Piano Integrato di Attività e Organizzazione

P.I.A.O.

2025-2027

2.2.1 SOTTOSEZIONE DI PROGRAMMAZIONE PERFORMANCE

Piano Triennale per la transizione digitale

Riferimento al Piano Triennale per l'informatica 2022-2024 pubblicato da AGID

Format AGID per la redazione

Allegato 02

Sommario

PARTE I - Componenti strategiche per la trasformazione digitale **4**

Introduzione **4**

Ruolo del Responsabile per la Transizione al Digitale **4**

Contesto Strategico **5**

Obiettivi e spesa complessiva prevista **7**

PARTE I - Componenti strategiche per la trasformazione digitale **11**

CAPITOLO 1 - Organizzazione e gestione del cambiamento **11**

Contesto normativo e strategico 11

Obiettivo 1.2 - Diffusione competenze digitali nel Paese e nella PA 12

Cosa deve fare l'Amministrazione 13

CAPITOLO 2. Il procurement per la trasformazione digitale **14**

PARTE II – Componenti tecnologiche **15**

CAPITOLO 3. Servizi **15**

Contesto normativo e strategico 16

Obiettivo 3.1 - Migliorare la capacità di erogare e-service 17

Obiettivo 3.2 - Migliorare la capacità di generare ed erogare servizi digitali 18

Obiettivo 3.3 - Consolidare l'applicazione delle Linee guida per la formazione, gestione e conservazione documentale 18

Cosa deve fare l'Amministrazione 18

CAPITOLO 4. Piattaforme **21**

Contesto normativo e strategico 22

Obiettivo 4.1 - Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA 25

Cosa deve fare l'Amministrazione 25

CAPITOLO 5. Dati e Intelligenza Artificiale **28**

CAPITOLO 6. Infrastrutture **29**

Contesto normativo e strategico 29

Obiettivi e risultati attesi 31

OB.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) 31

OB.6.2 - Garantire alle amministrazioni la disponibilità della connettività SPC 31

Cosa deve fare l'Amministrazione 32

CAPITOLO 7. Sicurezza informatica **33**

Contesto normativo e strategico 33

Obiettivi e risultati attesi 34
OB.7.3 - Gestione e mitigazione del rischio cyber 34
OB.7.5 - Implementare attività strutturate di sensibilizzazione cyber del personale 35
Cosa deve fare l'Amministrazione 35
APPENDICE 1. Acronimi 37

PARTE I - Componenti strategiche per la trasformazione digitale

Introduzione

Il Comune di Sacile è l'ente locale responsabile dell'amministrazione del territorio della città di Sacile, che è il sesto comune per popolazione nella regione Friuli-Venezia Giulia. La popolazione è di 20.030 abitanti (dato ISTAT al 01.01.202) distribuiti su un territorio di 32,62 km². La struttura amministrativa del Comune dispone di un servizio informatico incaricato di sviluppare e mantenere le reti, i dispositivi, i sistemi e i servizi ICT (Information & Communications Technology) utilizzati dagli uffici comunali, oltre alla gestione dei processi e dei progetti relativi alla digitalizzazione dell'Amministrazione.

Uno degli obiettivi principali del Comune è migliorare costantemente i servizi offerti ai cittadini attraverso l'innovazione tecnologica e la semplificazione burocratica, rendendo così l'interazione con la pubblica amministrazione più efficiente e accessibile.

Ruolo del Responsabile per la Transizione al Digitale

Il Responsabile per la Transizione Digitale (RTD) del Comune di Sacile è anche il Dirigente Segretario Generale (delibera n. 21 del 25.11.2020). Le sue responsabilità sono definite dall'art. 17 del decreto legislativo n. 82/2005. L'ufficio informatico gestisce operativamente tutte le questioni relative alla Transizione Digitale. All'interno del servizio presieduto dall'RTD, ci sono competenze tecniche, organizzative e amministrative che supportano la gestione degli adempimenti normativi. Il Piano Triennale per la Transizione Digitale (PTTD) 2025-2027, parte del Piano Integrativo di Attività e Organizzazione 2025-2027, segue il modello del Piano Triennale per l'Informatica (PTI) 2024-2026 dell'Agenzia per l'Italia Digitale (AgID).

Oltre a quanto sopra, il RTD ha il compito di promuovere e coordinare l'adozione di soluzioni digitali all'interno del Comune, garantendo l'interoperabilità tra i sistemi e la sicurezza delle informazioni trattate. Le attività dell'ufficio informatico includono la gestione dei progetti di digitalizzazione, l'implementazione di nuove tecnologie, e la formazione del personale comunale sull'uso degli strumenti digitali.

Il PTTD include iniziative specifiche per migliorare l'accesso ai servizi online da parte dei cittadini, come l'integrazione con il Sistema Pubblico di Identità Digitale (SPID), il potenziamento della piattaforma PagoPA per i pagamenti elettronici, e lo sviluppo di applicazioni mobile per facilitare l'interazione con i servizi comunali. Inoltre, il piano prevede azioni per l'aggiornamento infrastrutturale, come il miglioramento della connettività Internet nelle sedi comunali e l'adozione di soluzioni cloud per una maggiore efficienza operativa.

Al fine di monitorare e valutare i progressi della transizione digitale, vengono istituiti periodici report di avanzamento e incontri di verifica con tutti gli stakeholder coinvolti. Questo assicura che le strategie adottate siano in linea con gli obiettivi prefissati e consentono di apportare eventuali correttivi in corso d'opera.

Contesto Strategico

Il Responsabile per la Transizione Digitale (RTD), con il supporto dell'ufficio informatico, rappresenta la struttura amministrativa incaricata della pianificazione, acquisizione, sviluppo e mantenimento dei sistemi informativi e delle risorse informatiche distribuite presso tutte le sedi dove è presente personale dell'ente, oltre che delle infrastrutture di rete per la trasmissione dati e delle reti telefoniche fisse e mobili attualmente in uso.

Negli ultimi cinque anni è stato avviato un significativo processo di rinnovamento, tutt'ora in corso. Sono stati introdotti nuovi strumenti informatici, che hanno apportato miglioramenti in termini di efficienza e benefici, ma è ancora necessario investire sulla cultura, sulle motivazioni e sulla formazione digitale del personale. Inoltre, è indispensabile proseguire negli investimenti per completare la rete in fibra ottica che connette gli edifici comunali e scolastici.

Il Comune di Sacile dispone da tempo di una propria rete in fibra ottica, ma ad oggi essa non raggiunge ancora alcuni edifici comunali ed i plessi scolastici di competenza. È fondamentale, anche grazie alla collaborazione con la Regione Autonoma Friuli-Venezia Giulia, estendere questa connessione a tutti gli edifici e plessi scolastici attualmente esclusi. La connettività di rete veloce, sfruttando i servizi di connettività e sicurezza informatica già presenti nella sede municipale, costituisce un fattore abilitante. Senza reti di interconnessione in fibra ottica, risultano scarsamente applicabili le economie di scala su

connettività veloce, servizi di sicurezza informatica, servizi telefonici evoluti e attivazione di servizi cloud.

Attualmente, una parte significativa del territorio del Comune di Sacile non è coperta dagli operatori privati che offrono connettività in fibra fino all'abitazione (FTTH). Il Comune deve quindi compensare questa mancanza almeno per le sedi di sua competenza. Dopo essersi dotato di connettività Internet in fibra ottica ad alta velocità (1 Gbit/s simmetrico) e diverse tecnologie di backup, il Comune ha completato la migrazione al cloud, utilizzando provider certificati da AgID per la maggior parte dei servizi precedentemente gestiti in datacenter locali.

In risposta alle esigenze emerse dal nuovo contesto sociale ed economico creatosi a seguito della pandemia COVID-19, e per offrire servizi di qualità a cittadini ed imprese in modo semplice, efficiente e sicuro, il Comune di Sacile ha investito in dotazioni tecnologiche che consentono, per quanto possibile, il lavoro da remoto. Inoltre, ha intrapreso iniziative per permettere ai cittadini di comunicare con il Comune attraverso il sito web dedicato. L'obiettivo, ancora da completare, è garantire al cittadino un accesso completo alle istanze di parte tramite il sito web comunale.

Per affrontare il problema della sicurezza informatica, è stata implementata una strategia di cybersecurity che include il monitoraggio continuo delle minacce, l'adozione di soluzioni avanzate di protezione dei dati e la formazione del personale su pratiche di sicurezza. Questo è stato reso possibile grazie al progetto "Cybersecurity FVG – Training & Awareness", finanziato dal PNRR e organizzato dalla Regione Friuli-Venezia Giulia.

Infine, per accompagnare i processi di innovazione e transizione digitale in una società dove la padronanza delle tecnologie ICT sarà sempre più importante, l'Amministrazione ha attivato una serie di attività formative indirizzate sia ai dipendenti, tramite percorsi di formazione i cui contenuti rispettano il cosiddetto "Syllabus" delle Competenze Digitali, sia tramite il progetto finanziato dal PNRR organizzato dalla Regione FVG Cybersecurity FVG – Training & Awareness.

Il comune di Sacile ha partecipato ai progetti finanziati dagli Avvisi PNRR del Dipartimento per la Trasformazione Digitale (DTD):

- **Misura 1.4.1** ESPERIENZA DEL CITTADINO NEI SERVIZI PUBBLICI - COMUNI (APRILE 2022)" - M1C1 PNRR Investimento 1.4 "SERVIZI E CITTADINANZA DIGITALE" – PROGETTO REALIZZATO IN ATTESA DI VERIFICA
- **Misura 1.4.5** 'Piattaforma Notifiche Digitali" Comuni (Settembre 2022)" - PNRR M1C1 Investimento 1.4 "SERVIZI E CITTADINANZA DIGITALE" – PROGETTO REALIZZATO e VERIFICATO
- **Misura 1.3.1**. "Piattaforma Digitale Nazionale Dati - COMUNI (OTTOBRE 2022)" - PNRR M1C1 Investimento 1.3 "DATI E INTEROPERABILITÀ" – PROGETTO REALIZZATO e VERIFICATO
- Missione 1 - Componente 1 - Asse 1 - **Misura 1.7.2** "Rete dei servizi di facilitazione digitale"
- **Misura 1.4.4**- Estensione dell'utilizzo dell'anagrafe nazionale digitale (ANPR) - Adesione
  allo Stato Civile digitale (ANSC) - COMUNI (LUGLIO 2024)
- **Investimento 1.2** ABILITAZIONE AL CLOUD PER LE PA LOCALI COMUNI (SETTEMBRE 2024)'

Questi progetti mirano a migliorare la digitalizzazione dell'ente e dei servizi offerti ai cittadini.

Obiettivi e spesa complessiva prevista

Gli obiettivi generali che l'Amministrazione persegue in materia di digitalizzazione sono conformi ai principi guida stabiliti dal Piano Triennale di AgID, con particolare attenzione ai seguenti punti:

Principi guida	**Definizioni**	**Riferimenti normativi**
1. Digitale e mobile come prima opzione (*digital & mobile first*)	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*"	Art.3-bis Legge 241/1990 Art.1 c.1 lett. a) D.Lgs. 165/2001 Art.15 CAD Art.1 c.1 lett. b) Legge 124/2015 Art.6 c.1 DL 80/2021

Principi guida	Definizioni	Riferimenti normativi
2. cloud come prima opzione (*cloud first*)	le pubbliche amministrazioni, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano il paradigma cloud e utilizzano esclusivamente infrastrutture digitali adeguate e servizi *cloud* qualificati secondo i criteri fissati da ACN e nel quadro del SPC	Art.33-septies Legge 179/2012 Art. 73 CAD
3. interoperabile *by design* e *by default* (*API-first*)	i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e attraverso processi digitali collettivi, esponendo opportuni *e-Service*, a prescindere dai canali di erogazione del servizio che sono individuati logicamente e cronologicamente dopo la progettazione dell'interfaccia API;	Art.43 c.2 dPR 445/2000 Art.2 c.1 lett.c) D.Lgs 165/2001 Art.50 c2, art.50-ter e art.64-bis c.1-bis CAD
4. accesso esclusivo mediante identità digitale (*digital identity only*)	le pubbliche amministrazioni devono adottare in via esclusiva sistemi di identità digitale definiti dalla normativa	Art.64 CAD Art. 24, c.4, DL 76/2020 Regolamento EU 2014/910 "eIDAS"
5. servizi inclusivi, accessibili e centrati sull'utente (*user-centric*)	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	Legge 4/2004 Art.2 c.1, art.7 e art.53 CAD Art.8 c.1 lettera c) e lett.e), ed art.14 c.4-bis D.Lgs 150/2009
6. 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	Art.50 c.1 e c,2-bis, art.50-quater e art.52 c.2 CAD D.Lgs 36/2006 Art.24-quater c.2 DL90/2014
7. concepito per la sicurezza e la protezione dei dati personali (*data protection by design e by default*)	i servizi pubblici devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali	Regolamento EU 2016/679 "GDPR" DL 65/2018 "NIS" DL 105/2019 "PNSC" DL 82/2021 "ACN"
8. *once only* e concepito come 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	Art.43, art.59, art.64 e art.72 DPR 445/2000 Art.15 c.3, art.41, art.50 c.2 e c.2-ter, e art.60 CAD Regolamento EU 2018/1724 "*single digital gateway*" Com.EU (2017) 134 "EIF"
9. apertura come prima opzione (*openness*)	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	Art.9, art.17 c.1 ed art.68-69 CAD Art.1 c.1 D.Lgs 33/2013 Art.30 D.Lgs 36/2023

Principi guida	Definizioni	Riferimenti normativi
10. 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	Art.15 c.2-bis CAD Art.21 D.lgs. 36/2023 Regolamento EU 2020/852 "principio DNSH"
11. 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.	Art.5, 117 e 118 Costituzione Art.14 CAD

Il monitoraggio delle spese relative all'anno 2024 è il seguente:

- Spesa corrente annua per acquisto o mantenimento di servizi informatici: Euro **45.972,12**
- Spesa corrente annua per noleggio di trasmissione dati e telefonia IP: Euro **27.500,00**
- Spesa in conto capitale annua per acquisto di tecnologie ICT: Euro **53.766,47**

La spesa per lo sviluppo ed il mantenimento delle tecnologie ICT nel corso del triennio 2025-2027 è suddivisa nelle seguenti macro-voci:

Previsione 2025:

- Spesa corrente annua per acquisto o mantenimento di servizi informatici: Euro **47.980,31**
- Spesa corrente annua per noleggio di trasmissione dati e telefonia IP: Euro **32.900,00**
- Spesa in conto capitale annua per acquisto di tecnologie ICT: Euro **8.500,00**

Previsione 2026:

- Spesa corrente annua per acquisto o mantenimento di servizi informatici: Euro **49.080,31**
- Spesa corrente annua per noleggio di trasmissione dati e telefonia IP: Euro **32.900,00**
- Spesa in conto capitale annua per acquisto di tecnologie ICT: Euro **9.000,00**

Previsione 2027:

- Spesa corrente annua per acquisto o mantenimento di servizi informatici: Euro **49.080,31**
- Spesa corrente annua per noleggio di trasmissione dati e telefonia IP: Euro **32.900,00**
- Spesa in conto capitale annua per acquisto di tecnologie ICT: Euro **9.000,00**

(fonte: Bilancio 2025-2027 del Comune di Sacile)

PARTE I - Componenti strategiche per la trasformazione digitale

CAPITOLO 1 - Organizzazione e gestione del cambiamento

La trasformazione digitale richiede un processo integrato, finalizzato alla costruzione di ecosistemi digitali strutturati sostenuti da organizzazioni pubbliche che mirano alla semplicità, e che sono trasparenti, aperte, digitalizzate e con servizi di qualità, erogati in maniera proattiva per anticipare le esigenze del cittadino.

È quindi necessario seguire un approccio innovativo che affronti, in maniera sistematica, tutti gli aspetti legati a organizzazione, processi, regole, dati e tecnologie. Sono quindi necessari strumenti utili alla mappatura di tali aspetti ed è necessario agevolare lo scambio di buone pratiche, rendendo tutti gli operatori pubblici sviluppatori dell'innovazione amministrativa, attraverso la diffusione di una cultura amministrativa digitale.

L'art. 6 del Decreto-legge n. 80/2021 introduce il Piano Integrato di Attività e Organizzazione (PIAO) al fine di "*assicurare la qualità e la trasparenza dell'attività amministrativa e migliorare la qualità dei servizi ai cittadini e alle imprese e procedere alla costante e progressiva semplificazione e reingegnerizzazione dei processi* (..)", ma sono molteplici le fonti normative che richiamano le amministrazioni a quella che il CAD definisce, all'art.15, come una "*riorganizzazione strutturale e gestionale*", finalizzata allo sfruttamento delle opportunità offerte dal digitale.

Nonostante gran parte dell'attività delle pubbliche amministrazioni sia già composta da procedimenti e procedure ben definite, non vuol dire che questa non possa essere reingegnerizzata sia da un punto di vista della semplificazione sia da un punto di vista della digitalizzazione.

Occorre che ogni singolo ente pubblico divenga un "ecosistema amministrativo digitale", alla cui base ci siano piattaforme organizzative e tecnologiche, ma in cui il valore pubblico sia generato in maniera attiva da cittadini, imprese e operatori pubblici.

Essendo l'azione amministrativa composta da processi collettivi è necessario introdurre dei "processi digitali collettivi" basati su *e-service,* ovvero interfacce API che scambiano dati/informazioni in maniera automatica e interoperabile.

Questo permette la realizzazione del principio *once-only* e, al tempo stesso, consente agli attori pubblici e privati di generare valore all'interno dell'ecosistema con al centro la singola Pubblica Amministrazione, che lo regola garantendo correttezza amministrativa, trasparenza, apertura, sicurezza informatica e protezione dei dati personali.

Contesto normativo e strategico

Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (in breve CAD) art. 17.

- Circolare n. 3 del 1° ottobre 2018 del Ministro per la Pubblica Amministrazione sul Responsabile per la transizione al digitale.

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

- RA1.2.2 - Diffusione competenze digitali di base nella PA
    - Monitoraggio 2024 - Partecipazione di almeno 40 dipendenti comunali a iniziative di miglioramento del livello di competenze e di riqualificazione in ambito digitale
    - Target 2025 - Partecipazione di almeno 60 dipendenti comunali a iniziative di miglioramento del livello di competenze e di riqualificazione in ambito digitale
    - Target 2026 - Partecipazione di almeno 80 dipendenti comunali a iniziative di miglioramento del livello di competenze e di riqualificazione in ambito digitale
    - Target 2027 - Partecipazione di almeno 100 dipendenti comunali a iniziative di miglioramento del livello di competenze e di riqualificazione in ambito digitale

- RA1.2.3 - Diffusione delle competenze specialistiche ICT
    - Monitoraggio 2024 – formazione continua su diversi temi specialistici IT del personale impiegato nell'ufficio sistemi informativi (3 persone)
    - Target 2025 – formazione continua su diversi temi specialistici del personale impiegato nell'ufficio sistemi informativi aumentando le occasioni formative per rendere quanto più possibile il personale intercambiabile

Cosa deve fare l'Amministrazione

Sono riportate di seguito le Linee d'Azione che declinano gli obiettivi del Piano Triennale 2024-2026 di AgID con riferimento al raggiungimento degli obiettivi definiti al paragrafo precedente.

OB 1.2 - Diffusione competenze digitali nel Paese e nella PA

Formazione continua del personale su temi relativi al mondo digitale, alla sicurezza informatica ed al potenziamento delle competenze digitali

Attività Operative: Il comune promuove a tutti gli operatori dei percorsi formativi per potenziare le competenze digitali ed approfondire i temi sulla sicurezza informatica. Il comune di Sacile ha aderito all'iniziativa "Syllabus per la formazione digitale" ed ha promosso 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

Deadline: dicembre 2026

Strutture responsabili: Sistemi Informativi

Capitolo di spesa/fonti di finanziamento: risorse finanziarie proprie

CAPITOLO 2. Il procurement per la trasformazione digitale

Per questo capitolo del Piano Triennale per l'Informatica 2025-2027 del Comune di Sacile non sono previste Linee d'Azione che declinano obiettivi individuali derivanti dal Piano Triennale per l'Informatica 2024-2026 di AgID, se non quello di utilizzare le piattaforme di procurement messe a disposizione a livello nazionale (Es: acquistinretepa.it di CONSIP) o regionale (eAppalti FVG).

PARTE II – Componenti tecnologiche

CAPITOLO 3. Servizi

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 essere considerata come una soluzione agile e scalabile, che permette di standardizzare i processi digitali e di facilitare il processo di change management nelle organizzazioni governative locali.

Per garantire la possibilità a tutti gli Enti di cogliere questa 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 non solo un intervento tecnologico ma anche un controllo per la gestione del cambiamento, che coinvolge diverse fasi chiave quali la formazione continua, il coinvolgimento attivo degli stakeholder, il monitoraggio dell'impatto del cambiamento e una comunicazione efficace.

Per gli enti locali 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. Questo approccio consente di colmare il gap informativo interno e di risparmiare tempo e 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) il layer focale per la condivisione di dati e processi.

La sostenibilità e la crescita collaborativa nell'ambito dell'architettura a microservizi non si limitano al singolo ente locale. In molte situazioni, altre istituzioni come Regioni, Unioni o Enti capofila (HUB tecnologici) possono svolgere 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 il processo di digitalizzazione.

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.

Contesto normativo e strategico

In materia di qualità dei servizi pubblici digitali esistono una serie di riferimenti normativi e strategici cui le amministrazioni devono attenersi. Di seguito un elenco delle principali fonti.

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

- RA3.1.2 - Aumento del numero di Richieste di Fruizione Autorizzate su PDND
    - **Monitoraggio 2024** – Il comune interopera attraverso richieste di Fruizione

Autorizzate su PDND
- **Target 2025** – Il 40% dei servizi interoperato attraverso delle Richieste di Fruizione Autorizzate su PDND
- **Target 2026** - Il 100% dei servizi interoperato attraverso delle Richieste di Fruizione Autorizzate su PDND

Obiettivo 3.2 - Migliorare la capacità di generare ed erogare servizi digitali

- RA3.2.2 - Incremento dell'accessibilità dei servizi digitali
  - **Monitoraggio 2024** – Il comune di Sacile pubblica e aggiorna la dichiarazione di accessibilità dei propri siti istituzionali registrati su IndicePA
  - **Target 2025** – Il comune di Sacile pubblica e aggiorna la dichiarazione di accessibilità dei propri siti istituzionali registrati su IndicePA
  - **Target 2026** – Il comune di Sacile pubblica e aggiorna la dichiarazione di accessibilità dei propri siti istituzionali registrati su IndicePA

- RA3.2.3 - Incremento e diffusione dei modelli standard di siti e servizi digitali, disponibili in Designers Italia
  - **Monitoraggio 2024** – Il comune di Sacile adotta i modelli standard di siti e servizi digitali disponibili nel sito internet comunale
  - **Target 2025** - Il comune di Sacile adotta i modelli standard di siti e servizi digitali disponibili nel sito internet comunale ed in tutti i siti collegati alla attività comunale

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

- RA3.3.1 - Monitorare l'attuazione delle linee guida
  - **Target 2025** – Il comune di Sacile adotta e pubblica 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 in "Amministrazione trasparente"
  - **Target 2026** - Il comune di Sacile adotta e pubblica il manuale di conservazione e la nomina del Responsabile della conservazione in "Amministrazione trasparente"

Cosa deve fare l'Amministrazione

Sono riportate di seguito le Linee d'Azione che declinano gli obiettivi del Piano Triennale 2024-2026 di AgID con riferimento al raggiungimento degli obiettivi definiti al paragrafo precedente.

OB 3.1 - Migliorare la capacità di erogare e-service

Aumento del numero di Richieste di Fruizione Autorizzate su PDND

Attività Operative: Il comune di Sacile ha completato il progetto PNRR 1.3.1 per integrarsi alla piattaforma PDND. Eseguito questo passaggio preliminare chiede ai fornitori delle applicazioni, che ad oggi utilizza, di interoperare con le altre amministrazioni pubbliche attraverso le API pubblicate nella piattaforma nazionale PDND

Deadline: dicembre 2026

Strutture responsabili: Area sistemi informativi ed innovazione digitale

Capitolo di spesa/fonti di finanziamento: risorse finanziarie proprie.

OB 3.2 - Migliorare la capacità di generare ed erogare servizi digitali

Formazione continua del personale su temi relativi al mondo digitale, alla sicurezza informatica ed al potenziamento delle competenze digitali

Attività Operative: Il comune di Sacile ha attivato Web Analytics Italia per la rilevazione delle statistiche di utilizzo del proprio sito web istituzionale presente su IndicePA, pubblica regolarmente gli obiettivi di accessibilità e la dichiarazione di accessibilità sul proprio sito web.

A partire dall'anno 2025 effettuerà i effettua un test automatico di accessibilità sul proprio sito istituzionale indicato su https://indicepa.gov.it/ipa-portale/, utilizzando la piattaforma Mauve++

Deadline: dicembre 2026

Strutture responsabili: Sistemi Informativi

Capitolo di spesa/fonti di finanziamento: risorse finanziarie proprie.

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

Monitorare l'attuazione delle linee guida relative alla gestione documentale

Attività Operative: Il comune di Sacile ha adottato e monitora le linee guida sulla formazione, gestione e conservazione dei documenti informatici in vigore. Le amministrazioni devono seguire queste linee guida oltre alla normativa esistente.

Il comune di Sacile pubblicherà su "Amministrazione trasparente" entro giugno 2025 una versione aggiornata del manuale di gestione documentale, la nomina del responsabile della gestione documentale per ogni AOO, e il coordinatore della gestione documentale.

Il comune di Sacile pubblicherà su "Amministrazione trasparente" entro giugno 2026 - il manuale di conservazione e la nomina del responsabile della conservazione.

Deadline: dicembre 2026

Strutture responsabili: Sistemi Informativi

Capitolo di spesa/fonti di finanziamento: risorse finanziarie proprie.

CAPITOLO 4. Piattaforme

La maturità raggiunta da alcune piattaforme, già presentate nelle precedenti edizioni del Piano, consente ora di concentrarsi sui servizi che esse offrono a cittadini, imprese e altre amministrazioni, in continuità con quanto descritto nel capitolo precedente “Servizi”.

L'obiettivo comune di tutte queste piattaforme è quello di migliorare i servizi già erogati, come verrà dettagliato nei risultati attesi e nelle linee di azione. In questa sezione, la descrizione di ciascuna piattaforma riporterà tale obiettivo, mentre gli altri elementi descrittivi saranno specifici della piattaforma esaminata. Nella seconda parte di questo capitolo verranno descritte le piattaforme che attestano attributi e, infine, si parlerà delle basi di dati di interesse nazionale.

pagoPA

pagoPA è una piattaforma che permette ai cittadini di pagare la Pubblica Amministrazione in modo rapido e intuitivo. Offre vari metodi di pagamento elettronici per soddisfare diverse esigenze. Gli enti pubblici possono integrarsi con diversi attori del mercato e adottare soluzioni innovative per la riscossione. L'obiettivo di pagoPA è rendere i pagamenti dei servizi pubblici più efficienti e semplici, riducendo l'uso del contante.

AppIO

L'app IO è un progetto open source che offre un unico canale per tutti i servizi pubblici digitali, parte della strategia del Governo italiano per la cittadinanza digitale. La sua visione è facilitare l'interazione dei cittadini con la Pubblica Amministrazione tramite un'app semplice sullo smartphone. L'app concretizza l'articolo 64 bis del Codice dell'Amministrazione Digitale, creando un punto di accesso unico ai servizi digitali, gestito dalla Presidenza del Consiglio dei Ministri.

SEND

La piattaforma SEND (Servizio Notifiche Digitali) accelera e rende più economico e sicuro l’invio e la ricezione delle notifiche legali. Permette di ricevere, scaricare documenti notificati e pagare online su SEND o nell'app IO. SEND solleva gli enti dagli adempimenti di gestione delle comunicazioni legali e riduce l’incertezza della reperibilità del destinatario.

SPID

L'identità digitale SPID rappresenta una soluzione per accedere ai servizi online della Pubblica Amministrazione tramite un'unica identità digitale. Grazie a credenziali articolate su tre livelli di sicurezza, consente l'accesso ai servizi fornendo dati identificativi certificati.

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.

SUAP e SUE

Gli Sportelli Unici per le Attività Produttive (SUAP) e per l'Edilizia (SUE) sono fondamentali nella Pubblica Amministrazione, fungendo da punto di contatto tra imprese, professionisti, cittadini e istituzioni. Facilitano gli adempimenti per attività produttive ed edilizie, e sono essenziali in un contesto che richiede digitalizzazione per migliorare la competitività e accelerare i processi amministrativi. La semplificazione diventa così cruciale per rendere accessibili a tutti le opportunità digitali.

Contesto normativo e strategico

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. 64- 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 e 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” (2021)
- 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

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

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

- RA4.1.1 - Incremento dei servizi sulla piattaforma pagoPA
  - **Monitoraggio 2024**– Ricevuti 4607 pagamenti attraverso il canale pagoPA
  - **Target 2025 –** Incremento dei servizi pagabili con pagoPA per superare i 5000 pagamenti nell'anno
  - **Target 2026** – Incremento dei servizi pagabili con pagoPA per superare i 6000 pagamenti nell'anno
- RA4.1.2 - Incremento dei servizi sulla Piattaforma IO (l'App dei servizi pubblici)
  - **Monitoraggio 2024 -** Attivati 15 nuovi servizi del comune di Sacile nell'App IO
  - **Target 2025 -** Incremento di ulteriori 5 servizi nell'App IO
  - **Target 2026** Incremento di ulteriori 5 servizi nell'App IO
- RA4.1.3 - Incremento degli enti che usano SEND
  - **Monitoraggio 2024** – Adesione alla piattaforma ed invio delle prime notifiche
  - **Target 2025** – Invio dei primi 100 atti di notifica attraverso SEND
  - **Target 2026** – Invio di tutti gli atti prodotti dal comune attraverso SEND
- RA4.1.4 - Incremento dell'adozione e dell'utilizzo di SPID e CIE da parte delle Pubbliche Amministrazioni
  - **Monitoraggio 2024 -** Il Comune utilizza SPID e CIE nel sito istituzionale
  - **Target 2025 –** Incremento del numero di autenticazioni CIE e SPID
  - **Target 2026 -** Incremento del numero di autenticazioni CIE del 50% rispetto alla *baseline*

Cosa deve fare l'Amministrazione

Sono riportate di seguito le Linee d'Azione che declinano gli obiettivi del Piano Triennale 2024-2026 di AgID con riferimento al raggiungimento degli obiettivi definiti al paragrafo precedente.

OB. 4.1 - Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA

Incremento dei servizi sulla piattaforma pagoPA

Attività Operative: Attivazione del servizio di pagamento PagoPA per tutti quei servizi residuali che ancora non sono stati attivati

Deadline: dicembre 2025

Strutture responsabili: Area sistemi informativi ed innovazione digitale, Servizio Tributi e Servizio Urbanistica;

Capitolo di spesa/fonti di finanziamento: nessuna risorsa finanziaria richiesta.

Incremento dei servizi sulla Piattaforma IO (l'App dei servizi pubblici)

Attività Operative: Integrare ed attivare i software in uso al comune, sollecitando i fornitori degli stessi, per comunicare al cittadino attraverso l'app IO

Deadline: dicembre 2026

Strutture responsabili: Sistemi Informativi

Capitolo di spesa/fonti di finanziamento: nessuna risorsa finanziaria richiesta.

Attivazione ed utilizzo della Piattaforma Notifiche Digitali (SEND)

Attività Operative: Integrare i software in uso presso il comune di Sacile, sollecitando i fornitori degli stessi, alla piattaforma delle notifiche digitali. Utilizzarla attivamente per i principali fruitori: la Polizia Locale e il Servizio Tributi

Deadline: dicembre 2026

Strutture responsabili: Area sistemi informativi ed innovazione digitale. Servizio Polizia Locale. Servizio Tributi

Capitolo di spesa/fonti di finanziamento: nessuna risorsa finanziaria richiesta.

Utilizzo in tutti i siti comunali dell'Identità digitale (SPID e CIE)

Attività Operative: Adeguare tutti i siti del comune ai modelli più recenti presentati in Designer Italia; Promuovere azioni di sensibilizzazione presso la popolazione per incentivare l'utilizzo di SPID e CIE per l'accesso ai servizi online offerti dai siti comunali e della pubblica amministrazione.

Deadline: dicembre 2025

Strutture responsabili: Sistemi Informativi

Capitolo di spesa/fonti di finanziamento: nessuna risorsa finanziaria richiesta

CAPITOLO 5. Dati e Intelligenza Artificiale

Per questo capitolo del Piano Triennale per l'Informatica 2025-2027 del Comune di Sacile non sono previste Linee d'Azione che declinano obiettivi derivanti dal Piano Triennale per l'Informatica 2024-2026 di AgID.

CAPITOLO 6. Infrastrutture

La strategia "Cloud Italia", pubblicata a settembre 2021, è un'opportunità per riorganizzare le pubbliche amministrazioni. Non riguarda solo la tecnologia, ma ogni ente deve esplorarne a fondo le opportunità.

La Strategia Cloud affronta tre sfide: l'autonomia tecnologica, il controllo sui dati e la resilienza dei servizi digitali. Supporta le PA nella migrazione verso un ambiente cloud sicuro, in linea con gli obiettivi del PNRR e con il principio cloud first, che promuove l'adozione prioritaria delle tecnologie cloud.

Ogni nuova iniziativa deve considerare prima il cloud rispetto ad altre tecnologie. Se il cloud non viene adottato, la decisione deve essere giustificata. L'adozione del cloud è essenziale per la trasformazione digitale, migliorando l'erogazione dei servizi della PA.

L'attuazione dell'art.33-septies del Decreto-legge n.179 del 2012 è un'occasione per modernizzare gli applicativi e migliorare i servizi verso cittadini, professionisti e imprese.

Il datacenter del Comune di Sacile è stato classificato in categoria B e quindi soggetto obbligato ad attuare percorsi di dismissione dei servizi informatici erogati "on premise" (cioè in via diretta tramite proprie infrastrutture), migrando gli stessi presso datacenter più sicuri certificati da AgID ed ACN ed implementando quindi scenari di esternalizzazione denominati "SaaS" (Software as a Service). Le Amministrazioni che attueranno questo percorso di migrazione possono avvalersi dei finanziamenti previsti nell'apposito Avviso PNRR che consente di allinearsi ai principi del "cloud first" e della "sicurezza e privacy by default" richiamati nel Piano Triennale.

Per realizzare un’adeguata evoluzione tecnologica e supportare il paradigma cloud è indispensabile investire in servizi di connettività affidabili, veloci, ridondanti e sicuri. Per questo il Comune di Sacile si vede impegnato con priorità a potenziare la sua rete proprietaria in fibra ottica, per la connessione degli edifici e le reti geografiche regionali o offerte da provider di mercato.

Contesto normativo e strategico

In materia di infrastrutture esistono una serie di riferimenti sia normativi che strategici a cui le amministrazioni devono attenersi. Di seguito un elenco delle principali fonti.

Riferimenti normativi nazionali:

- 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);
- Determinazioni ACN in attuazione al precedente Regolamento n.

306/2022 (con allegato) su e n. 307/2022 (con allegato)

- Decreti direttoriali ACN prot. N. 29 del 2 gennaio 2023, n. 5489 dell'8 febbraio 2023 e n. 20610 del 28 luglio 2023;
- Strategia italiana per la Banda Ultra Larga 2023-2026
- Piano Nazionale di Ripresa e Resilienza:
  - Investimento 1.1: "Infrastrutture digitali"
  - Investimento 1.2: "Abilitazione e facilitazione migrazione al cloud"

Riferimenti 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 Tof the Council on European data governance (Data Governance Act) (2020)

Obiettivi e risultati attesi

Sono richiamati di seguito gli obiettivi e le linee d'azione concernenti la componente tecnologica "Infrastrutture" estratti dal Piano Triennale per l'Informatica 2024-2026 di AgID declinati per il contesto del Comune di Sacile.

OB.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)

- R.A.6.1.1 - **Numero di amministrazioni migrate**
  - Monitoraggio 2024 – Il comune ha avviato la migrazione al cloud nei limiti delle connettività di rete veloce preesistente. Si è dotato di una connettività aggiuntiva veloce ed ha completato la migrazione al cloud dei servizi "core";
  - Target 2025 – Il Comune migra al cloud alcuni servizi applicativi non "core"
  - Target 2026 – Il Comune completa la migrazione al cloud dei servizi applicativi non "core"

OB.6.2 - Garantire alle amministrazioni la disponibilità della connettività SPC

- R.A.6.2.1 - **Disponibilità di servizi di connettività Internet a banda larga e ultra-larga per le PA locali**

- Monitoraggio 2024 – Il Comune proroga le attuali convenzioni CONSIP SPC2 e Telefonia fissa 5 in attesa che le nuove convenzioni SPC per la connettività e la telefonia vengano aggiudicate;
- Target 2025 - Il Comune aderirà alla nuova convenzione SPC di CONSIP per la telefonia fissa e la connettività.

Cosa deve fare l'Amministrazione

Sono riportate di seguito le Linee d'Azione che declinano gli obiettivi del Piano Triennale 2024-2026 di AgID con riferimento al raggiungimento degli obiettivi definiti al paragrafo precedente.

OB.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)

Migrazione al cloud di tutte quelle applicazioni ancora ospitate "on premise"
Attività Operative: Identificare e migrare al cloud le applicazioni che ancora risultano essere ospitate "in locale" in sinergia con quanto attuabile attraverso l'avviso PNRR 1.2 - Migrazione al cloud.

Deadline: dicembre 2026

Strutture responsabili: Sistemi Informativi

Capitolo di spesa/fonti di finanziamento: risorse assegnate dal bando PNRR 1.2 - Migrazione al cloud.

OB.6.2 - Disponibilità di servizi di connettività Internet a banda larga e ultra-larga per le PA locali

Nuove convenzioni CONSIP SPC per la connettività a banda ultralarga e telefonia fissa
Attività Operative: Analisi tecnico-economica delle possibili soluzioni per incrementare banda, velocità e sicurezza di nuovi servizi di connettività Internet ai fini della sua acquisizione tramite CONSIP per le sedi principali e periferiche;

Deadline: dicembre 2025

Strutture responsabili: Sistemi Informativi

Capitolo di spesa/fonti di finanziamento: risorse finanziarie proprie.

CAPITOLO 7. Sicurezza informatica

L'evoluzione delle tecnologie moderne ha reso necessaria la migrazione verso il digitale, esponendo però imprese e servizi pubblici a nuovi rischi di attacchi cyber. La sicurezza e la resilienza delle reti sono essenziali per garantire la protezione del Paese e lo sviluppo futuro.

Con il decreto-legge 14 giugno 2021, n. 82, è stata creata l'Agenzia per la Cybersicurezza Nazionale (ACN) per sviluppare e rafforzare le capacità cyber nazionali, assicurando un'azione istituzionale unitaria e implementando la Strategia nazionale di cybersicurezza. La sicurezza dell'ecosistema digitale è fondamentale per la Pubblica Amministrazione, poiché i beni ICT, che supportano le funzioni essenziali dello Stato, sono spesso bersagli di attacchi cyber.

Il Piano Nazionale di Ripresa e Resilienza e i Fondi per la Strategia nazionale di cybersicurezza prevedono risorse significative per migliorare la sicurezza cibernetica della Pubblica Amministrazione e del sistema Paese nel suo complesso.

Contesto normativo e strategico

In materia di sicurezza informatica esistono una serie di riferimenti normativi e strategici a cui le amministrazioni devono attenersi. Di seguito un elenco delle principali fonti.

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)

Obiettivi e risultati attesi

Sono richiamati di seguito gli obiettivi e le linee d'azione concernenti la componente tecnologica "Infrastrutture" estratti dal Piano Triennale per l'Informatica 2024-2026 di AgID declinati per il contesto del Comune di Sacile.

OB.7.3 - Gestione e mitigazione del rischio cyber

- R.A.7.3.1 - **Definizione del framework per la gestione del rischio cyber**
    - Monitoraggio 2024 – Il comune si è già dotato di un nuovo firewall che persegue il paradigma “Zero Trust”. Il nuovo dispositivo protegge la rete locale del municipio e di tutti gli edifici collegati da una rete in fibra ottica

propria. Il RTD persegue una strategia di protezione operativa reale dotando la rete di strumenti evoluti, dimettendo progressivamente i dispositivi ed i software obsoleti, rinforzando le policy di sicurezza obbligatorie a cui tutti gli operatori si devono attenere e monitorando i punti di vulnerabilità noti.

- Target 2025 – Il Comune attiva un nuovo firewall che persegue il paradigma "Zero Trust" in un secondo sito non connesso alla rete LAN municipale. Il RTD dismette ulteriori dispositivi ed i software obsoleti, rinforza le policy di sicurezza obbligatorie a cui tutti gli operatori si devono attenere e monitora i punti di vulnerabilità noti. Il RTD inoltra a tutti i dipendenti una campagna di sensibilizzazione sui temi della cyber sicurezza.
- Target 2026 –Il RTD persegue iniziative di miglioramento continue che possano eliminare vulnerabilità informatiche e punti di ingresso per eventuali cyber attacchi.. Il RTD coinvolge tutti gli operatori abilitati ad utilizzare dispositivi del comune di Sacile con campagne di formazione e sensibilizzazione sui temi della cyber sicurezza.

OB.7.5 - Implementare attività strutturate di sensibilizzazione cyber del personale

- R.A.7.5.1 - **Definizione dei piani di formazione in ambito cyber**
  - Monitoraggio 2024 – Il comune coinvolto da una iniziativa della regione Friuli Venezia Giulia, ha formato i dipendenti attraverso il corso "Cybersecurity FVG – Training & Awareness" per renderli più consapevoli sui rischi, sulle modalità di attacco e sulla prevenzione di violazioni della sicurezza informatica
  - Target 2025 – Il Comune continua a proporre a tutti i dipendenti e collaboratori i corsi "Cybersecurity FVG – Training & Awareness" visto il successo dell'iniziativa e per mantenere alta la consapevolezza sui temi di cyber sicurezza.

Cosa deve fare l'Amministrazione

Sono riportate di seguito le Linee d'Azione che declinano gli obiettivi del Piano Triennale 2024-2026 di AgID con riferimento al raggiungimento degli obiettivi definiti al paragrafo precedente.

OB.7.3 - Gestione e mitigazione del rischio cyber

Aumento del grado di protezione reale dal rischio cyber

Attività Operative: Il RTD persegue una strategia di protezione operativa reale dotando la rete di strumenti evoluti, dimettendo progressivamente i dispositivi ed i software obsoleti, rinforzando le policy di sicurezza obbligatorie a cui tutti gli operatori si devono attenere e monitorando i punti di vulnerabilità noti.

Deadline: dicembre 2025

Strutture responsabili: Area sistemi informativi ed innovazione digitale

Capitolo di spesa/fonti di finanziamento: risorse finanziarie proprie.

OB.7.5 - Implementare attività strutturate di sensibilizzazione cyber del personale

Formazione continua del personale su temi della cyber sicurezza

Attività Operative: Il RTD persegue una strategia di protezione operativa reale dotando la rete di strumenti evoluti, dimettendo progressivamente i dispositivi ed i software obsoleti, rinforzando le policy di sicurezza obbligatorie a cui tutti gli operatori si devono attenere e monitorando i punti di vulnerabilità noti.

Deadline: dicembre 2025

Strutture responsabili: Sistemi Informativi

Capitolo di spesa/fonti di finanziamento: corsi di formazione promossi ed offerti dalla regione Friuli-Venezia Giulia.

APPENDICE 1. Acronimi

Acronimo	Definizione
ACN	Agenzia per la Cybersicurezza Nazionale
AGID	Agenzia per l'Italia Digitale
ANPR	Anagrafe nazionale popolazione residente
ANSC	Anagrafe Nazionale dello Stato Civile
API	Application Programming Interface
CAD	Codice dell'amministrazione digitale
FTTH	Fiber to the home – Fibra ottica fino alla sede del cliente (punto di consegna in fibra ottica nella abitazione/edificio)
GDPR	General Data Protection Regulation
ICT	Information & Communications Technology
NIS	Network and Information Security
LAN	Local Area Network – Rete informatica locale
PagoPA	Piattaforma per i pagamenti elettronici
PDND	Piattaforma Digitale Nazionale Dati
PNRR	Piano Nazionale di Ripresa e Resilienza
PNSC	Piano Nazionale per la Sicurezza Cibernetica
PTI	Piano Triennale per l'Informatica
PTTD	Piano Triennale per la Transizione Digitale
RTD	Responsabile per la Transizione Digitale
SPID	Sistema Pubblico di Identità Digitale
WAN	Wide Area Network – Rete informatica geografica