

Piano Triennale per l'Informatica

aggiornamento 2024-2026

Approvato con Determinazione del Dirigente dell'Area Amministrativa e Contabile n. 46 del
16.12.2024

Sede Legale Via della Pace 37, int. 5- Loc. Renaccio

53100 Siena - C.F.: 92058220523

Tel. 0577 247075 - Fax 0577 279500

e-mail: segreteria@atotoscanasud.it - Pec: segreteria@pec.atotoscanasud.it

Sommario

Introduzione	4
I principi guida.....	4
Ruolo del Responsabile per la Transizione al Digitale	5
La spesa per la transizione digitale.....	5
Le priorità da affrontare.....	6
Capitolo 1 - Organizzazione della PA e gestione del cambiamento.....	7
Attività 1.1 - Il ruolo del Responsabile e dell'Ufficio per la transizione al digitale.....	7
Intervento 1.1.1 – Mappatura dei processi.....	8
Intervento 1.1.2 Istituzione e potenziamento ufficio RTD.....	8
Intervento 1.1.3 - Integrazione degli obiettivi di digitalizzazione nel PIAO	9
Attività 1.2 - Competenze digitali per il Paese e per la PA	10
Intervento 1.2.1 - Pianificazione della formazione in ambito digitale.....	11
Capitolo 2 - Il procurement per la trasformazione digitale.....	12
Attività 2.1 - Il procurement per la trasformazione digitale.....	13
Attività 2.2 - Digitalizzazione delle procedure di affidamento	13
Attività 2.3 - Le gare strategiche per la trasformazione digitale.....	14
Capitolo 3 - Servizi digitali.....	16
Attività 3.1 - E-Service in interoperabilità tramite PDND.....	16
Intervento 3.1.1 - Piattaforma Nazionale Dati	18
Attività 3.2 - Progettazione dei servizi: accessibilità e design.....	18
Intervento 3.2.1 Nuovo sito internet dell'Ente	21
Attività 3.3 Formazione, gestione e conservazione dei documenti informatici.....	22
Intervento 3.3.1 Redazione, adozione e aggiornamento del Manuale di Gestione Documentale e del Manuale di conservazione.	24
Capitolo 4 - Piattaforme	26
Attività 4.1 - Piattaforme nazionali che erogano servizi a cittadini/imprese o ad altre PA	26
Intervento 4.1.1 - Integrazione notifiche digitali	27
Attività 4.2 - Basi dati interesse nazionale.....	27
Capitolo 5 - Dati e Intelligenza Artificiale.....	28
Attività 5.1 - Open data e data governance	28
Intervento 5.1.1 - Ricognizione dei dati e pubblicazione dataset	32
Attività 5.2 - Intelligenza artificiale per la Pubblica Amministrazione	33

Intervento 5.2.1 - Interventi previsti in ambito IA.....	35
Capitolo 6 - Infrastrutture	36
Attività 6.1 - Infrastrutture digitali e Cloud.....	36
Intervento 6.1.1 - Realizzazione piano di migrazione al cloud	38
Attività 6.2 - Il sistema pubblico di connettività	39
Capitolo 7 - Sicurezza informatica	41
Attività 7.1 - Governance della cybersicurezza	43
Intervento 7.1.1 Adozione del Framework Nazionale per la Cyber Security e la Data Protection (FNCS) – contestualizzazione, definizione dei ruoli, individuazione della struttura per la gestione della cybersicurezza e nomina del responsabile	45
Intervento 7.1.2 Definizione del framework documentale a supporto della gestione cyber.....	45
Attività 7.2 Promuovere attività legate al miglioramento della cultura <i>cyber</i> delle Amministrazioni.....	46
Attività 7.3 Implementare soluzioni di difesa proattive.....	47
Intervento 7.3.1 Adozione degli Indicatori di Compromissione	47

Introduzione

L'Autorità per il servizio di gestione integrata dei rifiuti urbani ATO Toscana Sud (in breve, ATO Toscana Sud) è l'Ente istituito con legge R.T. n. 69/2011 per la pianificazione, programmazione e controllo della gestione integrata dei rifiuti urbani sul territorio delle Province di Arezzo, Siena e Grosseto. Alle 98 amministrazioni comunali afferenti le suddette province si sono aggiunti successivamente anche 6 Comuni della Provincia di Livorno: nello specifico i Comuni di Campiglia Marittima, Castagneto Carducci, Piombino, San Vincenzo, Sassetta e Suvereto.

L'ente è tenuto all'attuazione di tutte le disposizioni derivanti dal D.LGS. 82/2005 Codice dell'Amministrazione Digitale – CAD, secondo quanto previsto dall'art. 2 c. 2 lettera a dello stesso D.LGS., e all'osservazione di quanto previsto dalle Linee Guida AGID.

In questi anni l'Ente ha potenziato tutte le strutture riguardanti l'accesso al Cloud, attuato misure per la cyber security, attivato il potenziamento della connettività, implementato le tecnologie e la strumentazione per l'utilizzo dello smart working.

La strategia indicata nel PTI è improntata ai seguenti principi:

- fornire strumenti alla Pubblica Amministrazione per erogare servizi esclusivamente in modalità digitale, rendendo più efficaci e veloci i processi di interazione con cittadini, imprese e altre pubbliche amministrazioni. L'interazione implica un reciproco scambio di informazioni o azioni tra le parti coinvolte, con l'obiettivo di raggiungere un determinato risultato;
- favorire lo sviluppo di una società digitale, dove i servizi mettono al centro i cittadini e le imprese, attraverso la digitalizzazione della Pubblica Amministrazione che costituisce il motore di sviluppo per tutto il Paese;
- promuovere lo sviluppo sostenibile, etico ed inclusivo, attraverso l'innovazione e la digitalizzazione al servizio delle persone, delle comunità e dei territori, nel rispetto della sostenibilità ambientale;
- contribuire alla diffusione delle nuove tecnologie digitali nel tessuto produttivo italiano, incentivando la standardizzazione, l'innovazione e la sperimentazione nell'ambito dei servizi pubblici.

Come previsto dal PTI “... i singoli enti pubblici individuano i propri specifici obiettivi di digitalizzazione, semplificazione e reingegnerizzazione all'interno del PIAO, come previsto dal DM 24 giugno 2022, che ormai integra la maggior parte delle forme di pianificazione delle PA su prospettiva triennale.”

I principi guida

I 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.

1. digitale e mobile come prima opzione (*digital & mobile first*);
2. cloud come prima opzione (*cloud first*);
3. interoperabile by design e by default (*API-first*);

4. accesso esclusivo mediante identità digitale (*digital identity only*);
5. servizi inclusivi, accessibili e centrati sull'utente (*user-centric*);
6. dati pubblici un bene comune (*open data by design e by default*);
7. concepito per la sicurezza e la protezione dei dati personali (*data protection by design e by default*);
8. *once only* e concepito come transfrontaliero;
9. apertura come prima opzione (*openness*);
10. sostenibilità digitale;
11. sussidiarietà, proporzionalità e appropriatezza della digitalizzazione;

Ruolo del Responsabile per la Transizione al Digitale

Come previsto dall'articolo 17 del CAD il processo di transizione al digitale è governato dall'Ufficio per la transizione al digitale, coordinato dal Responsabile per la transizione al digitale (d'ora in avanti RTD).

ATO Toscana Sud ha nominato con determinazione del Direttore Generale n. 48 del 31.03.2023 il Responsabile per la transizione al digitale nella figura di Massimiliano Terranzani. La nomina è stata successivamente rinnovata fino all'attuale scadenza del 31.12.2024.

Il presente Piano tiene conto delle attività svolte anche nel corso del 2023 e stabilisce le priorità operative sulla base dell'attuabilità degli obiettivi.

La spesa per la transizione digitale

Nel bilancio di previsione 2024-2026, approvato con Delibera di Assemblea dei Sindaci n. 12 del 30.11.2023, l'ente ha stanziato apposite risorse per far fronte alla transizione digitale. Di seguito i capitoli di spesa dedicati agli acquisti di beni e servizi in ambito digitale, come risulta dal bilancio di previsione assestato.

Cap	Descrizione	2024	2025	2026
212	Altre spese per servizi amministrativi	7.000,00	7.000,00	7.000,00
345	Acquisto beni durevoli	28.000,00	6.000,00	6.000,00
359	Sviluppo software e manutenzione evolutiva	5.000,00	2.000,00	2.000,00
501	Licenze	13.500,00	8.500,00	8.500,00
508	Gestione e manutenzione applicazioni	25.000,00	19.000,00	19.000,00
602	Acquisto di servizi per formazione specialistica	8.000,00	8.000,00	8.000,00
702	Altre prestazioni professionali e specialistiche *	235.000,00	125.000,00	125.000,00

* questo capitolo comprende anche spese non strettamente riferite all'attuazione del processo di transizione al digitale.

Le priorità da affrontare

Molte azioni pianificate nell'ambito di ciascuna priorità non sono solamente necessarie, ma soggette a obbligo, pena sanzione da parte delle Autorità Competenti. Ai sensi dell'art. 18 bis del Codice Amministrazione Digitale "Sanzioni per mancata transizione al digitale" sono sanzionabili i soggetti inadempienti verso l'applicazione delle Linee Guida AGID e del CAD – Codice Amministrazione Digitale.

Funzionalmente, si è provveduto a organizzare il Piano Triennale per l'Informatica – aggiornamento 2024 - 2026, coerentemente con il modello strategico, suddividendo il documento secondo i capitoli del PTI e individuando per ognuno le attività di rilievo e i relativi interventi pianificati.

I tempi di attuazione degli interventi, secondo diverse gradualità e urgenze e nel rispetto della legge, e dei "milestone" dei bandi PNRR, saranno tralasciati al 2024/2026.

Il modello strategico del PTI classifica le sfide organizzative e tecnologiche che le amministrazioni devono affrontare in tre **macroaree**:

- processi
- applicazioni
- tecnologie

a loro volta declinate nei diversi componenti puntualmente descritti nell'articolazione dei capitoli del Piano, alla quale si farà riferimento per l'individuazione delle linee di azione di competenza dell'ente e degli interventi previsti.



Figura 1: Componenti nel PT 2024-2026

Capitolo 1 - Organizzazione della PA e gestione del cambiamento

Attività 1.1 - Il ruolo del Responsabile e dell'Ufficio per la transizione al digitale

Il PTI individua come necessità la trasformazione dell'ente in «ecosistema amministrativo digitale», attraverso riorganizzazione interna, processi di analisi e re-ingegnerizzazione di procedimenti, partecipazione a iniziative di collaborazione tra enti.

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.

- Normativa di riferimento:
 - 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.

- Linee di azione applicabili

Obiettivo 1.1 - Migliorare i processi di trasformazione digitale della PA

RA1.1.1 - Rafforzare la collaborazione e lo scambio di pratiche e soluzioni tra Amministrazioni

◆ *Da marzo 2024 - Le Amministrazioni e gli Enti interessati possono proporre ad AGID l'attivazione di una comunità digitale tematica/territoriale su retedigitale.gov.it - CAP1.PA.01*

◆ *Da luglio 2024 - Le Amministrazioni e gli Enti interessati utilizzano i format presenti nel kit per proporre nuove comunità digitali ed effettuare monitoraggi semestrali delle attività in esse svolte - CAP1.PA.02*

RA1.1.2 - Individuazione e diffusione di modelli organizzativi/operativi degli Uffici Transizione digitale, anche in forma associata

◆ *Da marzo 2024 - 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 - CAP1.PA.03*

◆ *Da marzo 2024 - 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 - CAP1.PA.04*

- ◆ *Da luglio 2024 - 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 - CAP1.PA.05*
- ◆ *Da dicembre 2025 - Le PA partecipanti alle iniziative laboratoriali sperimentano i modelli proposti e forniscono ad AGID il feedback sui nuovi modelli organizzativi/operativi dell'UTD adottati - CAP1.PA.06*

Intervento 1.1.1 – Mappatura dei processi

La mappatura dei processi dell'ente è necessaria per la documentazione, l'analisi, la re-ingegnerizzazione delle attività che l'ente svolge e dei servizi che eroga. La sua realizzazione consente ai soggetti coinvolti – e ai nuovi assunti – di conoscere meglio la realtà nella quale opera e valutare azioni di miglioramento nell'organizzazione e nell'esecuzione del lavoro.

Questa attività è inoltre strettamente correlata all'analisi dei flussi documentali.

La revisione dei processi 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 già presenti nell'ente come, ad esempio, il Catalogo dei procedimenti o il Catalogo dei servizi erogati.

L'ente ha adottato una mappatura dei processi ai fini della prevenzione della corruzione, che costituisce uno specifico allegato al Piao ed integra la Sotto-sezione di programmazione rischi corruttivi e trasparenza. La mappatura riporta espressamente i processi afferenti al Servizio "Sistemi Informatici e Servizi Generali" quali, tra gli altri, i processi Gestione Protocollo, Gestione informatica, Gestione archivi dell'ente, Acquisti e forniture, Gestione dei mezzi e delle attrezzature dell'ente.

Inoltre, l'ente ha redatto l'elenco delle tipologie di procedimento amministrativo di propria competenza, pubblicato in Amministrazione Trasparente – Sezione Attività e Procedimenti. nel quale figurano gli Acquisti di beni e servizi e la Gestione dei flussi documentali.

Si ritiene pertanto che i processi afferenti alla trasformazione digitale dell'ente trovino già esplicitazione nelle attività sopra indicate e non sia necessaria una indicazione distinta. Nel corso degli anni sarà effettuato un aggiornamento periodico per verificare l'attivazione di nuovi processi o la modifica di quelli esistenti.

Modalità di realizzazione: Verifica necessità di aggiornamento

Responsabilità: RTD – Dirigente Area amm.va e contabile

Tempi: verifica continuativa

Risultati attesi: Pubblicazione mappatura processi ed elenco tipologie di procedimento costantemente aggiornati

Intervento 1.1.2 Istituzione e potenziamento ufficio RTD

Sede Legale Via della Pace 37, int. 5- Loc. Renaccio

53100 Siena - C.F.: 92058220523

Tel. 0577 247075 – Fax 0577 279500

e-mail: segreteria@atotoscanasud.it – Pec: segreteria@pec.atotoscanasud.it

Secondo quanto indicato nel PTI occorre istituire, ove non sia stato già fatto, l'Ufficio per la transizione al digitale, in forma singola o associata, con conseguente nomina del Responsabile per la transizione al digitale (RTD). Nell'ottica del suddetto ecosistema, la struttura organizzativa va potenziata. Ove ciò non sia sostenibile a livello di singolo ente, per le PA diverse da quelle centrali è possibile ricorrere all'istituzione di UTD associati a livello di Unione di Comuni o attraverso lo strumento della convenzione tra amministrazioni, con eventuale coinvolgimento di Province, Regioni, Province autonome e loro società in house.

In merito a questa indicazione, ATO Toscana Sud ha nominato con determinazione del Direttore Generale n. 48 del 31.03.2023 il Responsabile per la transizione al digitale nella figura di Massimiliano Terranzani. La nomina è stata successivamente rinnovata fino all'attuale scadenza del 31.12.2024.

Il PTI raccomanda inoltre di provvedere al potenziamento del ruolo e della dotazione di risorse umane e strumentali dell'UTD e alla 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'ente ha già considerato l'ipotesi di costituire un UTD in comune con altri enti, ma si tratta di una soluzione attualmente non percorribile a causa dei limiti di spesa del personale che impediscono ogni possibile manovra organizzativa di questo genere. Tuttavia, seppur salvaguardando l'autonomia del ruolo, il RTD può contare sul supporto e la disponibilità del Dirigente amministrativo e del Direttore Generale per quanto riguarda la messa a disposizione di ogni tipo di risorse finanziarie, strumentali e di misure organizzative necessarie all'attuazione degli interventi del Piano. In questo senso, la trasformazione digitale costituisce linea strategica dell'ente la cui attuazione vede impegnate anche figure diverse e sovraordinate al RTD.

Modalità di realizzazione: Valutazione ipotesi di rinnovo attuale incarico di RTD o conferimento nuovo incarico

Responsabilità: Direttore Generale

Tempi: entro dicembre 2024

Risultati attesi: Pubblicazione provvedimento amministrativo di rinnovo o di conferimento nuovo incarico

Intervento 1.1.3 - Integrazione degli obiettivi di digitalizzazione nel PIAO

All'interno del PIAO - Piano Integrato di Attività e Organizzazione, previsto dall'articolo 6 del decreto-legge n. 80 del 9 giugno 2021, occorre ricomprendere gli obiettivi specifici di digitalizzazione, semplificazione e re-ingegnerizzazione, sulla base delle priorità del singolo ente.

In merito a questa indicazione, l'ente ha inserito nel Piao 2024-2026 un importante obiettivo di digitalizzazione quale la realizzazione del nuovo sito internet in compliance con le Linee Guida Agid. Altri obiettivi specifici saranno inseriti nel prossimo Piao ed in particolare quelli relativi all'attuazione delle misure previste dal presente Piano.

Modalità di realizzazione: Integrazione degli obiettivi di digitalizzazione nella sottosezione di Programmazione della Performance del Piao e nel Piano dettagliato degli Obiettivi

Responsabilità: Direttore Generale – Dirigente Area Amm.va e contabile

Tempi: entro termini di approvazione Piao

Risultati attesi: Inserimento di almeno il 50% degli interventi previsti dal presente Piano triennale per l'informatica coerentemente con le tempistiche di realizzazione previste dal PTI Agid.

Attività 1.2 - Competenze digitali per il Paese e per la PA

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 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. 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.

Nella programmazione delle attività formative, deve essere rispettato quanto previsto all'art. 6 comma 2 lettera b) del DLgs 80/2021 laddove si prescrive il "raggiungimento della completa alfabetizzazione digitale" dei pubblici dipendenti. Nella realizzazione del PIAO quindi si evidenzieranno sia gli obiettivi finalizzati all'acquisizione di competenze digitali da parte dei cittadini che quelle finalizzate al personale.

➤ **Normativa di riferimento:**

- 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) 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

➤ **Linee di azione applicabili:**

Obiettivo 1.2 - Diffusione competenze digitali nel Paese e nella PA

- ◆ *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 - CAP1.PA.07*
- ◆ *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 – CAP1.PA.08*

Intervento 1.2.1 - Pianificazione della formazione in ambito digitale

In merito a questa indicazione, Ato toscana sud ha redatto un programma formativo all'interno del Piao Sezione Organizzazione e capitale umano - Sottosezione di programmazione piano triennale dei fabbisogni di personale. Il programma individua 4 aree di contenuto prevalente sulle quali concentrare gli interventi formativi: area amministrativa ed economica, area informatica, area specialistica tecnica, area obbligatoria. Per l'area informatica è stato previsto, nel corso del 2024, l'attuazione di corsi di formazione per l'attuazione del piano triennale per l'informatica Agid e per le procedure di sicurezza informatica (almeno 8 ore), principalmente per il personale del Servizio Sistemi Informatici.

Per quanto riguarda la piattaforma Syllabus, è stato nominato il responsabile per la formazione nella persona dell'RTD Massimiliano Terranzani e sono stati accreditati tutti i dipendenti dell'ente. Inoltre, 2 dipendenti hanno avviato i percorsi formativi "Competenze digitali per la p.a." L'obiettivo è di raggiungere entro il 31.12.2025 le percentuali di dipendenti formati indicate dalla direttiva del Ministro della p.a.

Modalità di realizzazione: Formazione dei dipendenti su Syllabus - "Competenze digitali per la p.a."

Responsabilità: RTD

Tempi: entro dicembre 2025

Risultati attesi: Completamento ciclo informativo per almeno il 75% dei dipendenti

Capitolo 2 - Il procurement per la trasformazione digitale

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 all'esterno. Ne consegue che grande attenzione va prestata affinché l'acquisizione di risorse dal mercato (procurement) sia realizzata con efficacia ed efficienza. 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.

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 della transizione al digitale venga coinvolto negli acquisti ICT e per la transizione digitale.

➤ Normative di riferimento:

- 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»
- Regole tecniche AGID del 1° giugno 2023 «Requisiti tecnici e modalità di certificazione delle Piattaforme di approvvigionamento digitale»

- Decisione di esecuzione Piano Nazionale di ripresa e resilienza
 - 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

Attività 2.1 - Il procurement per la trasformazione digitale

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.

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.

L'Ato Toscana sud non è iscritta nell'elenco delle stazioni appaltanti qualificate ai sensi dell'art. 63 del codice dei contratti, in quanto normalmente effettua acquisti di forniture e servizi di valore inferiore alla soglia prevista per l'affidamento diretto e non sono previsti affidamenti di lavori superiori alla soglia di 500 mila euro. Nel caso in cui, in futuro, si dovessero effettuare affidamenti che richiedano la qualificazione, l'ente si rivolgerà ad una centrale di committenza qualificata ai sensi dell'art. 62 comma 6 del codice.

➤ Linee di azione applicabili:

Obiettivo 2.1 - Rafforzare l'ecosistema nazionale di approvvigionamento digitale

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

Giugno 2025 - I soggetti aggregatori devono dotarsi di piattaforme di approvvigionamento che digitalizzano la fase di esecuzione dell'appalto - CAP2.PA.01

Dicembre 2026 - Le stazioni appaltanti devono digitalizzare la fase di esecuzione dell'appalto - CAP2.PA.02

Attività 2.2 - Digitalizzazione delle procedure di affidamento

Nelle disposizioni della Parte II del Libro I artt. 19-36 «Digitalizzazione del ciclo di vita dei contratti pubblici» del Codice dei contratti pubblici, risulta centrale e obbligatorio dal primo

gennaio 2024 lo svolgimento degli acquisti della Pubblica Amministrazione attraverso le piattaforme di approvvigionamento digitale (art. 25). Le stesse 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 (dalla programmazione fino all'esecuzione del contratto). In tal senso, 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.

➤ **Linee di azione applicabili:**

Obiettivo 2.2 - Diffondere l'utilizzo degli appalti innovativi

RA2.2.1 - Incremento della partecipazione di PMI e start up agli appalti di innovazione

◆ *Dicembre 2024 - Le PAL coinvolte nel programma Smarter Italy partecipano alla definizione dei fabbisogni: Salute e benessere, Valorizzazione dei beni culturali, Protezione dell'ambiente - CAP2.PA.03*

L'ente ha implementato un processo per la gestione totalmente digitale delle procedure di approvvigionamento ricorrendo sistematicamente a Consip e al Mercato elettronico della pubblica amministrazione per ogni affidamento di valore superiore a 5.000 euro. Quindi l'ente utilizza gli strumenti offerti dal portale acquistinretepa.it come piattaforma di approvvigionamento digitale.

Attività 2.3 - Le gare strategiche per la trasformazione digitale

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.

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.

➤ Linee di azione applicabili:

*Obiettivo 2.3 - Favorire e monitorare l'utilizzo dei servizi previsti dalle Gare strategiche
RA2.3.1 - Incremento del livello di trasformazione digitale mediante la disponibilità di Gare strategiche allo scopo definite*

◆ *Settembre 2024 - Le PA, nel proprio piano acquisti, programmano i fabbisogni di adesione alle iniziative strategiche disponibili per il perseguimento degli obiettivi del Piano triennale per l'anno 2025 - CAP2.PA.04*

◆ *Settembre 2025 - Le PA programmano i fabbisogni di adesione alle iniziative strategiche per il perseguimento degli obiettivi del Piano triennale per l'anno 2026 - CAP2.PA.05*

◆ *Settembre 2026 - Le PA programmano i fabbisogni di adesione alle iniziative strategiche per il perseguimento degli obiettivi del Piano triennale per l'anno 2027 - CAP2.PA.06*

L'ente non ha realizzato un programma dei fabbisogni coordinato con le iniziative strategiche, gli obiettivi dell'Ente, la programmazione di bilancio. Infatti, negli ultimi anni l'ente non ha redatto e approvato il Programma triennale degli acquisti perché non sono stati previsti affidamenti di beni e servizi di valore superiore a 140 mila euro.

Capitolo 3 - Servizi digitali

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.

Attività 3.1 - E-Service in interoperabilità tramite PDND

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.

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

➤ Normativa di riferimento:

- 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»
- 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)

➤ Linee di azione applicabili

Obiettivo 3.1 - Migliorare la capacità di erogare e-service

RA3.1.1 - Incremento del numero di «e-service» registrati sul Catalogo Pubblico PDND

◆ *Da gennaio 2024 - Le PA cessano di utilizzare modalità di interoperabilità diverse da PDND – CAP3.PA.01*

◆ *Da gennaio 2024 - Le Amministrazioni iniziano la migrazione dei servizi erogati in interoperabilità dalle attuali modalità alla PDND - CAP3.PA.02*

- ◆ *Da gennaio 2024 - 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» - CAP3.PA.03*
 - ◆ *Da gennaio 2024 - Le PA locali rispondono ai bandi pubblicati per l'erogazione di API su PDND - CAP3.PA.04*
 - ◆ *Da gennaio 2024 - Le PA centrali siglano accordi per l'erogazione di API su PDND - CAP3.PA.05*
- RA3.1.2 - Aumento del numero di Richieste di Fruizione Autorizzate su PDND*
- ◆ *Da gennaio 2024 - Le PA utilizzano le API presenti sul Catalogo - CAP3.PA.06*
 - ◆ *Da gennaio 2025 - Le PA effettuano richieste di fruizione di servizi erogati da privati - CAP3.PA.07*
- RA3.1.3 - Ampliamento del numero delle amministrazioni coinvolte nell'evoluzione delle Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni*
- ◆ *Da gennaio 2024 - 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 - CAP3.PA.08*

Intervento 3.1.1 - Piattaforma Nazionale Dati

A seguito di un'analisi approfondita dei procedimenti seguiti dall'ente, si ritiene che sulla PDND non risultino dati utili per lo svolgimento delle attività dell'ente.

Nei prossimi mesi si verificherà se le attività dell'ente generino dati che possano essere messi in condivisione di altri enti attraverso la piattaforma e inserendo API in catalogo (<https://www.interop.pagopa.it/catalogo>).

Modalità di realizzazione: Verifica dati da condividere sulla PDND

Responsabilità: RTD – Dirigente Area Amministrativa e Contabile

Tempi: entro dicembre 2025

Risultati attesi: Report di verifica

Attività 3.2 - Progettazione dei servizi: accessibilità e design

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.

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.

➤ Normativa di riferimento:

- 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 relativa 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»
- 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

➤ **Linee di azione applicabili:**

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

RA3.2.2 - Incremento dell'accessibilità dei servizi digitali

◆ *Marzo 2024 - Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web – CAP3.PA.09*

◆ *Settembre 2024 - 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++ - CAP3.PA.10*

◆ *Settembre 2024 - 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 - CAP3.PA.11*

◆ *Dicembre 2024 - 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 - CAP3.PA.12*

◆ *Marzo 2025 - Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web - CAP3.PA.13*

- ◆ *Settembre 2025 - 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 - CAP3.PA.14*
- ◆ *Marzo 2026 - Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web - CAP3.PA.15*
- ◆ *Settembre 2026 - 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 - CAP3.PA.16*

Intervento 3.2.1 Nuovo sito internet dell'Ente

Con determinazione del Dirigente dell'Area Amministrativa e Contabile n. 22 del 7.5.2024 è stato effettuato l'affidamento del servizio di realizzazione del nuovo sito web istituzionale dell'ente e del servizio di manutenzione ordinaria ed evolutiva dello stesso per la durata di 5 anni. Le attività di realizzazione del nuovo sito sono ad oggi in via di ultimazione.

Le azioni da intraprendere sono le seguenti:

- si esegue il test usabilità con il kit predisposto da Designers Italia: <https://designers.italia.it/risorse-per-progettare/validare/test-di-usabilita/>;
- si effettua il test di accessibilità secondo le modalità ed utilizzando le piattaforme di cui alle "Linee guida AGID sull'accessibilità degli strumenti informatici" e la piattaforma MAUVE++ <https://mauve.isti.cnr.it/>;
- si utilizza l'App messa a disposizione dal Ministero per l'Innovazione <https://docs.italia.it/italia/designers-italia/app-valutazione-modelli-docs/it/versione-attuale/index.html> per la verifica della corretta adesione ai modelli di Designers Italia
- si pubblicano gli obiettivi di accessibilità sul proprio sito web entro marzo di ogni anno;
- si comunicano ad AGID (form.agid.gov.it) entro marzo di ogni anno gli obiettivi di accessibilità del proprio sito;
- si pubblica, tramite l'applicazione form.agid.gov.it, una dichiarazione di accessibilità per il sito web ed eventuali app entro settembre di ogni anno;
- si effettuano interventi di tipo adeguativo e/o correttivo sui contenuti/sezioni individuate prioritariamente dalle analisi di accessibilità e usabilità anche in linea con quanto previsto dalle Linee Guida AGID sui siti web luglio 2022.
- si organizzano corsi di formazione su aspetti tecnici e/o normativi;
- si monitorano costantemente gli eventuali feedback dei cittadini sia per quanto attiene l'accessibilità, che per quanto attiene la fruibilità;
- si analizzano periodicamente gli esiti dei risultati e si programmano tutte le iniziative necessarie a migliorare l'usabilità e l'accessibilità del sito da parte dei cittadini;

Modalità di realizzazione: Nuovo sito internet

Responsabilità: RTD

Tempi: entro dicembre 2024; rispetto altre scadenze

Risultati attesi: Corretta messa in esercizio del nuovo sito internet ed esecuzione delle altre attività sopra descritte.

Attività 3.3 Formazione, gestione e conservazione dei documenti informatici

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.

Secondo quanto indicato dal PTI, 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;
- nomina dei ruoli e delle responsabilità previsti;
- adozione del Manuale di gestione documentale e del Manuale di conservazione;
- 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 disposizioni 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.

➤ Normativa di riferimento:

- 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)
- 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.

➤ Linee di azione applicabili

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

◆ *Dal primo gennaio 2022 sono entrate in vigore le linee guida sulla formazione, gestione e conservazione dei documenti informatici. Oltre al rispetto della normativa previgente le amministrazioni sono tenute a rispettare quanto previsto dalle suddette linee guida.*

◆ *Giugno 2025 - 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 – CAP3.PA.17

♦ *Giugno 2026 - Le PA devono verificare che in «Amministrazione trasparente» sia pubblicato il manuale di conservazione e la nomina del responsabile della conservazione - CAP3.PA.18*

Intervento 3.3.1 Redazione, adozione e aggiornamento del Manuale di Gestione Documentale e del Manuale di conservazione.

ATO Toscana Sud ha adottato, conformemente alle Linee guida AGID di cui all' art. 71 del CAD e delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di cui all'art. 71 del decreto legislativo n. 82 del 2005, entrate in vigore con il 1° gennaio 2022, il Manuale di Gestione Documentale e il Manuale di conservazione con determinazione del Direttore Generale n. 76 del 19.06.2023.

Attualmente, il software che governa l'intero flusso documentale è fornito dalla società Halley Informatica srl, il sistema di conservazione è affidato a Unimatica spa, l'ente ha nominato quale Responsabile della gestione documentale e Responsabile della conservazione l'RTD Massimiliano Terranzani.

L'ente prevede di aggiornare nel primo semestre 2025 il Manuale di gestione documentale e il Manuale di conservazione per ottemperare alle indicazioni delle Linee Guida.

Propedeutica alla revisione dei manuali è l'analisi delle eventuali criticità nella struttura nel processo di dematerializzazione dei documenti e alla corretta procedura di protocollazione rispetto a quanto previsto dalle linee guida e dalla normativa (qualità dei documenti prodotti, modalità di protocollazione, fascicolazione digitale, firme digitali ecc.).

Una volta approvati, i manuali saranno inviati ed illustrati a tutti i dipendenti affinché ne sia assicurata la corretta applicazione.

Per quanto riguarda i documenti analogici, l'ATO ha già implementato ormai da diversi anni una procedura di produzione interamente digitale dei documenti, eliminando quasi completamente il ricorso a documenti cartacei. I pochi documenti cartacei tuttora in produzione riguardano documenti endoprocedimentali (quindi a valenza esclusivamente interna) oppure rara documentazione cartacea in arrivo. La documentazione in arrivo è ormai quasi tutta in formato digitale perché l'ente interloquisce sostanzialmente con altre p.a. e con imprese tramite pec.

L'ATO effettua la protocollazione informatica di tali rari documenti analogici e la loro conservazione in originale tramite fascicoli cartacei. Considerato lo scarso volume di tale documentazione, l'ente non intende al momento attivare la procedura di certificazione delle copie digitali di originali analogici secondo quanto previsto dall'allegato 3 delle Linee Guida "Certificazione di processo" e dall'art. 22 del CAD, al fine di conferire alla copia informatica lo stesso valore probatorio dell'originale analogico. In futuro si valuterà il ricorso a tale procedura nel caso in cui la produzione di documenti analogici dovesse crescere di volume.

Modalità di realizzazione: Aggiornamento manuali

Responsabilità: RTD – Dirigente amm.vo contabile

Tempi: entro giugno 2025 aggiornamento Manuale di gestione documentale, entro giugno 2026 aggiornamento Manuale di conservazione.

Risultati attesi: Pubblicazione manuali aggiornati

Capitolo 4 - Piattaforme

Attività 4.1 - Piattaforme nazionali che erogano servizi a cittadini/imprese o ad altre PA

Il capitolo 4 del Piano Triennale per l'informatica Agid 2024-2026 è dedicato alle piattaforme della Pubblica Amministrazione che offrono funzionalità fondamentali nella digitalizzazione dei processi e dei servizi della PA. Vengono illustrate le piattaforme che offrono servizi a cittadini e a imprese quali PagoPA, Applo, Send, Spid e Cie, NoiPA, Fascicolo sanitario elettronico e SUAP/SUE nell'ottica di migliorare i servizi erogati con le modalità dettagliate nei risultati attesi e nelle linee di azione.

Le Piattaforme elencate non riguardano le attività dell'ente in quanto l'Ato non eroga servizi a cittadini e imprese.

Una riflessione a parte merita la piattaforma SEND (raggiungibile da selfcare.pagopa.it), che è stata ideata per rendere 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.

➤ Normativa di riferimento

- 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

➤ Linee di azione applicabili

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

RA4.1.3 - Incremento degli enti che usano SEND

◆ Dicembre 2026 - 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 - CAP4.PA.03

Intervento 4.1.1 - Integrazione notifiche digitali

Si valuterà se sussistono le condizioni per l'attivazione di SEND, considerato che l'art. 26 comma 3 del DL 76/2020 dispone: *“Ai fini della notificazione di atti, provvedimenti, avvisi e comunicazioni, in alternativa alle modalità previste da altre disposizioni di legge, anche in materia tributaria, le amministrazioni possono rendere disponibili telematicamente sulla piattaforma i corrispondenti documenti informatici...”*. Si tratta quindi di un'implementazione facoltativa, comunque di utilità trascurabile considerato che le nostre attività non prevedono al momento notifiche nei confronti di terzi.

Modalità di realizzazione: Adesione a SEND

Responsabilità: RTD – Dirigente amm.vo contabile

Tempi: entro dicembre 2026

Risultati attesi: Valutazione opportunità di adesione a SEND

Attività 4.2 - Basi dati interesse nazionale

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.

Le attività e i processi di competenza dell'Ato non rientrano nelle basi dati di interesse nazionale elencate nell'art. 60 comma 3 bis del CAD né nelle ulteriori basi dati aggiunte da Agid ai sensi dell'art. 60 comma 3-ter del CAD.

➤ **Normativa di riferimento**

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

➤ Linee d'azione applicabili

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

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

◆ *Da gennaio 2025 - 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 - CAP4.PA.23*

◆ *Da gennaio 2025 - La PA titolari di basi di dati di interesse nazionale le adeguano all'aggiornamento delle regole tecniche – CAP4.PA.24*

Capitolo 5 - Dati e Intelligenza Artificiale

Attività 5.1 - Open data e data governance

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 fornir ai vertici decisionali strumenti data-driven da utilizzare nei processi organizzativi e/o produttivi. La 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.

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 nel Piano triennale ICT di ciascuna amministrazione anche 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.

I dati di elevato valore, introdotti dalla Direttiva (UE) 2019/1024 (cosiddetta Direttiva Open Data), sono definiti dalla stessa Direttiva come quei dati al cui riutilizzo possono essere associati importanti benefici per la società, l'ambiente e l'economia. A tale scopo, la Direttiva ha individuato sei categorie (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) in corrispondenza delle quali il Regolamento (UE) 2023/138 ha poi identificato puntualmente le relative serie di dati da considerare come preziose per il riutilizzo.

Il PTI definisce i seguenti obiettivi per questa attività:

- Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese
- Aumentare la qualità dei dati e dei metadati
- Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati per i quali le PA sono chiamate a definire i relativi interventi.

➤ Normativa di riferimento

- 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»
- 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

➤ Linee di azione applicabili

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

RA5.1.1 - Aumento del numero di dataset aperti di tipo dinamico in coerenza con quanto previsto dalle Linee guida Open Data

Sede Legale Via della Pace 37, int. 5- Loc. Renaccio

53100 Siena - C.F.: 92058220523

Tel. 0577 247075 - Fax 0577 279500

e-mail: segreteria@atotoscanasud.it - Pec: segreteria@pec.atotoscanasud.it

- ◆ *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 - CAP5.PA.01*
- ◆ *Le PA adeguano i metadati relativi ai dati non geografici alle specifiche nazionali e documentano i propri dataset nel Catalogo nazionale dati.gov.it - CAP5.PA.02*
- ◆ *Le PA partecipano, in funzione delle proprie necessità, a interventi di formazione e sensibilizzazione sulle politiche open data - CAP5.PA.03*

RA5.1.2

- ◆ *Da giugno 2024 - 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 – CAP5.PA.04*

Obiettivo 5.2 - Aumentare la qualità dei dati e dei metadati**RA5.2.1 - Aumento del numero di dataset con metadati di qualità conformi agli standard di riferimento europei e nazionali**

- ◆ *Da giugno 2024 - 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 - CAP5.PA.05*

RA5.2.3 - Aumento del numero di amministrazioni non ancora presenti nel catalogo dati.gov.it che rendono disponibili dataset di tipo aperto

- ◆ *Dicembre 2024 - 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 - CAP5.PA.06*
- ◆ *Dicembre 2024 - 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 - CAP5.PA.07*
- ◆ *Dicembre 2024 - 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 - CAP5.PA.08*
- ◆ *Dicembre 2024 - Ogni PA centrale (non ancora presente nel catalogo dati.gov.it) pubblica e documenta nel catalogo almeno 15 dataset - CAP5.PA.09*
- ◆ *Dicembre 2025 - 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 - CAP5.PA.10*
- ◆ *Dicembre 2025 - 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 2024 nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 5 dataset - CAP5.PA.11

◆ *Dicembre 2025 - Ogni Comune con popolazione tra 100.001 e 250.000 abitanti, ogni Provincia e Città Metropolitana (non ancora presenti nel 2024 nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 10 dataset - CAP5.PA.12*

◆ *Dicembre 2025 - 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 2024 nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 15 dataset - CAP5.PA.13*

◆ *Dicembre 2025 - Ogni PA centrale (non ancora presente nel 2024 nel catalogo dati.gov.it) pubblica e documenta nel catalogo almeno 30 dataset - CAP5.PA.14*

◆ *Dicembre 2026 - 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 3 dataset - CAP5.PA.15*

◆ *Dicembre 2026 - 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 2024 nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 10 dataset - CAP5.PA.16*

◆ *Dicembre 2026 - Ogni Comune con popolazione tra 100.001 e 250.000 abitanti, ogni Provincia e Città Metropolitana (non ancora presenti nel 2024 nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 15 dataset - CAP5.PA.17*

◆ *Dicembre 2026 - 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 2024 nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 30 dataset - CAP5.PA.18*

◆ *Dicembre 2026 - Ogni PA centrale (non ancora presente nel 2024 nel catalogo dati.gov.it) pubblica e documenta nel catalogo almeno 45 dataset - CAP5.PA.19*

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

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

◆ *Da gennaio 2024 - 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 - CAP5.PA.20*

Intervento 5.1.1 - Riconoscimento dei dati e pubblicazione dataset

Il Responsabile per la Transizione digitale, in collaborazione con i referenti tematici che gestiscono e trattano dati nell'ambito delle singole unità organizzative effettuerà il

censimento e l'analisi dei dati di elevato valore utilizzati nell'ente e definirà una strategia di pubblicazione.

Si valuterà la possibile adesione al catalogo Opentoscana pubblicato dalla Regione Toscana, al quale conferire i dataset disponibili in formato open coerentemente con il modello di interoperabilità e con i modelli di riferimento di dati nazionali ed europei. Dovrà essere valutata la dotazione dei documenti e dei dataset di metadati e di licenze d'uso.

Modalità di realizzazione: Censimento dei dataset da pubblicare in formato open e valutazione adesione al portale della Regione Toscana

Responsabilità: RTD

Tempi: entro dicembre 2025

Risultati attesi: Relazione del RTD che

- Individui i data set potenzialmente disponibili (compresi quelli definiti di "alto valore");
- Preveda la dotazione di metadati e di licenze d'uso per i data set di cui sopra;
- Preveda le modalità di pubblicazione dei dati in formato open (accordo con la Regione o inserimento nella sezione OPEN DATA del sito istituzionale dell'ente).

Attività 5.2 - Intelligenza artificiale per la Pubblica Amministrazione

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.

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.

- **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.
- **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*.
- **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.

- **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.
- **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.
- **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.
- **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*.
- **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.
- **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.
- **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*.

➤ Normativa di riferimento

- Comunicazione della Commissione al Parlamento Europeo e al Consiglio, «Piano Coordinato sull'Intelligenza Artificiale», COM (2021) 205 del 21 aprile 2021
- «Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale» (*AI Act*), COM (2021) 206, 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

➤ Linee di azione applicabili

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

RA5.4.1 - Linee guida per promuovere l'adozione dell'IA nella Pubblica Amministrazione

◆ Dicembre 2025 - Le PA adottano le Linee per promuovere l'adozione dell'IA nella Pubblica Amministrazione - CAP5.PA.21

RA5.4.2 - Linee guida per il procurement di IA nella Pubblica Amministrazione

◆ Dicembre 2025 - Le PA adottano le Linee guida per il procurement di IA nella Pubblica Amministrazione - CAP5.PA.22

RA5.4.3 - Linee guida per lo sviluppo di applicazioni di IA per la Pubblica Amministrazione

◆ Dicembre 2025 - Le PA adottano le Linee guida per lo sviluppo di applicazioni di IA nella Pubblica Amministrazione - CAP5.PA.23

RA5.4.4 - Realizzazione di applicazioni di IA a valenza nazionale

◆ Dicembre 2026 - Le PA adottano le applicazioni di IA a valenza nazionale - CAP5.PA.24

Obiettivo 5.5 - Dati per l'intelligenza artificiale

RA5.5.1 - Basi di dati nazionali strategiche

◆ Dicembre 2026 - Le PA adottano le basi dati nazionali strategiche – CAP5.PA.25

Intervento 5.2.1 - Interventi previsti in ambito IA

Nell'ambito dell'attività 1.2 - Competenze digitali per il Paese e per la PA, l'ente intende favorire interventi formativi sull'intelligenza artificiale anche tramite Syllabus.

Fondamentale è il ruolo dell'RTD nell'effettuare analisi di utilità dell'intelligenza artificiale ai processi lavorativi gestiti dall'ente. Analisi che dovrà essere compiuta entro dicembre 2025.

Modalità di realizzazione: Analisi dell'utilità dell'impiego dell'IA nei processi lavorativi dell'ente

Responsabilità: RTD

Tempi: entro dicembre 2025

Risultati attesi: Relazione del RTD che individui i processi lavorativi ai quali applicare l'IA.

Capitolo 6 - Infrastrutture

Attività 6.1 - Infrastrutture digitali e Cloud

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.

Il PTI ha ribadito che:

- 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 dalle Circolari AGID n. 2 e n. 3 del 2018 e, successivamente, 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.
- 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.

➤ Normative di riferimento

- 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
- Piano Nazionale di Ripresa e Resilienza:
 - Investimento 1.1: «Infrastrutture digitali»
 - Investimento 1.2: «Abilitazione e facilitazione migrazione al cloud»

➤ **Linee di azione applicabili**

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)

Sede Legale Via della Pace 37, int. 5- Loc. Renaccio

53100 Siena - C.F.: 92058220523

Tel. 0577 247075 - Fax 0577 279500

e-mail: segreteria@atotoscanasud.it - Pec: segreteria@pec.atotoscanasud.it

RA6.1.1 - Numero di amministrazioni migrate

- ◆ *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 - CAP6.PA.01*
- ◆ *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 - CAP6.PA.02*
- ◆ *Le PA avviano il percorso di migrazione verso il cloud in coerenza con quanto previsto dalla Strategia Cloud Italia - CAP6.PA.03*
- ◆ *Le PA continuano ad applicare il principio cloud first e ad acquisire servizi cloud solo se qualificati - CAP6.PA.04*
- ◆ *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 - CAP6.PA.05*

Linee di azione 2024-2026

- ◆ *Da gennaio 2024 - 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 - CAP6.PA.06*
- ◆ *Da gennaio 2024 - 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 - CAP6.PA.07*
- ◆ *Gennaio 2024 - 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 - CAP6.PA.08*
- ◆ *Settembre 2024 - 4.083 amministrazioni concludono la migrazione in coerenza con il piano di migrazione e, ove richiesto dal Dipartimento per la Trasformazione Digitale o da AGID, trasmettono le informazioni necessarie per verificare il completamento della migrazione - CAP6.PA.09*
- ◆ *Giugno 2026 - 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 - CAP6.PA.10*

Intervento 6.1.1 - Realizzazione piano di migrazione al cloud

A giugno 2023 l'ente ha affidato a Terrecablate reti e servizi srl il servizio di connettività in fibra dedicata con potenza di banda 300/300 Mbps. L'ente quindi ha potenziato la propria infrastruttura di rete al fine di implementare il passaggio in cloud dei propri sistemi.

L'Ente rientra tra quelli definiti "di Gruppo B", ovvero "Data center che non garantiscono requisiti minimi di affidabilità e sicurezza dal punto di vista infrastrutturale e/o organizzativo, o non garantiscono la continuità dei servizi." Pertanto, è necessario procedere alla definizione di un piano di migrazione verso soluzioni cloud qualificate, in regola con le disposizioni di legge e le indicazioni del PTI.

Il piano di migrazione al cloud prevede le seguenti fasi:

1) Analisi delle infrastrutture e degli applicativi dell'amministrazione.

L'ente ha già avviato il censimento delle macchine e degli applicativi in uso connessi al datacenter. Questa attività sarà conclusa entro dicembre 2024

2) Valutazione delle soluzioni di migrazione attuabili

L'attività sarà conclusa entro febbraio 2025.

3) Passaggio in cloud delle infrastrutture e degli applicativi.

L'ente ha già avviato contatti con la software house Halley Toscana srl per la migrazione in cloud della suite in uso per la gestione del protocollo, degli atti amministrativi e della contabilità. Entro giugno 2026 dovrà essere effettuato il passaggio in cloud di tale suite e di tutte le infrastrutture verso il SaaS come soluzione prioritaria rispetto alle altre tipologie IaaS e PaaS.

Modalità di realizzazione: Attuazione del piano di migrazione al cloud

Responsabilità: RTD

Tempi: entro giugno 2026

Risultati attesi: Tutte le infrastrutture e gli applicativi sono migrati in cloud e dismessi dai data center.

Attività 6.2 - Il sistema pubblico di connettività

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;

Tramite il contratto stipulato con Terre Cablate reti e servizi srl, l'ente risulta già connesso al servizio pubblico di connettività.

- Normative di riferimento
 - 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
- Linee di azione applicabili

Obiettivo 6.2 - Garantire alle amministrazioni la disponibilità della connettività SPC

RA6.2.1 - Rete di connettività

◆ *Da gennaio 2025 - 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 – CAP6.PA.11*

Capitolo 7 - Sicurezza informatica

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, AgID metterà 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). Sempre in relazione al contesto della cybersicurezza, sono previste dal PTI alcune Linee d'azione istituzionali che coinvolgono ACN nella definizione di specifiche Linee Guida destinate alle PA, che serviranno quale riferimento per l'individuazione degli interventi.

Si rileva come le disposizioni della direttiva NIS2, recepita con D. Lgs 4 settembre 2024, n. 138, e la recente legge sulla cybersicurezza nazionale e sui reati informatici n. 90 del 28

giugno 2024 non modifichino comunque gli adempimenti previsti per le pubbliche amministrazioni dal Piano Triennale ICT. Gli interventi definiti in relazione alle linee di azione applicabili saranno rimodulati tenendo conto delle normative applicabili per l'Ente.

Entro il 31 dicembre 2024, aziende e pubbliche amministrazioni dovranno svolgere un assessment per comprendere se siano o meno soggette agli obblighi della Direttiva NIS2, seguendo il dettato degli artt. 6 e 7, degli Allegati I, II, III e IV del D.Lgs 4 settembre 2024, n. 138, nonché di ogni altro atto che verrà emanato. Il perimetro di applicazione della direttiva è coerente con quello definito sinteticamente dalla legge n. 90 del 28 giugno 2024, «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici», rif. Art. 1 comma 1:

“Le pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, le regioni e le province autonome di Trento e di Bolzano, le città metropolitane, i comuni con popolazione superiore a 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e le aziende sanitarie locali [...] le rispettive società in house che forniscono servizi informatici, i servizi di trasporto di cui al primo periodo del presente comma ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008.”

L'Ente non è quindi soggetto all'applicazione della direttiva NIS2, né rientra tra quelli nel perimetro definito dalla L. 90/2024. Si procede con l'applicazione delle indicazioni ritenute utili e/o derivanti da altre fonti normative quali il GDPR.

➤ Normativa di riferimento

- 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, del 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»;
- Legge n. 90 del 28 giugno 2024, «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici»
- D.Lgs 4 settembre 2024, n. 138 Recepimento della direttiva (UE) 2022/2555, 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

Attività 7.1 - Governance della cybersicurezza

La governance della cybersicurezza è un sistema di obiettivi, ruoli, responsabilità, politiche, processi e procedure volti a garantire la sicurezza dei dati e la continuità operativa di un'organizzazione o un insieme di organizzazioni (per esempio Pubbliche Amministrazioni, le imprese, i professionisti e gli istituti educativi).

Una buona governance della cybersicurezza offre la struttura e la guida necessarie per affrontare le sfide della

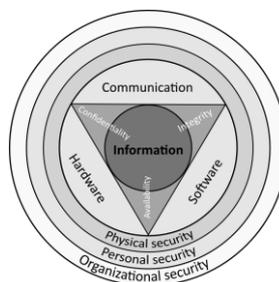


Figura 1: I livelli di protezione dell'informazione

cybersicurezza in modo efficace ed efficiente, delineando responsabilità chiare, definendo obiettivi strategici e garantendo che la cybersicurezza sia integrata in tutti gli aspetti organizzativi. Tale strategia serve, tra l'altro, a definire efficacemente ruoli e responsabilità e ad impostare un'attività di monitoraggio tesa al miglioramento continuo della propria postura di cybersicurezza.

La governance rappresenta uno sforzo collaborativo che coinvolge tutte le parti interessate all'interno di un'organizzazione, garantendo che la cybersicurezza sia integrata in ogni aspetto delle decisioni e operazioni organizzative. In particolare:

- a livello strategico, la direzione e i vertici dell'organizzazione devono collaborare alla definizione di una guida per la gestione della cybersicurezza, inclusa l'identificazione degli obiettivi strategici, la pianificazione delle iniziative prioritarie, la selezione dei modelli ai quali conformarsi;
- a livello tattico, i singoli responsabili di funzione devono promuovere la corretta implementazione della strategia nei propri ambiti, nonché monitorare il raggiungimento degli obiettivi;
- a livello operativo, è altresì importante che i gruppi di lavoro interni e i collaboratori esterni acquisiscano consapevolezza ed esprimano comportamenti coerenti con la strategia.

Una gestione efficace della cybersicurezza richiede un'attenta assegnazione dei ruoli e delle responsabilità all'interno delle organizzazioni. Le azioni chiave per tale assegnazione includono la definizione coerente dei ruoli, la comprensione degli stakeholder coinvolti, l'identificazione delle competenze necessarie e l'adozione di approcci mirati alla dimensione e al contesto specifico dell'organizzazione. Infatti, un sistema di ruoli e responsabilità rappresenta l'insieme di politiche, procedure, regole e definizioni che chiariscono i compiti, i risultati attesi e le responsabilità di ogni individuo o gruppo di individui e concorre alla definizione della struttura organizzativa. Pertanto, l'assegnazione efficace dei ruoli e delle responsabilità contribuisce a promuovere e coltivare una cultura organizzativa improntata alla cybersicurezza.

Questa attività è strettamente connessa alla Linea d'azione istituzionale prevista per ACN:

RA7.1.1 - Giugno 2024 - *L'Agenzia fornisce le Linee guida per l'identificazione di ruoli, competenze e organizzazione per la definizione di un modello di governance della cybersicurezza nella PA, comprensive delle linee di implementazione da parte delle PA - (ACN) - CAP7.01*

➤ Linee di azione applicabili

Obiettivo 7.1 - Adottare una governance della cybersicurezza diffusa nella PA

RA7.1.1 - Identificazione di un modello, con ruoli e responsabilità, di gestione della cybersicurezza

◆ *Da settembre 2024 - Le singole PA definiscono il modello unitario, assicurando un coordinamento centralizzato a livello dell'istituzione, di governance della cybersicurezza - CAP7.PA.01*

◆ *Da dicembre 2024 - Le PA adottano un modello di governance della cybersicurezza - CAP7.PA.02*

◆ *Da dicembre 2024 - Le PA nominano i Responsabili della cybersicurezza e delle loro strutture organizzative di supporto - CAP7.PA.03*

RA7.1.2 - Definizione del framework documentale a supporto della gestione cyber

◆ *Da dicembre 2024 - Le PA formalizzano i processi e le procedure inerenti alla gestione della cybersicurezza - CAP7.PA.04*

Intervento 7.1.1 Adozione del Framework Nazionale per la Cyber Security e la Data Protection (FNCS) – contestualizzazione, definizione dei ruoli, individuazione della struttura per la gestione della cybersicurezza e nomina del responsabile

Alla data di approvazione di questo Piano Triennale, non risultano ancora disponibili le Linee guida per l'identificazione di ruoli, competenze e organizzazione per la definizione di un modello di governance della cybersicurezza nella PA, comprensive delle linee di implementazione da parte delle PA, il cui rilascio da parte di ACN è previsto dal PTI per il mese di Giugno 2024.

In attesa di tale indicazione, e ritenuto l'Ente escluso dal perimetro di applicazione della direttiva NIS2 e della L.90/2024, l'ente si concentrerà sull'implementazione delle misure minime di sicurezza come da documento assunto agli atti con prot. n. 2712 del 7.06.2024.

Modalità di realizzazione: Attuazione Misure Minime di Sicurezza informatica

Responsabilità: RTD

Tempi: tempistiche previste dal documento prot. n. 2712 del 7.06.2024

Risultati attesi: Miglioramento sistema di prevenzione rischi informatici

Intervento 7.1.2 Definizione del framework documentale a supporto della gestione cyber

Nel corso dell'ultimo anno, l'ente ha adottato importanti azioni finalizzate alla corretta gestione dei rischi cyber e per la protezione dei dati personali.

L'ente ha adottato le Misure Minime di sicurezza informatica con rilevazione assunta agli atti con prot. n. 2712 del 7.06.2024. Il documento prevede delle azioni di implementazione da effettuare entro date predeterminate. Nel periodo coperto dal presente Piano, l'ente effettuerà le opportune azioni di monitoraggio finalizzate a presidiare la corretta attuazione delle misure pianificate.

L'ente ha implementato una strategia di backup attraverso tre soluzioni:

- Software dedicato con 3 copie complete di backup e 3 fasi incremental;
- Backup attraverso piattaforma cloud Nextcloud;
- PC NAS che esegui 2 copie complete di backup settimanalmente.

Con Determinazione del Direttore Generale n. 6 del 22.01.2024 è stato approvato il "Disciplinare sull'uso di internet, posta elettronica e altri strumenti informatici", diffuso tra tutti i dipendenti.

Per quanto riguarda le politiche di tutela della protezione dei dati personali, l'ente ha:

- nominato il Data Protection Officer (DPO) con determinazione del Direttore Generale N. 363 del 29.12.2022;
- approvato il registro dei trattamenti con determinazione del Direttore Generale n. 73 del 15.06.2023;
- approvato la procedura per la gestione di data breach e istituito il Registro data breach ai sensi del Regolamento (UE) n.679/2016 con determinazione del Direttore Generale n. 3 del 16.01.2024;
- redatto le informative privacy distinte per categorie di destinatari e pubblicate nell'apposita sezione del sito internet dell'ente;
- nominato i responsabili esterni al trattamento dei dati ai sensi dell'art. 28 del GDPR;
- redatto i documenti di valutazione di impatto sulla protezione dei dati per alcune tipologie di trattamento.

Quale ulteriore azione a supporto della gestione del rischio cyber, l'ente provvederà a redigere un documento di dettaglio dedicato alla descrizione del sistema di backup.

Modalità di realizzazione: Descrizione del sistema di backup

Responsabilità: RTD

Tempi: entro giugno 2025

Risultati attesi: Redazione documento descrittivo del sistema di backup.

Attività 7.2 Promuovere attività legate al miglioramento della cultura cyber delle Amministrazioni

Obiettivo 7.5 - Implementare attività strutturate di sensibilizzazione cyber del personale

RA7.5.1 - Definizione dei piani di formazione in ambito cyber

◆ *Da giugno 2024 - Le PA promuovono l'accesso e l'utilizzo di attività strutturate di sensibilizzazione e formazione in ambito cybersicurezza - CAP7.PA.17*

◆ *Da dicembre 2024 - Le PA definiscono piani di formazione inerenti alla cybersecurity, diversificati per ruoli, posizioni organizzative e attività delle risorse dell'organizzazione - CAP7.PA.18*

RA7.5.2 - Adozione di strumenti atti alla formazione in ambito cyber

◆ *Da dicembre 2025 - Le PA realizzano iniziative per verificare e migliorare la consapevolezza del proprio personale – CAP7.PA.19*

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

◆ Dicembre 2025 - Le PA, sulla base delle proprie esigenze, partecipano ai corsi di formazione base ed avanzato erogati dal CERT-AgID – CAP7.PA.22

L'Ente promuove la formazione del personale in ambito cyber diffondendo tempestivamente informazioni in merito agli strumenti formativi disponibili. Sono invitati a iscriversi alle varie risorse formative (Syllabus, Accademia dei comuni digitali, eventuali strumenti messi a disposizione da AgID, ACN o altro) sia il personale operativo in ambito ICT e cybersicurezza che il personale apicale, in modo da stimolare una crescita della consapevolezza del rischio cyber a livello dell'intera struttura.

L'attività di formazione riguarda anche l'RTD, che potrà accedere anche alle risorse dedicate disponibili sul portale ReTeDigitale (<https://www.retedigitale.gov.it/>).

Tale azione sarà realizzata mediante l'intervento 1.2.1 Pianificazione della formazione in ambito digitale.

Attività 7.3 Implementare soluzioni di difesa proattive**Obiettivo 7.6 - Contrastare il rischio cyber attraverso attività di supporto proattivo alla PA****RA7.6.1 - Distribuzione di Indicatori di Compromissione alle PA**

◆ Da febbraio 2024 - Le PA dovranno dotarsi degli strumenti idonei all'acquisizione degli IoC ed accreditarsi al CERT-AgID - CAP7.PA.20

RA7.6.2 - Fornitura di strumenti funzionali all'esecuzione dei piani di autovalutazione dei sistemi esposti

◆ Da ottobre 2024 - Le PA dovranno usufruire degli strumenti per la gestione dei rischi cyber messi a disposizione dal CERT-AgID - CAP7.PA.21

Intervento 7.3.1 Adozione degli Indicatori di Compromissione

L'Ente procede ad iscriversi al servizio di comunicazione del flusso di Indicatori di compromissione (Feed IoC) del CERT-AgID per la protezione dell'Amministrazione da minacce Malware e Phishing. Il flusso viene integrato negli strumenti di protezione già in uso (firewall, antivirus, antimalware, sistemi di monitoraggio della rete etc).

Modalità di realizzazione: Configurazione degli strumenti di protezione in uso per ricevere e integrare automaticamente il flusso degli Indicatori di Compromissione, implementazione di procedure di aggiornamento periodico e automatizzato per assicurare la tempestività nella rilevazione e mitigazione delle minacce, monitorare i log e reagire a eventuali rilevamenti di

compromissione e registrazione al servizio Feed IoC del CERT-AgID attraverso i canali ufficiali

Responsabilità: RTD

Tempi: entro dicembre 2025

Risultati attesi: Maggiore capacità di prevenzione e rilevamento delle minacce informatiche, in particolare malware e phishing, riduzione dei tempi di risposta a incidenti di sicurezza, miglioramento generale della sicurezza