

# Piano triennale per l'informatica [ 2024-2026 ]

The logo for ATER (Associazione Nazionale per la Trasmissione Elettronica) is displayed in a bold, black, stylized font. The letters are interconnected, with the 'A' and 'T' sharing a common horizontal base, and the 'E' and 'R' also sharing a common base. The 'R' has a distinctive curved tail that loops back towards the 'E'.

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

**ATER Potenza**  
Via Manhes, 33  
85100 – Potenza  
Pec: [info@pec.aterpotenza.it](mailto:info@pec.aterpotenza.it)  
Email: [info@aterpotenza.it](mailto:info@aterpotenza.it)



## Sommario

INTRODUZIONE.....	4
Cos'è il Piano Triennale .....	4
Finalità del piano triennale.....	4
Strategia.....	4
Principi guida .....	4
L'ecosistema digitale attuale dell'Ente.....	7
Trend tecnologici in atto .....	8
Ufficio per la Trasformazione Digitale (UTD) .....	9
Competenze digitali.....	9
Obiettivi e spesa complessiva prevista .....	10
Guida al Piano.....	11
Legenda dei simboli sulle linee d'azione dell'ente.....	11
Componenti tecnologiche .....	12
Contesto normativo.....	13
Obiettivo 3.2 – Migliorare la capacità di generare ed erogare servizi digitali .....	14
Formazione, gestione e conservazione dei documenti informatici .....	15
Contesto normativo.....	15
Risultati Attesi - OB 3.3.....	16
RA3.3.1 - Monitorare l'attuazione delle linee guida .....	16
Obiettivo 3.3 – Consolidare l'applicazione delle Linee guida per la formazione, gestione e conservazione documentale .....	16
Piattaforme.....	17
Piattaforme nazionali che erogano servizi a cittadini/imprese o ad altre PA.....	17
Dati e Intelligenza Artificiale .....	21
Open data e data governance .....	21
Contesto normativo e strategico.....	21
Risultati attesi - OB 5.3 .....	22
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.....	22
Obiettivo 5.3 – Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati.....	22
Intelligenza artificiale per la Pubblica Amministrazione .....	23
Contesto normativo e strategico.....	24
Risultati attesi - OB 5.4 .....	24
RA5.4.1 - Linee guida per promuovere l'adozione dell'IA nella Pubblica Amministrazione.....	24
RA5.4.2 - Linee guida per il procurement di IA nella Pubblica Amministrazione .....	25
RA5.4.3 - Linee guida per lo sviluppo di applicazioni di IA per la Pubblica Amministrazione.....	25
RA5.4.4 - Realizzazione di applicazioni di IA a valenza nazionale .....	25
Obiettivo 5.4 – Aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale.....	25
Risultati attesi - OB 5.5 .....	25
RA5.5.1 - Basi di dati nazionali strategiche .....	25
Obiettivo 5.5 – Dati per l'intelligenza artificiale.....	26
Infrastrutture.....	27
Infrastrutture digitali e Cloud .....	27

Contesto normativo e strategico.....	27
Risultati attesi - OB 6.1 .....	28
RA6.1.1 - Numero di amministrazioni migrate.....	28
Obiettivo 6.1 – Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la strategia «Cloud Italia» e migrando verso infrastrutture e servizi cloud qualificati (incluso PSN).....	29
Il sistema pubblico di connettività .....	30
Contesto normativo e strategico.....	30
Risultati attesi - OB 6.2 .....	30
RA6.2.1 - Rete di connettività.....	31
Obiettivo 6.2 – Garantire alle amministrazioni la disponibilità della connettività SPC .....	31
Sicurezza informatica .....	32
Contesto normativo e strategico.....	32
Risultati attesi - OB 7.1 .....	33
RA7.1.1 - Identificazione di un modello, con ruoli e responsabilità, di gestione della cybersicurezza .....	33
RA7.1.2 - Definizione del framework documentale a supporto della gestione cyber .....	33
Obiettivo 7.1 – Adottare una governance della cybersicurezza diffusa nella PA .....	33
Risultati attesi - OB 7.2 .....	34
RA7.2.1 - Definizione del framework documentale a supporto del processo di approvvigionamento IT .....	34
RA7.2.2 - Definizione delle modalità di monitoraggio del processo di approvvigionamento IT ...	34
Obiettivo 7.2 – Gestire i processi di approvvigionamento IT coerentemente con i requisiti di sicurezza definiti.....	34
Risultati attesi - OB 7.3 .....	35
RA7.3.1 - Definizione del framework per la gestione del rischio cyber .....	35
RA7.3.2 - Definizione delle modalità di monitoraggio del rischio cyber .....	35
Obiettivo 7.3 – Gestione e mitigazione del rischio cyber .....	35
Risultati attesi - OB 7.4 .....	35
RA7.4.1 - Definizione del framework documentale relativo alla gestione degli incidenti.....	35
RA7.4.2 - Definizione delle modalità di verifica e aggiornamento dei piani di risposta agli incidenti.....	36
Obiettivo 7.4 – Potenziare le modalità di prevenzione e gestione degli incidenti informatici.....	36
Risultati attesi - OB 7.5 .....	37
RA7.5.1 - Definizione dei piani di formazione in ambito cyber.....	37
RA7.5.2 - Adozione di strumenti atti alla formazione in ambito cyber.....	37
Obiettivo 7.5 – Implementare attività strutturate di sensibilizzazione cyber del personale .....	37
Risultati attesi - OB 7.6 .....	38
RA7.6.1 - Distribuzione di Indicatori di Compromissione alle PA .....	38
RA7.6.2 - Fornitura di strumenti funzionali all’esecuzione dei piani di autovalutazione dei sistemi esposti .....	38
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 .....	38
Obiettivo 7.6 – Contrastare il rischio cyber attraverso attività di supporto proattivo alla PA .....	39
CONCLUSIONI .....	40
Appendice - Glossario.....	40

## INTRODUZIONE

### Cos'è il Piano Triennale

Il Piano Triennale per l'informatica nella Pubblica Amministrazione 2024-2026 indica le linee di azione per promuovere la trasformazione digitale del settore pubblico e del Paese.

Il nuovo Piano presenta, rispetto alle precedenti edizioni, dei cambiamenti nella sua struttura e approfondisce alcuni contenuti per sostenere in modo efficace le pubbliche amministrazioni nel processo di implementazione e gestione dei servizi digitali.

Maggiori dettagli si possono trovare all'indirizzo <https://pianotriennale-ict.italia.it/>.

### Finalità del piano triennale

Gli scopi del Piano Triennale sono definiti principalmente nelle seguenti norme:

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

**art. 14-bis Agenzia per l'Italia digitale (AGID);**

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

### Strategia

- 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.



### 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.

PRINCIPI GUIDA	DEFINIZIONI	RIFERIMENTI NORMATIVI	ATTUAZIONE
1. Digitale e mobile come prima opzione ( <i>digital &amp; mobile first</i> )	Le pubbliche amministrazioni devono erogare i propri servizi pubblici in digitale e fruibili su dispositivi mobili, considerando alternative solo in via residuale e motivata, attraverso la « <i>riorganizzazione strutturale e gestionale</i> » dell'ente ed anche con una « <i>costante semplificazione e reingegnerizzazione dei processi</i> »	Art.3-bis Legge 241/1990 Art.1 c.1 lett. a) D.Lgs. 165/2001 Art.15 CAD Art.1 c.1 lett. b) Legge 124/2015 Art.6 c.1 DL 80/2021	Nel 2026 sarà acquistato e messo in funzione il software (e-Housing Plus) per l'erogazione di servizi alla propria utenza con app mobile.
2. cloud come prima opzione ( <i>cloud first</i> )	Le pubbliche amministrazioni, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano il paradigma cloud e utilizzano esclusivamente infrastrutture digitali adeguate e servizi <i>cloud</i> qualificati secondo i criteri fissati da ACN e nel quadro del SPC	Art.33-septies Legge 179/2012 Art. 73 CAD	Entro il 2025 sarà completata la valutazione circa l'adozione del cloud per tutte le proprie applicazioni.
3. interoperabile <i>by design</i> e <i>by default</i> ( <i>API-first</i> )	I servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e attraverso processi digitali collettivi, esponendo opportuni <i>e-Service</i> , a prescindere dai canali di erogazione del servizio che sono individuati logicamente e cronologicamente dopo la progettazione dell'interfaccia API;	Art.43 c.2 dPR 445/2000 Art.2 c.1 lett.c) D.Lgs 165/2001 Art.50 c2, art.50-ter e art.64-bis c.1-bis CAD	Entro il 2026 si avvierà un processo per verificare se le software-house fornitrici hanno messo in piedi modelli di sviluppo software "API-first" ovvero applicazioni concettualizzate e costruite come una continua interconnessione di servizi interni ed esterni resa possibile attraverso API; superando il vecchio modello Code-first in cui ogni applicazione è sviluppata mettendo assieme pezzi di codice sorgente. Nel modello Code-first i problemi sono frequenti e gli aggiornamenti e le evoluzioni del software spesso vengono resi difficili dalle limitazioni tecnologiche proprie di questo tipo di sviluppo.
4. accesso esclusivo mediante identità digitale ( <i>digital identity only</i> )	Le pubbliche amministrazioni devono adottare in via esclusiva sistemi di identità digitale definiti dalla normativa	Art.64 CAD Art. 24, c.4, DL 76/2020 Regolamento EU 2014/910 «eIDAS»	Al Portale Appalti già si accede con SPID o CIE e anche al software "e-Housing Plus", di cui al punto 1, si accederà con identità digitale.
5. servizi inclusivi, accessibili e centrati sull'utente ( <i>user-centric</i> )	Le pubbliche amministrazioni devono progettare servizi pubblici che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo	Legge 4/2004 Art.2 c.1, art.7 e art.53 CAD Art.8 c.1 lettera c) e lett.e), ed art.14 c.4-bis D.Lgs 150/2009	e-Housing Plus sarà implementato con questo tipo di approccio
6. dati pubblici un bene comune ( <i>open data by design e by default</i> )	Il patrimonio informativo della Pubblica Amministrazione è un bene fondamentale per lo sviluppo del Paese e deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile	Art.50 c.1 e c.2-bis, art.50- quater e art.52 c.2 CAD D.Lgs 36/2006 Art.24-quater c.2 DL90/2014	<i>Open data by design e by default</i> obbligano, ovviamente, l'Azienda a predisporre una valutazione di impatto privacy ogni volta che il trattamento di dati, operato dal servizio, comporta rischi elevati per la privacy delle persone. L'utilizzo di software e applicativi di aziende terze comporta che debba essere l'azienda terza a dover sviluppare le valutazioni del rischio dell'uso dell'applicativo, che ovviamente va disegnato in maniera conforme al regolamento. Valutazione che dovrà essere opportunamente documentata al titolare del trattamento.
7. concepito per la sicurezza e la protezione dei dati personali ( <i>data protection by design e by default</i> )	I servizi pubblici devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali	Regolamento EU 2016/679 «GDPR» DL 65/2018 «NIS» DL 105/2019 «PNSC» DL 82/2021 «ACN»	Vedi punto 6
8. <i>once only</i> e concepito come transfrontaliero	Le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite, devono dare accesso ai loro fascicoli digitali e devono rendere disponibili a livello transfrontaliero i servizi pubblici rilevanti	Art.43, art.59, art.64 e art.72 DPR 445/2000 Art.15 c.3, art.41, art.50 c.2 e c.2-ter, e art.60 CAD Regolamento EU 2018/1724 «single digital gateway» Com.EU (2017) 134 «EIF»	Vedi punto 1
9. apertura come prima opzione ( <i>openness</i> )	Le pubbliche amministrazioni devono tenere conto della necessità di prevenire il rischio di <i>lock-in</i> nei propri servizi, prediligere l'utilizzo di <i>software</i> con codice aperto o di <i>e-service</i> e, nel caso di <i>software</i> sviluppato per loro conto, deve essere reso disponibile il codice sorgente, nonché promuovere	Art.9, art.17 c.1 ed art.68-69 CAD Art.1 c.1 D.Lgs 33/2013 Art.30 D.Lgs 36/2023	Sarà chiesto alle software-hose di rendere disponibile il codice sorgente dei software in uso nell'Azienda.

	l'amministrazione aperta e la condivisione di buone pratiche sia amministrative che tecnologiche		
10. sostenibilità digitale	Le pubbliche amministrazioni devono considerare l'intero ciclo di vita dei propri servizi e la relativa sostenibilità economica, territoriale, ambientale e sociale, anche ricorrendo a forme di aggregazione	Art.15 c.2-bis CAD Art.21 D.lgs. 36/2023 Regolamento EU 2020/852 «principio DNSH»	
11. sussidiarietà, proporzionalità e appropriatezza della digitalizzazione	I processi di digitalizzazione dell'azione amministrativa coordinati e condivisi sono portati avanti secondo i principi di sussidiarietà, proporzionalità e appropriatezza della digitalizzazione, ovvero lo Stato deve intraprendere iniziative di digitalizzazione solo se sono più efficaci di quelle a livello regionale e locale, e in base alle esigenze espresse dalle amministrazioni stesse, limitandosi negli altri casi a quanto necessario per il coordinamento informatico dei dati, e al tempo stesso le singole amministrazioni devono garantire l'appropriatezza delle iniziative di digitalizzazione portate avanti autonomamente, cioè in forma non condivisa con altri enti al livello territoriale ottimale rispetto alle esigenze preminenti dell'azione amministrativa e degli utenti dei servizi pubblici.	Art.5, 117 e 118 Costituzione Art.14 CAD	

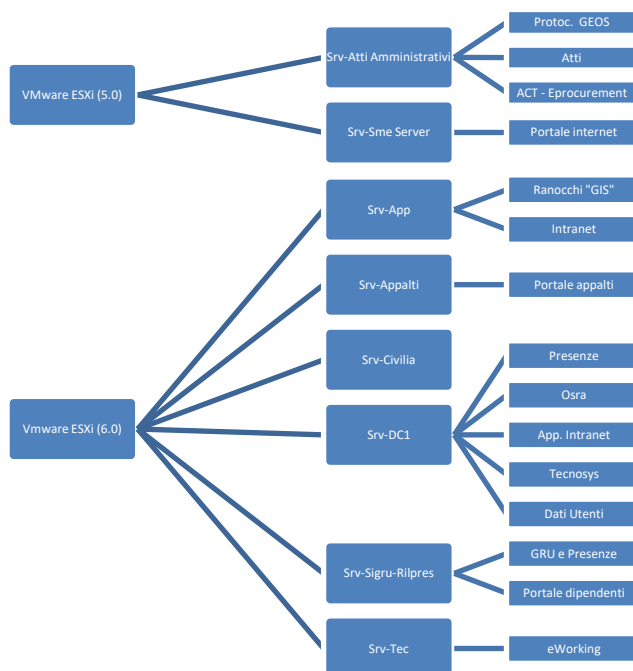
Tabella 1 - Principi guida del Piano triennale

## L'ecosistema digitale attuale dell'Ente

L'infrastruttura informatica dell'ATER di Potenza è basata su due server farm, entrambi ubicati in via Manhes (sede dell'ente).

L'infrastruttura è basata su una architettura a 2 nodi fisici che ospitano le macchine virtuali gestite da VMware ESXi.

Sulla stessa rete dedicata sono presenti anche 4 NAS che gestiscono i backup locali e un centro di aggiornamento dei file degli utenti del dominio.



La replica sul sito di Disaster Recovery viene gestita mediante Vmware Replication per le macchine virtuali, tramite rsync per il filesystem.

Le postazioni di lavoro fisse sono circa 50, tutte con S.O. Windows 10 e Windows 11 a 64bit e sono gestite, insieme alle utenze, da un dominio Windows, Active Directory Domain Services.

La connettività è gestita da Vodafone per la rete VOIP e i per le connessioni internet in uscita e da Fastweb per le connessioni al portale web aziendale.

La sicurezza di rete viene gestita da due firewall (TpLink e Sophos) e quella dei singoli PC e dall'Antivirus Webroot.

### Posta Elettronica

Da ottobre 2022 è stato abbandonato il vecchio server-mail Linux (Sme Server) e si è passati al servizio Workspace offerto da Google con 40 caselle di posta su Gmail, uno spazio di 30 Gb di archiviazione, un servizio cloud e una serie di applicazioni utili come la gestione delle riunioni in web conference.

Gli applicativi per la gestione dei processi sono tutti completamente integrati e web-based e sono forniti dalle softwarehouse Publisys S.p.A. e Tecnosys Italia SpA.

### Gestione documentale

Il protocollo informatico, la fascicolazione elettronica e l'Albo pretorio sono gestiti con il software "eWorking", così come tutta la gestione del patrimonio abitativo e dell'utenza.

Gli atti di volontà (delibere e determinazioni dirigenziali) sono attualmente gestiti all'interno della intranet per la numerazione, registrazione, pubblicazione e conservazione dei files mentre tutto l'iter autorizzativo e ancora in fase analogica (firme su base cartacea).

### Gestione giuridica ed economico/finanziaria

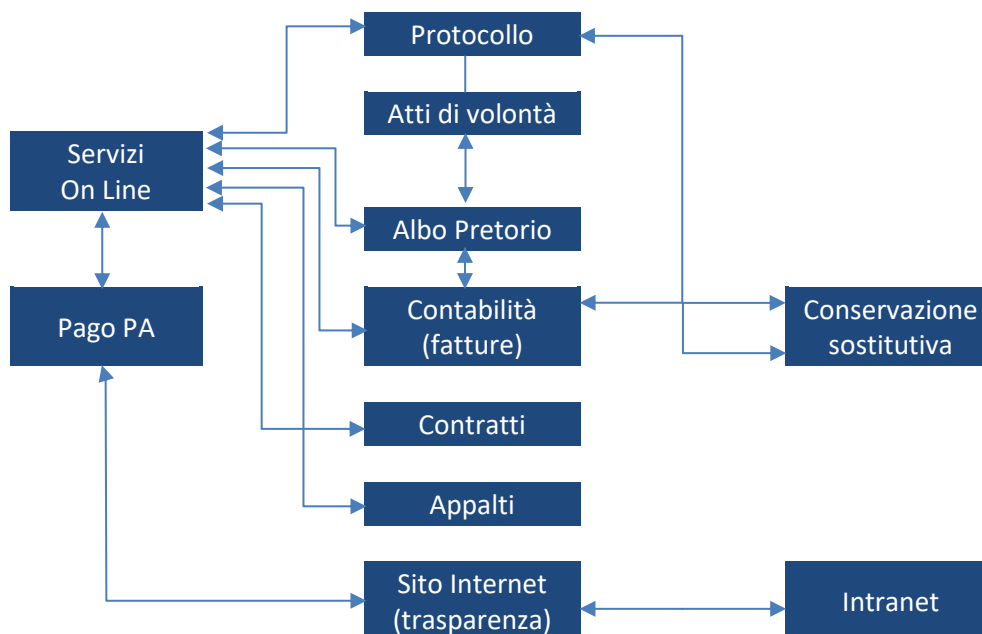
La gestione giuridica ed economica del personale e il portale per la gestione degli appalti, sono gestiti da software dedicati di Publisys, mentre la contabilità finanziaria e patrimoniale, ancora gestita su più software (Ranocchi "GIS", Civilia).

### Portale web

Il sito ufficiale e il sito intranet sono stati sviluppati internamente e sono essenzialmente di tipo statico.

All'interno del sito internet non sono presenti servizi di tipo on-line, tranne per la gestione delle Gare (con la partecipazione diretta degli operatori economici).

Nel corso dell'anno 2024 è stata implementata la modulistica in appositi pdf compilabili online.



### Trend tecnologici in atto

#### Accessi on line

E' prevista un'evoluzione tecnologica al fine di integrare l'accesso ai servizi on line (SPID e CdIE) con tecnologia OpenID Connect che rappresenta un salto di qualità dal punto di vista della sicurezza delle transazioni in ottica di standardizzare l'accesso ai servizi online dei cittadini verso la Pubblica Amministrazione.

#### Gestione documentale

E' in fase di collaudo ed entrerà in funzione nel 2025, un nuovo software per la gestione documentale, denominato "Atti di Volontà", all'interno del portale eWorking, che renderà completamente digitale tutto il processo documentale e si integrerà sia con il gestionale del patrimonio/utenza, con il protocollo, con l'Albo Pretorio e con la contabilità armonizzata.

#### Gestione economica

Sempre nel 2025 la gestione della contabilità finanziaria e patrimoniale migrerà nel nuovo gestionale di Contabilità Armonizzata all'interno del portale eWorking.

### Portale web

Il sito internet ufficiale, entro la fine del 2025, sarà interamente gestito da un content management system (CMS), quindi con una gestione decentrata dei contenuti e un adeguamento alle normative in termini di usabilità e accessibilità come indicate da Agid.



All'interno del sito internet saranno previsti, entro il 2026, servizi on-line rivolti principalmente agli utenti (inquilini) per la consultazione dei propri documenti tecnici/amministrativi, a tutti i cittadini per le richieste che attualmente sono disponibili soltanto su modulistica statica e per l'accesso agli atti (entro il 2027).

E' in previsione l'upgrade della connettività gestita da Vodafone tramite fibra ottica a 1000Mbps in uscita (entro il 2026).

Tutto il percorso di innovazione tecnologica si completerà con il miglioramento della standardizzazione delle modalità operative degli uffici conformemente allo standard prestabilito nel Manuale di Gestione per la Qualità UNI EN ISO 9001-2015.

### Ufficio per la Trasformazione Digitale (UTD)

Con delibera n.65 del 17/10/2017 è stato istituito l'Ufficio per la Transizione al Digitale di cui fanno parte:

- il responsabile (RTD) Vincenzo Pignatelli - vincenzo.pignatelli@aterpotenza.it-;
- il collaboratore Vito Colangelo - vito.colangelo@aterpotenza.it -.

Il Piano Triennale per l'Informatica di AgID 2024 – 2026, pubblicato il 12/02/2024, pone l'accento sul ruolo del RTD e dell'UTD per perseguire una concreta inversione del paradigma lavorativo nella PA.

La programmazione del Piano Triennale per l'Informatica deve essere resa coerente con la specifica allocazione di azioni nelle Missioni e Programmi del Piano Integrato di Attività e Organizzazione (PIAO) mediante:

- ✓ obiettivi di mappatura e digitalizzazione dei processi;
- ✓ attivazione dei servizi online;
- ✓ sensibilizzazione dell'utenza all'impiego dell'identità digitale;
- ✓ utilizzo dei servizi in cloud (ove possibile);
- ✓ potenziamento delle infrastrutture;
- ✓ ridurre drasticamente l'utilizzo della carta.

Tutte queste azioni integrano una maggiore tracciabilità e trasparenza dei processi per tipologia di procedimento, rispettivamente al fine della prevenzione dalla corruzione e al fine di rendere realmente funzionale l'assolvimento dell'obbligo di pubblicazione nella sezione "Amministrazione trasparente" del sito web istituzionale, dei contenuti obbligatori ai sensi dell'art. 35 del D.Lgs.33/2013, (tipologie dei procedimenti), distribuendo i relativi contenuti in specifiche pagine web che guidino la navigazione dell'utente verso un'esperienza di fruizione dei servizi on line realmente intuitiva ed efficace.

In sede di PEG, i Programmi dovranno essere declinati in specifici obiettivi di qualità, i cui indicatori di produttività dovranno consentire di misurare il grado di digitalizzazione dei processi raggiunto, oltre al grado di soddisfazione dell'utenza.

### Competenze digitali

Tra i fattori abilitanti dei processi di trasformazione sono imprescindibili le competenze digitali. Il fabbisogno di competenze digitali nella PA riguarda tutti i dipendenti, compreso i dirigenti.

L'ATER Potenza ha aderito all'iniziativa del Dipartimento della Funzione Pubblica "Syllabus", il portale che mira a consentire a tutti i dipendenti l'accesso diretto a percorsi formativi sulle competenze con una modalità e-learning.

Sono stati abilitati tutti i dipendenti alla data dell'iscrizione (n.42) dei quali il 92% si è registrato.

Circa il 30% ha iniziato il percorso formativo e una media del 43 % ha concluso il percorso.

L'obiettivo del 2025 è quello di superare la soglia dell'70% della conclusione dei percorsi formativi assegnati.

Abilitati: 42    Donne: 21 (50%)    Uomini: 21 (50%)



Transizione digitale  
 Competenze digitali per la PA

Competenza	Abilitati
▼ Gestire dati, informazioni e contenuti digitali	42
▼ Produrre, valutare e gestire documenti informatici	42
▼ Conoscere gli Open Data	42
▼ Comunicare e condividere all'interno dell'amministrazione	42
▼ Comunicare e condividere con cittadini, imprese ed altre PA	42
▼ Proteggere i dispositivi	42
▼ Proteggere i dati personali e la privacy	42
▼ Conoscere l'identità digitale	42
▼ Erogare servizi on-line	42
▼ Conoscere gli obiettivi della trasformazione digitale	42
▼ Conoscere le tecnologie emergenti per la trasformazione digitale	42
Totale	

	Abilitati	Registrati	Percorsi iniziati	Percorsi conclusi	Percorsi scaduti
	42	39 (92.86%)	13 (30.95%)	21 (50%)	0 (0%)
	42	39 (92.86%)	12 (28.57%)	18 (42.86%)	0 (0%)
	42	39 (92.86%)	11 (26.19%)	19 (45.24%)	0 (0%)
	42	39 (92.86%)	12 (28.57%)	19 (45.24%)	0 (0%)
	42	39 (92.86%)	15 (35.71%)	18 (42.86%)	0 (0%)
	42	39 (92.86%)	11 (26.19%)	18 (42.86%)	0 (0%)
	42	39 (92.86%)	13 (30.95%)	18 (42.86%)	0 (0%)
	42	39 (92.86%)	12 (28.57%)	17 (40.48%)	0 (0%)
	42	39 (92.86%)	8 (19.05%)	21 (50%)	0 (0%)
	42	39 (92.86%)	16 (38.10%)	13 (30.95%)	0 (0%)
	42	39 (92.86%)	12 (28.57%)	16 (38.10%)	0 (0%)
Totale			135	198	0

## Obiettivi e spesa complessiva prevista

Gli obiettivi che l'azienda si è prefissa di realizzare nel triennio di riferimento sono i seguenti:

- **anno 2024:** digitalizzare dell'intero processo documentale di determinazioni e delibere (che è parzialmente digitalizzato), ivi compreso il protocollo digitale e l'albo pretorio on-line, che si concluderà entro l'anno con un costo di € 8.090,00; avvio di un nuovo software integrato di contabilità e gestione del Bilancio armonizzato per un costo di € 10.860,00; implementazione di tutta la gestione del personale sia dal punto di vista economico che giuridico attraverso un "Portale del dipendente" il cui costo di € 70.240,00 sarà spalmato nel quadriennio 2024-2028;
- **anno 2025:** implementazione del portale internet istituzionale attraverso il passaggio all'ambiente CMS secondo la Circolare n.61/2013 del 29 marzo 2013 dell'Agenzia per l'Italia Digitale in materia di accessibilità dei siti web delle pubbliche amministrazioni e le "Linee guida per i siti web della PA" (art. 4 della Direttiva 8/09 del Ministro per la pubblica amministrazione e l'innovazione) con un costo presumibile di € 25.000,00;
- **anno 2026:** acquisto e messa in funzione di un software (*e-Housing Plus*) per la gestione degli accessi degli utenti al proprio stato delle pratiche e dei pagamenti con annessa possibilità di richieste di "Prenotazioni", "Consultazioni", Avvio procedimento" e "Segnalazioni" sia tramite il portale istituzionale che con app mobile per un costo complessivo di € 12.500,00.

Annualità	Spesa complessiva
Anno 2024	€ 51.430.00
Anno 2025	€ 37.587.00
Anno 2026	€ 25.087.00

## Guida al Piano

Per rendere più leggibile il documento, ogni unità minima codificata (linea d'azione) comprende le seguenti componenti:

- ✓ **Codice:** il codice della linea d'azione definito da AGID/MiD;
- ✓ **Oggetto:** la descrizione dell'azione da compiere o della richiesta specifica indicata da AGID/MiD;
- ✓ **Periodo:** la data ufficiale di partenza o di fine (scadenza) del progetto/attività descritta del campo oggetto;
- ✓ **Azione dell'Ente:** campo descrittivo che indica come l'ente ha raggiunto, sta raggiungendo o raggiungerà l'obiettivo;
- ✓ **Tempistiche di realizzazione e deadline:** programmazione rispetto la linea d'azione specificata;
- ✓ **Percentuale di avanzamento:** stato di avanzamento, in percentuale, della linea d'azione;
- ✓ **Budget previsto e budget speso:** budget che l'ente aveva previsto e quello realmente speso;
- ✓ **Capitoli di spesa:** i riferimenti specifici di bilancio dove i budget sono stati collocati;
- ✓ **Percentuale di completamento:** percentuale di avanzamento della specifica azione rispetto alle scadenze o alla pianificazione dell'ente;
- ✓ **Strutture responsabili e attori coinvolte:** eventuali strutture interne o esterne coinvolte nel completamento della linea d'azione;

## Legenda dei simboli sulle linee d'azione dell'ente.

Ogni linea d'azione può essere catalogata secondo il seguente schema:

<input type="radio"/>	<b>Da gestire</b> L'ente non ha ancora preso in gestione la linea d'azione indicata	
<input type="radio"/>	<b>Conclusa con successo</b> La linea d'azione è stata sviluppata con successo dal vostro ente	
<input type="radio"/>	<b>Non completata</b> L'ente non ha completato per tempo l'azione richiesta	
<input type="radio"/>	<b>In corso di attuazione</b> La linea d'azione è in fase di attuazione da parte del vostro ente	
<input type="radio"/>	<b>Pianificata</b> La linea d'azione è stata pianificata con successo dal vostro ente	
<input type="radio"/>	<b>In attesa di sblocco</b> La linea d'azione è attualmente bloccata da altre istituzioni	
<input type="radio"/>	<b>Non di competenza dell'ente</b> La linea d'azione non è di competenza del vostro ente	

Il miglioramento della qualità dei servizi pubblici digitali costituisce la premessa indispensabile per l'incremento del loro utilizzo da parte degli utenti interni ed esterni ad ATER Potenza.

In questo processo di trasformazione digitale è essenziale che i servizi abbiano un chiaro valore per l'utente, il valore pubblico dichiarato anche all'interno del PIAO; questo obiettivo richiede un approccio multidisciplinare nell'adozione di metodologie e tecniche interoperabili per la realizzazione di un servizio. La qualità finale dei servizi, così come il costo complessivo del servizio, non può infatti prescindere da un'attenta analisi dei molteplici livelli, tecnologici e organizzativi interni, che strutturano l'intero processo della prestazione erogata, semplificandoli e facilitandone la fruizione.

Ciò implica un'adeguata semplificazione dei processi interni, coordinata dal Responsabile per la transizione al digitale, con il necessario supporto di efficienti procedure digitali.

E' necessario migliorare la capacità di generare ed erogare servizi di qualità attraverso:

- un utilizzo più consistente di soluzioni *Software as a Service* già esistenti;
- il riuso e la condivisione di software e competenze tra le diverse amministrazioni, in particolare tra i diversi ATER provinciali o similari;
- l'adozione di modelli e strumenti validati e a disposizione di tutti;
- il costante monitoraggio dei propri servizi online;
- l'incremento del livello di accessibilità dei servizi erogati tramite siti web e app mobili;
- lo scambio di buone pratiche tra le diverse amministrazioni, da attuarsi attraverso la definizione, la modellazione e l'organizzazione di comunità di pratica.

Gli strumenti per la condivisione di conoscenza e di soluzioni a disposizione delle amministrazioni sono:

- le linee guida emanate ai sensi dell'art. 71 del CAD;
- <https://designers.italia.it>;
- <https://developers.italia.it/>
- <https://forum.italia.it/>

Nel caso i servizi richiedano un accesso da parte dell'utente esterno, è necessario che sia consentito attraverso un sistema di autenticazione previsto dal CAD, assicurando l'accesso tramite l'identità digitale SPID/eIDAS.

Allo stesso modo, se è richiesto un pagamento, tale servizio dovrà essere reso disponibile anche attraverso il sistema di pagamento pagoPA.

## Contesto normativo


### Riferimenti normativi italiani:


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


### Riferimenti normativi europei:


1. [Regolamento \(UE\) 2014/910 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno \(in breve eIDAS\)](#)
2. [Regolamento \(UE\) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali \(in breve GDPR\)](#)
3. [European Interoperability Framework -Implementation Strategy \(2017\)](#)
4. [Interoperability solutions for public administrations, businesses and citizens \(2017\)](#)

### Obiettivo 3.2 – Migliorare la capacità di generare ed erogare servizi digitali

Codice	<b>CAP3.PA.09</b>
Oggetto	Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web
Periodo	Entro il 31/03/2025
Tempistica	Dal 30/09/2024 al 31/03/2025
Azione	E' prevista l'implementazione del portale internet istituzionale attraverso il passaggio all'ambiente CMS secondo la Circolare n.61/2013 del 29 marzo 2013 dell'Agenzia per l'Italia Digitale in materia di accessibilità dei siti web delle pubbliche amministrazioni e le "Linee guida per i siti web della PA" (art. 4 della Direttiva 8/09 del Ministro per la pubblica amministrazione e l'innovazione)
% avanzamento	
Budget previsto	€ 25.000,00
Capitolo spesa	11.04.09
% completamento	
Strutture/persone coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP3.PA.11</b>
Oggetto	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.
Periodo	Entro il 23/09/2025
Tempistica	Dal 30/02/2025 al 31/08/2025
Azione	Aggiornare la dichiarazione di accessibilità
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persone coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP3.PA.13</b>
Oggetto	Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web.
Periodo	Entro il 31/03/2025
Tempistica	Dal 01/01/2025 al 31/03/2025
Azione	Gli obiettivi di accessibilità sono in corso di definizione e saranno dettagliati con la messa in funzione del nuovo portale.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persone coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	CAP3.PA.14
Oggetto	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.
Periodo	Entro il 23/09/2025
Tempistica	Dal 01/01/2025 al 31/03/2025
Azione	La dichiarazione di accessibilità sarà possibile dopo la messa in funzione del nuovo portale.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

### Formazione, gestione e conservazione dei documenti informatici

La Pubblica Amministrazione è tenuta ad assicurare la rispondenza alle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agenda per l'Italia Digitale, adottate ai sensi dell'art.71 del CAD, 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 nelle 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»;
- rispetto delle misure minime di sicurezza ICT, emanate da AGID con circolare del 18 aprile 2017, n. 2/2017;
- rispetto delle in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR);
- trasferimento dei documenti al sistema di conservazione, ai sensi del paragrafo 4 e dell'art. 44, comma 1-bis, del CAD.

### Contesto normativo

*Riferimenti normativi italiani:*

- [Legge 241/1990, Nuove norme sul procedimento amministrativo.](#)
- [DPR 445/2000, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.](#)
- [Decreto legislativo 196/2003, Codice in materia di protezione dei dati personali.](#)
- [Decreto legislativo 42/2004, Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137.](#)
- [Decreto legislativo 82/2005 e ss.mm.ii., Codice dell'amministrazione digitale.](#)
- [Decreto legislativo 33/2013, Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni.](#)

- [Decreto del Presidente della Repubblica 22 febbraio 2013, Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.](#)
- [Circolare 18 aprile 2017, n. 2/2017 dell’Agenzia per l’Italia Digitale, misure minime di sicurezza ICT.](#)
- [Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici \(2021\)](#)
- [Vademecum per l’implementazione delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici, AGID \(2022\).](#)
- [Modelli di interoperabilità tra sistemi di conservazione, AGID \(2022\).](#)
- [La conservazione delle basi di dati, AGID \(2023\)](#)

*Riferimenti normativi europei:*


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

**Risultati Attesi - OB 3.3**

**RA3.3.1 - Monitorare l’attuazione delle linee guida**

- **Target 2024** - Costruzione baseline per il monitoraggio dell’attuazione delle Linee Guida
- **Target 2025** - Il 100% delle amministrazioni devono avere adottato e 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 in «Amministrazione trasparente»
- **Target 2026** - Il 100% delle amministrazioni devono avere adottato e pubblicato il manuale di conservazione e la nomina del Responsabile della conservazione in «Amministrazione trasparente»

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

<b>Codice</b>	<b>CAP3.PA.17</b>
<b>Oggetto</b>	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.
<b>Periodo</b>	Entro il 30/06/2025
<b>Tempistica</b>	Dal 30/06/2024 al 30/06/2025
<b>Azione</b>	E’ stato approvato il manuale di gestione del protocollo in data 09/01/2024 e con delibera n.65/2017 è stato nominato l’ufficio del Responsabile della transizione digitale che si occupa anche della gestione documentale, Il manuale di gestione documentale sarà approvato prima dell’avvio del gestionale documentale.
<b>% avanzamento</b>	70%
<b>Budget previsto</b>	23.000,00
<b>Capitolo spesa</b>	11.04.09 / 12.11.06
<b>% completamento</b>	70%
<b>Strutture/persone coinvolte</b>	UD Risorse / SIA / Resp. Trans. Digitale
<b>Status</b>	



## Piattaforme

---

Come per i precedenti Piani, il Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026 prende in esame l'evoluzione delle piattaforme che offrono funzionalità fondamentali nella digitalizzazione dei processi e dei servizi.

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

#### PagoPA

È la piattaforma che consente ai cittadini di effettuare pagamenti digitali verso la Pubblica Amministrazione in modo veloce e intuitivo ed offre la possibilità ai cittadini di scegliere tra i diversi metodi di pagamento elettronici in base alle proprie esigenze e abitudini.

#### Riferimenti normativi italiani:

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

#### AppIO

È un progetto open source nato con l'obiettivo di mettere a disposizione di enti e cittadini un unico canale da cui fruire di tutti i servizi pubblici digitali, attraverso un'applicazione semplice e intuitiva disponibile sullo smartphone.

#### Riferimenti normativi italiani:

- [Decreto legislativo 7 marzo 2005, n. 82 «Codice dell'amministrazione digitale» \(CAD\), art. 64-bis](#)
- [Decreto-legge 14 dicembre 2018, n. 135, convertito con modificazioni dalla Legge 11 febbraio 2019, n. 12 «Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la Pubblica Amministrazione», art. 8](#)
- [Decreto-legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 «Misure urgenti per la semplificazione e l'innovazione digitale», art. 24, lett. F](#)
- [Decreto-legge 31 maggio 2021, n. 77 «Governance del Piano nazionale di rilancio e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure», art. 42](#)
- [Linee guida AGID per l'accesso telematico ai servizi della Pubblica Amministrazione \(2021\)](#)

#### SEND

La piattaforma SEND - Servizio Notifiche Digitali, di cui all'art. 26 del decreto-legge 76/2020 s.m.i., rende più veloce, economico e sicuro l'invio e la ricezione delle notifiche a valore legale: permette di riceverle, scaricare i documenti notificati e pagare eventuali spese direttamente online su SEND o nell'app IO.

#### Riferimenti normativi italiani:

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

## **SPID**

L'identità digitale SPID è la soluzione che permette di accedere a tutti i servizi online della Pubblica Amministrazione con un'unica identità digitale. Attraverso credenziali classificate su tre livelli di sicurezza, abilita ad accedere ai servizi, ai quali fornisce dati identificativi certificati.

### *Riferimenti normativi italiani:*

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

## **CIE**

l'identità digitale CIE (CIEId) consente la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi.

### *Riferimenti normativi italiani:*

- [Legge 15 maggio 1997, n. 127- Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e di controllo](#)
- [Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa](#)
- [Decreto-legge 31 gennaio 2005, n. 7 - Disposizioni urgenti per l'università e la ricerca, per i beni e le attività culturali, per il completamento di grandi opere strategiche, per la mobilità dei pubblici dipendenti, \(e per semplificare gli adempimenti relativi a imposte di bollo e tasse di concessione, nonché altre misure urgenti\)](#)
- [Decreto Ministeriale del Ministro dell'Interno 23 dicembre 2015 - Modalità tecniche di emissione della Carta d'identità elettronica](#)
- [Decreto-legge 16 luglio 2020, n. 76, Misure urgenti per la semplificazione e l'innovazione digitale](#)
- [Decreto Ministeriale del Ministro dell'Interno 8 settembre 2022 - Modalità di impiego della carta di identità elettronica](#)

#### *Riferimenti normativi europei:*

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

#### **NoiPA**

è la piattaforma realizzata dal Dipartimento dell'Amministrazione Generale del personale e dei servizi (DAG) del Ministero dell'Economia e delle Finanze (MEF) per la gestione del personale della PA.

Offre servizi stipendiali, di Gestione Presenze e tutte le attività di implementazione di nuove soluzioni che rispondono alle linee di sviluppo dell'Amministrazione Digitale, volte a migliorare l'efficienza e l'efficacia della Pubblica Amministrazione e nella gestione delle risorse umane.

#### *Riferimenti normativi italiani:*

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

#### **Fascicolo Sanitario Elettronico**

Il Fascicolo Sanitario Elettronico ha l'obiettivo di garantire la diffusione e l'accessibilità dei servizi di sanità digitale in modo omogeneo e capillare su tutto il territorio nazionale a favore dei cittadini e degli operatori sanitari delle strutture pubbliche, private accreditate e private.


#### *Riferimenti normativi italiani:*


- [Decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla Legge 17 dicembre 2012, n. 221 «Ulteriori misure urgenti per la crescita del Paese»](#)
- [Decreto del Presidente del Consiglio dei Ministri 29 settembre 2015, n. 178 «Regolamento in materia di fascicolo sanitario elettronico»](#)
- [Legge 11 dicembre 2016, n. 232 «Bilancio di previsione dello Stato per l'anno finanziario 2017 e bilancio pluriennale per il triennio 2017-2019»](#)
- [Decreto-legge 19 maggio 2020, n. 34, convertito con modificazioni dalla Legge 17 luglio 2020, n. 77 «Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19»](#)
- [Decreto-legge 28 ottobre 2020, n. 137, convertito con modificazioni dalla Legge 18 dicembre 2020, n. 176 «Ulteriori misure urgenti in materia di tutela della salute, sostegno ai lavoratori e alle imprese, giustizia e sicurezza, connesse all'emergenza epidemiologica da COVID-19»](#)
- [Decreto-legge 27 gennaio 2022, n. 4, convertito con modificazioni dalla Legge 28 marzo 2022, n. 25 «Misure urgenti in materia di sostegno alle imprese e agli operatori economici, di lavoro, salute e servizi territoriali, connesse all'emergenza da COVID-19, nonché per il contenimento degli effetti degli aumenti dei prezzi nel settore elettrico»](#)

- [Decreto del Ministero dell’Economia e delle Finanze 23 dicembre 2019 «Utilizzo del Fondo per il finanziamento degli investimenti e lo sviluppo infrastrutturale - Fascicolo sanitario elettronico» \(Piano di digitalizzazione dei dati e documenti sanitari\)](#)
- [Decreto del Ministero della Salute 20 maggio 2022 «Adozione delle Linee guida per l’attuazione del Fascicolo sanitario elettronico» pubblicato sulla GU Serie Generale n. 160 11.07.2022](#)
- [Decreto del Ministero della Salute 7 settembre 2023 «Fascicolo sanitario elettronico 2.0»](#)
- [Linee Guida per l’attuazione del Fascicolo Sanitario Elettronico \(2022\)](#)
- [M6 - Salute C2 1.3.1 «Rafforzamento dell’infrastruttura tecnologica e degli strumenti per la raccolta, l’elaborazione, l’analisi dei dati e la simulazione \(FSE\)»](#)

## SUAP e SUE

Gli Sportelli Unici per le Attività Produttive (SUAP) e per l’Edilizia (SUE) assumono un ruolo centrale come punto di convergenza per imprese, professionisti e cittadini nell’interazione con le istituzioni, nell’ambito degli adempimenti previsti per le attività produttive e gli interventi edilizi.

Codice	<b>CAP4.PA.07</b>
Oggetto	Le PA devono adeguarsi alle evoluzioni previste dall’ecosistema SPID (tra cui OpenID Connect, uso professionale, Attribuite Authorities, servizi per i minori e gestione degli attributi qualificati).
Periodo	Entro il 31/12/2026
Tempistica	Dal 01/03/2025 al 31/12/2026
Azione	Il servizio sarà allineato dopo la messa in funzione del nuovo portale.
% avanzamento	10%
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persone coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP4.PA.08</b>
Oggetto	Le PA che intendono aderire a NoiPA esprimono manifestazione di interesse e inviano richiesta.
Periodo	Entro il 31/12/2026
Tempistica	Dal 01/03/2025 al 31/12/2026
Azione	Sarà valutata l’opportunità di aderire a NoiPA entro il 31/12/2026.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persone coinvolte	AU / Direzione / Resp. Trans. Digitale
Status	

### Open data e data governance

Il presente Piano triennale mira ad assicurare maggiore efficacia all'attività amministrativa in tutti i processi che coinvolgono l'utilizzo dei dati, sia con riferimento alla condivisione dei dati tra pubbliche amministrazioni per finalità istituzionali, sia con riferimento al riutilizzo dei dati, anche per finalità commerciali, secondo il paradigma dei dati aperti.

Le "Linee guida recanti regole tecniche per l'apertura dei dati e il riutilizzo dell'informazione del settore pubblico" 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, deve essere tenuta in conto nella governance dei dati.

Il processo di formazione e pubblicazione dei dati 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 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.

### Contesto normativo e strategico

Riferimenti normativi italiani:

- [Decreto legislativo 30 giugno 2003, n. 196 «Codice in materia di protezione dei dati personali»](#)
- [Decreto legislativo 7 marzo 2005, n. 82 «Codice dell'amministrazione digitale» \(in breve CAD\) artt. 50, 50-ter., 51, 52, 59, 60](#)
- [Decreto legislativo 24 gennaio 2006, n. 36 «Attuazione della direttiva \(UE\) 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico che ha abrogato la direttiva 2003/98/CE»](#)
- [Decreto legislativo 27 gennaio 2010, n. 32 «Attuazione della direttiva 2007/2/CE, che istituisce un'infrastruttura per l'informazione territoriale nella Comunità europea \(INSPIRE\)»](#)
- [Decreto legislativo 14 marzo 2013, n. 33 «Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni» \(Decreto trasparenza\)](#)
- [Decreto legislativo 10 agosto 2018, n. 101 «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento \(UE\) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE» \(regolamento generale sulla protezione dei dati\)](#)
- [Decreto-legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 «Misure urgenti per la semplificazione e l'innovazione digitale»](#)
- [Decreto-legge 31 maggio 2021, n. 77, convertito con modificazioni dalla Legge 29 luglio 2021, n. 108 «Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure»](#)
- [Linee Guida AGID per i cataloghi dati \(2017\)](#)
- [Linee Guida AGID per l'implementazione della specifica GeoDCAT-AP \(2017\)](#)

- [Linee Guida AGID recanti regole tecniche per la definizione e l'aggiornamento del contenuto del Repertorio Nazionale dei Dati Territoriali \(2022\)](#)
- [Linee Guida AGID recanti regole tecniche per l'attuazione del decreto legislativo 24 gennaio 2006, n. 36 e s.m.i. relativo all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico adottate con Determinazione AGID n. 183/2023 del 3 agosto 2023](#)
- [Manuale RNDT - Guide operative per la compilazione dei metadati RNDT](#)
- Piano Nazionale di Ripresa e Resilienza - [Investimento 1.3: «Dati e interoperabilità»](#)

#### Riferimenti normativi europei:

- [Direttiva 2007/2/CE del Parlamento europeo e del Consiglio, del 14 marzo 2007, che istituisce un'infrastruttura per l'informazione territoriale nella Comunità europea \(Inspire\)](#)
- [Regolamento \(CE\) n. 1205/2008 del 3 dicembre 2008 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda i metadati](#)
- [Regolamento \(CE\) n. 976/2009 della Commissione, del 19 ottobre 2009, recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda i servizi di rete](#)
- [Regolamento \(UE\) 2010/1089 del 23 novembre 2010 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda l'interoperabilità dei set di dati territoriali e dei servizi di dati territoriali](#)
- [Regolamento \(UE\) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali \(in breve GDPR\)](#)
- [Direttiva \(UE\) 2019/1024 del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico](#)
- [Decisione \(UE\) 2019/1372 del 19 agosto 2019 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda il monitoraggio e la comunicazione](#)
- [Regolamento \(UE\) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento \(UE\) 2018/1724 \(Regolamento sulla governance dei dati\)](#)
- [Regolamento di esecuzione \(UE\) 2023/138 della Commissione del 21 dicembre 2022 che stabilisce un elenco di specifiche serie di dati di elevato valore e le relative modalità di pubblicazione e riutilizzo](#)
- [Comunicazione della Commissione 2014/C 240/01 del 24 luglio 2014 - Orientamenti sulle licenze standard raccomandate, i dataset e la tariffazione del riutilizzo dei documenti](#)
- [Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni COM \(2020\) del 19 febbraio 2020 - Una strategia europea per i dati](#)


#### Risultati attesi - OB 5.3

##### 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

- **Target 2024** - Almeno 35.000 dataset documentati con licenze previste dalle Linee guida Open Data
- **Target 2025** - Aumento del 30% dei dataset documentati con licenze previste dalle Linee guida Open Data rispetto al target 2024 per ciascuna amministrazione
- **Target 2026** - Aumento del 50% dei dataset documentati con licenze previste dalle Linee guida Open Data rispetto al target 2024 per ciascuna amministrazione

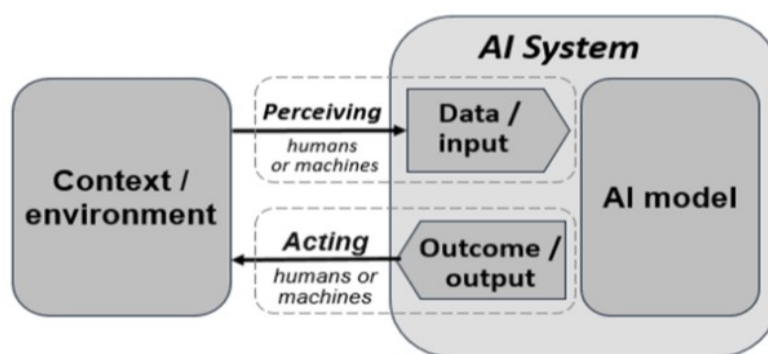
#### Obiettivo 5.3 – Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati

Codice	CAP5.PA.20
Oggetto	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.
Periodo	Dal 01/01/2025 al 30/06/2025
Tempistica	Entro il 30/06/2025
Azione	L'ente è in fase di verifica dell'attività indicata.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persone coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

## Intelligenza artificiale per la Pubblica Amministrazione

Per sistema di Intelligenza Artificiale (IA) si intende un sistema automatico che, per obiettivi espliciti o impliciti, deduce dagli input ricevuti come generare output come previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali. I sistemi di IA variano nei loro livelli di autonomia e adattabilità dopo l'implementazione.



L'intelligenza artificiale ha il potenziale per essere una tecnologia estremamente utile, o addirittura dirompente, per la modernizzazione del settore pubblico. L'IA sembra essere la risposta alla crescente necessità di migliorare l'efficienza e l'efficacia nella gestione e nell'erogazione dei servizi pubblici. Tra le potenzialità delle tecnologie di intelligenza artificiale si possono citare le capacità di:

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

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

Di seguito si riportano alcuni principi generali che dovranno essere adottati dalle pubbliche amministrazioni e declinati in fase di applicazione tenendo in considerazione lo scenario in veloce evoluzione.

1. **Miglioramento dei servizi e riduzione dei costi.** Le pubbliche amministrazioni concentrano l'investimento in tecnologie di intelligenza artificiale nell'automazione dei compiti ripetitivi connessi ai servizi istituzionali obbligatori e al funzionamento dell'apparato amministrativo.
2. **Analisi del rischio.** Le amministrazioni pubbliche analizzano i rischi associati all'impiego di sistemi di intelligenza artificiale per assicurare che tali sistemi non provochino violazioni dei diritti fondamentali della persona o altri danni rilevanti (adottano sistemi di IA con categorie di rischio definite dall'AI Act).
3. **Trasparenza, responsabilità e informazione.** Le pubbliche amministrazioni pongono particolare attenzione alla trasparenza e alla interpretabilità dei modelli di intelligenza artificiale al fine di garantire

la responsabilità e rendere conto delle decisioni adottate con il supporto di tecnologie di intelligenza artificiale.

4. **Inclusività e accessibilità.** Le pubbliche amministrazioni sono consapevoli delle responsabilità e delle implicazioni etiche associate all'uso delle tecnologie di intelligenza artificiale e assicurano che le tecnologie utilizzate rispettino i principi di equità, trasparenza e non discriminazione.
5. **Privacy e sicurezza.** Le pubbliche amministrazioni adottano elevati standard di sicurezza e protezione della privacy per garantire che i dati dei cittadini siano gestiti in modo sicuro e responsabile, garantendo la conformità dei propri sistemi di IA con la normativa vigente in materia di protezione dei dati personali e di sicurezza cibernetica.
6. **Formazione e sviluppo delle competenze.** Le pubbliche amministrazioni investono nella formazione e nello sviluppo delle competenze necessarie per gestire e applicare l'intelligenza artificiale in modo efficace nell'ambito dei servizi pubblici.
7. **Standardizzazione.** Le pubbliche amministrazioni tengono in considerazione, durante le fasi di sviluppo o acquisizione di soluzioni basate sull'intelligenza artificiale, le attività di normazione tecnica in corso a livello internazionale e a livello europeo da CEN e CENELEC con particolare riferimento ai requisiti definiti dall'AI Act.
8. **Sostenibilità:** Le pubbliche amministrazioni valutano attentamente gli impatti ambientali ed energetici legati all'adozione di tecnologie di intelligenza artificiale e adottando soluzioni sostenibili dal punto di vista ambientale.
9. **Foundation Models (Sistemi IA «ad alto impatto»):** Le pubbliche amministrazioni, prima di adottare foundation models «ad alto impatto», si assicurano che essi adottino adeguate misure di trasparenza che chiariscono l'attribuzione delle responsabilità e dei ruoli, in particolare dei fornitori e degli utenti del sistema di IA.
10. **Dati.** Le pubbliche amministrazioni, che acquistano servizi di intelligenza artificiale tramite API, valutano con attenzione le modalità e le condizioni con le quali il fornitore del servizio gestisce i dati forniti dall'amministrazione con particolare riferimento alla proprietà dei dati e alla conformità con la normativa vigente in materia di protezione dei dati e privacy.

## Contesto normativo e strategico

### Riferimenti normativi europei:

- 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

## Risultati attesi - OB 5.4

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

Linee guida che definiscono i passi metodologici e organizzativi che le pubbliche amministrazioni devono seguire per definire attività progettuali di innovazione mediante l'utilizzo di IA. Le Linee guida forniranno strumenti di valutazione sull'utilizzo dell'intelligenza artificiale per rispondere alle esigenze delle amministrazioni, illustrando casi d'uso e promuovendo buone pratiche.

- **Target 2024** - Redazione delle Linee guida
- **Target 2025** - Almeno 150 progetti di innovazione mediante IA (avviati)
- **Target 2026** - Almeno 400 progetti di innovazione mediante IA (avviati)



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

Linee guida che hanno l'obiettivo di orientare le pubbliche amministrazioni nella scelta delle procedure di approvvigionamento e nella definizione delle specifiche funzionali e non funzionali delle forniture al fine di garantire: la soddisfazione delle esigenze dell'amministrazione, adeguati livelli di servizio e la conformità con il quadro normativo vigente. Le Linee guida forniranno indicazione sulla gestione dei servizi di IA da parte della PA.

- **Target 2024** - Redazione delle Linee guida
- **Target 2025** - Almeno 100 iniziative di acquisizione di servizi di IA
- **Target 2026** - Almeno 300 iniziative di acquisizione di servizi di IA

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

Linee guida che hanno l'obiettivo di fornire alle pubbliche amministrazioni gli strumenti metodologici necessari per affrontare progetti di sviluppo di soluzioni IA, compresa la creazione di soluzioni basate su foundation models.


- **Target 2024** - Redazione delle Linee guida
- **Target 2025** - Almeno 50 progetti di sviluppo di soluzioni IA
- **Target 2026** - Almeno 100 progetti di sviluppo di soluzioni IA

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

Sviluppo e implementazione di soluzioni basate su IA finalizzate al miglioramento della qualità dei servizi pubblici, con l'obiettivo di garantire uniformi livelli di servizio su tutto il territorio nazionale.

- **Target 2024** - Identificazione delle soluzioni nazionali fondate sull'IA
- **Target 2025** - Sviluppo delle soluzioni nazionali
- **Target 2026** - Dispiegamento nei territori delle soluzioni realizzate

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

Codice	CAP5.PA.24
Oggetto	Le PA adottano le applicazioni di IA a valenza nazionale.
Periodo	Entro il 31/12/2026
Tempistica	Dal 30/06/2026 al 31/12/2026
Azione	L'ente verificherà l'adozione dell'attività indicata.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persone coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

#### Risultati attesi - OB 5.5


##### RA5.5.1 - Basi di dati nazionali strategiche

Sviluppo di raccolte di dataset al fine di assicurare una base di conoscenza condivisa per le soluzioni di Intelligenza Artificiale nella Pubblica Amministrazione, preservando allo stesso tempo le peculiarità della Pubblica Amministrazione italiana e le specificità culturali nazionali.

- **Target 2024** - Ricognizione delle basi di dati strategiche

- **Target 2025** - Digitalizzazione delle basi di dati strategiche
- **Target 2026** - Promozione delle basi di dati strategiche

#### Obiettivo 5.5 – Dati per l'intelligenza artificiale

Codice	<b>CAP5.PA.25</b>
Oggetto	Le PA adottano le basi dati nazionali strategiche.
Periodo	Entro il 31/12/2026
Tempistica	Dal 30/06/2026 al 31/12/2026
Azione	L'ente è in fase di verifica dell'attività indicata.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persone coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

### Infrastrutture digitali e Cloud

Con il principio cloud first, si vuole guidare e favorire l'adozione sicura, controllata e completa delle tecnologie cloud da parte del settore pubblico, in linea con i principi di tutela della privacy e con le raccomandazioni delle istituzioni europee e nazionali. In particolare, le pubbliche amministrazioni, in fase di definizione di un nuovo progetto, e/o di sviluppo di nuovi servizi, in via prioritaria devono valutare l'adozione del paradigma cloud prima di qualsiasi altra tecnologia.

Tutte le Amministrazioni sono obbligate ad effettuare una valutazione in merito all'adozione del cloud che rappresenta l'evoluzione tecnologica più dirompente degli ultimi anni e che sta trasformando radicalmente tutti i sistemi informativi della società a livello mondiale. Nel caso di eventuale esito negativo, tale valutazione dovrà essere motivata.

#### Punti di attenzione e azioni essenziali per tutti gli enti

- 1) L'attuazione dell'art.33-septies Decreto-legge 179/2012, e del principio cloud-first, deve essere tra gli obiettivi prioritari dell'ente. Occorre curare da subito anche gli aspetti di sostenibilità economico-finanziaria nel tempo dei servizi attivati, avendo cura di verificare gli impatti della migrazione sui propri capitoli di bilancio relativamente sia ai costi correnti sia agli investimenti in conto capitale.
- 2) La gestione dei servizi in cloud deve essere presidiata dall'ente in tutto il ciclo di vita degli stessi e quindi è necessaria la disponibilità di competenze specialistiche all'interno dell'Ufficio RTD, in forma singola o associata.

#### Approfondimento tecnologico per gli RTD

- 1) La piena abilitazione al cloud richiede l'evoluzione del parco applicativo software verso la logica as a service delle applicazioni esistenti, andando oltre il mero lift-and-shift dei server, progettando opportuni interventi di rearchitect, replatform o repurchase per poter sfruttare le possibilità offerte oggi dalle moderne piattaforme computazionali e dagli algoritmi di intelligenza artificiale. In tal senso, occorre muovere verso architetture a «micro-servizi» le cui caratteristiche sono, in sintesi, le seguenti:
  - ogni servizio non ha dipendenze esterne da altri servizi e gestisce autonomamente i propri dati (self-contained);
  - ogni servizio comunica con l'esterno attraverso API/webservice e senza dipendenza da stati pregressi (lightweight/stateless);
  - ogni servizio può essere implementato con differenti linguaggi e tecnologie, in modo indipendente dagli altri servizi (implementation-independent);
  - ogni servizio può essere dispiegato in modo automatico e gestito indipendentemente dagli altri servizi (independently deployable);
  - ogni servizio implementa un insieme di funzioni legate a procedimenti e attività amministrative, non ha solo scopo tecnologico (business-oriented).
- 2) È compito dell'Ufficio RTD curare sia gli aspetti di pianificazione della migrazione/abilitazione al cloud che l'allineamento dello stesso con l'implementazione delle relative opportunità di riorganizzazione dell'ente offerte dall'abilitazione al cloud e dalle nuove architetture a micro-servizi.
- 3) La gestione del ciclo di vita dei servizi in cloud dell'amministrazione richiede la strutturazione di opportuni presidi organizzativi e strumenti tecnologici per il cloud-cost-management, in forma singola o associata.

#### Contesto normativo e strategico

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

#### Riferimenti normativi nazionali:

- [Decreto legislativo 7 marzo 2005, n. 82, «Codice dell'amministrazione digitale» articoli. 8-bis e 73;](#)
- [Decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, «Ulteriori misure urgenti per la crescita del Paese», articolo 33-septies;](#)
- [Decreto legislativo 18 maggio 2018, n. 65, «Attuazione della direttiva \(UE\) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione»](#)
- [Decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla L. 18 novembre 2019, n. 133 «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica»](#)
- [Decreto-legge 17 marzo 2020, n. 18, convertito con modificazioni dalla Legge 24 aprile 2020, n. 27 «Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19», art. 75](#)
- [Decreto-legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 «Misure urgenti per la semplificazione e l'innovazione digitale», art. 35](#)
- [Decreto-legge 31 maggio 2021, n. 77, convertito con modificazioni dalla Legge 29 luglio 2021, n. 108 «Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure»](#)
- [Decreto-legge 14 giugno 2021, n. 82, convertito con modificazioni dalla Legge 4 agosto 2021, n. 109 «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale»](#)
- [Circolare AGID n. 1/2019 del 14 giugno 2019 - Censimento del patrimonio ICT delle Pubbliche Amministrazioni e classificazione delle infrastrutture idonee all'uso da parte dei Poli Strategici Nazionali;](#)
- [Strategia italiana per la banda ultra-larga \(2021\)](#)
- [Strategia Cloud Italia \(2021\);](#)
- [Regolamento AGID, di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la Pubblica Amministrazione e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la Pubblica Amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la Pubblica Amministrazione \(2021\)](#)
- [Determinazioni ACN in attuazione al precedente Regolamento n. 306/2022 \(con allegato\) su e n. 307/2022 \(con allegato\)](#)
- [Decreti direttoriali ACN prot. N. 29 del 2 gennaio 2023, n. 5489 dell'8 febbraio 2023 e n. 20610 del 28 luglio 2023;](#)
- [Piano Nazionale di Ripresa e Resilienza:](#)
  - [Investimento 1.1: «Infrastrutture digitali»](#)
  - [Investimento 1.2: «Abilitazione e facilitazione migrazione al cloud»](#)

#### Riferimenti europei:


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


#### Risultati attesi - OB 6.1

##### RA6.1.1 - Numero di amministrazioni migrate


- **Target 2024** - 4.083 amministrazioni migrate con infrastrutture e servizi cloud qualificati/adequati e almeno 100 amministrazioni migrate con almeno un servizio verso il PSN (Target PNRR, M1C1-139 e M1C1-17)
- **Target 2025** - Il 75% delle amministrazioni individuate ai sensi dell'art. 1, co.3, legge n.196/2009 completano la realizzazione dei piani di migrazione trasmessi a DTD e AGID
- **Target 2026** - Il 100% delle amministrazioni individuate ai sensi dell'art. 1, co.3, legge n.196/2009 completano la realizzazione dei piani di migrazione trasmessi a DTD e AGID


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

Codice	<b>CAP6.PA.01</b>
Oggetto	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.
Periodo	Entro il 31/12/2026
Tempistica	Dal 30/06/2026 al 31/12/2026
Azione	L'ente è in fase di verifica dell'attività indicata.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP6.PA.03</b>
Oggetto	Le PA avviano il percorso di migrazione verso il cloud in coerenza con quanto previsto dalla Strategia Cloud Italia.
Periodo	Entro il 31/12/2026
Tempistica	Dal 30/06/2026 al 31/12/2026
Azione	L'ente è in fase di verifica dell'attività indicata.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP6.PA.05</b>
Oggetto	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.
Periodo	Entro il 31/12/2026
Tempistica	Dal 30/06/2026 al 31/12/2026

Azione	L'ente è in fase di verifica dell'attività indicata.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP6.PA.06</b>
Oggetto	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.
Periodo	Entro il 31/12/2026
Tempistica	Dal 30/06/2026 al 31/12/2026
Azione	L'ente è in fase di verifica dell'attività indicata.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

## 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;

## Contesto normativo e strategico

Riferimenti normativi italiani:


- [Decreto legislativo 7 marzo 2005, n. 82, «Codice dell'amministrazione digitale», articoli. 8-bis e 73;](#)
- [Strategia italiana per la Banda Ultra Larga 2023-2026](#)

## Risultati attesi - OB 6.2

### RA6.2.1 - Rete di connettività

- **Target 2024** - Aggiudicazione della nuova gara da parte di Consip per nuovi servizi di connettività a banda ultra-larga nell'ambito SPC.
- **Target 2025** - Il 20 % delle amministrazioni avviano la migrazione ai nuovi servizi di connettività SPC.
- **Target 2026** - Il 50% delle amministrazioni hanno concluso la migrazione

### Obiettivo 6.2 – Garantire alle amministrazioni la disponibilità della connettività SPC

Codice	<b>CAP6.PA.11</b>
Oggetto	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.
Periodo	Entro il 31/12/2025
Tempistica	Dal 01/01/2025 al 31/12/2025
Azione	L'ente verificherà la possibilità di aderire al Sistema Pubblico di Connettività (SPC) per le Pubbliche Amministrazioni - Edizione n° 3 di Consip.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persone coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

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.

### Contesto normativo e strategico

#### *Riferimenti normativi italiani:*

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

#### *Riferimenti normativi europei:*



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

#### Risultati attesi - OB 7.1


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


- **Target 2024** - Identificare e approvare un modello unitario e centralizzato di governance della cybersicurezza, comprensivo delle linee di implementazione da parte delle PA.
- **Target 2025** - Approvare e rendere noti ruoli e responsabilità relativi alla gestione della cybersicurezza


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

- **Target 2024** - n.d.
- **Target 2025** - Approvare e rendere noti i processi e le procedure inerenti alla gestione interna della cybersicurezza

#### Obiettivo 7.1 – Adottare una governance della cybersicurezza diffusa nella PA

Codice	<b>CAP7.PA.02</b>
Oggetto	Le PA adottano un modello di governance della cybersicurezza.
Periodo	Entro il 31/12/2025
Tempistica	Dal 01/01/2025 al 31/12/2025
Azione	L'ente attuerà il modello con l'entrata in funzione del nuovo portale e l'adeguamento dell'infrastruttura SPC.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persone coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP7.PA.03</b>
Oggetto	Le PA nominano i Responsabili della cybersicurezza e delle loro strutture organizzative di supporto.
Periodo	Entro il 31/12/2025
Tempistica	Dal 01/01/2025 al 31/12/2025
Azione	Vedi CAP7.PA.02.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persone coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP7.PA.04</b>
Oggetto	Le PA formalizzano i processi e le procedure inerenti alla gestione della cybersicurezza.
Periodo	Entro il 31/12/2025
Tempistica	Dal 01/01/2025 al 31/12/2025
Azione	Vedi CAP7.PA.02.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

## Risultati attesi - OB 7.2


### RA7.2.1 - Definizione del framework documentale a supporto del processo di approvvigionamento IT

- **Target 2024** - Definire ed approvare i requisiti di sicurezza nei processi di approvvigionamento IT
- **Target 2025** - Definire ed approvare processi e modalità di approvvigionamento e governo del rischio nella gestione delle terze parti
- **Target 2026** - Definire contratti e accordi con fornitori e terze parti IT per rispettare gli obiettivi di sicurezza definiti nel processo di approvvigionamento


### RA7.2.2 - Definizione delle modalità di monitoraggio del processo di approvvigionamento IT

- **Target 2024** - n.d.
- **Target 2025** - Definire e formalizzare le modalità e il piano di audit e verifiche per la valutazione dei fornitori e delle terze parti IT per confermare il rispetto degli obblighi contrattuali definiti
- **Target 2026** - Definire e promuovere attività di controllo e verifica sui fornitori e sulle terze parti IT al fine di confermare gli obblighi e requisiti di sicurezza

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

Codice	<b>CAP7.PA.05</b>
Oggetto	Le PA definiscono e approvano i requisiti di sicurezza relativi al processo di approvvigionamento IT.
Periodo	Entro il 31/12/2025
Tempistica	Dal 01/01/2025 al 31/12/2025
Azione	Vedi CAP7.PA.02.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP7.PA.06</b>
--------	-------------------

Oggetto	Le PA definiscono e promuovono i processi di gestione del rischio sui fornitori e terze parti IT, la contrattualistica per i fornitori e le terze parti IT, comprensive dei requisiti di sicurezza da rispettare.
Periodo	Entro il 31/12/2025
Tempistica	Dal 01/01/2025 al 31/12/2025
Azione	Vedi CAP7.PA.02.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

### Risultati attesi - OB 7.3


#### RA7.3.1 - Definizione del framework per la gestione del rischio cyber

- **Target 2024** - Adottare i processi e gli strumenti per le attività di cyber risk management e security by design
- **Target 2025** - Promuovere attività di classificazione dati e servizi, identificando Piani e strumenti per garantirne la continuità operativa dei servizi offerti

#### RA7.3.2 - Definizione delle modalità di monitoraggio del rischio cyber

- **Target 2026** - Integrare attività di monitoraggio e mitigazione del rischio cyber nei normali processi di progettazione e gestione dei sistemi informativi della PA

### Obiettivo 7.3 – Gestione e mitigazione del rischio cyber

Codice	<b>CAP7.PA.11</b>
Oggetto	Le PA integrano le attività di monitoraggio del rischio cyber, come definito dal relativo Piano, nelle normali attività di progettazione, analisi, conduzione e dismissione di applicativi e sistemi informativi.
Periodo	Entro il 31/12/2025
Tempistica	Dal 01/01/2025 al 31/12/2025
Azione	Vedi CAP7.PA.02.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

### Risultati attesi - OB 7.4

#### RA7.4.1 - Definizione del framework documentale relativo alla gestione degli incidenti


- **Target 2024**
  - Definire i presidi per la gestione degli eventi di sicurezza


- Formalizzare i processi e le procedure relative alla gestione degli incidenti

#### RA7.4.2 - Definizione delle modalità di verifica e aggiornamento dei piani di risposta agli incidenti


- **Target 2025** - Definire le modalità di verifica dei piani di risposta e ripristino a seguito di incidenti informatici
- **Target 2026** - Definire le modalità di aggiornamento dei Piani di risposta e ripristino a seguito di incidenti informatici


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

Codice	<b>CAP7.PA.13</b>
Oggetto	Le PA definiscono i presidi per la gestione degli eventi di sicurezza, formalizzandone i processi e le procedure.
Periodo	Entro il 31/12/2025
Tempistica	Dal 01/01/2025 al 31/12/2025
Azione	Saranno definiti i parametri, integrando quelli già esistenti, in un apposito documento che sarà approvato con delibera dell'AU.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP7.PA.14</b>
Oggetto	Le PA formalizzano ruoli, responsabilità e processi, nonché le capacità tecnologiche a supporto della prevenzione e gestione degli incidenti informatici.
Periodo	Entro il 31/12/2025
Tempistica	Dal 01/01/2025 al 31/12/2025
Azione	Ruoli, responsabilità e processi saranno formalizzati all'interno del documento di cui al CAP7.PA.13.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP7.PA.15</b>
Oggetto	Le PA definiscono le modalità di verifica dei Piani di risposta a seguito di incidenti informatici.
Periodo	Entro il 31/12/2025
Tempistica	Dal 01/01/2025 al 31/12/2025
Azione	La modalità di verifica dei Piani sarà compresa nel documento di cui al CAP7.PA.13.
% avanzamento	
Budget previsto	
Capitolo spesa	

% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP7.PA.16</b>
Oggetto	Le PA definiscono le modalità di aggiornamento dei Piani di risposta e ripristino a seguito dell'accadimento di incidenti informatici.
Periodo	Entro il 31/12/2025
Tempistica	Dal 01/01/2025 al 31/12/2025
Azione	Le modalità di aggiornamento dei Piani sarà compresa nel documento di cui al CAP7.PA.13.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

## Risultati attesi - OB 7.5


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

- **Target 2024** - Definire processi e procedure per la realizzazione di attività di sensibilizzazione cyber
- **Target 2025** - Definire piani di formazione diversificati per ruoli e posizioni organizzative


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


- **Target 2026** - Acquisire strumenti informatici a supporto dei programmi formativi

## Obiettivo 7.5 – Implementare attività strutturate di sensibilizzazione cyber del personale

Codice	<b>CAP7.PA.17</b>
Oggetto	Le PA promuovono l'accesso e l'utilizzo di attività strutturate di sensibilizzazione e formazione in ambito cybersicurezza.
Periodo	Entro il 31/12/2026
Tempistica	Dal 01/01/2026 al 31/12/2026
Azione	Saranno acquisiti strumenti adatti per la formazione.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP7.PA.18</b>
Oggetto	Le PA definiscono piani di formazione inerenti alla cybersecurity, diversificati per ruoli, posizioni organizzative e attività delle risorse dell'organizzazione.

Periodo	Entro il 31/12/2026
Tempistica	Dal 01/01/2026 al 31/12/2026
Azione	Nel programma triennale per la formazione saranno inseriti i piani inerenti alla cybersecurity.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP7.PA.19</b>
Oggetto	Le PA realizzano iniziative per verificare e migliorare la consapevolezza del proprio personale.
Periodo	Entro il 31/12/2026
Tempistica	Dal 01/01/2026 al 31/12/2026
Azione	A seguito del programma di formazione saranno avviate le verifiche.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

## Risultati attesi - OB 7.6

### RA7.6.1 - Distribuzione di Indicatori di Compromissione alle PA

- **Target 2024** - Distribuzione degli IoC al 30% delle PA
- **Target 2025** - Distribuzione degli IoC al 60% delle PA
- **Target 2026** - Distribuzione degli IoC al 100% delle PA


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


- **Target 2024** - Almeno il 20% delle PA fruiscono degli strumenti o servizi per l'autovalutazione messi a disposizione sul Portale del CERT-AGID.
- **Target 2025** - Almeno il 60% delle PA fruiscono degli strumenti o servizi per l'autovalutazione messi a disposizione sul Portale del CERT-AGID.
- **Target 2026** - Il 100% delle PA fruiscono degli strumenti o servizi per l'autovalutazione messi a disposizione sul Portale del CERT-AGID.


### 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

- **Target 2024** - Pubblicazione della versione aggiornata del portale CERT-AGID con contenuti informativi relativi alle campagne malevole veicolate verso le PA
- **Target 2025** - Erogazione di due corsi di formazione, base ed avanzato, sulla sicurezza nella PA
- **Target 2026** - Fornitura di documentazione di supporto agli RTD per la gestione della sicurezza IT nelle PA in aggiunta alle attività formative

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

Codice	<b>CAP7.PA.20</b>
Oggetto	Le PA dovranno dotarsi degli strumenti idonei all'acquisizione degli IoC ed accreditarsi al CERT-AGID.
Periodo	Entro il 31/12/2026
Tempistica	Dal 01/01/2026 al 31/12/2026
Azione	Gli indicatori di compromissione sono importanti e pertanto l'ente si doterà di strumenti per i log e gli audit trail più efficaci per le indagini durante le fasi di incident response.
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP7.PA.21</b>
Oggetto	Le PA dovranno usufruire degli strumenti per la gestione dei rischi cyber messi a disposizione dal CERT-AGID.
Periodo	Entro il 31/12/2026
Tempistica	Dal 01/01/2026 al 31/12/2026
Azione	
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

Codice	<b>CAP7.PA.22</b>
Oggetto	Le PA, sulla base delle proprie esigenze, partecipano ai corsi di formazione base ed avanzato erogati dal CERT-AGID.
Periodo	Entro il 31/12/2026
Tempistica	Dal 01/01/2026 al 31/12/2026
Azione	
% avanzamento	
Budget previsto	
Capitolo spesa	
% completamento	
Strutture/persona coinvolte	UD Risorse / SIA / Resp. Trans. Digitale
Status	

### Appendice - Glossario

#### **AGID**

Agenzia per l'Italia Digitale è l'agenzia tecnica della Presidenza del Consiglio col compito di garantire la realizzazione degli obiettivi dell'Agenda digitale e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione.

#### **API**

API (Application Programming Interface) è un insieme di definizioni e protocolli che consentono a software diversi di comunicare tra loro.

#### **API-first**

Principio per cui i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e attraverso processi digitali collettivi.

#### **CAD**

Codice Amministrazione Digitale è un testo unico che riunisce e organizza le norme in merito all'informatizzazione della PA nei rapporti con cittadini e imprese.

#### **CITD**

Comitato Interministeriale per la Trasformazione Digitale promuove, indirizza, coordina l'azione del Governo nelle materie dell'innovazione tecnologica, dell'attuazione dell'agenda digitale italiana ed europea, della strategia italiana per la banda ultra-larga, della digitalizzazione delle pubbliche amministrazioni e delle imprese, nonché della trasformazione, crescita e transizione digitale del Paese.

#### **Cloud first**

Strategia che promuove l'utilizzo dei servizi cloud come prima scelta per la gestione dei dati e dei processi aziendali.

#### **Decennio Digitale**

Insieme di regole e principi guida dettati dalla Commissione Europea per guidare i Paesi Membri nel raggiungimento degli obiettivi fissati per il Decennio Digitale 2020-2030.

#### **Digital & mobile first**

Principio per cui le pubbliche amministrazioni devono erogare i propri servizi pubblici in digitale e devono essere fruibili su dispositivi mobili.

#### **Digital identity only**

Principio per cui le pubbliche amministrazioni devono erogare i propri servizi pubblici in digitale e devono essere fruibili su dispositivi mobili.

#### **Gold plating**

Fenomeno in cui un progetto viene implementato con caratteristiche o dettagli aggiuntivi che vanno oltre i requisiti richiesti, senza alcuna reale necessità o beneficio tangibile.

#### **Governo come Piattaforma**

Approccio strategico nella progettazione e nell'erogazione dei Servizi Pubblici in cui il governo agisce come una piattaforma aperta che facilita l'erogazione di servizi da parte di entità pubbliche e private.



## **ICT**

Information and Communication Technology (Tecnologie dell'Informazione e della Comunicazione).

### **Interoperabilità**

Rende possibile la collaborazione tra Pubbliche amministrazioni e tra queste e soggetti terzi, per mezzo di soluzioni tecnologiche che assicurano l'interazione e lo scambio di informazioni senza vincoli sulle implementazioni, evitando integrazioni ad hoc.

### **Lock-in**

Fenomeno che si verifica quando l'amministrazione non può cambiare facilmente fornitore alla scadenza del periodo contrattuale perché non sono disponibili le informazioni essenziali sul sistema che consentirebbero a un nuovo fornitore di subentrare al precedente in modo efficiente.

### **Once-only**

Principio secondo cui l'amministrazione non richiede al cittadino dati e informazioni di cui è già in possesso.

### **Open data by design e by default**

Principio per cui il patrimonio informativo della Pubblica Amministrazione deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile.

### **Openess**

Principio per cui le pubbliche amministrazioni devono tenere conto della necessità di prevenire il rischio di lock-in nei propri servizi, prediligere l'utilizzo di software con codice aperto o di e-Service e, nel caso di software sviluppato per loro conto, deve essere reso disponibile il codice sorgente, nonché promuovere l'amministrazione aperta e la condivisione di buone pratiche sia amministrative che tecnologiche.

### **PDND**

Piattaforma Digitale Nazionale Dati (PDND) è lo strumento che abilita l'interoperabilità dei sistemi informativi degli Enti e dei Gestori di Servizi Pubblici.

### **PIAO**

Piano Integrato di Attività e Organizzazione è un documento unico di programmazione e governance che va a sostituire tutti i programmi che fino al 2022 le Pubbliche Amministrazioni erano tenute a predisporre, tra cui i piani della performance, del lavoro agile (POLA) e dell'anticorruzione.

### **PNC**

Piano Nazionale per gli investimenti complementari è il piano nazionale di investimenti finalizzato a integrare gli interventi del PNRR tramite risorse nazionali.

### **PNRR**

Piano Nazionale di Ripresa e Resilienza è il piano nazionale di investimenti finalizzato allo sviluppo sostenibile e al rilancio dell'economia tramite i fondi europei del Next Generation EU.

### **Privacy by design e by default**

Principio per cui i servizi pubblici devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali.

### **RTD**

Responsabile per la Trasformazione Digitale è il dirigente all'interno della Pubblica Amministrazione che garantisce operativamente la trasformazione digitale dell'amministrazione, coordinando lo sviluppo dei servizi pubblici digitali e l'adozione di nuovi modelli di relazione con i cittadini, trasparenti e aperti.

**SIPA**

Sistema Informativo delle Pubbliche Amministrazioni (SIPA) insieme coordinato di risorse, norme, procedure, tecnologie e dati volti a supportare la gestione informatizzata delle attività e dei processi all'interno delle pubbliche amministrazioni.

**User-centric**

Principio per cui le pubbliche amministrazioni devono progettare servizi pubblici che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo.

**UTD**

Ufficio per la Transizione Digitale è l'ufficio dell'amministrazione a cui viene affidato il delicato processo di transizione alla modalità operativa digitale.

Potenza, 29/03/2024