art. 34
- Decreto-legge 31 maggio 2021, n. 77, convertito con modificazioni dalla Legge 29 luglio 2021, n. 108 «Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure», art. 39
- Linee Guida AGID per transitare al nuovo modello di interoperabilità (2017)
- Linee Guida AGID sull'interoperabilità tecnica delle Pubbliche Amministrazioni (2021)
- Linee Guida AGID sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi e delle basi di dati (2021)
- Linee Guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici
- Decreto 12 novembre 2021 del Ministero dello sviluppo economico di modifica dell'allegato tecnico del decreto del Presidente della Repubblica 7 settembre 2010, n. 160
- DECRETO 22 settembre 2022 della Presidenza Del Consiglio Dei Ministri
- Piano Nazionale di Ripresa e Resilienza:
 - Investimento M1C1 1.3: «Dati e interoperabilità»
 - Investimento M1C1 2.2: «Task Force digitalizzazione, monitoraggio e performance»

Riferimenti normativi europei:

- Regolamento (UE) 2014/910 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (in breve eIDAS)
- Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (in breve GDPR)

- European Interoperability Framework -Implementation Strategy (2017)
- Interoperability solutions for public administrations, businesses and citizens (2017)

Obiettivo 3.1 – Migliorare la capacità di erogare e-service

Risultati attesi:

- RA3.1.1 - Incremento del numero di «e-service» registrati sul Catalogo Pubblico PDND
- RA3.1.2 - Aumento del numero di Richieste di Fruizione Autorizzate su PDND
- RA3.1.3 - Ampliamento del numero delle amministrazioni coinvolte nell'evoluzione delle Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni

CAP3.PA.01

Le PA cessano di utilizzare modalità di interoperabilità diverse da PDND.

Azioni previste/eseguite: il Comune di San Sperate ha iniziato il processo di migrazione dei servizi in interoperabilità.

CAP3.PA.02

Le Amministrazioni possono iniziare la migrazione dei servizi erogati in interoperabilità dalle attuali modalità alla PDND

Azioni previste/eseguite: il Comune di San Sperate ha iniziato il processo di migrazione dei servizi in interoperabilità.

CAP3.PA.03

Le PA continuano a popolare il Catalogo delle API della Piattaforma Digitale Nazionale Dati con le API conformi alle "Linee guida sull'interoperabilità tecnica delle pubbliche amministrazioni".

Azioni previste/eseguite: il Comune di San Sperate ha iniziato il processo di migrazione dei servizi in interoperabilità.

CAP3.PA.04

Le PA locali rispondono ai bandi pubblicati per l'erogazione di API su PDND.

Azioni previste/eseguite: il Comune di San Sperate attualmente non ha API di erogazione attive. Nel prossimo triennio verrà iniziato il processo di migrazione dei servizi in interoperabilità.

CAP3.PA.05

Le PA centrali siglano accordi per l'erogazione di API su PDND.

Azioni previste/eseguite: il Comune di San Sperate non è una PA Centrale, obiettivo non applicabile.

CAP3.PA.06

Le PA utilizzano le API presenti sul Catalogo.

Azioni previste/eseguite: il Comune di San Sperate utilizza le API relative a SEND e ANNSCU, e nel prossimo triennio si prevedono nuove implementazioni.

CAP3.PA.07

Le PA effettuano richieste di fruizione di servizi erogati da privati.

Azioni previste/eseguite: il Comune di San Sperate valuterà la possibilità di utilizzare servizi erogati da privati.

CAP3.PA.08

Le PA evidenziano le esigenze che non trovano riscontro nella “Linee guida sull’interoperabilità tecnica delle pubbliche amministrazioni” e partecipano alla definizione di pattern e profili di interoperabilità per l’aggiornamento delle stesse.

Azioni previste/eseguite: il Comune di San Sperate non ha evidenziato esigenze che non trovano riscontro nella “Linee guida sull’interoperabilità tecnica delle pubbliche amministrazioni”

Progettazione dei servizi: accessibilità e design

Scenario

Il miglioramento della qualità e dell’inclusività dei servizi pubblici digitali costituisce la premessa indispensabile per l’incremento del loro utilizzo da parte degli utenti, siano questi cittadini, imprese o altre pubbliche amministrazioni. Nell’attuale processo di trasformazione digitale è essenziale che i servizi abbiano un chiaro valore per l’utente. Questo obiettivo richiede un approccio multidisciplinare nell’adozione di metodologie e tecniche interoperabili per la progettazione di un servizio. La qualità finale, così come il costo complessivo del servizio, non può infatti prescindere da un’attenta analisi dei molteplici layer, tecnologici e organizzativi interni, che strutturano l’intero processo della prestazione erogata, celandone la complessità sottostante.

Ciò implica anche la necessità di un’adeguata semplificazione dei procedimenti e un approccio sistematico alla gestione dei processi interni, sotto il coordinamento del Responsabile per la transizione al digitale, dotato di un ufficio opportunamente strutturato e con il fondamentale coinvolgimento delle altre strutture responsabili dell’organizzazione e del controllo strategico. È cruciale, inoltre, il rispetto degli obblighi del CAD in materia di progettazione, accessibilità, privacy, gestione dei dati e riuso, al fine di massimizzare l’efficienza dell’investimento di denaro pubblico e garantire la sovranità digitale con soluzioni software strategiche sotto il completo controllo della Pubblica Amministrazione.

Occorre quindi agire su più livelli e migliorare la capacità delle pubbliche amministrazioni di generare ed erogare servizi di qualità attraverso:

- l'adozione di modelli e strumenti validati e a disposizione di tutti;
- il costante monitoraggio da parte delle PA dei propri servizi online;
- l'incremento del livello di accessibilità dei servizi erogati tramite siti web e app mobile;
- lo scambio di buone pratiche tra le diverse amministrazioni, da attuarsi attraverso la definizione, la modellazione e l'organizzazione di comunità di pratica;
- il riuso e la condivisione di software e competenze tra le diverse amministrazioni.

Per incoraggiare tutti gli utenti a privilegiare il canale online rispetto a quello esclusivamente fisico, rimane necessaria una decisa accelerazione nella semplificazione dell'esperienza d'uso complessiva e un miglioramento dell'inclusività dei servizi, nel pieno rispetto delle norme riguardanti l'accessibilità e il Regolamento generale sulla protezione dei dati. Per il monitoraggio dei propri servizi, le PA possono utilizzare Web Analytics Italia, una piattaforma nazionale open source che offre rilevazioni statistiche su indicatori utili al miglioramento continuo dell'esperienza utente. Per la realizzazione dei propri servizi digitali, le PA possono utilizzare il Design System del Paese, che consente la realizzazione di interfacce coerenti e accessibili by default, concentrando i budget di progettazione e sviluppo sulle parti e i processi caratterizzanti dello specifico servizio digitale.

Contesto normativo

Riferimenti normativi italiani:

- Legge 9 gennaio 2004, n. 4 (Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici)
- Decreto legislativo 7 marzo 2005, n. 82 «Codice dell'amministrazione digitale» (in breve CAD), art. 7, 17, 23, 53, 54, 68, 69 e 71
- Decreto Ministeriale 30 aprile 2008 (Regole tecniche disciplinanti l'accessibilità agli strumenti didattici e formativi a favore degli alunni disabili).
- Legge 3 marzo 2009, n. 18 - Ratifica ed esecuzione della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità
- Decreto Legislativo 10 agosto 2018, n. 106 (Attuazione della direttiva (UE) 2016/2102 relativo all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici)
- Decreto-Legge 16 luglio 2020, n. 76 (Misure urgenti per la semplificazione e l'innovazione digitale)
- Decreto Legislativo 27 maggio 2022, n. 82 - «Attuazione della direttiva (UE) 2019/882 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sui requisiti di accessibilità dei prodotti e dei servizi.»
- Linee Guida AGID su acquisizione e riuso del software per la Pubblica Amministrazione (2019)
- Linee Guida AGID sull'accessibilità degli strumenti informatici (2020)

- Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici (2021)
- Linee Guida AGID di design per i siti internet e i servizi digitali della PA (2022)
- Determinazione AGID n.354/2022 del 22 dicembre 2022 - Linee Guida sull'accessibilità degli strumenti informatici adottate con Determinazione n. 437/2019 del 20 dicembre 2019 e rettificata con Determinazione n. 396/2020 del 10 settembre 2020 - Rettifica per adeguamento a norma tecnica europea armonizzata sopravvenuta
- Piano Nazionale di Ripresa e Resilienza:
 - Investimento 1.3: «Dati e interoperabilità»
 - Investimento 1.4: «Servizi digitali e cittadinanza digitale»

Riferimenti normativi europei:

- Direttiva (UE) 2016/2102 del 26 ottobre 2016 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici
- Decisione di esecuzione (UE) 2018/1524 della Commissione dell'11 ottobre 2018 che stabilisce una metodologia di monitoraggio e definisce le disposizioni riguardanti la presentazione delle relazioni degli Stati membri conformemente alla direttiva (UE) 2016/2102 del Parlamento europeo e del Consiglio relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici
- Direttiva (UE) 2019/882 del parlamento europeo e del consiglio, del 17 aprile 2019, sui requisiti di accessibilità dei prodotti e dei servizi
- Decisione di esecuzione (UE) 2021/1339 della Commissione dell'11 agosto 2021 che modifica la decisione di esecuzione (UE) 2018/2048 per quanto riguarda la norma armonizzata per i siti web e le applicazioni mobili

Obiettivo 3.2 – Migliorare la capacità di generare e erogare e-service

Risultati attesi:

- RA3.2.1 - Diffusione del modello di riuso di software tra le amministrazioni in attuazione delle Linee Guida AGID sull'acquisizione e il riuso del software per la Pubblica Amministrazione
- RA3.2.2 - Incremento dell'accessibilità dei servizi digitali
- RA3.2.3 - Incremento e diffusione dei modelli standard di siti e servizi digitali, disponibili in Designers Italia

CAP3.PA.09

Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web.

Azioni previste/eseguite: il Comune di San Sperate ha pubblicato, come ogni, i propri obiettivi di accessibilità per l'anno 2026, e pubblicati nella sezione Amministrazione Trasparente del portale istituzionale.

CAP3.PA.10

Le Regioni, le Province Autonome, le città metropolitane e i capoluoghi delle Città metropolitane effettuano un test automatico di accessibilità sul proprio sito istituzionale indicato su <https://indicepa.gov.it/ipa-portale/>, utilizzando la piattaforma Mauve++.

Azioni previste/eseguite: il Comune di San Sperate non rientra nell'elenco di PA con obbligo test automatico con Mauve++.

CAP3.PA.11

Le PA pubblicano, entro il 23 settembre, esclusivamente tramite l'applicazione form.AGID.gov.it, la dichiarazione di accessibilità per ciascuno dei propri siti web e APP mobili.

Azioni previste/eseguite: il Comune di San Sperate ha pubblicato correttamente le dichiarazioni di accessibilità per l'anno 2025 ed entro la scadenza verranno pubblicati anche i dati relativi all'anno 2026.

CAP3.PA.12

Tutte le Regioni, le Province autonome, le Città metropolitane, i Comuni capoluogo delle Città metropolitane attivano Web Analytics Italia per la rilevazione delle statistiche di utilizzo del proprio sito web istituzionale presente su IndicePA.

Azioni previste/eseguite: il Comune di San Sperate non rientra tra le categorie di PA indicate nella linea d'azione.

Formazione, gestione e conservazione dei documenti informatici

Scenario

Il tema della dematerializzazione degli archivi cartacei risulta cruciale affinché le amministrazioni possano conseguire i propri obiettivi di digitalizzazione. Le nuove Linee guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agenzia per l'Italia digitale, adottate ai sensi dell'art. 71 del CAD e in vigore dal 1° gennaio 2022, rappresentano un importante contributo nel rafforzamento e nell'armonizzazione del quadro normativo di riferimento in tema di produzione, gestione e conservazione dei documenti informatici, mirando a semplificare e rendere più accessibile la materia, integrandola ove necessario, per ricondurla in un unico documento sistematico di pratico utilizzo. Al loro interno sono delineati i necessari adeguamenti organizzativi e funzionali richiesti alle pubbliche amministrazioni, chiamate a consolidare e rendere concreti i principi di trasformazione digitale enunciati nel CAD e nel Testo Unico sulla Documentazione Amministrativa - TUDA.

Le Linee guida costituiscono la premessa fondamentale dell'agire amministrativo in ambiente digitale, in attuazione degli obiettivi di semplificazione, trasparenza, partecipazione e di economicità, efficacia ed efficienza, già prescritti dalla Legge n.241/1990, assicurando la corretta impostazione metodologica per la loro realizzazione nel complesso percorso di

transizione digitale. La Pubblica Amministrazione è tenuta ad assicurare la rispondenza alle Linee guida, adeguando i propri sistemi di gestione informatica dei documenti, al fine di garantire effetti giuridici conformi alle stesse nei processi documentali, nonché ad ottemperare alle seguenti misure:

- gestione appropriata dei documenti sin dalla loro fase di formazione per il corretto adempimento degli obblighi di natura amministrativa, giuridica e archivistica tipici della gestione degli archivi pubblici, come delineato nel paragrafo 1.11 delle Linee guida;
- gestione dei flussi documentali mediante aggregazioni documentali informatiche, come specificato nel paragrafo 3.3;
- nomina dei ruoli e delle responsabilità previsti, come specificato ai paragrafi 3.1.2 e 4.4;
- adozione del Manuale di gestione documentale e del Manuale di conservazione, come specificato ai paragrafi 3.5 e 4.7;
- pubblicazione dei provvedimenti formali di nomina e dei manuali in una parte chiaramente identificabile dell'area "Amministrazione trasparente", prevista dall'art. 9 del D.Lgs. 33/2013;
- rispetto delle misure minime di sicurezza ICT, emanate da AGID con Circolare del 18 aprile 2017, n. 2/2017;
- rispetto delle in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR);
- trasferimento dei documenti al sistema di conservazione, ai sensi del paragrafo 4 e dell'art. 44, comma 1-bis, del CAD.

Il corretto assolvimento di tali obblighi incide significativamente non solo sull'efficacia e l'efficienza della Pubblica Amministrazione, migliorando i processi interni e facilitando gli scambi informativi tra le amministrazioni e il settore privato, ma rappresenta anche un elemento fondamentale nella prestazione di servizi di alta qualità ai cittadini e alle imprese, assicurando trasparenza, accessibilità e protezione di dati e documenti.

Nell'ambito delle sue funzioni di vigilanza, verifica, controllo e monitoraggio, e conformemente a quanto stabilito dall'articolo 18-bis del CAD, l'Agenzia per l'Italia digitale ha pianificato di avviare un'attività di monitoraggio riguardante l'adempimento degli obblighi specificati dalle Linee guida. A questo scopo, entro il 2024 verrà sviluppato un modello basato su indicatori chiari e dettagliati, supportato da un accurato percorso metodologico. Questo permetterà di procedere con un monitoraggio efficace e sistematico, da realizzarsi entro il 2025 per le disposizioni sulla Gestione documentale, ed entro il 2026 per quelle relative alla Conservazione digitale. Per il futuro a breve termine, al fine di consentire alle amministrazioni di realizzare le attività di dematerializzazione degli archivi cartacei sarà necessario definire ulteriori adeguati strumenti di procurement che possano supportare il conseguimento degli obiettivi di digitalizzazione.

Contesto normativo

Riferimenti normativi italiani:

- Legge 241/1990, Nuove norme sul procedimento amministrativo
- DPR 445/2000, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
- Decreto legislativo 196/2003, Codice in materia di protezione dei dati personali.
- Decreto legislativo 42/2004, Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137.
- Decreto legislativo 82/2005 e ss.mm.ii., Codice dell'amministrazione digitale.
- Decreto legislativo 33/2013, Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni.
- Decreto del Presidente della Repubblica 22 febbraio 2013, Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.
- Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, misure minime di sicurezza ICT.
- Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici (2021)
- Vademecum per l'implementazione delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici, AGID (2022)
- Modelli di interoperabilità tra sistemi di conservazione, AGID (2022)
- La conservazione delle basi di dati, AGID (2023)

Riferimenti normativi europei:

- Regolamento (UE) 910/2014, Regolamento eIDAS in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.
- Regolamento (UE) 679/2016 (GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Obiettivo 3.3 – Consolidare l'applicazione delle Linee guida per la formazione, gestione e conservazione documentale

Risultati attesi:

- RA3.3.1 - Monitorare l'attuazione delle linee guida

CAP3.PA.13

Le PA devono verificare che in "Amministrazione trasparente" sia pubblicato il manuale di

gestione documentale, la nomina del responsabile della gestione documentale per ciascuna AOO e qualora siano presenti più AOO la nomina del coordinatore della gestione documentale.

Azioni previste/eseguite: il Comune di San Sperate non ha ancora nominato il Responsabile per la gestione documentale ed è in fase di prima stesura del relativo manuale, che risulta ancora non approvato e pubblicato.

CAP3.PA.14

Le PA devono verificare che in “Amministrazione trasparente” sia pubblicato il manuale di conservazione e la nomina del responsabile della conservazione.

Azioni previste/eseguite: il Comune di San Sperate non ha ancora nominato il Responsabile per la gestione documentale ed è in fase di prima stesura del relativo manuale, che risulta ancora non approvato e pubblicato.

Single Digital Gateway

Scenario

Nel triennio precedente è stata attuata la parte core del Regolamento Europeo EU 2018/1724 sul Single Digital Gateway (SDG) che, con l'obiettivo di costruire uno sportello unico digitale a livello europeo per consentire a cittadini e imprese di esercitare più facilmente i propri diritti e fare impresa all'interno dell'Unione europea, ha di fatto messo online le 21 procedure richieste (19 applicabili in Italia) delle pubbliche amministrazioni direttamente coinvolte in quanto titolari dei servizi. Il Regolamento, entrato in vigore il 2 ottobre 2018, infatti, ha stabilito le norme per:

- l'istituzione e la gestione di uno sportello digitale unico per offrire ai cittadini e alle imprese europee un facile accesso a:
 - informazioni di alta qualità;
 - procedure efficienti e interamente online;
 - servizi di assistenza e di risoluzione dei problemi;
- l'uso di procedure da parte di utenti transfrontalieri e l'applicazione del principio once only in accordo con le specifiche normative dei differenti Stati Membri.

A dicembre 2023 AGID ha completato le attività di integrazione e collaudo delle componenti architetturali nazionali SDG, sia per l'interoperabilità tra PA italiane, sia per quella tra PA italiane e quelle degli Stati Membri. Le pubbliche amministrazioni competenti per i procedimenti amministrativi relativi alle procedure (di cui all'Allegato II del Regolamento UE 2018/1724) hanno adeguato i propri procedimenti amministrativi alle specifiche tecniche di implementazione del Single Digital Gateway.

Dopo aver reso disponibile online i servizi relativi delle procedure previste, le attività per il Single Digital Gateway del triennio 2024-2026 riguarderanno prevalentemente azioni di

mantenimento, monitoraggio e miglioramento della qualità e dell'accesso ai servizi digitali offerti dallo Sportello per l'Italia, in particolare:

1. monitoraggio delle componenti nazionali e dei servizi delle PA competenti per garantire l'operatività di tutta la filiera coinvolta nell'attuazione dei processi nazionali e transfrontalieri del Single Digital Gateway (SDG) attraverso la progettazione e sviluppo di un Operation Center, capace di mettere a sistema tutti gli stakeholder coinvolti che dovranno lavorare in maniera sinergica e standardizzata nella gestione dei processi di operation. Il sistema prevede la predisposizione di un servizio di supporto continuativo di gestione del portafoglio delle applicazioni realizzate e rilasciate, che comprende la presa in carico e la risoluzione delle richieste utente pervenute ad AGID da cittadini e pubbliche amministrazioni (help desk);
2. supporto alla diffusione dello sportello e del suo utilizzo presso i cittadini e le imprese: rientrano in questa azione attività di supporto alla diffusione dei servizi e attività statistiche di monitoraggio e analisi riguardanti le visite degli utenti alle pagine web impattate dalle singole procedure, nonché al catalogo dei servizi.

Contesto normativo

Riferimenti normativi italiani:

- Linee di indirizzo per i Soggetti sub-attuatori individuati tramite Accordi di collaborazione ai sensi dell'art. 15 della Legge n. 241/1990 e dell'art. 5, comma 6 del D.Lgs. n. 50/2016 per la realizzazione della misura 1.3.2 «Single Digital Gateway» PNRR
- Piano Nazionale di Ripresa e Resilienza:
 - Investimento 1.3: «Dati e interoperabilità»
 - Investimento 1.4: «Servizi digitali e cittadinanza digitale»

Riferimenti normativi europei:

- Regolamento (UE) 2018/1724 del Parlamento europeo e del Consiglio, del 2 ottobre 2018, che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE) n. 1024/2012

Obiettivo 3.4 – SDG (Single Digital Gateway) - Monitorare e migliorare la qualità e l'accesso ai servizi digitali offerti dallo Sportello per l'Italia

Risultati attesi:

- RA3.4.1 - Piena operatività dell'Operation Center
- RA3.4.2 - Diffusione e pieno utilizzo dello Sportello

CAP3.PA.15

Le PA italiane aderenti agli Accordi e interessate usano gli strumenti dell'Operation Center e svolgono azioni correttive sul funzionamento dei servizi e delle procedure sulla base delle segnalazioni ricevute.

Azioni previste/eseguite: il Comune di San Sperate non rientra nelle PA aderente agli accordi per il Single Digital Gateway.

CAP3.PA.16

Le PA italiane aderenti agli Accordi in base alle proprie esigenze partecipano alle azioni di sensibilizzazione effettuate da AGID.

Azioni previste/eseguite: il Comune di San Sperate non rientra nelle PA aderente agli accordi per il Single Digital Gateway.

Capitolo 4 - Piattaforme

Introduzione al Capitolo

Come per i precedenti Piani, il Piano triennale per l'informatica nella Pubblica Amministrazione 2024-26 prende in esame l'evoluzione delle piattaforme della Pubblica Amministrazione, che offrono funzionalità fondamentali nella digitalizzazione dei processi e dei servizi della PA. La raggiunta maturità di alcune piattaforme, già presentate nelle precedenti edizioni del Piano, permette qui di focalizzarsi sui servizi che esse offrono a cittadini, a imprese e ad altre amministrazioni, in continuità con quanto descritto nel capitolo precedente «Servizi».

Nella prima parte di questo capitolo, quindi, si illustrano le piattaforme nazionali che erogano servizi a cittadini e imprese: PagoPA, Applo, Send, Spid e Cie, NoiPA, Fascicolo sanitario elettronico e SUAP/SUE. L'obiettivo riferibile a tutte queste piattaforme è comune, si tratta di migliorare i servizi già erogati nei termini che verranno dettagliati nei risultati attesi e nelle linee di azione. In questa sezione, la descrizione di ciascuna piattaforma riporterà lo stesso obiettivo mentre gli altri elementi descrittivi saranno specifici della piattaforma presa in esame. Nella seconda parte di questo capitolo verranno descritte le piattaforme che attestano attributi ed infine si parlerà di basi di dati di interesse nazionale.

Piattaforme nazionali che erogano servizi a cittadini/imprese o ad altre PA

Scenario

PAGO PA - pagoPA è la piattaforma che consente ai cittadini di effettuare pagamenti digitali verso la Pubblica Amministrazione in modo veloce e intuitivo. pagoPA offre la possibilità ai cittadini di scegliere tra i diversi metodi di pagamento elettronici in base alle proprie esigenze e abitudini, grazie all'opportunità per i singoli enti pubblici di interfacciarsi con diversi attori del mercato e integrare i propri servizi di incasso con soluzioni innovative. L'obiettivo di pagoPA, infatti, è portare a una maggiore efficienza e semplificazione nella gestione dei pagamenti dei servizi pubblici, sia per i cittadini sia per le amministrazioni, favorendo una costante diminuzione dell'uso del contante.

APP IO - L'app IO è l'esito di un progetto open source nato con l'obiettivo di mettere a disposizione di enti e cittadini un unico canale da cui fruire di tutti i servizi pubblici digitali, quale pilastro della strategia del Governo italiano per la cittadinanza digitale. La visione alla base di IO è mettere al centro il cittadino nell'interazione con la Pubblica Amministrazione, attraverso un'applicazione semplice e intuitiva disponibile direttamente sul proprio smartphone. In particolare, l'app IO rende concreto l'articolo 64 bis del Codice dell'Amministrazione Digitale, che istituisce un unico punto di accesso per tutti i servizi digitali, erogato dalla Presidenza del Consiglio dei Ministri.

SEND - La piattaforma SEND - Servizio Notifiche Digitali (anche noto come Piattaforma Notifiche Digitali di cui all'art. 26 del decreto-legge 76/2020 s.m.i.) rende più veloce, economico e sicuro l'invio e la ricezione delle notifiche a valore legale: permette infatti di riceverle, scaricare i documenti notificati e pagare eventuali spese direttamente online su SEND o nell'app IO. SEND solleva gli enti da tutti gli adempimenti legati alla gestione delle comunicazioni a valore legale e riduce l'incertezza della reperibilità del destinatario.

SPID - L'identità digitale SPID è la soluzione che permette di accedere a tutti i servizi online della Pubblica Amministrazione con un'unica identità digitale. Attraverso credenziali classificate su tre livelli di sicurezza, abilita ad accedere ai servizi, ai quali fornisce dati identificativi certificati. SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia Digitale, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese.

A dicembre 2023 sono state rilasciate ai cittadini oltre 36 milioni e mezzo di identità digitali SPID, che hanno permesso nel 2023 di totalizzare oltre 1.000.000.000 di autenticazioni a servizi online di pubbliche amministrazioni e privati. Attualmente la federazione SPID è composta da più di 15.000 fornitori di servizi pubblici e 177 fornitori di servizi privati. Nell'ambito del PNRR il sub-investimento M1C1 1.4.4 «Rafforzamento dell'adozione delle piattaforme nazionali di identità digitale (SPID, CIE) e dell'Anagrafe nazionale della popolazione residente (ANPR)», di cui è soggetto titolare il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri, include fra le sue finalità che i gestori delle identità SPID assicurino l'innalzamento del livello dei servizi, della qualità, sicurezza e di interoperabilità degli stessi stabiliti dalle Linee guida AGID, come previsto dall'art. 18 bis del D.L. 24/02/2023 n. 13, convertito dalla L. 21/04/2023 n. 41.

A tal fine, è necessario che il Sistema SPID evolva in base alle seguenti indicazioni:

- attuazione delle «Linee guida OpenID Connect in SPID» (Determinazione del Direttore Generale di AGID n. 616/2021) comprensive dell'Avviso SPID n. 41 del 23/3/2023 versione 2.0 e il «Regolamento - SPID OpenID Connect Federation 1.0» (Determinazione del Direttore Generale di AGID n. 249/2022);
- attuazione delle «Linee guida operative per la fruizione dei servizi SPID da parte dei minori» (Determinazione del Direttore Generale di AGID n. 133/2022);
- attuazione delle «Linee guida recanti le regole tecniche dei Gestori di attributi qualificati» (Determinazione del Direttore Generale di AGID n. 215/2022);
- promozione dell'utilizzo dello SPID dedicato all'uso professionale per l'accesso ai servizi online rivolti a professionisti e imprese.

CIE - L'identità digitale CIE (CIEId), sviluppata e gestita dall'Istituto Poligrafico e Zecca dello Stato, consente la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, ai sensi del CAD, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale al momento del rilascio della CIE. La CIEId è comprovata dal

cittadino attraverso l'uso della CIE o delle credenziali rilasciate dal Ministero. Alla data di metà dicembre 2023 sono state rilasciate ai cittadini oltre 40 milioni di Carte di Identità Elettroniche, che hanno permesso nel 2023 di totalizzare circa 32.000.000 di autenticazioni a servizi online di pubbliche amministrazioni e privati. Attualmente la federazione CIE è composta da più di 10.000 fornitori di servizi pubblici e circa 100 fornitori di servizi privati. Come sancito dal Decreto 8 settembre 2022 «Modalità di impiego della carta di identità elettronica», sono previste le seguenti evolutive sul servizio CIEId:

- Ampliamento del set di attributi forniti tramite autenticazione con CIEId, come previsto dall'art. 6;
- ampliamento delle funzionalità del portale del cittadino, come previsto dall'art. 14, tra cui la possibilità di visualizzare, esprimere o revocare la volontà in merito alla donazione di organi e tessuti;
- implementazione dei servizi correlati al NIS (Numero Identificativo Servizi), come previsto dall'art. 17;
- implementazione di una piattaforma di firma elettronica qualificata remota attraverso l'utilizzo della CIE;
- implementazione dell'integrazione con il sistema ANPR, al fine di ricevere giornalmente i dati afferenti ai soggetti deceduti e procedere al blocco tempestivo della CIEId;
- sviluppo di un meccanismo di controllo genitoriale per consentire un accesso controllato ai servizi online offerti ai minori.

NoiPA - NoiPA è la piattaforma dedicata a tutto il personale della Pubblica Amministrazione, che offre servizi evoluti per la gestione, integrata e flessibile, di tutti i processi in ambito HR, inclusi i relativi adempimenti previsti dalla normativa vigente. Inoltre, attraverso il portale Open Data NoiPA, è possibile la piena fruizione dell'ampio patrimonio informativo gestito, permettendo la consultazione, in forma aggregata, dei dati derivanti dalla gestione del personale delle pubbliche amministrazioni servite.

Fascicolo Sanitario Elettronico - Il Fascicolo Sanitario Elettronico (FSE 2.0) ha l'obiettivo di garantire la diffusione e l'accessibilità dei servizi di sanità digitale in modo omogeneo e capillare su tutto il territorio nazionale a favore dei cittadini e degli operatori sanitari delle strutture pubbliche, private accreditate e private. La verifica formale e semantica della corretta implementazione e strutturazione dei documenti secondo gli standard ha lo scopo di assicurare omogeneità a livello nazionale per i servizi del FSE 2.0 disponibili ai cittadini e ai professionisti della Sanità. Attraverso interventi sistematici di formazione, si intende superare le criticità legate alle competenze digitali dei professionisti del sistema sanitario, innalzandone significativamente il livello per un utilizzo pieno ed efficace del FSE 2.0.

SUAP e SUE - Nel panorama della Pubblica Amministrazione, gli Sportelli Unici per le Attività Produttive (SUAP) e per l'Edilizia (SUE) assumono un ruolo centrale come punto di convergenza per imprese, professionisti e cittadini nell'interazione con le istituzioni,

nell'ambito degli adempimenti previsti per le attività produttive (quali, ad esempio, la produzione di beni e servizi, le attività agricole, commerciali e artigianali, le attività turistiche alberghiere ed extra-alberghiere, i servizi resi dalle banche e dagli intermediari finanziari e i servizi di telecomunicazione, ecc.) e gli interventi edilizi. Si tratta di due pilastri fondamentali in un contesto in continua evoluzione, dove la digitalizzazione si configura non solo come una necessità imprescindibile, ma anche come una leva strategica fondamentale per favorire la competitività delle imprese, stimolare la crescita economica del Paese e ottimizzare la tempestività nell'evasione delle richieste. In questo scenario, la semplificazione e l'accelerazione dei procedimenti amministrativi diventano così il mezzo con cui costruire un futuro in cui le opportunità digitali diventino accessibili a tutti. Nell'ambito delle iniziative previste dal Piano Nazionale di Ripresa e Resilienza (PNRR), è stato avviato il percorso di trasformazione incentrato sulla digitalizzazione e la semplificazione dei sistemi informatici, partendo dalla redazione delle Specifiche tecniche, elaborate attraverso il lavoro congiunto del Gruppo tecnico (istituito dal Ministero delle Imprese e del Made in Italy e dal Dipartimento della Funzione Pubblica e coordinato dall'Agenzia per l'Italia Digitale), le quali delineano l'insieme delle regole e delle modalità tecnologiche che i Sistemi Informatici degli Sportelli Unici (SSU) devono adottare, per la gestione ottimale dei procedimenti amministrativi riguardanti le attività produttive, conformemente alle disposizioni del DPR 160/2010 e ss.mm.ii. La fase operativa di questo percorso è stata condotta partendo da un'attenta analisi della situazione esistente, rafforzata, successivamente, dalla somministrazione di un questionario di valutazione, volto ad identificare la maturità tecnologica iniziale degli sportelli unici, grazie alla diretta collaborazione delle amministrazioni coinvolte.

Attualmente, è terminata la raccolta delle informazioni, perfezionata con altre attività di indagine, come la consulta dei fornitori dei servizi IT relativi alle piattaforme, i tavoli tematici regionali e il coinvolgimento di altri stakeholder e si sta procedendo con la definizione dei piani di intervento, da realizzarsi attraverso risorse finanziarie messe a disposizione dal Dipartimento della Funzione Pubblica, tramite la pubblicazione di bandi/stipula di accordi per l'adeguamento delle piattaforme. In tale percorso di trasformazione, che vedrà impegnate le pubbliche amministrazioni nel prossimo triennio, per garantire il raggiungimento delle milestone definite nell'ambito del PNRR, deve essere assicurato il supporto tecnico necessario all'adeguamento delle soluzioni informatiche alle Specifiche tecniche, attraverso la condivisione delle conoscenze e dell'esperienza maturata nel campo, utili a fornire una corretta interpretazione delle stesse durante la fase di realizzazione degli interventi.

SIOPE+ - L'art. 1, comma 533, della Legge n. 232 del 2016 (Legge di bilancio 2017), al fine di favorire il monitoraggio del ciclo completo delle entrate e delle spese, ha previsto l'obbligo per tutte le Amministrazioni pubbliche di:

- ordinare gli incassi e i pagamenti al proprio tesoriere o cassiere esclusivamente attraverso ordinativi informatici emessi secondo lo standard OPI emanato dall'Agenzia per l'Italia digitale (AGID),

- trasmettere gli ordinativi al proprio tesoriere/cassiere per il tramite dell'infrastruttura SIOPE+ gestita dalla Banca d'Italia.

L'attuazione del sistema SIOPE+ si è realizzata attraverso successivi decreti del Ministero dell'Economia e delle Finanze che, gradualmente, hanno esteso i nuovi adempimenti alle amministrazioni pubbliche e, in particolare, agli Enti Locali che hanno adottato SIOPE+ nel corso del 2018. Grazie al Decreto del Ministero dell'Economia e delle Finanze del 8 agosto 2019, con la quale si consentiva alle PA in contabilità finanziaria di poter aderire volontariamente al SIOPE+, fino al dicembre 2023 hanno aderito circa 650 istituzioni scolastiche statali. In tale ambito è stato definito il "Progetto di digitalizzazione completa dei pagamenti degli enti locali in SIOPE+ e la corretta alimentazione e allineamento della PCC". Il Progetto nasce dalla condivisione degli obiettivi, delle metodologie e degli strumenti definiti negli anni dai vari portatori di interesse del progetto SIOPE+ (MEF, AGID, Banca d'Italia, ABI, Poste, ANCI, IFEL e UPI). La gestione del progetto è caratterizzata dal metodo della condivisione, attraverso la costituzione di un comitato di coordinamento che svolge le funzioni di indirizzo, controllo e supporto alle attività del Progetto. L'iniziativa progettuale ha come finalità due obiettivi:

- ridurre, fino ad una progressiva eliminazione, l'utilizzo, da parte degli enti locali, di documenti esterni ai mandati informatici (cd. OPI) per il pagamento delle spese di personale;
- ridurre lo scostamento fra l'ammontare del debito commerciale degli enti locali rilevato dalla Piattaforma dei Crediti Commerciali e l'importo risultante dalle evidenze contabili delle amministrazioni locali.

Tale finalità comporterà la realizzazione delle procedure contabili e informatiche che consentono di pagare le spese di personale senza l'utilizzo di documenti esterni e di compilare correttamente gli OPI per l'alimentazione della PCC.

IT-Wallet - Il Sistema di Portafoglio digitale italiano (Sistema IT-Wallet) è l'ecosistema di soluzioni pubbliche e private che permettono a tutti i cittadini di disporre e gestire in maniera efficace della propria identità digitale e dei propri documenti e attestazioni, attraverso applicazioni mobile. Ha l'obiettivo di rendere più semplice, accessibile, sicuro e trasparente il processo di presentazione dei propri dati e l'accesso ai servizi erogati da pubbliche amministrazioni e soggetti privati, sia nel mondo fisico che in quello digitale, mettendo al centro il cittadino secondo i principi di self-sovereignty, once-only e data minimization.

Il Sistema IT-Wallet si colloca nel più ampio contesto europeo dell'European Digital Identity Framework, un insieme di regole contenute all'interno del Regolamento (UE) n. 2024/1183 (c.d. "eIDAS 2") che modifica il già in essere Reg. (UE) n. 910/2014 (c.d. "eIDAS"). Le citate regole puntano, soprattutto, a superare la frammentazione di identità digitali presenti negli Stati Membri, e richiedono che ogni Stato Membro notifichi alla Commissione entro il 2026 almeno un Wallet nazionale da qualificare quale "EUDI Wallet". Quest'ultimo dovrà anzitutto disporre delle funzionalità, dei livelli di sicurezza e certificazione minimi prescritte dal

regolamento. L'obiettivo di eIDAS 2 è quello di fornire ai cittadini europei strumenti interoperabili che consentano di accedere a vari tipi di servizi, anche a livello transfrontaliero.

Di seguito viene presentato anche il contesto normativo e strategico riferito al Sistema IT-Wallet, tuttavia i relativi risultati attesi e le relative linee di azione saranno definiti nella prossima edizione del Piano triennale.

Contesto normativo

In materia di Piattaforme esistono una serie di riferimenti, normativi o di indirizzo, cui le Amministrazioni devono attenersi. Di seguito si riporta un elenco delle principali fonti, generali o specifiche, della singola piattaforma citata nel capitolo.

PagoPA - Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 «Codice dell'amministrazione digitale» (CAD), art. 5
- Decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla Legge 17 dicembre 2012, n. 221 comma 5 bis, art. 15, «Ulteriori misure urgenti per la crescita del Paese»
- Decreto-legge 14 dicembre 2018, n. 135, convertito con modificazioni dalla Legge 11 febbraio 2019, n. 12 «Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la Pubblica Amministrazione», art 8, comma 2-3
- Decreto-legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 «Misure urgenti per la semplificazione e l'innovazione digitale», comma 2, art. 24, lettera a)
- Linee Guida AGID per l'Effettuazione dei Pagamenti Elettronici a favore delle Pubbliche Amministrazioni e dei Gestori di Pubblici Servizi (2018)

AppIO - Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 «Codice dell'amministrazione digitale» (CAD), art. 4-bis
- Decreto-legge 14 dicembre 2018, n. 135, convertito con modificazioni dalla Legge 11 febbraio 2019, n. 12 «Disposizioni urgenti in materia di sostegno e semplificazione per le imprese per la pubblica Amministrazione», art. 8
- Decreto-legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 «Misure urgenti per la semplificazione e l'innovazione digitale», art. 24, lett. F
- Decreto-legge 31 maggio 2021, n. 77 «Governance del Piano nazionale di rilancio e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure», art. 42

- Linee guida AGID per l'accesso telematico ai servizi della Pubblica Amministrazione (2021)

SEND - Riferimenti normativi italiani:

- Decreto-legge 14 dicembre 2018, n. 135, convertito con modificazioni dalla Legge 11 febbraio 2019, n. 12 «Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la Pubblica Amministrazione», art. 8
- Legge n. 160 del 2019 «Bilancio di previsione dello Stato per l'anno finanziario 2020 e bilancio pluriennale per il triennio 2020-2022» art. 1, commi 402 e 403
- Decreto-legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 «Misure urgenti per la semplificazione e l'innovazione digitale»
- Decreto-legge 31 maggio 2021, n. 77 «Governance del Piano nazionale di rilancio e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure», art. 38

SPID - Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 «Codice dell'amministrazione digitale» (CAD), art. 64
- Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014 recante la Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese
- Regolamento AGID recante le regole tecniche dello SPID (2014)
- Regolamento AGID recante le modalità attuative per la realizzazione dello SPID (2014)
- Linee Guida AGID per la realizzazione di un modello di R.A.O. pubblico (2019)
- Linee guida per il rilascio dell'identità digitale per uso professionale (2020)
- Linee guida AGID recanti Regole Tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD (2020)
- Linee Guida AGID «OpenID Connect in SPID»
- Linee guida AGID per la fruizione dei servizi SPID da parte dei minori (2022)
- Linee guida AGID recanti le regole tecniche dei gestori di attributi qualificati (2022)

CIE - Riferimenti normativi italiani:

- Legge 15 maggio 1997, n. 127- Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e di controllo
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
- Decreto-legge 31 gennaio 2005, n. 7 - Disposizioni urgenti per l'università e la ricerca, per i beni e le attività culturali, per il completamento di grandi opere strategiche, per

la mobilità dei pubblici dipendenti, (e per semplificare gli adempimenti relativi a imposte di bollo e tasse di concessione, nonché altre misure urgenti)

- Decreto Ministeriale del Ministro dell'Interno 23 dicembre 2015 - Modalità tecniche di emissione della Carta d'identità elettronica
- Decreto-legge 16 luglio 2020, n. 76, Misure urgenti per la semplificazione e l'innovazione digitale
- Decreto Ministeriale del Ministro dell'Interno 8 settembre 2022 - Modalità di impiego della carta di identità elettronica

CIE - Riferimenti normativi europei:

- Regolamento (UE) n. 1157 del 20 giugno 2019 sul rafforzamento della sicurezza delle carte d'identità dei cittadini dell'Unione e dei titoli di soggiorno rilasciati ai cittadini dell'Unione e ai loro familiari che esercitano il diritto di libera circolazione

NoiPA - Riferimenti normativi italiani:

- Legge 27 dicembre 2006, n. 296 «Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato» (legge finanziaria 2007) art. 1 commi 446 e 447
- Legge 23 dicembre 2009, n. 191 «Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato» (legge finanziaria 2010) art. 2, comma 197
- Decreto-legge 6 luglio 2011, n. 98, convertito con modificazioni dalla L. 15 luglio 2011, n. 11 «Disposizioni urgenti per la stabilizzazione finanziaria»
- Legge 19 giugno 2019, n. 56 «Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo»
- Decreto del Ministro dell'Economia e delle Finanze 31 ottobre 2002 «Modifiche delle norme sull'articolazione organizzativa del Dipartimento per le politiche di sviluppo e di coesione del Ministero dell'Economia e delle Finanze»
- Decreto del Ministro dell'Economia e delle Finanze 6 luglio 2012 «Contenuti e modalità di attivazione dei servizi in materia stipendiale erogati dal Ministero dell'Economia e delle Finanze»

FSE - Riferimenti normativi italiani:

- Decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla Legge 17 dicembre 2012, n. 221 «Ulteriori misure urgenti per la crescita del Paese»
- Decreto del Presidente del Consiglio dei Ministri 29 settembre 2015, n. 178 «Regolamento in materia di fascicolo sanitario elettronico»
- Legge 11 dicembre 2016, n. 232 «Bilancio di previsione dello Stato per l'anno finanziario 2017 e bilancio pluriennale per il triennio 2017-2019»
- Decreto-legge 19 maggio 2020, n. 34, convertito con modificazioni dalla Legge 17 luglio 2020, n. 77 «Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19»

- Decreto-legge 28 ottobre 2020, n. 137, convertito con modificazioni dalla Legge 18 dicembre 2020, n. 176 «Ulteriori misure urgenti in materia di tutela della salute, sostegno ai lavoratori e alle imprese, giustizia e sicurezza, connesse all'emergenza epidemiologica da COVID-19»
- Decreto-legge 27 gennaio 2022, n. 4, convertito con modificazioni dalla Legge 28 marzo 2022, n. 25 «Misure urgenti in materia di sostegno alle imprese e agli operatori economici, di lavoro, salute e servizi territoriali, connesse all'emergenza da COVID-19, nonché per il contenimento degli effetti degli aumenti dei prezzi nel settore elettrico»
- Decreto del Ministero dell'Economia e delle Finanze 23 dicembre 2019 «Utilizzo del Fondo per il finanziamento degli investimenti e lo sviluppo infrastrutturale - Fascicolo sanitario elettronico» (Piano di digitalizzazione dei dati e documenti sanitari)
- Decreto del Ministero della Salute 20 maggio 2022 «Adozione delle Linee guida per l'attuazione del Fascicolo sanitario elettronico» pubblicato sulla GU Serie Generale n. 160 11.07.2022
- Decreto del Ministero della Salute 7 settembre 2023 «Fascicolo sanitario elettronico 2.0» Linee Guida per l'attuazione del Fascicolo Sanitario Elettronico (2022) Piano Nazionale di Ripresa e Resilienza:
 - M6 - Salute C2 1.3.1 «Rafforzamento dell'infrastruttura tecnologica e degli strumenti per la raccolta, l'elaborazione, l'analisi dei dati e la simulazione (FSE)»

SIOPE+ - Riferimenti normativi italiani:

- Legge 11 dicembre 2016, n. 232 Bilancio di previsione dello Stato per l'anno finanziario 2017 e bilancio pluriennale per il triennio 2017-2019
- Legge 30 dicembre 2020, n. 178 Bilancio di previsione dello Stato per l'anno finanziario 2021 e bilancio pluriennale per il triennio 2021-2023
- Legge 31 dicembre 2009, n. 196 Legge di contabilità e finanza pubblica
- Delibera numero 114, del 23 Dicembre 2015 Programma complementare di azione e coesione per la governance dei sistemi di gestione e controllo 2014-2020
- Delibera numero 114, del 23 Dicembre 2015 Programma complementare di azione e coesione per la governance dei sistemi di gestione e controllo 2014-2020
- Legge 27 dicembre 2013, n. 147 Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (Legge di stabilità 2014)
- Decreto del Ministro dell'economia e delle finanze del 8 agosto 2019, concernente la codifica gestionale delle Autorità amministrative indipendenti, con decorrenza 1° gennaio 2020, inserite nell'elenco delle amministrazioni pubbliche di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n.196 e successive modificazioni, escluse la Commissione di garanzia dell'attuazione della legge sullo sciopero nei servizi pubblici essenziali (CGSSE) e l'Agenzia nazionale di valutazione del sistema universitario e della ricerca (ANVUR).

- Decreto del Ministro dell'economia e delle finanze del 23 luglio 2019, concernente la codifica gestionale delle Fondazioni lirico-sinfoniche, con decorrenza 1° gennaio 2020, di cui al decreto legislativo 29 giugno 1996, n. 367, e successive modificazioni, e di cui alla legge 11 novembre 2003, n. 310.
- Decreto del Ministro dell'economia e delle finanze del 30 maggio 2018 concernente l'estensione di SIOPE + agli enti soggetti alla rilevazione SIOPE
- Decreto Mef 29 maggio 2018 concernente la codifica gestionale delle Autorità di sistema portuali
- Decreto MEF del 26 febbraio 2018 concernente l'anticipo dell'avvio a regime di SIOPE+ per singoli enti
- Decreto MEF del 14 giugno 2017

IT-Wallet - Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (CAD), art. 64- quater, come introdotto dal decreto-legge 2 marzo 2024, n. 19, convertito con modificazioni dalla Legge 29 aprile 2024, n. 56, art. 20, comma 1, lettera e), "Ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR)"

IT-Wallet - Riferimenti normativi europei:

- Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale

Obiettivo 4.1 – Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA

Risultati attesi:

- RA4.1.1 - Incremento dei servizi sulla piattaforma pagoPA
- RA4.1.2 - Incremento dei servizi sulla Piattaforma IO (l'App dei servizi pubblici)
- RA4.1.3 - Incremento degli enti che usano SEND
- RA4.1.4 - Incremento dell'adozione e dell'utilizzo di SPID e CIE da parte delle Pubbliche Amministrazioni
- RA4.1.5 - Promuovere l'adesione ai servizi della piattaforma NoiPA per supportare l'azione amministrativa nella gestione del personale
- RA4.1.6 - Incremento del livello di alimentazione e digitalizzazione del Fascicolo Sanitario Elettronico
- RA4.1.7 - Semplificazione e creazione di un catalogo di tutte le procedure SUAP e SUE e relativi regimi amministrativi applicati su tutto il territorio nazionale
- RA4.1.8 - Miglioramento del processo di digitalizzazione del sistema pubblico dei pagamenti avviato nel 2017 con la realizzazione di SIOPE+

- RA4.1.9 - Incremento delle Pubbliche amministrazioni che rendono disponibili attestazioni elettroniche nel Sistema IT-Wallet

CAP4.PA.01

Le PA aderenti a pagoPA assicurano l'attivazione di nuovi servizi in linea con i target sopra descritti e secondo le modalità attuative definite nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR).

Azioni previste/eseguite: il Comune di San Sperate ha partecipato all'avviso PNRR 1.4.3 – PagoPA, attivato il connettore con i propri gestionali interni. Attualmente viene utilizzata come una delle modalità principali per ricevere i pagamenti. Nell'anno 2026 è stato aggiunto un servizio di pagamento.

CAP4.PA.02

Le PA aderenti a App IO assicurano l'attivazione di nuovi servizi in linea con i target sopra descritti e secondo le modalità attuative definite nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR).

Azioni previste/eseguite: il Comune di San Sperate ha partecipato all'avviso PNRR 1.4.3 – APP IO, attivato il connettore con i propri gestionali interni. Sono stati attivati nr. 10 servizi ad oggi attivi.

CAP4.PA.03

Le PA centrali e i Comuni, in linea con i target sopra descritti e secondo la roadmap di attuazione prevista dal Piano Nazionale di Ripresa e Resilienza (PNRR), si integreranno a SEND.

Azioni previste/eseguite: il Comune di San Sperate ha eseguito l'integrazione a SEND.

CAP4.PA.04

Le PA e i gestori di pubblici servizi proseguono il percorso di adesione a SPID e CIE, dismettendo le altre modalità di autenticazione associate ai propri servizi online e integrando lo SPID uso professionale per i servizi diretti a professionisti e imprese

Azioni previste/eseguite: il Comune di San Sperate ha concluso il percorso di adesione a SPID e CIE, dismettendo le altre modalità di autenticazione associate ai propri servizi online al cittadino.

CAP4.PA.05

Le PA e i gestori di pubblici servizi interessati cessano il rilascio di credenziali proprietarie a cittadini dotabili di SPID e/o CIE.

Azioni previste/eseguite: il Comune di San Sperate ha cessato il rilascio di credenziali proprietarie a cittadini dotabili di SPID e/o CIE. Solo le forze dell'ordine, per consultazioni anagrafiche, utilizzando user/password rilasciate dal servizio informatico.

CAP4.PA.06

Le PA e i gestori di pubblici servizi interessati adottano lo SPID e la CIE by default: le nuove applicazioni devono nascere SPID e CIE-only a meno che non ci siano vincoli normativi o tecnologici, se dedicate a soggetti dotabili di SPID o CIE. Le PA che intendono adottare lo SPID di livello 2 e 3 devono anche adottare il «Login with eIDAS» per l'accesso transfrontaliero ai propri servizi.

Azioni previste/eseguite: il Comune di San Sperate ha adottato SPID e CIE by default.

CAP4.PA.07

Le PA devono adeguarsi alle evoluzioni previste dall'ecosistema SPID (tra cui OpenID Connect, uso professionale, Attribute Authorities, servizi per i minori e gestione degli attributi qualificati).

Azioni previste/eseguite: il Comune di San Sperate è in fase di adeguamento per la linea d'azione indicata.

CAP4.PA.08

Le PA che intendono aderire a NoiPA esprimono manifestazione di interesse e inviano richiesta.

Azioni previste/eseguite: il Comune di San Sperate non ha aderito a NoiPA e non ha attualmente intenzione di aderire.

CAP4.PA.09

Le Regioni e le Province Autonome rispettano le scadenze delle attività previste nel proprio Piano di adeguamento tecnologico, in coerenza con i decreti attuativi che definiscono i contenuti del FSE e la standardizzazione da parte di HL7Italia.

Azioni previste/eseguite: il Comune di San Sperate non rientra nelle Pubbliche Amministrazioni menzionate nella linea d'azione.

CAP4.PA.10

Le Regioni e le Province Autonome rispettano le scadenze delle attività previste nel proprio Piano di adeguamento tecnologico, in coerenza con i decreti attuativi che definiscono i contenuti del FSE e la standardizzazione da parte di HL7Italia.

Azioni previste/eseguite: il Comune di San Sperate non rientra nelle Pubbliche Amministrazioni menzionate nella linea d'azione.

CAP4.PA.11

UnionCamere realizza il Catalogo Unico dei procedimenti del SUAP e gli Enti interessati (PAC/PALComuni, Regioni, Enti Terzi, Unioncamere) avviano la prima alimentazione del Catalogo.

Azioni previste/eseguite: il Comune di San Sperate utilizza il SUAP-E Sardegna, in linea con le richieste indicate.

CAP4.PA.12

Identificazione della migliore soluzione da adottare dalle PA interessate nei procedimenti SUAP/SUE, in funzione del loro contesto, sulla base delle possibili soluzioni messe a disposizione dalle specifiche tecniche - (PAC/PAL-Comuni, Regioni, Enti Terzi).

Azioni previste/eseguite: il Comune di San Sperate utilizza il SUAP-E Sardegna, in linea con le richieste indicate.

CAP4.PA.13

PAC/PAL-Comuni, Regioni, Enti Terzi e Unioncamere devono adeguare le proprie componenti informatiche interessate nei procedimenti SUAP alle specifiche tecniche di cui al Decreto interministeriale 26/09/2023

Azioni previste/eseguite: il Comune di San Sperate utilizza il SUAP-E Sardegna, in linea con le richieste indicate.

CAP4.PA.14

Messa a disposizione di soluzioni alternative all'adeguamento alle specifiche tecniche dei propri sistemi informatici SSU, in ambito SUAP/SUE, quali, ad esempio: Impresa in un giorno per i comuni e Soluzione Sussidiaria per gli enti terzi - (Regioni, Consorzi, Unioncamere).

Azioni previste/eseguite: il Comune di San Sperate utilizza il SUAP-E Sardegna, in linea con le richieste indicate.

CAP4.PA.15

Gli Enti interessati (PAC/PAL-Comuni, Regioni, Enti Terzi, Unioncamere) aggiornano il Catalogo Unico dei procedimenti del SUAP

Azioni previste/eseguite: il Comune di San Sperate utilizza il SUAP-E Sardegna, in linea con le richieste indicate.

CAP4.PA.16

Aggiornamento costante del Catalogo Unico dei procedimenti del SUAP - (PAC/PAL-Comuni, Regioni, Enti Terzi, Unioncamere).

Azioni previste/eseguite: il Comune di San Sperate utilizza il SUAP-E Sardegna, in linea con le richieste indicate.

CAP4.PA.17 / CAP4.PA.18/ CAP4.PA.19/

Enti Locali selezionati tramite avviso di progetto sperimentano il modello operativo relativo al "progetto di digitalizzazione completa dei pagamenti degli enti locali in SIOPE+ e la corretta alimentazione e allineamento della PCC"

Azioni previste/eseguite: il Comune di San Sperate non è coinvolto da questa linea d'azione specifica

Piattaforme che attestano attributi

Scenario

Negli ultimi anni le iniziative intraprese dai vari attori coinvolti nell'ambito del Piano hanno favorito una importante accelerazione nella diffusione di alcune delle principali piattaforme abilitanti, in termini di adozione da parte delle PA e di fruizione da parte degli utenti. Il Piano descrive lo sviluppo di nuove piattaforme e il consolidamento di quelle già in essere, attraverso l'aggiunta di nuove funzionalità. Tali piattaforme rendono disponibili i dati di settore a cittadini e PA, consentono di razionalizzare i servizi per le amministrazioni e di semplificare, tramite l'utilizzo delle tecnologie digitali, l'interazione tra cittadini e PA (vedi Piattaforma Digitale Nazionale Dati – PDND). Ad esempio, dal luglio 2023 la Piattaforma INAD è andata in esercizio sia tramite il sito web sia tramite le API esposte su PDND. La piattaforma è quindi a disposizione delle pubbliche amministrazioni per entrambe le modalità di fruizione. Si invitano pertanto le PA a fruire dei relativi servizi, compatibilmente con il loro dimensionamento.

Le seguenti Piattaforme hanno la caratteristica di attestare attributi anagrafici e di settore.

ANPR: è l'Anagrafe Nazionale che raccoglie tutti i dati anagrafici dei cittadini residenti in Italia e dei cittadini italiani residenti all'estero, aggiornata con continuità dai comuni italiani. Consente di avere un set di dati anagrafici dei cittadini certo, accessibile, affidabile e sicuro su cui sviluppare servizi integrati ed evoluti per semplificare e velocizzare le procedure tra pubbliche amministrazioni e con i cittadini. Sul portale ANPR, nell'area riservata del cittadino, sono attualmente disponibili i servizi che consentono di:

- visualizzare i propri dati anagrafici;
- effettuare una richiesta di rettifica per errori materiali;
- richiedere autocertificazioni precompilate con i dati anagrafici presenti in ANPR;
- richiedere un certificato anagrafico in bollo o in esenzione (sono disponibili 15 tipologie differenti di certificati);
- comunicare un cambio di residenza;
- visualizzare il proprio domicilio digitale, costantemente allineato con l'Indice Nazionale dei Domicili Digitali (INAD);
- comunicare un punto di contatto (mail o telefono).

A dicembre 2022 sono stati resi disponibili i servizi per consentire, da parte dei Comuni, l'invio e il continuo aggiornamento dei dati elettorali dei cittadini in ANPR e a settembre 2024 è stata completata l'adesione ai servizi da parte dei comuni italiani, che hanno inviato i dati elettorali dei cittadini. La presenza dei dati elettorali in ANPR ha consentito di mettere a disposizione dei cittadini, nell'area riservata del portale, i seguenti servizi:

- visualizzazione dei dati relativi alla propria posizione elettorale e al seggio di esercizio del voto;

- servizio di richiesta e rilascio dei certificati di godimento dei diritti politici e di iscrizione nelle liste elettorali;
- servizio di richiesta di iscrizione nelle liste elettorali comunali da parte dei cittadini comunitari residenti in Italia.

La presenza dei dati elettorali in ANPR, inoltre, ha consentito il rilascio di servizi su PDND che consentono di verificare in tempo reale la posizione elettorale di un cittadino da parte di altre Amministrazioni che ne abbiano necessità per fini istituzionali. Una prima applicazione si è avuta con l'integrazione di questi servizi con la Piattaforma Referendum, piattaforma online attivata a luglio 2024 per consentire la sottoscrizione di proposte referendarie e di iniziativa popolare, verificando in tempo reale la posizione elettorale del cittadino sottoscrittore. Al fine di agevolare lo sviluppo di sistemi integrati ed evoluti, che semplifichino e velocizzino le procedure tra le Pubbliche Amministrazioni, ANPR ha rilasciato 28 e-service sulla Piattaforma Nazionale Digitale Dati (PDND - Interoperabilità), consentendo la consultazione dei dati ANPR da parte di altri Enti aventi diritto, nel rispetto dei principi del Regolamento Privacy.

Un ulteriore significativo strumento di semplificazione per i Comuni e per i cittadini sarà costituito dall'integrazione di ANPR con i servizi dello Stato civile digitale. Si prevede, infatti, la completa digitalizzazione dei registri dello Stato civile tenuti dai Comuni (nascita, matrimonio, unione civile, cittadinanza e morte), con conseguente eliminazione dei registri cartacei, e la conservazione dei relativi atti digitali in un unico archivio nazionale del Ministero dell'Interno, permettendone la consultazione a livello nazionale e offrendo la possibilità di produrre estratti o certificati tramite il sistema centrale, senza doverli richiedere necessariamente al Comune che li ha generati. A partire da ottobre 2023 alcuni Comuni pilota hanno iniziato ad utilizzare i servizi resi disponibili da ANPR per lo stato civile e, ad oggi, 14 comuni utilizzano i servizi, formando atti digitali di stato civile con effetti giuridici conservati nella piattaforma centrale.

ANPR si sta integrando con le anagrafi settoriali del lavoro, della pensione e del welfare e ogni nuova anagrafe che abbia come riferimento la popolazione residente sarà logicamente integrata con ANPR. Tra le piattaforme che attestano attributi, per rafforzare gli interventi nei settori di istruzione, università e ricerca, accelerare il processo di automazione amministrativa e migliorare i servizi per i cittadini e le pubbliche amministrazioni, sono istituite due Anagrafi:

- **ANIST:** Anagrafe nazionale dell'istruzione, a cura del Ministero dell'Istruzione e del Merito
- **ANIS:** Anagrafe nazionale dell'istruzione superiore, a cura del Ministero dell'Università e della Ricerca.

Le due Anagrafi mirano ad assicurare:

- la centralizzazione dei dati attualmente distribuiti su tutto il territorio italiano in oltre 10.000 scuole (ANIST) e 500 istituti di formazione superiore (ANIS);
- la disponibilità e l'accesso ai dati per:

- scuole e istituti di formazione superiore (IFS), al fine di facilitare il reperimento delle informazioni relative al percorso scolastico e/o accademico dei propri studenti, efficientando le procedure di iscrizione;
- cittadini, al fine rendere possibile, attraverso il Portale dedicato, la consultazione online dei dati relativi al proprio percorso scolastico e/o accademico, anche a fini certificativi;
- PA per fini istituzionali;
- soggetti privati autorizzati, per gli scopi previsti dalla legge.
- l'interoperabilità con altre banche dati (es. con ANPR per la gestione dei dati anagrafici degli studenti, eliminando duplicazioni e rischi di disallineamento);
- il riconoscimento nell'UE ed extra-EU dei titoli di studio.

L'iter normativo di ANIS è stato concluso il 18 gennaio 2023 e a settembre dello stesso anno è stato rilasciato il portale nazionale ANIS (<https://anis.mur.gov.it/>) con l'attivazione dei seguenti servizi online verso i cittadini:

- consultazione dei propri titoli di studio;
- possibilità di presentare una richiesta di rettifica degli stessi, ove necessario;
- possibilità di ottenere attestazioni dei propri titoli di studio, firmate digitalmente dal MUR, da utilizzare nei rapporti con soggetti privati.

Sono stati rilasciati, inoltre, i servizi sulla PDND, per consentire la verifica e il recupero dei dati relativi ai titoli di studio e alle iscrizioni da parte degli Enti aventi diritto. Il Regolamento sulle modalità di attuazione e funzionamento dell'Anagrafe nazionale dell'istruzione (ANIST) è entrato in vigore il 23 marzo 2024 e si prevede l'attivazione del portale entro il 2024, consentendo ai cittadini di consultare online i dati relativi alle frequenze e ai titoli di studio, richiedere una eventuale rettifica degli stessi, nonché ottenere il rilascio di certificazioni spendibili nei rapporti con i privati.

Contesto normativo

INAD - Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (CAD), art. 3- bis e 6-quater
- Decreto-legge 6 novembre 2021, n. 152, convertito con modificazioni dalla Legge 29 dicembre 2021, n. 233 "Disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per la prevenzione delle infiltrazioni mafiose"
- Linee Guida AGID sull'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese (2023)

ANPR - Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 “Codice dell'amministrazione digitale” (CAD), art. 62
- Decreto del Presidente del Consiglio dei Ministri 10 novembre 2014, n. 194, Regolamento recante modalità di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (ANPR) e di definizione del piano per il graduale subentro dell'ANPR alle anagrafi della popolazione residente
- Decreto del Presidente del Consiglio dei Ministri, 23 agosto 2013, n. 109, Regolamento recante disposizioni per la prima attuazione dell'articolo 62 del decreto legislativo 7 marzo 2005, n. 82
- Decreto del Ministero dell'interno del 3 novembre 2021 Modalità di erogazione da parte dell'Anagrafe nazionale della popolazione residente dei servizi telematici per il rilascio di certificazioni anagrafiche on-line e per la presentazione on-line delle dichiarazioni anagrafiche.
- Decreto del Ministero dell'Interno del 17 ottobre 2022, Modalità di integrazione nell'ANPR delle liste elettorali e dei dati relativi all'iscrizione nelle liste di sezione di cui al decreto del Presidente della Repubblica 20 marzo 1967, n. 223
- Decreto del Ministero dell'interno del 18 ottobre 2022, Aggiornamento della piattaforma di funzionamento dell'Anagrafe nazionale della popolazione residente per l'erogazione dei servizi resi disponibili ai comuni per l'utilizzo dell'Archivio nazionale informatizzato dei registri dello stato civile
- Decreto del Ministero dell'interno del 3 marzo 2023 - Modalità di attribuzione, da parte dell'Anagrafe nazionale della popolazione residente

ANIS - Riferimenti normativi italiani:

- Decreto-legge 9 maggio 2003, n. 105 “Disposizioni urgenti per le università e gli enti di ricerca nonché in materia di abilitazione all'esercizio delle attività professionali”, art. 1-bis
- Decreto legislativo 7 marzo 2005, n. 82 “Codice dell'amministrazione digitale” (CAD), art. 62- quinquies
- Decreto-legge del 6 novembre 2021, n. 152 "Disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per la prevenzione delle infiltrazioni mafiose", art. 31-ter
- Decreto del Ministero dell'Università e Ricerca del 19 gennaio 2022 "Prima attuazione delle disposizioni istitutive dell'Anagrafe nazionale dell'istruzione superiore (ANIS)"
- Decreto del Ministero dell'Università e della Ricerca del 30 settembre 2022 "Seconda attuazione delle disposizioni istitutive dell'Anagrafe nazionale dell'istruzione superiore (ANIS)"

ANIST - Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 “Codice dell'amministrazione digitale” (CAD), art. 62- quater

- Decreto del Ministero dell'Istruzione e del Merito del 7 dicembre 2023, n. 234, "Regolamento sulle modalità di attuazione e funzionamento dell'Anagrafe nazionale dell'istruzione"

Obiettivo 4.2 – Ottenere la piena interoperabilità tra le piattaforme

Risultati attesi:

- RA4.2.1 - Adesione ai nuovi servizi offerti da ANPR
- RA4.2.2 - Disponibilità dei dati su iscrizioni e titoli di studio su ANIS
- RA4.2.3 - Realizzazione della piattaforma ANIST

CAP4.PA.20

Dalla «fine dell'adozione controllata» i Comuni potranno richiedere l'adesione servizi di Stato civile su ANPR.

Azioni previste/eseguite: il Comune di San Sperate ha aderito all'avviso all'Avviso Misura 1.4.4 - Estensione dell'utilizzo dell'anagrafe nazionale digitale (ANPR) - Adesione allo Stato Civile digitale (ANSC) - Comuni (luglio 2024)

CAP4.PA.21

Le Università e gli AFAM statali possono trasmettere i propri dati per l'integrazione su ANIS attraverso servizi resi fruibili dalla PDND secondo quanto descritto nell'area tecnica del sito <https://www.anis.mur.gov.it/area-tecnica/documentazione>.

Azioni previste/eseguite: il Comune di San Sperate non rientra nella casistica di Pubbliche Amministrazioni indicate in questa linea d'azione.

CAP4.PA.22

Le Università possono trasmettere i propri dati per l'integrazione su ANIS attraverso l'uso di una web application.

Azioni previste/eseguite: il Comune di San Sperate non rientra nella casistica di Pubbliche Amministrazioni indicate in questa linea d'azione.

CAP4.PA.23

Le istituzioni scolastiche possono prendere visione delle informazioni di interesse nell'area tecnica del portale messo a disposizione.

Azioni previste/eseguite: il Comune di San Sperate non rientra nella casistica di Pubbliche Amministrazioni indicate in questa linea d'azione.

CAP4.PA.24

Le istituzioni scolastiche accedono alle funzionalità della piattaforma

Azioni previste/eseguite: il Comune di San Sperate non rientra nella casistica di Pubbliche Amministrazioni indicate in questa linea d'azione.

Basi dati interesse nazionale

Scenario

I dati resi disponibili attraverso le piattaforme sono principalmente quelli relativi alle basi dati di interesse nazionale definite dall'art. 60 del CAD e riportate nell'elenco disponibile sul sito AGID. Il citato art. 60 del CAD prevede caratteristiche minime di sicurezza, accessibilità e interoperabilità ed il rispetto delle Linee guida per l'attuazione del CAD e delle vigenti regole del Sistema statistico nazionale. A tale proposito, si richiama la Determinazione AGID N. 68/2013 DIG che, in attuazione dell'art. 2-bis del decreto-legge n. 179/2012, nel testo introdotto dalla legge di conversione 17 dicembre 2012, n. 221, ha definito le regole tecniche per l'identificazione delle basi di dati critiche tra quelle di interesse nazionale e per definirne le modalità di aggiornamento atte a garantire la qualità dei dati presenti. In modo da verificare costantemente il livello di aderenza a tali prescrizioni, saranno definiti i processi di individuazione di ulteriori basi dati di interesse nazionale e di monitoraggio delle stesse. Tali processi coinvolgeranno le amministrazioni titolari delle basi dati le quali dovranno adottare tutte le misure atte a garantire il rispetto dei requisiti e dovranno fornirne evidenza per consentirne l'adeguato monitoraggio. In questo ambito sono coinvolte anche tutte le altre amministrazioni che potranno proporre l'individuazione di nuove basi dati di interesse nazionale.

Contesto normativo

Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 «Codice dell'amministrazione digitale» (in breve CAD) art. 60

Obiettivo 4.3 – Migliorare la sicurezza, accessibilità e l'interoperabilità delle basi dati di interesse nazionale

Risultati attesi:

- RA4.3.1 - Incremento del numero di basi dati di interesse nazionale conformi alle regole tecniche

CAP4.PA.25

Le PA interessate avanzano la richiesta di inserimento delle proprie basi di dati nell'elenco di Basi di dati di interesse nazionale gestito da AGID secondo il processo definito.

Azioni previste/eseguite: il Comune di San Sperate non possiede basi dati di interesse nazionale.

CAP4.PA.26

La PA titolari di basi di dati di interesse nazionale le adeguano all'aggiornamento delle regole tecniche.

Azioni previste/eseguite: il Comune di San Sperate non possiede basi dati di interesse nazionale.

Capitolo 5 – Dati e Intelligenza Artificiale

Open data e data governance

Scenario

La valorizzazione del patrimonio informativo pubblico è un obiettivo strategico per la Pubblica Amministrazione per affrontare efficacemente le nuove sfide dell'economia basata sui dati (data economy), supportare gli obiettivi definiti dalla Strategia europea in materia di dati, garantire la creazione di servizi digitali a valore aggiunto per cittadini, imprese e, in generale, per tutti i portatori di interesse e fornire ai vertici decisionali strumenti data-driven da utilizzare nei processi organizzativi e/o produttivi. L'ingente quantità di dati prodotti dalla Pubblica Amministrazione, se caratterizzati da un'alta qualità, potrà costituire, inoltre, la base per una grande varietà di applicazioni come, per esempio, quelle riferite all'intelligenza artificiale. La costruzione di un'economia dei dati è l'obiettivo che l'Unione Europea intende perseguire attraverso una serie di iniziative di regolazione avviate ormai dal 2020. La citata Strategia europea dei dati ha introdotto la creazione di spazi di dati (data spaces) comuni e interoperabili al fine di superare le barriere legali e tecniche alla condivisione dei dati e, di conseguenza, sfruttare l'enorme potenziale dell'innovazione guidata dai dati. Con l'adozione dell'atto sulla governance dei dati (Data Governance Act), inoltre, sono stati definiti e rafforzati i meccanismi per aumentare la disponibilità dei dati e superare gli ostacoli tecnici al riutilizzo di alcune particolari tipologie di dati altrimenti non disponibili. In Italia, con il recepimento della Direttiva Europea (UE) 2019/1024 (cosiddetta Direttiva Open data) sull'apertura dei dati e il riutilizzo dell'informazione del settore pubblico, attuato con il Decreto lgs. n. 200/2021, che ha modificato il Decreto lgs. n. 36/2006, l'obiettivo strategico sopra delineato può essere perseguito attraverso l'implementazione delle nuove regole tecniche definite con le Linee guida sui dati aperti. Tale documento, adottato con la Determinazione AGID n. 183/2023 ai sensi dell'art. 71 del CAD in applicazione dell'art. 12 del citato Decreto Lgs. N. 36/2006 e s.m.i., è finalizzato a supportare le pubbliche amministrazioni e gli altri soggetti interessati nel processo di apertura dei dati e, quindi, favorire l'aumento dell'offerta di dati pubblici preziosi a fini di riutilizzo. Tra questi tipi di dati rientrano anche quelli di elevato valore, identificati con il Regolamento di esecuzione (UE) 2023/138 sulla base delle sei categorie tematiche (dati geospaziali, dati relativi all'osservazione della Terra e all'ambiente, dati meteorologici, dati statistici, dati relativi alle imprese e alla proprietà delle imprese, dati relativi alla mobilità) stabilite con la Direttiva Open Data. Con riferimento a tale Regolamento, il 22 dicembre 2023 è stata adottata da AGID una specifica Guida operativa sulle serie di dati di elevato valore come documento di orientamento per le pubbliche amministrazioni per una più efficace implementazione delle disposizioni europee. Per garantire la creazione di servizi digitali sempre più efficienti, i dati scambiati reciprocamente tra gli enti erogatori di servizi dovranno essere pienamente interoperabili, non solo da un punto di vista tecnico ma anche semantico. In altre parole, nello sviluppo di un servizio digitale, oltre a utilizzare applicazioni informatiche interoperabili, per la ricezione o l'invio dei

dati, si dovrà garantire l'effettiva comprensione del significato e del formato delle informazioni scambiate, usufruendo di riferimenti nazionali come ad esempio le ontologie, i vocabolari controllati e gli schemi di dati presenti sul Catalogo Nazionale per l'Interoperabilità semantica dei dati (National Data Catalog – NDC).

Al fine di valutare l'impatto del processo di apertura dei dati e la conseguente ricaduta economica e sociale, dovranno essere attivate azioni mirate al monitoraggio del riutilizzo dei dati resi disponibili dalle pubbliche amministrazioni. Per poter abilitare attività di sviluppo di applicazioni innovative, inoltre, dovrà essere garantito un adeguato livello di qualità dei dati con la disponibilità di un sistema di misurazione e di assessment basato sui pertinenti standard ISO. Tali standard ISO, relativi sia alle caratteristiche della qualità che alla loro misurazione, sono indicati come riferimento utile nelle Linee Guida Open Data, che forniscono raccomandazioni ed esempi su come garantire un livello minimo della stessa qualità. Le medesime Linee Guida richiamano, per i dati della ricerca in particolare ma con raccomandazione di applicarli per tutte le tipologie di dati, i requisiti di reperibilità, accessibilità, interoperabilità e riutilizzabilità che rappresentano i 4 principi del framework FAIR (Findable - Accessible - Interoperable - Reusable). Al fine di supportare le PA a implementare le indicazioni delle Linee Guida e, quindi, in generale, garantire il livello di qualità richiesto, anche alla luce dell'utilizzo dei dati nei sistemi di IA (trattati in seguito), è necessario fornire opportuni strumenti per la misura delle caratteristiche di qualità così come definite negli Standard indicati. In questo ambito, ci sono esperienze di sviluppo e di sperimentazione in corso, come il tool euFAIR dell'Università del Salento, che possono costituire il punto di partenza per l'implementazione di un sistema nazionale di misura della qualità dei dati. In tale contesto, Istat provvede alla predisposizione delle nomenclature e metodologie di base per la classificazione e la rilevazione dei fenomeni di carattere demografico, economico e sociale (art. 15, lett. e), d. lgs. n. 322/1989), nonché alla definizione dei metodi e dei formati da utilizzare da parte delle pubbliche amministrazioni per lo scambio e l'utilizzo in via telematica dell'informazione statistica e finanziaria (art. 2, d.P.R. n. 166/2010). In virtù di questo suo ruolo Istat può fornire supporto per assicurare una governance della semantica relativamente alle nomenclature e alle metodologie classificatorie, diffondendo una cultura del dato che sensibilizzi la PA all'utilizzo del Catalogo Nazionale Dati (NDC).

Al fine di sviluppare servizi digitali che ottimizzino l'impatto su cittadini, PA e imprese è inoltre opportuno adottare un approccio use case driven per aiutare le PA ad individuare una scala di priorità per la documentazione e la condivisione dei dati e degli asset semantici sulle piattaforme nazionali (portali nazionali dei dati - dati.gov.it e geodati.gov.it, PDND e NDC), fermo restando quanto indicato nelle Linee guida Open Data, in termini di criteri di priorità per il riutilizzo, relativamente ai dati aperti. L'uso di una semantica comune nello scambio dei dati è garanzia di "coerenza semantica" dei dati stessi. Inoltre, l'adozione di una semantica unica riferita ai dati di dettaglio, come rappresentati nel NDC, consente uno scambio di informazioni coerenti e rappresenta una garanzia di consistenza dei dati aggregati che ogni

organizzazione pubblica come dati aperti (Linked Open Data - LOD). In linea con i principi enunciati e in continuità con le azioni avviate con i Piani precedenti e alla luce delle novità normative e tecniche descritte, il presente Piano triennale mira ad assicurare maggiore efficacia all'attività amministrativa in tutti i processi che coinvolgono l'utilizzo dei dati, sia con riferimento alla condivisione dei dati tra pubbliche amministrazioni per finalità istituzionali, sia con riferimento al riutilizzo dei dati, anche per finalità commerciali, secondo il paradigma dei dati aperti. Rispetto alle precedenti edizioni del Piano triennale, alcuni obiettivi e risultati attesi sono stati rimodulati in modo da creare una più chiara associazione tra obiettivo/risultato atteso e soggetto responsabile.

Ove applicabile, per l'attuazione delle linee di azione definite di seguito, le PA di piccole dimensioni, come i comuni al di sotto di 5.000 abitanti, possono sfruttare meccanismi di sussidiarietà (ad esempio attraverso le Regioni e Province autonome, i Comuni capoluogo di provincia, le Unioni dei Comuni, le Città metropolitane e le Province, anche tramite i relativi uffici associati tra quelli esistenti).

A tal proposito, si richiamano le funzioni di raccolta ed elaborazione dati attribuite dalla Legge n. 56 del 2014 alle Province e alle Città metropolitane, a servizio degli enti locali del territorio. Le "Linee guida recanti regole tecniche per l'apertura dei dati e il riutilizzo dell'informazione del settore pubblico" (Linee guida Open Data, d'ora in avanti) forniscono elementi utili di data governance in relazione ad aspetti organizzativi che possano abilitare un processo di apertura ed interoperabilità dei dati efficiente ed efficace. Anche l'interoperabilità, garantita dalla adozione di una semantica unica, come descritto nelle Linee guida sull'interoperabilità tecnica delle pubbliche amministrazioni, deve essere tenuta in conto nella governance dei dati. Il processo di formazione e pubblicazione dei dati può seguire lo schema proposto nelle suddette Linee guida che si compone delle seguenti fasi:

1. identificazione (ricognizione, analisi dei vincoli, priorità e percorso di apertura dei dati)
2. analisi (analisi della qualità, bonifica, analisi di processo)
3. arricchimento (vocabolari controllati, ontologie, mashup e linking nei linked open data - LOD)
4. modellazione e documentazione (schemi dei dati, modelli dati, conservazione e storicizzazione)
5. validazione (qualità dei dati)
6. pubblicazione (meta datazione, politiche di accesso e licenza, modalità di pubblicazione).

Per attuare tale processo, ferma restando l'autonomia organizzativa delle attività di ciascuna amministrazione, è necessario definire una chiara data governance anche interna con l'individuazione di ruoli e relative responsabilità e integrare le sue fasi sia verticalmente, rispetto ai processi interni già consolidati, che orizzontalmente rispetto alle necessità specifiche dell'Amministrazione. Un ruolo determinante è svolto dal RTD che, sulla base della Circolare n. 3 del 1° ottobre 2018 del Ministro per la Pubblica Amministrazione, può costituire

un apposito Gruppo di lavoro come possibile struttura per il governo del processo di apertura dei dati, in cui, oltre ad un responsabile, siano coinvolti i referenti tematici che gestiscono e trattano dati nell'ambito delle singole unità organizzative. È importante, inoltre, garantire il raccordo e la consultazione con le altre figure coinvolte nel processo di digitalizzazione della Pubblica Amministrazione, quali il responsabile per la conservazione documentale, il responsabile per la prevenzione della corruzione e la trasparenza, il responsabile della protezione dei dati, il responsabile per la sicurezza. L'attività di apertura e di pubblicazione dei dati, infine, può essere tracciata oltre che nel Piano triennale ICT anche come obiettivo del PIAO di ciascuna amministrazione, sulla base di una eventuale scala di priorità basata, per esempio, su un approccio di tipo demand-driven che tenga conto dell'impatto economico e sociale nonché del livello di interesse e delle necessità degli utilizzatori.

Analogamente per i processi di data governance e per le attività di messa a disposizione di asset semantici per garantire l'interoperabilità dei dati, si potrà prevedere un percorso di definizione di modalità di pubblicazione di ontologie, vocabolari controllati e schemi dati, anche attraverso gli HUB nazionali e regionali (ad es. per la messa a disposizione da parte degli enti di cataloghi o di altre soluzioni condivise, per la delega di processi di servizio relativi ai dati, ecc.). Sono necessari, infine, momenti di confronto su esperienze, buone pratiche, nuove soluzioni tecnologiche, procedure organizzative, servizi innovativi intorno al tema degli open data. Uno di questi momenti potrebbe essere una Conferenza nazionale a cadenza annuale in cui coinvolgere PA, imprese pubbliche e private, accademia, utenti, comunità, sviluppatori per fare sintesi sul livello di maturità dei dati in Italia. Inoltre, per migliorare l'esperienza dell'utente nella ricerca e nell'utilizzo di dati disponibili su Catalogo Nazionale dei Dati Aperti è in previsione la realizzazione - entro fine 2025 - di un assistente virtuale (chatbot) che sfrutti l'Intelligenza Artificiale.

Contesto normativo

Riferimenti normativi italiani:

- Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"
- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (in breve CAD) artt. 50, 50-ter., 51, 52, 59, 60
- Decreto legislativo 24 gennaio 2006, n. 36 "Attuazione della direttiva (UE) 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico che ha abrogato la direttiva 2003/98/CE"
- Decreto legislativo 27 gennaio 2010, n. 32 "Attuazione della direttiva 2007/2/CE, che istituisce un'infrastruttura per l'informazione territoriale nella Comunità europea (INSPIRE)"
- Decreto legislativo 14 marzo 2013, n. 33 "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni" (Decreto trasparenza)

- Decreto legislativo 10 agosto 2018, n. 101 “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE” (regolamento generale sulla protezione dei dati)
- Decreto-legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 “Misure urgenti per la semplificazione e l'innovazione digitale”
- Decreto-legge 31 maggio 2021, n. 77, convertito con modificazioni dalla Legge 29 luglio 2021, n. 108 “Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure”
- Linee Guida AGID per i cataloghi dati (2017)
- Linee Guida AGID per l'implementazione della specifica GeoDCAT-AP (2017)
- Linee Guida AGID recanti regole tecniche per la definizione e l'aggiornamento del contenuto del Repertorio Nazionale dei Dati Territoriali (2022)
- Linee Guida AGID recanti regole tecniche per l'attuazione del decreto legislativo 24 gennaio 2006, n. 36 e s.m.i. relativo all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico adottate con Determinazione AGID n. 183/2023 del 3 agosto 2023
- Manuale RNDT - Guide operative per la compilazione dei metadati RNDT
- Piano Nazionale di Ripresa e Resilienza - Investimento 1.3: “Dati e interoperabilità”

Riferimenti normativi europei:

- Direttiva 2007/2/CE del Parlamento europeo e del Consiglio, del 14 marzo 2007, che istituisce un'Infrastruttura per l'informazione territoriale nella Comunità europea (Inspire)
- Regolamento (CE) n. 1205/2008 del 3 dicembre 2008 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda i metadati
- Regolamento (CE) n. 976/2009 della Commissione, del 19 ottobre 2009, recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda i servizi di rete
- Regolamento (UE) 2010/1089 del 23 novembre 2010 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda l'interoperabilità dei set di dati territoriali e dei servizi di dati territoriali
- Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (in breve GDPR)
- Direttiva (UE) 2019/1024 del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico

- Decisione (UE) 2019/1372 del 19 agosto 2019 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda il monitoraggio e la comunicazione
- Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati)
- Regolamento di esecuzione (UE) 2023/138 della Commissione del 21 dicembre 2022 che stabilisce un elenco di specifiche serie di dati di elevato valore e le relative modalità di pubblicazione e riutilizzo
- Comunicazione della Commissione 2014/C 240/01 del 24 luglio 2014 - Orientamenti sulle licenze standard raccomandate, i dataset e la tariffazione del riutilizzo dei documenti
- Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni COM (2020) del 19 febbraio 2020 – Una strategia europea per i dati

Obiettivo 5.1 – Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese

Risultati attesi:

- RA5.1.1 - Aumento del numero di dataset aperti di tipo dinamico in coerenza con quanto previsto dalle Linee guida Open Data
- RA5.1.2 - Aumento del numero di dataset resi disponibili attraverso i servizi di rete di cui al framework creato con la Direttiva 2007/2/EC (INSPIRE) e relativi Regolamenti attuativi, con particolare riferimento ai dati di elevato valore di cui al Regolamento di esecuzione (UE) 2023/138
- RA5.1.3 - Disponibilità delle categorie di dati protetti di cui all'art. 3 del Regolamento (UE) 2022/868 (DGA)

CAP5.PA.01

Le PA adeguano i metadati relativi ai dati geografici all'ultima versione delle specifiche nazionali e documentano i propri dataset nel Catalogo nazionale geodati.gov.it

Azioni previste/eseguite: il Comune di San Sperate non ha dati geografici nel catalogo nazionale.

CAP5.PA.02

Le PA adeguano i metadati relativi ai dati non geografici alle specifiche nazionali e documentano i propri dataset nel Catalogo nazionale dati.gov.it.

Azioni previste/eseguite: il Comune di San Sperate attualmente non è censito in tale banca dati.

CAP5.PA.03

Le PA partecipano, in funzione delle proprie necessità, a interventi di formazione e sensibilizzazione sulle politiche open data.

Azioni previste/eseguite: il Comune di San Sperate provvederà ad aderire a interventi di formazione e sensibilizzazione sulle politiche open data nel corso del triennio indicato.

CAP5.PA.04

Le PA attuano le indicazioni sui dati di elevato valore presenti nel Regolamento di esecuzione (UE) 2023/138, nelle Linee guida Open Data nonché nella specifica guida operativa.

Azioni previste/eseguite: il Comune di San Sperate non possiede dati di elevato valore da pubblicare.

Obiettivo 5.2 – Aumentare la qualità dei dati e dei metadati

Risultati attesi:

- RA5.2.1 - Aumento del numero di dataset con metadati di qualità conformi agli standard di riferimento europei e nazionali
- RA5.2.2 - Aumento del numero di dataset di tipo aperto resi disponibili dalle pubbliche amministrazioni e documentati nel portale dati.gov.it
- RA5.2.3 - Aumento del numero di amministrazioni non ancora presenti nel catalogo dati.gov.it che rendono disponibili dataset di tipo aperto
- RA5.2.4 - Aumento del numero di dataset documentati sul portale dati.gov.it che rispettano la caratteristica di qualità “attualità” (o tempestività di aggiornamento) di cui allo Standard ISO/IEC 25012

CAP5.PA.05

Le PA pubblicano i metadati relativi ai dati di elevato valore, secondo le indicazioni presenti nel Regolamento di esecuzione (UE) e nelle Linee guida sui dati aperti e relativa guida operativa, nei cataloghi nazionali dati.gov.it e geodati.gov.it.

Azioni previste/eseguite: il Comune di San Sperate non possiede dati di elevato valore da pubblicare.

CAP5.PA.06

Ogni Comune con popolazione tra 10.000 e 100.000 abitanti, ogni Unione di Comuni o altri tipi di consorzi e associazioni, ogni Comunità Montana o isolana pubblica (non ancora presenti nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 3 dataset.

Azioni previste/eseguite: il Comune di San Sperate non rientra nella tipologia interessata dalla linea di azione.

CAP5.PA.07

Ogni Comune con popolazione tra 100.001 e 250.000 abitanti, ogni Provincia e Città

Metropolitana (non ancora presenti nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 5 dataset.

Azioni previste/eseguite: il Comune di San Sperate non rientra nella tipologia interessata dalla linea di azione.

CAP5.PA.08

Ogni Comune con popolazione > 250.000 abitanti, ogni Regione ed ogni altro ente territoriale regionale, ogni Università, Ente e centro di ricerca (non ancora presenti nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 10 dataset.

Azioni previste/eseguite: il Comune di San Sperate non rientra nella tipologia interessata dalla linea di azione.

CAP5.PA.09

Ogni PA centrale (non ancora presente nel catalogo dati.gov.it) pubblica e documenta nel catalogo almeno 15 dataset.

Azioni previste/eseguite: il Comune di San Sperate non rientra nella tipologia interessata dalla linea di azione.

CAP5.PA.10

Ogni Comune con popolazione tra 5.000 e 10.000 abitanti (non ancora presente nel 2024 nel catalogo dati.gov.it) pubblica e documenta nel catalogo almeno 1 dataset.

Azioni previste/eseguite: il Comune di San Sperate non ha ancora pubblicato dataset.

Obiettivo 5.3 – Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati

Risultati attesi:

- RA5.3.1 - Aumento del numero di dataset di tipo aperto documentati nel portale dati.gov.it che adottano le licenze previste dalle Linee guida Open Data

CAP5.PA.11

Le PA attuano le linee guida contenenti regole tecniche per l'implementazione del Decreto Legislativo n. 36/2006 relativamente ai requisiti e alle raccomandazioni su licenze e condizioni d'uso.

Azioni previste/eseguite: il Comune di San Sperate non ha ancora adeguato le pubblicazioni a tale linea di azione.

Intelligenza artificiale per la Pubblica Amministrazione

Scenario

Per sistema di Intelligenza Artificiale (IA) si intende un sistema automatico che, per obiettivi espliciti o impliciti, deduce dagli input ricevuti come generare output come previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali. I sistemi di IA variano nei loro livelli di autonomia e adattabilità dopo l'implementazione (Fonte: OECD AI principles overview). L'intelligenza artificiale ha il potenziale per essere una tecnologia estremamente utile, o addirittura dirompente, per la modernizzazione del settore pubblico. L'IA sembra essere la risposta alla crescente necessità di migliorare l'efficienza e l'efficacia nella gestione e nell'erogazione dei servizi pubblici. Tra le potenzialità delle tecnologie di intelligenza artificiale si possono citare le capacità di:

- automatizzare attività di ricerca e analisi delle informazioni semplici e ripetitive, liberando tempo di lavoro per attività a maggior valore;
- aumentare le capacità predittive, migliorando il processo decisionale basato sui dati;
- supportare la personalizzazione dei servizi incentrata sull'utente, aumentando l'efficacia dell'erogazione dei servizi pubblici anche attraverso meccanismi di proattività.

L'Unione Europea mira a diventare leader strategico nell'impiego dell'intelligenza artificiale nel settore pubblico. Questa intenzione è chiaramente espressa nella Comunicazione "Piano Coordinato sull'Intelligenza Artificiale" COM (2021) 205 del 21 aprile 2021 in cui la Commissione europea propone specificamente di "rendere il settore pubblico un pioniere nell'uso dell'IA". Il Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 (AI Act) stabilisce regole armonizzate sull'intelligenza artificiale. L'AI Act affronta i rischi legati all'utilizzo dell'IA, classificandoli in quattro diversi livelli: rischio inaccettabile (divieto), rischio elevato, rischio limitato e rischio minimo. L'AI Act introduce obblighi di trasparenza per i grandi modelli generalisti di IA. Il regolamento intende porre le basi per costruire un ecosistema di eccellenza nell'IA e rafforzare la capacità dell'Unione Europea di competere a livello globale con soluzioni di intelligenza artificiale affidabile.

La "Comunicazione sulla promozione delle start-up e dell'innovazione nell'IA affidabile", COM (2024) del 24 gennaio 2024, ha lanciato l'iniziativa "GenAI4EU" che ha l'obiettivo di promuovere lo sviluppo di grandi ecosistemi di innovazione aperta, favorendo la collaborazione tra startup di IA e utilizzatori di IA nell'industria e nel settore pubblico. L'Unione Europea promuove la cooperazione tra startup, operatori dell'industria delle tecnologie dell'informazione e pubbliche amministrazioni per lo sviluppo di applicazioni di intelligenza artificiale generativa affidabile.

L'AI Act ha introdotto una importante sfida in materia di normazione tecnica. La Commissione Europea ha adottato il 25 maggio 2023 la Decisione C(2023)3215 - Standardisation request M/5932 con la quale ha affidato agli Enti di normazione europei CEN e CENELEC la redazione

di norme tecniche europee a vantaggio dei sistemi di intelligenza artificiale in conformità con i principi dell'AI Act. Il "Dispositivo per la ripresa e la resilienza" ha tra gli obiettivi quello di favorire la creazione di una industria dell'intelligenza artificiale nell'Unione Europea al fine di assumere un ruolo guida a livello globale nello sviluppo e nell'adozione di tecnologie di IA antropocentriche, affidabili, sicure e sostenibili. In Italia il PNRR prevede importanti misure di finanziamento sia per la ricerca in ambito di intelligenza artificiale sia per lo sviluppo di piattaforme di IA per i servizi della Pubblica Amministrazione.

In applicazione dell'AI Act, il DTD di concerto con ACN e AGID promuoverà l'obiettivo di innalzare i livelli di cybersecurity dell'Intelligenza Artificiale per assicurare che sia progettata, sviluppata e impiegata in maniera sicura, anche in coerenza con le linee guida internazionali sulla sicurezza dell'Intelligenza Artificiale. La cybersecurity è un requisito essenziale dell'IA al fine di garantire resilienza, privacy, correttezza ed affidabilità, ovvero un cyberspazio più sicuro.

La "Strategia italiana per l'intelligenza artificiale 2024-2026" stabilisce gli obiettivi di promozione e sviluppo dell'IA, suddividendoli in quattro macroaree: Ricerca, Pubblica Amministrazione, Industria, Formazione. La strategia include, inoltre, azioni abilitanti specifiche in termini di infrastrutture e coordinamento. L'obiettivo complessivo è creare un quadro di azioni sinergiche che consenta di condividere buone pratiche e di favorire uno scambio efficace di conoscenze e competenze tra il mondo accademico, le imprese e la Pubblica Amministrazione. Il Piano triennale declina in linee di azione operative gli obiettivi per la Pubblica Amministrazione definiti nella "Strategia italiana per l'intelligenza artificiale 2024-2026". La Pubblica Amministrazione italiana conta esperienze rilevanti nello sviluppo e utilizzo di soluzioni di intelligenza artificiale. A titolo esemplificativo si citano le esperienze di:

- Agenzia delle entrate e INAIL, utilizzo di algoritmi di machine learning per analizzare schemi e comportamenti sospetti, aiutando nella prevenzione e rilevazione di frodi;
- INPS, adozione di chatbot per semplificare e personalizzare l'interazione con l'utente, migliorando l'accessibilità e l'usabilità dei servizi;
- INPS, adozione di chatbot per semplificare e personalizzare l'interazione con l'utente, migliorando l'accessibilità e l'usabilità dei servizi;

Collaborazioni con partner pubblici e privati per progetti di ricerca finalizzati allo sviluppo di LLM italiani. L'affermarsi dei grandi modelli generalisti di IA costituisce un importante fattore di accelerazione per lo sviluppo e l'adozione di soluzioni di intelligenza artificiale. Per grandi modelli generalisti di IA si intendono sistemi di grandi dimensioni in grado di svolgere un'ampia gamma di compiti specifici, come la generazione di video, testi, immagini, la conversazione in linguaggio naturale, l'elaborazione o la generazione di codice informatico. L'AI Act definisce come grandi modelli generalisti di IA ad elevato impatto i modelli addestrati con una grande quantità di dati e con complessità, capacità e prestazioni elevate. Le amministrazioni pubbliche che intendono adottare soluzioni basate su intelligenza artificiale valutano le opportunità offerte dalle tecnologie di edge computing in termini di efficienza,

reattività e gestione dei dati in contesti locali con particolare attenzione all'utilizzo di sensoristica, computazione decentrata e di sistemi realizzati con modelli IA anche di piccole dimensioni e/o con reti di agenti intelligenti.

Ambienti di sperimentazione e sviluppo

Per sostenere il raggiungimento degli obiettivi definiti dalla “Strategia italiana per l'intelligenza artificiale 2024-2026” e del Piano triennale, AGID intende istituire, gestire e promuovere “Ambienti di Sperimentazione e Sviluppo di Intelligenza Artificiale”. Le finalità degli “Ambienti” sono:

- accelerare l'apprendimento e lo sviluppo delle competenze delle pubbliche amministrazioni nella gestione, acquisizione e sviluppo di soluzioni basate sulle tecnologie di IA;
- aumentare la consapevolezza dei soggetti coinvolti nella catena del valore delle soluzioni di IA (Abilitatori, Sperimentatori/Sviluppatori, Utilizzatori), circa le modalità tecnico/amministrative più efficaci per la conduzione di progetti di IA;
- promuovere lo sviluppo di proof of concept (POC) e di soluzioni basate su IA che rispondano alle esigenze e ai casi d'uso di interesse delle pubbliche amministrazioni.

I soggetti destinatari degli “Ambienti” sono:

- abilitatori: soggetti che forniscono tecnologie di IA abilitanti che fungono da elementi costitutivi (building blocks) per lo sviluppo di soluzioni avanzate. Queste tecnologie includono: strumenti di Machine Learning, Large Language Models (LLM), Small Language Models (SLM).
- sperimentatori/sviluppatori: soggetti in grado di sviluppare proof of concept o soluzioni basate sulle tecnologie di IA abilitanti per soddisfare i casi d'uso di interesse delle pubbliche amministrazioni.
- utilizzatori: pubbliche amministrazioni interessate all'adozione di soluzioni basate su tecnologie di intelligenza artificiale.

Il riuso dei risultati degli “Ambienti Sperimentazione e Sviluppo di Intelligenza Artificiale”, inclusi proof of concept e soluzioni, sarà promosso anche attraverso soggetti aggregatori (Hub) nazionali e regionali.

Principi generali per l'utilizzo dell'intelligenza artificiale nella Pubblica Amministrazione

Le amministrazioni pubbliche devono affrontare molte sfide nel perseguire l'utilizzo dell'intelligenza artificiale. Di seguito si riportano alcuni principi generali che dovranno essere adottati dalle pubbliche amministrazioni e declinati in fase di applicazione tenendo in considerazione lo scenario in veloce evoluzione.

1. **Miglioramento dei servizi e riduzione dei costi.** Le pubbliche amministrazioni concentrano l'investimento in tecnologie di intelligenza artificiale nell'automazione dei compiti ripetitivi connessi ai servizi istituzionali obbligatori e al funzionamento dell'apparato amministrativo. Il conseguente recupero di risorse è destinato al miglioramento della qualità dei servizi anche mediante meccanismi di proattività.
2. **Analisi del rischio.** Le amministrazioni pubbliche analizzano i rischi associati all'impiego di sistemi di intelligenza artificiale per assicurare che tali sistemi non provochino violazioni dei diritti fondamentali della persona o altri danni rilevanti. Le pubbliche amministrazioni adottano la classificazione dei sistemi di IA secondo le categorie di rischio definite dall'AI Act.
3. **Trasparenza, responsabilità e informazione.** Le pubbliche amministrazioni pongono particolare attenzione alla trasparenza e alla interpretabilità dei modelli di intelligenza artificiale al fine di garantire la responsabilità e rendere conto delle decisioni adottate con il supporto di tecnologie di intelligenza artificiale. Le amministrazioni pubbliche forniscono informazioni adeguate agli utenti al fine di consentire loro di prendere decisioni informate riguardo all'utilizzo dei servizi che sfruttano l'intelligenza artificiale.
4. **Inclusività e accessibilità.** Le pubbliche amministrazioni sono consapevoli delle responsabilità e delle implicazioni etiche associate all'uso delle tecnologie di intelligenza artificiale. Le pubbliche amministrazioni assicurano che le tecnologie utilizzate rispettino i principi di equità, trasparenza e non discriminazione.
5. **Privacy e sicurezza.** Le pubbliche amministrazioni adottano elevati standard di sicurezza e protezione della privacy per garantire che i dati dei cittadini siano gestiti in modo sicuro e responsabile. In particolare, le amministrazioni garantiscono la conformità dei propri sistemi di IA con la normativa vigente in materia di protezione dei dati personali e di sicurezza cibernetica.
6. **Formazione e sviluppo delle competenze.** Le pubbliche amministrazioni investono nella formazione e nello sviluppo delle competenze necessarie per gestire e applicare l'intelligenza artificiale in modo efficace nell'ambito dei servizi pubblici. A tale proposito si faccia riferimento agli obiettivi individuati nel Capitolo 1.
7. **Standardizzazione.** Le pubbliche amministrazioni tengono in considerazione, durante le fasi di sviluppo o acquisizione di soluzioni basate sull'intelligenza artificiale, le attività di normazione tecnica in corso a livello internazionale e a livello europeo da CEN e CENELEC con particolare riferimento ai requisiti definiti dall'AI Act.
8. **Sostenibilità.** Le pubbliche amministrazioni valutano attentamente gli impatti ambientali ed energetici legati all'adozione di tecnologie di intelligenza artificiale e adottando soluzioni sostenibili dal punto di vista ambientale.
9. **Foundation Models** (Sistemi IA "ad alto impatto"). Le pubbliche amministrazioni, prima di adottare foundation models "ad alto impatto", si assicurano che essi adottino adeguate misure di trasparenza che chiariscono l'attribuzione delle responsabilità e dei ruoli, in particolare dei fornitori e degli utenti del sistema di IA.

10. **Dati.** Le pubbliche amministrazioni, che acquistano servizi di intelligenza artificiale tramite API, valutano con attenzione le modalità e le condizioni con le quali il fornitore del servizio gestisce i dati forniti dall'amministrazione con particolare riferimento alla proprietà dei dati e alla conformità con la normativa vigente in materia di protezione dei dati e privacy.

Dati per l'intelligenza artificiale

La disponibilità di dati di alta qualità e il rispetto dei valori e dei diritti europei, quali la protezione dei dati personali, la tutela dei consumatori e la normativa in materia di concorrenza sono i prerequisiti fondamentali nonché un presupposto per lo sviluppo e la diffusione dei sistemi di IA. La disponibilità di dati rappresenta peraltro un requisito chiave per l'adozione di un approccio all'intelligenza artificiale attento alle specificità nazionali.

La Strategia Europea per i dati è implementata dal punto normativo dagli atti sopra citati che costituiscono il quadro regolatorio entro il quale deve muoversi una Pubblica Amministrazione che intende operare con sistemi di IA sui dati aperti. Riguardo l'utilizzo dei dati da parte di sistemi di intelligenza artificiale, l'AI Act richiede ai fornitori di sistemi di IA di adottare una governance dei dati e appropriate procedure di gestione dei dati (con particolare attenzione alla generazione e alla raccolta dei dati, alle operazioni di preparazione dei dati, alle scelte di progettazione e alle procedure per individuare e affrontare le distorsioni e le potenziali distorsioni per correlazione o qualsiasi altra carenza pertinente nei dati). L'AI Act pone particolare attenzione agli aspetti qualitativi dei set di dati utilizzati per addestrare, convalidare e testare i sistemi di IA (tra cui rappresentatività, pertinenza, completezza e correttezza). La Commissione Europea ha avviato una specifica attività presso il CEN e il CENELEC per definire norme tecniche europee per rispondere a tali esigenze.

Nel contesto nazionale, considerando un'architettura istituzionale che organizza i territori in regioni e comuni, con l'obiettivo di garantire livelli di servizio uniformi, diventa cruciale progettare e implementare soluzioni nazionali basate sull'IA. Queste soluzioni devono essere in grado, da un lato, di superare eventuali disparità cognitive che caratterizzano le diverse amministrazioni territoriali e, dall'altro, di assicurare un pieno coordinamento tra territori differenti riguardo a servizi chiave per la società. Riguardo l'affermarsi dei grandi modelli generalisti di IA nel settore pubblico, una sfida fondamentale consiste nella creazione di dataset di elevata qualità, rappresentativi della realtà della Pubblica Amministrazione, con particolare riguardo al corpus normativo nazionale e comunitario, ai procedimenti amministrativi e alla struttura organizzativa della Pubblica Amministrazione italiana stessa.

Contesto normativo

Riferimenti normativi europei:

- Comunicazione della Commissione al Parlamento Europeo e al Consiglio, "Piano Coordinato sull'Intelligenza Artificiale", COM (2021) 205 del 21 aprile 2021

- Decisione della Commissione “on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence” C (2023) 3215 del 22 maggio 2023
- Comunicazione della Commissione al Parlamento Europeo e al Consiglio “Sulla promozione delle start-up e dell'innovazione nell'IA affidabile”, COM (2024) 28 del 24 gennaio 2024
- Regolamento del Parlamento europeo e del Consiglio “che stabilisce regole armonizzate sull'intelligenza artificiale”, (UE) 2024/1689 del 13 giugno 2024
- Strategia italiana per l'intelligenza artificiale 2024-2026

Obiettivo 5.4 – Aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale

Risultati attesi:

- RA5.4.1 - Linee guida per promuovere l'adozione dell'IA nella Pubblica Amministrazione
- RA5.4.2 - Linee guida per il procurement di IA nella Pubblica Amministrazione
- RA5.4.3 - Linee guida per lo sviluppo di applicazioni di IA per la Pubblica Amministrazione
- RA5.4.4 - Realizzazione di applicazioni di IA a valenza nazionale

CAP5.PA.12

Le PA dovranno rispettare le Linee per promuovere l'adozione dell'IA nella Pubblica Amministrazione

Azioni previste/eseuite: il Comune di San Sperate non ha ancora adottato soluzioni basate sull'IA.

CAP5.PA.13

Le PA dovranno rispettare le Linee guida per il procurement di IA nella Pubblica Amministrazione

Azioni previste/eseuite: il Comune di San Sperate non ha ancora adottato soluzioni basate sull'IA.

CAP5.PA.14

Le PA dovranno rispettare le Linee guida per lo sviluppo di applicazioni di IA nella Pubblica Amministrazione

Azioni previste/eseuite: il Comune di San Sperate non svilupperà internamente applicazioni basate sull'IA.

CAP5.PA.15

Le PA trasmettono periodicamente all'AgID i dati fondamentali delle iniziative nell'ambito delle tecnologie di IA

Azioni previste/eseguite: il Comune di San Sperate rimane in attesa delle indicazioni pratiche per l'adempimento.

CAP5.PA.16

Le PA trasmettono periodicamente all'AgID i dati fondamentali delle iniziative nell'ambito delle tecnologie di IA

Azioni previste/eseguite: il Comune di San Sperate rimane in attesa delle indicazioni per valutare le azioni pratiche da seguire.

Obiettivo 5.5 – Dati per l'intelligenza artificiale

Risultati attesi: RA5.5.1 - Basi di dati nazionali strategiche

CAP5.PA.17

Le PA adottano le basi dati nazionali strategiche

Azioni previste/eseguite: il Comune di San Sperate rimane in attesa delle indicazioni e/o linee guida per valutare le azioni pratiche da seguire.

Capitolo 6 – Infrastrutture

Infrastrutture digitali e Cloud

Scenario

La strategia “Cloud Italia”, pubblicata a settembre 2021 dal Dipartimento per la Trasformazione Digitale e dall’Agenzia per la Cybersicurezza Nazionale nell’ambito del percorso attuativo definito dall’art.33-septies del Decreto-Legge n.179 del 2012 e gli investimenti del PNRR legati all’abilitazione cloud rappresentano una grande occasione per supportare la riorganizzazione strutturale e gestionale delle pubbliche amministrazioni. Non si tratta di una operazione unicamente tecnologica, le cui opportunità vanno esplorate a fondo da ogni ente.

La Strategia Cloud risponde a tre sfide principali: assicurare l’autonomia tecnologica del Paese, garantire il controllo sui dati e aumentare la resilienza dei servizi digitali. In coerenza con gli obiettivi del PNRR, la strategia traccia un percorso per accompagnare le PA italiane nella migrazione dei dati e degli applicativi informatici verso un ambiente cloud sicuro. Con il principio cloud first, si vuole guidare e favorire l’adozione sicura, controllata e completa delle tecnologie cloud da parte del settore pubblico, in linea con i principi di tutela della privacy e con le raccomandazioni delle istituzioni europee e nazionali. In particolare, le pubbliche amministrazioni, in fase di definizione di un nuovo progetto, e/o di sviluppo di nuovi servizi, in via prioritaria devono valutare l’adozione del paradigma cloud prima di qualsiasi altra tecnologia. Secondo tale principio, quindi, tutte le Amministrazioni sono obbligate ad effettuare una valutazione in merito all’adozione del cloud che rappresenta l’evoluzione tecnologica più dirompente degli ultimi anni e che sta trasformando radicalmente tutti i sistemi informativi della società a livello mondiale. Nel caso di eventuale esito negativo, tale valutazione dovrà essere motivata.

L’adozione del paradigma cloud rappresenta, infatti, la chiave della trasformazione digitale abilitando una vera e propria rivoluzione del modo di pensare i processi di erogazione dei servizi della PA verso cittadini, professionisti ed imprese. L’attuazione dell’art.33-septies del Decreto-legge n. 179 del 2012, non rappresenta solo un adempimento legislativo, ma è soprattutto una occasione perché ogni ente attivi gli opportuni processi di gestione interna con il fine di modernizzare i propri applicativi e al contempo migliorare la fruizione dei procedimenti, delle procedure e dei servizi erogati.

È anche quindi una grande occasione per:

- ridurre il debito tecnologico accumulato negli anni dalle amministrazioni;
- mitigare il rischio di lock-in verso i fornitori di sviluppo e manutenzione applicativa;
- ridurre significativamente i costi di manutenzione di centri elaborazione dati (data center) obsoleti e delle applicazioni legacy, valorizzando al contempo le infrastrutture digitali del Paese più all’avanguardia che stanno attuando il percorso di adeguamento

rispetto ai requisiti del Regolamento AGID e relativi atti successivi dell'Agenzia per la Cybersicurezza Nazionale;

- incrementare la postura di sicurezza delle infrastrutture pubbliche per proteggerci dai rischi cyber.

In tal modo, le infrastrutture digitali saranno più affidabili e sicure e la Pubblica Amministrazione potrà rispondere in maniera organizzata agli attacchi informatici, garantendo continuità e qualità nella fruizione di dati e servizi. Nell'ambito dell'attuazione normativa della Strategia Cloud Italia e dell'articolo 33-septies del Decreto-Legge n.179/2012 è stato realizzato il Polo Strategico Nazionale (PSN), l'infrastruttura promossa dal Dipartimento per la Trasformazione Digitale che, insieme alle altre infrastrutture digitali qualificate e sicure, consente di fornire alle amministrazioni tutte le soluzioni tecnologiche adeguate e gli strumenti per realizzare il percorso di migrazione.

Il Regolamento attuativo dell'articolo 33-septies del Decreto-Legge n.179/2012, nella sua prima edizione, ha fissato al 28 febbraio 2023 il termine per la trasmissione dei piani di migrazione da parte delle amministrazioni. Dopo la presentazione dei Piani di migrazione, le amministrazioni devono gestire al meglio il trasferimento in cloud di dati, servizi e applicativi. Una fase da condurre e concludere entro il 30 giugno 2026, avendo cura dei riferimenti tecnici e normativi necessari per completare una migrazione di successo. Per realizzare al meglio il proprio piano di migrazione, le amministrazioni possono far riferimento al sito cloud.italia.it dove sono disponibili diversi strumenti a supporto, tra cui:

- il manuale di abilitazione al cloud, che da un punto di vista tecnico accompagna le PA nel percorso che parte dall'identificazione degli applicativi da migrare in cloud fino ad arrivare alla valutazione degli indicatori di risultato a migrazione avvenuta;
- un framework di lavoro che descrive il modello organizzativo delle unità operative (unità di controllo, unità di esecuzione e centri di competenza) che eseguiranno il programma di abilitazione;
- articoli tecnici di approfondimento relativi ai principali aspetti da tenere in considerazione durante una migrazione al cloud.

In particolare, mediante l'accesso agli strumenti sopra citati le amministrazioni possono trovare suggerimenti utili riguardo ai seguenti temi:

- come riconoscere e gestire possibili situazioni di lock-in;
- raccomandazioni sugli aspetti legati al back up dei dati e al disaster recovery;
- consigli sulla scelta della migliore strategia di migrazione dal re-host al re-architect in base alle caratteristiche degli applicativi da migrare;
- come migliorare la migrazione in cloud grazie a un approccio DevOps;
- come definire e separare correttamente i ruoli tra Unità di Controllo (chi governa il progetto di migrazione) e Unità di esecuzione (chi realizza la migrazione);
- come misurare costi/benefici derivanti dalla migrazione;

- come stabilire un perimetro di responsabilità condivise tra amministrazione utente e fornitore di servizi cloud;
- come sfruttare al massimo le opportunità del cloud grazie alle applicazioni cloud native, al re-architect e al re-purchase.

In caso di disponibilità all'interno del Catalogo dei servizi cloud per la PA qualificati da ACN di una soluzione SaaS che risponda alle esigenze delle amministrazioni, è opportuno valutare la migrazione verso il SaaS come soluzione prioritaria (principio SaaS-first) rispetto alle altre tipologie IaaS e PaaS.

Quindi, anche al fine di riqualificare la spesa della PA in sviluppo e manutenzione applicativa, le amministrazioni possono promuovere anche iniziative per la realizzazione di applicativi cloud native da erogare come SaaS mediante accordi verso altre amministrazioni anche attraverso il riuso di codice disponibile sul catalogo Developers Italia, nel rispetto della normativa applicabile.

Altro aspetto da curare è quello dei costi operativi correnti. Con la migrazione al cloud, ci sono grandi opportunità di risparmio economico, ma occorre strutturarsi per una corretta gestione dei costi cloud, sia da un punto di vista contrattuale che tecnologico. Inoltre, con il crescere di servizi digitali forniti ad uno stesso ente da una molteplicità di fornitori diversi, anche via cloud, cresce notevolmente la complessità della gestione del parco applicativo, rendendo difficile la concreta integrazione tra i software dell'ente, l'effettiva possibilità di interoperabilità verso altri enti, la corretta gestione dei dati, ecc. Questo richiede all'Ufficio RTD, in forma singola o associata, l'evoluzione verso nuove architetture a "microservizi". Lo stesso concetto di "Sistema Pubblico di Connettività" (SPC), ancora presente nel CAD all'art.73, dovrà trovare una sua evoluzione basata sulla nuova logica cloud. Oggi è proprio il cloud computing, con la sua natura decentrata, policentrica e federata, a rendere possibile il disegno originario del SPC e salvaguardare pienamente l'autonomia degli enti, la neutralità tecnologica e la concorrenza sulle soluzioni ICT destinate alle PA.

Accanto agli aspetti di natura organizzativa è necessario porre attenzione anche ad una serie di elementi di natura più tecnologica. Lo sviluppo delle infrastrutture digitali, infatti, è parte integrante della strategia di modernizzazione del settore pubblico: esse devono essere affidabili, sicure, energeticamente efficienti ed economicamente sostenibili e garantire l'erogazione di servizi essenziali per il Paese.

L'evoluzione tecnologica espone, tuttavia, i sistemi a nuovi e diversi rischi, anche con riguardo alla tutela dei dati personali. L'obiettivo di garantire una maggiore efficienza dei sistemi non può essere disgiunto dall'obiettivo di garantire contestualmente un elevato livello di sicurezza delle reti e dei sistemi informativi utilizzati dalla Pubblica Amministrazione. Tuttavia, molte infrastrutture della PA risultano ancora prive dei requisiti di sicurezza e di affidabilità necessari e, inoltre, sono carenti sotto il profilo strutturale e organizzativo. Ciò espone il Paese a numerosi rischi, tra cui quello di interruzione o indisponibilità dei servizi e quello di attacchi cyber, con conseguente accesso illegittimo da parte di terzi a dati (o flussi di dati)

particolarmente sensibili o perdita e alterazione degli stessi dati. Lo scenario delineato pone l'esigenza immediata di attuare un percorso di razionalizzazione delle infrastrutture per garantire la sicurezza dei servizi oggi erogati tramite infrastrutture classificate come gruppo B, mediante la migrazione degli stessi verso infrastrutture conformi a standard di qualità, sicurezza, performance e scalabilità, portabilità e interoperabilità.

Con il presente documento, in coerenza con quanto stabilito dall'articolo 33-septies del decreto-legge 18 ottobre 2012, n. 179, si ribadisce che:

- con riferimento alla classificazione dei data center di cui alla Circolare AGID 1/2019 e ai fini della strategia di razionalizzazione dei data center, le categorie "infrastrutture candidabili ad essere utilizzate da parte dei PSN" e "Gruppo A" sono rinominate "A";
- al fine di tutelare l'autonomia tecnologica del Paese, consolidare e mettere in sicurezza le infrastrutture digitali delle pubbliche amministrazioni di cui all'articolo 2, comma 2, lettere a) e c) del decreto legislativo 7 marzo 2005, n. 82, garantendo, al contempo, la qualità, la sicurezza, la scalabilità, l'efficienza energetica, la sostenibilità economica e la continuità operativa dei sistemi e dei servizi digitali, il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei ministri promuove lo sviluppo di un'infrastruttura ad alta affidabilità localizzata sul territorio nazionale, anche detta Polo Strategico Nazionale (PSN), per la razionalizzazione e il consolidamento dei Centri per l'elaborazione delle informazioni (CED) destinata a tutte le pubbliche amministrazioni;
- le amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, nel rispetto dei principi di efficienza, efficacia ed economicità dell'azione amministrativa, migrano i loro Centri per l'elaborazione delle informazioni (CED) e i relativi sistemi informatici, privi dei requisiti fissati dalla Circolare AGID 1/2019 e, successivamente, dal regolamento di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179 (di seguito Regolamento cloud e infrastrutture), verso l'infrastruttura del PSN o verso altra infrastruttura propria già esistente e in possesso dei requisiti fissati dalla Circolare AGID 1/2019 e, successivamente, dal Regolamento cloud e infrastrutture. Le amministrazioni centrali, in alternativa, possono migrare i propri servizi verso soluzioni cloud qualificate, nel rispetto di quanto previsto dal Regolamento cloud e infrastrutture;
- le amministrazioni locali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, nel rispetto dei principi di efficienza, efficacia ed economicità dell'azione amministrativa, migrano i loro Centri per l'elaborazione delle informazioni (CED) e i relativi sistemi informatici, privi dei requisiti fissati dalla Circolare AGID 1/2019 e, successivamente, dal regolamento cloud e infrastrutture, verso l'infrastruttura PSN o verso altra infrastruttura della PA già esistente in possesso dei requisiti fissati dallo stesso Regolamento cloud e infrastrutture. Le amministrazioni locali, in alternativa, possono migrare i propri servizi verso soluzioni cloud qualificate nel rispetto di quanto previsto dal Regolamento cloud e infrastrutture;

- le amministrazioni non possono investire nella costruzione di nuovi data center per ridurre la frammentazione delle risorse e la proliferazione incontrollata di infrastrutture con conseguente moltiplicazione dei costi. È ammesso il consolidamento dei data center nel rispetto di quanto previsto dall'articolo 33-septies del Decreto-legge 179/2012 e dal Regolamento di cui al comma 4 del citato articolo 33-septies.

Nel delineare il processo di razionalizzazione delle infrastrutture è necessario far riferimento anche a quanto previsto dalla “Strategia Cloud Italia”. In tal senso il documento prevede:

1. la creazione del PSN, la cui gestione e controllo di indirizzo siano autonomi da fornitori extra UE, destinato ad ospitare sul territorio nazionale principalmente dati e servizi strategici la cui compromissione può avere un impatto sulla sicurezza nazionale, in linea con quanto previsto in materia di perimetro di sicurezza nazionale cibernetica dal Decreto-legge 21 settembre 2019, n. 105 e dal DPCM 81/2021;
2. un percorso di qualificazione dei fornitori di cloud pubblico e dei loro servizi per garantire che le caratteristiche e i livelli di servizio dichiarati siano in linea con i requisiti necessari di sicurezza, affidabilità e rispetto delle normative rilevanti e iii) lo sviluppo di una metodologia di classificazione dei dati e dei servizi gestiti dalle pubbliche amministrazioni, per permettere una migrazione di questi verso la soluzione cloud più opportuna (PSN o adeguata tipologia di cloud qualificato).

Con riferimento al punto i) creazione del PSN, a dicembre 2022, in coerenza con la relativa milestone PNRR associata, è stata realizzata e testata l’infrastruttura PSN. Si ricorda che tale infrastruttura eroga servizi professionali di migrazione verso l’infrastruttura PSN, servizi di housing, hosting e cloud nelle tipologie IaaS, PaaS. Per maggiori informazioni sui servizi offerti da PSN si rimanda alla convenzione pubblicata sul sito della Presidenza del Consiglio dei Ministri.

Al 30 giugno 2024 risultano 257 tra PA Centrali, relative articolazioni organizzative di primo livello e Prefetture, Aziende Sanitarie Locali e Aziende Ospedaliere che hanno sottoscritto il contratto d’utenza per la migrazione verso il PSN a valere sulla misura 1.1 del PNRR. Con riferimento ai punti ii) qualificazione e iii) classificazione a dicembre 2021 è stata pubblicata la prima edizione del Regolamento cloud e infrastrutture e a gennaio 2022 i relativi atti successivi modificati successivamente. A giugno 2024 è entrato in vigore il nuovo Regolamento Cloud ACN. In particolare, il nuovo Regolamento, adottato da ACN con Decreto Direttoriale n. 21007/24 del 27 giugno 2024 e applicabile dal 1° agosto 2024, aggiorna i livelli minimi e le caratteristiche al mutato scenario di rischio e i termini legati al procedimento di rilascio delle qualifiche. Il Regolamento norma anche l’utilizzo delle infrastrutture di housing e i servizi di prossimità (cosiddetti edge), sempre più diffusi in ragione dell’esigenza di ridurre i tempi di latenza per gli utenti finali. Le nuove qualifiche saranno valide per 36 mesi e soggette ad attività di monitoraggio grazie alla quale ACN potrà verificare nel tempo il rispetto dei requisiti necessari al trattamento dei dati e dei servizi in linea con il livello di

classificazione. Le informazioni sul Regolamento possono essere reperite sul sito istituzionale dell'Agenzia per la Cybersicurezza Nazionale. Con riferimento al tema del cloud federato, si premette che la definizione tecnica coerentemente con la ISO/IEC 22123-1:2023 è la seguente: "modello di erogazione di servizi cloud forniti da 2 o più cloud service provider che si uniscono mediante un accordo che preveda un insieme concordato di procedure, processi e regole comuni finalizzato all'erogazione di servizi cloud". Le amministrazioni con infrastrutture classificate "A" che hanno deciso di investire sui propri data center per valorizzare i propri asset ai fini della razionalizzazione dei centri elaborazione dati, adeguandoli secondo le modalità e i termini previsti ai requisiti di cui al Regolamento adottato ai sensi del comma 4 dell'articolo 33-septies del Decreto-legge 179/2012, hanno la facoltà di valutare la possibilità di stringere accordi in tal senso per raggiungere maggiori livelli di affidabilità, sicurezza ed elasticità, purché siano rispettati i principi di efficacia ed efficienza dell'azione amministrativa e la normativa applicabile. Le amministrazioni che dovessero stipulare tali accordi realizzerebbero così le infrastrutture cloud federate della PA che si affiancano all'infrastruttura Polo Strategico Nazionale nel rispetto dell'articolo 33-septies del decreto-legge 18 ottobre 2012, n. 179. Per "infrastrutture di prossimità" (o edge computing) si intendono i nodi periferici (edge nodes), misurati come numero di nodi di calcolo come definiti dal nuovo Regolamento Cloud ACN 2024; si può trattare di un singolo server o di un altro insieme di risorse di calcolo connesse, operati nell'ambito di un'infrastruttura di edge computing, generalmente situati all'interno di un edge data center che opera all'estremità dell'infrastruttura, e quindi fisicamente più vicini agli utenti destinatari rispetto a un nodo cloud in un data center centralizzato". Le amministrazioni che intendono realizzare e/o utilizzare infrastrutture di prossimità verificano la conformità di queste ai requisiti del Regolamento di cui al comma 4 dell'articolo 33-septies del DL 179/2012.

Punti di attenzione e azioni essenziali per tutti gli enti

1) L'attuazione dell'art.33-septies Decreto-legge 179/2012, e del principio cloud-first, deve essere tra gli obiettivi prioritari dell'ente. Occorre curare da subito anche gli aspetti di sostenibilità economicofinanziaria nel tempo dei servizi attivati, avendo cura di verificare gli impatti della migrazione sui propri capitoli di bilancio relativamente sia ai costi correnti (OPEX) sia agli investimenti in conto capitale (CAPEX).

2) La gestione dei servizi in cloud deve essere presidiata dall'ente in tutto il ciclo di vita degli stessi e quindi è necessaria la disponibilità di competenze specialistiche all'interno dell'Ufficio RTD, in forma singola o associata.

Approfondimento tecnologico per gli RTD

1) La piena abilitazione al cloud richiede l'evoluzione del parco applicativo software verso la logica as a service delle applicazioni esistenti, andando oltre il mero lift-and-shift dei server, progettando opportuni interventi di rearchitect, replatform o repurchase per poter sfruttare le possibilità offerte oggi dalle moderne piattaforme computazionali e dagli algoritmi di

intelligenza artificiale. In tal senso, occorre muovere verso architetture a “microservizi” le cui caratteristiche sono, in sintesi, le seguenti:

- ogni servizio non ha dipendenze esterne da altri servizi e gestisce autonomamente i propri dati (self-contained)
- ogni servizio comunica con l'esterno attraverso API/webservice e senza dipendenza da stati pregressi (lightweight/stateless)
- ogni servizio può essere implementato con differenti linguaggi e tecnologie, in modo indipendente dagli altri servizi (implementation-independent)
- ogni servizio può essere dispiegato in modo automatico e gestito indipendentemente dagli altri servizi (independently deployable)
- ogni servizio implementa un insieme di funzioni legate a procedimenti e attività amministrative, non ha solo scopo tecnologico (business-oriented)

2) È compito dell'Ufficio RTD curare sia gli aspetti di pianificazione della migrazione/abilitazione al cloud che l'allineamento dello stesso con l'implementazione delle relative opportunità di riorganizzazione dell'ente offerte dall'abilitazione al cloud e dalle nuove architetture a microservizi.

3) La gestione del ciclo di vita dei servizi in cloud dell'amministrazione richiede la strutturazione di opportuni presidi organizzativi e strumenti tecnologici per il cloud-cost-management, in forma singola o associata.

Contesto normativo

Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82, “Codice dell'amministrazione digitale”, articoli. 8-bis e 73;
- Decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, “Ulteriori misure urgenti per la crescita del Paese”, articolo 33-septies;
- Decreto legislativo 18 maggio 2018, n. 65, “Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione”
- Decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla L. 18 novembre 2019, n. 133 “Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica”
- Decreto-legge 17 marzo 2020, n. 18, convertito con modificazioni dalla Legge 24 aprile 2020, n. 27 “Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19”, art. 75;

- Decreto-legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 “Misure urgenti per la semplificazione e l'innovazione digitale”, art. 35;
- Decreto-legge 31 maggio 2021, n. 77, convertito con modificazioni dalla Legge 29 luglio 2021, n. 108 “Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure”;
- Decreto-legge 14 giugno 2021, n. 82, convertito con modificazioni dalla Legge 4 agosto 2021, n. 109 “Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la Cybersicurezza Nazionale”
- Circolare AGID n. 1/2019, del 14 giugno 2019 - Censimento del patrimonio ICT delle Pubbliche Amministrazioni e classificazione delle infrastrutture idonee all'uso da parte dei Poli Strategici Nazionali;
- Strategia italiana per la banda ultra-larga (2021);
- Strategia Cloud Italia (2021);
- Regolamento AGID, di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la Pubblica Amministrazione e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la Pubblica Amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la Pubblica Amministrazione (2021 prima edizione, successivamente abrogata ai sensi dell'articolo 26 del Decreto Direttoriale ACN n.21007/24);
- Determinazioni ACN in attuazione al precedente Regolamento n. 306/2022 (con allegato) su e n. 307/2022 (con allegato) successivamente abrogati ai sensi dell'articolo 26 del Decreto Direttoriale ACN n.21007/24;
- Decreti direttoriali ACN prot. N. 29 del 2 gennaio 2023, n. 5489 dell'8 febbraio 2023 e n. 20610 del 28 luglio 2023 successivamente abrogati ai sensi dell'articolo 26 del Decreto Direttoriale ACN n.21007/24;
- Regolamento per le infrastrutture digitali e per i servizi cloud per la pubblica amministrazione, ai sensi dell'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221 (2024);
- Piano Nazionale di Ripresa e Resilienza:
 - M1C1 Investimento 1.1: “Infrastrutture digitali”
 - M1C1 Investimento 1.2: “Abilitazione e facilitazione migrazione al cloud”

Riferimenti normativi europei:

- European Commission Cloud Strategy, Cloud as an enabler for the European Commission Digital Strategy, 16 May 2019.
- Strategia europea sui dati, Commissione Europea 19.2.2020 COM (2020) 66 final;
- Data Governance and data policy at the European Commission, July 2020;
- Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) (2020)

Obiettivo 6.1 – Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la strategia «Cloud Italia» e migrando verso infrastrutture e servizi cloud qualificati (incluso PSN)

Risultati attesi: RA6.1.1 - Numero di amministrazioni migrate

CAP6.PA.01

Le PA proprietarie di data center di gruppo B richiedono l'autorizzazione ad AGID per le spese in materia di data center nelle modalità stabilite dalla Circolare AGID 1/2019 e prevedono in tali contratti, qualora autorizzati, una durata massima coerente con i tempi strettamente necessari a completare il percorso di migrazione previsti nei propri piani di migrazione.

Azioni previste/eseguite: il Comune di San Sperate non possiede datacenter di gruppo B.

CAP6.PA.02

Le PA proprietarie di data center classificati da AGID nel gruppo A continuano a gestire e mantenere tali data center in coerenza con quanto previsto dalla Strategia Cloud Italia e dal Regolamento cloud.

Azioni previste/eseguite: il Comune di San Sperate non possiede datacenter di gruppo A.

CAP6.PA.03

Le PA avviano il percorso di migrazione verso il cloud in coerenza con quanto previsto dalla Strategia Cloud Italia.

Azioni previste/eseguite: il Comune di San Sperate ha avviato il percorso di migrazione in cloud in coerenza con quanto previsto con la normativa vigente. È stata già realizzata la misura PNRR 1.2 e le relative azioni contemplate.

CAP6.PA.04

Le PA continuano ad applicare il principio cloud first e ad acquisire servizi cloud solo se qualificati

Azioni previste/eseguite: il Comune di San Sperate continua ad applicare il principio cloud first e ad acquisire servizi cloud solo se qualificati.

CAP6.PA.05

Le PA aggiornano l'elenco e la classificazione dei dati e dei servizi digitali in presenza di dati e servizi ulteriori rispetto a quelli già oggetto di conferimento e classificazione come indicato nel Regolamento e di conseguenza aggiornano, ove necessario, anche il piano di migrazione.

Azioni previste/eseguite: il Comune di San Sperate aggiornerà quando necessario il piano di migrazione, qualora questo fosse necessario.

CAP6.PA.06

Le PA, ove richiesto dal Dipartimento per la Trasformazione Digitale o da AGID, trasmettono le informazioni relative allo stato di avanzamento dell'implementazione dei piani di migrazione.

Azioni previste/eseguite: il Comune di San Sperate non ha ricevuto richieste di questo tipo. Se dovessero essere presentate istanze tali, l'Ente provvederà a trasmettere le informazioni richieste.

CAP6.PA.07

Le amministrazioni che intendono realizzare e/o utilizzare infrastrutture di prossimità verificano la conformità di queste ai requisiti del Regolamento di cui al comma 4 dell'articolo 33-septies del Decreto-legge 179/2012 e ne danno apposita comunicazione ad ACN.

Azioni previste/eseguite: il Comune di San Sperate non ha intenzione di realizzare e/o utilizzare infrastrutture di prossimità verificano la conformità.

CAP6.PA.08

Le PA con data center di tipo «A» che hanno avviato gli adeguamenti sui propri data center ai requisiti di cui al Regolamento cloud e relativi atti successivi, trasmettono ad ACN la dichiarazione di cui al medesimo Regolamento.

Azioni previste/eseguite: il Comune di San Sperate non possiede datacenter di gruppo A.

CAP6.PA.09

Le amministrazioni concludono la migrazione in coerenza con il piano di migrazione trasmesso ai sensi del Regolamento cloud e, ove richiesto dal Dipartimento per la Trasformazione Digitale o da AGID, trasmettono le informazioni necessarie per verificare il completamento della migrazione.

Azioni previste/eseguite: il Comune di San Sperate non ha inviato nessun piano di migrazione e attualmente non sono attive procedure di migrazione.

Il sistema pubblico di connettività

Scenario

Il Sistema Pubblico di Connettività (SPC) garantisce alle amministrazioni aderenti sia l'interscambio di informazioni in maniera riservata che la realizzazione della propria infrastruttura di comunicazione. A tale Sistema possono interconnettersi anche le reti regionali costituendo così una rete di comunicazione nazionale dedicato per l'interscambio di informazioni tra le pubbliche amministrazioni sia centrali che locali. Per effetto della legge n. 87 del 3 luglio 2023, di conversione del Decreto-legge 10 maggio 2023, n. 51 la scadenza dell'attuale Contratto Quadro è stata prorogata al 31 dicembre 2024; entro questa data sarà reso disponibile alle amministrazioni interessate il nuovo Contratto Quadro che prevederà oltre ai servizi di connettività anche i servizi di telefonia fissa come da informativa Consip del 13 aprile 2023. Il Sistema Pubblico di Connettività fornisce un insieme di servizi di rete che:

- permette alla singola Pubblica Amministrazione, centrale o locale, di interconnettere le proprie sedi e realizzare così anche l'infrastruttura interna di comunicazione;
- realizza un'infrastruttura condivisa di interscambio consentendo l'interoperabilità tra tutte le reti delle pubbliche amministrazioni salvaguardando la sicurezza dei dati;
- garantisce l'interconnessione della Pubblica Amministrazione alla rete internet;

Contesto normativo

Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82, "Codice dell'amministrazione digitale", articoli. 8-bis e 73;
- Strategia italiana per la Banda Ultra Larga 2023-2026

Obiettivo 6.2 – Garantire alle amministrazioni la disponibilità della connettività SPC

Risultati attesi: RA6.2.1 - Rete di connettività

CAP6.PA.10

Sulla base delle proprie esigenze, le pubbliche amministrazioni iniziano la fase di migrazione della loro infrastruttura di rete utilizzando i servizi resi disponibili dalla nuova gara di connettività SPC.

Azioni previste/eseguite: il Comune di San Sperate valuterà la possibilità di utilizzare i servizi resi disponibili dalla nuova gara di connettività SPC.

Capitolo 7 – Sicurezza informatica

Sicurezza informatica

Scenario

L'evoluzione delle moderne tecnologie e la conseguente possibilità di ottimizzare lo svolgimento dei procedimenti amministrativi con l'obiettivo di rendere efficace, efficiente e più economica l'azione amministrativa, ha reso sempre più necessaria la "migrazione" verso il digitale che, però, al contempo, sta portando alla luce nuovi rischi, esponendo imprese e servizi pubblici a possibili attacchi cyber. In quest'ottica, la sicurezza e la resilienza delle reti e dei sistemi, su cui tali tecnologie poggiano, sono il baluardo necessario a garantire, nell'immediato, la sicurezza del Paese e, in prospettiva, lo sviluppo e il benessere dello Stato e dei cittadini. La recente riforma dell'architettura nazionale cyber, attuata attraverso l'adozione del decreto-legge 14 giugno 2021, n. 82 che ha istituito l'Agenzia per la Cybersicurezza Nazionale (ACN), ha come obiettivo, tra gli altri, quello di sviluppare e rafforzare le capacità cyber nazionali, garantendo l'unicità istituzionale di indirizzo e azione, anche mediante la redazione e l'implementazione della Strategia nazionale di cybersicurezza, che considera cruciale, per il corretto "funzionamento" del sistema Paese, la sicurezza dell'ecosistema digitale alla base dei servizi erogati dalla Pubblica Amministrazione, con specifica attenzione ai beni ICT. Tali beni supportano le funzioni e i servizi essenziali dello Stato e, purtroppo, come dimostrano gli ultimi rapporti di settore, sono tra i bersagli preferiti degli attacchi cyber.

Per garantire lo sviluppo e il rafforzamento delle capacità cyber nazionali, con il Piano Nazionale di Ripresa e Resilienza e con i Fondi per l'attuazione e la gestione della Strategia nazionale di cybersicurezza sono state destinate significative risorse alla sicurezza cibernetica e alle misure tese a realizzare un percorso di miglioramento della postura di sicurezza del sistema Paese nel suo insieme e, in particolare, della Pubblica Amministrazione. Gli obiettivi e i risultati attesi, definiti successivamente nel presente capitolo, sono in linea con specifici interventi realizzati dall'ACN in favore delle pubbliche amministrazioni per cui sono state individuate specifiche aree di miglioramento. In particolare, il riferimento è alla necessità di:

- prevedere dei modelli di gestione centralizzati della cybersicurezza, coerentemente con il ruolo trasversale associato (obiettivo 7.1 di questo Piano);
- definire processi di gestione e mitigazione del rischio cyber, sia interni sia legati alla gestione delle terze parti di processi IT (obiettivi 7.2, 7.3, 7.4);
- promuovere attività legate al miglioramento della cultura cyber delle amministrazioni (obiettivo 7.5).

All'interno di questo contesto, anche AGID collaborerà mettendo a disposizione della Pubblica Amministrazione una serie di piattaforme e di servizi, che verranno erogati tramite il proprio

CERT, finalizzati alla conoscenza e al contrasto dei rischi cyber legati al patrimonio ICT della PA (obiettivo 7.6)

Contesto normativo

Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82, “Codice dell’amministrazione digitale”, articolo 51
- Decreto del Presidente del Consiglio dei ministri 17 febbraio 2017, “Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali”
- Decreto Legislativo 18 maggio 2018, n. 65, “Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione”
- Decreto del Presidente del Consiglio dei ministri 8 agosto 2019, “Disposizioni sull’organizzazione e il funzionamento del computer security incident response team - CSIRT italiano”
- Decreto-legge 21 settembre 2019, n. 105, “Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica”
- Decreto-legge 19 luglio 2020, n. 76, “Misure urgenti per la semplificazione e l’innovazione digitale”
- Decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, “Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all’articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misura volte a garantire elevati livelli di sicurezza”;
- Decreto-legge 14 giugno 2021 n. 82, “Disposizioni urgenti in materia di cybersicurezza, definizione dell’architettura nazionale di cybersicurezza e istituzione dell’Agenzia per la Cybersicurezza Nazionale”;
- Decreto legislativo 8 novembre 2021 n. 207, “Attuazione della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche (rifusione)”;
- Decreto-legge 21 marzo 2022 n. 21, “Misure urgenti per contrastare gli effetti economici e umanitari della crisi Ucraina”, articoli 27, 28 e 29;
- Decreto del Presidente del Consiglio dei ministri 17 maggio 2022, Adozione della Strategia nazionale di cybersicurezza 2022-2026 e del relativo Piano di implementazione 2022-2026;
- Misure minime di sicurezza ICT per le pubbliche amministrazioni, 18 marzo 2017;
- Linee guida sulla sicurezza nel procurement ICT, del mese di aprile 2020;
- Strategia Cloud Italia, adottata a settembre 2021
- Piano Nazionale di Ripresa e Resilienza - Investimento 1.5: “Cybersecurity”;

Riferimenti normativi europei:

- Direttiva 6 luglio 2016 n. 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
- Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»)
- Direttiva 14 dicembre 2022 n. 2022/2555/UE relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (Testo rilevante ai fini del SEE)

Obiettivo 7.1 – Adottare una governance della cybersicurezza diffusa nella PA

Risultati attesi: RA6.2.1 - Rete di connettività

CAP7.PA.01

Le singole PA definiscono il modello unitario, assicurando un coordinamento centralizzato a livello dell'istituzione, di governance della cybersicurezza.

Azioni previste/eseguite: il Comune di San Sperate non rientra nei perimetri del decreto NIS2 e Legge 90/2024, sta seguendo le indicazioni delle Misure minime di sicurezza ICT per le pubbliche amministrazioni secondo l'allegato 2/2017.

CAP7.PA.02

Le PA adottano un modello di governance della cybersicurezza.

Azioni previste/eseguite: il Comune di San Sperate non rientra nei perimetri del decreto NIS2 e Legge 90/2024, sta seguendo le indicazioni delle Misure minime di sicurezza ICT per le pubbliche amministrazioni secondo l'allegato 2/2017.

CAP7.PA.03

Le PA nominano i Responsabili della cybersicurezza e delle loro strutture organizzative di supporto.

Azioni previste/eseguite: il Comune di San Sperate non rientra nei perimetri del decreto NIS2 e Legge 90/2024, sta seguendo le indicazioni delle Misure minime di sicurezza ICT per le pubbliche amministrazioni secondo l'allegato 2/2017. Non è stata ancora nominata nessuna figura di responsabile cybersicurezza.

CAP7.PA.04

Le PA formalizzano i processi e le procedure inerenti alla gestione della cybersicurezza.

Azioni previste/eseguite: il Comune di San Sperate non rientra nei perimetri del decreto NIS2 e Legge 90/2024, sta seguendo le indicazioni delle Misure minime di sicurezza ICT per le pubbliche amministrazioni secondo l'allegato 2/2017.

Obiettivo 7.2 – Gestire i processi di approvvigionamento IT coerentemente con i requisiti di sicurezza definiti

Risultati attesi:

- RA7.2.1 - Definizione del framework documentale a supporto del processo di approvvigionamento IT
- RA7.2.2 - Definizione delle modalità di monitoraggio del processo di approvvigionamento IT

CAP7.PA.05

Le PA definiscono e approvano i requisiti di sicurezza relativi al processo di approvvigionamento IT.

Azioni previste/eseguite: il Comune di San Sperate è in fase di definizione di un modello interno che definisca come l'ente gestisce il ciclo di vita dei contratti ICT in coerenza con le Linee guida AgID sul procurement ICT e il Codice degli Contratti Pubblici.

CAP7.PA.06

Le PA definiscono e promuovono i processi di gestione del rischio sui fornitori e terze parti IT, la contrattualistica per i fornitori e le terze parti IT, comprensive dei requisiti di sicurezza da rispettare.

Azioni previste/eseguite: il Comune di San Sperate è in fase di definizione di un modello interno che definisca come l'ente gestisce il ciclo di vita dei contratti ICT in coerenza con le Linee guida AgID sul procurement ICT e il Codice degli Contratti Pubblici.

CAP7.PA.07

Le PA realizzano le attività di controllo definite nel Piano di audit e verifica verso i fornitori e terze parti IT.

Azioni previste/eseguite: il Comune di San Sperate è in fase di definizione di un modello interno che definisca come l'ente gestisce il ciclo di vita dei contratti ICT in coerenza con le Linee guida AgID sul procurement ICT e il Codice degli Contratti Pubblici.

Obiettivo 7.3 – Gestione e mitigazione del rischio cyber

Risultati attesi:

- RA7.3.1 - Definizione del framework per la gestione del rischio cyber
- RA7.3.2 - Definizione delle modalità di monitoraggio del rischio cyber

CAP7.PA.08

Le PA definiscono e formalizzano il processo di cyber risk management e security by design, coerentemente con gli strumenti messi a disposizione da ACN.

Azioni previste/eseguite: il Comune di San Sperate non rientra nei perimetri del decreto NIS2 e Legge 90/2024, sta seguendo le indicazioni delle Misure minime di sicurezza ICT per le pubbliche amministrazioni secondo l'allegato 2/2017.

CAP7.PA.09

Le PA promuovono il censimento dei dati e servizi della PA, identificandone la rilevanza e quindi le modalità per garantirne la continuità operativa.

Azioni previste/eseguite: il Comune di San Sperate non rientra nei perimetri del decreto NIS2 e Legge 90/2024, sta seguendo le indicazioni delle Misure minime di sicurezza ICT per le pubbliche amministrazioni secondo l'allegato 2/2017.

CAP7.PA.10

Le PA realizzano o acquisiscono gli strumenti atti alla messa in sicurezza dell'integrità, confidenzialità e disponibilità dei servizi e dei dati, come definito dalle relative procedure.

Azioni previste/eseguite: il Comune di San Sperate non rientra nei perimetri del decreto NIS2 e Legge 90/2024, sta seguendo le indicazioni delle Misure minime di sicurezza ICT per le pubbliche amministrazioni secondo l'allegato 2/2017.

CAP7.PA.11

Le PA integrano le attività di monitoraggio del rischio cyber, come definito dal relativo Piano, nelle normali attività di progettazione, analisi, conduzione e dismissione di applicativi e sistemi informativi.

Azioni previste/eseguite: il Comune di San Sperate non rientra nei perimetri del decreto NIS2 e Legge 90/2024, sta seguendo le indicazioni delle Misure minime di sicurezza ICT per le pubbliche amministrazioni secondo l'allegato 2/2017.

Obiettivo 7.4 – Potenziare le modalità di prevenzione e gestione degli incidenti informatici

Risultati attesi:

- RA7.4.1 - Definizione del framework documentale relativo alla gestione degli incidenti
- RA7.4.2 - Definizione delle modalità di verifica e aggiornamento dei piani di risposta agli incidenti

CAP7.PA.12

Le PA definiscono i presidi per la gestione degli eventi di sicurezza, formalizzandone i processi e le procedure.

Azioni previste/eseguite: il Comune di San Sperate non rientra nei perimetri del decreto NIS2 e Legge 90/2024, sta seguendo le indicazioni delle Misure minime di sicurezza ICT per le pubbliche amministrazioni secondo l'allegato 2/2017.

CAP7.PA.13

Le PA formalizzano ruoli, responsabilità e processi, nonché le capacità tecnologiche a supporto della prevenzione e gestione degli incidenti informatici.

Azioni previste/eseguite: il Comune di San Sperate non rientra nei perimetri del decreto NIS2 e Legge 90/2024, sta seguendo le indicazioni delle Misure minime di sicurezza ICT per le pubbliche amministrazioni secondo l'allegato 2/2017.

CAP7.PA.14

Le PA definiscono le modalità di verifica dei Piani di risposta a seguito di incidenti informatici.

Azioni previste/eseguite: il Comune di San Sperate non rientra nei perimetri del decreto NIS2 e Legge 90/2024, sta seguendo le indicazioni delle Misure minime di sicurezza ICT per le pubbliche amministrazioni secondo l'allegato 2/2017.

CAP7.PA.15

Le PA definiscono le modalità di aggiornamento dei Piani di risposta e ripristino a seguito dell'accadimento di incidenti informatici.

Azioni previste/eseguite: il Comune di San Sperate non rientra nei perimetri del decreto NIS2 e Legge 90/2024, sta seguendo le indicazioni delle Misure minime di sicurezza ICT per le pubbliche amministrazioni secondo l'allegato 2/2017.

Obiettivo 7.5 – Implementare attività strutturate di sensibilizzazione cyber del personale

Risultati attesi:

- RA7.5.1 - Definizione dei piani di formazione in ambito cyber
- RA7.5.2 - Adozione di strumenti atti alla formazione in ambito cyber

CAP7.PA.16

Le PA promuovono l'accesso e l'utilizzo di attività strutturate di sensibilizzazione e formazione in ambito cybersicurezza.

Azioni previste/eseguite: il Comune di San Sperate ha promosso attività strutturate di sensibilizzazione e formazione in ambito cybersicurezza nel triennio di riferimento del piano.

CAP7.PA.17

Le PA definiscono piani di formazione inerenti alla cybersecurity, diversificati per ruoli, posizioni organizzative e attività delle risorse dell'organizzazione.

Azioni previste/eseguite: il Comune di San Sperate sta definendo un piano di formazione inerente alla cybersicurezza.

CAP7.PA.18

Le PA realizzano iniziative per verificare e migliorare la consapevolezza del proprio personale.

Azioni previste/eseguite: il Comune di San Sperate sta definendo un piano di formazione e monitoraggio skill acquisite inerente alla cybersicurezza.

Obiettivo 7.6 – Contrastare il rischio cyber attraverso attività di supporto proattivo alla PA

Risultati attesi:

- RA7.6.1 - Distribuzione di Indicatori di Compromissione alle PA
- RA7.6.2 - Fornitura di strumenti funzionali all'esecuzione dei piani di autovalutazione dei sistemi esposti
- RA7.6.3 - Supporto formativo e informativo rivolto alle PA e in particolare agli RTD per l'aumento del livello di consapevolezza delle minacce cyber

CAP7.PA.19

Le PA, di cui all'all'art. 2 comma 2 del CAD, dovranno accreditarsi al CERT-AGID ed aderire al flusso di Indicatori di compromissione (Feed IoC) del CERT-AGID per la protezione della propria Amministrazione da minacce Malware e Phishing

Azioni previste/eseguite: il Comune di San Sperate si è correttamente accreditato al CERT-AGID, come da disposizioni normative.

CAP7.PA.20

Le PA dovranno usufruire degli strumenti per la gestione dei rischi cyber messi a disposizione dal CERTAGID.

Azioni previste/eseguite: il Comune di San Sperate si è correttamente accreditato al CERT-AGID, come da disposizioni normative. L'utilizzo degli strumenti è stato avviato e si attendono i primi risultati per effettuare le proprie analisi interne.

CAP7.PA.21

Le PA, sulla base delle proprie esigenze, partecipano ai corsi di formazione base ed avanzato erogati dal CERT-AGID.

Azioni previste/eseguite: il Comune di San Sperate si è correttamente accreditato al CERT-AGID, come da disposizioni normative. Si stanno programmando i corsi di formazione base e avanzati per il personale tecnico accreditato nella piattaforma.

APPENDICE 1. Definizioni e Acronimi

Per una più semplice fruizione del presente Piano Triennale si assumono valide le seguenti definizioni e acronimi:

- **AgID**: Agenzia per l'Italia Digitale
- **ANPR**: Anagrafe Nazionale Popolazione Residente
- **ANAC**: Autorità nazionale anticorruzione
- **AOO**: Area Organizzativa Omogenea
- **API**: Application Programming Interface
- **APP**: Applicazione Mobile
- **BDNCP**: Banca dati nazionale dei contratti pubblici, istituita presso ANAC
- **CAD**: Codice dell'amministrazione digitale
- **CERT**: Computer Emergency Response Team
- **CITD**: Comitato Interministeriale per la Trasformazione Digitale promuove, indirizza, coordina l'azione del Governo nelle materie dell'innovazione tecnologica, dell'attuazione dell'agenda digitale italiana ed europea, della strategia italiana per la banda ultra-larga, della digitalizzazione delle pubbliche amministrazioni e delle imprese, nonché della trasformazione, crescita e transizione digitale del Paese.
- **eIDAS**: electronic IDentification, Authentication and trust Services – Regolamento europeo per l'identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno
- **GDPR**: General Data Protection Regulation - Regolamento generale sulla protezione dei dati
- **ICT**: Information and Communications Technology
- **IPA**: Indice delle Pubbliche amministrazioni
- **MEPA**: Mercato Elettronico della Pubblica Amministrazione
- **PA**: Pubbliche Amministrazioni
- **PDND**: Piattaforma Digitale Nazionale Dati (PDND) e lo strumento che abilita l'interoperabilità dei sistemi informativi degli Enti e dei Gestori di Servizi Pubblici
- **PIAO**: Piano Integrato di Attività e Organizzazione e un documento unico di programmazione e governance che va a sostituire tutti i programmi che fino al 2022 le Pubbliche Amministrazioni erano tenute a predisporre, tra cui i piani della performance, del lavoro agile (POLA) e dell'anticorruzione
- **PNRR**: Piano Nazionale di Ripresa e Resilienza e il piano nazionale di investimenti finalizzato allo sviluppo sostenibile e al rilancio dell'economia tramite i fondi europei del Next Generation EU
- **RTD**: Responsabile della Transazione al digitale
- **U-RTD**: Ufficio Responsabile della Transazione al digitale
- **SPC**: Sistema Pubblico di Connettività
- **SPID**: Sistema Pubblico di Identità Digitale

APPENDICE 2. Crediti e versioni

Autore:	realizzato dall'istruttore informatico Alberto Mameli.
Supervisione:	verificato dal Responsabile Transizione Digitale Dott.ssa Iride Atzori
Data di realizzazione:	maggio 2026
Versione:	1.0 del 29/05/2026
Revisioni:	nessuna revisione.