

ISTITUTO NAZIONALE DI FISICA NUCLEARE

IL CONSIGLIO DIRETTIVO

Deliberazione n. 17194

Oggetto: *Approvazione Piano triennale per l'Informatica 2024- 2026*

Il Consiglio Direttivo dell'Istituto Nazionale di Fisica Nucleare, riunito in Roma in data 25 settembre 2024 alla presenza di n. 34 suoi componenti su un totale di n. 34

Premesso che

- Il Codice dell'Amministrazione Digitale (CAD) di cui al D.Lgs. 82/2005 e successive modifiche e integrazioni prescrive che le amministrazioni pubbliche di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, numero 165, ai fini del contenimento delle spese di funzionamento delle proprie strutture, adottino piani triennali per l'individuazione di misure finalizzate alla razionalizzazione dell'utilizzo delle dotazioni strumentali, anche informatiche, che corredano le stazioni di lavoro nell'automazione d'ufficio;
- con decreto del Presidente del Consiglio dei Ministri 17 luglio 2020, registrato dalla Corte dei Conti con il numero 2053/2020, è stato approvato, ai sensi dell'art. 14-bis, comma 2, lettera b), del decreto legislativo 7 marzo 2005, n. 82, il Piano triennale per l'informatica nella pubblica amministrazione 2020-2022; l'adozione del Piano triennale per l'informatica nella Pubblica Amministrazione 2020-2022 è stata resa nota con apposito comunicato pubblicato sulla Gazzetta Ufficiale (GU Serie Generale n. 255 del 15-10-2020);
- Con decreto del Presidente del Consiglio dei Ministri 12 gennaio 2024, registrato dalla Corte dei conti al n. 294/2023, è stato approvato, ai sensi dell'art. 14-bis, comma 2, lettera b), del decreto legislativo 7 marzo 2005, n. 82, il Piano triennale per l'informatica nella pubblica amministrazione 2024-2026;

Visto che:

- per quanto riguarda i beni e servizi informatici e di connettività, la L. 208/2015 (Legge di stabilità 2016), all'art. 1, commi 512-516, ha rafforzato e generalizzato l'obbligo di utilizzo delle centrali di acquisto (Consip e altri soggetti aggregatori regionali) per l'approvvigionamento di tali beni, prevedendo la necessaria autorizzazione dell'autorità amministrativa di vertice per gli acquisti effettuati al di fuori di tali modalità, nei modi consentiti dalla legge;
- la medesima legge ha inoltre affidato all'Agenzia per l'Italia Digitale il compito di predisporre il Piano triennale per l'Informatica nella Pubblica Amministrazione contenente, per ciascuna amministrazione o categoria di amministrazioni, l'elenco dei beni e servizi informatici e di connettività e dei relativi costi, suddivisi in spese da sostenere per innovazione e spese per la gestione corrente, individuando altresì i beni e servizi la cui acquisizione riveste particolare rilevanza strategica;
- il Piano 2020-2022 ed i successivi aggiornamenti 2021-2023 e 2022-2024, nonché il piano 2024-2026, introducono un'importante innovazione con riferimento ai destinatari degli obiettivi individuati per ciascuna delle tematiche affrontate, assegnando alle singole amministrazioni centrali e locali la realizzazione degli obiettivi elencati.

Richiamata la disposizione numero 26218 del 04/12/2023 con la quale la medesima ha individuato il Responsabile della

ISTITUTO NAZIONALE DI FISICA NUCLEARE

Transizione digitale, ai sensi dell'art. 17 del Codice dell'Amministrazione Digitale (CAD) - D.lgs. 82/2005, indicando il dott. Enrico Pasqualucci;

Considerato opportuno approvare l'allegato Piano Triennale per l'Informatica 2024-2026, al fine di perseguire la razionalizzazione nell'acquisizione di beni e servizi informatici e di telecomunicazione in funzione della realizzazione di un'amministrazione digitale e aperta, dotata di servizi facilmente utilizzabili e di qualità;

Tutto ciò premesso, con n. 34 voti favorevoli

DELIBERA

1. per le motivazioni di cui in premessa, di approvare il Piano Triennale per l'Informatica 2024-2026 che si allega alla presente deliberazione per formarne parte integrante e sostanziale;
2. di dare atto che il Piano verrà attuato secondo criteri, termini e modalità previste dallo stesso strumento pianificatorio e adeguato alla luce di eventuali nuove normative, linee guida o decreti attuativi ed ulteriori specifiche tecniche;
3. di pubblicare il Piano suddetto sul sito web istituzionale del Comune nell'apposita sezione denominata "Amministrazione Trasparente/Altri Contenuti" in attesa di precise indicazioni da parte di AGID sulla posizione esatta in cui pubblicare il piano stesso;
4. di comunicare la pubblicazione del presente Piano ai Responsabili di Settore/servizio e titolari di posizione organizzativa con particolare riferimento alla necessità di contribuire, per quanto di competenza, alle attività del Responsabile della Transizione Digitale.

Piano Triennale per l'Informatica

nella **Pubblica Amministrazione**



Istituto Nazionale di Fisica Nucleare
via Enrico Fermi, 54
00044 – Frascati (Roma)

Pec: Amm.ne.Centrale@pec.infn.it
Email: presidenza@presid.infn.it

Edizione
2024-2026

Settembre 2024

Sommario

INTRODUZIONE	5
<i>Finalità del Piano triennale.....</i>	<i>6</i>
<i>Strategia</i>	<i>7</i>
<i>Modello strategico</i>	<i>7</i>
<i>Principi guida.....</i>	<i>9</i>
<i>Percorso di elaborazione del Piano triennale</i>	<i>11</i>
<i>Articolazione del Piano e guida alla lettura.....</i>	<i>12</i>
PARTE PRIMA – COMPONENTI STRATEGICHE PER LA TRASFORMAZIONE DIGITALE	14
CAPITOLO 1 - ORGANIZZAZIONE E GESTIONE DEL CAMBIAMENTO	15
<i>L’ecosistema digitale amministrativo</i>	<i>15</i>
<i>La collaborazione istituzionale.....</i>	<i>16</i>
<i>Il ruolo del Responsabile e dell’Ufficio per la transizione al digitale</i>	<i>18</i>
<i>Competenze digitali per il Paese e per la PA.....</i>	<i>22</i>
<i>Monitoraggio</i>	<i>27</i>
<i>Strumenti per l’attuazione del Piano.....</i>	<i>30</i>
<i>Risorse e fonti di finanziamento.....</i>	<i>30</i>
<i>La transizione digitale e l'INFN.....</i>	<i>31</i>
<i>L'organizzazione dell'RTD nell'INFN</i>	<i>31</i>
<i>Il Comitato di Coordinamento per la Transizione Digitale</i>	<i>32</i>
<i>Le aree di intervento</i>	<i>32</i>
Area Accessibilità	32
Area Sicurezza Informatica	33
Area Auditing cyber-security-privacy	33
Area Protezione dati personali	34
Area Infrastruttura di Autenticazione e Autorizzazione.....	35
Area Protocollo Informatico	35
Area conservazione documentale	36
CAPITOLO 2 - IL PROCUREMENT PER LA TRASFORMAZIONE DIGITALE	38
<i>Il procurement per la trasformazione digitale.....</i>	<i>38</i>
Gli acquisti di beni e servizi standardizzati	38
Gli acquisti di innovazione per la trasformazione digitale.....	39
L’ecosistema digitale degli acquisti pubblici.....	39
Organizzazione della stazione appaltante nel nuovo Codice dei Contratti Pubblici	39
La qualificazione della Stazione appaltante.....	40
L’organizzazione della Stazione appaltante e il ruolo del RUP	40
La collaborazione tra stazioni appaltanti.....	41
<i>Le gare strategiche per la trasformazione digitale.....</i>	<i>43</i>
<i>Strumenti per l’attuazione del Piano.....</i>	<i>45</i>
<i>Risorse e fonti di finanziamento.....</i>	<i>45</i>
<i>Il procurement e l'INFN</i>	<i>45</i>
PARTE SECONDA – COMPONENTI TECNOLOGICHE	47
CAPITOLO 3 - SERVIZI	48
<i>E-Service in interoperabilità tramite PDND.....</i>	<i>49</i>
<i>Progettazione dei servizi: accessibilità e design</i>	<i>53</i>
<i>Formazione, gestione e conservazione dei documenti informatici</i>	<i>57</i>
<i>Single Digital Gateway</i>	<i>59</i>
<i>Strumenti per l’attuazione del Piano.....</i>	<i>61</i>
<i>Risorse e fonti di finanziamento.....</i>	<i>63</i>
CAPITOLO 4 - PIATTAFORME	65
<i>Piattaforme nazionali che erogano servizi a cittadini/imprese o ad altre PA.....</i>	<i>65</i>
<i>Piattaforme che attestano attributi</i>	<i>76</i>
<i>Basi dati interesse nazionale.....</i>	<i>80</i>

<i>Strumenti per l'attuazione del Piano</i>	81
<i>Risorse e fonti di finanziamento</i>	82
<i>L'INFN e le piattaforme</i>	83
CAPITOLO 5 - DATI E INTELLIGENZA ARTIFICIALE	85
<i>Open data e data governance</i>	85
<i>Intelligenza artificiale per la Pubblica Amministrazione</i>	94
Principi generali per l'utilizzo dell'intelligenza artificiale nella Pubblica Amministrazione	95
Dati per l'intelligenza artificiale.....	96
<i>Strumenti per l'attuazione del Piano</i>	99
<i>Risorse e fonti di finanziamento</i>	100
CAPITOLO 6 - INFRASTRUTTURE	102
<i>Infrastrutture digitali e Cloud</i>	102
Punti di attenzione e azioni essenziali per tutti gli enti	107
Approfondimento tecnologico per gli RTD	107
<i>Il sistema pubblico di connettività</i>	111
<i>Strumenti per l'attuazione del Piano</i>	112
<i>Risorse e fonti di finanziamento</i>	112
<i>Infrastrutture cloud e connettività nell'INFN</i>	112
CAPITOLO 7 - SICUREZZA INFORMATICA	114
<i>Sicurezza informatica</i>	114
<i>Strumenti per l'attuazione del Piano</i>	121
<i>Risorse e fonti di finanziamento</i>	121
<i>L'INFN e la sicurezza informatica</i>	121
CREDITS.....	124
RINGRAZIAMENTI.....	124
APPENDICE - GLOSSARIO	126
PARTE TERZA - STRUMENTI	128
STRUMENTO 1 - APPROVVIGIONAMENTO ICT	129
I. <i>Obiettivo</i>	129
II. <i>Destinatari</i>	129
III. <i>Crediti</i>	129
1.1. GLI ACCORDI QUADRO CONSIP E GLI INDICATORI DI DIGITALIZZAZIONE	130
1.2. GLI STRUMENTI CONSIP	136
1.3. DESCRIZIONE SINTETICA DEGLI STRUMENTI CONSIP	138
1.4. RIFERIMENTI.....	143
STRUMENTO 2 - GESTIONE ASSOCIATA DELL'ICT	144
I. <i>Obiettivo</i>	144
II. <i>Destinatari</i>	144
III. <i>Crediti</i>	144
1.1. INTRODUZIONE	145
1.2. ORGANIZZAZIONE DEI SISTEMI INTERCOMUNALI CON GESTIONE ASSOCIATA	148
1.4. QUALIFICAZIONE DEI CENTRI SERVIZI SUL DIGITALE.....	150
1.5. ALLEGATO A - STATO DELL'ARTE DELL'ASSOCIAZIONISMO ICT E BENEFICI	152
1.6. RIFERIMENTI.....	159
STRUMENTO 3 - SERVIZI PRIORITARI SECONDO L'EGOVERNMENT BENCHMARK	160
I. <i>Obiettivo</i>	160
II. <i>Destinatari</i>	160
III. <i>Crediti</i>	160
1.7. EGOVERNMENT BENCHMARK.....	161
1.8. EGOVERNMENT BENCHMARK E DESI	162
1.9. SERVIZI PRIORITARI	163
1.10. IL SISTEMA DI VALUTAZIONE	167
1.11. INDICAZIONI PER IL MIGLIORAMENTO DEI SERVIZI DELLA PUBBLICA AMMINISTRAZIONE	169
STRUMENTO 4 - SMART AREA: SERVIZI DIGITALI TERRITORIALI AVANZATI	171
I. <i>Obiettivo</i>	171
II. <i>Destinatari</i>	171
III. <i>Crediti</i>	171

1.12.	GLOSSARIO	172
1.13.	PRINCIPI GENERALI.....	173
1.14.	CASI D'USO.....	174
1.15.	STRATEGIE DI IMPLEMENTAZIONE PER UNA SMART AREA: LINEE GUIDA GENERALI	175
STRUMENTO 5 - INTELLIGENZA ARTIFICIALE NELLA PUBBLICA AMMINISTRAZIONE		177
I.	<i>Obiettivo</i>	177
II.	<i>Destinatari</i>	177
III.	<i>Crediti</i>	177
1.16.	AI ACT: UN APPROCCIO BASATO SUL RISCHIO	178
1.17.	LA VISIONE DEL LABORATORIO ARTIFICIAL INTELLIGENCE AND INTELLIGENT SYSTEMS (AIIS) DEL CINI	179
1.18.	POSSIBILI OBIETTIVI	179
1.19.	SUGGERIMENTI PER LE AZIONI DIRETTE ALLE PA.....	180
1.20.	L'ESPERIENZA DI INAIL.....	182
1.21.	L'ESPERIENZA DI INPS	189
1.22.	L'ESPERIENZA DI ISTAT	193

INTRODUZIONE

Il Piano Triennale per l'informatica nella Pubblica Amministrazione (di seguito Piano triennale) è uno strumento fondamentale per promuovere la trasformazione digitale del Paese attraverso quella della Pubblica Amministrazione italiana.

In un contesto socioeconomico in continua evoluzione, l'informatica e le nuove tecnologie emergenti rivestono oggi un ruolo fondamentale e necessitano di un Piano e di una programmazione di ampio respiro in ambito pubblico, che tenga conto delle molteplici variabili sul tema e dei cambiamenti in atto.

L'evoluzione delle soluzioni tecnologiche rese disponibili e l'adeguamento delle norme rivolte all'ambito della digitalizzazione, nonché gli interventi finanziari europei e nazionali sul tema, stanno accompagnando e rafforzando notevolmente la strada della trasformazione digitale già in corso.

Fin dalla sua prima edizione (2017-2019) il Piano triennale ha rappresentato il documento di supporto e di orientamento per le pubbliche amministrazioni italiane nella pianificazione delle attività sul percorso di innovazione tecnologica e nelle edizioni successive ha costituito il riferimento per declinare le strategie che si sono susseguite nel tracciato operativo composto da obiettivi e attività.

L'edizione 2021-2023 prefigurava un quadro di sintesi degli investimenti nel digitale nell'ambito della Strategia Italia Digitale 2026, in quel momento appena pubblicata; l'aggiornamento 2022-2024 del Piano è stato caratterizzato dalla presenza sempre più pervasiva del Piano Nazionale di Ripresa e Resilienza (PNRR), che ha rappresentato e rappresenta una straordinaria opportunità di accelerazione della fase di esecuzione della trasformazione digitale della PA.

Le problematiche dell'amministrazione pubblica possono trovare nuove soluzioni grazie alla trasformazione digitale, se questa viene vista come "riforma" dell'azione amministrativa e quindi come un nuovo tipo di "capacità istituzionale" che ogni ente pubblico deve strutturare nel proprio funzionamento interno (*"riorganizzazione strutturale e gestionale"* ex art.15 CAD) ed esterno (facendo sistema con gli altri enti pubblici e anche con le imprese, i professionisti, le università/centri di ricerca, il terzo settore, ecc.).

Il Piano triennale 2024-26 presenta alcuni cambiamenti nella sua struttura, rispetto alle edizioni precedenti; inoltre, alcuni contenuti sono stati approfonditi per sostenere in modo efficace le pubbliche amministrazioni nel processo di implementazione e gestione dei servizi digitali. L'introduzione delle tecnologie non porta a cambiamenti se non si ripensa l'organizzazione dei procedimenti e l'attività amministrativa, con una revisione dei processi delle amministrazioni secondo il principio *once only*.

Il nuovo Piano triennale si inserisce in un contesto di riferimento più ampio definito dal programma strategico "Decennio Digitale 2030", istituito dalla Decisione (UE) 2022/2481 del Parlamento Europeo e del Consiglio del 14 dicembre 2022, i cui obiettivi sono articolati in quattro dimensioni: competenze digitali, servizi pubblici digitali, digitalizzazione delle imprese e infrastrutture digitali sicure e sostenibili.

La strategia alla base del Piano triennale 2024-26 nasce quindi dalla necessità di ripensare alla programmazione della digitalizzazione delle pubbliche amministrazioni basata su nuove leve strategiche, tenendo conto di tutti gli attori coinvolti nella trasformazione digitale del Paese, e degli obiettivi fissati per il 2030 dal percorso tracciato dalla Commissione europea per il Decennio Digitale.

Gli investimenti del Piano Nazionale di Ripresa e Resilienza e del Piano nazionale per gli investimenti complementari, oltre a quelli previsti dalla Programmazione Europea 2021-2027, rappresentano l'occasione per vincere queste sfide.

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)

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

Art. 14-bis Agenzia per l'Italia digitale (AGID)

(..)2. AGID svolge le funzioni di:

- a) emanazione di Linee guida contenenti regole, standard e guide tecniche, nonché di indirizzo, vigilanza e controllo sull'attuazione e sul rispetto delle norme di cui al presente Codice, anche attraverso l'adozione di atti amministrativi generali, in materia di agenda digitale, digitalizzazione della Pubblica Amministrazione, sicurezza informatica, interoperabilità e cooperazione applicativa tra sistemi informatici pubblici e quelli dell'Unione europea;
- b) programmazione e coordinamento delle attività delle amministrazioni per l'uso delle tecnologie dell'informazione e della comunicazione, mediante la redazione e la successiva verifica dell'attuazione del Piano triennale per l'informatica nella Pubblica Amministrazione contenente la fissazione degli obiettivi e l'individuazione dei principali interventi di sviluppo e gestione dei sistemi informativi delle amministrazioni pubbliche. Il predetto Piano è elaborato dall'AGID, anche sulla base dei dati e delle informazioni acquisiti dai soggetti di cui all'articolo 2, comma 2, ed è approvato dal Presidente del Consiglio dei ministri o dal Ministro delegato entro il 30 settembre di ogni anno (...)

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

Art. 1.

- Comma 512. Al fine di garantire l'ottimizzazione e la razionalizzazione degli acquisti di beni e servizi informatici e di connettività, fermi restando gli obblighi di acquisizione centralizzata previsti per i beni e servizi dalla normativa vigente, le amministrazioni pubbliche e le società inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1 della legge 31 dicembre 2009, n. 196, provvedono ai propri approvvigionamenti esclusivamente tramite Consip SpA o i soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi soggetti. (..)

- Comma 513. L'Agenzia per l'Italia digitale (AGID) predispone il Piano triennale per l'informatica nella Pubblica Amministrazione che è approvato dal Presidente del Consiglio dei Ministri o dal Ministro delegato. Il Piano contiene, per ciascuna amministrazione o categoria di amministrazioni, l'elenco dei beni e servizi informatici e di connettività e dei relativi costi, suddivisi in spese da sostenere per innovazione e spese per la gestione corrente, individuando altresì i beni e servizi la cui acquisizione riveste particolare rilevanza strategica.
- Comma 514. Ai fini di cui al comma 512, Consip SpA o il soggetto aggregatore interessato, sentita l'AGID per l'acquisizione dei beni e servizi strategici indicati nel Piano triennale per l'informatica nella Pubblica Amministrazione di cui al comma 513, programma gli acquisti di beni e servizi informatici e di connettività, in coerenza con la domanda aggregata di cui al predetto Piano. (...) Consip SpA e gli altri soggetti aggregatori promuovono l'aggregazione della domanda funzionale all'utilizzo degli strumenti messi a disposizione delle pubbliche amministrazioni su base nazionale, regionale o comune a più amministrazioni.

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.

Modello strategico

Il modello strategico del Piano triennale 2024-26 definisce una architettura organizzativa e tecnologica che ha l'obiettivo di supportare la collaborazione tra i livelli istituzionali, nel rispetto dell'autonomia degli stessi enti, come previsto anche dall'art. 14 del Decreto legislativo 7 marzo 2005, n. 82 (CAD) sui rapporti tra Stato, Regioni e autonomie locali.

Art. 14 - Rapporti tra Stato, Regioni e autonomie locali

1. In attuazione del disposto dell'articolo 117, secondo comma, lettera r), della Costituzione, lo Stato disciplina il coordinamento informatico dei dati dell'amministrazione statale, regionale e locale, dettando anche le regole tecniche necessarie per garantire la sicurezza e l'interoperabilità dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime.
2. Lo Stato, le regioni e le autonomie locali promuovono le intese e gli accordi e adottano, attraverso la Conferenza unificata, gli indirizzi utili per realizzare gli obiettivi dell'Agenda digitale europea e nazionale e realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso e per l'individuazione delle Linee guida.

La Presidenza del Consiglio dei Ministri, anche avvalendosi dell'AGID, assicura il coordinamento informatico dell'amministrazione statale, regionale e locale, con la finalità di progettare e monitorare l'evoluzione strategica del sistema informativo della Pubblica Amministrazione, favorendo l'adozione di infrastrutture e standard che riducano i costi sostenuti dalle amministrazioni e migliorino i servizi erogati (..).

2-bis. Le regioni promuovono sul territorio azioni tese a realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso tra le autonomie locali.

2-ter. Le regioni e gli enti locali digitalizzano la loro azione amministrativa e implementano l'utilizzo delle tecnologie dell'informazione e della comunicazione per garantire servizi migliori ai cittadini e alle imprese, secondo le modalità di cui al comma 2.

In una logica di miglioramento continuo, il modello strategico del Piano triennale 2024-26 propone una architettura organizzativa e tecnologica che ha l'obiettivo di fornire una visione complessiva della Pubblica Amministrazione digitale che parte dal "sistema informativo" del singolo ente per arrivare a definire le relazioni con i servizi, le piattaforme e le infrastrutture nazionali erogate a livello centrale.

Il modello strategico del Piano triennale 2024-26 classifica le sfide organizzative e tecnologiche che le amministrazioni devono affrontare in tre macroaree:

- processi
- applicazioni
- tecnologie

Tale modello ha l'obiettivo di indirizzare le sfide legate sia al funzionamento del sistema informativo di un singolo organismo pubblico, sia al funzionamento del sistema informativo pubblico complessivo dell'intero Paese, nell'ottica del principio *cloud-first* e di una architettura policentrica e federata.

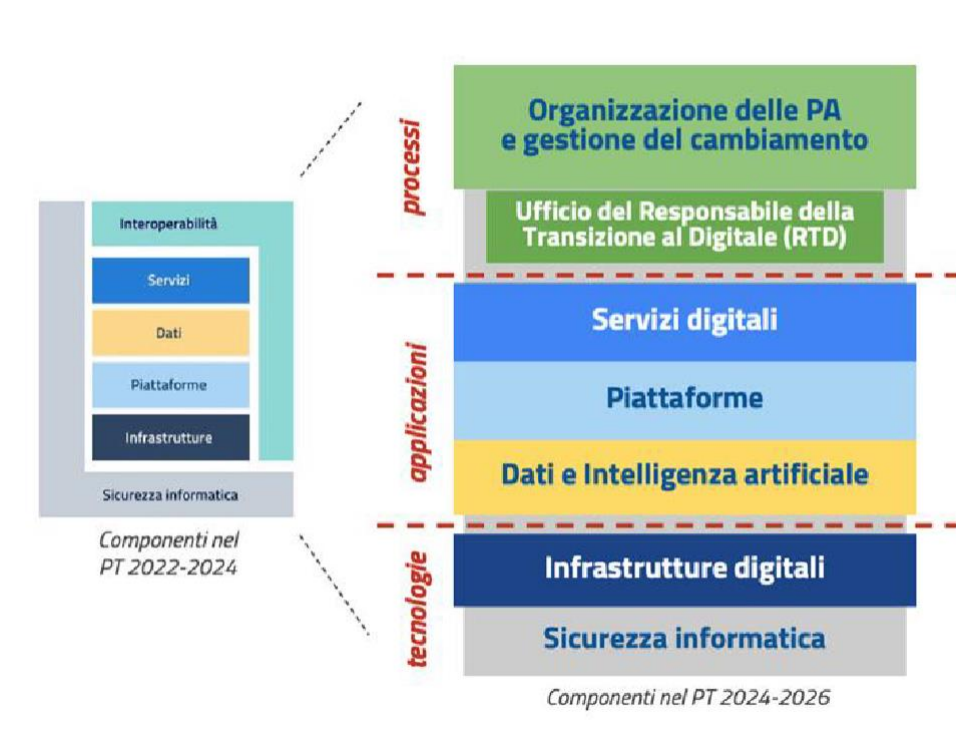


Figura 1 - Modello strategico del Piano triennale 2024-26

Per ogni livello dell'architettura è necessario tracciare, a partire dal Piano triennale, strumenti, regole tecniche e traiettorie evolutive pluriennali, che permettano una pianificazione degli investimenti su un piano istituzionale multilivello, a valere su molteplici fonti di finanziamento.

In questo contesto assume fondamentale rilevanza il Piano integrato di attività e organizzazione (PIAO), introdotto dall'art. 6 del Decreto-legge 80/2021 al fine di *"assicurare la qualità e la trasparenza dell'attività amministrativa e migliorare la qualità dei servizi ai cittadini e alle imprese e procedere alla costante e progressiva semplificazione e reingegnerizzazione dei processi (...)".* Il PIAO implementa quella che il CAD definisce all'art.15 come una *"riorganizzazione strutturale e gestionale"*, per sfruttare le opportunità offerte dal digitale.

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

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.

I principi sono riassunti nella tabella seguente, con i relativi riferimenti normativi:

Principi guida	Definizioni	Riferimenti normativi
1. Digitale e mobile come prima opzione (<i>digital & 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
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
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
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"
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
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
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 "PNIS" DL 82/2021 "ACN"
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"

Principi guida	Definizioni	Riferimenti normativi
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 l'amministrazione aperta e la condivisione di buone pratiche sia amministrative che tecnologiche	Art.9, art.17 c.1 ed art.68-69 CAD Art.1 c.1 D.Lgs 33/2013 Art.30 D.Lgs 36/2023
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

Percorso di elaborazione del Piano triennale

Il Piano triennale 2024-26 è il risultato di un'attività di scambio e concertazione tra amministrazioni e soggetti istituzionali che hanno contribuito anche alla redazione delle precedenti edizioni. Nel mese di settembre 2023 è stato istituito un Tavolo di concertazione, con l'obiettivo di costituire una struttura permanente per un'azione concertata di definizione dei contenuti e delle strategie indicate dal Piano stesso. Hanno partecipato ai lavori del Tavolo coordinato dall'Agenzia per l'Italia Digitale: Agenzia per la Cybersicurezza Nazionale (ACN), Associazione Nazionale Comuni Italiani (ANCI), Commissione per l'Innovazione Tecnologica e la Digitalizzazione della Conferenza delle Regioni e delle Province autonome (CITD), Dipartimento della Funzione Pubblica (DFP), Dipartimento per la Trasformazione Digitale (DTD), Istituto nazionale Assicurazione Infortuni sul Lavoro (INAIL), Istituto Nazionale della Previdenza Sociale (INPS), Istituto Poligrafico e Zecca dello Stato (IPZS), Istituto Nazionale di Statistica (ISTAT), Ministero dell'Economia e delle Finanze (MEF), pagoPA S.p.A, Unione Province d'Italia (UPI). Altri *stakeholders* potranno aggiungersi nel tempo, con contributi su specifici

aspetti. Consip, ad esempio, ha fornito alcuni chiarimenti sul tema delle gare strategiche ICT.

Il Piano triennale è stato sottoposto anche ad un percorso di confronto allargato con università, mondo della ricerca e mondo delle imprese e sono stati accolti e integrati nel Piano i loro suggerimenti, con la prospettiva di rendere sempre più stretta questa collaborazione.

Articolazione del Piano e guida alla lettura

Il Piano è strutturato in tre parti:

- Parte prima – Componenti strategiche per la trasformazione digitale: è articolata in 2 capitoli che descrivono le leve strategiche su cui investire per accelerare il processo di trasformazione digitale delle PA, focalizzando l'attenzione su un approccio innovativo che affronti, in maniera sistematica, tutti gli aspetti legati a organizzazione, processi, regole, dati e tecnologie.
- Parte seconda – Componenti tecnologiche: le componenti tecnologiche del modello strategico sono riportate nei capitoli (numerati da 3 a 7) su Servizi, Piattaforme, Dati e intelligenza artificiale, Infrastrutture, Sicurezza. Il tema dell'interoperabilità diventa trasversale a tutti i capitoli ed è evidenziato in particolare nel capitolo dedicato ai Servizi. Il capitolo "Dati" è integrato da una sezione nuova dedicata all'intelligenza artificiale. Sono riportati alcuni principi generali che dovranno essere adottati dalle pubbliche amministrazioni e declinati in fase di applicazione, tenendo in considerazione lo scenario in veloce evoluzione.
- Parte terza – Strumenti. La novità di questo Piano è quella di riportare una sezione verticale dedicata agli strumenti che le amministrazioni possono prendere a riferimento come modelli di supporto, esempi di buone pratiche, *check-list* per pianificare i propri interventi. Questa sezione è destinata ad ampliarsi e ad essere sistematicamente aggiornata sul sito AGID, nelle pagine dedicate al Piano triennale. Nelle parti prima e seconda, alla fine di ciascun capitolo è presente un breve paragrafo che elenca anche gli specifici strumenti legati all'argomento trattato in quel capitolo stesso

Per meglio comprendere la terminologia utilizzata nel Piano si è ritenuto opportuno fornire un "Glossario" in appendice. Inoltre, per offrire un quadro di maggiore dettaglio su alcune tematiche chiave, sul sito web di AGID, sempre nella sezione dedicata al Piano triennale, saranno riportati opportuni approfondimenti.

La struttura del Piano triennale 2024-26, mantiene, ove possibile all'interno dei capitoli, la stessa impostazione delle precedenti edizioni:

- Lo **Scenario** introduce brevemente i temi affrontati nel capitolo, illustra lo stato dell'arte in raccordo con i Piani precedenti e offre un'anteprima delle traiettorie future, evidenziando anche i relativi punti di attenzione ed azioni essenziali utili a tutti gli enti;
- Il **Contesto normativo e strategico** elenca i riferimenti a cui le amministrazioni devono attenersi, in termini di fonti normative con *link* a documenti e/o siti ufficiali e riferimenti ad attività progettuali finanziate, compresi i riferimenti agli specifici investimenti del PNRR;
- le sezioni **Obiettivi e Risultati attesi** descrivono i macro-obiettivi del Piano sul tema specifico e, per ciascun obiettivo individuano i risultati attesi (RA) e relativi target annuali, ove presenti, per il triennio 2024-2026;
- la sezione **Linee di azione istituzionali** specifica tempi e linee di azione (attività) a carico di AGID, Dipartimento per la Trasformazione Digitale, ACN e altri soggetti istituzionali per il conseguimento di ciascun obiettivo;
- la sezione **Linee di azione per le PA** specifica le linee di azione (attività) a carico delle diverse PA, che derivano dalle azioni dei soggetti istituzionali sopra indicati.

Al fine di fornire informazioni e riferimenti operativi di supporto alle amministrazioni destinatarie del Piano sono stati inseriti due ulteriori paragrafi alla fine di ciascun capitolo:

- **Strumenti per l'attuazione del Piano**

Sono elencati gli strumenti collegati ai contenuti del capitolo specifico, con i *link* relativi. Si tratta di piattaforme web, *tools*, linee guida, documentazione di riferimento.

- **Risorse e fonti di finanziamento**

Sono inseriti gli eventuali riferimenti alle risorse e fonti di finanziamento disponibili per supportare gli interventi da parte delle amministrazioni. Ad esempio, vengono segnalate le opportunità di ricorrere a gare strategiche ICT, di rispondere ad avvisi e bandi pubblici e di intercettare misure PNRR di interesse.

Come per le edizioni precedenti, questo Piano rappresenta un lavoro comune *in progress*, e negli aggiornamenti previsti per gli anni 2025 e 2026 verranno ulteriormente dettagliate tematiche e azioni ad oggi in fase di definizione.

PARTE PRIMA – Componenti strategiche per la trasformazione digitale

Capitolo 1 - Organizzazione e gestione del cambiamento

L'ecosistema digitale amministrativo

La trasformazione digitale richiede un processo integrato, finalizzato alla costruzione di ecosistemi digitali strutturati sostenuti da organizzazioni pubbliche semplificate, trasparenti, aperte, digitalizzate e con servizi di qualità, erogati in maniera proattiva per anticipare le esigenze del cittadino. Gli ecosistemi vengono quindi qui intesi con un significato diverso da quello usato in precedenti versioni del Piano triennale.

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

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

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

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

Essendo l'azione amministrativa composta da processi collettivi è necessario introdurre dei "processi digitali collettivi" basati su e-service, ovvero interfacce API che scambiano dati/informazioni in maniera automatica e interoperabile, come illustrato nel capitolo 3 - Servizi.

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

Si tratta di passare da una concezione di *"Piattaforma per Governo"*, ovvero piattaforme per singoli scopi dell'ente, a una visione più profonda del paradigma, ovvero il *"Governo come Piattaforma"* come riportato anche nella Comunicazione EU (2021)118 sulla Bussola Digitale 2030, secondo cui l'ecosistema non è un elemento esterno all'ente, ma è qualcosa sostenuto dall'ente pubblico per abilitare servizi migliori.

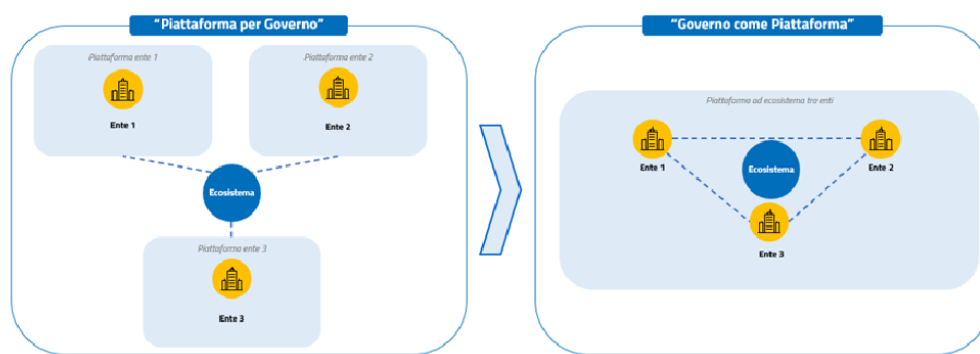


Figura 2 - Duplice concezione: da Piattaforma per Governo a Governo come Piattaforma

Per facilitare l'innovazione occorre analizzare l'attuale impianto normativo che impatta sulla trasformazione digitale, per generare proposte di semplificazione amministrativa in grado di rimuovere gli ostacoli all'innovazione nelle pubbliche amministrazioni.

Da questo punto di vista, nel corso dei prossimi anni si ritiene necessario:

- definire un processo integrato finalizzato alla costruzione di ecosistemi digitali strutturati sostenuti da organizzazioni pubbliche semplificate, trasparenti, aperte, digitalizzate e con servizi di qualità erogati e definire schemi organizzativi per il raccordo tra Ufficio del RTD (Responsabile per la transizione al digitale) e il resto dell'organizzazione pubblica in cui lo stesso ufficio è inserito;
- definire uno strumento agile per la catalogazione dei macro-processi delle singole organizzazioni pubbliche e per la mappatura tra questi processi, i servizi erogati e i sottostanti servizi digitali applicativi che li sostengono.

In questo sistema risultano fondamentali i processi di collaborazione istituzionale e il ruolo del Responsabile per la transizione al digitale e dell'Ufficio transizione digitale (di seguito RTD e UTD), come funzioni e agenti cruciali del cambiamento, sia di processo che tecnologico.

La collaborazione istituzionale

Il processo di trasformazione digitale coinvolge, a tutti i livelli, decisori pubblici, dirigenza pubblica, cittadini e imprese nella logica della partecipazione e della consultazione. Per affrontare questa trasformazione è necessario delineare e seguire un iter di transizione che richiede collaborazione tra tutte le componenti istituzionali, nel quadro di un sistema nazionale per la trasformazione digitale di cui facciano parte Governo, Enti centrali, Regioni e Province autonome, Enti locali e che sia aperto anche a tutto il partenariato economico e sociale.

La collaborazione consiste nel coinvolgimento delle varie strutture operative esistenti con la missione di sostenere la continua trasformazione digitale del Paese, per rendere esigibili i diritti di cittadinanza digitale e contribuire alla sostenibilità e alla crescita economica e sociale.

In questo senso si rileva l'importante lavoro di interlocuzione con il territorio svolto dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri che ha portato alla stipula di accordi istituzionali strategici con le principali rappresentanze territoriali, nello specifico con: la Conferenza delle Regioni e delle Province autonome, l'Associazione Nazionale Comuni Italiani e l'Unione delle Province Italiane.

Come suggerito da diverse associazioni di categoria ICT, si ritiene importante porre l'attenzione anche

sulla collaborazione tra pubblico e privato, ritenuta altrettanto strategica per sfruttare appieno le caratteristiche dell'Italia nel contesto digitale e diventare un Paese innovativo. Supportare e contribuire a realizzare un ambiente florido di micro, piccole e medie imprese è un ulteriore fattore di sostegno all'innovazione che, in una logica di crescita integrata sia nel pubblico che nel privato, accelera l'economia, come dimostrato in altri Paesi in cui questo segmento è stato sviluppato con successo.

Tale approccio è volto a: i) suggerire un rafforzamento dell'adozione di politiche specifiche per le micro, piccole e medie imprese, per favorirne il finanziamento e l'accesso nella PA, ii) aumentare la digitalizzazione della Pubblica Amministrazione; iii) favorire e rafforzare la concorrenza tutelando le MPMI e migliorando ancora il processo già in atto di modifiche di alcune norme sugli appalti; iv) rimodulare gli incentivi fiscali per le aziende modellandoli sulle specificità delle piccole e medie imprese; v) intervenire sul sistema scolastico per incentivare la creazione di professionisti dell'innovazione.

Per arrivare all'integrazione effettiva dei processi e al ridisegno dei servizi pubblici delineato dalle norme vigenti è necessario prevedere percorsi e strumenti che portino ogni Pubblica Amministrazione ad essere in grado di erogare ed utilizzare gli e-service all'interno di domini strutturati, ovvero "spazi di interoperabilità e cooperazione applicativa", e di permettere scambi di dati e informazioni attraverso interfacce API sia con le altre pubbliche amministrazioni che con gli attori privati interessati.

Per favorire questo processo è necessario che alcune amministrazioni possano svolgere il ruolo di coordinamento (*hub* nazionali e/o regionali).

Nello specifico si evidenziano due possibili scenari per gli enti locali:

1. gli enti locali hanno l'opportunità di interfacciarsi direttamente con le amministrazioni capofila (*hub* nazionali e/o regionali), attraverso spazi di interoperabilità (es. Piattaforma Digitale Nazionale Dati – PDND) per definire processi digitali integrati a supporto dei servizi erogati ai cittadini;
2. le amministrazioni capofila possono agevolare i bisogni ed il raggiungimento degli obiettivi dei singoli enti locali attraverso la condivisione dei processi. Nello specifico, gli enti locali possono delegare in via amministrativa le amministrazioni capofila, le quali gestiscono la totalità o parte dei processi per conto degli enti locali. Questo secondo approccio consente agli enti locali l'utilizzo dei processi delle amministrazioni capofila efficientando la gestione e la riduzione notevole di risorse pubbliche.

Quali primi esempi di tali spazi di interoperabilità, nati tutti dalla collaborazione tra Governo, Amministrazioni centrali, Regioni e Enti locali, si possono citare alcuni interventi in corso di realizzazione nell'ambito del PNRR:

- il Fascicolo Sanitario Elettronico 2.0;
- la Piattaforma Digitale Nazionale Dati – PDND;
- il Sistema degli Sportelli Unici (SSU) riferito a SUAP/SUE;
- l'implementazione nazionale dello Sportello Digitale Unico europeo - SDG;
- l'ecosistema nazionale di approvvigionamento digitale (*e-procurement*)
- l'Hub del Turismo Digitale (TDH).

Risulta quindi di fondamentale importanza per tutte le pubbliche amministrazioni:

1. una forte collaborazione tra i vari livelli istituzionali coinvolti per la corretta strutturazione di e-service, e quindi di servizi digitali integrati ed interoperabili; quindi, tra gli obiettivi prioritari

- di ciascun ente dovrebbe esserci l'individuazione di quei procedimenti/procedure più richiesti/utilizzati da cittadini/imprese, che possono beneficiare dell'applicazione dei principi *once-only* e *API-first* attraverso la reingegnerizzazione (quando erogati in autonomia) oppure attraverso processi digitali collettivi (quando coinvolgono più enti per pareri, verifiche, ecc.).
2. il presidio di tutto il ciclo di vita degli *e-service* da parte dell'ente; è necessario poter disporre di competenze specialistiche adeguate all'interno dell'Ufficio per la transizione al digitale in forma singola o associata.

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

Scenario

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

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

Circa la metà risultano essere amministrazioni comunali, in particolare di piccole dimensioni, o loro aggregazioni; ma il *trend* di nomina degli RTD presso tali tipologie di PA risulta essere in costante aumento e si rileva che alcune PA locali, sulla base delle proprie esigenze, hanno colto l'opportunità di procedere alla nomina del RTD e alla costituzione dell'Ufficio per la transizione digitale in forma associata, in aderenza a quanto previsto dal comma 1-septies dell'art. 17 del CAD.

La collaborazione tra amministrazioni è infatti una delle leve a disposizione degli Enti per mettere a fattor comune risorse e competenze per raggiungere gli obiettivi di trasformazione digitale, attraverso la nomina del RTD e dell'UTD in forma associata, che permette di individuare un unico ufficio dirigenziale generale a cui affidare la transizione alla modalità operativa digitale e i conseguenti processi di digitalizzazione.

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

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

Il processo di collaborazione tra enti va incoraggiato e viene agevolato dalla condivisione di pratiche e soluzioni tra gli enti stessi e dalla disponibilità di modelli attuativi da sperimentare e adattare alla singola realtà territoriale o tematica.

La costituzione di un UTD in forma associata, prevista per le PA diverse da quelle centrali dall'art. 17 comma 1-septies, è diversa dalla gestione associata della funzione ICT che spesso caratterizza le Unioni di Comuni. Come chiarito dalla Circolare 3 del 2018 del Ministro per la Pubblica Amministrazione, può “avvenire in forza di convenzioni o, per i Comuni, anche mediante l'Unione di Comuni” e quindi può rappresentare un'opportunità per le Amministrazioni e gli enti pubblici di mettere a fattor comune risorse per favorire la transizione digitale.

Si possono quindi individuare alcune azioni utili per tutte le pubbliche amministrazioni:

1. occorre istituire, ove non sia stato già fatto, l'Ufficio per la transizione al digitale, in forma singola o associata, con conseguente nomina del Responsabile per la transizione al digitale (RTD). Nell'ottica del suddetto ecosistema, la struttura organizzativa va potenziata. Ove ciò non sia sostenibile a livello di singolo ente, per le PA diverse da quelle centrali è possibile ricorrere all'istituzione di UTD associati a livello di Unione di Comuni o attraverso lo strumento della convenzione tra amministrazioni, con eventuale coinvolgimento di Province, Regioni, Province autonome e loro società *in house*;
2. per strutturare l'ente come ecosistema digitale amministrativo è essenziale il potenziamento del ruolo e della dotazione di risorse umane e strumentali dell'UTD e la definizione, con appositi atti, di schemi organizzativi chiari rispetto al raccordo e all'attribuzione di competenze (“*ratione materiae*”) tra RTD ed altre figure dirigenziali dell'ente. L'erogazione dei servizi pubblici passa sempre più da strumenti digitali; quindi, è fondamentale la progettazione di sistemi informativi e servizi digitali e sicuri *by design*, affinché siano moderni, accessibili, di qualità e di facile fruizione;
3. la mappatura dei processi dell'ente, e la loro revisione in chiave digitale, può prendere le mosse da quanto già fatto nell'ente per la valutazione del rischio corruttivo, integrando opportunamente la mappatura già realizzata con altre informazioni presenti nell'ente come, ad esempio, il Catalogo dei procedimenti dell'ente e il Catalogo dei servizi erogati dall'ente;
4. all'interno del PIAO – Piano Integrato di Attività e Organizzazione, previsto dall'articolo 6 del decreto-legge n. 80 del 9 giugno 2021, occorre ricomprendere gli obiettivi specifici di digitalizzazione, semplificazione e reingegnerizzazione, a partire dalla mappatura di cui sopra e dalle priorità del singolo ente.

A sostegno del rafforzamento dei RTD e degli UTD continua, inoltre, ad essere strategica la disponibilità di strumenti utili ed iniziative per favorire l'aggiornamento sulle materie di competenza e per condividere soluzioni e pratiche, nonché di occasioni di incontro e tavoli di confronto interistituzionali.

È in quest'ottica che AGID mette a disposizione la [piattaforma di community ReTeDigitale](#) dedicata ai RTD e al personale degli UTD, le comunità digitali tematiche/ territoriali al suo interno e le iniziative laboratoriali con l'obiettivo di supportare i processi di trasformazione digitale nelle Amministrazioni centrali, locali e negli Enti presenti nell'Indice dei domicili digitali della Pubblica Amministrazione e dei Gestori di pubblici servizi.

Risulta fondamentale inoltre sfruttare al massimo i tavoli di incontro istituzionale e favorire le occasioni di scambio e condivisione tra amministrazioni e tra RTD anche attraverso il rilancio della Conferenza dei RTD con incontri periodici e iniziative di prossimità sul territorio per favorire la più ampia partecipazione anche da parte dei piccoli enti.

Inoltre, va incentivato l'approccio proattivo delle amministrazioni e degli enti pubblici nel condividere dati, esperienze, proposte; sono *in primis* da valorizzare e promuovere le iniziative a livello territoriale

che vedono la partecipazione congiunta di RTD e UTD di enti diversi, che attraverso attività di *scouting* e condivisione favoriscono la diffusione delle eccellenze e l'individuazione di soluzioni ai problemi più diffusi.

Il livello locale-territoriale di rete va, come prima richiamato, esteso al mondo imprenditoriale, per favorire ulteriormente gli scambi tra pubblico e privato.

Contesto normativo e strategico

Riferimenti normativi italiani:

- [Decreto legislativo 7 marzo 2005, n. 82 “Codice dell'amministrazione digitale” \(in breve CAD\) art. 17.](#)
- [Circolare n. 3 del 1° ottobre 2018 del Ministro per la Pubblica Amministrazione sul Responsabile per la transizione al digitale.](#)

Obiettivo 1.1 - Migliorare i processi di trasformazione digitale della PA

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

- **Target 2024** - 18 comunità digitali tematiche/territoriali su [retedigitale.gov.it](#) gestite da AGID, PA o Enti locali
- **Target 2025** - Almeno 2 ulteriori comunità digitali tematiche/territoriali su [retedigitale.gov.it](#) gestite da AGID, PA o Enti locali
- **Target 2026** - Almeno 2 ulteriori comunità digitali tematiche/territoriali su [retedigitale.gov.it](#) gestite da AGID, PA o Enti locali

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

- **Target 2024** - Vademecum per la nomina di RTD e UTD in forma associata
- **Target 2025**
 - Report sulle PA pilota che hanno adottato il modello di nomina RTD e organizzazione dell'UTD in forma associata
 - Raccolta di modelli organizzativi/operativi degli UTD
- **Target 2026** - Report sulle PA pilota che hanno adottato nuovi modelli organizzativi/operativi dell'UTD

Linee di azione istituzionali

RA1.1.1

- **Giugno 2024** - Predisposizione del kit per richiesta, gestione e monitoraggio di una comunità digitale tematica/territoriale su [retedigitale.gov.it](#) da parte di PA ed Enti locali - (AGID) - CAP1.01
- **Gennaio 2025** - Primo report di monitoraggio sulle comunità digitali su [retedigitale.gov.it](#) - (AGID) - CAP1.02
- **Giugno 2025** - Campagna di diffusione dei risultati delle *community* e di promozione di nuove comunità - (AGID) - CAP1.03
- **Gennaio 2026** - Secondo report di monitoraggio sulle comunità digitali su [retedigitale.gov.it](#) - (AGID) - CAP1.04

- **Giugno 2026** - Campagna di diffusione dei risultati delle *community* e di promozione di nuove comunità - (AGID) - CAP1.05

RA1.1.2

- **Marzo 2024** - Rilascio della prima versione del Vademecum sulla nomina del Responsabile per la transizione al digitale e sulla costituzione dell'Ufficio per la transizione al digitale in forma associata - (AGID) - CAP1.06
- **Aprile 2024** - Avvio dei lavori del Laboratorio Modelli organizzativi/operativi degli UTD - (AGID) - CAP1.07
- **Giugno 2024** - Rilascio versione finale del Vademecum sulla nomina del Responsabile per la transizione al digitale e sulla costituzione dell'Ufficio per la transizione al digitale in forma associata - (AGID) - CAP1.08
- **Settembre 2025** - Raccolta *feedback* delle esperienze delle PA pilota che hanno adottato modello di nomina del RTD e di organizzazione dell'UTD in forma associata - (AGID) - CAP1.09
- **Novembre 2025** - Conclusione del laboratorio Modelli organizzativi/operativi ufficio RTD e redazione report finale - (AGID) - CAP1.10
- **Settembre 2026** - Raccolta *feedback* delle esperienze delle PA pilota che hanno adottato nuovi modelli organizzativi/operativi dell'UTD - (AGID) - CAP1.11

Linee di azione per le PA

RA1.1.1

- **Da marzo 2024** - Le Amministrazioni e gli Enti interessati possono proporre ad AGID l'attivazione di una comunità digitale tematica/territoriale su retedigitale.gov.it - CAP1.PA.01
- **Da luglio 2024** - Le Amministrazioni e gli Enti interessati utilizzano i *format* presenti nel kit per proporre nuove comunità digitali ed effettuare monitoraggi semestrali delle attività in esse svolte - CAP1.PA.02

RA1.1.2

- **Da marzo 2024** - Le PA partecipanti alle iniziative laboratoriali forniscono contributi e proposte di modifica e integrazione al Vademecum sulla nomina del Responsabile per la transizione al digitale e sulla costituzione dell'Ufficio per la transizione al digitale in forma associata - CAP1.PA.03
- **Da marzo 2024** - Le PA partecipanti alle iniziative laboratoriali e che hanno adottato modelli organizzativi/operativi per l'Ufficio per la transizione al digitale condividono le esperienze, gli strumenti sviluppati e i processi implementati - CAP1.PA.04
- **Da luglio 2024** - Le PA partecipanti alle iniziative laboratoriali sperimentano i modelli proposti e forniscono ad AGID il *feedback* delle esperienze di nomina RTD e UTD in forma associata realizzate - CAP1.PA.05
- **Da dicembre 2025** - Le PA partecipanti alle iniziative laboratoriali sperimentano i modelli proposti e forniscono ad AGID il *feedback* sui nuovi modelli organizzativi/operativi dell'UTD adottati - CAP1.PA.06

Competenze digitali per il Paese e per la PA

Scenario

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

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

Il tema delle competenze digitali acquista un particolare rilievo nel contesto della vita pubblica, che vede confrontarsi gli utenti di servizi pubblici digitali e la Pubblica Amministrazione, erogatrice dei medesimi servizi. LA PA, in particolare, necessita di competenze digitali per i propri dipendenti (a tutti i livelli, dirigenziali e non dirigenziali), e di competenze digitali specifiche del settore professionale e di intervento (come, ad esempio, nella Sanità e nella Giustizia), ma soprattutto esprime un fabbisogno crescente di competenze ICT specialistiche.

Come già indicato nelle precedenti edizioni del Piano triennale per l'informatica nella PA, l'Italia ha definito una propria "Strategia nazionale per le competenze digitali" con un Piano operativo di attuazione, verificato e aggiornato sulla base di un ciclo annuale di monitoraggio, nell'ambito dell'iniziativa strategica nazionale "Repubblica Digitale". La maggior parte delle azioni presenti nel Piano operativo è finanziata e inclusa nel PNRR.

Per quanto riguarda in particolare i cittadini, nel 2023 hanno preso avvio le attività correlate all'investimento 1.7 del PNRR, "Competenze digitali di base", che si pone l'obiettivo di ridurre la quota di cittadini a rischio di esclusione digitale tramite:

- il potenziamento della Rete dei Centri di facilitazione digitale con la messa in esercizio sul territorio di 3.000 Punti Digitale Facile entro il 2024 per l'accrescimento delle competenze digitali di base di 2 milioni di cittadini al 2026 (sub-investimento 1.7.2);
- la creazione di una rete di giovani volontari per lo sviluppo e il miglioramento delle competenze digitali, su 3 cicli annuali per realizzare 700.000 interventi di facilitazione e/o educazione digitale sul territorio a fine 2025 nell'ambito del "Servizio Civile Digitale (sub-investimento 1.7.1).

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

Il fabbisogno di competenze digitali nella Pubblica Amministrazione riguarda tutta la popolazione dei pubblici dipendenti: tanto dei dirigenti, chiamati a esercitare la propria funzione pubblica in un

contesto essenzialmente trasformato dalla tecnologia, che del personale di livello non dirigenziale, Esempi di iniziative in risposta a tale fabbisogno sono:

- l’iniziativa “Syllabus per la formazione digitale”, che mira a consentire a tutti i dipendenti delle amministrazioni aderenti l’accesso, attraverso la piattaforma *online* del Dipartimento della Funzione Pubblica [Syllabus](#), a percorsi formativi sulle competenze digitali erogati in e-learning e personalizzati a partire da una rilevazione *online*, strutturata ed omogenea dei fabbisogni individuali di formazione. L’iniziativa rimarca la responsabilità collettiva di tutte le PA al perseguimento degli obiettivi di *upskilling* e *reskilling* dei dipendenti pubblici previsti nell’ambito della Missione 1, Componente 1, sub-investimento 2.3.1 del PNRR. La Direttiva introduce, infatti, una serie puntuale di *milestone* e *target* per tutte le amministrazioni al fine di assicurare, entro il 2025, il completamento della formazione sulle competenze digitali messa a disposizione a titolo gratuito sulla piattaforma Syllabus, da parte di un numero progressivamente crescente di dipendenti pubblici;
- le proposte formative della Scuola Nazionale dell’Amministrazione, che nel 2024 vedranno l’attivazione di corsi sia in modalità *e-learning* che *blended* e in presenza, su tematiche quali la cybersicurezza e i sistemi in *cloud*, le tecnologie abilitanti per l’organizzazione, la digitalizzazione nel PNRR, la progettazione della trasformazione digitale e la gestione dell’innovazione, fino al ruolo di intelligenza artificiale (IA) e dati nei sistemi decisionali di supporto alla PA.;
- a livello territoriale, nell’ambito dell’accordo stipulato tra ANCI e il Dipartimento per la Trasformazione Digitale, è stata costituita l’*Academy* ANCI, specificamente dedicata alla formazione di funzionari e dirigenti comunali. L’*Academy* realizzerà iniziative volte ad accrescere le competenze degli operatori comunali a fornire un’informazione costante, attraverso incontri *online* e in presenza, mirati sia all’attuazione degli Avvisi emanati dal Dipartimento nell’ambito della Misura 1 Componente 1 del PNRR, sia - di più ampio respiro - alle priorità legate al processo di digitalizzazione della PA (tali iniziative, nel 2023 hanno registrato circa 5.000 partecipanti).

La Strategia nazionale per le competenze digitali prevede inoltre lo sviluppo di competenze specialistiche ICT per fronteggiare le sfide legate alle tecnologie emergenti e al possesso delle competenze chiave per i lavori del futuro con il coordinamento di Ministero dell’Università e Ricerca e Ministero dell’Impresa e del *Made in Italy*.

In particolare, le azioni di formazione e divulgazione hanno l’obiettivo di ridurre il divario di genere presente in ambito ICT, incentivando la partecipazione della popolazione femminile ai corsi di laurea e alle professioni ICT ed eliminando gli stereotipi che alimentano il divario nelle STEM e in ICT. Le azioni rispondono alla necessità di costituire strutture di supporto per il genere femminile, non solo per l’orientamento e la scelta di percorsi di studio, ma anche in termini di *reskilling* e *upskilling*, oltre che di supporto nel progresso di carriera.

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

Queste azioni sono in linea con quelle proposte dalle Associazioni di categoria ICT: i) il potenziamento dei Licei Scientifici e gli ITIS con indirizzo tecnologico aumentando il numero di classi del 50% rispetto all’attuale programmazione, ii) l’aumento del numero degli Istituti Tecnologici Superiori (ITS), iii) il

monitoraggio del proseguimento degli studenti nei percorsi post-diploma e nel mondo del lavoro, premiando le scuole superiori e i docenti il cui tasso di giovani NEET (Non in Educazione, Occupazione o Formazione) nei 12 mesi successivi al diploma sia inferiore a una percentuale prefissata, iv) la creazione di un fondo per lo sviluppo di programmi formativi in collaborazione con le aziende, v) l'adattamento rapido dei programmi alle richieste del mercato vi) la riduzione del gap di competenze tecnologiche da parte dei docenti.

Il PNRR sostiene le azioni del Piano volte a favorire l'incremento di specialisti ICT e l'occupazione di queste risorse nei settori considerati strategici per la crescita del Paese, con particolare riferimento agli investimenti dedicati al potenziamento delle condizioni di supporto alla ricerca e all'innovazione (M4C2 Investimento 3).

Lo sviluppo di una rete di formazione digitale per le amministrazioni locali, al fine di supportare la trasformazione tecnologica e dei processi, è l'auspicio anche delle Associazioni di impresa ICT. Le micro e piccole imprese digitali locali, che costituiscono oltre il 90% delle imprese ICT italiane, possono creare una rete di piccoli fornitori qualificati che siano punto di riferimento sul territorio. Collaborare con queste realtà locali offre vantaggi duplici per le pubbliche amministrazioni: evitare la dipendenza unicamente da grandi aziende e favorire la presenza locale, contribuendo all'occupazione nelle aree periferiche.

Per ciò che concerne il ruolo degli specialisti ICT all'interno delle PA occorre quindi promuovere strumenti per la definizione della "famiglia professionale" degli specialisti ICT nella PA, e per il loro corretto inquadramento all'interno del CCNL e per strutturare dei chiari percorsi di carriera, anche perché oggi, per queste figure professionali, le PA non sono concorrenziali rispetto al mercato.

Inoltre, nell'ambito del PNRR, e in particolare dell'investimento 2.3 M1C1, è prevista l'attivazione di almeno 20 "comunità di competenze" (*community of Practice*), trasversali alle amministrazioni, tra le quali si annoverano anche quelle dedicate alla *digital transformation*: l'intervento, a titolarità della Scuola Nazionale dell'Amministrazione, è destinato a sviluppare e contaminare *best practice* all'interno della PA.

Contesto normativo e strategico

Riferimenti normativi europei:

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

Obiettivo 1.2 - Diffusione competenze digitali nel Paese e nella PA

RA1.2.1 - Diffusione competenze digitali di base per cittadini e imprese

- **Target 2024** - 48% popolazione 16-74 anni con competenze digitali almeno di base (rilevazione Istat-Eurostat 2023)
- **Target 2025** - 2 milioni di cittadini che hanno fruito dei servizi di facilitazione e formativi dei progetti PNRR “Competenze digitali di base” misura 1.7
- **Target 2026** - 57% popolazione 16-74 anni con competenze digitali almeno di base (rilevazione Istat-Eurostat 2025)

RA1.2.2 - Diffusione competenze digitali di base nella PA

- **Target 2024** - Partecipazione di almeno 136.000 dipendenti pubblici a iniziative di miglioramento del livello di competenze e di qualificazione in ambito digitale
- **Target 2025** - Partecipazione di ulteriori 107.200 dipendenti pubblici a iniziative di miglioramento del livello di competenze e di qualificazione in ambito digitale
- **Target 2026** - Partecipazione di ulteriori 136.800 dipendenti pubblici a iniziative di miglioramento del livello di competenze e di qualificazione in ambito digitale

RA1.2.3 - Diffusione delle competenze specialistiche ICT

- **Target 2024** - 4% quota di specialisti ICT sul totale occupati (rilevazione 2023 Istat-Eurostat)
- **Target 2025** - 100.000 persone formate su competenze ICT (risultato complessivo iniziativa Fondo Repubblica Digitale – Fondo complementare PNRR)
- **Target 2026** - 5% quota di specialisti ICT sul totale occupati (rilevazione 2025 Istat-Eurostat)

Linee di azione Istituzionali

RA1.2.1

- **Gennaio 2024** - Pubblicazione dell’Avviso PNRR per la terza annualità del Servizio Civile Digitale - (Dipartimento per la Trasformazione Digitale) - CAP1.12
- **Ottobre 2024** - Terzo aggiornamento del Piano operativo della Strategia nazionale per le competenze digitali, sulla base del rapporto di monitoraggio sull’attuazione e dei dati rilevati sul 2023-2024, a cura del Comitato tecnico guida di Repubblica Digitale - (Dipartimento per la Trasformazione Digitale) - CAP1.13
- **Dicembre 2024** - Avvio dei 3000 punti di facilitazione digitale (Punti Digitale Facile) previsti dal progetto di potenziamento e sviluppo della rete dei servizi di facilitazione digitale, incluso nel PNRR - (Dipartimento per la Trasformazione Digitale) - CAP1.14
- **Dicembre 2025** - Raggiungimento della quota di 700mila servizi di facilitazione ed educazione digitale erogati attraverso le tre annualità PNRR del progetto Servizio Civile Digitale - (Dipartimento per la Trasformazione Digitale) - CAP1.15

RA1.2.2

- **Gennaio 2024** - Ampliamento del catalogo formativo nell'ambito dell'iniziativa "Syllabus per la formazione digitale" su tematiche specifiche connesse alla transizione digitale - (Dipartimento della Funzione Pubblica) - CAP1.16
- **Giugno 2024** - Attivazione del 100% dei corsi SNA inclusi nella programmazione didattica dell'area Innovazione e Trasformazione Digitale della PA - (Scuola Nazionale dell'Amministrazione) - CAP1.17
- **Dicembre 2024** - Erogazione di almeno 10 *webinar* su Intelligenza Artificiale per cittadini, imprese e PA - (AGID) - CAP1.18

RA1.2.3

- **Febbraio 2024** - Pubblicazione di un *position paper* della Coalizione Nazionale Repubblica Digitale sul quadro di interventi per l'incremento delle competenze specialistiche ICT - (Dipartimento per la Trasformazione Digitale) - CAP1.19

Nell'ambito delle attività di supporto alla diffusione delle competenze specialistiche ICT, sono inoltre previste le seguenti azioni per gli anni accademici, a partire dall'anno accademico 2023/2024:

- finanziamento di borse di dottorato in programmi dedicati alla transizione digitale (Ministero dell'Università e della Ricerca).
- finanziamento di borse di studio per dottorato di ricerca e innovativi per la Pubblica Amministrazione e il patrimonio culturale (Ministero dell'Università e della Ricerca).
- sostegno finanziario alle università per aumentare le iscrizioni ai corsi di studio in materie ICT nell'ambito della misura "Piano Laureati ICT". (Ministero dell'Università e della Ricerca).
- creazione di tre *Digital Education Hub* (DEH) per migliorare le capacità del sistema di istruzione superiore di offrire formazione sul digitale a studenti e lavoratori universitari. (Ministero dell'Università e della Ricerca).

Si evidenzia che all'interno dei capitoli successivi di questo Piano sono definite Linee di azione specifiche per la realizzazione di un'offerta formativa per dipendenti pubblici su temi specialistici quali accessibilità, dati, intelligenza artificiale, sicurezza informatica, ecc.

Linee di azione per le PA

Linee di azione vigenti

- Le PA, in funzione delle proprie necessità, partecipano alle iniziative pilota, alle iniziative di sensibilizzazione e a quelle di formazione di base e specialistica per il proprio personale, come previsto dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali - CAP1.PA.07
- Le PA aderiscono all'iniziativa "Syllabus per la formazione digitale" e promuovono la partecipazione alle iniziative formative sulle competenze di base da parte dei dipendenti pubblici, concorrendo al conseguimento dei target del PNRR in tema di sviluppo del capitale umano della PA e in linea con il Piano strategico nazionale per le competenze digitali - CAP1.PA.08
- Le PA, in funzione della propria missione istituzionale, realizzano iniziative per lo sviluppo delle

Monitoraggio

Scenario

Il Codice dell'Amministrazione Digitale, all'art.14-bis lettera c), ha attribuito ad AGID il compito di realizzare il monitoraggio delle attività e la verifica dei risultati delle amministrazioni, in termini sia di coerenza con il Piano triennale e sia di costi/benefici dei sistemi informativi delle singole PA.

Allo stesso tempo, tali azioni di monitoraggio e verifica hanno l'obiettivo di supportare l'attuazione fisica, finanziaria e procedurale del Piano triennale nel suo complesso.

Il monitoraggio della trasformazione digitale del Paese si articola su più livelli:

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

Queste attività vengono condotte in coerenza con gli indicatori del Programma europeo [Decennio Digitale](#), che prevede un sistema di monitoraggio strutturato, trasparente e condiviso, basato sull'indice di digitalizzazione dell'economia e della società (DESI), e integrato con nuovi indicatori, per misurare i progressi compiuti verso ciascuno degli obiettivi per il 2030.

Per individuare la proposta di nuovi indicatori e nuove metodologie di valorizzazione maggiormente attinenti con le caratteristiche della digitalizzazione italiana, è in fase di costituzione un gruppo di lavoro AGID-ISTAT-DTD. Il gruppo di lavoro avrà anche l'obiettivo di delineare sistema di valutazione dei servizi digitali pubblici che sia coerente con il quadro di riferimento europeo e con i principi dell'*eGovernment benchmark*.

Nell'edizione 2022-2024 del Piano triennale è stato inoltre avviato il percorso di allineamento dei risultati attesi con i target degli [interventi PNRR in materia di digitalizzazione](#) M1C1.

A partire dagli esiti delle attività indicate, AGID avvierà il processo di definizione di indice di digitalizzazione della PA italiana che permetta di ottenere una visione del livello di maturità digitale degli enti pubblici e di introdurre le azioni correttive necessarie al raggiungimento degli obiettivi previsti dalle strategie nazionali ed europee

Osservatorio sulla Digitalizzazione nel Territorio Italiano

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

quindi come strumento di analisi istituzionale che ha il potenziale di diventare un asset strategico per il monitoraggio del Piano triennale per l'informatica nella Pubblica Amministrazione.

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

Contesto normativo e strategico

Riferimenti normativi italiani:

- [Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" \(in breve CAD\) art. 14-bis lettera c\)](#)

Riferimenti normativi europei:

- [Ministerial Declaration on eGovernment - Tallinn declaration - 6 ottobre 2017](#)
- [Regolamento \(UE\) 2018/1724 del 2 ottobre 2018 che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento \(UE\) 1024/2012](#)
- [Berlin Declaration on Digital Society and Value-based Digital Government – 8 dicembre 2020](#)
- [Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al comitato delle regioni Bussola per il digitale 2030: il modello europeo per il decennio digitale](#)
- [Decisione \(UE\) 2022/2481 del Parlamento europeo e del Consiglio del 14 dicembre 2022 che istituisce il programma strategico per il decennio digitale 2030](#)
- [Decisione di esecuzione \(UE\) della Commissione Europea del 30 giugno 2023 che definisce gli indicatori chiave di prestazione per misurare i progressi compiuti verso il conseguimento degli obiettivi digitali di cui all'articolo 4, paragrafo 1, della decisione \(UE\) 2022/2481 del Parlamento europeo e del Consiglio](#)

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

RA1.3.1 - Definizione di un indice di digitalizzazione della PA italiana

- **Target 2024** - Misurazione della *baseline* degli indicatori dell'indice di digitalizzazione della PA su un primo campione rappresentativo di Amministrazioni
- **Target 2025** - Almeno 1.000 amministrazioni alimentano l'indice di digitalizzazione
- **Target 2026** - Almeno 3.000 amministrazioni alimentano l'indice di digitalizzazione

RA1.3.2 - Acquisizione ed elaborazione di informazioni analitiche da Enti locali

- **Target 2024** - Raccolta dati tramite *survey*, coinvolgendo attivamente gli Enti locali per ottenere un quadro iniziale dello stato di digitalizzazione
- **Target 2025** - Secondo ciclo di raccolta dati tramite *survey*, permettendo un confronto con i dati raccolti nell'anno precedente e identificando eventuali *trend*
- **Target 2026** - Consolidamento i dati raccolti nei due anni precedenti per ottenere una visione approfondita e affidabile dello stato di digitalizzazione, fornendo basi solide per le decisioni future

RA1.3.3 - Aumento delle tipologie e delle fonti dati integrate all'interno dell'Osservatorio

- **Target 2024** - Integrazione di 5 nuove fonti dati nell'Osservatorio, laddove possibile attraverso l'accesso diretto a registri, database e documenti ufficiali *machine-readable*, ampliando la varietà e la profondità delle informazioni disponibili
- **Target 2025** - Ulteriori 5 fonti dati, continuando a diversificare le fonti integrate per ottenere una visione più completa e dettagliata della digitalizzazione delle pubbliche amministrazioni locali
- **Target 2026** - Integrazione di altre 5 fonti dati nell'Osservatorio, garantendo una copertura informativa sempre più esaustiva e approfondita

Linee di azione Istituzionali

RA1.3.1

- **Marzo 2024** - Definizione dei valori *target* delle tabelle di marcia nazionali strategiche per il Decennio Digitale - (Dipartimento per la Trasformazione Digitale) - CAP1.20
- **Marzo 2024** - Costituzione del Gruppo di lavoro tra AGID, ISTAT e DTD per la proposta di nuove metodologie di valorizzazione degli indicatori del Digital Decade maggiormente attinenti con le caratteristiche della digitalizzazione italiana - (AGID, ISTAT, Dipartimento per la Trasformazione Digitale) - CAP1.21
- **Giugno 2024** - Definizione di *KPI (Key Performance Indicator)* che facciano parte dell'indice di digitalizzazione e definizione del campione - (AGID) - CAP1.22
- **Dicembre 2024** - Raccolta dati dal campione per alimentazione indice di digitalizzazione del campione e presentazione dei risultati - (AGID) - CAP1.23
- **Giugno 2025** - Aggiornamento *KPI* dell'indice di digitalizzazione - (AGID) - CAP1.24
- **Dicembre 2025** - Raccolta dati dal campione per alimentazione indice di digitalizzazione del campione e presentazione dei risultati - (AGID) - CAP1.25
- **Giugno 2026** - Aggiornamento *KPI* dell'indice di digitalizzazione - (AGID) - CAP1.26
- **Dicembre 2026** - Raccolta dati dal campione per alimentazione indice di digitalizzazione del campione e presentazione dei risultati - (AGID) - CAP1.27

RA1.3.2 e RA1.3.3

- **Giugno 2024** - Avvio della prima fase di raccolta e verifica dei dati da integrare nell'Osservatorio, garantendo l'accuratezza e la completezza delle informazioni - (Dipartimento per la Trasformazione Digitale) - CAP1.28
- **Dicembre 2024** - Pubblicazione del primo report sullo stato della digitalizzazione, comunicando i risultati e le tendenze emerse dalla fase iniziale di monitoraggio - (Dipartimento per la Trasformazione Digitale) - CAP1.29
- **Marzo 2025** - Avvio della seconda fase di raccolta e verifica dei dati, adottando eventuali miglioramenti identificati nella fase precedente - (Dipartimento per la Trasformazione Digitale) - CAP1.30
- **Dicembre 2025** - Pubblicazione del secondo report sullo stato della digitalizzazione, fornendo un'analisi più approfondita e identificando le aree di miglioramento - (Dipartimento per la Trasformazione Digitale) - CAP1.31

Linee di azione per le PA

RA1.3.1

- **Febbraio 2025** - Le PA che fanno parte del campione alimentano l'indice di digitalizzazione secondo la metodologia definita dal Gruppo di lavoro - CAP1.PA.10

RA1.3.2 e RA1.3.3

- **Settembre 2024** – Gli Enti locali partecipano alla prima fase della raccolta dati, garantendo l'accuratezza e la completezza delle informazioni - CAP1.PA.11
- **Settembre 2025** – Gli Enti locali partecipano alla seconda fase della raccolta dati, garantendo l'accuratezza e la completezza delle informazioni - CAP1.PA.12

Strumenti per l'attuazione del Piano

OB1.1

- [Piattaforma AGID Rete digitale](#)
- [Community e Laboratori AGID di supporto ai RTD](#)

OB1.3

- [Piattaforma PA digitale 2026](#)

Risorse e fonti di finanziamento

OB1.2

- PNRR:
 - Competenze digitali di base dei cittadini: M1C1 Investimento 1.7 PNRR - Competenze digitali di base
 - Competenze specialistiche ICT: M4C2 Investimento 3 Fondo Complementare PNRR per il Fondo per la Repubblica Digitale M1 - C2 - Inv. 1 Transizione 4.0 M4-C2.1 - inv. 1.5 Creazione e rafforzamento di "ecosistemi dell'innovazione".

La transizione digitale e l'INFN

Il contesto in cui opera l'Ente

L'Istituto Nazionale di Fisica Nucleare (INFN) è l'ente pubblico di ricerca, vigilato dal MUR, dedicato allo studio dei costituenti fondamentali della materia e alle loro interazioni; la sua attività di ricerca, teorica e sperimentale si estende ai campi della fisica subnucleare, nucleare e delle astro-particelle. L'Ente considera inoltre con grande attenzione tutte le applicazioni, derivanti da tale ricerca di base, che abbiano un significativo impatto sulla società, il territorio e il suo tessuto produttivo, e costituiscano un importante stimolo per l'innovazione tecnologica del nostro Paese.

L'INFN è impegnato da anni nella informatizzazione delle proprie procedure e nella costruzione di un sistema informativo coerente centrato su un sistema di autenticazione ed autorizzazione (AAI) atto a regolare sia gli accessi al calcolo scientifico, sia quelli al calcolo gestionale attraverso l'attribuzione di ruoli in un unico database autoritativo.

Tale sistema è stato integrato con SPID e CIE (vedi capitolo 4); è in programma per il 2024 l'introduzione del doppio fattore di autenticazione e l'upgrade del livello di sicurezza a LoA3 per poterlo armonizzare e possibilmente integrare con le richieste dei sistemi esterni (ad esempio le piattaforme di *e-procurement*).

In questo senso le maggiori difficoltà provengono dalla scarsa integrabilità delle procedure e delle piattaforme acquistate sul mercato, per le quali le autorizzazioni necessitano di inserimento manuale e che normalmente non consentono un facile scambio di dati e documenti con le procedure interne dell'ente, ed ancor più dalla mancanza totale di interfacce della piattaforma Consip.

Per quanto riguarda l'informatizzazione delle procedure interne, da qualche anno ci si è orientati verso la loro reingegnerizzazione, coniugando semplificazione burocratica e realizzazione di architetture software basate su micro-servizi, rendendo i propri prodotti software adeguati alla realizzazione del principio *cloud-first* su una infrastruttura interna già esistente di *business-continuity* distribuita su due siti (il CNAF, in fase di trasferimento al nuovo tecnopolo di Bologna, ed i Laboratori Nazionali di Legnaro – LNL – vicino Padova) e dotata di un sistema di *disaster recovery* in un terzo (presso i Laboratori Nazionali di Frascati – LNF).

L'obiettivo finale, già da un paio d'anni perseguito, è di implementare, anche al proprio interno, il principio *once-only*, interfacciando le varie parti del sistema tramite API definite secondo gli stessi standard utilizzati per l'interoperabilità con le banche dati di interesse generale (ad esempio la PDND), costruendo così un ambiente di sviluppo il più possibile omogeneo e pronto ad utilizzare le informazioni certificate provenienti da banche dati pubbliche.

L'organizzazione dell'RTD nell'INFN

Responsabile per la Transizione Digitale

Nominato con disposizione presidenziale 26218 del 04 dicembre 2023

Enrico Pasqualucci

enrico.pasqualucci@infn.it

Ufficio per la transizione Digitale

Resp. Claudio Ciamei

claudio.ciamei@infn.it

Responsabile dell'Ufficio

Comitato di Coordinamento della Transizione Digitale

rtd-sc@lists.infn.it

Il Comitato di Coordinamento per la Transizione Digitale

L'Istituto, occupandosi di ricerca scientifica che richiede l'elaborazione di grandi quantità di dati, ha costruito negli anni strutture interne dedicate alla gestione di centri di calcolo, alla gestione del calcolo scientifico, alla sicurezza informatica ed alla gestione della propria rete, che si appoggia sulla rete GARR della ricerca. Come la necessità di calcolo distribuito per l'analisi dei dati dei grandi esperimenti aveva reso l'Istituto protagonista nella realizzazione del sistema GRID, l'emergere di tecnologie di tipo *cloud* ha reso disponibili competenze interne su questo argomento dedicate ad offrire servizi al mondo della ricerca, ma anche alla realizzazione di una infrastruttura di servizi nazionali sulla quale sono ospitati i servizi gestionali non acquistati su *cloud* esterne.

È stato quindi naturale fin da subito affiancare l'RTD, oltre che con l'UTD, con le figure professionali che guidano le varie attività dell'ente in campo informatico e dalle opportune competenze in campo giuridico (DPO, ufficio legale), formando un comitato di coordinamento, recentemente formalizzato ai sensi del DPCM 5 dicembre 2023 e composto, oltre che dall'RTD, da:

- Componenti del DPO e dell'Ufficio Legale
- Responsabile della Prevenzione della Corruzione e della Trasparenza
- Presidente della Commissione Calcolo e Reti
- Gruppo Auditing
- Direttore dei Sistemi Informativi
- Responsabile Sicurezza Informatica
- Responsabile della Gestione Documentale
- Responsabile della Conservazione
- License Manager
- Responsabile della Infrastruttura di Autenticazione ed Autorizzazione
- Rappresentante del gruppo Data Cloud

Il comitato si riunisce una volta al mese per consentire di definire e monitorare le attività che sono state delineate per poter supportare il processo di trasformazione digitale dell'Istituto. Si è inoltre provveduto alla nomina di un referente per la Transizione al Digitale in ogni struttura INFN, per favorire la trasmissione di informazioni e le linee guida prodotte dall'Ufficio Transizione al Digitale e che possa costituire un presidio di supporto per le strutture stesse. Allo stesso tempo, l'RTD dispone di un gruppo di *auditing*, dedicato al monitoraggio dell'attuazione delle norme del GDPR e delle indicazioni e delle direttive da seguire per tutte le aree interessate alla trasformazione digitale.

Le aree di intervento

Di seguito si riportano le diverse aree di intervento con la descrizione degli obiettivi del triennio.

Area Accessibilità

Per affrontare l'argomento accessibilità, l'approccio seguito è stato quello di creare dei gruppi di lavoro ad hoc che affrontassero le varie aree di intervento (Siti, Applicazioni e Documenti). Si prevede la definizione di linee guida, formalizzate attraverso la pubblicazione di pillole formative e note tecniche, per la redazione di documenti e per la realizzazione di *web application* in modo da garantire l'accessibilità dei propri prodotti (identificare strumenti, pubblicare how-to, definire linee guida e fare formazione di editori web e di documenti). Per quanto riguarda i siti web, è stato prodotto un nuovo template per tutti i siti ufficiali delle strutture dell'ente, che sono attualmente in fase di realizzazione.

Si aggiunge la pianificazione di un programma triennale di formazione sull'accessibilità previsto per tutto il Personale INFN.

Area Sicurezza Informatica

Dotare l'Ente di strumenti organizzativi, tra i quali un Sistema di Gestione della Sicurezza delle Informazioni ISO/IEC 27001, procedurali e operativi, nonché di un'infrastruttura centrale per la gestione di tutti gli aspetti della cybersecurity: protezione, controllo, risposta e governo.

Migliorare la postura di sicurezza dell'Ente attraverso attività specifiche e mirate:

- aumento della consapevolezza dell'utenza;
- adozione di policy di sicurezza comuni/coordinate e strumenti/infrastrutture centralizzati;
- definizione di una baseline per la configurazione sicura dei servizi informatici esposti.

Il piano si articola sulle seguenti linee d'azione generali:

- formazione del personale e miglioramento della consapevolezza in materia di sicurezza informatica e, in particolare, in riferimento alle pratiche di gestione della posta elettronica (riconoscimento del phishing), delle credenziali di accesso (introduzione all'utilizzo di password manager) e – in generale – di approccio all'utilizzo delle risorse informatiche;
- diminuzione del perimetro d'attacco e miglioramento della postura di sicurezza delle strutture mediante l'adozione di politiche coordinate e comuni per quanto riguarda la configurazione dei servizi esposti e degli strumenti di controllo e prevenzione;
- creazione di una struttura operativa centrale in grado di assolvere e coordinare le funzioni fondamentali di protezione, controllo, risposta e governo per tutto l'Ente;
- creazione di un'infrastruttura centralizzata per la raccolta dei dati di sicurezza dalle varie strutture, l'analisi degli stessi e la threat intelligence, al fine di implementare le opportune e necessarie attività preventive/proattive e reattive e il coordinamento con CERT/CSIRT nazionali e internazionali;
- promozione dell'utilizzo di un cybersecurity framework e di tool di risk assessment e monitoring;
- gestione del Rischio: Individuazione di un sistema di Valutazione del Rischio standardizzato da adottare in tutte le strutture come quello messo a disposizione dall'ACN "Tool di Risk Management", che permetta di valutare tutti gli aspetti inerenti alla sicurezza dell'informazione e permetta ai Titolari dei dati una visione complessiva efficace ed efficiente.

Area Auditing cyber-security-privacy

La diffusione delle minacce informatiche, le normative cogenti (GDPR, NIS 1-2 regolamenti interni, ecc.) e le esperienze di certificazione 27001-9001-27017-27018 adottati in alcune strutture INFN hanno portato alla costituzione di un gruppo nazionale di monitoraggio delle misure adottate per la gestione dei sistemi ai fini della cyber-security e per la gestione dei dati personali.

Tale organismo, costituito con personale qualificato da enti di certificazione e seguendo lo standard UNI EN ISO 19011:2012, verifica il rispetto dei requisiti delle norme o di altre prescrizioni stabilite dall'organizzazione e fornisce informazioni per azioni correttive, preventive e di miglioramento.

Sono obiettivi generali, in continuità con gli anni precedenti:

- misure atte a mitigare, eliminare e prevenire i rischi di violazione di riservatezza, di integrità e disponibilità dei dati trattati e valutazione della continua adeguatezza degli obiettivi in linea con misure e standard definiti dalla Direzione;
- miglioramento del livello di compliance dell'Ente rispetto a normative sulla sicurezza informatica (nazionali e locali), privacy, clausole contrattuali, CAD (Codice di amministrazione Digitale);
- misurazione e analisi del funzionamento del Sistema di Gestione e rispondenza ai requisiti di sicurezza delle informazioni (audit interni, riesame della Direzione), gestione delle non conformità e azioni correttive, miglioramento continuo;
- mantenimento di una struttura organica e indipendente del servizio di Audit che garantisca i principi definiti negli standard, in modo da assicurare l'obiettività e l'imparzialità del processo, come indicato nell' Art.17 comma 1 lettera C del CAD.

Area Protezione dati personali

L'INFN considera i dati personali trattati per il raggiungimento dei fini istituzionali una componente fondamentale del proprio patrimonio immateriale e ritiene la loro tutela e valorizzazione un obiettivo strategico per incrementare la propria efficacia ed efficienza operativa.

L'INFN ritiene fondamentale, oltre che doveroso, strutturare ogni attività che coinvolga il trattamento di dati personali secondo i principi della *privacy by design* e *by default* ex art. 25 del Regolamento europeo n. 2016/679 (GDPR o Regolamento).

La predisposizione del nuovo Piano per la Transizione Digitale risulta ancora occasione particolarmente significativa per individuare i mezzi e definire le modalità di ciascun trattamento di dati personali effettuato nell'INFN mettendo in atto misure tecniche ed organizzative adeguate ad attuare in modo efficace i principi di protezione dei dati previsti dal GDPR ed integrando, negli stessi trattamenti, le garanzie dirette a tutelare i dati ed i diritti degli interessati.

Obiettivi previsti:

- completamento della messa in produzione del Registro dei trattamenti, realizzato in formato elettronico, ed articolato in schede predefinite secondo il contenuto stabilito dell'art. 30 del Regolamento, esso può essere implementato ed aggiornato dalle singole strutture mediante un'interfaccia web. Consente di descrivere i trattamenti focalizzando l'attenzione sugli elementi prestabiliti dal GDPR;
- proseguimento nell'attività di revisione dei trattamenti alla luce delle prescrizioni del Regolamento: l'obiettivo di strutturare i procedimenti amministrativi che coinvolgono il trattamento di dati personali in modo coerente con il principio di **privacy by design** e **by default** appare trasversale rispetto tutti i procedimenti e le attività.

È già in atto l'avvio di una revisione complessiva dei procedimenti amministrativi per verificarne la conformità al GDPR. Essa deve muovere dai trattamenti in essere, in tutto o in parte digitali, progettati e gestiti dalla Direzione Sistemi Informativi a partire dai procedimenti centralizzati e con particolare riguardo a quelli esternalizzati che devono essere progettati secondo modelli aderenti ai principi del Regolamento, garantendo maggiori standard di tutela ai dati trattati: si pensi, per esempio, ai dati raccolti nelle procedure concorsuali di reclutamento o di formazione (borse di studio o assegni di ricerca) o a quelli trattati per l'attribuzione di benefici assistenziali dei dipendenti.

In questo contesto appare utile progettare e realizzare una procedura informatizzata per la realizzazione della DPIA, adattata alla realtà dell'Istituto e compatibile con il nuovo registro elettronico del trattamento.

L'INFN, tenuto conto del crescente coinvolgimento in progetti di ricerca in ambito sanitario, attribuisce particolare rilevanza all'organizzazione delle attività secondo processi diretti a salvaguardare i principi di minimizzazione dei dati, limitazione delle finalità del trattamento e del periodo di conservazione oltre che a garantire l'adeguata sicurezza dei dati stessi.

A tal fine ritiene fondamentale strutturare trattamenti informatizzati dei dati di progetto in modo da accogliere dati già resi anonimi dalle Istituzioni sanitarie e, nel caso in cui i dati oggetto di studio pervenissero in forma pseudonimizzata, trattarli mediante infrastrutture informatiche, inclusi servizi *cloud* certificati, secondo standard internazionali.

Area Infrastruttura di Autenticazione e Autorizzazione

In questa area si prevede:

- l'introduzione di un framework standard per la gestione di attività di messa in produzione di un determinato prodotto o servizio;
- l'introduzione di uno standard FITSM/ITIL/ISO indispensabile per permettere un'organizzazione del lavoro che garantisca l'ottenimento di risultati condivisi e documentati;
- la realizzazione di una anagrafe INFN: per l'INFN è strategico disporre di informazioni omogenee per tutto il personale che prende parte alle varie attività dell'Ente. Non si tratta infatti di registrare e categorizzare solo il personale che usa le risorse informatiche, ma anche di collocare opportunamente in appositi DB il personale che si reca in visita alle strutture, che partecipa a eventi, che accede ai Laboratori come operatore per conto di Ditte esterne e di disporre di un meccanismo di registrazione delle persone fisiche, comprensivo di dati aggiuntivi utili a determinare la possibilità ed il livello di accesso della persona fisica tramite una ben definita identità digitale con appropriate caratteristiche;
- il dispiegamento dell'autenticazione a doppio fattore. Come previsto nel precedente piano triennale, è stato implementato un sistema di autenticazione a doppio fattore che è attualmente in fase pilota alla quale partecipano un gruppo limitato di *power users*. Nel corso dei prossimi mesi si analizzeranno i feedback sul sistema e si estenderà la fase pilota gradualmente a tutti gli utenti dopo aver eventualmente implementato correttivi per un migliore fruibilità del sistema;
- uno studio di fattibilità della realizzazione di un autenticatore unico per INFN-AAI: nelle strutture INFN ci sono ancora molteplici sistemi di autenticazione che potrebbero essere ricondotti ad un unico sistema centralizzato. Passare ad un autenticatore unico permetterebbe tra l'altro anche una più agevole implementazione di autenticazione a molti fattori per i servizi non-Web, mantenendo le funzionalità in produzione e quelle previste dall'autenticazione a molti fattori;
- Identity Assurance Framework: adesione ai profili di garanzia delle identità digitali definiti della Federazione GARR-IDEM. Tali profili, compatibili con quelli definiti dalle comunità di operatori di federazione europei eduGAIN e REFEDS, permettono di associare all'identità digitale gli attributi indispensabili per l'accesso a risorse anche critiche (ad esempio sistemi di supercalcolatori) che richiedono garanzie sull'aggiornamento e la qualità degli attributi relativi all'identità digitale stessa ed un comune standard di gestione e comunicazione.

Area Protocollo Informatico

La registrazione informatica dei documenti è rappresentata dall'insieme di dati in forma elettronica allegati o connessi al documento informatico al fine dell'identificazione univoca di tutti i documenti prodotti e acquisiti. Per la Pubblica Amministrazione vale quanto disposto ai sensi dell'articolo 53 comma 5 del TUDA.

La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare, per tutti i documenti ricevuti o spediti dalla Pubblica Amministrazione e per tutti i documenti informatici che non rientrano tra le tipologie specificate dall'art. 53, comma 5 del TUDA.

Le pubbliche amministrazioni hanno l'obbligo di effettuare la registrazione informatica di tutti i documenti prodotti ed acquisiti, in conformità a quanto stabilito nelle Linee guida emanate dall'AGID ed entrate in vigore il 1° gennaio 2022, che costituiscono la versione aggiornata delle regole tecniche in materia di formazione, protocollazione, gestione e conservazione del documento informatico, già precedentemente regolate nei DPCM del 2013 e 2014.

Nell'ambito di ciascuna Area Organizzativa Omogenea dell'Ente, in seno all'Unità Organizzativa di Servizio/Direzione è costituito l'Ufficio Protocollo i cui compiti sono:

- garantire le operazioni di registrazione di protocollo di tutti i documenti in ingresso e in uscita;
- garantire le registrazioni dei documenti esclusi dalla registrazione di protocollo, per cui è prevista una registrazione particolare ai sensi dell'art. 53 comma 5 del TUDA;
- garantire le modalità di formazione, gestione e archiviazione dei fascicoli informatici delle aggregazioni documentali informatiche con l'insieme minimo dei metadati ad essi associati;
- seguire il regolare ripristino della funzionalità del sistema in caso di guasti o anomalie; curare le operazioni di annullamento delle registrazioni effettuate, autorizzate dal RGD (Responsabile Gestione Documentale);
- aprire e chiudere il registro di emergenza autorizzato dal RGD, curandone la conservazione dei dati in attesa del riversamento nell'applicativo di protocollo informatico dopo il ripristino del sistema;
- garantire il riallineamento dell'archivio di protocollo dopo la compilazione del registro di emergenza.

Alla guida delle attività di gestione del protocollo informatico e dell'archivio di ciascuna AOO è posto un Responsabile (Responsabile della Gestione Documentale) ed un suo Vicario che sono anche responsabili del servizio di protocollo.

L'attività di coordinamento del protocollo informatico di tutte le AOO è a carico del CNGD (Coordinatore Nazionale della Gestione Documentale) il cui compito è garantire una gestione unica dei documenti secondo criteri uniformi di classificazione ed archiviazione.

D'intesa con il RTD e con il Responsabile della Conservazione è stato redatto il nuovo Manuale della Gestione Documentale, entrato in vigore il 1° febbraio 2022, e pubblicato sul sito dell'Amministrazione Centrale.

Obiettivi generali:

- educare gli utenti attraverso percorsi di formazione mirata alla corretta attività di protocollazione dei documenti informatici (gestione, classificazione e fascicolazione);
- istruire i RGD e vicari delle strutture nell'adottare gli stessi criteri nel trattamento della documentazione amministrativa e non;
- istruire i referenti locali dell'RTD attraverso una formazione mirata;
- utilizzare l'anno 2024 per individuare un software di gestione documentale adatto alle esigenze dell'INFN con l'obiettivo di impostare una unica AOO per tutto l'Ente.

Area conservazione documentale

La conservazione sostitutiva è un processo regolamentato dal Codice dell'Amministrazione Digitale (D.lgs. 82/2005), che stabilisce le regole, i requisiti, i ruoli e le responsabilità dell'intero processo.

La Conservazione consente di sostituire i documenti cartacei con documenti in formato digitale dal valore legale, fiscale e tributario.

Conservare i documenti elettronici significa archivarli con modalità digitali, seguendo processi certificati che mantengano la validità giuridica dei documenti conservati, garantendone integrità e autenticità nel tempo.

Il processo di conservazione sostitutiva parte da uno o più documenti elettronici, che, raccolti in classi documentali, saranno raggruppati ed in tempi stabiliti inviati in conservazione (pacchetto di versamento o SIP). Al SIP viene apposta un'impronta informatica (una sequenza numerica detta chiave di hash) che rappresenta univocamente la sequenza di documenti elettronici inviati. L'impronta informatica viene firmata digitalmente, trasformandosi così nel pacchetto di archiviazione che sarà conservato.

Infine, nella fase finale di conservazione, viene apposta la marca temporale sul pacchetto di archiviazione per consentire al pacchetto di archiviazione di mantenere la sua validità nel tempo oltre le scadenze dei certificati di firma.

Obiettivi generali:

- inviare in conservazione tutte le classi documentali previste dalla normativa;
- metadatazione della documentazione in base ai requisiti delle Linee Guida AGID;
- produzione del Massimario di scarto per l'invio allo scarto dei documenti.

Linee di azione

L'INFN ha aderito all'iniziativa "Syllabus per la formazione digitale", registrando tutti i propri dipendenti ed invitandoli a seguire i corsi. Questa non è tuttavia l'unica iniziativa dedicata allo sviluppo del capitale umano, poiché l'Istituto promuove e finanzia la formazione continua dei propri dipendenti attraverso l'Ufficio Formazione. In particolare, un corso completo di amministrazione digitale ha raggiunto nel 2023 il 70% del personale amministrativo. Sono previsti corsi per tutti gli anni a seguire per raggiungere tutto il personale interessato e fornire aggiornamenti su temi specifici. Inoltre, l'introduzione di ogni procedura informatizzata è oggetto di formazione specifica. - CAP1.PA.07 e CAP1.PA.08

Capitolo 2 - Il *procurement* per la trasformazione digitale

Il *procurement* per la trasformazione digitale

Scenario

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

La concreta attuazione del processo di trasformazione digitale richiede la disponibilità di risorse professionali e strumentali, disponibili in parte all'interno dell'amministrazione pubblica e in parte e all'esterno. Ne consegue che grande attenzione va prestata affinché l'acquisizione di risorse dal mercato (*procurement*) sia realizzata con efficacia ed efficienza.

La stessa riforma nazionale del *procurement* pubblico introdotta dal Codice dei Contratti pubblici (Decreto lgs. N. 36 del 31 marzo 2023) soprattutto con riferimento alla Parte II, "Della digitalizzazione del ciclo di vita dei contratti", introduce un profondo percorso di trasformazione digitale degli acquisti della Pubblica Amministrazione volto alla semplificazione, velocizzazione delle procedure e maggiore trasparenza.

Ciò è tanto più importante se si tiene conto che nel decennio 2013-2022 la Pubblica Amministrazione italiana ha effettuato acquisti per un valore complessivo di oltre 2.900 Miliardi di euro e ha stipulato contratti con oltre 35.000 fornitori. Con un valore che si avvicina al 10% del PIL, la spesa pubblica in appalti è anche uno strumento di politica industriale per il Paese.

Di questa grande massa di risorse, la spesa in ICT è valutata in oltre 7 miliardi di euro per l'anno 2022, in aumento rispetto al 2021. Le progettualità in essere e prospettiche si focalizzano principalmente sull'aggiornamento dell'esistente, mentre ancora limitati sono gli investimenti verso l'introduzione di soluzioni digitali che puntino su tecnologie innovative *data-driven* o verso le nuove frontiere definite dall'adozione di sistemi di intelligenza artificiale.

Gli acquisti di beni e servizi standardizzati

A partire dall'anno 2000 il nostro Paese ha realizzato un programma di "Razionalizzazione degli acquisti", che si basa su strategie di aggregazione e centralizzazione degli acquisti pubblici, in tutti i settori, compreso l'ICT, la digitalizzazione e la trasformazione digitale.

L'attuazione del programma di razionalizzazione ha portato negli anni alla costruzione di un sistema di governance incentrato su ANAC, il rafforzamento di Consip quale centrale nazionale di acquisto, la costituzione del sistema dei soggetti aggregatori regionali e del relativo Tavolo tecnico coordinato dal Ministero dell'Economia e delle Finanze, un'imponente digitalizzazione del sistema appalti con la costituzione della Banca dati nazionale dei contratti pubblici (BDNCP).

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

Gli acquisti di innovazione per la trasformazione digitale

A partire dal 2013, il nostro Paese si è dotato di norme specifiche anche per promuovere gli appalti di ricerca e innovazione, che definiscono un quadro di coordinamento istituzionale tra i livelli ministeriali di governo, i soggetti finanziatori e le agenzie che attuano gli acquisti. La stessa Agenda Digitale Italiana persegue l'obiettivo prioritario della modernizzazione dei rapporti tra Pubblica Amministrazione, cittadini e imprese, attraverso azioni coordinate dirette a favorire lo sviluppo di domanda e offerta di servizi digitali innovativi e a promuovere la crescita di capacità industriali adeguate a sostenere lo sviluppo di prodotti e servizi innovativi.

Gli acquisti di innovazione, nel prossimo triennio, sono indirizzati prioritariamente alla sperimentazione di modelli di commercializzazione ed acquisto di sistemi di intelligenza artificiale ed alla crescita di capacità industriali nel settore, anche attraverso collaborazioni internazionali.

Allo stato attuale, [Smarter Italy](#) è il principale programma di sperimentazione di appalti di innovazione.

L'ecosistema digitale degli acquisti pubblici

Nelle disposizioni della Parte II del Libro I artt. 19-36 "Digitalizzazione del ciclo di vita dei contratti pubblici" del Codice dei contratti pubblici, risulta centrale e obbligatorio dal primo gennaio 2024 lo svolgimento degli acquisti della Pubblica Amministrazione attraverso le piattaforme di approvvigionamento digitale (art. 25). Le stesse devono essere interoperabili, tramite Piattaforma Digitale Nazionale dei Dati (PDND), con la Banca dati nazionale dei contratti pubblici (BDNCP) (art. 23) di ANAC, l'infrastruttura tecnologica abilitante la gestione in digitale del ciclo di vita dei contratti pubblici (dalla programmazione fino all'esecuzione del contratto). In tal senso, la digitalizzazione dei contratti pubblici rappresenta un esempio virtuoso di infrastruttura pubblica al servizio di un complesso ecosistema composto da amministrazioni centrali, stazioni appaltanti, operatori economici e molti altri attori. In tale contesto, la PDND assume un ruolo centrale, non solo ai fini della messa in interoperabilità delle banche dati degli enti certificanti (oltre 10 amministrazioni centrali) che devono proseguire nel rendere disponibili i loro dati ai fini della piena operatività del Fascicolo Virtuale dell'Operatore Economico (FVOE, art. 24, Delibera ANAC n. 262 del 20 giugno 2023), ma anche in quanto consente l'accesso agli e-service di ANAC che abilitano l'operatività del ciclo di vita del *procurement*.

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

Organizzazione della stazione appaltante nel nuovo Codice dei Contratti Pubblici

La efficace realizzazione di un processo di acquisto, dalla programmazione alla esecuzione, necessita risorse professionali e organizzazione. Il nuovo Codice prevede che le stazioni appaltanti, per condurre acquisti complessi, siano dotate di risorse umane, risorse strumentali, adeguata esperienza. Pertanto, introduce il sistema di qualificazione delle stazioni appaltanti.

Il principio del risultato costituisce criterio prioritario per l'esercizio del potere discrezionale e per l'individuazione della regola del caso concreto, nonché per valutare la responsabilità del personale

che svolge funzioni amministrative o tecniche nelle fasi di programmazione, progettazione, affidamento ed esecuzione dei contratti e attribuire gli incentivi al personale coinvolto negli appalti

Nell'attuazione delle procedure di acquisto si richiede quel passaggio da un approccio puramente amministrativo a uno orientato al soddisfacimento delle esigenze concrete, la cui necessità è stata già individuata negli orientamenti della Commissione Europea.

La qualificazione della Stazione appaltante

La qualificazione delle Stazioni appaltanti è uno strumento per attestare la capacità di gestire direttamente, secondo criteri di qualità, efficienza e professionalizzazione, e nel rispetto dei principi di economicità, efficacia, tempestività e correttezza, le attività che caratterizzano il processo di acquisizione e riguarda almeno una delle fasi di progettazione, affidamento o esecuzione del contratto.

Il Codice dei contratti pubblici individua tre livelli di qualificazione, base, per servizi e forniture fino alla soglia di 750.000 euro; intermedia, fino a 5 milioni di euro e avanzata, senza limiti di importo.

Si precisa che il Codice, all'art. 114 comma 8, stabilisce che per i contratti di servizi e forniture di particolare importanza il direttore dell'esecuzione deve essere diverso dal RUP.

L'allegato II.14 del suddetto Codice, all'art. 32, stabilisce che sono considerati servizi di particolare importanza, indipendentemente dall'importo, gli interventi particolarmente complessi sotto il profilo tecnologico, le prestazioni che richiedono l'apporto di una pluralità di competenze, gli interventi caratterizzati dall'utilizzo di componenti o di processi produttivi innovativi o dalla necessità di elevate prestazioni per quanto riguarda la loro funzionalità. In via di prima applicazione del Codice sono individuati, tra i servizi di particolare importanza, quelli di telecomunicazione e i servizi informatici.

Sono, inoltre, considerate forniture di particolare importanza le prestazioni di importo superiore a 500.000 euro.

L'organizzazione della Stazione appaltante e il ruolo del RUP

Il "nuovo RUP", nel Codice è stato ridenominato responsabile unico di progetto (art. 15 D.lgs. 36/2023), avvicinandolo alla figura di un *project manager*, con capacità di gestione delle risorse finanziarie, strumentali ed umane di cui può disporre. Il nuovo Codice riconosce la complessità di una procedura che va dalla pianificazione all'esecuzione e consente alle amministrazioni di definire modelli organizzativi che sembrano più efficaci per la gestione dell'intero ciclo di vita dell'acquisto. Per ogni acquisto, si prevede la nomina di un responsabile di (sub)procedimento per le fasi di programmazione, progettazione, affidamento ed esecuzione. Le relative responsabilità sono ripartite in base ai compiti svolti in ciascuna fase, ferme restando le funzioni di supervisione, indirizzo e coordinamento del RUP.

Le stazioni appaltanti possono inoltre istituire una struttura di supporto al RUP e affidare incarichi di assistenza al medesimo. Il Direttore dell'esecuzione è la figura professionale che va a potenziare il RUP negli acquisti di particolare importanza. Fermo restando il rispetto delle disposizioni di servizio eventualmente impartite dal RUP, il Direttore dell'esecuzione opera in autonomia in ordine al coordinamento, alla direzione e al controllo tecnico-contabile nell'esclusivo interesse all'efficiente e sollecita esecuzione del contratto.

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

La collaborazione tra stazioni appaltanti

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

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

Contesto normativo e strategico

Riferimenti normativi italiani:

- [Legge 24 dicembre 2007, n. 244 "Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato" \(legge finanziaria 2008\) art. 1 co. 209 -214](#)
- [Decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla Legge 17 dicembre 2012, n. 221 "Ulteriori misure urgenti per la crescita del Paese", art. 19](#)
- [Legge 27 dicembre 2017, n. 205 "Bilancio di previsione dello Stato per l'anno finanziario 2018 e bilancio pluriennale per il triennio 2018-2020", art. 1 co. 411-415](#)
- [Decreto Legislativo 27 dicembre 2018, n. 148 - Attuazione della direttiva \(UE\) 2014/55 del Parlamento europeo e del Consiglio del 16 aprile 2014, relativa alla fatturazione elettronica negli appalti pubblici](#)
- [Decreto del Ministero dell'Economia e delle Finanze del 27 dicembre 2019 "Modifica del decreto 7 dicembre 2018 recante: Modalità e tempi per l'attuazione delle disposizioni in materia di emissione e trasmissione dei documenti attestanti l'ordinazione degli acquisti di beni e servizi effettuata in forma elettronica da applicarsi agli enti del Servizio sanitario nazionale"](#)
- [Decreto legislativo 31 marzo 2023, n. 36 "Codice dei contratti pubblici", artt. 19-26](#)
- [Circolare AGID n. 3 del 6 dicembre 2016 "Regole Tecniche aggiuntive per garantire il colloquio e la condivisione dei dati tra sistemi telematici di acquisto e di negoziazione"](#)
- [Regole tecniche AGID del 1° giugno 2023 «Requisiti tecnici e modalità di certificazione delle Piattaforme di approvvigionamento digitale»](#)
- Decisione di esecuzione Piano Nazionale di ripresa e resilienza
 - [Riforma 1.10 - M1C1-70 "Recovery procurement platform"](#) per la modernizzazione del sistema nazionale degli appalti pubblici e il sostegno delle politiche di sviluppo attraverso la digitalizzazione e il rafforzamento della capacità amministrativa delle amministrazioni aggiudicatrici

Riferimenti normativi europei:

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

Obiettivo 2.1 - Rafforzare l'ecosistema nazionale di approvvigionamento digitale

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

- **Target 2024** - 100% delle piattaforme di approvvigionamento dei soggetti aggregatori certificate
- **Target 2025** - 50% delle piattaforme certificate da terza parte
- **Target 2026** - 100% delle piattaforme certificate da terza parte

Obiettivo 2.2 - Diffondere l'utilizzo degli appalti innovativi

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

- **Target 2024** - 50% di PMI e *start up* innovative che partecipano ad appalti di innovazione sul totale degli operatori economici che partecipano alle gare
- **Target 2025** - 50% di PMI e *start up* innovative che partecipano ad appalti di innovazione sul totale degli operatori economici che partecipano alle gare
- **Target 2026** - 50% di PMI e *start up* innovative che partecipano ad appalti di innovazione sul totale degli operatori economici che partecipano alle gare

RA2.2.3 - Incremento della diffusione degli appalti di innovazione nelle PA

- **Target 2024** – Definizione della *baseline* consistente nel numero di amministrazioni che hanno pubblicato procedure di tipo pre-commerciale e partenariato per l'innovazione nel triennio 2022-2024
- **Target 2025** - Incremento del 10% sulla *baseline* individuata nel target 2024
- **Target 2026** - Incremento del 10% rispetto all'anno precedente

Linee di azione istituzionali

RA2.1.1

- **Dicembre 2024** - Gestione e monitoraggio del processo di certificazione delle piattaforme di approvvigionamento digitale - (AGID, ANAC) - CAP2.01
- **Settembre 2025** - Aggiornamento delle regole tecniche ampliando l'ambito di riferimento della interoperabilità - (AGID, ANAC, Dipartimento per la Trasformazione Digitale) - CAP2.02
- **Dicembre 2025** - Definizione della regolazione tecnica della fase di esecuzione, comprendendo la definizione del formato e della modalità di trasmissione su rete PEPPOL degli ordini e delle fatture elettroniche - (AGID) - CAP2.03

RA2.2.1

- **Marzo 2024** - Pubblicazione dei regolamenti per l'adesione, da parte delle PA, al programma *Smarter Italy* e agli altri programmi nazionali per la promozione e il finanziamento della domanda pubblica di innovazione - (Struttura di progetto *Smarter Italy*) - CAP2.04
- **Giugno 2024** - Pubblicazione di raccomandazioni per le consultazioni di mercato preliminari agli appalti di innovazione - (AGID) - CAP2.05
- **Giugno 2024** - Pubblicazione di linee guida alle PA per l'emersione dei fabbisogni di innovazione nella fase di programmazione degli acquisti - (AGID) - CAP2.06
- **Dicembre 2024** - Selezione e avvio dei progetti *Smarter Italy* sulle tematiche di "Salute e benessere" e "Protezione dell'ambiente" - (AGID) - CAP2.07

- **Dicembre 2026** - Completamento dei progetti *Smarter Italy* - (Ministero dell'Università e della Ricerca, Ministero delle Imprese e del *Made in Italy*, AGID) - CAP2.08

Linee di azione per le PA

RA2.1.1

- **Giugno 2025** - I soggetti aggregatori devono dotarsi di piattaforme di approvvigionamento che digitalizzano la fase di esecuzione dell'appalto - CAP2.PA.01
- **Dicembre 2026** - Le stazioni appaltanti devono digitalizzare la fase di esecuzione dell'appalto - CAP2.PA.02

RA2.2.1

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

Le gare strategiche per la trasformazione digitale

Scenario

Le gare strategiche ICT sono strumenti che consentono alle Amministrazioni di acquisire servizi necessari ad implementare le strategie per la trasformazione digitale della Pubblica Amministrazione.

In generale, quindi, sono disponibili servizi per operare sulla definizione di processi e sull'erogazione di servizi digitali, sulla analisi e realizzazione delle componenti applicative e infrastrutturali, con specifico riferimento al paradigma *cloud*.

In sinergia con le previsioni del Piano triennale e al fine di indirizzare e governare la trasformazione digitale della PA italiana, AGID opera una funzione di indirizzo strategico e *governance* centralizzata di tutte le iniziative, anche mediante la costituzione di organismi di coordinamento e controllo, finalizzati alla direzione strategica e tecnica delle stesse.

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

- fornisce ai soggetti aggregatori gli indirizzi strategici delle nuove iniziative da pubblicare;
- monitora il rispetto dei vincoli contrattuali e la qualità della fornitura;
- monitora lo stato di avanzamento degli Accordi Quadro;
- analizza i progetti implementati dalle Amministrazioni per monitorare la coerenza delle iniziative e l'andamento degli indicatori di digitalizzazione e gli obiettivi del Piano triennale perseguibili con l'iniziativa, oltre a favorire modalità di *co-working* o co-partecipazione finanziaria tra le amministrazioni;
- analizza le proposte di standardizzazione di processi, modelli, soluzioni, metriche, metodologie di stima dei servizi e, nella sua componente pubblica, ne valuta l'adozione;
- valuta le eventuali proposte di evoluzione e/o adeguamento dei servizi da parte del fornitore. È inoltre in corso l'implementazione di ulteriori azioni concrete volte ad accompagnare le pubbliche amministrazioni per una acquisizione sempre più consapevole degli strumenti disponibili all'interno del paniere delle gare strategiche, al fine di garantire contratti di elevata standardizzazione e qualità.

Le gare strategiche ICT si pongono pertanto il duplice obiettivo di:

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

Le iniziative strategiche ICT sono realizzate attraverso appalti aggiudicati da Consip nella forma dell'accordo quadro, che consentono a tutte le Amministrazioni di acquistare rapidamente i servizi necessari per attuare il percorso di transizione al digitale secondo il paradigma dell'ordine diretto, ove l'Amministrazione non abbia esigenze progettuali peculiari ovvero attraverso lo strumento dell'appalto specifico tra i fornitori selezionati da Consip, con garanzie di qualità e prezzi vantaggiosi.

In particolare, le Amministrazioni possono accedere, ad oggi, a un piano molto ricco di gare strategiche che nell'ultimo anno è stato ampliato con le seconde edizioni di alcune iniziative sulla base dell'andamento di adesione registrato per le prime edizioni. In particolare, a novembre 2023 risultavano attive 14 gare per 60 lotti, con un massimale di circa 10 miliardi. Sono in corso di attivazione 4 ulteriori gare, per 29 lotti, per un massimale di circa 13 miliardi.

Contesto normativo

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

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

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

- **Target 2024** - Mappa indicatori del Piano triennale e gare strategiche attive come alle lettere d) e g) dell'art. 14-bis comma 2 del Codice per l'Amministrazione Digitale
- **Target 2025** - Programma di iniziative strategiche necessarie al raggiungimento degli obiettivi del presente piano, di cui alle lettere d) e g) dell'art. 14-bis comma 2 del Codice per l'Amministrazione Digitale
- **Target 2026** - Disponibilità nuove gare strategiche necessarie al raggiungimento degli obiettivi del Piano triennale di cui alle lettere d) e g) dell'art. 14-bis comma 2 del Codice per l'Amministrazione Digitale

Linee di azione istituzionali

RA2.3.1

- **Maggio 2024** - Pubblicazione della mappatura dei risultati attesi della presente edizione del Piano Triennale per l'informatica nella PA con le gare strategiche attive - (AGID) - CAP2.09
- **Marzo 2025** - Individuazione nuove gare strategiche a seguito del confronto tra AGID, Consip e i soggetti aggregatori di cui all'articolo 9 del decreto-legge 24 aprile 2014, n. 66 - (AGID, Consip e soggetti aggregatori di cui all'articolo 9 del decreto-legge

24 aprile 2014, n. 66) - CAP2.10

- **Settembre 2025** - Definizione delle strategie delle nuove iniziative individuate - (AGID, Consip e soggetti aggregatori di cui all'articolo 9 del decreto-legge 24 aprile 2014, n. 66) - CAP2.11
- **Luglio 2026** - Disponibilità per le amministrazioni delle nuove iniziative strategiche - (Consip e soggetti aggregatori di cui all'articolo 9 del decreto-legge 24 aprile 2014, n. 66) - CAP2.12

Linee di azione per le PA

RA2.3.1

- **Settembre 2024** - Le PA, nel proprio piano acquisti, programmano i fabbisogni di adesione alle iniziative strategiche disponibili per il perseguimento degli obiettivi del Piano triennale per l'anno 2025 - CAP2.PA.04
- **Settembre 2025** - Le PA programmano i fabbisogni di adesione alle iniziative strategiche per il perseguimento degli obiettivi del Piano triennale per l'anno 2026 - CAP2.PA.05
- **Settembre 2026** - Le PA programmano i fabbisogni di adesione alle iniziative strategiche per il perseguimento degli obiettivi del Piano triennale per l'anno 2027 - CAP2.PA.06

Strumenti per l'attuazione del Piano

- Mappatura Gare strategiche (vedi Parte Terza – Strumenti – Strumento 1 – Approvvigionamento ICT)

Risorse e fonti di finanziamento

- [Portale informativo Consip Gare Strategiche](#)

Il procurement e l'INFN

L'INFN a partire dal 1° gennaio 2024 ha adottato una gestione digitalizzata del ciclo di vita degli appalti come previsto dal decreto lgs. N. 36 del 31 marzo 2023 attraverso l'uso generalizzato di piattaforme certificate. L'Ente aveva già digitalizzato le procedure interne per gli acquisti fino alla soglia per la quale le regole interne non prevedono procedure centralizzate. Entro il 2024 verrà terminata la messa in funzione della procedura interna di gestione della fase post-ordine. Questo strumento gestisce tutte le fasi successive a un ordine, dalla ricezione della merce alla verifica degli articoli, fino all'archiviazione del mandato di pagamento. Parte fondamentale in questi processi, sviluppati dai servizi informativi interni, è l'integrazione con l'anagrafica per i ruoli autorizzativi e con la contabilità per la gestione della disponibilità finanziaria e degli impegni di spesa. Inoltre, la trasmissione automatica dei dati delle procedure interne al sistema di Business Intelligence rende possibile l'analisi dei dati per supportare i processi decisionali.

Riteniamo necessario avviare un processo di integrazione tra le procedure interne di acquisto e le procedure certificate in uso. Tale processo è stato avviato all'inizio del 2024 e parte

dall'integrazione del sistema di autenticazione; sarebbe auspicabile ed è in fase di studio un ulteriore passo per l'interscambio di documenti e di informazioni con i prodotti utilizzati che integrano gli accessi alla BDNCP, allo scopo di evitare la duplicazione di operazioni manuali e la copia di documenti da e verso di essi, che costituisce, oltre che un inutile aggravio di lavoro per l'amministrazione, una possibile sorgente di errore nell'inserimento dei dati.

L'INFN è, al momento della elaborazione di questo piano, stazione appaltante qualificata senza limiti di importo. A livello di amministrazione centrale, è iniziato un processo di coinvolgimento dell'RTD nei processi di acquisto centralizzato, in particolare per quanto riguarda il software gestionale. Questo permette di mantenere il controllo, ad esempio, sulle qualifiche dei fornitori.

D'altro canto, la Commissione Calcolo e Reti (CCR) svolge il compito di centralizzare gli acquisti delle licenze software diffuse nell'Ente, allo stesso tempo costituisce canale di finanziamento per l'infrastruttura informatica dei servizi. Grazie al coinvolgimento delle persone rilevanti nel gruppo di coordinamento dell'RTD, questo ne permette il coinvolgimento negli acquisti ICT per la transizione digitale.

PARTE SECONDA – Componenti tecnologiche

Capitolo 3 - Servizi

Negli ultimi anni, la digitalizzazione è diventata una forza trainante per l'innovazione nei servizi pubblici, con gli enti locali al centro di questo cambiamento.

L'adozione di tecnologie digitali è essenziale per migliorare l'efficienza, aumentare la trasparenza e garantire la qualità dei servizi offerti ai cittadini. In questo processo di trasformazione è indispensabile anche definire un *framework* di riferimento per guidare ed uniformare le scelte tecnologiche. In particolare, l'architettura a microservizi può esser considerata come una soluzione agile e scalabile, che permette di standardizzare i processi digitali e di facilitare anche il processo di *change management* nelle organizzazioni governative locali.

Per garantire la possibilità a tutti gli Enti di poter cogliere questa enorme opportunità, anche a coloro che si trovano in condizioni di carenze di *know-how* e risorse, il presente Piano propone e promuove un'evoluzione del modello di interoperabilità passando dalla sola condivisione dei dati a quella della condivisione dei servizi.

I vantaggi dell'utilizzo di un'architettura basata su micro-servizi sono:

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

La transizione verso un'architettura a microservizi richiede la consapevolezza che non sia necessario solo un intervento tecnologico ma che richiede soprattutto un controllo per la gestione del cambiamento che, come abbiamo visto nel cap. 1 coinvolge diverse fasi chiave, quali la formazione continua, il coinvolgimento attivo degli *stakeholder*, il monitoraggio dell'impatto del cambiamento e naturalmente anche una comunicazione efficace.

Per gli enti locali che potrebbero non avere un *know-how* interno sufficiente, l'architettura a microservizi offre l'opportunità di sfruttare le soluzioni e i servizi già sviluppati da altri enti. Questo approccio non solo consente di colmare il *gap* informativo interno, ma fornisce anche un vantaggio significativo in termini di risparmio di tempo e ottimizzazione delle risorse.

L'architettura a microservizi, attraverso la condivisione di processi e lo sviluppo *once only* riduce la duplicazione degli sforzi e dei costi. La condivisione di *e-service* vede nella Piattaforma Digitale Nazionale Dati Interoperabilità (PDND) il *layer* focale per la condivisione di dati e processi.

La sostenibilità e la crescita collaborativa nell'ambito dell'architettura a microservizi non si limita al singolo ente locale. In molte situazioni, possono entrare in gioco altre istituzioni a supporto, come Regioni, Unioni o Enti capofila (*HUB* tecnologici), che possono agire svolgendo un ruolo fondamentale nello sviluppo fornendo soluzioni tecnologiche e/o amministrative, per facilitare l'integrazione e l'implementazione del processo di innovazione. Questo approccio consente agli enti più piccoli di beneficiare delle risorse condivise e delle soluzioni già implementate, accelerando così il processo di digitalizzazione.

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

collaborazione istituzionale diventa così un elemento fondamentale per plasmare un futuro digitale condiviso e orientato all'innovazione.

E-Service in interoperabilità tramite PDND

Scenario

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

A fine di raggiungere la completa interoperabilità dei *dataset* e dei servizi chiave tra le PA centrali e locali e di valorizzare il capitale informativo delle pubbliche amministrazioni, nell'ambito del Sub-Investimento M1C1_1.3.1 "Piattaforma nazionale digitale dei dati" del Piano Nazionale di Ripresa e Resilienza, è stata realizzata la Piattaforma Digitale Nazionale Dati (PDND).

La PDND è lo strumento per gestire l'autenticazione, l'autorizzazione e la raccolta e conservazione delle informazioni relative agli accessi e alle transazioni effettuate suo tramite. La Piattaforma fornisce un insieme di regole condivise per semplificare gli accordi di interoperabilità snellendo i processi di istruttoria, riducendo oneri e procedure amministrative. Un ente può aderire alla Infrastruttura interoperabilità PDND siglando un accordo di adesione, attraverso le funzionalità messe a disposizione dell'infrastruttura.

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

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

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

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

- costituzione di tavoli e gruppi di lavoro;
- avvio di progettualità congiunte;
- capitalizzazione di soluzioni realizzate dalla PA in open source o su siti o forum per condividere la conoscenza ([Developers Italia](#) e [Forum Italia](#))

Maggiori dettagli sulla [Piattaforma Digitale Nazionale Dati](#) sono disponibili sul portale di progetto.

Contesto normativo

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

Riferimenti normativi italiani:

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

Riferimenti normativi europei:

- [Regolamento \(UE\) 2014/910 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno \(in breve eIDAS\)](#)

- [Regolamento \(UE\) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali \(in breve GDPR\)](#)
- [European Interoperability Framework -Implementation Strategy \(2017\)](#)
- [Interoperability solutions for public administrations, businesses and citizens \(2017\)](#)

Obiettivo 3.1 - Migliorare la capacità di erogare e-service

RA3.1.1 - Incremento del numero di “e-service” registrati sul Catalogo Pubblico PDND

- **Target 2024** - 400 API totali registrate sul Catalogo API della Piattaforma Digitale Nazionale Dati (Target PNRR, M1C1-18, Q4 2024)
- **Target 2025** - 850 API totali registrate sul Catalogo API della Piattaforma Digitale Nazionale Dati (Target ITA, M1C1-27-ITA-1 – T/IT, Q4 2025)
- **Target 2026** - 2000 API totali registrate sul Catalogo API della Piattaforma Digitale Nazionale Dati (Target PNRR, M1C1-27, Q2 2026)

RA3.1.2 - Aumento del numero di Richieste di Fruizione Autorizzate su PDND

- **Target 2024** - 2.000 Richieste di Fruizione Autorizzate su PDND
- **Target 2025** - 3.500 Richieste di Fruizione Autorizzate su PDND
- **Target 2026** - 7.000 A Richieste di Fruizione Autorizzate su PDND

RA3.1.3 - Ampliamento del numero delle amministrazioni coinvolte nell'evoluzione delle Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni

- **Target 2024** - Costruzione *baseline* con identificazione del numero delle PA che evidenziano nuove esigenze applicative e partecipano alla definizione di *pattern* e/o profili di interoperabilità
- **Target 2025** - Incremento del 10% rispetto alla *baseline*
- **Target 2026** - Incremento del 25% rispetto alla *baseline*

Linee di azione istituzionali

RA3.1.1

- **Marzo 2024** - Aggiornamento delle Linee Guida di Interoperabilità per includere il nuovo pattern di sicurezza relativo agli scambi massivi - (AGID) - CAP3.01
- **Luglio 2024** - Aggiornamento delle Linee guida PDND per includere funzionalità di gestione di variazione del dato, scambi asincroni, erogazione inversa e intermediari - (AGID, Dipartimento per la Trasformazione Digitale) - CAP3.02
- **Settembre 2024** - Attivazione della PDND per la gestione dei processi di notifica di variazione del dato - (PagoPA S.p.A, Dipartimento per la Trasformazione Digitale) - CAP3.03
- **Marzo 2025** - Razionalizzazione degli *use case* significativi e identificazione degli *e-service* Pattern ricorrenti, con l'obiettivo di supportare gli enti nell'individuazione degli *e-service* e dei dati più rilevanti da esporre - (Dipartimento per la Trasformazione Digitale) - CAP3.04
- **Marzo 2025** - Attivazione della PDND per la gestione delle funzionalità di intermediazione - (PagoPA S.p.A, Dipartimento per la Trasformazione Digitale) - CAP3.05

RA3.1.2

- **Luglio 2024** - Aggiornamento delle Linee guida PDND per includere funzionalità di gestione di variazione del dato, scambi asincroni, erogazione inversa e intermediari - (AGID, Dipartimento per la Trasformazione Digitale) - CAP3.06

- **Dicembre 2024** - Attivazione della PDND per la gestione dei processi di erogazione dei servizi da parte dei privati - (PagoPA S.p.A, Dipartimento per la Trasformazione Digitale) - CAP3.07

RA3.1.3

- **Maggio 2024** - Revisione delle “Linee guida sull’interoperabilità tecnica delle Pubbliche Amministrazioni” aggiungendo nuovi *pattern* e/o profili ai relativi documenti operativi sulla base delle esigenze espresse dalle PA entro gennaio 2024 - (AGID) - CAP3.08
- **Novembre 2024** - Aggiornamento delle “Linee guida sull’interoperabilità tecnica delle Pubbliche Amministrazioni” aggiungendo nuovi *pattern* e/o profili ai relativi documenti operativi sulla base delle esigenze espresse dalle PA - (AGID) - CAP3.09
- **Maggio 2025** - Aggiornamento delle “Linee guida sull’interoperabilità tecnica delle Pubbliche Amministrazioni” aggiungendo nuovi *pattern* e/o profili ai relativi documenti operativi sulla base delle esigenze espresse dalle PA - (AGID) - CAP3.10
- **Novembre 2025** - Revisione delle “Linee guida sull’interoperabilità tecnica delle Pubbliche Amministrazioni” aggiungendo nuovi *pattern* e/o profili ai relativi documenti operativi sulla base delle esigenze espresse dalle PA - (AGID) - CAP3.11

Linee di azione per le PA

RA3.1.1

- **Da gennaio 2024** - Le PA cessano di utilizzare modalità di interoperabilità diverse da PDND - CAP3.PA.01
- **Da gennaio 2024** - Le Amministrazioni iniziano la migrazione dei servizi erogati in interoperabilità dalle attuali modalità alla PDND - CAP3.PA.02
- **Da gennaio 2024** - Le PA continuano a popolare il Catalogo delle API della Piattaforma Digitale Nazionale Dati con le API conformi alle “Linee guida sull’interoperabilità tecnica delle pubbliche amministrazioni” - CAP3.PA.03
- **Da gennaio 2024** - Le PA locali rispondono ai bandi pubblicati per l’erogazione di API su PDND - CAP3.PA.04
- **Da gennaio 2024** - Le PA centrali siglano accordi per l’erogazione di API su PDND - CAP3.PA.05

RA3.1.2

- **Da gennaio 2024** - Le PA utilizzano le API presenti sul Catalogo - CAP3.PA.06
- **Da gennaio 2025** - Le PA effettuano richieste di fruizione di servizi erogati da privati - CAP3.PA.07

RA3.1.3

- **Da gennaio 2024** - Le PA evidenziano le esigenze che non trovano riscontro nella “Linee guida sull’interoperabilità tecnica delle pubbliche amministrazioni” e partecipano alla definizione di *pattern* e profili di interoperabilità per l’aggiornamento delle stesse - CAP3.PA.08

Progettazione dei servizi: accessibilità e design

Scenario

Il miglioramento della qualità e dell'inclusività dei servizi pubblici digitali costituisce la premessa indispensabile per l'incremento del loro utilizzo da parte degli utenti, siano questi cittadini, imprese o altre pubbliche amministrazioni.

Nell'attuale processo di trasformazione digitale è essenziale che i servizi abbiano un chiaro valore per l'utente. Questo obiettivo richiede un approccio multidisciplinare nell'adozione di metodologie e tecniche interoperabili per la progettazione di un servizio. La qualità finale, così come il costo complessivo del servizio, non può infatti prescindere da un'attenta analisi dei molteplici *layer*, tecnologici e organizzativi interni, che strutturano l'intero processo della prestazione erogata, celandone la complessità sottostante.

Ciò implica anche la necessità di un'adeguata semplificazione dei procedimenti e un approccio sistematico alla gestione dei processi interni, sotto il coordinamento del Responsabile per la transizione al digitale, dotato di un ufficio opportunamente strutturato e con il fondamentale coinvolgimento delle altre strutture responsabili dell'organizzazione e del controllo strategico.

È cruciale, inoltre, il rispetto degli obblighi del CAD in materia di progettazione, accessibilità, *privacy*, gestione dei dati e riuso, al fine di massimizzare l'efficienza dell'investimento di denaro pubblico e garantire la sovranità digitale con soluzioni software strategiche sotto il completo controllo della Pubblica Amministrazione.

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

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

Per incoraggiare tutti gli utenti a privilegiare il canale online rispetto a quello esclusivamente fisico, rimane necessaria una decisa accelerazione nella semplificazione dell'esperienza d'uso complessiva e un miglioramento dell'inclusività dei servizi, nel pieno rispetto delle norme riguardanti l'accessibilità e il Regolamento generale sulla protezione dei dati.

Per il monitoraggio dei propri servizi, le PA possono utilizzare [Web Analytics Italia](#), una piattaforma nazionale open source che offre rilevazioni statistiche su indicatori utili al miglioramento continuo dell'esperienza utente.

Per la realizzazione dei propri servizi digitali, le PA possono utilizzare il [Design System del Paese](#), che consente la realizzazione di interfacce coerenti e accessibili *by default*, concentrando i budget di progettazione e sviluppo sulle parti e i processi caratterizzanti dello specifico servizio digitale.

Contesto normativo e strategico

Riferimenti normativi italiani:

- [Legge 9 gennaio 2004, n. 4 \(Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici\)](#)
- [Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" \(in breve CAD\), art. 7, 17, 23, 53, 54, 68, 69 e 71](#)
- [Decreto Ministeriale 30 aprile 2008 \(Regole tecniche disciplinanti l'accessibilità agli strumenti didattici e formativi a favore degli alunni disabili\).](#)
- [Legge 3 marzo 2009, n. 18 - Ratifica ed esecuzione della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità](#)
- [Decreto Legislativo 10 agosto 2018, n. 106 \(Attuazione della direttiva \(UE\) 2016/2102 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici\)](#)
- [Decreto-Legge 16 luglio 2020, n. 76 \(Misure urgenti per la semplificazione e l'innovazione digitale\)](#)
- [Decreto Legislativo 27 maggio 2022, n. 82 - "Attuazione della direttiva \(UE\) 2019/882 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sui requisiti di accessibilità dei prodotti e dei servizi."](#)
- [Linee Guida AGID su acquisizione e riuso del software per la Pubblica Amministrazione \(2019\)](#)
- [Linee Guida AGID sull'accessibilità degli strumenti informatici \(2020\)](#)
- [Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici \(2021\)](#)
- [Linee Guida AGID di design per i siti internet e i servizi digitali della PA \(2022\)](#)
- [Determinazione AGID n.354/2022 del 22 dicembre 2022 - Linee Guida sull'accessibilità degli strumenti informatici adottate con Determinazione n. 437/2019 del 20 dicembre 2019 e rettificata con Determinazione n. 396/2020 del 10 settembre 2020 - Rettifica per adeguamento a norma tecnica europea armonizzata sopravvenuta.](#)
- Piano Nazionale di Ripresa e Resilienza:
 - Investimento 1.3: "[Dati e interoperabilità](#)"
 - Investimento 1.4: "[Servizi digitali e cittadinanza digitale](#)"

Riferimenti normativi europei:

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

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

RA3.2.1 - Diffusione del modello di riuso di software tra le amministrazioni in attuazione delle Linee

Guida AGID sull'acquisizione e il riuso del software per la Pubblica Amministrazione

- **Target 2024** - Almeno 100 amministrazioni che rilasciano *software open source* in Developers Italia e almeno 2.600 soggetti che riusano *software open source* presente in Developers Italia
- **Target 2025** - Almeno 125 amministrazioni che rilasciano *software open source* in Developers Italia e almeno 2.800 soggetti che riusano *software open source* presente in Developers Italia
- **Target 2026** - Almeno 150 amministrazioni che rilasciano *software open source* in Developers Italia e almeno 3.000 soggetti che riusano *software open source* presente in Developers Italia

RA3.2.2 - Incremento dell'accessibilità dei servizi digitali

- **Target 2024** - Il 100 % delle PA pubblica e aggiorna la dichiarazione di accessibilità dei propri siti istituzionali registrati su IndicePA
- **Target 2025** - Il 100 % delle PA aggiorna la dichiarazione di accessibilità dei propri siti istituzionali registrati su IndicePA
- **Target 2026** - Il 100 % delle PA aggiorna la dichiarazione di accessibilità dei propri siti istituzionali registrati su IndicePA

RA3.2.3 - Incremento e diffusione dei modelli standard di siti e servizi digitali, disponibili in Designers Italia

- **Target 2024** - 6.520 PA adottano i modelli standard di siti e servizi digitali disponibili
- **Target 2025** - 9.750 PA adottano i modelli standard di siti e servizi digitali disponibili
- **Target 2026** - 13.000 PA adottano i modelli standard di siti e servizi digitali disponibili

Linee di azione istituzionali

RA3.2.1

- **Dicembre 2024** - Il DTD condivide a livello europeo soluzioni già sviluppate nel catalogo di Developers Italia (*standard publiccode. yaml*, *software crawler*, struttura del catalogo), attraverso iniziative come il progetto FOSSEPS (*Free Open Source Software for European Public Services*) - (Dipartimento per la Trasformazione Digitale) - CAP3.12
- **Dicembre 2024** - Il DTD coordina la definizione di un inventario di *software* "critico", ovvero con valenza strategica per la sovranità digitale del Paese, e identificazione di soluzioni valide esistenti da preservare o lacune da colmare - (Dipartimento per la Trasformazione Digitale) - CAP3.13
- **Dicembre 2024** - Il DTD avvia i lavori di aggiornamento di Docs Italia per consentire agli enti un'agevole pubblicazione dei propri documenti - (Dipartimento per la Trasformazione Digitale) - CAP3.14
- **Dicembre 2025** - Il DTD conclude i lavori di aggiornamento di Docs Italia per consentire agli enti un'agevole pubblicazione dei propri documenti - (Dipartimento per la Trasformazione Digitale) - CAP3.15

RA3.2.2

- **Giugno 2024** - Avvio dell'erogazione del supporto finanziario e specialistico alle 55 PAL che hanno sottoscritto l'accordo PNRR con AGID - (AGID) - CAP3.16
- **Giugno 2024** - Monitoraggio automatico dell'accessibilità di 23.000 siti web della PA - (AGID) - CAP3.17
- **Dicembre 2024** - Aggiornamento dell'elenco degli errori di accessibilità più frequenti, individuati mediante monitoraggio esteso con MAUVE - (AGID) - CAP3.18

- **Dicembre 2024** - Erogazione di 50 iniziative di comunicazione, formazione e sensibilizzazione alla cultura dell'accessibilità su scala nazionale a soggetti target del settore pubblico e privato - (AGID) - CAP3.19
- **Dicembre 2024** - Invio alla Commissione Europa della relazione di monitoraggio nazionale dell'accessibilità, ai sensi della Direttiva (UE) 2016/2102 - (AGID) - CAP3.20
- **Giugno 2025** - Sviluppo di un sistema *open source* per la verifica automatica di accessibilità dei siti - (AGID) - CAP3.21

RA3.2.3

- **Marzo 2024** - Messa a disposizione di un modello standard di sito per le Aziende Sanitarie Locali - (Dipartimento per la Trasformazione Digitale) - CAP3.22
- **Giugno 2024** - Messa a disposizione delle PA di un modello standard di sito per i Musei Civici - (Dipartimento per la Trasformazione Digitale) - CAP3.23
- **Marzo 2024** - Messa a disposizione delle PA della versione Beta della documentazione del *design system* del Paese - (Dipartimento per la Trasformazione Digitale) - CAP3.24
- **Dicembre 2024** - Messa a disposizione delle PA della versione di esercizio della documentazione del *Design system* del Paese - (Dipartimento per la Trasformazione Digitale) - CAP3.25
- **Dicembre 2025** - Erogazione e/o partecipazione ad iniziative di formazione tecnica e sensibilizzazione alla cultura della progettazione su scala nazionale a soggetti target del settore pubblico, finalizzate al raggiungimento degli obiettivi della Decade Digitale - (Dipartimento per la Trasformazione Digitale) - CAP3.26
- **Gennaio 2025** - Avvio raccolta *feedback* derivanti dalle implementazioni del modello standard di sito per le Aziende Sanitarie Locali, da parte delle ASL che lo hanno implementato, in ottica di miglioramento evolutivo - (Dipartimento per la Trasformazione Digitale) - CAP3.27
- **Marzo 2025** - Avvio raccolta *feedback* derivanti dalle implementazioni del modello standard di sito i musei civici, da parte dei musei civici che lo hanno implementato, in ottica di miglioramento evolutivo - (Dipartimento per la Trasformazione Digitale) - CAP3.28

Linee di azione per le PA

RA3.2.2

- **Marzo 2024** - Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web - CAP3.PA.09
- **Settembre 2024** - Le Regioni, le Province Autonome, le città metropolitane e i capoluoghi delle Città metropolitane effettuano un test automatico di accessibilità sul proprio sito istituzionale indicato su <https://indicepa.gov.it/ipa-portale/>, utilizzando la piattaforma Mauve++ - CAP3.PA.10
- **Settembre 2024** - Le PA pubblicano, entro il 23 settembre, esclusivamente tramite l'applicazione form.AGID.gov.it, la dichiarazione di accessibilità per ciascuno dei propri siti web e APP mobili - CAP3.PA.11
- **Dicembre 2024** - Tutte le Regioni, le Province autonome, le Città metropolitane, i Comuni capoluogo delle Città metropolitane attivano *Web Analytics Italia* per la rilevazione delle statistiche di utilizzo del proprio sito web istituzionale presente su IndicePA - CAP3.PA.12
- **Marzo 2025** - Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web - CAP3.PA.13
- **Settembre 2025** - Le PA pubblicano, entro il 23 settembre, esclusivamente tramite l'applicazione form.AGID.gov.it, la dichiarazione di accessibilità per ciascuno dei propri siti web e APP mobili - CAP3.PA.14
- **Marzo 2026** - Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web - CAP3.PA.15

- **Settembre 2026** - Le PA pubblicano, entro il 23 settembre, esclusivamente tramite l'applicazione form.AGID.gov.it, la dichiarazione di accessibilità per ciascuno dei propri siti web e APP mobili - CAP3.PA.16

Formazione, gestione e conservazione dei documenti informatici

Scenario

Le nuove Linee guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agenzia per l'Italia Digitale, adottate ai sensi dell'art. 71 del CAD e in vigore dal 1° gennaio 2022, rappresentano un importante contributo nel rafforzamento e nell'armonizzazione del quadro normativo di riferimento in tema di produzione, gestione e conservazione dei documenti informatici, mirando a semplificare e rendere più accessibile la materia, integrandola ove necessario, per ricondurla in un unico documento sistematico di pratico utilizzo.

Al loro interno sono delineati i necessari adeguamenti organizzativi e funzionali richiesti alle pubbliche amministrazioni, chiamate a consolidare e rendere concreti i principi di trasformazione digitale enunciati nel CAD e nel Testo Unico sulla Documentazione Amministrativa - TUDA.

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

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

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

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

Nell'ambito delle sue funzioni di vigilanza, verifica, controllo e monitoraggio, e conformemente a

quanto stabilito dall'articolo 18-bis del Codice dell'Amministrazione Digitale - CAD, l'Agenzia per l'Italia Digitale ha pianificato di avviare un'attività di monitoraggio riguardante l'adempimento degli obblighi specificati dalle Linee guida.

A questo scopo, entro il 2024 verrà sviluppato un modello basato su indicatori chiari e dettagliati, supportato da un accurato percorso metodologico. Questo permetterà di procedere con un monitoraggio efficace e sistematico, da realizzarsi entro il 2025 per le disposizioni sulla Gestione documentale, e entro il 2026 per quelle relative alla Conservazione digitale.

Contesto normativo

Riferimenti normativi italiani:

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

Riferimenti normativi europei:

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

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

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”

Linee di azione istituzionali

RA3.3.1

- **Giugno 2024** - Pubblicazione di un modello per il monitoraggio - (AGID) - CAP3.29
- **Dicembre 2025** - Completamento attività di monitoraggio relativo al target 2025 - (AGID) - CAP3.30
- **Dicembre 2026** - Completamento attività di monitoraggio relativo al target 2026 - (AGID) - CAP3.31

Linee di azione per le PA

RA3.3.1

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

- **Giugno 2025** - Le PA devono verificare che in “Amministrazione trasparente” sia pubblicato il manuale di gestione documentale, la nomina del responsabile della gestione documentale per ciascuna AOO e qualora siano presenti più AOO la nomina del coordinatore della gestione documentale - CAP3.PA.17
- **Giugno 2026** - Le PA devono verificare che in “Amministrazione trasparente” sia pubblicato il manuale di conservazione e la nomina del responsabile della conservazione - CAP3.PA.18

Single Digital Gateway

Scenario

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

Il Regolamento, entrato in vigore il 2 ottobre 2018, infatti, ha stabilito le norme per:

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

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

procedimenti amministrativi alle specifiche tecniche di implementazione del *Single Digital Gateway*.

Dopo aver reso disponibile *online* i servizi relativi delle procedure previste, le attività per il *Single Digital Gateway* del triennio 2024-2026 riguarderanno prevalentemente azioni di mantenimento, monitoraggio e miglioramento della qualità e dell'accesso ai servizi digitali offerti dallo Sportello per l'Italia, in particolare:

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

Contesto normativo e strategico

Riferimenti normativi italiani:

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

Riferimenti normativi europei:

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

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

RA3.4.1 - Piena operatività dell'*Operation Center*

- **Target 2024** - Metodologia di monitoraggio definita e condivisa con le PA interessate
- **Target 2025** - 100% delle richieste di supporto di cittadini e imprese prese in carico dall'*help desk* dell'*Operation Center*
- **Target 2026** - n.a.

RA3.4.2 - Diffusione e pieno utilizzo dello Sportello

- **Target 2024** - 5 PA italiane aderenti agli Accordi sono coinvolte nella diffusione dello sportello e forniscono i dati relativi agli utenti che hanno utilizzato le procedure SDG
- **Target 2025** - 10 PA italiane aderenti agli Accordi sono coinvolte nella diffusione dello sportello

e forniscono i dati relativi agli utenti che hanno utilizzato le procedure SDG

- **Target 2026** - 15 PA italiane aderenti agli Accordi sono coinvolte nella diffusione dello sportello e forniscono i dati relativi agli utenti che hanno utilizzato le procedure SDG

Linee di azione istituzionali

RA3.4.1

- **Giugno 2024** - Definizione della metodologia di monitoraggio e progettazione della piattaforma di monitoraggio (*Operation Center*) e del relativo modello di gestione - (AGID) - CAP3.32
- **Dicembre 2024** - Completamento realizzazione piattaforma di monitoraggio (*Operation Center*) - (AGID) - CAP3.33

RA3.4.2

- **Giugno 2024** - Definizione e redazione di un documento di indicazioni per la diffusione dello sportello - (AGID) - CAP3.34
- **Dicembre 2024** - I ciclo di azioni di sensibilizzazione sulle attività di diffusione e utilizzo presso le PA italiane aderenti agli Accordi - (AGID) - CAP3.35
- **Dicembre 2025** - II ciclo di azioni di sensibilizzazione sulle attività di diffusione e utilizzo presso le PA italiane aderenti agli Accordi - (AGID) - CAP3.36
- **Dicembre 2026** - III ciclo di azioni di sensibilizzazione sulle attività di diffusione e utilizzo presso le PA italiane aderenti agli Accordi - (AGID) - CAP3.37

Linee di azione per le PA

RA3.4.1

- **Da gennaio 2025** - Le PA italiane aderenti agli Accordi e interessate usano gli strumenti dell'*Operation Center* e svolgono azioni correttive sul funzionamento dei servizi e delle procedure sulla base delle segnalazioni ricevute - CAP3.PA.19

RA3.4.2

- **Dicembre 2024** - Le PA italiane aderenti agli Accordi in base alle proprie esigenze partecipano alle azioni di sensibilizzazione effettuate da AGID - CAP3.PA.20
- **Dicembre 2025** - Le PA italiane aderenti agli Accordi in base alle proprie esigenze partecipano alle azioni di sensibilizzazione effettuate da AGID - CAP3.PA.21
- **Dicembre 2026** - Le PA italiane aderenti agli Accordi in base alle proprie esigenze partecipano alle azioni di sensibilizzazione effettuate da AGID - CAP3.PA.22

Strumenti per l'attuazione del Piano

OB3.1

Di seguito si presentano i principali strumenti operativi a disposizione delle amministrazioni per l'attuazione delle attività in carico alle pubbliche amministrazioni

- *Landing page* PDND: <https://www.interop.pagopa.it>
- Tutte le richieste di informazioni relative all'accordo di adesione e più in generale alla piattaforma possono essere sottoposte inviando una mail a: selfcare@assistenza.pagopa.it, o tramite il tasto "Assistenza" presente nella pagina di login (<https://selfcare.pagopa.it>).

OB3.2

- [Designers Italia](#)

Le Linee guida di *design* per i siti internet e i servizi digitali della Pubblica Amministrazione chiedono di realizzare interfacce coerenti nell'esperienza d'uso, privilegiando le indicazioni e gli strumenti previsti su Designers Italia.

Il DTD e AGID mettono a disposizione su questo canale i modelli di sito e servizi digitali, un *design system* completo di documentazione e librerie di progettazione e di sviluppo, e risorse per affrontare le diverse fasi di progetto di un servizio pubblico digitale.

- [Developers Italia](#)

È il punto di riferimento per il *software* della Pubblica Amministrazione. Nella sezione piattaforme offre una serie di informazioni, strumenti e risorse tecniche e normative per l'utilizzo delle piattaforme abilitanti a disposizione delle pubbliche amministrazioni. Il Catalogo del software a riuso e *open source*, gestito da DTD ed AGID, permette alle Pubbliche Amministrazioni di svolgere le valutazioni comparative, propedeutiche all'acquisizione di *software* e servizi connessi. La sezione Interoperabilità fornisce informazioni sullo sviluppo di interfacce per la programmazione delle applicazioni (API) e su tutti gli strumenti connessi, come la Piattaforma Digitale Nazionale Dati (PDND) e il Catalogo Nazionale Dati per l'interoperabilità semantica (schema.gov.it)

- [Forum Italia](#)

Forum Italia è uno spazio di confronto, per domande, risposte sugli argomenti della trasformazione digitale.

- [Docs Italia](#)

Docs Italia è il luogo per la divulgazione e la consultazione di documenti pubblici digitali in modo nativamente digitale, responsive e accessibile.

- [Web Analytics Italia \(WAI\)](#)

Le Linee guida di *design* per i siti internet e i servizi digitali della Pubblica Amministrazione richiedono di effettuare la raccolta e l'analisi statistica del traffico e del comportamento utente rispetto all'accesso e utilizzo di siti e servizi digitali.

È necessario inoltre pubblicare le informazioni, opportunamente aggregate e anonimizzate, derivanti dal monitoraggio statistico attivato sul singolo sito e/o servizio

AGID mette a disposizione delle PA la piattaforma di analisi statistica *Web Analytics Italia* che permette di monitorare le statistiche in tempo reale dei visitatori dei siti della Pubblica Amministrazione e di beneficiare di strumenti ad hoc per pubblicare le statistiche dei siti monitorati (art. 7 CAD).

- [Form AGID](#)

Applicazione messa a disposizione da AGID attraverso cui le pubbliche amministrazioni possono inviare informazioni e dichiarazioni strutturate e ufficiali relativamente ai propri servizi ICT.

L'applicazione, ad esempio, è usata dalle amministrazioni nell'attività di definizione e pubblicazione degli obiettivi annuali di accessibilità.

- [MAUVE ++](#)

Nell'ambito della misura "PNRR 1.4.2 - *Citizen inclusion*" AGID e CNR hanno realizzato una piattaforma, gratuita e *open source*, per la verifica automatica dell'accessibilità dei siti web.

Il progetto denominato M.A.U.V.E. (*Multiguide Accessibility and Usability Validation Environment*) prevede un costante potenziamento della piattaforma mediante una serie di funzionalità per effettuare test di accessibilità.

- [eGLUBox-PA](#)
eGLU-box PA è una piattaforma funzionale al miglioramento della qualità dei servizi utilizzabile per la gestione dei test di usabilità automatizzati.

La piattaforma è già utilizzata da varie amministrazioni centrali, Università e Regioni.

Per utilizzare eGLU-box PA basta collegarsi a <https://egluboxpa.ddns.net/> ed effettuare la registrazione in qualità di conduttore (funzione 'Registrati').

- [Monitoraggio accessibilità e elenco errori ricorrenti](#)
Il sito espone un primo set di dati relativi all'accessibilità digitale della Pubblica Amministrazione, risultante dall'esito del monitoraggio dei siti della PA e da quanto dichiarato dalle amministrazioni relativamente allo stato di conformità dei propri siti web.

OB3.4

- [The Your Europe portal](#) - *Providing access to a network of national portals in compliance with the single digital gateway regulation*
- Documento informativo sulle Metodologia di monitoraggio messo a disposizione da AGID (giugno 2024)

Risorse e fonti di finanziamento

OB3.4

- PNRR Investimento M6 C2 I1.3.1, per un importo pari a € 1.379.990.000
- Misura PNRR M1C1-1.3.1 (ob 2.4, 2.5, 2.6)
- Piano Nazionale di Ripresa e Resilienza, misura 1.3.2 "Single Digital Gateway"

I servizi e l'accessibilità nell'INFN

L'amministrazione dell'INFN sta iniziando nel 2024 un percorso di revisione dei processi amministrativi in ottica di semplificazione e migliore mappatura su processi informatizzati, anche attraverso l'uso di servizi di consulenza.

Gia' da qualche anno il software gestionale prodotto internamente ha adottato per tutti i nuovi prodotti un'architettura a micro-servizi, che offre maggiori vantaggi in termini di resilienza, affidabilità e scalabilità. Questa soluzione ottimizza le risorse e consente di sfruttare al meglio l'infrastruttura cloud, garantendo una gestione più efficiente e flessibile dei servizi, oltre a favorire una migliore interconnessione tra di essi. Tutti gli applicativi di recente realizzazione rispettano le Linee Guida dell'AgID e le misure minime di sicurezza previste, per garantire la privacy e la protezione dei dati degli utenti. L'adozione di queste pratiche garantisce un elevato livello di sicurezza informatica e compliance con le normative vigenti. Le metodologie Agile utilizzate per lo sviluppo permettono di coniugare velocità e flessibilità, offrendo soluzioni rapide e di qualità che rispondono in maniera ottimale alle esigenze dell'utenza. Questo, unito ad una revisione delle procedure e ad uno snellimento dei processi, migliora l'efficienza e l'esperienza complessiva dei servizi offerti.

Questi prodotti implementano API REST, compatibili con le API per l'interoperabilità con i servizi della PDND, nell'ottica di condividere se necessario i dati disponibili, ma soprattutto di utilizzare i dati presenti e condivisi dalle altre PA, come anche descritto nel capitolo 4. Lo scopo è di rendere il software gestionale utilizzato il più possibile interconnesso, anche internamente, scambiando i dati necessari ad implementare il principio *once-only* e rendendo coerente l'intero sistema gestionale dell'Ente. A questo proposito, l'INFN stipula nel 2024 un accordo di adesione alla PDND e pianifica per il 2025 di cominciarne ad utilizzare le API.

In questa ottica il coinvolgimento dell'RTD e del suo comitato di coordinamento insieme all'UTD nell'acquisto di servizi esternalizzati consentirà anche di richiedere le specifiche corrette per attuare più semplicemente che in passato questi principi senza dover richiedere modifiche successive in fase di esecuzione del contratto, con conseguente aggravio di lavoro per tutte le parti in gioco ed eventuale aumento dei costi.

L'attuale architettura di *data warehouse* si basa su accessi diretti a database. Nella nuova architettura a micro-servizi, anche questo passaggio di dati dovrebbe avvenire senza accedere direttamente ai database dei prodotti. Pertanto, durante gli anni 2024 e 2025, una nuova architettura di *data warehouse* dovrebbe consentirci di incrociare tutti i dati presenti nei nuovi e-service con quelli provenienti dai prodotti di tipo *legacy*, migliorando la disponibilità di informazioni per il sistema di business intelligence e, di conseguenza, la possibilità per il management di prendere decisioni informate sulla base di dati oggettivi.

Nel contempo, tra il 2024 ed il 2026 alcune procedure amministrative informatizzate tramite framework obsoleti verranno riscritti con la nuova architettura o esternalizzati, anche considerando l'eventuale riuso di software di altri enti.

Un grande sforzo verso la sensibilizzazione alla formazione corretta di documenti digitali accessibili è continuamente compiuto attraverso corsi specifici interni di amministrazione digitale, complementari ai corsi del Syllabus, il cui uso viene incoraggiato. Allo stesso tempo l'UTD ha prodotto e pubblicato sul sito della DSI alcune brevi pillole formative che intendono essere di supporto al personale amministrativo nella produzione di documenti. Inoltre, la Direzione Sistemi Informativi (DSI) ha pubblicato una nota tecnica specifica su come produrre un documento accessibile.

Poiché tutti i servizi interni dell'INFN sono basati su applicazioni web, uno studio è stato effettuato sulle modalità di sviluppo per la creazione di servizi accessibili. Anche su questo tema, una nota tecnica è stata prodotta per guidare gli sviluppatori.

Per quanto riguarda i siti web, è in corso un lavoro di ristrutturazione dei siti rivolti al pubblico. Questo lavoro ha prodotto dei template in cui è stata posta particolare cura nel garantire l'accessibilità. I nuovi siti dell'Istituto e delle sue unità operative verranno implementati e pubblicati tra il 2024 e 2025.

Capitolo 4 - Piattaforme

Come per i precedenti Piani, il Piano triennale per l'informatica nella Pubblica Amministrazione 2024- 26 prende in esame l'evoluzione delle piattaforme della Pubblica Amministrazione, che offrono funzionalità fondamentali nella digitalizzazione dei processi e dei servizi della PA.

La raggiunta maturità di alcune piattaforme, già presentate nelle precedenti edizioni del Piano, permette qui di focalizzarsi sui servizi che esse offrono a cittadini, a imprese e ad altre amministrazioni, in continuità con quanto descritto nel capitolo precedente "Servizi".

Nella prima parte di questo capitolo, quindi, si illustrano le piattaforme nazionali che erogano servizi a cittadini e imprese: PagoPA, Applo, Send, Spid e Cie, NoiPA, Fascicolo sanitario elettronico e SUAP/SUE.

L'obiettivo riferibile a tutte queste piattaforme è comune, si tratta di migliorare i servizi già erogati nei termini che verranno dettagliati nei risultati attesi e nelle linee di azione. In questa sezione, la descrizione di ciascuna piattaforma riporterà lo stesso obiettivo mentre gli altri elementi descrittivi saranno specifici della piattaforma presa in esame. Nella seconda parte di questo capitolo verranno descritte le piattaforme che attestano attributi ed infine si parlerà di basi di dati di interesse nazionale.

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

Scenario

pagoPA

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

AppIO

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

SEND

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

SEND solleva gli enti da tutti gli adempimenti legati alla gestione delle comunicazioni a valore legale e riduce l'incertezza della reperibilità del destinatario.

SPID

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

SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia Digitale, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese.

A dicembre 2023 sono state rilasciate ai cittadini oltre 36 milioni e mezzo di identità digitali SPID, che hanno permesso nel 2023 di totalizzare oltre 1.000.000.000 di autenticazioni a servizi *online* di pubbliche amministrazioni e privati. Attualmente la federazione SPID è composta da più di 15.000 fornitori di servizi pubblici e 177 fornitori di servizi privati.

Nell'ambito del PNRR il sub-investimento M1C1 1.4.4 "Rafforzamento dell'adozione delle piattaforme nazionali di identità digitale (SPID, CIE) e dell'Anagrafe nazionale della popolazione residente (ANPR)", di cui è soggetto titolare il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri, include fra le sue finalità che i gestori delle identità SPID assicurino l'innalzamento del livello dei servizi, della qualità, sicurezza e di interoperabilità degli stessi stabiliti dalle Linee guida AGID, come previsto dall'art. 18 bis del D.L. 24/02/2023 n. 13, convertito dalla L. 21/04/2023 n. 41.

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

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

CIE

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

Alla data di metà dicembre 2023 sono state rilasciate ai cittadini oltre 40 milioni di Carte di Identità Elettroniche, che hanno permesso nel 2023 di totalizzare circa 32.000.000 di autenticazioni a servizi *online* di pubbliche amministrazioni e privati. Attualmente la federazione CIE è composta da più di 10.000 fornitori di servizi pubblici e circa 100 fornitori di servizi privati.

Come sancito dal Decreto 8 settembre 2022 "Modalità di impiego della carta di identità elettronica", sono previste le seguenti evolutive sul servizio CIEId:

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

NoiPA

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

Fascicolo Sanitario Elettronico

Il Fascicolo Sanitario Elettronico (FSE 2.0) ha l'obiettivo di garantire la diffusione e l'accessibilità dei servizi di sanità digitale in modo omogeneo e capillare su tutto il territorio nazionale a favore dei cittadini e degli operatori sanitari delle strutture pubbliche, private accreditate e private.

La verifica formale e semantica della corretta implementazione e strutturazione dei documenti secondo gli standard ha lo scopo di assicurare omogeneità a livello nazionale per i servizi del FSE 2.0 disponibili ai cittadini e ai professionisti della Sanità.

Attraverso interventi sistematici di formazione, si intende superare le criticità legate alle competenze digitali dei professionisti del sistema sanitario, innalzandone significativamente il livello per un utilizzo pieno ed efficace del FSE 2.0.

SUAP e SUE

Nel panorama della Pubblica Amministrazione, gli Sportelli Unici per le Attività Produttive (SUAP) e per l'Edilizia (SUE) assumono un ruolo centrale come punto di convergenza per imprese, professionisti e cittadini nell'interazione con le istituzioni, nell'ambito degli adempimenti previsti per le attività produttive (quali, ad esempio, la produzione di beni e servizi, le attività agricole, commerciali e artigianali, le attività turistiche alberghiere ed extra-alberghiere, i servizi resi dalle banche e dagli intermediari finanziari e i servizi di telecomunicazione, ecc.) e gli interventi edilizi. Si tratta di due pilastri fondamentali in un contesto in continua evoluzione, dove la digitalizzazione si configura non solo come una necessità imprescindibile, ma anche come una leva strategica fondamentale per favorire la competitività delle imprese, stimolare la crescita economica del Paese e ottimizzare la tempestività nell'evasione delle richieste. In questo scenario, la semplificazione e l'accelerazione dei procedimenti amministrativi diventano così il mezzo con cui costruire un futuro in cui le opportunità digitali diventino accessibili a tutti.

Nell'ambito delle iniziative previste dal Piano Nazionale di Ripresa e Resilienza (PNRR), è stato avviato il percorso di trasformazione incentrato sulla digitalizzazione e la semplificazione dei sistemi informatici, partendo dalla redazione delle Specifiche tecniche, elaborate attraverso il lavoro congiunto del Gruppo tecnico (istituito dal Ministero delle Imprese e del *Made in Italy* e dal Dipartimento della Funzione Pubblica e coordinato dall'Agenzia per l'Italia Digitale), le quali delineano l'insieme delle regole e delle modalità tecnologiche che i Sistemi Informatici degli Sportelli Unici (SSU) devono adottare, per la gestione ottimale dei procedimenti amministrativi riguardanti le attività produttive, conformemente alle disposizioni del DPR 160/2010 e ss.mm.ii.

La fase operativa di questo percorso è stata condotta partendo da un'attenta analisi della situazione esistente, rafforzata, successivamente, dalla somministrazione di un questionario di valutazione, volto ad identificare la maturità tecnologica iniziale degli sportelli unici, grazie alla diretta collaborazione delle amministrazioni coinvolte. Attualmente, è terminata la raccolta delle informazioni, perfezionata con altre attività di indagine, come la consulta dei fornitori dei servizi IT relativi alle piattaforme, i tavoli tematici regionali e il coinvolgimento di altri *stakeholder* e si sta procedendo con la definizione dei piani di intervento, da realizzarsi attraverso risorse finanziarie messe a disposizione dal Dipartimento della Funzione Pubblica, tramite la pubblicazione di bandi/stipula di accordi per l'adeguamento delle piattaforme.

In tale percorso di trasformazione, che vedrà impegnate le pubbliche amministrazioni nel prossimo triennio, per garantire il raggiungimento delle *milestone* definite nell'ambito del PNRR, deve essere assicurato il supporto tecnico necessario all'adeguamento delle soluzioni informatiche alle Specifiche tecniche, attraverso la condivisione delle conoscenze e dell'esperienza maturata nel campo, utili a fornire una corretta interpretazione delle stesse durante la fase di realizzazione degli interventi.

Contesto normativo e strategico

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

PagoPA

Riferimenti normativi italiani:

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

AppIO

Riferimenti normativi italiani:

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

SEND

Riferimenti normativi italiani:

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

SPID

Riferimenti normativi italiani:

- [Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" \(CAD\), art.64](#)
- [Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014 recante la Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese \(SPID\), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese](#)
- [Regolamento AGID recante le regole tecniche dello SPID \(2014\)](#)
- [Regolamento AGID recante le modalità attuative per la realizzazione dello SPID \(2014\)](#)
- [Linee Guida AGID per la realizzazione di un modello di R.A.O. pubblico \(2019\)](#)
- [Linee guida per il rilascio dell'identità digitale per uso professionale \(2020\)](#)
- [Linee guida AGID recanti Regole Tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD \(2020\)](#)
- [Linee Guida AGID "OpenID Connect in SPID" \(2021\)](#)
- [Linee guida AGID per la fruizione dei servizi SPID da parte dei minori \(2022\)](#)
- [Linee guida AGID recanti le regole tecniche dei gestori di attributi qualificati \(2022\)](#)

CIE

Riferimenti normativi italiani:

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

Riferimenti normativi europei:

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

NoiPA

Riferimenti normativi italiani:

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

FSE

Riferimenti normativi italiani:

- [Decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla Legge 17 dicembre 2012, n. 221 “Ulteriori misure urgenti per la crescita del Paese”](#)
- [Decreto del Presidente del Consiglio dei Ministri 29 settembre 2015, n. 178 “Regolamento in materia di fascicolo sanitario elettronico”](#)

- [Legge 11 dicembre 2016, n. 232 "Bilancio di previsione dello Stato per l'anno finanziario 2017 e bilancio pluriennale per il triennio 2017-2019"](#)
- [Decreto-legge 19 maggio 2020, n. 34, convertito con modificazioni dalla Legge 17 luglio 2020, n. 77 "Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19"](#)
- [Decreto-legge 28 ottobre 2020, n. 137, convertito con modificazioni dalla Legge 18 dicembre 2020, n. 176 "Ulteriori misure urgenti in materia di tutela della salute, sostegno ai lavoratori e alle imprese, giustizia e sicurezza, connesse all'emergenza epidemiologica da COVID-19"](#)
- [Decreto-legge 27 gennaio 2022, n. 4, convertito con modificazioni dalla Legge 28 marzo 2022, n. 25 "Misure urgenti in materia di sostegno alle imprese e agli operatori economici, di lavoro, salute e servizi territoriali, connesse all'emergenza da COVID-19, nonché per il contenimento degli effetti degli aumenti dei prezzi nel settore elettrico"](#)
- [Decreto del Ministero dell'Economia e delle Finanze 23 dicembre 2019 "Utilizzo del Fondo per il finanziamento degli investimenti e lo sviluppo infrastrutturale - Fascicolo sanitario elettronico" \(Piano di digitalizzazione dei dati e documenti sanitari\)](#)
- [Decreto del Ministero della Salute 20 maggio 2022 "Adozione delle Linee guida per l'attuazione del Fascicolo sanitario elettronico" pubblicato sulla GU Serie Generale n. 160 11.07.2022](#)
- [Decreto del Ministero della Salute 7 settembre 2023 "Fascicolo sanitario elettronico 2.0"](#)
- [Linee Guida per l'attuazione del Fascicolo Sanitario Elettronico \(2022\)](#)
- Piano Nazionale di Ripresa e Resilienza:
 - [M6 - Salute C2 1.3.1 "Rafforzamento dell'infrastruttura tecnologica e degli strumenti per la raccolta, l'elaborazione, l'analisi dei dati e la simulazione \(FSE\)"](#)

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

RA4.1.1 - Incremento dei servizi sulla piattaforma pagoPA

- **Target 2024** - +20.000 servizi per un totale di almeno 280.000
- **Target 2025** - +20.000 servizi per un totale di almeno 300.000
- **Target 2026** - +10.000 servizi per un totale di almeno 310.000

RA4.1.2 - Incremento dei servizi sulla Piattaforma IO (l'App dei servizi pubblici)

- **Target 2024** - +10.000 servizi per un totale di almeno 290.000
- **Target 2025** - +10.000 servizi per un totale di almeno 300.000
- **Target 2026** - +5.000 servizi per un totale di almeno 305.000

RA4.1.3 - Incremento degli enti che usano SEND

- **Target 2024** - +1.200 enti per un totale di almeno 2.000
- **Target 2025** - +2.000 enti per un totale di almeno 4.000
- **Target 2026** - +2.400 enti per un totale di almeno 6.400

RA4.1.4 - Incremento dell'adozione e dell'utilizzo di SPID e CIE da parte delle Pubbliche Amministrazioni

- **Target 2024**
 - Incremento del numero di autenticazioni SPID del 5%, rispetto al monitoraggio di novembre 2023 (992.721.372)

- Incremento del numero delle identità SPID per minori del 10%, del numero delle identità uso professionale del 10%, rispetto al monitoraggio di marzo 2024
- Incremento del numero di autenticazioni CIE del 25% rispetto alla *baseline* di 32.000.000 di autenticazioni al 2023
- **Target 2025**
 - Incremento del numero di autenticazioni SPID del 8%, rispetto al monitoraggio di novembre 2023 (992.721.372)
 - Incremento del numero delle identità SPID per minori del 20%, del numero delle identità uso professionale del 20%, rispetto al monitoraggio di marzo 2024
 - Incremento del numero di autenticazioni CIE del 35% rispetto alla *baseline*
- **Target 2026**
 - Incremento del numero di autenticazioni SPID del 10%, rispetto al monitoraggio di novembre 2023 (992.721.372)
 - Incremento del numero delle identità SPID per minori del 30%, del numero delle identità uso professionale del 30%, rispetto al monitoraggio di marzo 2024
 - Incremento del numero di autenticazioni CIE del 50% rispetto alla *baseline*

RA4.1.5 - Promuovere l'adesione ai servizi della piattaforma NoiPA per supportare l'azione amministrativa nella gestione del personale

- **Target 2024** - 5 campagne di promozione e diffusione dei servizi
- **Target 2025** - 6 campagne di promozione e diffusione dei servizi
- **Target 2026** - 7 campagne di promozione e diffusione dei servizi

RA4.1.6 - Incremento del livello di alimentazione e digitalizzazione del Fascicolo Sanitario Elettronico

- **Target 2024** - Tutti i documenti del Fascicolo Sanitario Elettronico devono essere digitalmente nativi e in formato standard
- **Target 2025** - L'85% dei medici di famiglia alimentano il Fascicolo Sanitario Elettronico
- **Target 2026** - Tutte le Regioni e Province Autonome adottano e utilizzano il Fascicolo Sanitario Elettronico

RA4.1.7 - Semplificazione e creazione di un catalogo di tutte le procedure SUAP e SUE e relativi regimi amministrativi applicati su tutto il territorio nazionale

- **Target 2024** - 200 procedure critiche di interesse per cittadini ed imprese semplificate e digitalizzate
- **Target 2025** - 50 ulteriori procedure critiche di interesse per cittadini ed imprese semplificate e digitalizzate
- **Target 2026** - 350 ulteriori procedure critiche di interesse per cittadini ed imprese semplificate e digitalizzate

Linee di azione istituzionali

RA4.1.1

- **Settembre 2024** - Introduzione di nuove funzionalità a disposizione degli Enti Creditori per gestire le opzioni di pagamento (es. piani rateali, maggiorazioni o riduzioni dell'importo) - (PagoPA S.p.A.) - CAP4.01
- **Dicembre 2024** - Introduzione di un modello per la gestione di pagamenti *corporate* massivi - (PagoPA S.p.A.) - CAP4.02

- **Dicembre 2024** - Implementazione di azioni incentivanti di *quality Improvement* verso Enti Creditori e PSP volti a migliorare la qualità dei pagamenti pagoPA - (PagoPA S.p.A.) - CAP4.03
- **Settembre 2025** - Introduzione di processi organizzativi e implementazioni tecnologiche integrate alla piattaforma che abilitano nuove funzionalità di domiciliazione del pagamento - (PagoPA S.p.A.) - CAP4.04
- **Dicembre 2025** - Revisione dell'esperienza di pagamento su tutti i canali di pagamento, in modo da migliorare l'efficacia sia dei processi *online* sia fisici, in particolare su ATM e POS - (PagoPA S.p.A.) - CAP4.05
- **Settembre 2026** - Digitalizzazione di alcuni servizi di pagamento degli Enti Creditori ad oggi non gestiti o gestiti solo parzialmente (es. ingressi museali, tassa di soggiorno, pagamenti sanità) - (PagoPA S.p.A.) - CAP4.06
- **Dicembre 2026** - Estensione del perimetro di intermediazione anche agli strumenti di Agenzia delle Entrate (estensione @e-bollo, I24 e F24) - (PagoPA S.p.A.) - CAP4.07

RA4.1.2

- **Dicembre 2026** - Sviluppo di nuove funzionalità atte a facilitare l'erogazione di servizi da parte dei soggetti di cui all'articolo 2, comma 2, del decreto legislativo 7 marzo 2005, n. 82, nonché la comunicazione elettronica con i cittadini, anche finalizzata al perfezionamento di istanze, richieste e/o procedimenti amministrativi - (PagoPA S.p.A.) - CAP4.08

RA4.1.3

- **Dicembre 2024** - Implementazione di funzionalità a supporto dell'attivazione degli Enti target per l'*onboarding* di servizi diversi di notificazione, con particolare riferimento alla possibilità per soggetti strutturati (vedi CAF) d'integrarsi B2B con la piattaforma - (PagoPA S.p.A.) - CAP4.09
- **Dicembre 2025** - Implementazione della comunicazione bidirezionale: la piattaforma potrà permettere la comunicazione a valore legale anche verso il mittente - (PagoPA S.p.A.) - CAP4.10

RA4.1.4

- **Marzo 2024** - Individuazione delle amministrazioni che offrono servizi - utilizzabili da minori - che prevedano l'adozione e l'utilizzo di SPID da parte dei minori stessi - (AGID) - CAP4.11
- **Marzo 2024** - Individuazione delle amministrazioni che offrono servizi - utilizzabili da professionisti e imprese - che prevedano l'adozione e l'utilizzo di SPID per uso professionale - (AGID) - CAP4.12
- **Luglio 2024** - Chiusura degli avvisi PNRR sull'investimento 1.4.4a relativi all'adozione di SPID e CIE da parte di Comuni e altre amministrazioni ad esclusione delle scuole - (Dipartimento per la Trasformazione Digitale) - CAP4.13
- **Gennaio 2025** - Completamento della federazione SPID OIDC ed attuazione completa del Regolamento SPID *OIDC Federation* - (AGID) - CAP4.14
- **Gennaio 2025** - Avvio adesione delle *Attribute Authorities* SPID - (AGID) - CAP4.15
- **Aprile 2025** - Sviluppo di un meccanismo di controllo genitoriale per consentire un accesso controllato ai servizi *online* offerti ai minori - (IPZS) - CAP4.16
- **Luglio 2025** - Ampliamento del set di attributi forniti tramite autenticazione con CIEId, come previsto dall'art. 6 del DPCM 8 settembre 2022 - (IPZS) - CAP4.17

RA4.1.5

- **Dicembre 2024** - Definire e realizzare campagne di promozione dei servizi e valorizzazione del patrimonio informativo - (MEF) - CAP4.18

- **Dicembre 2025** - Definire un modello di misurazione della qualità dei servizi erogati - (MEF) - CAP4.19

RA4.1.6

- **Aprile 2024** - Messa a disposizione la piattaforma per il monitoraggio degli indicatori mensili e trimestrali, secondo quanto previsto dalle Linee Guida per l'attuazione del Fascicolo Sanitario Elettronico - (Ministero della Salute, Dipartimento per la Trasformazione Digitale, Agenas) - CAP4.20
- **Luglio 2024** - Verifica degli indicatori previsti per il raggiungimento degli obiettivi PNRR M6C2 1.3 al 30 giugno - (Ministero della Salute, Dipartimento per la Trasformazione Digitale, Agenas) - CAP4.21
- **Luglio 2025** - Verifica degli indicatori previsti per il raggiungimento degli obiettivi PNRR al 30 giugno - (Ministero della Salute, Dipartimento per la Trasformazione Digitale, Agenas) - CAP4.22
- **Luglio 2026** - Verifica degli indicatori previsti per il raggiungimento degli obiettivi al 30 giugno - (Ministero della Salute, Dipartimento per la Trasformazione Digitale, Agenas) - CAP4.23

RA4.1.7

- **Luglio 2024** - Avvio verifiche tecniche di conformità dei sistemi informatici dalle PA interessate nei procedimenti SUAP alle specifiche tecniche di cui al DPR 160/2010 - (Ministero delle Imprese e del *Made in Italy*) - CAP4.24
- **Dicembre 2024** - Definizione della tassonomia dei procedimenti amministrativi che devono essere digitalizzati nell'ecosistema SSU, in ambito SUAP/SUE - 200 procedure - (Dipartimento della Funzione Pubblica, Conferenza dei Presidenti delle Regioni, ANCI, UPI) - CAP4.25
- **Dicembre 2024** - Semplificazione e standardizzazione nazionale dei moduli e dei procedimenti amministrativi nell'ecosistema SSU, in ambito SUAP/SUE - 200 procedure - (Dipartimento della Funzione Pubblica, Conferenza dei Presidenti delle Regioni, ANCI, UPI) - CAP4.26
- **Giugno 2026** - Definizione della tassonomia dei procedimenti amministrativi che devono essere digitalizzati nell'ecosistema SSU, in ambito SUAP/SUE - 400 procedure - (Dipartimento della Funzione Pubblica, Conferenza dei Presidenti delle Regioni, ANCI, UPI) - CAP4.27
- **Giugno 2026** - Semplificazione e standardizzazione nazionale dei moduli e dei procedimenti amministrativi nell'ecosistema SSU, in ambito SUAP/SUE - 200 procedure - (Dipartimento per la Funzione Pubblica, Conferenza dei Presidenti delle Regioni, ANCI, UPI) - CAP4.28

Linee di azione per le PA

RA4.1.1

- **Dicembre 2026** - Le PA aderenti a pagoPA assicurano l'attivazione di nuovi servizi in linea con i target sopra descritti e secondo le modalità attuative definite nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR) - CAP4.PA.01

RA4.1.2

- **Dicembre 2026** - Le PA aderenti a App IO assicurano l'attivazione di nuovi servizi in linea con i target sopra descritti e secondo le modalità attuative definite nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR) - CAP4.PA.02

RA4.1.3

- **Dicembre 2026** - Le PA centrali e i Comuni, in linea con i target sopra descritti e secondo la roadmap di attuazione prevista dal Piano Nazionale di Ripresa e Resilienza (PNRR), si integreranno a SEND - CAP4.PA.03

RA4.1.4

Linee d'azione vigenti

- Le PA e i gestori di pubblici servizi proseguono il percorso di adesione a SPID e CIE, dismettendo le altre modalità di autenticazione associate ai propri servizi online e integrando lo SPID uso professionale per i servizi diretti a professionisti e imprese - CAP4.PA.04
- Le PA e i gestori di pubblici servizi interessati cessano il rilascio di credenziali proprietarie a cittadini dotabili di SPID e/o CIE - CAP4.PA.05
- Le PA e i gestori di pubblici servizi interessati adottano lo SPID e la CIE *by default*: le nuove applicazioni devono nascere SPID e *CIE-only* a meno che non ci siano vincoli normativi o tecnologici, se dedicate a soggetti dotabili di SPID o CIE. Le PA che intendono adottare lo SPID di livello 2 e 3 devono anche adottare il "Login with eIDAS" per l'accesso transfrontaliero ai propri servizi - CAP4.PA.06
- Le PA devono adeguarsi alle evoluzioni previste dall'ecosistema SPID (tra cui OpenID Connect, uso professionale, *Attribute Authorities*, servizi per i minori e gestione degli attributi qualificati) - CAP4.PA.07

RA4.1.5

Linee di azione vigenti

- Le PA che intendono aderire a NoiPA esprimono manifestazione di interesse e inviano richiesta - CAP4.PA.08

RA4.1.6

- **Dicembre 2024** - Le Regioni e le Province Autonome rispettano le scadenze delle attività previste nel proprio Piano di adeguamento tecnologico, in coerenza con i decreti attuativi che definiscono i contenuti del FSE e la standardizzazione da parte di HL7Italia - CAP4.PA.09
- **Dicembre 2025** - Le Regioni e le Province Autonome rispettano le scadenze delle attività previste nel proprio Piano di adeguamento tecnologico, in coerenza con i decreti attuativi che definiscono i contenuti del FSE e la standardizzazione da parte di HL7Italia - CAP4.PA.10
- **Giugno 2026** - Le Regioni e le Province Autonome rispettano le scadenze delle attività previste dal proprio Piano di adeguamento tecnologico, in coerenza con i decreti attuativi che definiscono i contenuti del FSE e la standardizzazione da parte di HL7Italia - CAP4.PA.11

RA4.1.7

- **Gennaio 2024** - Realizzazione e prima alimentazione del Catalogo Unico dei procedimenti del SUAP - (PAC/PAL-Comuni, Regioni, Enti Terzi, Unioncamere) - CAP4.PA.12
- **Marzo 2024** - Identificazione della migliore soluzione da adottare dalle PA interessate nei procedimenti SUAP/SUE, in funzione del loro contesto, sulla base delle possibili soluzioni messe a disposizione dalle specifiche tecniche - (PAC/PAL-Comuni, Regioni, Enti Terzi) - CAP4.PA.13
- **Dicembre 2024** - Adeguamento alle specifiche tecniche delle infrastrutture delle PA interessate nei procedimenti SUAP/SUE - (PAC/PAL-Comuni, Regioni, Enti Terzi) - CAP4.PA.14
- **Dicembre 2024** - Messa a disposizione di soluzioni alternative all'adeguamento alle specifiche tecniche dei propri sistemi informatici SSU, in ambito SUAP/SUE, quali, ad esempio: Impresa

in un giorno per i comuni e Soluzione Sussidiaria per gli enti terzi - (Regioni, Consorzi, Unioncamere) - CAP4.PA.15

- **Dicembre 2024** - Aggiornamento del Catalogo Unico dei procedimenti del SUAP - (PAC/PAL-Comuni, Regioni, Enti Terzi, Unioncamere) - CAP4.PA.16
- **Giugno 2026** - Aggiornamento costante del Catalogo Unico dei procedimenti del SUAP - (PAC/PAL-Comuni, Regioni, Enti Terzi, Unioncamere) - CAP4.PA.17

Piattaforme che attestano attributi

Scenario

Negli ultimi anni le iniziative intraprese dai vari attori coinvolti nell'ambito del Piano, hanno favorito una importante accelerazione nella diffusione di alcune delle principali piattaforme abilitanti, in termini di adozione da parte delle PA e di fruizione da parte degli utenti. Il Piano descrive lo sviluppo di nuove piattaforme e il consolidamento di quelle già in essere attraverso l'aggiunta di nuove funzionalità. Tali piattaforme rendono disponibili i dati di settore ai cittadini e PA, consentono di razionalizzare i servizi per le amministrazioni e di semplificare tramite l'utilizzo delle tecnologie digitali l'interazione tra cittadini e PA (per la Piattaforma Digitale Nazionale Dati – PDND).

Ad esempio, nel luglio 2023 la Piattaforma INAD è andata in esercizio, in consultazione, sia tramite il sito web sia tramite le API esposte su PDND, attualmente in esercizio. La piattaforma è quindi a disposizione per entrambe le modalità di fruizione, da parte delle pubbliche amministrazioni. Si invitano pertanto le PA a fruire dei relativi servizi, compatibilmente con il loro dimensionamento.

In questo ambito vengono attuate le seguenti Piattaforme che hanno la caratteristica di attestare attributi anagrafici e di settore.

ANPR: è l'Anagrafe Nazionale che raccoglie tutti i dati anagrafici dei cittadini residenti in Italia e dei cittadini italiani residenti all'estero, aggiornata con continuità dagli oltre 7900 comuni italiani, consentendo di avere un set di dati anagrafici dei cittadini certo, accessibile, affidabile e sicuro su cui sviluppare servizi integrati ed evoluti per semplificare e velocizzare le procedure tra Pubbliche amministrazioni e con il cittadino.

Sul portale ANPR, nell'area riservata del cittadino, sono attualmente disponibili i servizi che consentono al cittadino di:

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

A dicembre 2022 sono stati resi disponibili i servizi per consentire, da parte dei Comuni, l'invio dei dati elettorali dei cittadini in ANPR. Attualmente oltre il 97% dei comuni italiani hanno aderito ai servizi, inviando i dati elettorali dei cittadini.

La presenza dei dati elettorali in ANPR consentirà ai cittadini di visualizzare nell'area riservata i dati relativi alla propria posizione elettorale e richiedere certificati di godimento dei diritti politici e di iscrizione nelle liste elettorali.

Inoltre, consentirà di verificare in tempo reale la posizione elettorale di un cittadino da parte di altre Amministrazioni che ne abbiano necessità per fini istituzionali. Una prima applicazione si avrà con l'integrazione dei servizi ANPR con la Piattaforma Referendum, piattaforma *online* che consentirà la sottoscrizione di proposte referendarie e di iniziativa popolare, verificando in tempo reale la posizione elettorale del cittadino sottoscrittore.

Al fine di agevolare lo sviluppo di sistemi integrati ed evoluti, che semplifichino e velocizzino le procedure tra le Pubbliche Amministrazioni, ANPR ha reso disponibili 28 e-service sulla Piattaforma Nazionale Digitale Dati (PDND) - Interoperabilità, consentendo la consultazione dei dati ANPR da parte di altri Enti aventi diritto, nel rispetto dei principi del Regolamento *Privacy*.

In aggiunta, l'integrazione dell'ANPR con i servizi dello Stato civile digitale ha un rilievo centrale e strategico nel processo di digitalizzazione della Pubblica Amministrazione e costituisce un significativo strumento di semplificazione per i Comuni e per i cittadini. Si prevede, infatti, la completa digitalizzazione dei registri dello Stato civile tenuti dai Comuni (nascita, matrimonio, unione civile, cittadinanza e morte), con conseguente eliminazione dei registri cartacei, e la conservazione dei relativi atti digitali in un unico archivio nazionale del Ministero dell'Interno, permettendone la consultazione a livello nazionale e offrendo la possibilità di produrre estratti o certificati tramite il sistema centrale, senza doverli richiedere necessariamente al Comune che li ha generati. Alcuni Comuni pilota ad ottobre 2023 hanno iniziato ad utilizzare i servizi resi disponibili da ANPR, formando atti digitali di stato civile con effetti giuridici.

ANPR si sta integrando con le anagrafi settoriali del lavoro, della pensione e del *welfare* e ogni nuova anagrafe che abbia come riferimento la popolazione residente sarà logicamente integrata con ANPR.

In questo contesto, per rafforzare gli interventi nei settori di istruzione, università e ricerca, accelerare il processo di automazione amministrativa e migliorare i servizi per i cittadini e le pubbliche amministrazioni, sono istituite due Anagrafi:

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

Le due Anagrafi mirano ad assicurare:

- La centralizzazione dei dati attualmente distribuiti su tutto il territorio italiano in oltre 10.000 scuole (ANIST) e 500 istituti di formazione superiore (ANIS);
- la disponibilità e l'accesso ai dati per:
 - scuole e istituti di formazione superiore (IFS), al fine di facilitare il reperimento delle informazioni relative al percorso scolastico e/o accademico dei propri studenti, efficientando le procedure di iscrizione;
 - cittadini, al fine rendere possibile, attraverso il Portale dedicato, la consultazione online dei dati relativi al proprio percorso scolastico e/o accademico, anche a fini certificativi;
 - PA per fini istituzionali;
 - soggetti privati autorizzati, per gli scopi previsti dalla legge.
- l'interoperabilità con altre banche dati (es. con ANPR per la gestione dei dati anagrafici degli studenti, eliminando duplicazioni e rischi di disallineamento);
- il riconoscimento nell'UE e extra-EU dei titoli di studio.

Per l'avvio progettuale di ANIST si attende la conclusione del relativo iter normativo.

Contesto normativo e strategico

ANPR

Riferimenti normativi italiani:

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

ANIS

Riferimenti normativi italiani:

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

ANIST

Riferimenti normativi italiani:

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

Riferimenti normativi italiani:

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

Obiettivo 4.2 - Ottenere la piena interoperabilità tra le piattaforme

RA4.2.1 - Adesione ai nuovi servizi offerti da ANPR

- **Target 2024** - 100% dei comuni che aderiscono ai servizi elettorali su ANPR
- **Target 2025** - 100% dei comuni che aderiscono ai servizi di stato civile su ANPR
- **Target 2026** - Piena interoperabilità con le altre basi dati di interesse nazionale (come definite nel CAD art. 60, comma 3-bis)

RA4.2.2 - Disponibilità dei dati su iscrizioni e titoli di studio su ANIS

- **Target 2024** - n.d.
- **Target 2025** - n.d.
- **Target 2026** - 100% dei dati su iscrizioni e titoli di studio disponibili e fruibili su ANIS

RA4.2.3 - Realizzazione della piattaforma ANIST

- **Target 2024** - Rilascio della piattaforma ANIST
- **Target 2025** - n.d.
- **Target 2026** - n.d.

Linee di azione istituzionali

RA4.2.1

- **Giugno 2024** - Organizzazione di *webinar* e corsi di formazione per gli Ufficiali d'Anagrafe, per gli Ufficiali Elettorali e per gli Ufficiali di Stato Civile - (Dipartimento per la Trasformazione Digitale) - CAP4.29
- **Dicembre 2025** - Supporto ai comuni tramite contributi per l'adesione ai servizi elettorali e allo stato civile disponibili da web app ANPR - (Dipartimento per la Trasformazione Digitale) - CAP4.30

RA4.2.2

- **Gennaio 2024** - Messa a disposizione sul portale ANIS nell'area tecnica una guida per gli IFS che identifica le modalità di interlocuzione, approfondendo dati contenuti, modalità di alimentazione e di consultazione di ANIS - (Dipartimento per la Trasformazione Digitale) - CAP4.31

- **Gennaio 2024** - Pubblicazione di bandi pubblici su [PA Digitale 2026](#) per il finanziamento delle attività atte all'integrazione e all'erogazione di e-service su PDND - (Dipartimento per la Trasformazione Digitale) - CAP4.32
- **Febbraio 2024** - Rilascio *web application* per il caricamento massivo dei dati - (Dipartimento per la Trasformazione Digitale) - CAP4.33

RA4.2.3

- **Giugno 2024** - Messa a disposizione di un portale dedicato ad ANIST comprensivo di un'area tecnica dove sarà pubblicata la documentazione di interesse per le scuole - (Dipartimento per la Trasformazione Digitale) - CAP4.34
- **Dicembre 2024** - Rilascio della piattaforma ANIST - (Dipartimento per la Trasformazione Digitale) - CAP4.35

Linee di azione per le PA

RA4.2.1

- **Da febbraio 2024** - Dalla "fine dell'adozione controllata" i Comuni potranno richiedere l'adesione servizi di Stato civile su ANPR - CAP4.PA.18

RA4.2.2

- **Da gennaio 2024** - Le Università e gli AFAM statali possono trasmettere i propri dati per l'integrazione su ANIS attraverso servizi resi fruibili dalla PDND secondo quanto descritto nell'area tecnica del sito <https://www.anis.mur.gov.it/area-tecnica/documentazione> - CAP4.PA.19
- **Da aprile 2024** - Le Università possono trasmettere i propri dati per l'integrazione su ANIS attraverso l'uso di una *web application* - CAP4.PA.20

RA4.2.3

- **Da luglio 2024** - Le istituzioni scolastiche possono prendere visione delle informazioni di interesse nell'area tecnica del portale messo a disposizione - CAP4.PA.21
- **Da gennaio 2025** - Le istituzioni scolastiche accedono alle funzionalità della piattaforma - CAP4.PA.22

Basi dati interesse nazionale

Scenario

I dati resi disponibili attraverso le piattaforme sono principalmente quelli relativi alle basi dati di interesse nazionale definite dall'art. 60 del CAD e riportate nell'elenco disponibile sul [sito AGID](#).

Il citato art. 60 del CAD prevede caratteristiche minime di sicurezza, accessibilità e interoperabilità ed il rispetto delle Linee guida per l'attuazione del CAD e delle vigenti regole del Sistema statistico nazionale.

A tale proposito, si richiama la [Determinazione AGID N. 68/2013 DIG](#) che, in attuazione dell'art. 2-bis del decreto-legge n. 179/2012, nel testo introdotto dalla legge di conversione 17 dicembre 2012, n. 221, ha definito le regole tecniche per l'identificazione delle basi di dati critiche tra quelle di interesse nazionale e per definirne le modalità di aggiornamento atte a garantire la qualità dei dati presenti.

In modo da verificare costantemente il livello di aderenza a tali prescrizioni, saranno definiti i processi di individuazione di ulteriori basi dati di interesse nazionale e di monitoraggio delle stesse. Tali processi

coinvolgeranno le amministrazioni titolari delle basi dati le quali dovranno adottare tutte le misure atte a garantire il rispetto dei requisiti e dovranno fornirne evidenza per consentirne l'adeguato monitoraggio. In questo ambito sono coinvolte anche tutte le altre amministrazioni che potranno proporre l'individuazione di nuove basi dati di interesse nazionale.

Contesto normativo e strategico

Riferimenti normativi italiani:

- [Decreto legislativo 7 marzo 2005, n. 82 “Codice dell'amministrazione digitale” \(in breve CAD\) art. 60](#)

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

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

- **Target 2024** - Aggiornamento delle schede descrittive delle basi dati di interesse nazionale
- **Target 2025** - 40% delle basi dati di interesse nazionale conformi alle regole tecniche
- **Target 2026** - 100% delle basi dati di interesse nazionale conformi alle regole tecniche

Linee di azione istituzionali

RA4.3.1

- **Dicembre 2024** - Definizione del processo di individuazione di nuove basi di dati di interesse nazionale - (AGID) - CAP4.36
- **Dicembre 2024** - Aggiornamento delle regole tecniche di cui all'art. 2-bis del decreto-legge n. 179/2012, convertito con la legge 17 dicembre 2012, n. 221 - (AGID) - CAP4.37
- **Dicembre 2025** - Primo monitoraggio delle basi di dati di interesse nazionale - (AGID) - CAP4.38

Linee di azione per le PA

RA4.3.1

- **Da gennaio 2025** - Le PA interessate avanzano la richiesta di inserimento delle proprie basi di dati nell'elenco di Basi di dati di interesse nazionale gestito da AGID secondo il processo definito - CAP4.PA.23
- **Da gennaio 2025** - La PA titolari di basi di dati di interesse nazionale le adeguano all'aggiornamento delle regole tecniche - CAP4.PA.24

Strumenti per l'attuazione del Piano

OB4.1

I portali delle piattaforme:

- [Developer Portal](#) un canale unico gestito da PagoPA rivolto a enti e sviluppatori, dove trovare guide, *tutorial* e strumenti per l'integrazione delle piattaforme digitali, quale evoluzione del *repository* PagoPA Docs che raccoglie tutta la documentazione delle piattaforme in carico a PagoPA

- Portali istituzionali dedicati alle piattaforme con documentazione a supporto dell'adesione da un punto di vista di gestione amministrativa, delle fasi di integrazione tecnologica e della comunicazione ai propri utenti:
 - [PagoPA](#)
 - [appIO](#)
 - [SEND](#)
 - [SPID/CIE](#)
 - [NoiPA](#)
 - [FSE](#)
 - [SUAP](#)

OB4.3

- [Schede informative basi di dati di interesse nazionale](#)

Portali istituzionali disponibili sulle seguenti basi dati di interesse nazionale:

- il [Repertorio nazionale dei dati territoriali \(RNDT\)](#) - Titolare: AGID;
- l'[Anagrafe nazionale della popolazione residente \(ANPR\)](#) - Titolare: Ministero dell'Interno;
- la [Banca dati nazionale dei contratti pubblici \(BDNCP\)](#) - Titolare: ANAC;
- il [Casellario giudiziale](#) - Titolare: Ministero della Giustizia;
- il [Registro delle imprese](#) - Titolare: UnionCamere;
- l'[Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato, non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese \(INAD\)](#) – Titolare: AGID
- l'[Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi \(IPA\)](#) – art. 6-ter - Titolare: AGID;
- l'[Indice nazionale dei domicili digitali delle imprese e dei professionisti \(INI-PEC\)](#) – art. 6-bis - Titolare: Ministero dello Sviluppo Economico;
- il [Catalogo dei dati delle Pubbliche amministrazioni](#) - Titolare: AGID;
- il [Sistema informativo nazionale federato delle infrastrutture \(SINFI\)](#) - Titolare: Ministero dello Sviluppo Economico.

Risorse e fonti di finanziamento

OB4.1

- Avvisi pubblici consultabili sul sito istituzionale [PA digitale 2026](#):
 - Avvisi pubblici - finalizzati alla migrazione e all'attivazione dei servizi di incasso delle Pubbliche Amministrazioni sulla piattaforma pagoPA - emanati dal Dipartimento della Trasformazione Digitale (DTD), nell'ambito della componente M1.C1 - Digitalizzazione, innovazione e sicurezza PA del Piano PNRR, e, in particolare, relativi al Sub-investimento 1.4.3 – Diffusione della piattaforma dei pagamenti elettronici pagoPA e dell'AppIO dei servizi pubblici.
 - Avvisi pubblici - finalizzati attivazione dei servizi digitali delle Pubbliche Amministrazioni sull'app IO - emanati dal Dipartimento della Trasformazione Digitale (DTD), nell'ambito della componente M1.C1 - Digitalizzazione, innovazione e sicurezza

PA del Piano PNRR, e, in particolare, relativi al Sub-investimento 1.4.3 – Diffusione della piattaforma dei pagamenti elettronici pagoPA e dell'AppIO dei servizi pubblici.

- Avvisi pubblici - finalizzati all'integrazione con la piattaforma SEND dei processi di notificazione degli atti a valore legale attualmente in uso presso le Pubbliche Amministrazioni - emanati dal Dipartimento della Trasformazione Digitale (DTD), nell'ambito della componente M1.C1 - Digitalizzazione, innovazione e sicurezza PA del Piano PNRR, e, in particolare, relativi al Sub-investimento 1.4.5 - Piattaforma notifiche digitali.
- Avvisi pubblici - finalizzati all'integrazione con la piattaforma SEND dei processi di notificazione degli atti a valore legale attualmente in uso presso le Pubbliche Amministrazioni - emanati dal Dipartimento della Trasformazione Digitale (DTD), nell'ambito della componente M1.C1 - Digitalizzazione, innovazione e sicurezza PA del Piano PNRR, e in particolare, la Misura 1.4.4 "Estensione dell'utilizzo delle piattaforme nazionali di identità digitale - SPID CIE e dell'anagrafe nazionale digitale (ANPR)"
- Avvisi pubblici consultabili su [PNRR Salute](#) e relativi al Sub-investimento: M6 C2 I1.3.1 Rafforzamento dell'infrastruttura tecnologica e degli strumenti per la raccolta, l'elaborazione, l'analisi dei dati e la simulazione (FSE)

OB4.2

- **ANIS** - Bando pubblicato su [PA Digitale 2026](#) per il finanziamento delle attività atte all'integrazione su ANIS

L'INFN e le piattaforme

La possibilità di utilizzare le piattaforme sopra descritte è di grande interesse per l'INFN. Mentre infatti piattaforme come SUAP/SUE o FSE non sono applicabili nel nostro caso, alcuni dati, come quelli anagrafici, possono essere utilizzati per avere una unica sorgente autoritativa ed evitare raccolte ulteriori e soggette ad errori ed imprecisioni. SPID e CIE sono invece già in uso ed integrate nel nostro sistema di autenticazione ed autorizzazione (AAI).

Sarebbe di grande interesse poter utilizzare il nostro IdP, che contiene i ruoli rilevanti del personale e dei collaboratori per l'ente, per regolare in maniera automatica gli accessi e le autorizzazioni anche alle applicazioni esterne all'ente, come già avviene per quelle interne. Questo ci permetterebbe da una parte di implementare il principio *once-only* e la circolarità dei dati utilizzando le fonti autoritative presenti nelle piattaforme, allo stesso tempo, di rendere il sistema compatto dal punto di vista dell'autorizzazione a compiere azioni o ad autorizzarne, centralizzando il controllo dei ruoli in un unico database ed evitando di dover inserire a mano le autorizzazioni in ogni applicativo.

A questo scopo l'INFN, pur non essendo destinato ad alimentare queste piattaforme, si è registrato per utilizzare le API della PDND per poter accedere direttamente ai dati anagrafici dell'ANPR, senza necessità di provvedere a richieste ridondanti nei confronti dei dipendenti, dei collaboratori e più in generale dei cittadini. Di grande interesse sono anche altri casi d'uso, legati ad esempio ai dati ISEE qualora presenti per la corretta erogazione di sussidi o borse di studio e, in prospettiva, ai dati sulle piattaforme ANIS ed ANIST per tenere aggiornate le qualifiche del proprio personale e dei collaboratori.

L'Istituto ha aderito alla piattaforma PagoPA e la utilizza per i pagamenti ad altre PA. Tuttavia, non offrendo servizi a pagamento ai cittadini, non la utilizza per ricevere pagamenti.

L'Istituto sta considerando l'adesione ad AppIO, per poterne utilizzare i servizi di firma remota. Ad oggi, infatti, tutti i dipendenti vengono forniti di firma digitale al momento della presa di servizio e tale firma è utilizzata per sottoscrivere il contratto di lavoro. Di conseguenza, non sono più necessarie firme olografe per alcun documento sottoscritto da dipendenti INFN. Rimangono tuttavia esclusi, ad esempio, alcuni contratti con personale non dipendente non dotato di firma digitale, per il quale AppIO potrebbe complementare il sistema già in uso per i dipendenti e che potrebbe in aggiunta permettere la presa di servizio senza necessità di presenza fisica.

L'INFN ha aderito a SPID e CIE, integrandoli nel proprio sistema di Autenticazione ed Autorizzazione (AAI), mantenendo la propria modalità di autenticazione interna per i propri utenti e l'ha resa compatibile con lo SPID.

Mantiene tuttavia le funzionalità di auto registrazione per permettere l'accesso a procedure (come le procedure concorsuali) per le quali c'è interesse alla partecipazione di cittadini non europei o di cittadini europei non dotati di SPID o appartenenti a paesi nei quali non è matura la diffusione di un sistema federato in eIDAS.

È in fase di studio l'adozione dello SPID di livello 2, con la contemporanea adozione del LoA3 anche per il sistema di autenticazione ed autorizzazione interno. Questo potrebbe permettere, se consentito dai software che realizzano le procedure di acquisto, di utilizzare una singola fase di autenticazione come prima fase di una possibile integrazione con le procedure autorizzative interne, già informatizzate e basate sull'uso dei ruoli presenti nel database dell'IdP.

L'Istituto si adegua alle evoluzioni previste dall'ecosistema SPID per applicazioni che possono essere di utilizzo pubblico. Tutte le applicazioni dei sistemi informativi usano già OpenID Connect per autorizzazione e autenticazione.

Capitolo 5 - Dati e Intelligenza Artificiale

Open data e data governance

Scenario

La valorizzazione del patrimonio informativo pubblico è un obiettivo strategico per la Pubblica Amministrazione per affrontare efficacemente le nuove sfide dell'economia basata sui dati (*data economy*), supportare gli obiettivi definiti dalla Strategia europea in materia di dati, garantire la creazione di servizi digitali a valore aggiunto per cittadini, imprese e, in generale, per tutti i portatori di interesse e fornire ai vertici decisionali strumenti *data-driven* da utilizzare nei processi organizzativi e/o produttivi. La ingente quantità di dati prodotti dalla Pubblica Amministrazione, se caratterizzati da un'alta qualità, potrà costituire, inoltre, la base per una grande varietà di applicazioni come, per esempio, quelle riferite all'intelligenza artificiale.

La costruzione di un'economia dei dati è l'obiettivo che l'Unione Europea intende perseguire attraverso una serie di iniziative di regolazione avviate ormai dal 2020. La citata Strategia europea dei dati ha introdotto la creazione di spazi di dati (*data spaces*) comuni e interoperabili al fine di superare le barriere legali e tecniche alla condivisione dei dati e, di conseguenza, sfruttare l'enorme potenziale dell'innovazione guidata dai dati.

Con l'adozione dell'atto sulla *governance* dei dati (*Data Governance Act*), inoltre, sono stati definiti e rafforzati i meccanismi per aumentare la disponibilità dei dati e superare gli ostacoli tecnici al riutilizzo di alcune particolari tipologie di dati altrimenti non disponibili.

In Italia, con il recepimento della Direttiva Europea (UE) 2019/1024 (cosiddetta Direttiva *Open Data*) sull'apertura dei dati e il riutilizzo dell'informazione del settore pubblico, attuato con il Decreto lgs. n. 200/2021, che ha modificato il Decreto lgs. n. 36/2006, l'obiettivo strategico sopra delineato può essere perseguito attraverso l'implementazione delle nuove regole tecniche definite con le Linee guida sui dati aperti. Tale documento, adottato con la Determinazione AGID n. 183/2023 ai sensi dell'art. 71 del CAD in applicazione dell'art. 12 del citato Decreto Lgs. N. 36/2006 e s.m.i., è finalizzato a supportare le pubbliche amministrazioni e gli altri soggetti interessati nel processo di apertura dei dati e, quindi, favorire l'aumento dell'offerta di dati pubblici preziosi a fini di riutilizzo.

Tra questi tipi di dati rientrano anche quelli di elevato valore, identificati con il Regolamento di esecuzione (UE) 2023/138 sulla base delle sei categorie tematiche (dati geospaziali, dati relativi all'osservazione della Terra e all'ambiente, dati meteorologici, dati statistici, dati relativi alle imprese e alla proprietà delle imprese, dati relativi alla mobilità) stabilite con la Direttiva *Open Data*. Con riferimento a tale Regolamento, il 22 dicembre 2023 è stata adottata da AGID una specifica [Guida operativa sulle serie di dati di elevato valore](#) come documento di orientamento per le pubbliche amministrazioni per una più efficace implementazione delle disposizioni europee.

Per garantire la creazione di servizi digitali sempre più efficienti, i dati scambiati reciprocamente tra gli enti erogatori di servizi dovranno essere pienamente interoperabili, non solo da un punto di vista tecnico ma anche semantico. In altre parole, nello sviluppo di un servizio digitale, oltre a utilizzare applicazioni informatiche interoperabili, per la ricezione o l'invio dei dati, si dovrà garantire l'effettiva comprensione del significato e del formato delle informazioni scambiate, usufruendo di riferimenti nazionali come ad esempio le ontologie, i vocabolari controllati e gli schemi di dati presenti sul Catalogo Nazionale per l'Interoperabilità semantica dei dati (*National Data Catalog – NDC*).

Al fine di valutare l'impatto del processo di apertura dei dati e la conseguente ricaduta economica e sociale, dovranno essere attivate azioni mirate al monitoraggio del riutilizzo dei dati resi disponibili dalle pubbliche amministrazioni. Per poter abilitare attività di sviluppo di applicazioni innovative, inoltre, dovrà essere garantito un adeguato livello di qualità dei dati con la disponibilità di un sistema di misurazione e di *assessment* basato sui pertinenti standard ISO.

L'uso di una semantica comune nello scambio dei dati è garanzia di "coerenza semantica" dei dati stessi. Inoltre, l'adozione di una semantica unica riferita ai dati di dettaglio, come rappresentati nel NDC, consente uno scambio di informazioni coerenti e rappresenta una garanzia di consistenza dei dati aggregati che ogni organizzazione pubblica come dati aperti (*Linked Open Data - LOD*).

In linea con i principi enunciati e in continuità con le azioni avviate con i Piani precedenti e alla luce delle novità normative e tecniche descritte, il presente Piano triennale mira ad assicurare maggiore efficacia all'attività amministrativa in tutti i processi che coinvolgono l'utilizzo dei dati, sia con riferimento alla condivisione dei dati tra pubbliche amministrazioni per finalità istituzionali, sia con riferimento al riutilizzo dei dati, anche per finalità commerciali, secondo il paradigma dei dati aperti.

Rispetto alle precedenti edizioni del Piano triennale, alcuni obiettivi e risultati attesi sono stati rimodulati in modo da creare una più chiara associazione tra obiettivo/risultato atteso e soggetto responsabile.

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

A tal proposito, si richiamano le funzioni di raccolta ed elaborazione dati attribuite dalla Legge n. 56 del 2014 alle Province e alle Città metropolitane, a servizio degli enti locali del territorio.

Le "Linee guida recanti regole tecniche per l'apertura dei dati e il riutilizzo dell'informazione del settore pubblico" (Linee guida *Open Data*, d'ora in avanti) forniscono elementi utili di *data governance* in relazione ad aspetti organizzativi che possano abilitare un processo di apertura ed interoperabilità dei dati efficiente ed efficace. Anche l'interoperabilità, garantita dalla adozione di una semantica unica, come descritto nelle Linee guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni, deve essere tenuta in conto nella *governance* dei dati.

Il processo di formazione e pubblicazione dei dati può seguire lo schema proposto nelle suddette Linee guida che si compone delle seguenti fasi:

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

Per attuare tale processo, ferma restando l'autonomia organizzativa delle attività di ciascuna amministrazione, è necessario definire una chiara *data governance* anche interna con l'individuazione

di ruoli e relative responsabilità e integrare le sue fasi sia verticalmente, rispetto ai processi interni già consolidati, che orizzontalmente rispetto alle necessità specifiche dell'Amministrazione. Un ruolo determinante è svolto dal RTD che, sulla base della Circolare n. 3 del 1° ottobre 2018 del Ministro per la Pubblica Amministrazione, può costituire un apposito Gruppo di lavoro come possibile struttura per il governo del processo di apertura dei dati, in cui, oltre ad un responsabile, siano coinvolti i referenti tematici che gestiscono e trattano dati nell'ambito delle singole unità organizzative. È importante, inoltre, garantire il raccordo e la consultazione con le altre figure coinvolte nel processo di digitalizzazione della Pubblica Amministrazione, quali il responsabile per la conservazione documentale, il responsabile per la prevenzione della corruzione e la trasparenza, il responsabile della protezione dei dati, il responsabile per la sicurezza.

L'attività di apertura e di pubblicazione dei dati, infine, può tracciata nel Piano triennale ICT di ciascuna amministrazione anche sulla base di una eventuale scala di priorità basata, per esempio, su un approccio di tipo *demand-driven* che tenga conto dell'impatto economico e sociale nonché del livello di interesse e delle necessità degli utilizzatori.

Analogamente, anche per le attività di messa a disposizione di *asset* semantici per garantire l'interoperabilità dei dati, si potrà prevedere un percorso di definizione di modalità di pubblicazione di ontologie, vocabolari controllati e schemi dati.

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](#)

Di seguito, con il termine amministrazione ci si riferisce ai soggetti destinatari, individuati nel par. 1.3, delle Linee guida *Open Data*.

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

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

- **Target 2024** - Documentazione nel Catalogo nazionale dei dati aperti di almeno 400 *dataset* dinamici
- **Target 2025** – Aumento di *dataset* aperti di tipo dinamico documentati nel Catalogo nazionale dei dati aperti per ogni amministrazione titolare:
 - Se l'amministrazione ha già pubblicato un numero di *dataset* <10, deve arrivare a un minimo di 10 *dataset* aperti di tipo dinamico pubblicati e documentati nel Catalogo
 - Se l'amministrazione ha già pubblicato un numero di *dataset* ≥ 10 deve aumentare del 25% rispetto al 2024 il numero di *dataset* aperti di tipo dinamico pubblicati e documentati nel Catalogo
- **Target 2026** - Aumento di *dataset* aperti di tipo dinamico pubblicati e documentati nel Catalogo nazionale dei dati aperti per ogni amministrazione titolare:
 - se l'amministrazione ha già pubblicato un numero di *dataset* <20, deve arrivare a un minimo di 20 *dataset* aperti di tipo dinamico pubblicati e documentati nel Catalogo;
 - se l'amministrazione ha già pubblicato un numero di *dataset* ≥ 20 deve aumentare del 50%, rispetto al 2024, il numero di *dataset* aperti di tipo dinamico pubblicati e documentati nel Catalogo

RA5.1.2 - Aumento del numero di dataset resi disponibili attraverso i servizi di rete di cui al framework creato con la Direttiva 2007/2/EC (INSPIRE) e relativi Regolamenti attuativi, con particolare riferimento ai dati di elevato valore di cui al Regolamento di esecuzione (UE) 2023/138

- **Target 2024** - Documentazione nel Repertorio nazionale dei dati territoriali (RNDT) e conseguente esposizione nel geoportale INSPIRE di almeno 2.500 dataset
- **Target 2025** - Aumento di *dataset* territoriali documentati su RNDT per ogni amministrazione titolare:
 - se l'amministrazione ha già pubblicato un numero di *dataset* <10, deve arrivare a un minimo di 10 *dataset* territoriali documentati su RNDT
 - se l'amministrazione ha già pubblicato un numero di *dataset* ≥ 10 deve aumentare del 15% rispetto al 2024 il numero di *dataset* territoriali documentati su RNDT
- **Target 2026** - Aumento di *dataset* territoriali documentati sul Repertorio nazionale dei dati territoriali (RNDT) per ogni amministrazione titolare:
 - se l'amministrazione ha già pubblicato un numero di *dataset* <20, deve arrivare a un minimo di 10 *dataset* territoriali documentati su RNDT
 - se l'amministrazione ha già pubblicato un numero di *dataset* ≥ 20 deve aumentare del 25% rispetto al 2024 il numero di *dataset* territoriali documentati su RNDT

Linee di azione istituzionali

RA5.1.1

- **Dicembre 2024** - Aggiornamento del Catalogo nazionale dei dati aperti - (AGID) - CAP5.01
- **Dicembre 2025** - Conclusione di 4 cicli di formazione e sulle politiche *open data* per il biennio 24-25 - (AGID) - CAP5.02

RA5.1.2

- **Maggio 2024** - Aggiornamento della guida operativa sui dati di elevato valore in vista dell'applicazione del Regolamento di esecuzione (UE) 2023/138, previa valutazione di opportunità e necessità - (AGID, Amministrazioni titolari dei dati di elevato valore) - CAP5.03

Linee di azione per le PA

RA5.1.1

Linee di azione vigenti

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

RA5.1.2

- **Da giugno 2024** - Le PA attuano le indicazioni sui dati di elevato valore presenti nel Regolamento di esecuzione (UE) 2023/138, nelle Linee guida *Open Data* nonché nella specifica guida operativa - CAP5.PA.04

Obiettivo 5.2 - Aumentare la qualità dei dati e dei metadati

RA5.2.1 - Aumento del numero di dataset con metadati di qualità conformi agli standard di riferimento europei e nazionali

- **Target 2024** - Documentazione di 22.000 *dataset* e servizi nel catalogo geodati.gov.it e di 55.000 *dataset* nel catalogo dati.gov.it
- **Target 2025** - Aumento del 15% del numero dei *dataset* documentati per ogni amministrazione rispetto al 2024
- **Target 2026** - Aumento del 30% del numero dei *dataset* documentati per ogni amministrazione rispetto al 2024

RA5.2.2 - Aumento del numero di dataset di tipo aperto resi disponibili dalle pubbliche amministrazioni e documentati nel portale dati.gov.it

- **Target 2024** - Documentazione di almeno 70.000 *dataset* nel catalogo dati.gov.it
- **Target 2025** - Aumento di *dataset* di tipo aperto documentati per ogni amministrazione titolare:
 - se l'amministrazione ha già pubblicato un numero di *dataset* <10, deve arrivare a un minimo di 10 *dataset* documentati
 - se l'amministrazione ha pubblicato un numero di *dataset* ≥ 10 deve aumentare del 20% rispetto al 2024 il numero di *dataset* documentati

- **Target 2026** - Aumento di dataset di tipo aperto documentati per ogni amministrazione titolare:
 - se l'amministrazione ha pubblicato un numero di *dataset* <20, deve arrivare a un minimo di 20 *dataset* documentati
 - se l'amministrazione ha pubblicato un numero di *dataset* ≥ 20 deve aumentare del 30% rispetto al 2024 il numero di *dataset* documentati

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

- **Target 2024** - Tutte le PA hanno pubblicato il numero minimo di *dataset* riportato nelle linee d'azione per l'anno 2024
- **Target 2025** - Tutte le PA hanno pubblicato il numero minimo di *dataset* riportato nelle linee d'azione per l'anno 2025
- **Target 2026** - Tutte le PA hanno pubblicato il numero minimo di *dataset* riportato nelle linee d'azione per l'anno 2026

RA5.2.4 - Aumento del numero di dataset documentati sul portale dati.gov.it che rispettano la caratteristica di qualità "attualità" (o tempestività di aggiornamento) di cui allo Standard ISO/IEC 25012

- **Target 2024** - Definizione baseline
- **Target 2025** - Almeno il 30% dei dati documentati nel portale per ciascuna PA
- **Target 2026** - Almeno il 50% dei dati documentati nel portale per ciascuna PA

Linee di azione istituzionali

RA5.2.1

- **Giugno 2024** - Aggiornamento dei profili metadati per adeguamento alle indicazioni del Regolamento di esecuzione (UE) sui dati di elevato valore, alle Linee guida sui dati aperti e alle indicazioni derivanti da iniziative europee di allineamento - (AGID) - CAP5.04
- **Dicembre 2024** - Completamento del IV ciclo di formazione e sensibilizzazione alle PA titolari di dati aperti e/o di dati territoriali per le attività relative alla implementazione delle Linee guida sui dati aperti e il riutilizzo dell'informazione del settore pubblico e del Regolamento di esecuzione (UE) sui dati di elevato valore - (AGID) - CAP5.05

RA5.2.2

- **Ottobre 2024** - Predisposizione di un documento che raccolga in modo coerente le cornici normative, il posizionamento delle piattaforme locali, nazionali e sovranazionali e i punti di contatto che riguardano i dati - (AGID, Dipartimento per la Trasformazione Digitale) - CAP5.06
- **Dicembre 2024** – Conclusione primo rilevamento dei dati di elevato valore documentati nei cataloghi nazionali come da indicazioni sulla reportistica del Regolamento di esecuzione (UE) e pubblicazione report - (AGID) - CAP5.07
- **Dicembre 2025** - Completamento del V ciclo di formazione e sensibilizzazione alle PA titolari di dati aperti e/o di dati territoriali per le attività relative alla implementazione delle Linee Guida sui dati aperti e il riutilizzo dell'informazione del settore pubblico e del Regolamento di esecuzione (UE) sui dati di elevato valore - (AGID) - CAP5.08
- **Dicembre 2025** – Rilevamento annuale dei dati di elevato valore documentati nei cataloghi nazionali come da indicazioni sulla reportistica del Regolamento di esecuzione (UE) e pubblicazione report - (AGID) - CAP5.09

- **Dicembre 2026** - Completamento del VI ciclo di formazione e sensibilizzazione alle PA titolari di dati aperti e/o di dati territoriali per le attività relative alla implementazione delle Linee guida sui dati aperti e il riutilizzo dell'informazione del settore pubblico e del Regolamento di esecuzione (UE) sui dati di elevato valore - (AGID) - CAP5.10
- **Dicembre 2026** - Rilevamento annuale dei dati di elevato valore documentati nei cataloghi nazionali come da indicazioni sulla reportistica del Regolamento di esecuzione (UE) e pubblicazione report - (AGID) - CAP5.11

Linee di azione per le PA

RA5.2.1

- **Da giugno 2024** - Le PA pubblicano i metadati relativi ai dati di elevato valore, secondo le indicazioni presenti nel Regolamento di esecuzione (UE) e nelle Linee guida sui dati aperti e relativa guida operativa, nei cataloghi nazionali dati.gov.it e geodati.gov.it - CAP5.PA.05

RA5.2.3

- **Dicembre 2024** - Ogni Comune con popolazione tra 10.000 e 100.000 abitanti, ogni Unione di Comuni o altri tipi di consorzi e associazioni, ogni Comunità Montana o isolana pubblica (non ancora presenti nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 3 *dataset* - CAP5.PA.06
- **Dicembre 2024** - Ogni Comune con popolazione tra 100.001 e 250.000 abitanti, ogni Provincia e Città Metropolitana (non ancora presenti nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 5 *dataset* - CAP5.PA.07
- **Dicembre 2024** - Ogni Comune con popolazione > 250.000 abitanti, ogni Regione ed ogni altro ente territoriale regionale, ogni Università, Ente e centro di ricerca (non ancora presenti nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 10 *dataset* - CAP5.PA.08
- **Dicembre 2024** - Ogni PA centrale (non ancora presente nel catalogo dati.gov.it) pubblica e documenta nel catalogo almeno 15 *dataset* - CAP5.PA.09
- **Dicembre 2025** - Ogni Comune con popolazione tra 5.000 e 10.000 abitanti (non ancora presente nel 2024 nel catalogo dati.gov.it) pubblica e documenta nel catalogo almeno 1 *dataset* - CAP5.PA.10
- **Dicembre 2025** - Ogni Comune con popolazione tra 10.000 e 100.000 abitanti, ogni Unione di Comuni o altri tipi di consorzi e associazioni, ogni Comunità Montana o isolana pubblica (non ancora presenti nel 2024 nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 5 *dataset* - CAP5.PA.11
- **Dicembre 2025** - Ogni Comune con popolazione tra 100.001 e 250.000 abitanti, ogni Provincia e Città Metropolitana (non ancora presenti nel 2024 nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 10 *dataset* - CAP5.PA.12
- **Dicembre 2025** - Ogni Comune con popolazione > 250.000 abitanti, ogni Regione ed ogni altro ente territoriale regionale, ogni Università, Ente e centro di ricerca (non ancora presenti nel 2024 nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 15 *dataset* - CAP5.PA.13
- **Dicembre 2025** - Ogni PA centrale (non ancora presente nel 2024 nel catalogo dati.gov.it) pubblica e documenta nel catalogo almeno 30 *dataset* - CAP5.PA.14
- **Dicembre 2026** - Ogni Comune con popolazione tra 5.000 e 10.000 abitanti (non ancora presente nel 2024 nel catalogo dati.gov.it) pubblica e documenta nel catalogo almeno 3 *dataset* - CAP5.PA.15

- **Dicembre 2026** - Ogni Comune con popolazione tra 10.000 e 100.000 abitanti, ogni Unione di Comuni o altri tipi di consorzi e associazioni, ogni Comunità Montana o isolana pubblica (non ancora presenti nel 2024 nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 10 *dataset* - CAP5.PA.16
- **Dicembre 2026** - Ogni Comune con popolazione tra 100.001 e 250.000 abitanti, ogni Provincia e Città Metropolitana (non ancora presenti nel 2024 nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 15 *dataset* - CAP5.PA.17
- **Dicembre 2026** - Ogni Comune con popolazione > 250.000 abitanti, ogni Regione ed ogni altro ente territoriale regionale, ogni Università, Ente e centro di ricerca (non ancora presenti nel 2024 nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 30 *dataset* - CAP5.PA.18
- **Dicembre 2026** - Ogni PA centrale (non ancora presente nel 2024 nel catalogo dati.gov.it) pubblica e documenta nel catalogo almeno 45 *dataset* - CAP5.PA.19

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

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

- **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

Linee di azione istituzionali

RA5.3.1

- **Dicembre 2024** - Ciclo di formazione e sensibilizzazione alle PA titolari di dati aperti e/o di dati territoriali dedicato alle licenze e condizioni d'uso applicabili ai dati, sulla base delle relative indicazioni presenti nelle Linee Guida e nel Regolamento di esecuzione (UE) sui dati di elevato valore - (AGID) - CAP5.12
- **Dicembre 2025** - Produzione di linee guida e guide operative sulla governance dei dati - (AGID, ISTAT) - CAP5.13

Linee di azione per le PA

RA5.3.1

- **Da gennaio 2024** - Le PA attuano le linee guida contenenti regole tecniche per l'implementazione del Decreto Legislativo n. 36/2006 relativamente ai requisiti e alle raccomandazioni su licenze e condizioni d'uso - CAP5.PA.20

Intelligenza artificiale per la Pubblica Amministrazione

Scenario

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

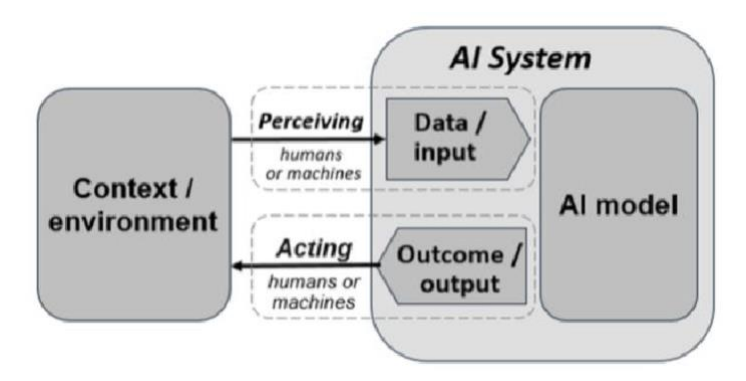


Figura 3 - Sistema di intelligenza artificiale (Fonte OECD)

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

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

L'Unione Europea mira a diventare *leader* strategico nell'impiego dell'intelligenza artificiale nel settore pubblico. Questa intenzione è chiaramente espressa nella Comunicazione "Piano Coordinato sull'Intelligenza Artificiale" COM (2021) 205 del 21 aprile 2021 in cui la Commissione europea propone specificamente di "rendere il settore pubblico un pioniere nell'uso dell'IA".

La revisione del Piano sull'intelligenza artificiale è stata accompagnata dalla "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. La proposta di regolamento mira ad affrontare i rischi legati all'utilizzo dell'IA, classificandoli in quattro diversi livelli: rischio inaccettabile (divieto), rischio elevato, rischio limitato e rischio minimo. Inoltre, il regolamento intende porre le basi per costruire un ecosistema di eccellenza nell'IA e rafforzare la capacità dell'Unione Europea di competere a livello globale.

L'AI Act ha introdotto una importante sfida in materia di normazione tecnica. La Commissione Europea ha adottato il 25 maggio 2023 la Decisione C(2023)3215 - *Standardisation request M/5932* con la quale ha affidato agli Enti di normazione europei CEN e CENELEC la redazione di norme tecniche europee a vantaggio dei sistemi di intelligenza artificiale in conformità con i principi dell'AI Act.

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

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

La Pubblica Amministrazione italiana conta esperienze rilevanti nello sviluppo e utilizzo di soluzioni di intelligenza artificiale. A titolo esemplificativo si citano le esperienze di:

- **Agenzia delle entrate**, utilizzo di algoritmi di *machine learning* per analizzare schemi e comportamenti sospetti, aiutando nella prevenzione e rilevazione di frodi;
- **INPS**, adozione di *chatbot* per semplificare e personalizzare l'interazione con l'utente, migliorando l'accessibilità e l'usabilità dei servizi;
- **ISTAT**, utilizzo di *foundation models* per generare ontologie a partire dalla descrizione in linguaggio naturale del contesto semantico al fine di migliorare la qualità della modellazione dei dati.

In questo contesto, l'affermarsi dei *foundation models* costituisce un importante fattore di accelerazione per lo sviluppo e l'adozione di soluzioni di intelligenza artificiale. Per *foundation models* si intendono sistemi di grandi dimensioni in grado di svolgere un'ampia gamma di compiti specifici, come la generazione di video, testi, immagini, la conversazione in linguaggio naturale, l'elaborazione o la generazione di codice informatico. L'*AI Act* definisce inoltre come *foundation models* “ad alto impatto” i modelli addestrati con una grande quantità di dati e con complessità, capacità e prestazioni elevate.

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

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

1. **Miglioramento dei servizi e riduzione dei costi.** Le pubbliche amministrazioni concentrano l'investimento in tecnologie di intelligenza artificiale nell'automazione dei compiti ripetitivi connessi ai servizi istituzionali obbligatori e al funzionamento dell'apparato amministrativo. Il conseguente recupero di risorse è destinato al miglioramento della qualità dei servizi anche mediante meccanismi di proattività.
2. **Analisi del rischio.** Le amministrazioni pubbliche analizzano i rischi associati all'impiego di sistemi di intelligenza artificiale per assicurare che tali sistemi non provochino violazioni dei diritti fondamentali della persona o altri danni rilevanti. Le pubbliche amministrazioni adottano la classificazione dei sistemi di IA secondo le categorie di rischio definite dall'*AI Act*.
3. **Trasparenza, responsabilità e informazione.** Le pubbliche amministrazioni pongono particolare attenzione alla trasparenza e alla interpretabilità dei modelli di intelligenza artificiale al fine di garantire la responsabilità e rendere conto delle decisioni adottate con il

supporto di tecnologie di intelligenza artificiale. Le amministrazioni pubbliche forniscono informazioni adeguate agli utenti al fine di consentire loro di prendere decisioni informate riguardo all'utilizzo dei servizi che sfruttano l'intelligenza artificiale.

4. **Inclusività e accessibilità.** Le pubbliche amministrazioni sono consapevoli delle responsabilità e delle implicazioni etiche associate all'uso delle tecnologie di intelligenza artificiale. Le pubbliche amministrazioni assicurano che le tecnologie utilizzate rispettino i principi di equità, trasparenza e non discriminazione.
5. **Privacy e sicurezza.** Le pubbliche amministrazioni adottano elevati standard di sicurezza e protezione della *privacy* per garantire che i dati dei cittadini siano gestiti in modo sicuro e responsabile. In particolare, le amministrazioni garantiscono la conformità dei propri sistemi di IA con la normativa vigente in materia di protezione dei dati personali e di sicurezza cibernetica.
6. **Formazione e sviluppo delle competenze.** Le pubbliche amministrazioni investono nella formazione e nello sviluppo delle competenze necessarie per gestire e applicare l'intelligenza artificiale in modo efficace nell'ambito dei servizi pubblici. A tale proposito si faccia riferimento agli obiettivi individuati nel Capitolo 1.
7. **Standardizzazione.** Le pubbliche amministrazioni tengono in considerazione, durante le fasi di sviluppo o acquisizione di soluzioni basate sull'intelligenza artificiale, le attività di normazione tecnica in corso a livello internazionale e a livello europeo da CEN e CENELEC con particolare riferimento ai requisiti definiti dall'*AI Act*.
8. **Sostenibilità:** Le pubbliche amministrazioni valutano attentamente gli impatti ambientali ed energetici legati all'adozione di tecnologie di intelligenza artificiale e adottando soluzioni sostenibili dal punto di vista ambientale.
9. **Foundation Models (Sistemi IA "ad alto impatto").** Le pubbliche amministrazioni, prima di adottare *foundation models* "ad alto impatto", si assicurano che essi adottino adeguate misure di trasparenza che chiariscono l'attribuzione delle responsabilità e dei ruoli, in particolare dei fornitori e degli utenti del sistema di IA.
10. **Dati.** Le pubbliche amministrazioni, che acquistano servizi di intelligenza artificiale tramite API, valutano con attenzione le modalità e le condizioni con le quali il fornitore del servizio gestisce i dati forniti dall'amministrazione con particolare riferimento alla proprietà dei dati e alla conformità con la normativa vigente in materia di protezione dei dati e *privacy*.

Dati per l'intelligenza artificiale

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

La Strategia Europea per i dati è implementata dal punto normativo dagli atti sopra citati che costituiscono il quadro regolatorio entro il quale deve muoversi una Pubblica Amministrazione che intende operare con sistemi di IA sui dati aperti.

Riguardo l'utilizzo dei dati da parte di sistemi di intelligenza artificiale, l'*AI Act* richiede ai fornitori di sistemi di IA di adottare una governance dei dati e appropriate procedure di gestione dei dati (con particolare attenzione alla generazione e alla raccolta dei dati, alle operazioni di preparazione dei dati, alle scelte di progettazione e alle procedure per individuare e affrontare le distorsioni e le potenziali distorsioni per correlazione o qualsiasi altra carenza pertinente nei dati). L'*AI Act* pone particolare

attenzione agli aspetti qualitativi dei set di dati utilizzati per addestrare, convalidare e testare i sistemi di IA (tra cui rappresentatività, pertinenza, completezza e correttezza). La Commissione Europea ha avviato una specifica attività presso il CEN e il CENELEC per definire norme tecniche europee per rispondere a tali esigenze.

Nel contesto nazionale, tenuto conto di una architettura istituzionale che organizza i territori in regioni e comuni, che devono avere livelli di servizio omogenei, diventa cruciale progettare e implementare soluzioni nazionali basate sull'IA. Queste soluzioni devono essere in grado, da un lato, di superare eventuali disparità che caratterizzano le diverse amministrazioni territoriali e, dall'altro, di assicurare un pieno coordinamento tra territori differenti riguardo a servizi chiave per la società.

Riguardo l'affermarsi dei *foundation models* nel settore pubblico, una sfida fondamentale consiste nella creazione di dataset di elevata qualità, rappresentativi della realtà della Pubblica Amministrazione, con particolare riguardo al corpus normativo nazionale e comunitario, ai procedimenti amministrativi e alla struttura organizzativa della Pubblica Amministrazione italiana stessa.

Contesto normativo 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

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

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

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 5.5 - Dati per l'intelligenza artificiale

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

Linee di azione istituzionali

RA5.4.1

- **Dicembre 2024** - Redazione Linee guida per promuovere l'adozione dell'IA nella Pubblica Amministrazione - (AGID) - CAP5.14

RA5.4.2

- **Dicembre 2024** - Redazione Linee guida per il *procurement* di IA nella Pubblica Amministrazione - (AGID) - CAP5.15

RA5.4.3

- **Dicembre 2024** - Redazione Linee guida per lo sviluppo di applicazioni di IA nella Pubblica Amministrazione - (AGID) - CAP5.16

RA5.4.4

- **Dicembre 2024** - Identificazione delle soluzioni nazionali fondate sull'IA - (AGID) - CAP5.17
- **Dicembre 2025** - Coordinamento delle attività di sviluppo delle soluzioni nazionali - (AGID) - CAP5.18

RA5.5.1

- **Dicembre 2024** - Identificazione delle basi di dati nazionali strategiche - (AGID) - CAP5.19
- **Dicembre 2025** - Coordinamento delle attività di digitalizzazione delle basi di dati nazionali strategiche - (AGID) - CAP5.20

Linee di azione per le PA

RA5.4.1

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

RA5.4.2

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

RA5.4.3

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

RA5.4.4

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

RA5.5.1

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

Strumenti per l'attuazione del Piano

OB5.3

- [Guida Operativa sulle serie di dati di elevato valore](#)
- [Guide operative RNDT](#)
- [Guida operativa GeoDCAT-AP](#)
- [Portale nazionale dei dati aperti dati.gov.it](#)
 - [Validatore semantico](#)
 - [SPARQL endpoint](#)
 - [Configuratore metadati](#)
- [Repertorio Nazionale dei Dati Territoriali](#) geodati.gov.it
 - Editor
 - Validatore
 - Uploader di file di metadati
 - Gestione cataloghi locali
- [Geoportale INSPIRE](#)
 - [Validatore INSPIRE](#)
- [Portale data.europa.eu](#)
- Catalogo Nazionale per l'interoperabilità semantica dei dati schema.gov.it
 - Validatore semantico
 - SPARQL endpoint
 - Visualizzatore di ontologie e vocabolari per il *repository semantic*

OB5.4

- Guida alle pubbliche amministrazioni per l'implementazione di "Smart Area" (vedi Parte terza
- Strumento 4)

Risorse e fonti di finanziamento

OB5.3

- Risorse proprie delle PA considerando la clausola di invarianza finanziaria presente nel D. Lgs. 36/2006 e s.m.i. di recepimento della Direttiva (UE) 2019/1024 (*Open Data*)
- [Intervento PNRR M2C4M1 I.1.1 "Realizzazione di un sistema avanzato ed integrato di monitoraggio e previsione" \(SIM\)](#) - per dati territoriali e ambientali, compresi i *dataset* di elevato valore
- [PNRR Misura Dati e interoperabilità](#)

Dati aperti e intelligenza artificiale nell'INFN

L'Istituto gestisce dataset di carattere amministrativo che non sono stati finora ritenuti di interesse per il riutilizzo da parte di cittadini e imprese, ma ne monitora l'evoluzione e, nel caso si presenti la necessità, prevede di renderli disponibili come open data coerenti con il modello di interoperabilità. A questo scopo, ritiene necessario pianificare la partecipazione ai corsi sulle politiche Open Data previsti dal piano per il 2025. L'Istituto è tuttavia coinvolto in progetti di open data riguardanti il proprio obiettivo primario, aderendo agli assi di intervento codificati dal Piano Nazionale per la Scienza Aperta. A tale scopo, ha emanato il Disciplinare per l'accesso aperto ai prodotti della ricerca dell'Istituto Nazionale di Fisica Nucleare e ha istituito un apposito archivio istituzionale.

In qualità di ente di ricerca, l'INFN ha esperienza di lungo periodo nell'uso e nello sviluppo sia di algoritmi di *machine learning*, oggi largamente utilizzati nell'analisi dei dati sperimentali, che nello studio di modelli di funzionamento di reti neurali per simulare il funzionamento del cervello. Tale attività è rimasta tuttavia a lungo correlata solamente alla ricerca. Nel corso del 2023-2024, sono cominciate sperimentazioni sull'uso di librerie *open source* per coadiuvare gli esperti del calcolo nel supporto all'utenza, utilizzando nodi di calcolo sulla *cloud* interna. In particolare, una prima sperimentazione ha coinvolto un servizio di *ticketing* tramite *e-mail* nel quale l'IA produce bozze di messaggi di risposta, poi revisionate dagli esperti prima dell'invio, ma con enorme risparmio di tempo. La cura adeguata deve essere messa nella trasparenza dell'informazione e nel rispetto della *privacy*.

La Direzione Sistemi informativi continuerà nel 2024-2025 la sperimentazione di *chat* automatiche, sempre basati su librerie *open source* e su risorse di calcolo *on premises*, per supportare gli utenti dei propri prodotti software.

Nel corso del 2024 è avviata una sperimentazione di uso di prodotti commerciali volti alla gestione ed alla analisi di documentazione scientifica ed amministrativa ed alla produttività di ufficio.

Queste attività, tutte basate su *foundation models*, sono volte a migliorare i servizi e ridurre i costi di gestione, riducendo i tempi necessari alla produzione di documentazione ed al supporto. Necessitano tuttavia di attenzione nel regolare l'accesso ai dati dell'utenza.

Siamo pertanto fortemente interessati alle linee guide che saranno via via diffuse da AgID su

uso e governance di tali prodotti e prevediamo per il 2025 di utilizzarli per la produzione di linee guida interne per:

- creare strumenti per l'analisi del rischio come modelli, linee guida e best practices;
- assicurare trasparenza, equità e non discriminazione nell'utilizzo dell'AI, fornendo informativa agli interessati;
- adottare elevati standard di sicurezza cibernetica e protezione della privacy, utilizzando per le attività di test ambienti certificati;
- definire un programma di formazione e sviluppo delle competenze necessarie per gestire e applicare i sistemi in favore del personale coinvolto;
- tenere in considerazione le attività di normazione tecnica in corso a livello internazionale e a livello europeo da CEN e CENELEC e standard ISO/IEC 20546.

Sarà inoltre necessario valutare la sostenibilità ambientale ed energetica e valutare gli eventuali acquisiti di sistemi di AI ispirandosi alle Standard Contractual Clauses predisposte dalla Commissione Europea, ma emanate nell'ambito della "Procurement of AI community", una delle community presenti nel sito della Commissione Europea (<https://public-buyers-community.ec.europa.eu/communities/procurement-ai>).

Capitolo 6 - Infrastrutture

Infrastrutture digitali e *Cloud*

Scenario

La strategia “*Cloud Italia*”, pubblicata a settembre 2021 dal Dipartimento per la Trasformazione Digitale e dall'Agenzia per la Cybersicurezza Nazionale nell'ambito del percorso attuativo definito dall'art.33-septies del Decreto-Legge n.179 del 2012 e gli investimenti del PNRR legati all'abilitazione *cloud* rappresentano una grande occasione per supportare la riorganizzazione strutturale e gestionale delle pubbliche amministrazioni.

Non si tratta di una operazione unicamente tecnologica, le cui opportunità vanno esplorate a fondo da ogni ente.

La Strategia *Cloud* risponde a tre sfide principali: assicurare l'autonomia tecnologica del Paese, garantire il controllo sui dati e aumentare la resilienza dei servizi digitali. In coerenza con gli obiettivi del PNRR, la strategia traccia un percorso per accompagnare le PA italiane nella migrazione dei dati e degli applicativi informatici verso un ambiente *cloud* sicuro.

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

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

L'adozione del paradigma *cloud* rappresenta, infatti, la chiave della trasformazione digitale abilitando una vera e propria rivoluzione del modo di pensare i processi di erogazione dei servizi della PA verso cittadini, professionisti ed imprese.

L'attuazione dell'art.33-septies del Decreto-legge n. 179 del 2012, non rappresenta solo un adempimento legislativo, ma è soprattutto una occasione perché ogni ente attivi gli opportuni processi di gestione interna con il fine di modernizzare i propri applicativi e al contempo migliorare la fruizione dei procedimenti, delle procedure e dei servizi erogati.

È anche quindi una grande occasione per:

- ridurre il debito tecnologico accumulato negli anni dalle amministrazioni;
- mitigare il rischio di *lock-in* verso i fornitori di sviluppo e manutenzione applicativa;
- ridurre significativamente i costi di manutenzione di centri elaborazione dati (*data center*) obsoleti e delle applicazioni *legacy*, valorizzando al contempo le infrastrutture digitali del Paese più all'avanguardia che stanno attuando il percorso di adeguamento rispetto ai requisiti del Regolamento AGID e relativi atti successivi dell'Agenzia per la Cybersicurezza Nazionale;
- Incrementare la postura di sicurezza delle infrastrutture pubbliche per proteggerci dai rischi *cyber*.

In tal modo, le infrastrutture digitali saranno più affidabili e sicure e la Pubblica Amministrazione potrà rispondere in maniera organizzata agli attacchi informatici, garantendo continuità e qualità nella fruizione di dati e servizi.

Nell'ambito dell'attuazione normativa della Strategia *Cloud* Italia e dell'articolo 33-septies del Decreto-Legge n.179/2021 è stata realizzato il Polo Strategico Nazionale (PSN), l'infrastruttura promossa dal Dipartimento per la Trasformazione Digitale che, insieme alle altre infrastrutture digitali qualificate e sicure, consente di fornire alle amministrazioni tutte le soluzioni tecnologiche adeguate e gli strumenti per realizzare il percorso di migrazione.

Il Regolamento attuativo dell'articolo 33-septies del Decreto-Legge n.179/2021 ha fissato al 28 febbraio 2023 il termine per la trasmissione dei piani di migrazione da parte delle amministrazioni.

Dopo la presentazione dei Piani di migrazione, le amministrazioni devono gestire al meglio il trasferimento in *cloud* di dati, servizi e applicativi. Una fase da condurre e concludere entro il 30 giugno 2026, avendo cura dei riferimenti tecnici e normativi necessari per completare una migrazione di successo.

Per realizzare al meglio il proprio piano di migrazione, le amministrazioni possono far riferimento al sito cloud.italia.it dove sono disponibili diversi strumenti a supporto, tra cui:

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

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

- come riconoscere e gestire possibili situazioni di *lock-in*;
- raccomandazioni sugli aspetti legati al *back up* dei dati e al *disaster recovery*;
- consigli sulla scelta della migliore strategia di migrazione dal *re-host* al *re-architect* in base alle caratteristiche degli applicativi da migrare;
- come migliorare la migrazione in *cloud* grazie a un approccio DevOps;
- come definire e separare correttamente i ruoli tra Unità di Controllo (chi governa il progetto di migrazione) e Unità di esecuzione (chi realizza la migrazione);
- come misurare costi/benefici derivanti dalla migrazione;
- come stabilire un perimetro di responsabilità condivise tra amministrazione utente e fornitore di servizi *cloud*;
- come sfruttare al massimo le opportunità del cloud grazie alle applicazioni *cloud* native, al *re-architect* e al *re-purchase*.

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

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

Altro aspetto da curare è quello dei costi operativi correnti. Con la migrazione al *cloud*, ci sono grandi opportunità di risparmio economico, ma occorre strutturarsi per una corretta gestione dei costi *cloud*, sia da un punto di vista contrattuale che tecnologico.

Inoltre, con il crescere di servizi digitali forniti ad uno stesso ente da una molteplicità di fornitori diversi, anche via *cloud*, cresce notevolmente la complessità della gestione del parco applicativo, rendendo difficile la concreta integrazione tra i *software* dell'ente, l'effettiva possibilità di interoperabilità verso altri enti, la corretta gestione dei dati, ecc. Questo richiede all'Ufficio RTD, in forma singola o associata, l'evoluzione verso nuove architetture a "micro-servizi".

Lo stesso concetto di "Sistema Pubblico di Connettività" (SPC), ancora presente nel CAD all'art.73, dovrà trovare una sua evoluzione basata sulla nuova logica cloud. Oggi è proprio il *cloud computing*, con la sua natura decentrata, policentrica e federata, a rendere possibile il disegno originario del SPC e salvaguardare pienamente l'autonomia degli enti, la neutralità tecnologica e la concorrenza sulle soluzioni ICT destinate alle PA.

Accanto agli aspetti di natura organizzativa è necessario porre attenzione anche ad una serie di elementi di natura più tecnologica.

Lo sviluppo delle infrastrutture digitali, infatti, è parte integrante della strategia di modernizzazione del settore pubblico: esse devono essere affidabili, sicure, energeticamente efficienti ed economicamente sostenibili e garantire l'erogazione di servizi essenziali per il Paese.

L'evoluzione tecnologica espone, tuttavia, i sistemi a nuovi e diversi rischi, anche con riguardo alla tutela dei dati personali. L'obiettivo di garantire una maggiore efficienza dei sistemi non può essere disgiunto dall'obiettivo di garantire contestualmente un elevato livello di sicurezza delle reti e dei sistemi informativi utilizzati dalla Pubblica Amministrazione.

Tuttavia, come già rilevato a suo tempo da AGID attraverso il Censimento del Patrimonio ICT della PA, molte infrastrutture della PA risultano prive dei requisiti di sicurezza e di affidabilità necessari e, inoltre, sono carenti sotto il profilo strutturale e organizzativo. Ciò espone il Paese a numerosi rischi, tra cui quello di interruzione o indisponibilità dei servizi e quello di attacchi *cyber*, con conseguente accesso illegittimo da parte di terzi a dati (o flussi di dati) particolarmente sensibili o perdita e alterazione degli stessi dati.

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

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

- con riferimento alla classificazione dei *data center* di cui alla Circolare AGID 1/2019 e ai fini della strategia di razionalizzazione dei *data center*, le categorie “infrastrutture candidabili ad essere utilizzate da parte dei PSN” e “Gruppo A” sono rinominate “A”;
- al fine di tutelare l'autonomia tecnologica del Paese, consolidare e mettere in sicurezza le infrastrutture digitali delle pubbliche amministrazioni di cui all'articolo 2, comma 2, lettere a) e c) del decreto legislativo 7 marzo 2005, n. 82, garantendo, al contempo, la qualità, la sicurezza, la scalabilità, l'efficienza energetica, la sostenibilità economica e la continuità operativa dei sistemi e dei servizi digitali, il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri promuove lo sviluppo di un'infrastruttura ad alta affidabilità localizzata sul territorio nazionale, anche detta Polo Strategico Nazionale (PSN), per la razionalizzazione e il consolidamento dei Centri per l'elaborazione delle informazioni (CED) destinata a tutte le pubbliche amministrazioni;
- le amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, nel rispetto dei principi di efficienza, efficacia ed economicità dell'azione amministrativa, migrano i loro Centri per l'elaborazione delle informazioni (CED) e i relativi sistemi informatici, privi dei requisiti fissati dalla Circolare AGID 1/2019 e, successivamente, dal regolamento di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179 (di seguito Regolamento *cloud* e infrastrutture), verso l'infrastruttura del PSN o verso altra infrastruttura propria già esistente e in possesso dei requisiti fissati dalla Circolare AGID 1/2019 e, successivamente, dal Regolamento *cloud* e infrastrutture. Le amministrazioni centrali, in alternativa, possono migrare i propri servizi verso soluzioni *cloud* qualificate, nel rispetto di quanto previsto dalle Circolari AGID n. 2 e n. 3 del 2018 e, successivamente, dal Regolamento *cloud* e infrastrutture;
- le amministrazioni locali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, nel rispetto dei principi di efficienza, efficacia ed economicità dell'azione amministrativa, migrano i loro Centri per l'elaborazione delle informazioni (CED) e i relativi sistemi informatici, privi dei requisiti fissati dalla Circolare AGID 1/2019 e, successivamente, dal regolamento *cloud* e infrastrutture, verso l'infrastruttura PSN o verso altra infrastruttura della PA già esistente in possesso dei requisiti fissati dallo stesso Regolamento *cloud* e infrastrutture. Le amministrazioni locali, in alternativa, possono migrare i propri servizi verso soluzioni *cloud* qualificate nel rispetto di quanto previsto dalle Circolari AGID n. 2 e n. 3 del 2018 e, successivamente, dal Regolamento *cloud* e infrastrutture;
- le amministrazioni non possono investire nella costruzione di nuovi *data center* per ridurre la frammentazione delle risorse e la proliferazione incontrollata di infrastrutture con conseguente moltiplicazione dei costi. È ammesso il consolidamento dei *data center* nel rispetto di quanto previsto dall'articolo 33-septies del Decreto-legge 179/2012 e dal Regolamento di cui al comma 4 del citato articolo 33-septies.

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

- i) la creazione del PSN, la cui gestione e controllo di indirizzo siano autonomi da fornitori extra UE, destinato ad ospitare sul territorio nazionale principalmente dati e servizi strategici la cui compromissione può avere un impatto sulla sicurezza nazionale, in linea con quanto previsto

in materia di perimetro di sicurezza nazionale cibernetica dal Decreto-legge 21 settembre 2019, n. 105 e dal DPCM 81/2021;

ii) un percorso di qualificazione dei fornitori di *cloud* pubblico e dei loro servizi per garantire che le caratteristiche e i livelli di servizio dichiarati siano in linea con i requisiti necessari di sicurezza, affidabilità e rispetto delle normative rilevanti e iii) lo sviluppo di una metodologia di classificazione dei dati e dei servizi gestiti dalle pubbliche amministrazioni, per permettere una migrazione di questi verso la soluzione *cloud* più opportuna (PSN o adeguata tipologia di *cloud* qualificato).

Con riferimento al punto i) creazione del PSN, a dicembre 2022, in coerenza con la relativa *milestone* PNRR associata, è stata realizzata e testata l'infrastruttura PSN. Si ricorda che tale infrastruttura eroga servizi professionali di migrazione verso l'infrastruttura PSN, servizi di *housing*, *hosting* e *cloud* nelle tipologie IaaS, PaaS.

Per maggiori informazioni sui servizi offerti da PSN si rimanda alla [convenzione pubblicata sul sito della Presidenza del Consiglio dei Ministri](#).

Nel 2023 sono stati pubblicati e conclusi tre avvisi per la migrazione verso il PSN a valere sulla misura 1.1 del PNRR che hanno visto l'adesione di oltre 300 tra amministrazioni centrali e aziende sanitarie locali e ospedaliere. Per quanto riguarda le ASL/AO, in particolare, è stata offerta l'opportunità di decidere la destinazione dei propri servizi tra PSN, Infrastrutture della PA adeguate e soluzioni *cloud* qualificate coerentemente con quanto disposto dall'articolo 33-septies del Decreto-legge 179/2012. 130 Aziende sanitarie hanno scelto di portare almeno parte dei propri servizi presso il PSN.

Con riferimento ai punti ii) qualificazione e iii) classificazione a dicembre 2021 sono stati pubblicati il Regolamento *cloud* e infrastrutture e a gennaio 2022 i relativi atti successivi. A febbraio e a luglio sono stati pubblicati ulteriori Decreti ACN ed è prevista la pubblicazione da parte di ACN di un nuovo Regolamento.

Con riferimento alla misura 1.2 del PNRR a marzo 2023 sono stati raccolti e ammessi a finanziamento più dei 12.464 piani di migrazione richiesti dal target è stato raggiunto e superato il target italiano previsto per settembre 2023 con la migrazione di oltre 1.100 enti locali che hanno migrato i loro servizi verso soluzioni *cloud* qualificate.

Con riferimento al tema del *cloud* federato, si premette che la definizione tecnica coerentemente con la ISO/IEC 22123-1:2023 è la seguente: "modello di erogazione di servizi *cloud* forniti da 2 o più *cloud service provider* che si uniscono mediante un accordo che preveda un insieme concordato di procedure, processi e regole comuni finalizzato all'erogazione di servizi *cloud*". Le amministrazioni con infrastrutture classificate "A" che hanno deciso di investire sui propri *data center* per valorizzare i propri asset ai fini della razionalizzazione dei centri elaborazione dati, adeguandoli secondo le modalità e i termini previsti ai requisiti di cui al Regolamento adottato ai sensi del comma 4 dell'articolo 33-septies del Decreto-legge 179/2012 e agli atti successivi di ACN, hanno la facoltà di valutare la possibilità di stringere accordi in tal senso per raggiungere maggiori livelli di affidabilità, sicurezza ed elasticità, purché siano rispettati i principi di efficacia ed efficienza dell'azione amministrativa e della normativa applicabile. Le amministrazioni che dovessero stipulare tali accordi

realizzerebbero così le infrastrutture *cloud* federate della PA che si affiancano all'infrastruttura Polo Strategico Nazionale nel rispetto dell'articolo 33-septies del decreto-legge 18 ottobre 2012, n. 179.

Per “infrastrutture di prossimità” (o *edge computing*) si intendono i nodi periferici (*edge nodes*), misurati come numero di nodi di calcolo con latenze inferiori a 20 millisecondi; si può trattare di un singolo *server* o di un altro insieme di risorse di calcolo connesse, operati nell'ambito di un'infrastruttura di *edge computing*, generalmente situati all'interno di un *edge data center* che opera all'estremità dell'infrastruttura, e quindi fisicamente più vicini agli utenti destinatari rispetto a un nodo *cloud* in un *data center* centralizzato”.

Le amministrazioni che intendono realizzare e/o utilizzare infrastrutture di prossimità verificano la conformità di queste ai requisiti del Regolamento di cui al comma 4 dell'articolo 33-septies del DL 179/2012.

Punti di attenzione e azioni essenziali per tutti gli enti

1) L'attuazione dell'art.33-septies Decreto-legge 179/2012, e del principio *cloud-first*, deve essere tra gli obiettivi prioritari dell'ente. Occorre curare da subito anche gli aspetti di sostenibilità 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 (OPEX) sia agli investimenti in conto capitale (CAPEX).

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

Approfondimento tecnologico per gli RTD

1) La piena abilitazione al *cloud* richiede l'evoluzione del parco applicativo *software* verso la logica *as a service* delle applicazioni esistenti, andando oltre il mero *lift-and-shift* dei server, progettando opportuni interventi di *rearchitect*, *replatform* o *repurchase* per poter sfruttare le possibilità offerte oggi dalle moderne piattaforme computazionali e dagli algoritmi di intelligenza artificiale. In tal senso, occorre muovere verso architetture a “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 \(Data Governance Act\) \(2020\)](#)

OB.6.1 - Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la strategia "Cloud Italia" e migrando verso infrastrutture e servizi *cloud* qualificati (incluso PSN)

RA6.1.1 - Numero di amministrazioni migrate

- **Target 2024** - 4.083 amministrazioni migrate con infrastrutture e servizi *cloud* qualificati/adeguati 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

Linee di azione istituzionali

RA6.1.1

- **Gennaio 2024** - Adozione del nuovo Regolamento di cui al comma 4 dell'articolo 33-septies del DL 179/2012 - (ACN) - CAP6.01
- **Giugno 2024** - Definizione delle modalità e i termini per la realizzazione del censimento dei Centri per l'elaborazione delle informazioni (CED) della Pubblica Amministrazione di cui al comma 1-ter dell'articolo 33-septies del DL 179/2012 - (AGID) - CAP6.02
- **Giugno 2024** - Definizione da parte di AGID e trasmissione a DTD e ACN di un piano di azione per l'avvio degli accertamenti di cui all'articolo 33-septies comma 4-quinquies del DL 179/2012 - (AGID, Dipartimento per la Trasformazione Digitale e ACN) - CAP6.03
- **Settembre 2024** - Predisposizione del documento riepilogativo dei risultati dei progetti di migrazione conclusi dalle amministrazioni in attuazione del PNRR - (Dipartimento per la Trasformazione Digitale) - CAP6.04

- **Giugno 2026** - Predisposizione del documento riepilogativo dei risultati dei progetti di migrazione conclusi dalle amministrazioni in attuazione del PNRR - (Dipartimento per la Trasformazione Digitale) - CAP6.05

Linee di azione per le PA

RA6.1.1

Linee di azione vigenti

- Le PA proprietarie di *data center* di gruppo B richiedono l'autorizzazione ad AGID per le spese in materia di *data center* nelle modalità stabilite dalla Circolare AGID 1/2019 e prevedono in tali contratti, qualora autorizzati, una durata massima coerente con i tempi strettamente necessari a completare il percorso di migrazione previsti nei propri piani di migrazione – CAP6.PA.01
- Le PA proprietarie di *data center* classificati da AGID nel gruppo A continuano a gestire e mantenere tali *data center* in coerenza con quanto previsto dalla Strategia *Cloud* Italia e dal Regolamento *cloud* – CAP6.PA.02
- Le PA avviano il percorso di migrazione verso il *cloud* in coerenza con quanto previsto dalla Strategia *Cloud* Italia – CAP6.PA.03
- Le PA continuano ad applicare il principio *cloud first* e ad acquisire servizi *cloud* solo se qualificati – CAP6.PA.04
- Le PA aggiornano l'elenco e la classificazione dei dati e dei servizi digitali in presenza di dati e servizi ulteriori rispetto a quelli già oggetto di conferimento e classificazione come indicato nel Regolamento e di conseguenza aggiornano, ove necessario, anche il piano di migrazione – CAP6.PA.05

Linee di azione 2024-2026

- **Da gennaio 2024** - Le PA, ove richiesto dal Dipartimento per la Trasformazione Digitale o da AGID, trasmettono le informazioni relative allo stato di avanzamento dell'implementazione dei piani di migrazione – CAP6.PA.06
- **Da gennaio 2024** - Le amministrazioni che intendono realizzare e/o utilizzare infrastrutture di prossimità verificano la conformità di queste ai requisiti del Regolamento di cui al comma 4 dell'articolo 33-septies del Decreto-legge 179/2012 e ne danno apposita comunicazione ad ACN – CAP6.PA.07
- **Gennaio 2024** - Le PA con *data center* di tipo "A" che hanno avviato gli adeguamenti sui propri *data center* ai requisiti di cui al Regolamento *cloud* e relativi atti successivi, trasmettono ad ACN la dichiarazione di cui al medesimo Regolamento – CAP6.PA.08
- **Settembre 2024** - 4.083 amministrazioni concludono la migrazione in coerenza con il piano di migrazione e, ove richiesto dal Dipartimento per la Trasformazione Digitale o da AGID, trasmettono le informazioni necessarie per verificare il completamento della migrazione – CAP6.PA.09
- **Giugno 2026** - Le amministrazioni concludono la migrazione in coerenza con il piano di migrazione trasmesso ai sensi del Regolamento *cloud* e, ove richiesto dal Dipartimento per la Trasformazione Digitale o da AGID, trasmettono le informazioni necessarie per verificare il completamento della migrazione – CAP6.PA.10

Il sistema pubblico di connettività

Scenario

Il Sistema Pubblico di Connettività (SPC) garantisce alle Amministrazioni aderenti sia l'interscambio di informazioni in maniera riservata che la realizzazione della propria infrastruttura di comunicazione. A tale Sistema possono interconnettersi anche le reti regionali costituendo così una rete di comunicazione nazionale dedicato per l'interscambio di informazioni tra le pubbliche amministrazioni sia centrali che locali.

Per effetto della legge n. 87 del 3 luglio 2023, di conversione del Decreto-legge 10 maggio 2023, n. 51 la scadenza dell'attuale Contratto Quadro è stata prorogata al 31 dicembre 2024; entro questa data sarà reso disponibile alle Amministrazioni interessate il nuovo Contratto Quadro che prevederà oltre ai servizi di connettività anche i servizi di telefonia fissa come da informativa Consip del 13 Aprile 2023.

Il Sistema Pubblico di Connettività fornisce un insieme di servizi di rete che:

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

Contesto normativo 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](#)

Obiettivo 6.2 - Garantire alle amministrazioni la disponibilità della connettività SPC

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

Linee di azione istituzionali

RA6.2.1

- **Dicembre 2024** - Consip aggiudica la nuova gara di connettività SPC - (CONSIP) - CAP6.06

RA6.2.1

- **Da gennaio 2025** - Sulla base delle proprie esigenze, le pubbliche amministrazioni iniziano la fase di migrazione della loro infrastruttura di rete utilizzando i servizi resi disponibili dalla nuova gara di connettività SPC – CAP6.PA.11

Strumenti per l'attuazione del Piano

- Il [Manuale di abilitazione al Cloud](#) nell'ambito del Programma nazionale di abilitazione al *cloud*: si tratta di un Documento che accompagna le pubbliche amministrazioni - da un punto di vista tecnico - nel percorso che parte dall'identificazione degli applicativi da migrare in *cloud* fino ad arrivare alla valutazione degli indicatori di risultato a migrazione avvenuta.
- [Framework di lavoro](#) relativo al programma nazionale di abilitazione al *cloud* che descrive il modello organizzativo delle unità operative (unità di controllo, unità di esecuzione e centri di competenza) che eseguiranno il programma di abilitazione.
- [un Kit](#) relativo al programma nazionale di abilitazione al *cloud* che raccoglie metodologie, strumenti e buone pratiche e fornisce alle pubbliche amministrazioni indicazioni per elaborare una propria strategia di migrazione dei servizi verso il *cloud*.

Risorse e fonti di finanziamento

- Gare Strategiche ICT Consip (es. Accordo Quadro *Public Cloud IaaS/PaaS*) e altri strumenti Consip (MEPA e SDAPA) (vedi Parte III - Strumenti).
- Finanziamenti PNRR per un ammontare complessivo di 1,9 miliardi di euro:
 - “Investimento 1.1: Infrastrutture digitali” (PA Centrali, ASL e Aziende Ospedaliere)
 - “Investimento 1.2: Abilitazione e facilitazione migrazione al *cloud*” (Comuni, Scuole, ASL e Aziende Ospedaliere).

Infrastrutture cloud e connettività nell'INFN

L'INFN ha già dati e servizi centrali e gestionali ospitati su tecnologie *cloud*, per la maggior parte *on premises* (ed in questo caso ospitati in una infrastruttura di alta affidabilità a livello geografico), in alcuni casi sul *cloud* del fornitore. È stato avviato un percorso di valutazione interna per decidere se e cosa migrare su *cloud* esterna di quanto attualmente ospitato *on premises*; parallelamente è stato anche avviato un processo di valutazione presso una azienda di consulenza esterna.

L'attività di calcolo scientifico non è parte di questo piano, ma tutto lo sviluppo in questo settore è volto verso tecnologie *cloud*, sia per le nuove infrastrutture che per quelle esistenti che, ove necessario, verranno riconfigurate (CAP6.PA.03).

L'INFN sviluppa o acquista servizi secondo il principio *cloud first* da alcuni anni, orientandosi verso fornitori qualificati. In aggiunta, tutti i nuovi prodotti della Direzione Servizi Informativi che abbiano un minimo di complessità vengono sviluppati utilizzando una tecnologia a micro-servizi, seguendo le linee guida AgID per lo sviluppo di software sicuro ed implementando API di tipo REST per garantirne l'integrità (CAP6.PA.04).

L'INFN provvederà ad una revisione della classificazione di dati e servizi entro la fine del 2025.

(CAP6.PA.05)

In relazione alle linee di azione CAP6.PA.06, CAP6.PA.07, CAP6.PA.09 e CAP6.PA.10, l'INFN adotta le seguenti iniziative:

- Completamento del processo di *assessment* interno, definizione della strategia, identificazione delle azioni necessarie al mantenimento *on premises* di dati e servizi digitali INFN (2024)
- Implementazione delle azioni tecniche e dei processi individuati dall'*assessment* interno, eventuali certificazioni (03/2025)
- Aggiornamento delle informazioni comunicate ad AGID, ACN e DTD (06/2025)
- Individuazione di specifici servizi da migrare in modalita' SaaS, e conseguente attuazione (linea di azione gia' svolta e da ripetere ciclicamente con cadenza almeno annuale).

Riguardo la connettività, questa linea di azione non riguarda l'INFN in quanto per esigenze di ricerca INFN è connesso alla rete GARR (<https://www.garr.it>) con alte prestazioni e non ha convenienza ad accedere tramite altro provider.

Capitolo 7 - Sicurezza informatica

Sicurezza informatica

Scenario

L'evoluzione delle moderne tecnologie e la conseguente possibilità di ottimizzare lo svolgimento dei procedimenti amministrativi con l'obiettivo di rendere efficace, efficiente e più economica l'azione amministrativa, ha reso sempre più necessaria la "migrazione" verso il digitale che, però, al contempo, sta portando alla luce nuovi rischi, esponendo imprese e servizi pubblici a possibili attacchi *cyber*. In quest'ottica, la sicurezza e la resilienza delle reti e dei sistemi, su cui tali tecnologie poggiano, sono il baluardo necessario a garantire, nell'immediato, la sicurezza del Paese e, in prospettiva, lo sviluppo e il benessere dello Stato e dei cittadini.

La recente riforma dell'architettura nazionale *cyber*, attuata attraverso l'adozione del decreto-legge 14 giugno 2021, n. 82 che ha istituito l'Agenzia per la Cybersicurezza Nazionale (ACN), ha come obiettivo, tra gli altri, quello di sviluppare e rafforzare le capacità *cyber* nazionali, garantendo l'unicità istituzionale di indirizzo e azione, anche mediante la redazione e l'implementazione della Strategia nazionale di cybersicurezza, che considera cruciale, per il corretto "funzionamento" del sistema Paese, la sicurezza dell'ecosistema digitale alla base dei servizi erogati dalla Pubblica Amministrazione, con specifica attenzione ai beni ICT. Tali beni supportano le funzioni e i servizi essenziali dello Stato e, purtroppo, come dimostrano gli ultimi rapporti di settore, sono tra i bersagli preferiti degli attacchi *cyber*.

Per garantire lo sviluppo e il rafforzamento delle capacità *cyber* nazionali, con il Piano Nazionale di Ripresa e Resilienza e con i Fondi per l'attuazione e la gestione della Strategia nazionale di cybersicurezza sono state destinate significative risorse alla sicurezza cibernetica e alle misure tese a realizzare un percorso di miglioramento della postura di sicurezza del sistema Paese nel suo insieme e, in particolare, della Pubblica Amministrazione.

Gli obiettivi e i risultati attesi, definiti successivamente nel presente capitolo, sono in linea con specifici interventi realizzati dall'ACN in favore delle pubbliche amministrazioni per cui sono state individuate specifiche aree di miglioramento. In particolare, il riferimento è alla necessità di:

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

All'interno di questo contesto, AGID metterà a disposizione della Pubblica Amministrazione una serie di piattaforme e di servizi, che verranno erogati tramite il proprio CERT, finalizzati alla conoscenza e al contrasto dei rischi *cyber* legati al patrimonio ICT della PA (obiettivo 7.6)

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 \(direttiva NIS 2\) \(Testo rilevante ai fini del SEE\)](#)

Obiettivo 7.1 - Adottare una governance della cybersicurezza diffusa nella PA

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

- **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
- **Target 2026** - n.d.

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
- **Target 2026** - n.d.

Linee d'azione istituzionali

RA7.1.1

- **Giugno 2024** - L'Agenzia fornisce le Linee guida per l'identificazione di ruoli, competenze e organizzazione per la definizione di un modello di *governance* della cybersicurezza nella PA, comprensive delle linee di implementazione da parte delle PA - (ACN) - CAP7.01
- **Settembre 2024** - L'Agenzia promuove la creazione di un ruolo di Responsabile della Cybersicurezza della PA e i suoi compiti e responsabilità - (ACN) - CAP7.02

Linee di azione per le PA

RA7.1.1

- **Da settembre 2024** - Le singole PA definiscono il modello unitario, assicurando un coordinamento centralizzato a livello dell'istituzione, di *governance* della cybersicurezza - CAP7.PA.01
- **Da dicembre 2024** - Le PA adottano un modello di *governance* della cybersicurezza - CAP7.PA.02
- **Da dicembre 2024** - Le PA nominano i Responsabili della cybersicurezza e delle loro strutture organizzative di supporto - CAP7.PA.03

RA7.1.2

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

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

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 2025** - 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

Linee di azione istituzionali

RA7.2.1

- **Dicembre 2024** - L'Agenzia fornisce le Linee guida per la definizione dei requisiti di sicurezza nel processo di approvvigionamento IT - (ACN) - CAP7.03

RA7.2.2

- **Giugno 2025** - L'Agenzia fornisce le Linee guida per la realizzazione degli *audit* e delle verifiche di sicurezza sulle terze parti - (ACN) - CAP7.04

Linee di azione per le PA

RA7.2.1

- **Da giugno 2024** - Le PA definiscono e approvano i requisiti di sicurezza relativi al processo di approvvigionamento IT - CAP7.PA.05
- **Da dicembre 2024** - 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 - CAP7.PA.06

RA7.2.2

- **Da dicembre 2025** - Le PA realizzano le attività di controllo definite nel Piano di *audit* e verifica verso i fornitori e terze parti IT - CAP7.PA.07

Obiettivo 7.3 - Gestione e mitigazione del rischio cyber

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
- **Target 2026** - n.d.

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

- **Target 2024** - n.d.
- **Target 2025** - n.d.

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

Linee di azione istituzionali

RA7.3.1

- **Dicembre 2024** - L'Agenzia fornisce le Linee guida per la definizione dei processi di *cyber risk management* e *security by design* - (ACN) - CAP7.05

Linee di azione per le PA

RA7.3.1

- **Da dicembre 2024** - Le PA definiscono e formalizzano il processo di *cyber risk management* e *security by design*, coerentemente con gli strumenti messi a disposizione da ACN - CAP7.PA.08
- **Dicembre 2025** - Le PA promuovono il censimento dei dati e servizi della PA, identificandone la rilevanza e quindi le modalità per garantirne la continuità operativa - CAP7.PA.09
- **Dicembre 2025** - Le PA realizzano o acquisiscono gli strumenti atti alla messa in sicurezza dell'integrità, confidenzialità e disponibilità dei servizi e dei dati, come definito dalle relative procedure - CAP7.PA.10
- **Dicembre 2026** - 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 - CAP7.PA.11

RA7.3.2

- **Da dicembre 2025** - 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 - CAP7.PA.12

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

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
- **Target 2025** - n.d.
- **Target 2026** - n.d.

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

- **Target 2024** - n.d.
- **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

Linee d'azione istituzionali

RA7.4.1

- **Giugno 2024** - L'Agenzia fornisce le Linee guida per la definizione dei processi e delle procedure per la gestione degli incidenti di sicurezza - (ACN) - CAP7.06

Linee di azione per le PA

RA7.4.1

- **Da giugno 2024** - Le PA definiscono i presidi per la gestione degli eventi di sicurezza, formalizzandone i processi e le procedure - CAP7.PA.13
- **Da dicembre 2024** - Le PA formalizzano ruoli, responsabilità e processi, nonché le capacità tecnologiche a supporto della prevenzione e gestione degli incidenti informatici - CAP7.PA.14

RA7.4.2

- **Da dicembre 2024** - Le PA definiscono le modalità di verifica dei Piani di risposta a seguito di incidenti informatici - CAP7.PA.15
- **Da dicembre 2025** - Le PA definiscono le modalità di aggiornamento dei Piani di risposta e ripristino a seguito dell'accadimento di incidenti informatici - CAP7.PA.16

Obiettivo 7.5 - Implementare attività strutturate di sensibilizzazione cyber del personale

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
- **Target 2026** - n.d.

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

- **Target 2024** - n.d.
- **Target 2025** - n.d.
- **Target 2026** - Acquisire strumenti informatici a supporto dei programmi formativi

Linee di azione istituzionali

RA7.5.1

- **Giugno 2024** - L'Agenzia realizza contributi a supporto dello sviluppo della consapevolezza cyber nella PA - (ACN) - CAP7.07

Linee di azione per le PA

RA7.5.1

- **Da giugno 2024** - Le PA promuovono l'accesso e l'utilizzo di attività strutturate di sensibilizzazione e formazione in ambito cybersicurezza - CAP7.PA.17
- **Da dicembre 2024** - Le PA definiscono piani di formazione inerenti alla *cybersecurity*, diversificati per ruoli, posizioni organizzative e attività delle risorse dell'organizzazione - CAP7.PA.18

RA7.5.2

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

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

RA7.6.1 - 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

Linee di azione istituzionali

RA7.6.1

- **Gennaio 2024** - Monitoraggio proattivo delle minacce *cyber* nel dominio della PA, mediante la diffusione di Indicatori di Compromissione e informazioni utili all'innalzamento del livello di difesa - (AGID) - CAP7.08

RA7.6.2

- **Settembre 2024** - Messa a disposizione dei RTD di strumenti e supporto per le autovalutazioni dei sistemi esposti e per l'individuazione, l'analisi e la gestione dei rischi *cyber* - (AGID) - CAP7.09

RA7.6.3

- **Gennaio 2024** - Diffusione di notizie, dati statistici e tecnici sulle campagne malevole attive sul territorio nazionale attraverso il portale del CERT-AGID - (AGID) - CAP7.10
- **Marzo 2025** - Erogazione di un corso di formazione base sulla sicurezza nella PA - (AGID) - CAP7.11
- **Settembre 2025** - Erogazione di un corso di formazione avanzato sulla sicurezza nella PA - (AGID) - CAP7.12
- **Giugno 2026** - Consegna documentazione di supporto ai RTD per la parte riguardante i temi legati alla *cybersecurity* - (AGID) - CAP7.13

Linee di azione per le PA

RA7.6.1

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

RA7.6.2

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

RA7.6.3

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

Strumenti per l'attuazione del Piano

- Servizi *Cyber* nazionali già attivati e in fase di attivazione da parte di ACN. In particolare, si evidenziano i seguenti servizi:
 - *HyperSOC*: sistema nazionale di monitoraggio delle vulnerabilità e fattori di rischio per la *constituency* nazionale;
 - Portale Servizi Agenzia (ACN) e servizi informativi dello [CSIRT Italia](#): sistema nazionale di *infossharing* tecnico e operativo a supporto dell'identificazione, analisi e mitigazione di minacce e incidenti;
 - Servizi di gestione del rischio *cyber*: strumenti e sistemi a supporto dell'identificazione, analisi e valutazione del rischio *cyber*;
- Linee guida e contenuti informativi pubblicati di ACN;
- Piattaforma Syllabus per lo sviluppo di ulteriori competenze nella PA.

Risorse e fonti di finanziamento

- PNRR Missione 1 Componente 1 - Investimento 1.5 "Cybersecurity";
- Fondo per l'attuazione della Strategia nazionale di cybersicurezza, articolo 1, comma 899, lettera a), della legge 29 dicembre 2022 n. 197
- Fondo per la gestione della Strategia nazionale di cybersicurezza, articolo 1, comma 899, lettera b), della legge 29 dicembre 2022 n. 197

L'INFN e la sicurezza informatica

L'INFN ha cominciato fin dal febbraio 2023 ad elaborare un modello unitario di *governance* della cybersicurezza (CAP7.PA.01, CAP7.PA.02). Il modello adottato prevede la presenza di un responsabile nazionale che siede in CCR e coordina le attività del NUCS INFN (Nucleo CyberSicurezza) strutturato in gruppi di lavoro dedicati a funzioni operative e di R&D specifiche (CSIRT, SOC, vulnerability scan) e all'elaborazione di policy standard; il responsabile nazionale è coadiuvato da referenti locali (uno per ogni struttura) e lavora di concerto con altri gruppi specifici (Harmony, DPO, EPIC, RTD). Il responsabile nazionale è stato nominato ed è parte del gruppo di coordinamento dell'RTD, attivo dal 2021 (CAP7.PA.03).

È in corso la definizione formale di ruoli, responsabilità e processi di nomina di tutte le figure

coinvolte nella gestione della CS (responsabile nazionale, coordinatori dei gruppi di lavoro, referenti locali, ...).

È in programma l'analisi puntuale del Framework Nazionale per la Cybersecurity e la Data Protection in previsione della sua adozione come standard di gestione dei processi relativi alla cybersecurity. Nel corso del prossimo anno, in accordo con il piano AgID, verranno formalizzati i processi e le procedure inerenti alla gestione della cybersicurezza (CAP7.PA.04)

Per quanto riguarda gli approvvigionamenti, allo stato attuale facciamo riferimento solo alle Linee guida sulla sicurezza nel procurement ICT pubblicate da AGID – tutte le attività deve essere impostate. Al momento, è in corso una campagna di sensibilizzazione presso l'Amministrazione per rispettare i requisiti di sicurezza base nel *procurement* (CAP7.PA.05). Allo scopo di arrivare ad una pratica condivisa con tutte le strutture dell'ente, l'attività di auditing interno, già attiva da qualche anno con personale certificato sui temi della protezione dei dati personali e dello sviluppo sicuro, necessita di un quadro di riferimento per poter allargare le sue attività alla sfera amministrativa. È nostro obiettivo definire tale quadro di riferimento entro la fine del 2024, in modo da poter raggiungere gli obiettivi CAP7.PA.06 e CAP7.PA.07.

L'Ente ha formalizzato un piano di gestione del rischio informatico e lo ha adottato nel 2019 – detto piano deve essere revisionato ed eventualmente reso coerente con le prescrizioni di ACN e integrato con gli strumenti messi a disposizione da quest'ultima; vengono svolte periodicamente scansioni per la rilevazione di potenziali vulnerabilità riguardanti servizi esposti e sono in corso di acquisizione strumenti per migliorare la gestione del ciclo completo delle vulnerabilità (CAP7.PA.08).

I servizi essenziali dell'amministrazione, ove non migrati su cloud esterne, sono ospitati su una infrastruttura ad alta affidabilità (*Business Continuity*), con dati sincronizzati su due siti connessi a bassa latenza; un terzo sito ospita un sistema di *disaster recovery*. Questo dovrebbe garantire la continuità operativa dei servizi e l'integrità dei dati; per quanto riguarda la confidenzialità particolare attenzione è rivolta non solo allo sviluppo sicuro del software gestionale ed all'acquisto di software di qualità, ma anche alla formazione del personale attraverso i piani di formazione del NUCS INFN di cui più avanti ed i corsi di amministrazione digitale dell'UTD, che si orienteranno sempre più verso la sensibilizzazione alla importanza della accuratezza e della protezione del dato. Queste attività sono attualmente in corso (CAP7.PA.09, CAP7.PA.10), mentre sono in progettazione le attività CAP7.PA.11 e CAP7.PA.12.

L'attività di formazione in ambito cyber rientra pienamente nella missione del NUCS INFN ed è stata delineata per sommi capi in collaborazione con l'Ufficio Formazione dell'Ente; in particolare è iniziato un processo di raccolta e catalogazione di corsi e strumenti disponibili sui portali formativi a disposizione del personale dell'Ente in modo da delineare percorsi specifici dedicati all'utenza generica, al *management* e al personale professionalmente coinvolto nella gestione della sicurezza informatica; è prevista anche la realizzazione di campagne di miglioramento della consapevolezza focalizzate sul *phishing*.

L'Ente è già dotato di uno CSIRT (gestito da personale interno) nell'ambito delle attività istituzionali del quale sono state individuate le figure coinvolte e formalizzate le procedure da seguire nella gestione degli incidenti informatici. Lo CSIRT INFN è appena stato incluso nello *European Database of Cyber Security Teams* ed è iniziato un processo di adozione di standard operativi definiti e approvati dalla *Task Force CSIRT* di ENISA (FIRST CSIRT service framework, sim3 CSIRT maturity model, ...) (CAP7.PA.13). Sono in corso di definizione ruoli, responsabilità e processi, nonché le capacità tecnologiche a supporto della prevenzione e gestione degli incidenti informatici, previste come obiettivo del 2025 (CAP7.PA.14) e si

prevede nel 2025 di definire le verifiche dei piani di risposta a seguito di incidenti informatici (CAP7.PA.15).

L'Istituto è già abilitato alla ricezione degli IoC messi a disposizione da CERT-AGID (CAP7.PA.20), in alcune strutture se ne fa già uso in implementazioni sperimentali e di produzione di firewall DNS – è prevista la distribuzione centralizzata di questi IoC a tutte le strutture INFN e il loro utilizzo in piattaforme di malware sharing (MISP, attualmente in sperimentazione) e/o in eventuali altri strumenti messi a disposizione da CERT-AGID (CAP7.PA.21).

È in corso la valutazione dello strumento per il *risk assessment* elaborato da CERT-AGID e ACN in previsione della sua adozione come piattaforma di riferimento per l'Ente.

Si prevede di partecipare ai corsi di formazione base ed avanzato erogati dal CERT-AGID quando saranno disponibili (CAP7.PA.22).

Credits

L'edizione 2024 - 2026 del Piano triennale per l'informatica nella Pubblica Amministrazione è stata realizzata con i contributi di molte organizzazioni. Il processo di redazione è stato curato dal Servizio Piano Triennale di AGID. Ludovico Aniballi, Rosamaria Barrese, Stelio Pagnotta, Daniela Romano, Antonio Tappi e Fabio Massimi hanno lavorato alla stesura del documento finale.

La versione INFN è interamente basata sulla versione AGID ed è stata prodotta dal Comitato di Coordinamento del RTD. Ad ogni capitolo è stato aggiunto un paragrafo che descrive la postura dell'ente ed i piani relativi all'argomento del capitolo.

Ringraziamenti

Si ringrazia per la collaborazione alla stesura del Piano triennale per l'informatica nella Pubblica Amministrazione 2024 - 2026:

ANCI: Antonella Galdi, Moira Benelli, Mauro Savini

ACN: Tutta l'Agenzia, in particolare il Servizio programmi industriali, tecnologici di ricerca e formazione
Commissione per l'Innovazione Tecnologica e la Digitalizzazione della Conferenza delle Regioni e delle Province autonome: Giovanni Gentili, Benedetta Cerbini, Valeria Palazzari

Comune di Modena: Luca Salvatore, Ludovica Carla Ferrari

Consip: Marco Mizzau, Patrizia Bramini, Arianna Volpe

Consorzio CINI: Ernesto Damiani, Daniele Nardi, Piercosma Bisconti Lucidi

Dipartimento per la Funzione pubblica: Elio Gullo, Sauro Angeletti, Valentina Albano, Maria Laura Comito

Dipartimento per la trasformazione digitale: Rocco Affinito, Luca Artesi, Adriano Avenia, Gabriella Barone, Silvia Conticelli, Daniele De Bernardin, Vincenzo De Falco, Fabio Di Loreto, Sara Ghazanfari, Giuseppe Iacono, Matteo Fortini, Mariachiara Fortuna, Vincenzo Fortunato, Jiwon Lee, Mariangela Antonella Maselli, Nicola Mastropietro, Gandolfo Miserendino, Rosalia Moffa, Pietro Morandini, Elisabetta Oliveri, Marco Maria Pedrazzo, Alessandra Pepe, Luca Rigoni, Fabiana Rocchi, Fabrizio Salvatore, Francesco Sbordone, Raffaella Francesca Sisti, Emiliano Vernini

INAIL: Ester Rotoli, Francesco Saverio Colasuonno, Mariano Michele Bonaccorso

INPS: Massimiliano D'Angelo, Pierpaolo Bonanni, Vincenzo Di Nicola, Gioia Valeri

ISTAT: Massimo Fedeli, Emanuela Virardi, Sara Letardi, Roberta Radini

Istituto Poligrafico e della Zecca dello Stato: Stefano Imperatori, Antonio Gentile, Salvatore Grimaldi, Andrea Spallacci

MEF: Giuseppe Parise, Roberta Lotti

Osservatorio Agenda Digitale del Politecnico di Milano: Giuliano Noci, Michele Benedetti, Alfredo De Meo, Claudio Russo, Alessandra Thi Mandelli

PagoPa: Alessandro Moricca, Maurizio Fatarella, Alessio Biasutto, Patrizio Caligiuri, Francesco Capitanata, Raffaele Cesarano, Federica Ciampa, Gloriana Cimmino, Alessandro Conti, Giuseppe De Giorgi, Matteo De Santi, Ilaria Durante, Lorenzo Fredianelli, Riccardo Fusari, Giaime Gabrielli, Valeria Gesmundo, Elisa Mastrantonio, Stefano Menotti, Andrea Pasuch, Paola Pironi, Michelangelo Quaglia, Matteo Utzeri, Salvatore Valenza, Daniele Vecchia, Sara Villani

Unione Province d'Italia: Piero Antonelli, Gaetano Palombelli

Università di Modena e Reggio Emilia: Luca Chiantore, Francesco Leali, Marko Bertogna

Si ringraziano, per le idee fornite e per il tempo dedicato al confronto: il prof. Donato Limone, i Responsabili della transizione al digitale delle Regioni e delle Province autonome, delle Città metropolitane e dei loro Comuni capoluogo, CNR, Fondazione CRUI, ENEA, INFN, Ministero dell'Istruzione e del Merito, Ministero dell'università e della ricerca, Assintel, Assinter, Anitec-Assinform, Asstel, AIIP, Confindustria, Confartigianato, Unioncamere.

Si ringraziano inoltre: Sauro Del Turco, Fabrizio Donzella, Morena Ragone, Andrea Sammarco, Dimitri Tartari

Per AGID, hanno contribuito:

Gualtiero Asunis, Enrica Massella, Antonio Romano, Luca Ventura
Federico Abramo, Elena Alfonsi, Giovanni Amato, Alessandra Antolini, Luigi Avena, Roberto Bianca, Diana Bonofiglio, Claudio Celeghin, Mirko Cappuccia, Antonio Colella, Michela Collacchi, Marcello Cotta, Valentina De Grazia, Salvatore Di Gioia, Claudio Distefano, Mauro Draoli, Maria Luisa De Santis, Antonio Florio, Matteo Galassi, Francesco Grasso, Stefano Ianniello, Angelo La Venuta, Letizia Leo, Paola Liberace, Monica Manganiello, Emanuela Mariotti, Saverio Mastropierro, Giovanni Melardi, Maura Montironi, Daniela Pascale, Alfio Raia, Antonio Rotundo, Angela Scanu, Vincenzo Travascio, Stefano Van der Byl, Caterina Vignato

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.
- **Openness:** 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.

PARTE TERZA - Strumenti

Strumento 1 - Approvvigionamento ICT

Definire contratti coerenti con gli obiettivi del Piano triennale attraverso il Piano delle Gare strategiche Consip

Versione 1.0 del 21/12/2023

I. Obiettivo

Il documento fornisce indicazioni operative per la definizione di contratti di approvvigionamento ICT coerenti con gli obiettivi del Piano triennale attraverso gli strumenti di acquisto di Consip.

II. Destinatari

Tutte le pubbliche amministrazioni.

III. Crediti

Il documento è stato redatto in collaborazione con Consip.

1.1. GLI ACCORDI QUADRO CONSIP E GLI INDICATORI DI DIGITALIZZAZIONE

Le iniziative strategiche ICT sono realizzate attraverso appalti aggiudicati da Consip nella forma dell'Accordo quadro, che consentono a tutte le Amministrazioni di acquistare rapidamente i servizi necessari per attuare il percorso di transizione al digitale secondo il paradigma dell'ordine diretto, ove l'Amministrazione non abbia esigenze progettuali peculiari ovvero attraverso lo strumento dell'appalto specifico tra i fornitori selezionati da Consip, con garanzie di qualità e prezzi vantaggiosi.

In particolare, le Amministrazioni possono accedere, ad oggi, a un piano molto ricco di gare strategiche che nell'ultimo anno è stato ampliato con le seconde edizioni di alcune iniziative sulla base dell'andamento di adesione registrato per le prime edizioni (Figura 4).

Stato	Gare	Lotti	Massimale
Attive	14	60	Circa 10 miliardi
In corso di attivazione	4	29	Circa 3 miliardi
Totale	18	89	Circa 13 miliardi

Figura 4 - Stato del Piano delle gare strategiche

Le gare attive possono essere raggruppate, a loro volta, in macroaree di servizi e di seguito è mostrata la distribuzione dei massimali per ciascuna macroarea.

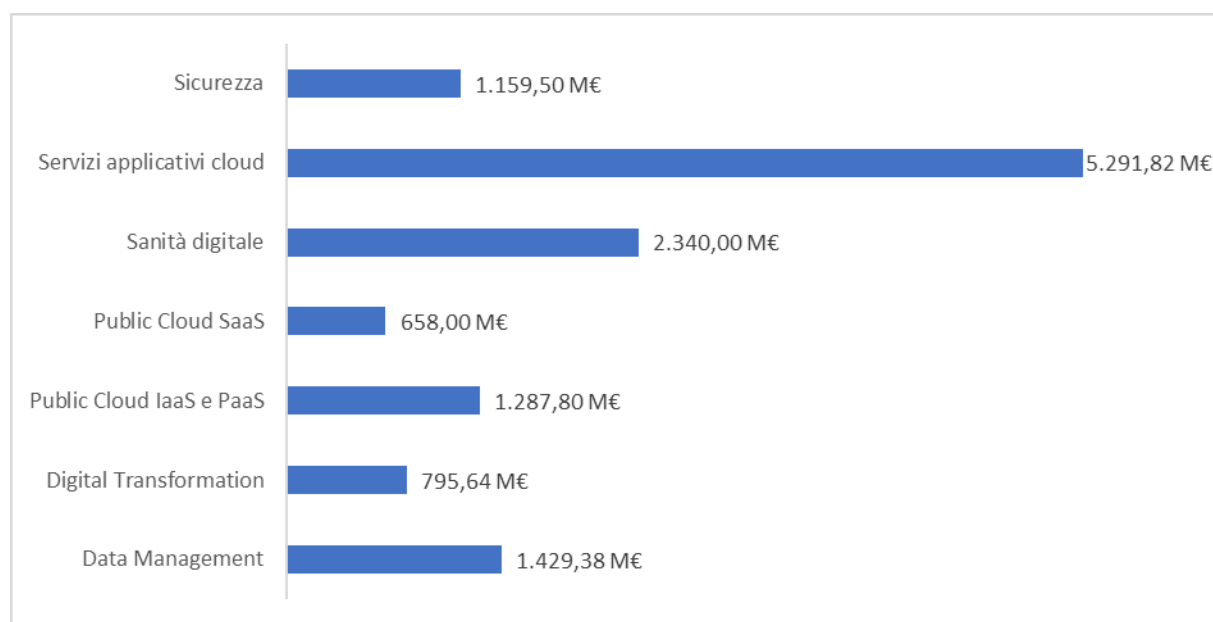


Figura 5- Distribuzione massimali per le macroaree di servizio

Come evidente, l'insieme delle gare strategiche fornisce, quindi, un set articolato di strumenti per supportare una Pubblica Amministrazione nel compiere il suo *Digital Journey*, ossia un percorso completo di attuazione di una trasformazione digitale a partire dalla definizione della strategia fino alla attuazione attraverso risorse infrastrutturali, di dati ed applicative (Figura 6).

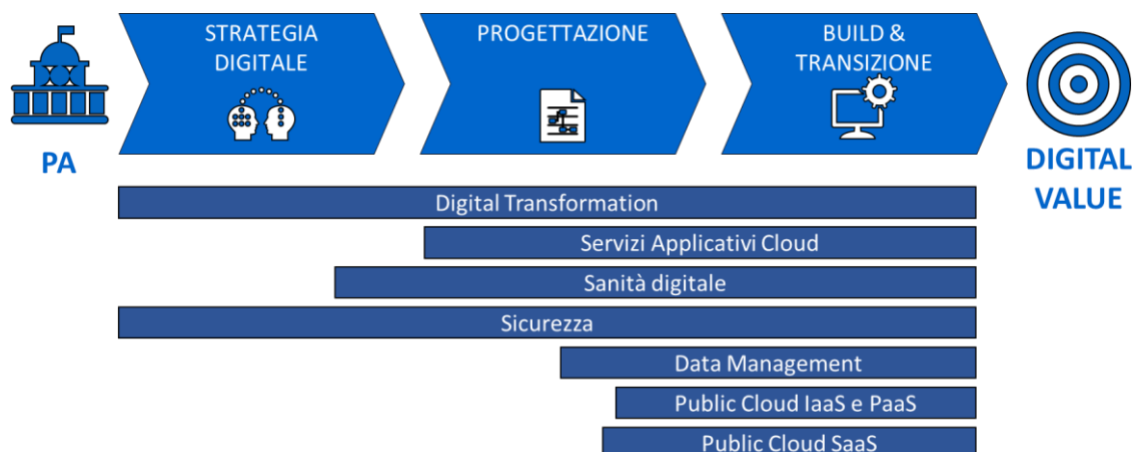


Figura 6- Cluster di progetti su più gare strategiche per un percorso digitale completo

Le attività di monitoraggio condotte da AGID hanno consentito l'individuazione, nell'ultimo anno, di più di 20 *Digital Journey* attraverso la stipula di più di 100 contratti esecutivi.

AGID, inoltre, attraverso i Comitati tecnici, previsti nell'ambito dei compiti di *governance* degli Organismi di coordinamento e controllo di cui fa parte, ha avviato delle azioni congiunte con gli aggiudicatari degli accordi quadro e con le amministrazioni contraenti, finalizzate alla rilevazione sempre più accurata di elementi indispensabili alla misurazione della crescita digitale del Paese.

Le Amministrazioni hanno, quindi, attraverso il piano delle gare strategiche, l'opportunità di definire contratti coerenti con gli obiettivi del Piano triennale attraverso un modello ben definito di indicatori di digitalizzazione e di categorie che sono, nell'ambito delle attività di monitoraggio, oggetto di rilevazione e contribuiscono alla misurazione dell'incremento del livello di trasformazione digitale mediante l'utilizzo dei servizi previsti dalle stesse gare strategiche.

Si riportano, in figura 7 gli elementi principali di monitoraggio di AGID nelle gare strategiche:



Figura 7 - Gli elementi di monitoraggio di AGID

Il monitoraggio condotto da AGID garantisce quindi alle Amministrazioni un indirizzo chiaro per l'allineamento alla strategia di crescita digitale del Paese attraverso l'aderenza ai principali obiettivi del Piano triennale che devono essere indirizzati all'atto della stipula dei contratti esecutivi all'interno di ciascun accordo quadro e che sono, come detto, oggetto di rilevazione e di successive elaborazioni ed aggregazioni mirate a fornire una misura della digitalizzazione del Paese.

AGID, nell'ambito del proprio ruolo istituzionale, ha monitorato, a diversi livelli di aggregazione, in che modo e con quale efficacia il ricorso alle iniziative strategiche stiano contribuendo al raggiungimento degli obiettivi del Piano Triennale. Tale analisi è stata svolta utilizzando i dati estrapolati dai Contratti Esecutivi stipulati dalle Amministrazioni e mappando:

- il raggiungimento attraverso l'adesione degli obiettivi di Piano Triennale riferiti al Piano triennale per l'Informatica 2020-2022, secondo una macro-classificazione in sei ambiti (Servizi, dati, piattaforme, infrastrutture, interoperabilità e Sicurezza);
- il raggiungimento attraverso l'adesione degli obiettivi di Piano triennale riferiti al Piano triennale per l'Informatica 2020-2022, secondo una classificazione in sotto ambiti di specificazione;
- la realizzazione dei principi guida, attraverso l'adesione, del Piano triennale per l'Informatica 2020-2022;
- gli Indicatori Generali di Digitalizzazione (IGD) definiti nelle gare strategiche.

Per classificare le Amministrazioni contraenti e creare dei *cluster* di tipologia di pubbliche amministrazioni è stata utilizzata la classificazione ISTAT che prevede il raggruppamento di PAC e PAL per tipologia, quali:

- le PAC sono state aggregate in: Ministeri, Organi Costituzionali, Autorità indipendenti, Enti (Enti di Ricerca, Enti Assistenziali e Previdenziali, Agenzie nazionali, organizzazioni quali Cassa Depositi e Prestiti, Pago PA SPA, Invitalia, ecc.), società ICT in house;
- le PAL sono state aggregate in: Regioni e Province Autonome, Comuni e Province, Sanità, Università e Ricerca, società ICT in house.

Di seguito vengono presentati esempi dell'analisi effettuata che danno un'idea di quanto lo strumento delle iniziative strategiche stia aiutando la trasformazione digitale delle PA e gli ambiti ove ciò sia più significativo. I dati presentati nel seguito rappresentano lo stato dell'arte a settembre 2023.

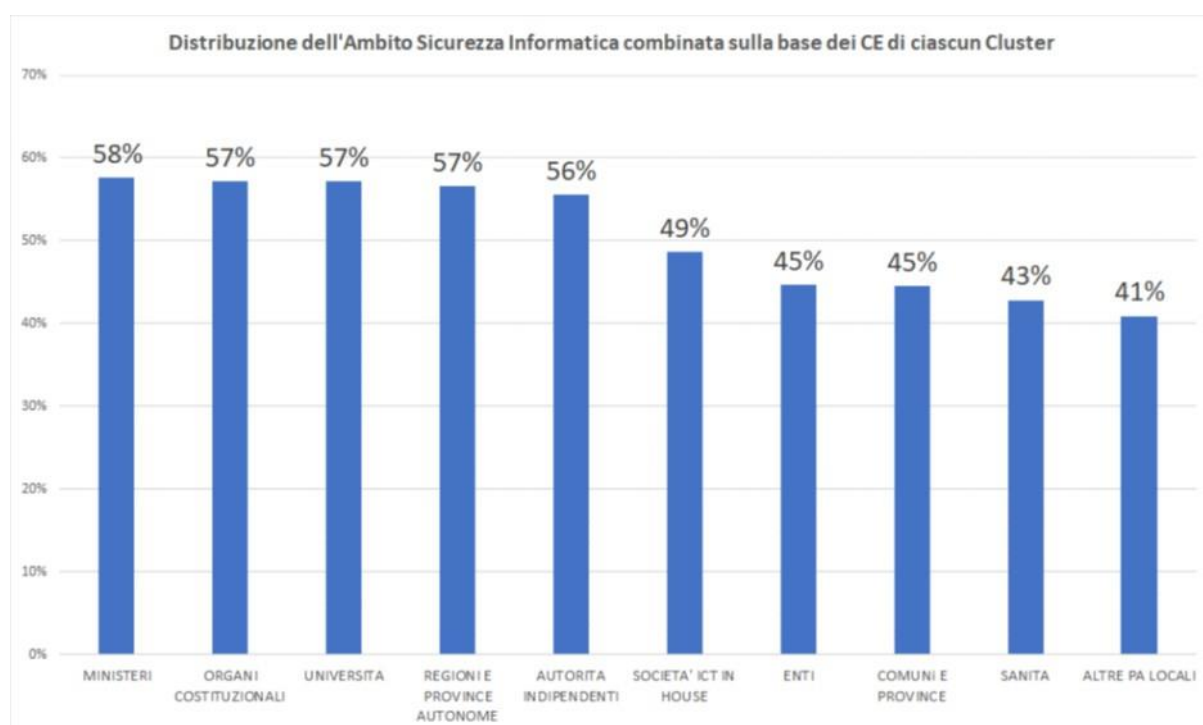


Figura 8 - Obiettivo sicurezza per ciascun cluster di PAC

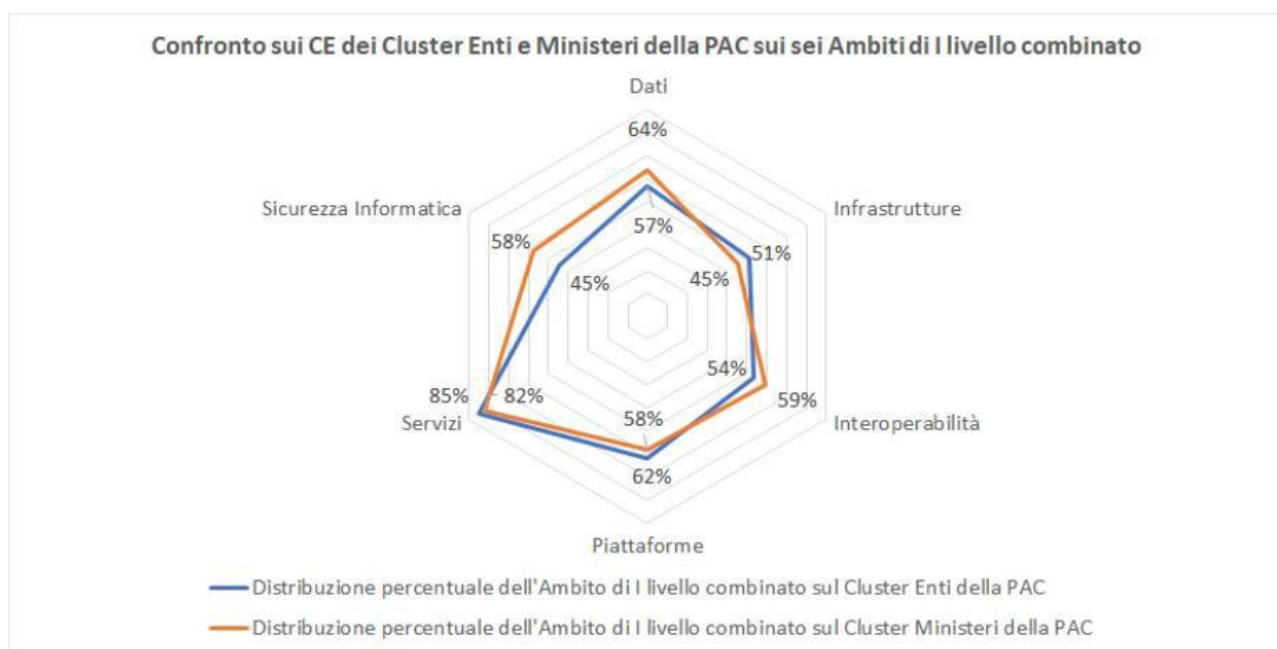


Figura 9 - Ambiti di primo livello e PAC

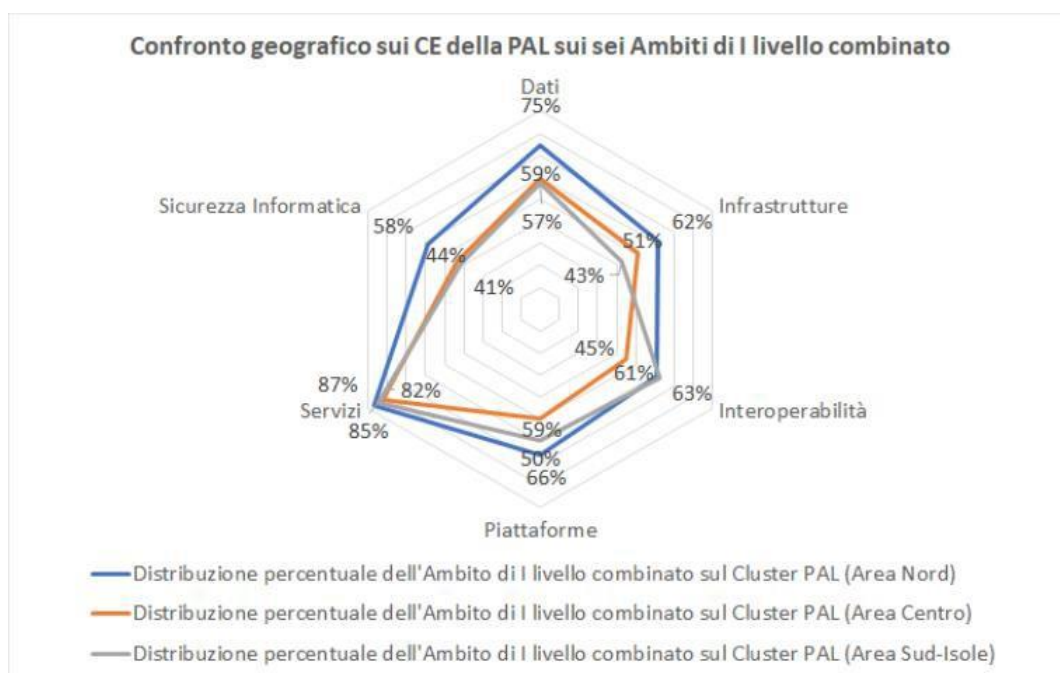


Figura 10 - Ambiti di primo livello e PAL

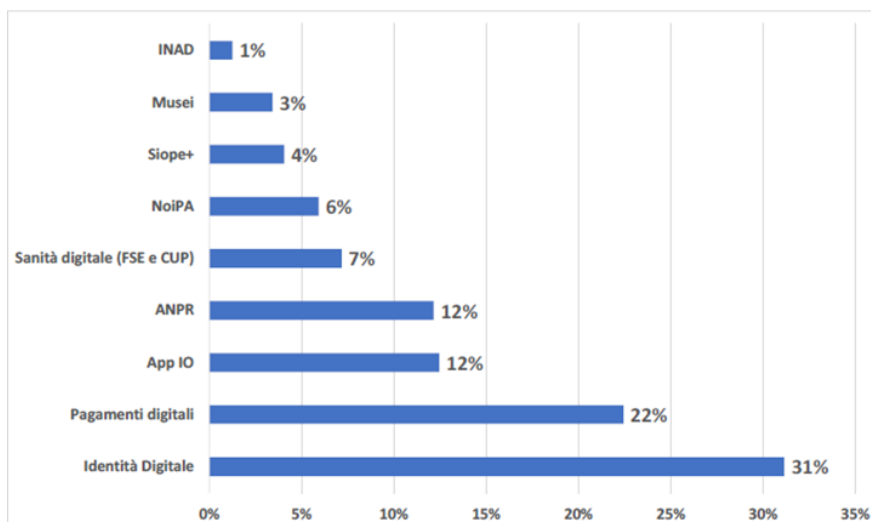


Figura 11 - Percentuale di contratti che afferiscono alla realizzazione della piattaforma

1.1.1. L'INDICATORE DI INCREMENTO DEL LIVELLO DI TRASFORMAZIONE DIGITALE MEDIANTE I SERVIZI PREVISTI DALLE GARE STRATEGICHE (R.A.7.1B - PT 2022-24)

Rispetto agli obiettivi del Piano Triennale 2022-2024, l'indicatore **R.A.7.1b "Incremento del livello di trasformazione digitale mediante l'utilizzo dei servizi previsti dalle Gare strategiche"**, è parte del sistema di monitoraggio AGID dei risultati attesi, appartiene all'obiettivo "7.1 - Rafforzare le leve per l'innovazione delle PA e dei territori" e intende rappresentare un'indicazione sul livello di efficacia degli interventi di digitalizzazione operati dalle PA attraverso l'utilizzo delle Gare strategiche.

Il modello di calcolo del R.A.7.1b è stato costruito a partire da nove indicatori generali di digitalizzazione comuni a tutte le iniziative del programma delle gare strategiche, i quali, a loro volta, sono stati opportunamente pesati e classificati ed il valore dell'indicatore è dimensionato per variare su una scala da 0 a 10.

I nove indicatori generali di digitalizzazione sono, infatti, classificati nei seguenti tre sub-indicatori:

1. **Digitalizzazione:** cui afferiscono gli Indicatori che contribuiscono in maniera diretta alla digitalizzazione;
2. **Standardizzazione:** cui afferiscono gli Indicatori propedeutici alla digitalizzazione;
3. **Efficientamento:** cui afferiscono gli Indicatori che rappresentano i benefici del processo di trasformazione digitale.

Nella seguente tabella (tabella 2) si illustra, nel dettaglio, l'associazione dei nove indicatori generali di digitalizzazione ai suddetti tre sub-indicatori e il peso di quest'ultimi nel calcolo del valore complessivo dell'indicatore R.A.7.1b.

Indicatori generali di digitalizzazione delle gare strategiche	Sub-indicatori	Peso attribuito (%)
Numero servizi aggiuntivi offerti all'utenza interna, esterna (cittadini), esterna (imprese), altre PA.	Digitalizzazione	60%
Obiettivi CAD raggiunti con l'intervento	Digitalizzazione	60%
Integrazione con infrastrutture immateriali	Digitalizzazione	60%
Integrazione con Basi Dati di interesse nazionale	Standardizzazione	30%
Riuso di processi per erogazione servizi	Standardizzazione	30%
Riuso soluzioni tecniche	Standardizzazione	30%
Collaborazione con altre Amministrazioni (progetto in coworking, realizzato anche mediante contratti esecutivi diversi per Amministrazione)	Standardizzazione	30%
Riduzione % della spesa per l'erogazione del servizio	Efficientamento	10%
Riduzione % dei tempi di erogazione del servizio	Efficientamento	10%

Tabella 2 - Indicatori generali di digitalizzazione delle gare strategiche, sub-indicatori e peso nel calcolo dell'indicatore R.A.7.1b

Il valore rilevato per l'indicatore R.A.7.1b è, a novembre 2023, pari a 6. Nel periodo di osservazione, che decorre dalla data di avvio della misurazione di questo indicatore, si osserva un andamento inizialmente in calo del valore del R.A.7.1b, dovuto essenzialmente alla concomitante riduzione del sub-indicatore "Digitalizzazione", per poi stabilizzarsi intorno al valore 6.

Il fenomeno può essere conseguenza di varie cause come, ad esempio, gli insiemi di gare/lotti che mutano nel tempo secondo le attivazioni ed il conseguente ciclo di monitoraggio o, più verosimilmente, per i possibili effetti dovuti all'opera di sensibilizzazione di AGID verso le PA che ha portato le stesse ad una valorizzazione più diffusa e accurata degli indicatori.

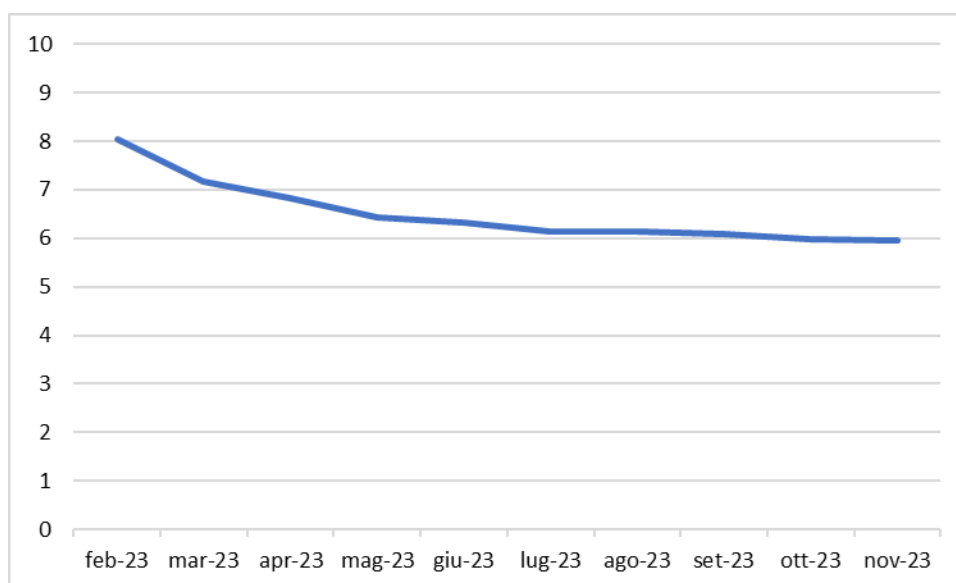


Figura 12 - Andamento storico dell'indicatore R.A.7.1.b

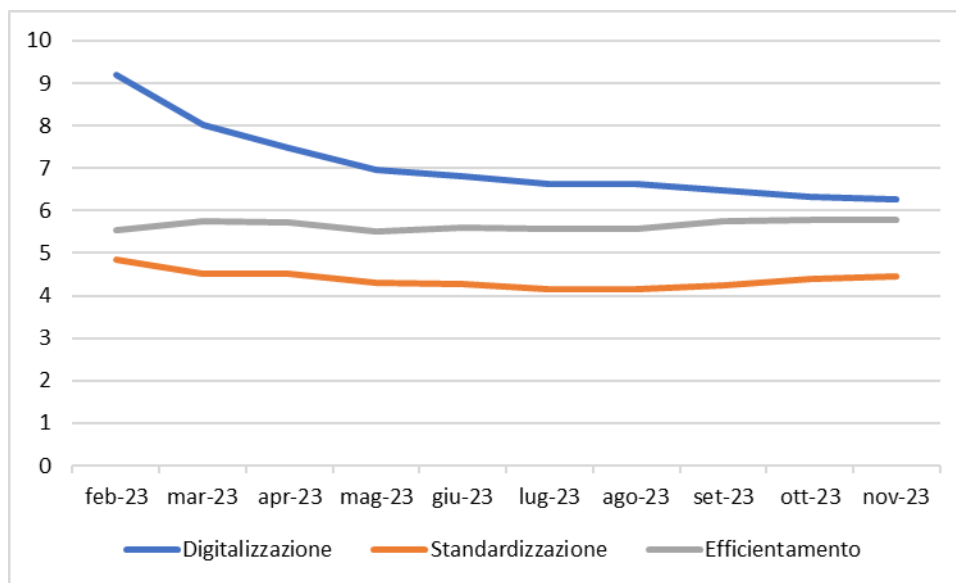


Figura 13 - Andamento storico dei sub indicatori

1.2. GLI STRUMENTI CONSIP

Nel seguito si fornisce una vista sintetica delle iniziative attive, che contribuiscono alla realizzazione degli obiettivi del Piano Triennale, a disposizione delle Amministrazioni e utilizzabili in alcuni casi anche con fondi PNRR.

Capitolo del Piano Triennale 2024-2026 di riferimento	Strumento Consip di acquisizione	Modalità di acquisto	Gara strategica	Utilizzabile con fondi PNRR
Cap. 3 - Servizi	Digital Transformation	Ordine diretto	SI	SI
Cap. 3 - Servizi	Sanità digitale- SICA	Appalto specifico Ordine diretto	SI	SI
Cap. 3 - Servizi	Sanità digitale- SISSC	Appalto specifico Ordine diretto	SI	SI
Cap. 3 - Servizi	Sanità digitale- SIG	Appalto specifico Ordine diretto	SI	SI
Cap. 3 - Servizi Cap. 5 - Dati e intelligenza artificiale Cap. 4 - Piattaforme	Data Management	Ordine diretto	SI	SI
Cap. 3 - Servizi Cap. 4 - Piattaforme	Servizi applicativi Cloud	Ordine diretto	SI	SI
Cap. 3 - Servizi Cap. 6 - Infrastrutture	Cloud Enabling	Ordine diretto	SI	SI
Cap. 6 - Infrastrutture	Public Cloud IaaS e PaaS	Appalto specifico Ordine diretto	SI	SI (Lotti 2-11)
Cap. 6 - Infrastrutture	S_RIPA	Ordine diretto	SI	NO
Cap. 6 - Infrastrutture	Licenze Software Multibrand	Ordine diretto	NO	SI
Cap. 6 - Infrastrutture	Microsoft Enterprise Agreement	Ordine diretto	NO	SI
Cap. 6 - Infrastrutture	Public Cloud SaaS - B.I.	Appalto specifico Ordine diretto	SI	SI
Cap. 6 - Infrastrutture	Public Cloud SaaS - Pr.In.Co.	Appalto specifico Ordine diretto	SI	SI
Cap. 6 - Infrastrutture	Public Cloud SaaS - CRM	Appalto specifico Ordine diretto	SI	SI
Cap. 6 - Infrastrutture	Public Cloud SaaS - IT Service Management	Appalto specifico Ordine diretto	SI	SI
Cap. 6 - Infrastrutture	SPC Connettività	Ordine diretto	SI	NO
Cap. 6 - Infrastrutture	Servizi PEC e REM-IT	Ordine diretto	NO	NO
Cap. 7 – Sicurezza informatica	Sicurezza da remoto	Ordine diretto	SI	SI
Cap. 7 – Sicurezza informatica	Sicurezza on premise – gestione e protezione	Appalto specifico	SI	SI
Cap. 7 – Sicurezza informatica	Sicurezza on premise – Protezione Perimetrale, endpoint e anti-APT	Ordine diretto (con /senza valutazione preliminare)	SI	SI

Tabella 3 - Strumenti Consip di acquisizione

1.3. DESCRIZIONE SINTETICA DEGLI STRUMENTI CONSIP

1.3.1. SERVIZI APPLICATIVI IT

Accordo quadro dedicato allo sviluppo software e ai servizi correlati, nello specifico comprende:

- *Sviluppo, Manutenzione evolutiva, adeguativa e migliorativa* di software ad hoc;
- *Personalizzazione e parametrizzazione* di soluzioni commerciali o di software open source o di software in riuso;
- Servizi di *Gestione del portafoglio applicativo*, in particolare gestione applicativi e basi dati, gestione dei contenuti di siti web, manutenzione correttiva;
- *Servizi Tecnico-Specialistici*, consistenti in progetti/attività/studi di natura ICT e di livello specialistico);
- *Servizi accessori* (ad es. servizio assistenza in remoto, formazione, etc).

1.3.2. DIGITAL TRANSFORMATION

Accordo Quadro che rende disponibili servizi di indirizzo della trasformazione digitale e della sua adozione, nei seguenti ambiti:

- *Strategia della Trasformazione Digitale*: attraverso i servizi di disegno strategia digitale, di definizione del Piano Strategico ICT e di disegno mappa dei servizi digitali della PA;
- *Digitalizzazione dei processi*: attraverso i servizi di disegno del modello di erogazione del servizio digitale, disegno di processi digitali, supporto specialistico per l'implementazione di servizi digitali;
- *Gestione della Transizione al Digitale*: attraverso i servizi di *change management* dedicati alla Progettazione della transizione al digitale e all'affiancamento alla transizione digitale;
- *PMO*.

1.3.3. SANITÀ DIGITALE-SICA

Accordo Quadro dedicato ai sistemi informativi clinico assistenziali, che rende disponibili servizi per lo sviluppo di soluzioni applicative in ambito Clinico-Assistenziale, focalizzando l'attenzione sulla gestione clinica, sulla gestione delle cronicità e sull'assistenza del cittadino, sia dipartimentale sia da remoto, favorendo nuovi strumenti di assistenza telematica (medicina personalizzata o di precisione). I servizi comprendono:

- *Cartella clinica e Enterprise Imaging*: Piattaforme di Cartella Clinica Elettronica CCE multi disciplinare, Sistema di gestione dei pazienti e Order Management, Order Entry, Gestione applicativa LIS, RIS e PACS, gestione applicativa Anatomia Patologica, Digital Patology, Clinical Data Repository;
- *Telemedicina*: Piattaforme di Telemedicina (Tele-monitoraggio, Tele-assistenza, Tele-refertazione, Tele-consul, etc.);
- *Supporto alla digitalizzazione del SSN*: Servizi di consulenza strategica, supporto organizzativo, monitoraggio e PMO.

1.3.4. SANITÀ DIGITALE- SISSC

Accordo Quadro dedicato ai sistemi informativi sanitari e servizi al cittadino, che rende disponibili servizi applicativi per supportare le PPAA del SSN, focalizzando l'attenzione sulla centralità del

cittadino, l'interoperabilità dei dati e dei servizi attraverso lo sviluppo e l'implementazione dei documenti sanitari standard riconosciuti a livello Nazionale. I servizi comprendono:

- *CUP e interoperabilità dati sanitari*: Sistema centralizzato informatizzato di prenotazione delle prestazioni sanitarie, piattaforme di interoperabilità dati (ESB, orchestratori, etc.), servizi di integrazione (sistema TS, INI, ANA, territoriali, etc.);
- *Piattaforme applicative, portali ed APP*: Monitoraggio spesa Sanitaria, Trasfusionale, Medicina di Base, E-prescription, Sistema di Anagrafe Sanitaria Centralizzata, Fascicolo Sanitario Elettronico, portali e APP in ambito sanitario, Servizi OnLine per Cittadino ed Operatori Sanitari;
- *Servizi di supporto*: Servizi di consulenza strategica, supporto organizzativo, monitoraggio e PMO.

1.3.5. SANITÀ DIGITALE- SIG

Accordo Quadro dedicato ai sistemi informativi gestionali per sviluppare soluzioni applicative di supporto ai processi amministrativi, alla gestione e all'interoperabilità dei dati e dei servizi attraverso lo sviluppo e l'implementazione dei documenti sanitari standard riconosciuti a livello Nazionale. I servizi comprendono:

- *Procedimenti amministrativi contabili*: Programmazione, budget, acquisti, fatturazione elettronica, controllo di gestione, gestione personale, organizzazione e performance management, gestione magazzino, farmaci, logistica, procedimenti amministrativi, Work flow Management;
- *Data driven*: Data WareHouse, Business Intelligence, Big Data, Analytics, Intelligenza Artificiale, Machine Learning, Sistemi Predittivi, Repository, Gestione documentale, protocollo informatico, conservazione;
- *Servizi di supporto*: Servizi di consulenza strategica, supporto organizzativo, monitoraggio e PMO.

1.3.6. DATA MANAGEMENT

Accordo Quadro che mette a disposizione delle PA servizi applicativi e professionali per la realizzazione di sistemi informativi a supporto dei processi decisionali. In particolare sono inclusi:

- *Servizi applicativi*:
 - o In ambito Data Warehouse e Business Intelligence, con sviluppo/manutenzione evolutiva software ad hoc, personalizzazione pacchetti software di mercato, manutenzione correttiva, gestione applicativa e supporto specialistico;
 - o In ambito Big Data/Analytics, con valutazione, analisi e acquisizione dei dati, realizzazione del modello di analisi, conduzione della soluzione di analisi;
 - o In ambito Open Data, con analisi dei dati, produzione, pubblicazione, aggiornamento e conservazione dataset;
 - o In ambito AI/ML tramite supporto specialistico.
- *PMO e Demand*: Servizi di demand management e PMO per definire ed accompagnare la trasformazione digitale nelle PPAA.

1.3.7. SERVIZI APPLICATIVI CLOUD

Accordo Quadro che mette a disposizione delle PA un catalogo di servizi IT per supportare la trasformazione digitale e l'innovazione tecnologica, attraverso la realizzazione di servizi digitali

disegnati sulla centralità del cittadino, sulla semplificazione delle interazioni con la PA e che consente di migrare gli applicativi esistenti al Cloud. L'AQ comprende le seguenti tipologie di servizi:

- *Servizi applicativi*, con sviluppo e manutenzione evolutiva di software, migrazione applicativa al cloud, configurazione e/o personalizzazione di software, sviluppo e evoluzione di software in modalità co-working tra più amministrazioni, manutenzione correttiva, supporto tecnico-specialistico ICT, gestione del portafoglio applicativo;
- *Servizi accessori* con gestione operativa, gestione dell'identità e dell'accesso utente, acquisizione e classificazione di dati, e-learning e assistenza virtuale, contact center e help desk;
- *Servizi di demand e PMO*, con project management, supporto al monitoraggio, change management, demand management, customer satisfaction.

1.3.8. CLOUD ENABLING

Accordo Quadro che rende disponibili servizi professionali tecnici e di supporto all'adozione del cloud e PMO, in particolare:

- *Servizi professionali di supporto* relativi a:
 - o identificazione della strategia di migrazione al cloud;
 - o fattibilità e definizione delle responsabilità e delle competenze necessarie;
 - o verifica e monitoraggio dei risultati raggiunti;
 - o PMO.
- *Servizi professionali tecnologici, comprendenti:*
 - o progettazione dell'architettura e delle risorse tecnologiche necessarie per la migrazione,
 - o trasferimento dei dati dai sistemi source ai sistemi target,
 - o implementazione delle policy di sicurezza e di scalabilità delle risorse, delle metriche di *alert* e di performance dei sistemi,
 - o supporto alle Amministrazioni nella formazione del personale su tematiche tecnologiche cloud.

1.3.9. PUBLIC CLOUD IAAS E PAAS

Accordo Quadro che rende disponibili strumenti e servizi per la realizzazione del modello strategico Cloud della PA; l'AQ comprende le seguenti tipologie di servizi:

- *Servizi Public Cloud Iaas e Paas*, con diverse categorie di servizi tra cui spazio archiviazione virtuale, risorse per la creazione di reti, prodotti per la sicurezza degli ambienti virtuali, tool per sviluppare applicativi, etc.;
- *Servizi supporto all'adozione e PMO*, per il supporto tematico alla Cloud governance (con servizi di Demand e PMO) e alla Cloud Strategy (Strategy, Roadmap ed Innovazione);
- *Servizi tecnologici*, mediante Cloud Solution Design & Architecture, Cloud Implementation/Migration, Cloud Service Management.

1.3.10. S-RIPA

Accordo Quadro per la progettazione della rete e l'erogazione dei servizi di connettività della Rete Internazionale della PA, nonché servizi di sicurezza, VoIP, comunicazione evoluta e servizi professionali. Rende disponibili:

- *Servizi di connettività IP:*
 - o servizi di connettività Satellitare;
 - o servizi di connettività Terrestre Best Effort;
 - o servizi di connettività Terrestre a banda Garantita.
- *Servizi di sicurezza:*
 - o Next Generation Firewalling;
 - o Data loss/leak prevention;
 - o Anti-APT.

1.3.11. LICENZE SOFTWARE MULTIBRAND

Convenzione che consente alle PA di approvvigionarsi dei prodotti software dei differenti brand e della relativa manutenzione; comprende:

- Fornitura di *prodotti software on premise* di tipo proprietario (a seconda del lotto/brand sono inclusi licenze, sottoscrizioni, prodotti di certificazione da remoto, ecc.);
- *Rinnovo della manutenzione per i prodotti software* già in uso (solo per alcuni lotti/brand);
- *Servizi connessi*, a seconda del lotto/brand: manutenzione dei prodotti software acquistati in Convenzione, consegna via web, call center.

1.3.12. MICROSOFT ENTERPRISE AGREEMENT

Convenzione che rende disponibili licenze per scopi eterogenei afferenti all'ambito tecnologico Microsoft e comprende *Licenze d'uso di tipo enterprise* «Microsoft Enterprise Agreement» *on premises* (installazione del software in locale) e *dual rights* (facoltà dell'Amministrazione di procedere alla installazione del software su macchine fisiche ovvero fruizione in modalità cloud). In particolare, la Convenzione consente l'acquisto di licenze del seguente tipo:

- **Infrastrutturale** che comprende sistemi operativi, sicurezza, system management, piattaforme di sviluppo, unified communication, business intelligence;
- **Applicativo** che comprende collaboration, content management e produttività individuale.

Nell'acquisto sono inclusi la consegna, la garanzia di 12 mesi, l'assistenza e il customer care.

1.3.13. PUBLIC CLOUD SAAS - B.I.

Accordo quadro che rende disponibili servizi SaaS qualificati nell'ambito della *Business Intelligence*: si tratta di uno strumento multi-brand che consente l'acquisto da diversi Cloud Service Provider (CSP).

Ciascun CSP offre un listino relativo a soluzioni tecnologiche BI SaaS proprietarie, contenenti almeno le seguenti funzionalità Base:

- *Data Visualization*
- *Data Preparation for BI*
- *Reporting e Dashboard*
- *Access management and security*
- *Data Source Integration*

1.3.14. PUBLIC CLOUD SAAS - PR.IN.CO.

Accordo Quadro per la Fornitura di prodotti SaaS per la produttività individuale e la *collaboration*. Lo

strumento consente l'acquisto, anche in bundle, dei seguenti servizi di produttività e *collaboration*:

- *Posta Elettronica*
- *Documentale (gestione documentale e file sharing)*
- *Collaboration (Instant Messaging e di Audio/Video Conference)*

1.3.15. PUBLIC CLOUD SAAS - CRM

Accordo Quadro che rende disponibili servizi SaaS per il CRM ed il marketing; lo strumento è multi-brand e consente quindi l'acquisto da diversi Cloud Service Provider (CSP). In particolare, l'AQ prevede:

- *CRM 'classico'*, comprendente le funzionalità per la gestione dei clienti (in questo caso dei cittadini), i cui utenti sono operatori interni all'organizzazione
- *Marketing*, con funzionalità rivolte alla creazione e gestione di campagne di contatto e comunicazione verso l'esterno

1.3.16. PUBLIC CLOUD SAAS - IT SERVICE MANAGEMENT

Accordo quadro per la fornitura di prodotti SaaS di IT Service Management; in particolare, sono resi disponibili 4 distinti "bundle" di funzionalità SaaS:

- *Bundle ITSM*, che comprende la sola componente di Service Management, per la gestione dei processi e dei sistemi IT secondo le pratiche ITIL;
- *Bundle Operation management*, che comprende le funzionalità legate alle Operation dei Servizi IT;
- *Bundle Asset management*, che comprende le funzionalità di gestione del ciclo di vita degli asset;
- *Bundle Contract management*, che comprende le funzionalità di gestione e pianificazione degli economics dei contratti, delle scadenze, dei livelli di Servizio ed i KPI, etc.

1.3.17. SPC CONNETTIVITÀ

Accordo Quadro che implementa quanto prescritto al Capo VIII del Codice dell'Amministrazione Digitale e rende pertanto disponibili i servizi di connettività nell'ambito del Sistema Pubblico di Connettività (SPC) per le Pubbliche Amministrazioni Centrali (PAC) e Territoriali o Locali (PAT o PAL) ed alcuni servizi aggiuntivi quali la comunicazione evoluta, il Voip e la Telepresenza. Comprende:

- *Servizi di Trasporto Dati (TR)*:
 - o Servizi di Trasporto Dati wired su portante Elettrica (STDE);
 - o Servizi di Trasporto Dati wired su portante Elettrica (STDO);
 - o Servizi di Trasporto Dati wireless Satellitari (STDS);
- *Servizi di Sicurezza Perimetrale (SICP)*:
 - o Servizi di Sicurezza Perimetrale Unificata (SPUN);
 - o Servizi di Sicurezza Centralizzata (SCEN).

1.3.18. SERVIZI PEC E REM-IT

Convenzione che mette a disposizione delle PA caselle PEC e garantire alle Amministrazioni il passaggio ai servizi di recapito certificato REM-IT i cui messaggi sostituiranno – in termini di validità legale – i messaggi di posta elettronica certificata. La Convenzione comprende:

- *Servizi PEC*: fornitura di caselle PEC di diversa capacità e potenzialità, servizi di supporto operative per la configurazione e l'interfacciamento con i sistemi informative dell'Amministrazione;

- *Servizi REM-IT*: fornitura delle future caselle REM-IT in continuità con i servizi PEC e servizi di adeguamento delle caselle PEC ai futuri servizi REM.

1.3.19. SICUREZZA DA REMOTO

Accordo Quadro che mette a disposizione delle PA servizi, erogati da remoto, per la sicurezza dei perimetri tecnologici delle infrastrutture e servizi per la compliance ed il controllo delle soluzioni di Sicurezza. L'AQ comprende:

- *Servizi di sicurezza "da remoto"*: Next Generation Firewall e Web Application Firewall, Gestione dell'identità e dell'accesso utente, Firma digitale remota, timbratura, marca temporale e sigillo elettronico, Security Operation Centre, Gestione continua delle vulnerabilità di sicurezza;
- *Servizi per la compliance ed il controllo delle soluzioni di sicurezza*: Security Strategy, Vulnerability Assessment, Testing del codice, Supporto all'analisi e gestione degli incidenti, Penetration Testing.

1.3.20. SICUREZZA ON PREMISE – GESTIONE E PROTEZIONE

Accordo Quadro che mette a disposizione delle PA un insieme di prodotti che consentono di assicurare la necessaria protezione contro gli attacchi informatici inerenti la protezione dei dati e dei canali web e-mail; l'Accordo Quadro fornisce inoltre gli strumenti a supporto della gestione degli eventi di sicurezza e dell'accesso controllato ai sistemi. L'AQ prevede:

- *Fornitura dei seguenti prodotti*: SIEM - Security Information & Event Management, SOAR - Security Orchestration, automation & response, web application firewall, secure web gateway, secure email gateway, database security, data loss prevention, privileged access management;
- *Servizi base* relativi all'installazione e configurazione, alla formazione e l'affiancamento, alla manutenzione, al contact center/ help desk, all'hardening su client e al supporto specialistico;
- *Servizi aggiuntivi* come hardening su altri sistemi, Data Assessment, privileged account assessment, servizi professionali erogati dal vendor, servizio di incident response.

1.3.21. SICUREZZA ON PREMISE – PROTEZIONE PERIMETRALE, ENDPOINT E ANTI-APT

Accordo Quadro che mette a disposizione delle PA prodotti e servizi connessi in grado di proteggere da attacchi informatici il perimetro infrastrutturale ICT e i terminali utente; l'AQ comprende:

- *Fornitura dei prodotti*: next generation firewall, network access control, endpoint protection platform/endpoint detection & response server protection platform (SPP), protezione anti APT (Advanced Persistent Threats).
- *Servizi connessi*, relativi a installazione e configurazione (inclusi nella fornitura), formazione e affiancamento, manutenzione, contact center/help desk.

1.4. RIFERIMENTI

[1] [L'Offerta Consip](#)

[2] [La vetrina delle iniziative Consip](#)

[3] [Gare e contratti](#)

Strumento 2 - Gestione associata dell'ICT

Versione 1.0 del 21/12/2023

I. Obiettivo

Il documento esamina i principi generali della gestione associata dell'ICT, con un focus specifico sulle Unioni di Comuni. Inoltre, analizza i fattori abilitanti che favoriscono l'implementazione di tali sistemi, con particolare attenzione all'organizzazione dei servizi intercomunali in gestione associata. Il documento esplora inoltre il ruolo delle *community* e della collaborazione digitale, evidenziando l'importanza della qualificazione dei centri servizi.

II. Destinatari

Enti territoriali quali: comuni, province, città metropolitane e regioni, comunità montane, comunità isolate, unioni di comuni e consorzi fra enti territoriali.

III. Crediti

Il documento è stato redatto dal Gruppo di ricerca sulla trasformazione digitale della PA dell'Osservatorio Agenda Digitale del Politecnico di Milano. Parte delle evidenze mostrate all'interno di questo documento sono i risultati di una collaborazione sviluppata nell'ambito del Progetto Italiae (CUP: J51H17000030007, appartenente al Programma Operativo Nazionale "Governance e Capacità Istituzionale" 2014-2020) tra il Dipartimento di Ingegneria Gestionale del Politecnico di Milano e il Dipartimento per gli Affari Regionali e le Autonomie della Presidenza del Consiglio dei Ministri.

1.1. INTRODUZIONE

La gestione associata è modello organizzativo che permette alle amministrazioni pubbliche di condividere tra loro risorse e competenze per l'erogazione di funzioni o di determinati servizi di loro competenza. La gestione associata della funzione ICT, nello specifico, può rivelarsi una alternativa vantaggiosa per specifiche tipologie di enti, in particolare per quelli di dimensione ridotte, caratterizzati da risorse e competenze specialistiche limitate. In questo contesto, esistono diverse configurazioni di governance multilivello incentrate sulla trasformazione digitale che permettono di ottimizzare l'utilizzo delle risorse disponibili nel mantenimento delle applicazioni e nell'affrontare le sfide legate alla introduzione ed evoluzione di soluzioni e infrastrutture, superando le limitazioni tipiche di una gestione individuale.

In allegato A è riportato un estratto della Ricerca "Innovazione e tecnologia a supporto del governo locale", svolta nell'ambito del Progetto "ITALIAE", promosso dal Dipartimento per gli Affari Regionali e le Autonomie e finanziato con il Programma Operativo Nazionale "Governance e capacità istituzionale" 2014 – 2020" che offre una fotografia dello stato dell'arte dell'associazionismo ICT e del ruolo del Responsabile della Transizione al Digitale (RTD) con particolare riferimento al modello dell'Unione di Comuni. Tale scelta deriva dalla rappresentatività di tale forma.

1.1.1. SISTEMI INTERCOMUNALI PER LA GESTIONE ASSOCIATA DELL'ICT

Sebbene i dati presentati nell'Allegato A dimostrino che la gestione associata dell'ICT in Unione sia una leva importante per la trasformazione digitale degli enti, soprattutto quelli di piccole dimensioni, esistono numerose altre forme di collaborazione sul digitale che possono portare a risultati simili. Queste forme possono portare a gradi molto diversi di integrazione tra enti, e dunque avere ricadute diverse sul livello di digitalizzazione degli stessi.

Nel seguito sono presentate le principali forme di gestione associata dell'ICT: le Unioni e Comunità Montane, i Consorzi e le Convenzioni.

1.1.2. LE UNIONI DI COMUNI

Le Unioni di Comuni (previste all'art. 32 TUEL), così come le Comunità Montane, Isolane e d'Arcipelago (artt. 27, 28 e 29 del TUEL) sono una forma di aggregazione tra due o più Comuni, che porta alla costituzione di un vero e proprio ente locale. Ai sensi dell'art. 28 D. Lgs. 267/2000, le Unioni possono svolgere l'esercizio associato delle funzioni delegate dai Comuni afferenti, o quelle individuate dalla Regione di appartenenza, tra cui anche il servizio informatico e trasformazione digitale. La creazione di un'Unione o Comunità Montana comporta dunque un trasferimento di funzioni dai singoli Comuni all'ente sovracomunale costituito, il quale assume così una piena autonomia decisionale e gestionale.

La natura del raccordo tra l'ente Unione e i Comuni afferenti può avere diverse conformazioni, sulla base delle modalità di gestione delle funzioni associate. Vi è un tipo di configurazione tendente a una *governance* accentrata, che prevede la gestione attraverso l'Unione delle funzioni comunali; dunque, una sostituzione *de facto* dell'Unione agli enti locali nelle funzioni trasferite, di cui assume sia la titolarità che l'esecuzione. Da un punto di vista operativo, nel caso più estremo del modello accentrato, i Comuni vedono il proprio personale dipendente concentrato presso l'Unione. In questi casi, la gestione associata del digitale si sostanzia tipicamente nella creazione dell'Ufficio ICT integrato, con la nomina del RTD in capo ad esso, il quale esercita tutte le sue funzioni per tutti i Comuni aderenti all'Unione e trasversalmente rispetto agli altri servizi offerti dall'ente.

Un'altra configurazione può essere invece definita decentrata e prevede una delega parziale della gestione del servizio ICT, in base alla quale una parte di attività viene trasferita all'Unione e una parte invece mantenuta, almeno a livello di titolarità, dai singoli Comuni membri. Nel caso di una gestione decentrata, il raccordo può essere garantito attraverso l'istituzione di un tavolo permanente che coinvolge gli enti locali dell'Unione per l'aggiornamento costante sulle linee guida, sugli adempimenti normativi e sulla conseguente strategia di intervento degli enti. Poiché l'integrazione dell'Unione è minore, anche la delega al digitale è parziale: l'Ufficio ICT ha delega parziale mentre i Comuni mantengono internamente parte delle attività legate a questa funzione. Anche in questi casi – tipicamente – la nomina del RTD avviene in capo all'Unione, ma egli assume un ruolo di regia, definendo obiettivi e strategie di digitalizzazione e monitorandone il conseguimento. A tal fine, si interfaccia con i referenti individuati nei Comuni che si occupano della gestione operativa e dell'attuazione di iniziative progettuali.

1.1.3. LE FORME CONSORTILI

Un altro modello di collaborazione intercomunale per la gestione associata del digitale è rappresentato dalle forme consortili, ovvero Consorzi e Consorzi obbligatori (art. 31 TUEL), società *in-house* (art. 114 TUEL). I soggetti che possono procedere all'istituzione del Consorzio possono essere dunque Comuni, Unioni e altri soggetti territoriali, cui fa spesso capo un ente capofila. Gli enti consorziati partecipano attraverso il versamento di una quota annua e con modulo di adesione per la cessione delle funzioni; nel caso delle società *in-house*, in quanto società di capitali, gli enti pubblici associati ne detengono una quota azionaria.

La collaborazione sul digitale tra Comuni nell'ambito di Consorzi prevede tipicamente una delega parziale delle funzioni dell'Ufficio ICT e una nomina del RTD in seno al Consorzio. Lo stesso può avvenire presso un ente socio, che viene preposto all'esercizio delle funzioni associate, assorbendo eventualmente anche unità di personale dal Consorzio stesso.

I Comuni possono fondare o stringere accordi con Consorzi e società *in-house* specificamente ed esclusivamente per la gestione del digitale, e per questa ragione tali istituti hanno la particolarità di essere in grado di offrire risorse altamente competenti e specializzate. Le attività più frequentemente gestite dai Comuni tramite i Consorzi sono infatti altamente specialistiche, come la gestione delle reti tecnologiche, ovvero della connettività interna al Comune e tra le sue sedi. A seguire, gli enti gestiscono tramite le società *in-house* anche l'infrastruttura tecnologica, comprendente quindi acquisto, manutenzione e aggiornamento hardware. Tra i principali benefici legati a questa gestione vi è dunque per i Comuni la possibilità di riallocare le proprie risorse umane su altre attività o funzioni dove ve ne è carenza, e maggiori competenze e maggiore efficienza per la gestione di beni e servizi informatici.

Oltre ai Consorzi specificatamente incentrati sul digitale, esistono casistiche diffuse sul territorio di associazioni nate con scopi diversi dal digitale, come ad esempio i Consorzi obbligatori, che fanno leva sulla forma di cooperazione esistente per gestire anche le funzioni ICT nei confronti degli enti già soci.

1.1.4. LE CONVENZIONI

La Convenzione, prevista all'art. 30 TUEL, non prevede la costituzione di una nuova organizzazione sovraordinata: essa risulta quindi maggiormente flessibile e reversibile rispetto – ad esempio - all'Unione di Comuni e rappresenta una forma associativa largamente diffusa tra i Comuni. All'interno di questa forma di collaborazione, le funzioni vengono trasferite a uno dei soggetti partecipanti – il

cosiddetto “ente capofila”. Le Convenzioni possono essere strette tra enti locali (Comuni, Unioni, Comunità Montane, Province) e altri enti pubblici (società partecipate, Agenzie territoriali, Aziende ospedaliere, e così via).

Per quanto concerne la gestione del digitale, solitamente il RTD e l'Ufficio ICT associato vengono istituiti presso l'ente “capofila”, il quale esplica le attività concorrenti a tali funzioni, raccordandosi con il personale individuato presso gli altri enti per l'esecuzione delle strategie di trasformazione digitale. A questo ente possono essere trasferite delle unità di personale dagli enti convenzionati. A causa della struttura fortemente decentrata delle Convenzioni, è necessario stabilire modelli e occasioni di raccordo e coordinamento fra gli enti.

Proprio per la molteplicità di enti che possono essere coinvolti nello strumento della Convenzione, la competenza di un Ufficio ICT associato può essere molto diversificata ed estesa, al punto che esso può divenire un punto di riferimento territoriale per la transizione digitale, specie in situazioni periferiche e fortemente frammentate. È il caso, ad esempio, di alcuni Centri Servizi Territoriali che vedono gli enti “capofila” individuati nelle Province o nei Comuni capoluogo. Gestiscono il ciclo di vita dei servizi digitali, dalla definizione del fabbisogno, al coordinamento dello sviluppo/acquisizione, fino alla manutenzione ed evoluzione, a favore di ampie platee di enti garantendo una coerenza di attuazione delle strategie di trasformazione digitale e una forte omogeneità territoriale.

1.1.5. I FATTORI ABILITANTI AI SISTEMI INTERCOMUNALI SULLA DIGITALIZZAZIONE

Nel seguito sono presentati i principali fattori critici che possono garantire maggiore successo e longevità ai sistemi intercomunali incentrati sul digitale.

- Forme associative già in essere su funzioni diverse dalla trasformazione digitale possono essere strumenti utili per sviluppare collaborazioni in materia ICT, facendo leva su strumenti amministrativi e modelli organizzativi associativi già esistenti e su un legame di fiducia fra gli enti.
- Dimensione dell'associazione superiore a 20.000 abitanti, dimensione minima utile per garantire efficienza negli acquisti di beni e servizi, nell'acquisizione e gestione del personale dedicato, negli investimenti e nella gestione di soluzioni e infrastrutture IT.
- Un ente leader della collaborazione, spesso individuabile nel capofila di una gestione del servizio in Convenzione o fra i Comuni relativamente più grandi della media di quelli associati in Unione, può avere un ruolo utile nel creare i presupposti organizzativi e tecnologici per l'avvio dei processi di associazionismo, nel gestire il processo di cambiamento, fino alla assunzione delle responsabilità di gestione a regime della trasformazione digitale.
- Il presidio politico è presupposto per lo sviluppo dell'associazionismo dell'IT, in quanto favorisce forme di collaborazione con altri enti e di delega delle attività. Tale evidenza è rafforzata dai casi in cui siano presenti Assessori con delega all'innovazione e alla digitalizzazione con esperienza e *background* tecnico.
- Gli enti sovraordinati, con specifico riferimento alle Regioni, attraverso normative/documenti di indirizzo e gruppi di lavoro dedicati a supportare la trasformazione digitale, possono favorire e accompagnare lo sviluppo di collaborazioni strutturate, vincolando gli enti ad adottare modelli associativi – in termini di strumenti amministrativi, area territoriale e attività delegate – di successo.
- L'omogeneità dei software gestionali tra enti è un fattore che può favorire la gestione associata dell'IT, in quanto garantisce una semplificazione gestionale, economicità e la riduzione delle tempistiche di centralizzazione dei servizi.
- Iniziativa propria degli enti, le collaborazioni di successo hanno maggiore consistenza e prospettiva quando originano da un'iniziativa dei membri stessi, in quanto espressione di una esigenza percepita e di un percorso di sviluppo consapevole.

1.2. ORGANIZZAZIONE DEI SISTEMI INTERCOMUNALI CON GESTIONE ASSOCIATA

La dinamica di avvio e sviluppo delle gestioni associate sull'ICT sono dipendenti dalla storicità (o meno) della forma di cooperazione, dall'ampiezza delle funzioni gestite, dalla struttura di governance, dal livello di delega e integrazione fra gli enti.

Di seguito viene proposta una schematizzazione delle fasi "tipo" di evoluzione della gestione associata del digitale, ovvero a) ricognizione del fabbisogno digitale degli enti, b) progettazione e c) implementazione tecnologica, gestionale e organizzativa, d) gestione e consolidamento delle attività di pertinenza dell'Ufficio ICT associato ed e) diffusione e ampliamento della forma associativa.



Figura 14 - Fasi "tipo" del percorso evolutivo dei sistemi intercomunalizzati

a) Ricognizione

La fase di ricognizione consiste nell'analisi del fabbisogno di trasformazione digitale degli enti e della fattibilità di associare la funzione ICT. In questa fase l'Unione, il Consorzio o l'ente "capofila" si occupano di approfondire, prevalentemente, questi aspetti:

- la digitalizzazione dei servizi;
- gli applicativi utilizzati;
- il grado di interoperabilità dei dati;
- le competenze digitali del personale;
- l'adozione di piattaforme e la dotazione di infrastrutture;
- la connettività;
- i processi e l'organizzazione.

b) Progettazione

Dopo la fase di approfondimento, viene definito il processo di associazione della funzione ICT e progettata la gestione associata, sotto gli aspetti:

- tecnologici: l'Unione, il Consorzio o l'ente capofila valuta le azioni di adeguamento tecnologico (es. omogeneizzazione applicativi, introduzione applicativi laddove non in uso, migrazione dei dati, adozione delle piattaforme etc.).
- gestionali: nel caso delle Unioni, viene valutata l'opportunità di associare la funzione ICT contestualmente ad altri servizi e/o funzioni. A questo segue la stipula degli accordi con gli enti locali per la cessione delle funzioni, a valle della quale avviene il trasferimento delle funzioni, con l'adozione del relativo modello di ripartizione dei costi. Vengono inoltre stabilite la governance e le modalità di raccordo con gli enti per le attività specifiche delegate all'Ufficio ICT associato.
- organizzativi: la progettazione della gestione associata dell'ICT per gli enti afferenti può comportare la possibilità di migrare la funzione ICT verso un ufficio centralizzato, con la contestuale adozione di personale, e relativi ruoli, e risorse, con l'eventuale trasferimento e riallocazione di unità di personale dai Comuni verso l'Unione, il Consorzio o l'ente "capofila".

c) Implementazione

In questa fase, coerentemente con la pianificazione, si attua il processo di associazione della funzione ICT. In questa fase, coerentemente con la pianificazione, si attua il processo di associazione della funzione ICT. Vengono quindi adottati i nuovi regolamenti, conferiti gli incarichi e individuati i referenti di ciascun ente.

In caso di organizzazioni già esistenti, la nomina del RTD può trovarsi sia a valle che a monte del processo. Nel primo caso sarà la risultanza del compimento dell'associazione della funzione ICT, mentre nel secondo caso sarà proprio questa figura a guidare il processo di associazionismo.

d) Gestione

Completata la fase di associazione della funzione ICT, vengono attuate le strategie e le azioni di trasformazione digitale degli enti, coerentemente con lo stato dell'arte rilevato, i bisogni locali e gli obiettivi regionali e nazionali. Le attività sono monitorate e aggiornate sulla base del loro svolgimento congiunto con gli enti associati.

e) Espansione

Consolidata la gestione associata dell'ICT, la collaborazione può espandersi verso: altre attività, funzioni potenzialmente associabili ed eventualmente altri enti. Nelle Unioni, in particolare, la funzione del digitale può naturalmente svilupparsi trasversalmente ai diversi servizi comunali, che possono quindi gradualmente essere gestiti in maniera associata. Convenzioni e Consorzi possono agevolmente estendere la collaborazione a nuovi enti, e diventare dunque dei punti di riferimento per la trasformazione digitale delle amministrazioni coinvolte.

1.3. LE COMMUNITY E LA COLLABORAZIONE SUL DIGITALE

Le *community* di innovazione sono gruppi di condivisione di esperienze, progetti e soluzioni digitali tra enti pubblici di diversi livelli e ambiti territoriali. Queste non sono disciplinate dalla normativa e di caratterizzano per un elevato grado di libertà di partecipazione e adesione. Esse nascono con l'obiettivo di favorire l'innovazione e la trasformazione digitale della PA, sfruttando le opportunità offerte dalle tecnologie e dalle reti di relazioni, rispondendo alla necessità degli enti locali, specialmente i più piccoli, di avere accesso a conoscenze e competenze ottimizzando le risorse esistenti e di svolgere progetti ambiziosi di lungo periodo.

Una fattispecie particolare delle *community* di innovazione sono le *community* di riuso, ovvero reti di conoscenza e collaborazione tra le PA che adottano delle soluzioni software condivise e aperte. Il riuso di software è infatti una modalità di acquisizione e cessione di soluzioni digitali, prevista dal CAD, che prevede la possibilità di riutilizzare gratuitamente software già sviluppati da altre amministrazioni con vantaggi in termini di risparmio, efficienza, interoperabilità e trasparenza.

La *community* di riuso può estendersi fino a diventare un vero e proprio "*living lab*", uno spazio di confronto e sperimentazione tra i membri, che permetta di ampliare la soluzione a nuovi scenari e bisogni, come ad esempio quelli legati ad altre comunità sul territorio. Il cuore del riuso si costituisce nello sviluppo e arricchimento del cosiddetto "kit di riuso", ovvero un pacchetto di linee guida, codice, dati e documentazione che permette ai riusanti di adottare e personalizzare la soluzione in base alle proprie esigenze. Gli enti riusanti, nella logica della collaborazione tipica delle *community*, si impegnano a contribuire all'evoluzione della soluzione adottata arricchendo, a loro volta, il "kit di riuso".

I vantaggi che le *community* fanno registrare sono riconducibili a: diffusione di soluzioni standardizzate per gli enti aderenti, manutenzione continua del software, quali l'aggiornamento tecnico e normativo, l'assistenza agli enti riusanti.

Nel seguito sono presentati i principali fattori che possono determinare il successo, in termini di capacità di coinvolgimento e di longevità, delle *community*:

1. **Governance:** le *community* devono avere obiettivi ben delineati e una struttura di responsabilità chiara al loro interno, favorendo anche sinergie tra il settore pubblico e il settore privato, coinvolgendo ove possibile anche attori quali università, centri di ricerca, imprese, associazioni, cittadini etc... Infine, le *community* devono avere un ente garante, che possa svolgere il ruolo di coordinatore, facilitatore, promotore e valutatore delle attività della *community*. Le *community* con una struttura e una rete di rapporti consolidata tende a intensificare le relazioni e i risultati facendo leva su un sistema di *accountability*.
2. **Orientamento al risultato:** le *community* devono avere un piano di lavoro definito e strutturato, che definisca responsabilità e risultati attesi. Le *community* devono inoltre condividere i risultati raggiunti, sia internamente che esternamente, attraverso strumenti di comunicazione e di disseminazione adeguati, attraverso attività di sensibilizzazione e di coinvolgimento degli stakeholder. Laddove le *community* concorrono alla realizzazione di una strategia di lungo periodo, coerente con le prescrizioni regionali e nazionali, tendono ad avere una maggiore longevità e capacità di coinvolgimento.
3. **Risorse:** le *community* devono disporre di risorse adeguate a svolgere le proprie attività, sia in termini materiali che di personale, messo a disposizione dagli enti partecipanti, con particolare riferimento all'ente garante. Le *community* con maggiori finanziamenti, anche regionali, e con competenze più specifiche tendono riescono a raggiungere più efficacemente gli obiettivi di innovazione digitale.
4. **Organizzazione e gestione:** l'organizzazione interna deve essere chiara e funzionale, prevedendo al contempo una divisione delle competenze e delle responsabilità tra gli enti afferenti e tra le persone coinvolte. Le *community* devono inoltre avere una *mission* concreta e realistica, che possa guidare le scelte e le azioni verso il raggiungimento degli obiettivi prefissati. Una piattaforma online, che possa facilitare la condivisione di informazioni, documenti, codici, feedback etc., e, infine, un'assistenza tecnica da parte della *community* stessa e/o dall'ente garante, che possa fornire supporto ai partecipanti.

1.4. QUALIFICAZIONE DEI CENTRI SERVIZI SUL DIGITALE

Il modello di cooperazione per la gestione dell'ICT degli enti locali può prevedere il coinvolgimento di strutture tecniche di servizio, con particolare riferimento a quelli di piccole e medie dimensioni. Tali strutture possono fornire competenze manageriali e tecniche necessarie a orientare e supportare gli enti, assumendo un ruolo attivo nel supporto nella definizione e attuazione delle strategie di trasformazione digitale, e come erogatori di servizi.

Le attività svolte dai centri servizi sono riassumibili in:

- pianificazione e monitoraggio: analizzare le strategie di trasformazione digitale locali, nazionali ed europee e definizione e monitoraggio di piani coerenti per gli enti territoriali di riferimento;
- informazione: comunicare e aggiornare gli enti territoriali di riferimento di novità normative, di evoluzioni del mercato, presenza di opportunità, etc.;
- formazione: attivare percorsi di *assessment* e di potenziamento delle competenze digitali del personale degli enti, stimolando uno scambio reciproco permanente di conoscenza tra enti di pari o diverso ordine;
- scambio di buone pratiche: *scouting*, qualificazione e circolazione di prassi organizzative e tecnologiche;

- coordinamento di comunità tematiche: coordinare le attività dei tavoli di lavoro attivati su specifiche tematiche in ambito ICT;
- aggregazione della domanda e dei bisogni: avere una visione panoramica dei fabbisogni e delle esigenze territoriali svolgendo procedure di acquisto di beni e servizi aggregate;
- fornitura di semi-lavorati: alla luce della conoscenza in ambito ICT, predisporre linee guida, bozze, schemi *et similia* (ad es. regolamenti, atti) a supporto delle attività di trasformazione digitale e di erogazione dei servizi;
- erogazione diretta di servizi: fornire servizi digitali a favore degli enti territoriali;
- gestione di progetti: supporto al coordinamento e all'attuazione di progetti di trasformazione digitale, soprattutto quelli di particolare complessità tecnica e amministrativa;
- accesso a finanziamenti: strutturare Uffici Finanziamenti in grado di attuare: ricognizione delle esigenze di finanziamento, *scouting* finanziamenti, supporto alla creazione di partenariati, supporto alla predisposizione della documentazione di gara, project management e rendicontazione di progetti finanziati in ambito ICT.

Nel seguito sono indicati alcuni preliminari elementi di qualificazione organizzativa e gestionale dei centri servizi che possono guidare la loro individuazione, prescindendo dalla loro natura istituzionale e dal loro livello di maturità (ovvero il divario fra la configurazione ottimale e quella attuale). Alcuni di questi elementi di qualificazione sono da considerarsi (a) imprescindibili: il possesso di questi è una condizione necessaria per il riconoscimento dello status di centro servizi. Altri elementi sono invece (b) acquisibili: ciò significa che l'ente – potenziale centro servizi – può integrarli progressivamente nel proprio spettro di competenze.

Macro-requisiti	Requisiti organizzativi e gestionali	Elemento di qualificazione imprescindibile vs. acquisibile
Allineamento di strategia	Aver adottato linee di azione, piani, programmi, provvedimenti (anche normativi) ad hoc riferiti all'ICT	IMPRESCINDIBILE
Possesso delle competenze ICT	Esperienza pregressa in ICT: dimostrabile approfondita e consolidata conoscenza del tema (es. informazione / formazione; linee guida; regolamenti; aver attivato/contribuito a progetti inerenti all'ICT per enti terzi)	IMPRESCINDIBILE
Possesso delle competenze ICT	Competenze interne in ICT: possesso di competenze interne ridondanti (più persone posseggono le medesime competenze, per evitare che la fuoriuscita di una persona causi il venire meno di competenze critiche per la collaborazione)	IMPRESCINDIBILE
Possesso delle competenze ICT	Capacità di mantenere e sviluppare competenze in ICT: processi consolidati di aggiornamento e sviluppo delle competenze	IMPRESCINDIBILE
Possesso delle competenze ICT	Capacità di promuovere ed erogare azioni di disseminazione riferite al tema ICT	ACQUISIBILE
Organizzazione	Possesso di adeguate risorse umane e infrastrutturali: dimensionamento delle risorse umane coerente con le attività del centro servizi	IMPRESCINDIBILE
Organizzazione	Capacità di procurement: processi di approvvigionamento di beni, servizi e professionisti strutturati in grado di intervenire in maniera tempestiva e attingendo a un mercato ampio	IMPRESCINDIBILE
Networking	Possesso e coerente ampiezza di relazioni con enti: esistenza di relazioni strutturate e formalizzate con enti, anche in ambiti diversi dall'ICT	IMPRESCINDIBILE
Networking	Adeguatezza dell'ampiezza dell'ambito territoriale di riferimento	ACQUISIBILE
Networking	Gestione della <i>community</i> : possesso di modelli e strumenti di gestione delle relazioni con altri enti per lo sviluppo congiunto di iniziative su ICT	ACQUISIBILE
Networking	Conoscenza e rapporti con soggetti con competenze in ICT: consapevolezza dei detentori di conoscenze a livello nazionale ed europeo e (eventuale) collaborazione pregressa	IMPRESCINDIBILE
Knowledge management	Gestione della conoscenza: adozione di modelli e strumenti (es. piattaforme collaborative) per la gestione e lo sviluppo di conoscenza	ACQUISIBILE

Tabella 4 - Elementi di qualificazione organizzativa e gestionale dei centri servizi sul digitale.

1.5. ALLEGATO A - STATO DELL'ARTE DELL'ASSOCIAZIONISMO ICT E BENEFICI

La maggiore concentrazione di Unioni di Comuni aventi una gestione associata dell'ICT si trova nell'area nordorientale e nella fascia di abitanti superiore ai 50.000 (Dati di Open Italiae (<https://openitaliae.it/>), elaborazione di Politecnico di Milano, 2023). Nel Nord-est, infatti, oltre la metà delle Unioni ha associato la funzione ICT, mentre nelle altre aree la percentuale non supera il

18%. Delle Unioni con oltre 50.000 abitanti, il 45% gestisce la funzione ICT in forma associata mentre per le altre fasce di popolazione la percentuale è inferiore al 17%. (figura 15).

L'area nordorientale potrebbe catturare l'effetto prodotto da politiche regionali, le quali ricoprono potenzialmente un ruolo determinante nel ciclo di vita delle Unioni attraverso, ad esempio, regolamentazioni *ad hoc* e sistemi di incentivazione volti a promuovere l'associazionismo intercomunale tramite premialità basate sul numero di funzioni svolte in forma associata o su altri aspetti rilevanti.

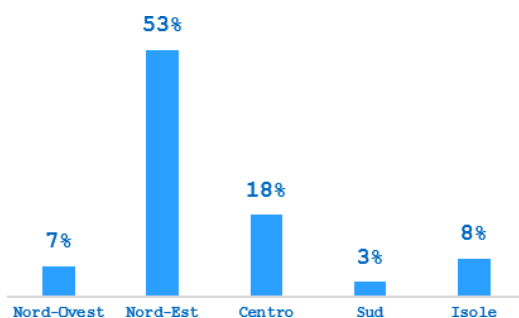


Figura 15- Percentuale di Unioni con ICT associato sul totale delle Unioni dell'area

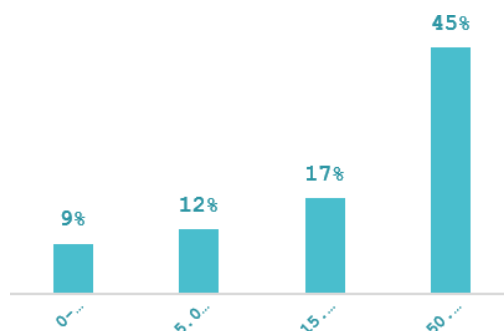


Figura 16 - Percentuale di Unioni con ICT associato sul totale delle Unioni della stessa classe dimensionale

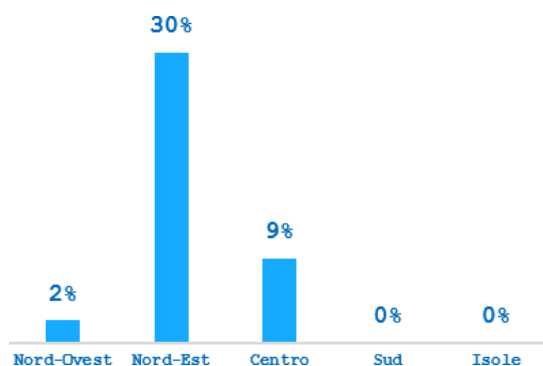


Figura 17 -Percentuale di Unioni con ICT e RTD associati sul totale delle Unioni dell'area

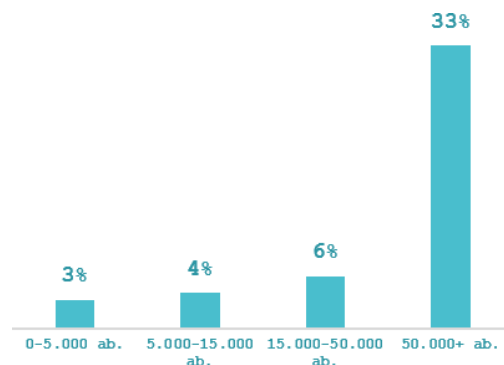


Figura 18 - Percentuale di Unioni con ICT e RTD associati sul totale delle Unioni della stessa classe dimensionale

Le tendenze legate all'area nordorientale e alla fascia di abitanti al di sopra dei 50.000 abitanti sono ricorrenti anche su funzioni associate ulteriori rispetto all'ICT. Nello specifico, le Unioni del Nord-est svolgono mediamente più funzioni e servizi in forma associata rispetto a quelle di altre aree geografiche del Paese. Oltre al contesto regionale, si rileva che le Unioni con oltre 50.000 abitanti e con meno di 5.000 abitanti sono quelle che mediamente gestiscono in forma associata il maggior numero di funzioni e servizi (figura 19). Si legga questo dato alla luce del fatto che le Unioni con meno di 5.000 abitanti sono costituite in media da soli 4 Comuni, mentre nelle Unioni di classe dimensionale pari a 5.000-15.000, 15.000-50.000 e oltre 50.000 abitanti ve ne sono, in media, rispettivamente 6, 8 e 9. Le Unioni al di sotto di 5.000 abitanti risultano, quindi, composte da Comuni di più piccole dimensioni, tipicamente più in sofferenza nella gestione delle funzioni e, dall'altro lato, il ridotto numero di enti aderenti può comportare minori sforzi di governance rispetto ad aggregazioni più ampie.

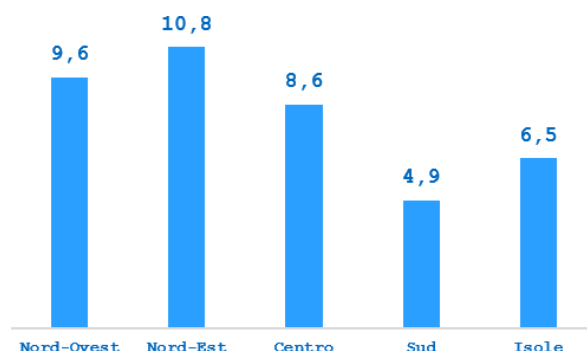


Figura 19 - Numero medio di funzioni associate per area geografica

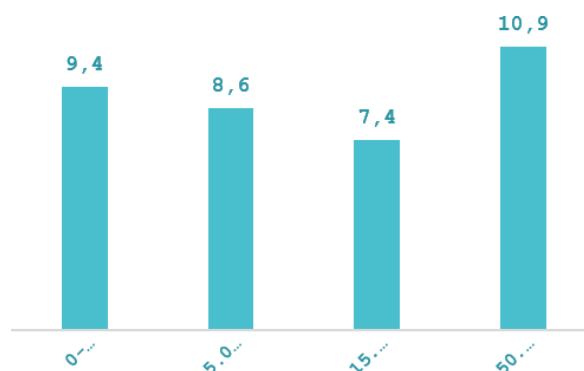


Figura 20 - Numero medio di funzioni associate per classe dimensionale

L'associazionismo intercomunale sul digitale risulta correlato al numero di altre funzioni associate. In particolar modo, nella figura sottostante si può osservare che le Unioni con ICT e RTD gestiti in forma associata tendono ad avere un numero medio di altre funzioni associate maggiore rispetto alle Unioni che non collaborano sul digitale. Si tratta infatti di 18,2 funzioni associate contro le 7,2 delle Unioni senza ICT o senza RTD associati (figura 21).

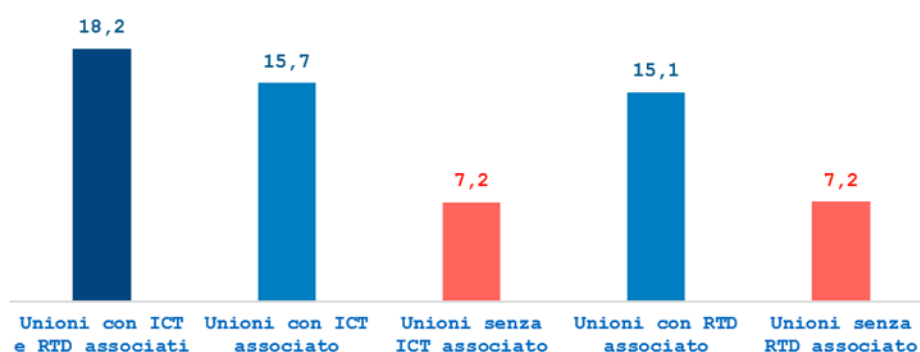


Figura 21 - Numero medio di funzioni associate. Elaborazione di Politecnico di Milano su dati di Open Italiae, 2023

Si può quindi concludere che alle Unioni con maggiore integrazione del digitale corrisponde anche un numero medio superiore di altre funzioni associate, il che suggerisce che la gestione associata del digitale – data la sua natura trasversale rispetto ad altre funzioni – sia capace di promuovere collaborazioni anche su altri ambiti di competenza degli enti locali.

La pratica della gestione associata dell'ICT, tuttavia, ha spazi di ampliamento e sviluppo. Nel caso specifico delle Unioni di Comuni, essa ricorre in meno di 1 Unione su 5 (Dati di Open Italiae (<https://openitaliae.it/>), elaborazione di Politecnico di Milano, 2023 – figura 22) e la diffusione di tale pratica non è omogenea sul territorio ma risulta piuttosto concentrata in specifici contesti geografici. Oltre il 50% delle Unioni di Comuni o Comunità Montane attualmente attive sono situate nelle aree geografiche del Nord-ovest e Nord-est del Paese (Dati di Open Italiae (<https://openitaliae.it/>), elaborazione di Politecnico di Milano, 2023).

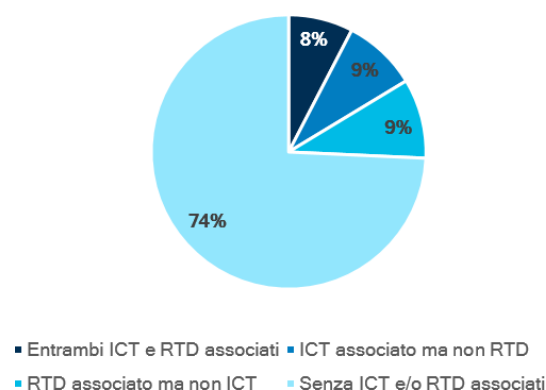


Figura 22 - Diffusione della gestione associata del digitale nelle Unioni di Comuni. Elaborazione di Politecnico di Milano su dati di Open Italiae, 2023

La gestione associata dell'ICT è foriera di benefici, maggiormente rilevabili negli enti di più piccole dimensioni. Questa è capace di favorire un maggior livello di digitalizzazione e efficienza di spesa, espressa come minore spesa pro capite in ICT.

I Comuni più piccoli, nonostante uno scarso livello di digitalizzazione, spendono relativamente molto di più dei Comuni di maggiori dimensioni, i quali raggiungono anche livelli di maturità digitale più elevati. Questo fattore è probabilmente dovuto alle economie di scala che i Comuni di medio-grandi dimensioni riescono a sfruttare. Oltre un certo numero di abitanti, la spesa torna nuovamente ad aumentare, a fronte di una maggior complessità gestionale e organizzativa da gestire. In questi casi, tuttavia la maggiore strutturazione consente agli enti di ottenere anche più elevati livelli di maturità digitale.

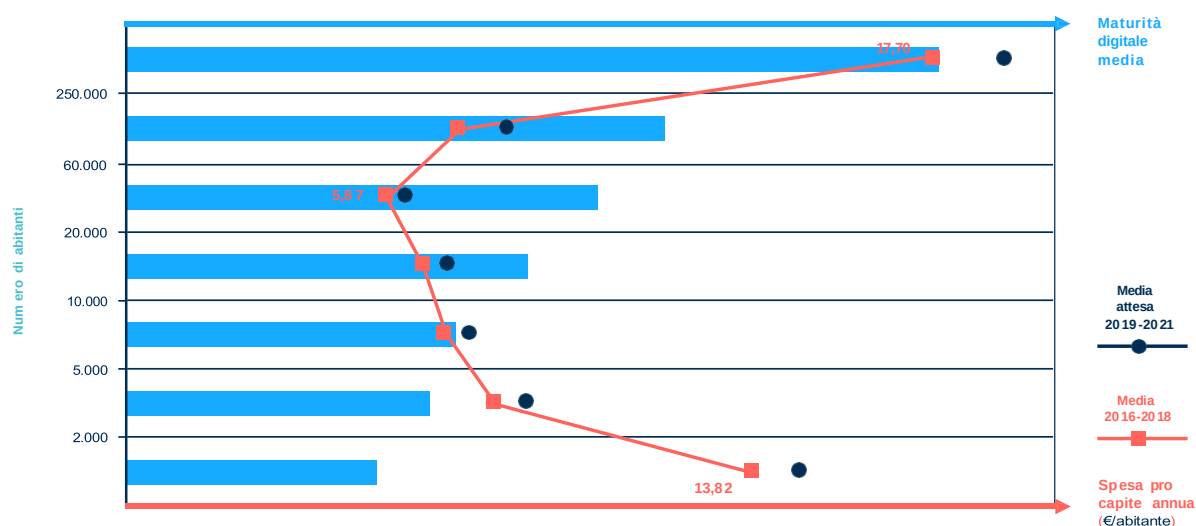


Figura 23 - Distribuzione della spesa pro capite annuale in soluzioni digitali per densità abitativa a fine 2019. Elaborazione dell'Osservatorio Agenda Digitale da Corte dei Conti, 2019

Una governance del digitale che vede il coinvolgimento di più enti, dunque, rappresenta potenzialmente una leva che le PA locali hanno a disposizione per “simulare” il comportamento di enti di maggiori dimensioni, col beneficio di velocizzare e rendere sostenibile il loro processo di trasformazione digitale.

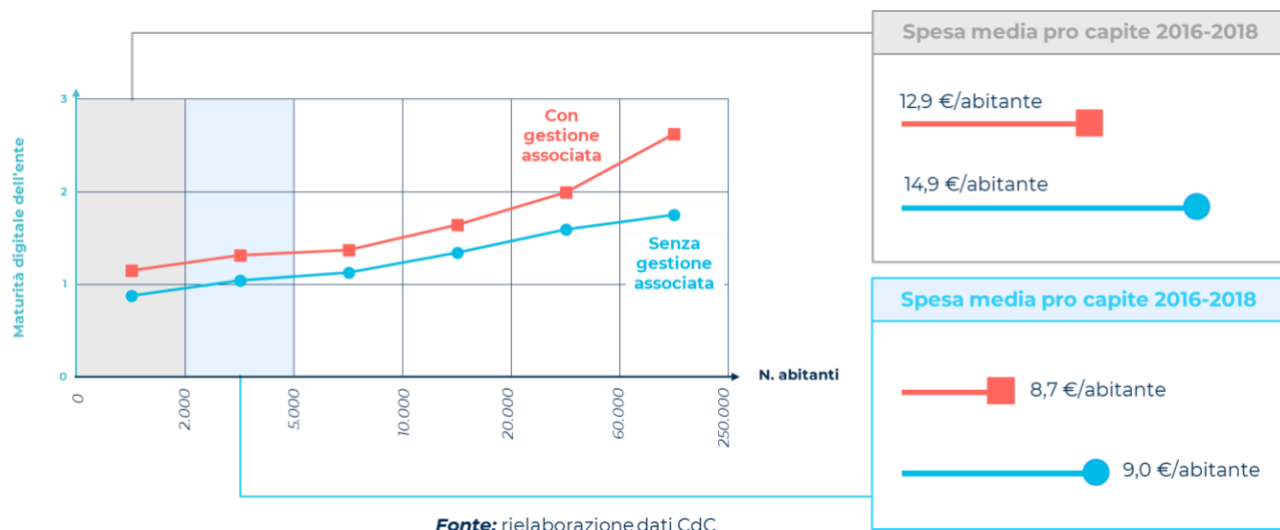


Figura 24 - Gestione associata e spesa in ICT nei Comuni per fasce dimensionali. Elaborazione dell'Osservatorio Agenda Digitale Politecnico di Milano da Corte dei Conti, 2019

Inoltre, i Comuni in Unione tendono a mostrare più frequentemente alti livelli di digitalizzazione dei servizi: la percentuale di Comuni in Unione con *front-office* dei servizi digitalizzati tende a superare quella dei Comuni *non* appartenenti a forme associative, soprattutto nei servizi rivolti alle imprese. Tale differenza è ancor più netta se si confrontano i Comuni appartenenti alla fascia fino a 5.000 abitanti (ad esempio, +23% nel *front-office* del SUAP; +19% nel *front-office* del SUE). Inoltre, i Comuni che gestiscono l'ICT in forma associata in Unione hanno il back-office dei servizi digitalizzato più frequentemente dei Comuni non appartenenti a Unioni o Comunità Montane (differenza media di circa +25%).

Questi dati sembrano indicare che l'appartenenza a una Unione di Comuni e la gestione associata dell'ICT in Unione possano influire positivamente sul livello di digitalizzazione dei Comuni, soprattutto per quelli più piccoli, e dunque anche favorire il rispetto della digitalizzazione di servizi determinato da normative (e.g. SUAP). Questo è dovuto sicuramente alla possibilità degli enti, o l'*obbligatorietà* nel caso dei Comuni più piccoli, di delegare la titolarità e l'esercizio delle funzioni legate al digitale a una entità con maggiori competenze, con il beneficio atteso di una maggiore omogeneizzazione dei sistemi e una razionalizzazione nell'utilizzo delle risorse.

Infine, i Comuni percepiscono due principali vantaggi legati alla gestione associata del digitale: da un lato essa contribuisce a una migliore allocazione interna delle risorse umane degli enti, dall'altro aumenta le competenze e l'efficienza nella selezione, nell'acquisto e nella gestione di beni e servizi digitali.



Figura 25 - Percentuale di Comuni con front-office digitalizzato – Dati Osservatorio Agenda Digitale Politecnico di Milano



Figura 26 - Percentuale di Comuni con meno di 5.000 abitanti con front-office digitalizzato – Dati Osservatorio Agenda Digitale Politecnico di Milano



Figura 27 - Percentuale di Comuni con back-office digitalizzato – Dati Osservatorio Agenda Digitale Politecnico di Milano

1.6. RIFERIMENTI

- [1] (2020). [Linee guida acquisizione e riuso software PA](#).
- [2] Codice dell'Amministrazione Digitale. (s.d.). art. 69 . *Riuso delle soluzioni e standard aperti*.
- [3] Commissione Europea. (2023). [Collections](#)
- [4] Corte dei Conti - Sezione delle autonomie . (2019). Questionario per la valutazione dello stato di attuazione del Piano Triennale per l'informatica nella PA.
- [5] Dipartimento per la Trasformazione Digitale e AGID. (s.d.). [Catalogo Software](#)
- [6] Enti locali italiani. (2022). "Un modello per quantificare i benefici del riuso". (P. d., Intervistatore)
- [7] Mola, A. (2020). *Ecosistema MyP3*. Regione del Veneto - Direzione ICT e Agenda Digitale.
- [8] Osservatorio Agenda Digitale. (2019). *Gestione associata e spesa pro-capite*. Milano: Politecnico di Milano.
- [9] Osservatorio Agenda Digitale. (2022). *Diffusione e benefici del riuso. La digitalizzazione e il riuso: una panoramica dagli enti locali* (p. 35-59). Milano: Politecnico di Milano .
- [10] Politecnico di Milano. (2023, Agosto). *Interviste a sistemi intercomunali*.
- [11] Politecnico di Milano. (2023). *Questionario sulla digitalizzazione degli enti locali*.
- [12] Provincia di Lecco . (2022). [La Provincia di Lecco promuove e coordina la gestione di un Centro Servizi Territoriale \(CST\) di ambito sovracomunale](#).
- [13] Regione Umbria. (2022). [Puntozero](#).
- [14] Tozzi, Q., Carocci, G., & Labella, B. (2011). Capitolo 2. Cos'è una buona pratica. In *Buone pratiche per la sicurezza in sanità. Manuale pratico per la rappresentazione, la valutazione e la diffusione* (p. 39-44). Il Pensiero Scientifico Editore.
- [15] Tramontano, L. (2021). *Manuale di diritto degli enti locali*. Santarcangelo di Romagna (RN): Maggioli.
- [16] Umbria Digitale. (2019). *La buona pratica S.I.SO Sistema Informativo SOciale - condivisione delle esperienze e scenari*. Perugia.

Strumento 3 - Servizi prioritari secondo l'eGovernment benchmark

Versione 1.0 del 21/12/2023

I. Obiettivo

Il documento fornisce i principi di base per l'individuazione e l'implementazione dei servizi digitali "prioritari" secondo l'eGovernment Action Plan Benchmark.

II. Destinatari

Pubbliche amministrazioni ed enti strumentali che erogano servizi digitali per conto delle pubbliche amministrazioni.

III. Crediti

Il documento è stato redatto in collaborazione con il Dipartimento per la Trasformazione Digitale.

1.7. EGOVERNMENT BENCHMARK

L'*eGovernment benchmark* è il principale strumento di monitoraggio utilizzato dall'Unione Europea per verificare il raggiungimento degli obiettivi del Decennio Digitale europeo.

L'*eGovernment benchmark* ha l'obiettivo di misurare il livello di maturità tecnologica e lo stato di digitalizzazione dei servizi pubblici di tutti i Paesi Membri e costituisce uno strumento fondamentale fornendo linee guida e individuando le "*best practice*" a livello europeo.

Il Benchmark riflette gli obiettivi dell'Unione Europea condivisi nella Dichiarazione di Tallinn del 2017, che ha definito le linee d'azione per la creazione di un mercato unico digitale (ivi compreso il monitoraggio tramite l'*eGovernment benchmark*) e all'interno della Dichiarazione di Berlino del 2020 con cui gli Stati Membri si sono impegnati a fondare il concetto stesso di governo digitale sull'inclusione dei cittadini e sulla creazione di un ambiente digitale sostenibile e rispettoso dei principi etici.

L'*eGovernment benchmark* Framework è un importante strumento che valuta l'integrazione e la presenza di alcune caratteristiche peculiari dei servizi digitali pubblici per verificarne affidabilità, efficienza ed efficacia per gli utenti.

I servizi digitali offerti ai cittadini che sono oggetto del monitoraggio effettuato dall'*eGovernment* vengono valutati in base a quattro "dimensioni chiave" che si compongono da quattordici indicatori totali. Le dimensioni chiave sono le seguenti:

- centralità dell'utente
- trasparenza
- disponibilità transfrontaliera
- fattori chiave abilitanti

ossia le precondizioni tecniche per la fornitura dei servizi digitali.

La Commissione Europea ogni anno effettua test su un campione di servizi, nazionali e locali, e stila una classifica dei paesi più virtuosi. Al fine di valutare tutti gli indicatori, l'*eGovernment benchmark* utilizza i cosiddetti "mystery shoppers", cittadini europei che, a seguito di specifica formazione, e sulla base di un sistema di criteri predefiniti, valutano la qualità dei servizi digitali disponibili in ogni stato membro comportandosi esattamente come potenziali utenti.

Con riferimento alla performance relativa ai servizi offerti ai cittadini transfrontalieri, Il "*Single Digital Gateway*" (Sportello Digitale Unico), permetterà a cittadini e imprese di accedere più facilmente alle informazioni, alle procedure e ai servizi di assistenza in diversi settori del mercato interno, consentendo, conseguentemente, lo sviluppo del mercato unico digitale.

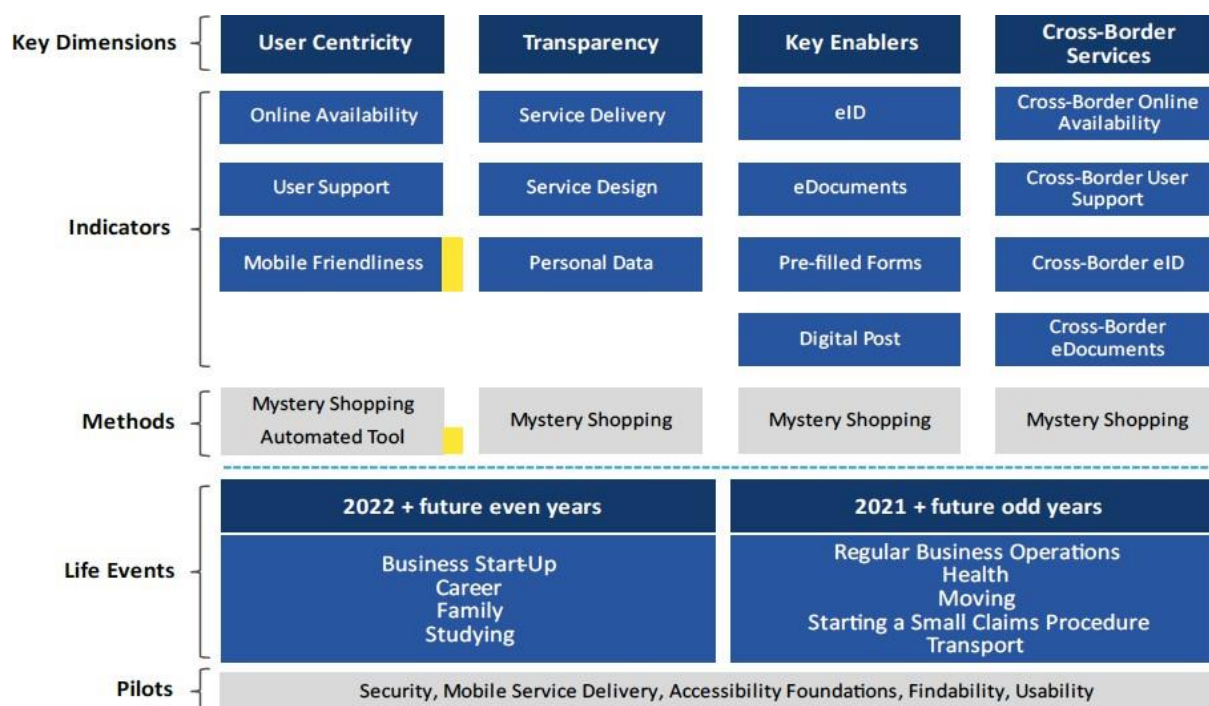


Figura 28 - eGovernment benchmark Framework

1.8. EGOVERNMENT BENCHMARK E DESI

Alcuni degli indicatori dell'eGovernment benchmark sono inclusi all'interno del DESI (*Digital Economy and Society Index*), in particolare l'eGovernment benchmark fornisce i dati che alimentano due dei KPI del Decennio Digitale europeo relativi ai servizi pubblici digitali: servizi pubblici digitali per i cittadini e servizi pubblici digitali per le imprese.

Id	Indicatore	Definizione	Indicatore EU 2023	Indicatore Italia 2023	Posizione su 28 Stati membri
desi_4a1	e-Government users	Persone, con età compresa tra i 16 e i 74 anni, che hanno utilizzato Internet, negli ultimi 12 mesi, per interagire con le autorità pubbliche su siti web o applicazioni mobili. (Punteggio: % utilizzatori di internet). Fonte: Eurostat – European Union survey on the use of ICT in households and by individuals (ISOC_CIEGI_AC_II_IGOVANYSI)	74,20%	76,26%	22
desi_4a2	Digital public services for citizens	La quota di procedimenti amministrativi che possono essere svolti online per i principali eventi della vita (nascita di un figlio, nuova residenza, ecc.) da parte dei cittadini (Punteggio da 0 a 100). Fonte: eGovernment benchmarking Reports (2012-2022)	77,03	67,91	21
desi_4a3	Digital public services for businesses	L'indicatore esprime la quota di servizi necessari per avviare un'impresa e condurre operazioni commerciali regolari che sono disponibili online sia per gli utenti nazionali che per quelli stranieri. I servizi erogati interamente in modalità digitale ricevono un punteggio più alto, mentre i servizi che forniscono solo informazioni (ma devono essere completati offline) ricevono un punteggio più limitato. (Punteggio da 0 a 100). Fonte: eGovernment benchmarking Reports (2012-2022)	83,73	74,71	24
desi_4a4	Pre-filled Forms	Quantità di dati precompilati nei moduli online dei servizi. (Punteggio da 0 a 100). Fonte: eGovernment benchmarking Reports (2012-2022)	68,18	47,11	24
desi_4a5	Transparency of service delivery, design and personal data	La misura in cui i processi di servizio sono trasparenti, i servizi sono progettati con il coinvolgimento degli utenti e gli utenti possono gestire i loro dati personali. (Punteggio da 0 a 100). Fonte: eGovernment benchmarking Reports (2012-2022)	64,73	49,2	25
desi_4a6	User support	La misura in cui il supporto online, le funzioni di aiuto e i meccanismi di feedback sono disponibili, anche a livello transfrontaliero. (Punteggio da 0 a 100). Fonte: eGovernment benchmarking Reports (2012-2022)	85,59	77,78	22
desi_4a7	Mobile friendliness	La misura in cui i servizi di e-government sono forniti attraverso un'interfaccia mobile-friendly, cioè, un'interfaccia che risponde al dispositivo mobile. (Punteggio da 0 a 100). Fonte: eGovernment benchmarking Reports (2012-2022)	93,27	91,4	20
desi_4b1	Access to e-health records	La misura di: (1) la disponibilità a livello nazionale di servizi di accesso online per i cittadini ai propri dati di cartelle cliniche elettroniche (tramite un portale per i pazienti o un'applicazione mobile per i pazienti) con misure aggiuntive che consentano ad alcune categorie di persone (ad esempio, tutori per i bambini, persone con disabilità, anziani) di accedere ai propri dati, e (2) la percentuale di individui che hanno la possibilità di ottenere o utilizzare il proprio set minimo di dati relativi alla salute attualmente memorizzati nei sistemi di cartelle cliniche elettroniche (EHR) pubblici e privati. (Punteggio da 0 a 100). Fonte: Digital decade e-Health indicators development report	71,71	71,32	16

Tabella 5 - Indicatori DESI riguardanti i servizi pubblici digitali, valore e posizionamento dell'Italia.

1.9. SERVIZI PRIORITARI

Il Sistema di monitoraggio dell'eGovernment benchmark per la valutazione delle prestazioni delle Istituzioni governative ha previsto quindi la predisposizione di un questionario composto da una lista di domande, per la valutazione di ognuna delle già citate dimensioni chiave, per l'assegnazione ad ogni Stato coinvolto di un punteggio complessivo per indicare il livello di maturità nel raggiungimento degli obiettivi dell'eGovernment benchmark. Si riporta la lista delle domande che compongono il

questionario, nonché dei requisiti misurati dalla Commissione relativamente ai servizi pubblici digitali.

Per misurare lo stato di avanzamento delle Pubbliche Amministrazioni, l'*eGovernment benchmark* utilizza nove momenti di vita, ovvero fasi significative nella vita di un cittadino che rappresentano occasioni di interazione tra governo e cittadini/imprese.

Nell'ambito del monitoraggio dell'*e-Government benchmark* sono individuati specifici servizi "prioritari" attraverso i quali i momenti di vita, considerati nella metodologia come classificazioni di azioni necessarie più o meno quotidiane, vengono resi operativi e funzionanti per il cittadino.

Lista dei servizi individuati e distinti per i momenti di vita a cui si riferiscono.

- Momenti della vita - Avvio d'impresa:
 - Servizi monitorati:
 - 1.1 Verificare i requisiti per avviare un'impresa
 - 1.2 Ottenere indicazioni su come scrivere un business plan
 - 1.3 Ottenere indicazioni su come esplorare le possibilità finanziarie
 - 2.1 Ottenere il certificato di assenza di oneri pendenti
 - 3.1 Registrazione della società per la prima volta
 - 4.1 Ottenere la carta/numero di identificazione fiscale
 - 4.2 Ottenere il numero di partita IVA
 - 5.1 Registrazione presso l'Ufficio della sicurezza sociale
 - 5.2 Ottenere indicazioni su come organizzare l'assicurazione pensionistica (obbligatoria)
 - 5.3 Chiedere indicazioni su come stipulare l'assicurazione sanitaria (obbligatoria)
 - 6.1 Registrare la propria azienda come datore di lavoro
 - 6.2 Registrare i dipendenti prima del primo giorno di lavoro
 - 6.3 Verificare gli obblighi contrattuali per l'assunzione dei dipendenti
 - 6.4 Verificare le condizioni di lavoro per l'assunzione dei dipendenti
 - 7.1 Verificare le condizioni per le autorizzazioni ambientali
 - 7.2 Ottenere il permesso di inquinamento/ambiente
- Momenti della vita - Carriera:
 - Servizi monitorati:
 - 1.1 Registrazione come disoccupato
 - 1.2 Calcolo dell'indennità di disoccupazione (durata e altezza)
 - 1.3 Richiedere l'indennità di disoccupazione
 - 1.4 Ricorso contro la decisione in caso di mancata concessione dell'indennità di disoccupazione
 - 2.1 Verificare l'ammissibilità a ulteriori indennità di disoccupazione
 - 2.2 Ottenere indicazioni su come ottenere l'indennità di alloggio
 - 2.3 Ottenere indicazioni su come organizzare una consulenza sui debiti
 - 2.4 Ottenere indicazioni su come organizzare programmi di promozione della salute
 - 2.5 Ottenere indicazioni su come organizzare l'assistenza durante l'invalidità, la malattia e gli infortuni sul lavoro
 - 2.6 Richiedere il rimborso delle tasse o di altri sussidi legati alla disoccupazione
 - 3.1 Verificare gli obblighi per il mantenimento dell'indennità di disoccupazione

- 3.2 Presentare le prove che dimostrano che si sta cercando lavoro
 - 3.3 Registrare le circostanze che impediscono la ricerca di lavoro
 - 4.1 Ottenere indicazioni su come trovare un lavoro
 - 4.2 Registrare l'occupazione per interrompere l'indennità di disoccupazione
 - 4.3 Dichiarare le imposte sul reddito personale
 - 5.1 Calcolare le pensioni future
 - 5.2 Richiedere la pensione statale
 - 5.3 Verificare il diritto alla pensione quando ci si trasferisce all'estero o si rientra da un altro Paese
- Momenti della vita - Famiglia:
 - Servizi monitorati:
 - 1.1 Verificare le condizioni per il congedo parentale
 - 1.2 Registrazione del bambino presso l'autorità competente
 - 1.3 Registrare l'autorità parentale (ad es. presso il tribunale in caso di non matrimonio)
 - 1.4 Richiedere gli assegni familiari
 - 2.1 Registrazione presso l'anagrafe civile/locale per sposarsi o chiudere un'unione civile
 - 2.2 Registrare il divorzio all'anagrafe per porre fine al matrimonio o all'unione civile.
 - 3.1 Ottenere il passaporto
 - 3.2 Ottenere il certificato di nascita
 - 4.1 Verificare i requisiti per la registrazione della morte di un parente
- Momenti della vita - Studio:
 - Servizi monitorati:
 - 1.1 Controllare i programmi di studio offerti dalle università
 - 1.2 Verificare i requisiti di ammissione per l'iscrizione all'istruzione superiore
 - 2.1 Ottenere il riconoscimento della dichiarazione di diploma
 - 2.2 Iscrivere all'istruzione superiore
 - 2.3 Richiedere le borse di studio
 - 2.4 Calcolare le possibilità finanziarie aggiuntive
 - 2.5 Richiedere prestazioni sociali aggiuntive
 - 3.1 Richiedere la portabilità della borsa di studio (all'estero)
 - 3.2 Monitorare i voti e i dati personali
 - 3.3 Ottenere indicazioni su come organizzare lo studio all'estero (ufficio internazionale)
 - 3.4 Ottenere indicazioni su come organizzare i tirocini e l'inizio della carriera
- Momenti della vita - Economia:
 - Servizi monitorati:
 - 1.1 Dichiarare l'imposta sulle società
 - 1.2 Dichiarare i contributi sociali
 - 1.3 Presentare i rapporti finanziari all'ufficio di registrazione delle imprese
 - 1.4 Trasmettere i dati aziendali agli uffici statistici
 - 2.1 Dichiarare l'IVA
 - 2.2 Richiedere il rimborso dell'IVA
 - 2.3 Ricorso contro la decisione sull'IVA
 - 3.1 Registrare la malattia di un dipendente presso l'amministrazione competente

- 3.2 Registrare la fine del contratto di un dipendente con l'autorità competente
 - 3.3 Registrazione del nuovo indirizzo presso l'autorità competente
- Momenti della vita - Salute:
 - Servizi monitorati:
 - 1.1 Ottenere indicazioni e informazioni su dove ottenere assistenza sanitaria
 - 1.2 Monitorare le informazioni online sull'iscrizione all'albo dei medici, sulle specializzazioni e sulle licenze necessarie, ecc.
 - 1.3 Ottenere la tessera europea di assicurazione malattia
 - 2.1 Registrarsi e (ri) fissare un appuntamento in ospedale
 - 2.2 Richiedere un consulto elettronico con un medico dell'ospedale (teleconsulto)
 - 2.3 Ottenere una prescrizione elettronica da un medico dell'ospedale
 - 2.4 Richiedere la cartella clinica elettronica
- Momenti della vita - Giustizia:
 - Servizi monitorati:
 - 1.1 Verificare le fasi procedurali per l'avvio di un procedimento per controversie di modesta entità
 - 1.2 Verificare la legislazione pertinente e i diritti di difesa del caso.
 - 2.1 Presentare la procedura per le controversie di modesta entità (presentare il reclamo al tribunale)
 - 2.2 Presentare prove/documenti di supporto
 - 3.1 Monitorare lo stato della causa
 - 3.2 Appello contro la decisione del tribunale
- Momenti della vita - Mobilità:
 - Servizi monitorati:
 - 1.1 Monitorare la disponibilità di strutture locali (ad es. scuole, strutture sanitarie, strutture sportive)
 - 1.2 Registrazione del nuovo indirizzo nel registro comunale
 - 1.3 Registrare il nuovo indirizzo presso altre organizzazioni
 - 1.4 Ottenere la prova di residenza
 - 1.5 Registrazione dell'uscita dal vecchio comune
 - 1.6 Richiedere il sussidio per le strutture per disabili o un beneficio simile per coprire le spese di modifica dell'abitazione al fine di continuare a vivere in modo indipendente.
 - 2.1 Verificare i diritti e i doveri per il trasferimento nel Paese
 - 2.2 Ottenere un certificato di registrazione
- Momenti della vita - Trasporti:
 - Servizi monitorati:
 - 1.1 Immatricolare un'auto usata
 - 1.2 Richiedere il sostegno del governo per un'auto ad alimentazione alternativa
 - 2.1 Ottenere un permesso di parcheggio
 - 2.2 Dichiarare la tassa di circolazione
 - 2.3 Ottenere il permesso per le strade a pedaggio o le vignette
 - 2.4 Ottenere i bollini per le emissioni
 - 3.1 Controllare le informazioni e pianificare un viaggio (con più tipi di trasporto pubblico)

- 3.2 Ottenere i biglietti del trasporto pubblico (tariffa standard)
- 3.3 Fare ricorso e chiedere il rimborso del biglietto

1.10. IL SISTEMA DI VALUTAZIONE

Il Sistema di monitoraggio dell'*eGovernment benchmark* per la valutazione delle prestazioni delle istituzioni governative ha previsto quindi la predisposizione di un questionario composto da una lista di domande, per la valutazione di ognuna delle già citate dimensioni chiave, per l'assegnazione ad ogni Stato coinvolto di un punteggio complessivo per indicare il livello di maturità nel raggiungimento degli obiettivi dell'*eGovernment benchmark*.

Lista delle domande che compongono il questionario di monitoraggio, nonché dei requisiti misurati dall'Unione europea relativamente ai servizi pubblici digitali nazionali e regionali.

- Caratteristiche monitorate - Servizi nazionali e regionali "Disponibilità online dei servizi"
 - Domande nel questionario:
 1. Le informazioni sul servizio sono disponibili online?
 2. Il servizio vero e proprio è disponibile online?
 3. Il servizio/le informazioni sul servizio è disponibile attraverso (uno dei) portali pertinenti?
 4. Il sito web fornisce un titolo descrittivo?
 5. Il sito web mostra etichette descrittive nella parte superiore della pagina per navigare verso altre (sotto) pagine?
- Caratteristiche monitorate - Servizi nazionali e regionali "Supporto all'utente (relativo al monitoraggio dei portali web)"
 - Domande nel questionario:
 1. Le FAQ sono disponibili?
 2. È disponibile una demo?
 3. È disponibile una funzionalità di supporto dal vivo?
 4. Il Dipartimento responsabile è identificato?
 5. Sono disponibili altri canali di accesso?
 6. Sono disponibili meccanismi di feedback?
 7. Esiste un forum di discussione o social media?
 8. È disponibile una procedura di reclamo?
- Caratteristiche monitorate - Servizi nazionali e regionali "Trasparenza nell'erogazione dei servizi"
 - Domande nel questionario:
 1. Si riceve una notifica di consegna del completamento della fase del processo online?
 2. Durante il servizio, i progressi vengono monitorati?
 3. Nel corso del servizio, è possibile salvare il lavoro svolto come bozza?
 4. Il sito comunica le aspettative sulla durata stimata dell'intero processo prima di iniziare il servizio?
 5. Sono chiare le tempistiche di consegna del servizio?
 6. Esiste un limite di tempo massimo entro il quale l'amministrazione deve effettuare la consegna?
 7. Sono disponibili informazioni pubbliche sulle prestazioni del servizio (di qualsiasi tipo: livelli di servizio, valutazione delle prestazioni)?

8. Quando si inserisce un campo di input in un modulo online, il sito web mostra un messaggio di errore quando l'input identificato è errato?
 9. Quando si inserisce un campo di input in un modulo online, il sito web mostra aiuti visivi e suggerimenti per compilare correttamente il modulo?
- Caratteristiche monitorate - Servizi nazionali e regionali "Trasparenza dei dati personali (relativo al monitoraggio dei portali web)"
 - Domande nel questionario:
 1. Qual è il grado di accesso online per gli utenti ai propri dati ritenuti dall'ente pubblico?
 - nessuno
 - viene data indicazione su come accedere ai propri dati offline
 - i dati sono disponibili su richiesta
 - l'utente è proattivamente informato dei dati che sono ritenuti dall'ente pubblico
 2. Appare una notifica in caso di dati personali errati?
 3. È possibile modificare i dati personali ritenuti dall'ente pubblico online?
 4. È presente una procedura di reclamo riguardante i dati?
 5. È possibile monitorare chi ha consultato i tuoi dati?
 - Caratteristiche monitorate - Servizi nazionali e regionali "Trasparenza del design del servizio (relativo al monitoraggio dei portali web)"
 - Domande nel questionario:
 1. Sono fornite informazioni sui processi chiave del policy making?
 2. Sono fornite informazioni sulla capacità dell'utente di partecipare al policy making?
 3. Sono fornite informazioni sul processo di progettazione e design del servizio?
 4. Sono fornite informazioni sulle modalità di partecipazione alla progettazione e design del servizio?
 - Caratteristiche monitorate - Servizi nazionali e regionali "Fattori chiave"
 - Domande nel questionario:
 1. È necessario un qualche tipo di autenticazione (online/offline) per accedere o ottenere il servizio?
 2. Se è necessaria un'autenticazione, è possibile autenticarsi online?
 3. Se è possibile autenticarsi online, si utilizza un identificativo elettronico generico (ad esempio una carta nazionale eID)?
 4. Se è possibile autenticarsi online per un servizio, è possibile accedere anche a un altro servizio di questo evento di vita (ma fornito da un diverso fornitore di servizi) senza dover rifare l'autenticazione?
 5. Se è possibile autenticarsi online per un servizio, si può anche decidere di utilizzare un eID privato (come il token dell'eBanking)?
 6. È necessario un qualche tipo di documentazione per accedere o ottenere il servizio?
 7. È possibile per l'utente presentare il documento richiesto dal fornitore del servizio per completare le procedure e le formalità necessarie per stabilire o svolgere una fase del processo online (certificato, diploma, prova di registrazione, ecc.)?

8. L'utente può ottenere in formato elettronico il documento che il fornitore del servizio deve fornire al destinatario del servizio per completare le procedure e le formalità necessarie per stabilire o eseguire una fase del processo online (certificato, diploma, prova di registrazione, ecc.)?
9. È necessario un qualche tipo di modulo elettronico per accedere o richiedere il servizio?
10. Quando si richiede questo servizio, i dati personali sono precompilati dal fornitore del servizio (sulla base di dati provenienti da fonti autentiche come il registro nazionale, i registri fiscali, i registri delle società, ecc.)?

Lista delle domande che compongono il questionario di monitoraggio, nonché dei requisiti misurati dall'Unione europea relativamente ai servizi pubblici digitali transfrontalieri.

- Caratteristiche monitorate Servizi Transfrontalieri “Disponibilità online dei servizi transfrontalieri”
 - Domande nel questionario:
 1. Vi sono informazioni disponibili per cittadini transfrontalieri?
 2. servizio disponibile per per cittadini transfrontalieri?
 3. Esiste una barriera nazionale relativa alla necessità di autenticarsi attraverso una eID?
 - barriera eDoc richiesto
 - barriera traduzione/riconoscimento documenti?
 - barriera problemi linguistici
 - La traduzione è poco chiara o errata
 - barriera mancanza di informazioni
 - barriera necessità di incontro faccia a faccia?
 - altre barriere
- Caratteristiche monitorate Servizi Transfrontalieri “Supporto all’utente nei servizi transfrontalieri (relativo al monitoraggio dei portali web)”
 - Domande nel questionario:
 1. Esiste una funzionalità di aiuto per cittadini transfrontalieri?
 2. Esiste un meccanismo di feedback per cittadini transfrontalieri?
 3. Esiste una procedura di reclamo per cittadini transfrontalieri?
- Caratteristiche monitorate Servizi Transfrontalieri “Fattori chiave nei servizi transfrontalieri”
 - Domande nel questionario:
 1. È necessaria un’autenticazione per accedere?
 2. L’autenticazione è richiesta tramite eID nazionale?
 3. È necessaria della documentazione per accedere?
 4. È necessario inviare un documento in forma elettronica?
 5. È necessario ottenere documento fornito dal servizio straniero

1.11. INDICAZIONI PER IL MIGLIORAMENTO DEI SERVIZI DELLA PUBBLICA AMMINISTRAZIONE

Di seguito sono elencate alcune funzionalità che dovrebbero essere integrate nel design dei servizi digitali per migliorare le performance dei servizi pubblici italiani rispetto al sistema di valutazione dell'eGovernment benchmark.

1. Utilizzo di identità digitale

Garantire l'utilizzo di identità digitali, come SPID (Sistema Pubblico di Identità Digitale) o CIE (Carta d'Identità Elettronica), per l'accesso ai servizi digitali.

2. Invio e ricezione di documenti online

Verificare la possibilità di inviare e ricevere documenti completamente online, semplificando e velocizzando le procedure amministrative.

3. Moduli pre-compilati

Garantire la presenza di moduli pre-compilati disponibili per cittadini e imprese, adottando il principio once-only, per semplificare e velocizzare le procedure amministrative.

4. Tracciamento dei Progressi

Assicurare un sistema efficace di tracciamento dei progressi relativi all'accesso al servizio, consentendo agli utenti di monitorare lo stato delle proprie attività.

5. Funzione "Save as a Draft"

Introdurre la possibilità di salvare una transazione in corso come bozza, facilitando gli utenti nell'espletamento di transazioni online più complesse.

6. Stima della durata del processo

Fornire un'indicazione chiara della durata stimata dell'intero processo transattivo, consentendo agli utenti di pianificare in modo più efficiente le proprie attività.

7. Termini di scadenza del servizio

Informare gli utenti sui termini di scadenza per la fruizione del servizio, garantendo trasparenza e chiarezza riguardo ai tempi disponibili.

8. Termine massimo di azione della PA

Specificare se la Pubblica Amministrazione ha un termine massimo entro cui agire, contribuendo a stabilire aspettative realistiche da parte degli utenti.

9. Rilascio di Notifica di Completamento

Garantire il rilascio di notifiche che confermino il completamento del servizio e della transazione effettuata.

10. Feedback sulla performance

Implementare un sistema di feedback che fornisca informazioni sulla performance del servizio, consentendo agli utenti di esprimere opinioni e suggerimenti.

Strumento 4 - Smart Area: servizi digitali territoriali avanzati

Versione 1.0 del 21/12/2023

I. Obiettivo

Il documento fornisce alcuni principi generali alle amministrazioni pubbliche che intendono dotare il proprio territorio di una infrastruttura digitale avanzata definita “Smart Area” con l’obiettivo di erogare, a cittadini e imprese servizi digitali negli ambiti: trasporti, sicurezza, risparmio energetico ed in generale per il miglioramento della qualità della vita del territorio.

II. Destinatari

Enti territoriali quali: comuni, province, città metropolitane e regioni, comunità montane, comunità isolate, unioni di comuni e consorzi fra enti territoriali.

III. Crediti

Il documento è stato redatto in collaborazione con il Comune di Modena e l’Università di Modena e Reggio Emilia sulla base dell’esperienza maturata nell’ambito del [MASA - Modena Automotive Smart Area](#).

1.12. GLOSSARIO

Smart Area

Zona territoriale dotata di una infrastruttura digitale progettata per erogare servizi finalizzati a migliorare la mobilità, la sicurezza, il risparmio energetico, la qualità ambientale e, in generale, la qualità della vita dei cittadini.

ADAS (Advanced Driver Assistance Systems).

I sistemi avanzati di assistenza alla guida sono dispositivi elettronici in grado di aumentare la sicurezza degli autoveicoli attraverso protezioni di tipo attivo. I sistemi di guida autonoma sono classificati su una scala da 0 a 5, dove 0 indica il controllo totale del veicolo da parte del guidatore e 5 rappresenta la guida completamente autonoma.

Edge computing

Modello di elaborazione dei dati che sposta la potenza di calcolo e l'elaborazione delle informazioni il più vicino possibile alla fonte dei dati. L'*Edge computing*, invece di inviare i dati a un cloud remoto per l'elaborazione, esegue le operazioni direttamente "sul campo", vicino ai dispositivi o alle sorgenti di dati. Gli *edge nodes* sono i nodi di elaborazione periferici di una architettura di edge computing.

GPU (Graphics Processing Unit)

Le Unità di Elaborazione Grafica sono processori progettati principalmente per gestire e accelerare le operazioni legate alla grafica, inclusi calcoli complessi necessari per la visualizzazione di immagini e video. Le GPU sono anche utilizzate come acceleratori computazionali in applicazioni di intelligenza artificiale e machine learning.

HPC (High-Performance Computing)

Il Calcolo ad Alte Prestazioni consente di elaborare grandi quantità di dati e risolvere problemi computazionalmente intensivi in tempi relativamente brevi. I sistemi HPC sono utilizzati per applicazioni che richiedono una notevole potenza di calcolo.

RSU (Road Side Unit)

Componente di un'infrastruttura intelligente. La RSU è un apparato installato lungo le strade che fornisce connettività e comunicazione tra i veicoli (V2V, *Vehicle-to-Vehicle*) e tra i veicoli e l'infrastruttura stradale (V2I, *Vehicle-to-Infrastructure*). Le RSU sono generalmente dotate di tecnologie di comunicazione wireless e possono essere integrate con sensori e dispositivi che supportano funzionalità per la gestione intelligente delle strade come il rilevamento del traffico o degli agenti inquinanti.

VRU (Vulnerable Road Users)

Letteralmente: Utenti Vulnerabili della Strada. Questo termine si riferisce a persone che, a causa della loro presenza sulla strada e delle loro caratteristiche fisiche, sono particolarmente esposte al rischio di incidenti stradali. Gli utenti vulnerabili della strada includono: disabili, bambini, anziani, pedoni, ciclisti, motociclisti scooteristi, utilizzatori di veicoli leggeri.

V2X o V2I

Comunicazione bidirezionale tra veicoli connessi ed elementi della città e della mobilità

1.13. PRINCIPI GENERALI

1.13.1. INFRASTRUTTURA

Una *Smart Area* è una zona urbana dotata di una avanzata infrastruttura digitale progettata per erogare servizi a cittadini e imprese al fine di migliorare e ottimizzare diversi aspetti della vita urbana. Le componenti chiave di questa infrastruttura includono:

- Connettività avanzata
 - o Connettività *Wired*: Utilizza fibre ottiche per garantire una connessione ad alta velocità e affidabile, facilitando la trasmissione rapida di dati.
 - o Connettività *Wireless*: sfrutta tecnologie come ad esempio 4G, 5G, LoRa e 4G *Narrowband* per fornire reti wireless efficienti e accessibili, consentendo la connessione di dispositivi e servizi in modo rapido e flessibile.
- Sensoristica avanzata
 - o Sensori in tempo reale (Smart Camera): integra telecamere intelligenti e dispositivi in grado di catturare e analizzare istantaneamente informazioni visive, migliorando la sorveglianza, la sicurezza e fornendo dati immediati su eventi o situazioni specifiche.
 - o Sensori non in tempo reale (sensori ambientali, contatori): include dispositivi di rilevamento ambientale e contatori che monitorano vari parametri nel corso del tempo. Questi sensori forniscono dati utili per analisi a lungo termine, consentendo la valutazione delle condizioni ambientali, dei flussi di persone o di altri parametri specifici.
- Elaborazione avanzata
 - o Elaborazione ad alte prestazioni (HPC e GPU): sfrutta potenti sistemi di elaborazione per gestire complessi calcoli e analisi dati ad alta velocità, consentendo una risposta rapida e una gestione efficiente delle informazioni.
 - o *Nodi Edge e Data Center*: Implementa nodi di elaborazione distribuiti sul territorio (edge nodes) e centri di dati centralizzati per gestire la raccolta, l'elaborazione e lo stoccaggio dati. Questa architettura consente una distribuzione efficiente delle risorse di calcolo, riducendo la latenza e ottimizzando la gestione delle informazioni.

L'integrazione di queste tecnologie in una Smart Area contribuisce a creare un ambiente urbano più sicuro e connesso, migliorando la qualità della vita dei cittadini e consentendo l'innovazione nei servizi urbani.

Le tecnologie impiegate consentono anche la comunicazione bidirezionale tra elementi della città e della mobilità, come pedoni e ciclisti, con veicoli dotati di dispositivi ADAS di livello 3 e 4 (V2X).

Tra le possibili tecnologie impiegate nella Smart Area, si citano ad esempio le telecamere intelligenti per il riconoscimento di ostacoli, operanti con software di intelligenza artificiale, e sistemi di video analisi per implementare soluzioni di "*Smart Parking*".

Le amministrazioni sono tenute a gestire le informazioni raccolte da una infrastruttura di tipo Smart Area garantendone l'anonimato, nel rispetto della normativa vigente, al fine di preservare la privacy dei cittadini.

1.14. CASI D'USO

Di seguito sono delineati alcuni casi d'uso realizzabili in una Smart Area, sulla base dell'esperienza del MASA.

1.14.1. PARCHEGGIO INTELLIGENTE (*SMART PARKING*)

Un insieme di unità intelligenti ("*Road side unit*" RSU) distribuite nella Smart Area è in grado di identificare in tempo reale gli spazi liberi, distinguendo le aree adibite a spazio di sosta. Le informazioni sulla disponibilità dei parcheggi sono istantaneamente comunicate agli utenti attraverso un'app dedicata. Il sistema fornisce le informazioni necessarie per il servizio di prenotazione dei parcheggi, e consente l'ottimizzazione del flusso del traffico, semplificando la ricerca di aree di sosta.

1.14.2. PARCHEGGIO AUTOMATICO (*VALET PARKING*)

Parcheggio automatico (*valet parking*). Le telecamere intelligenti della Smart Area consentono di raccogliere metadati utili a potenziare il sistema di percezione dei veicoli a guida autonoma consentendo operazioni di parcheggio automatico.

1.14.3. RILEVAMENTO OSTACOLI (*OBSTACLE DETECTION*)

Il sistema di unità intelligenti ("*road side unit*") è in grado di individuare in tempo reale la presenza di ostacoli e soggetti vulnerabili (VRU) presenti nell'area monitorata. Il sistema individua, segue, classifica e geolocalizza con precisione i veicoli e pedoni, comunicando in tempo reale tali informazioni a guidatori e mezzi dotati di una app dedicata. Inoltre, tali informazioni migliorano i sistemi di percezione dei veicoli dotati di ADAS. L'applicazione consente di aumentare la sicurezza stradale e di ridurre il rischio di incidenti legati alla presenza di ostacoli e pedoni in angoli ciechi del veicolo, la presenza di pedoni che sorraggiungono dietro autobus e veicoli di grandi dimensioni, incroci pericolosi a scarsa visibilità.

1.14.4. STRADE VERDI (*GREEN ROUTES*)

I dati raccolti in tempo reale consentono di schedare al meglio le velocità dei veicoli al fine di ottimizzare traffico, consumo di carburante, rischio. I suggerimenti di guida sono inoltrati dall'infrastruttura ai veicoli e ai guidatori mediante una apposita app. Le informazioni raccolte possono essere utilizzate nello scheduling delle temporizzazioni semaforiche e la gestione attiva del traffico attraverso "*smart semaphore*" controllabili dal sistema. L'infrastruttura consente di introdurre veicoli a guida autonoma/assistita come agenti per la regolazione del traffico.

1.14.5. ANALISI DEI FLUSSI DI TRAFFICO (*TRAFFIC FLOW ANALYSIS*).

L'infrastruttura della Smart Area consente di registrare con elevata frequenza (il MASE fino a 10 volte al secondo) la posizione di tutti i veicoli e pedoni presenti nell'area monitorata alimentando un database a granularità molto fine per l'analisi di traffico. Tali informazioni dettagliate forniscono uno strumento fondamentale per la stesura dei piani urbani di mobilità.

1.14.6. ANALISI DELL'INQUINAMENTO (*POLLUTION ANALYSIS*)

L'inserimento nelle “*road side unit*” di sensori per l'analisi degli agenti inquinanti (PM2.5, PM10, T/H e VOC/NOx) consente di correlare i dati di traffico con le emissioni inquinanti ed il loro impatto a breve e lungo termine. Tali dati permettono di fornire ai veicoli e ai conducenti informazioni per ottimizzare lo stile di guida al fine di ridurre gli agenti inquinanti. Inoltre, i dati raccolti possono alimentare un sistema per la limitazione selettiva degli accessi alle zone maggiormente sensibili in termini di traffico e di inquinamento. La disponibilità di tali dati offre l'opportunità di sviluppare applicazioni avanzate ed innovative. Nel contesto del MASA è in fase di valutazione la creazione di un'applicazione che utilizza la gamification per promuovere comportamenti virtuosi, ad esempio fornendo accesso a Zone a Traffico Limitato (ZTL) e sconti sui parcheggi come incentivi.

1.14.7. GUIDA CONNESSA (*CONNECTED DRIVE V2V, V2X*).

Le “*road side unit*” possono integrare i sistemi di comunicazione mobile attraverso soluzioni a basso costo che coprono l'eterogeneità dei protocolli: C-V2X, DSRC, WiFi, 4/5G/LTE. Ciò consente di poter valutare la migliore soluzione tecnologica per la comunicazione V2X in relazione a facilità di installazione, costi, latenze, banda e programmabilità.

1.14.8. GUIDA AUTONOMA (*AUTONOMOUS DRIVING*)

L'infrastruttura Smart Area consente di sperimentare applicazioni avanzate e innovative nell'ambito della guida autonoma. Un esempio sono i sistemi di planning che regolano la velocità e la traiettoria del veicolo dotato di ADAS in relazione alla confidenza di percezione dell'ambiente circostante. Questi strumenti sono utili nei casi in cui il veicolo non sia in grado di valutare cosa ci sia dietro ad un ostacolo, un autobus, un incrocio. L'infrastruttura Smart Area può fornire al sistema di guida autonoma informazioni utili a valutare il rischio di una determinata manovra, la velocità opportuna e la distanza di sicurezza da mantenere.

1.15. STRATEGIE DI IMPLEMENTAZIONE PER UNA SMART AREA: LINEE GUIDA GENERALI

L'implementazione di una Smart Area da parte di una pubblica amministrazione richiede una pianificazione integrata e l'attuazione di diverse fasi. Di seguito sono fornite alcune linee guida generali:

- Analisi delle esigenze e coinvolgimento degli stakeholder:
 - o Identificare le esigenze della comunità e delle aziende locali ed individuare i casi d'uso.
 - o Coinvolgere gli stakeholder chiave, tra cui cittadini, imprese, organizzazioni non profit e altri attori locali.
- Pianificazione Strategica
 - o Stabilire obiettivi chiari e misurabili per il progetto.
 - o Sviluppare una visione a lungo termine per la Smart Area.
 - o Stabilire un budget iniziale accurato considerando i costi associati all'acquisizione e all'installazione di tecnologie, sviluppo software, manutenzione, formazione del personale.
 - o Esplorare opportunità di finanziamento attraverso finanziamenti nazionali e comunitari ([Funding for cities](#), [Smart Cities Marketplace](#)), partnership pubblico-privato.

- Considerare le opportunità offerte dal programma di procurement innovativo [Smarter Italy](#).
- Infrastruttura tecnologica:
 - Valutare e implementare l'infrastruttura tecnologica necessaria, inclusi sensori, reti di comunicazione, piattaforme software.
- Connettività
 - Assicurarsi di avere una connettività affidabile e veloce per supportare le tecnologie Smart Area.
- Sicurezza dei dati:
 - Garantire la sicurezza dei dati raccolti e implementare misure adeguate di protezione della privacy.
- Applicazioni e servizi
 - Sviluppare applicazioni che abbiano un impatto immediato sulla qualità della vita dei cittadini.
- Collaborazione e standard:
 - Collaborare con altre amministrazioni, aziende private e organizzazioni per favorire l'adozione di standard comuni.
- Monitoraggio e valutazione:
 - Implementare sistemi di monitoraggio e valutazione per misurare l'impatto del progetto e apportare eventuali miglioramenti.
- Aggiornamenti continui
 - Essere pronti ad aggiornare e migliorare costantemente il progetto in base all'evoluzione delle tecnologie e delle esigenze della comunità.

Queste linee guida possono variare a seconda delle specifiche esigenze e delle caratteristiche dell'amministrazione e del territorio coinvolto, ma forniscono una base per un approccio strategico all'implementazione

Strumento 5 - Intelligenza Artificiale nella Pubblica Amministrazione

Versione 1.0 del 21/12/2023

I. Obiettivo

Il documento fornisce indicazioni operative per l'adozione dell'Intelligenza Artificiale basate sull'esperienza pratica per l'implementazione delle tecnologie di IA nella Pubblica Amministrazione.

II. Destinatari

Pubbliche amministrazioni ed enti strumentali che erogano servizi digitali per conto delle pubbliche amministrazioni.

III. Crediti

Il documento è stato redatto con il contributo di Consorzio Interuniversitario Nazionale per l'Informatica (CINI), INAIL, ISTAT, INPS.

1.16. AI ACT: UN APPROCCIO BASATO SUL RISCHIO

L'AI Act intende stabilire obblighi per fornitori e utenti per mitigare i rischi legati all'utilizzo dell'IA. I rischi sono classificati in quattro diversi livelli: rischio inaccettabile (divieto), rischio elevato, rischio limitato e rischio minimo.

A titolo informativo si riportano di seguito i profili di rischio previsti dal testo dell'AI Act emendato il 14 giugno 2023. In attesa dell'emanazione del regolamento tale classificazione può essere considerata una utile guida per le pubbliche amministrazioni che hanno intenzione di dotarsi di sistemi di intelligenza artificiale.

L'AI Act considera una minaccia per le persone e quindi vieta i sistemi di intelligenza artificiale a rischio inaccettabile. Essi comprendono:

- Manipolazione cognitiva comportamentale di persone o di specifici gruppi vulnerabili: ad esempio giocattoli ad attivazione vocale che incoraggiano i bambini a comportamenti pericolosi;
- Social scoring: classificazione delle persone in base al comportamento, allo status socio-economico o alle caratteristiche personali.
- Sistemi di identificazione biometrica in tempo reale e a distanza, come il riconoscimento facciale.

Possono essere ammesse alcune eccezioni. Ad esempio, i sistemi di identificazione biometrica "ex-post", in cui l'identificazione avviene dopo un ritardo significativo, saranno consentiti per perseguire reati gravi, ma solo dopo l'approvazione delle autorità giudiziarie.

L'AI Act considera ad alto rischio i sistemi di IA che possono avere conseguenze negativamente sulla sicurezza o sui diritti fondamentali dell'uomo. La proposta di regolamento individua due categorie di sistemi ad alto rischio:

1. sistemi di intelligenza artificiale utilizzati in prodotti che rientrano nella legislazione dell'UE sulla sicurezza dei prodotti. Si tratta di giocattoli, velivoli, automobili, dispositivi medici e ascensori.
2. sistemi di intelligenza artificiale che rientrano in otto aree specifiche e che dovranno essere registrati in un database dell'UE:
 - identificazione biometrica e categorizzazione delle persone fisiche
 - gestione e funzionamento di infrastrutture critiche
 - istruzione e formazione professionale
 - occupazione, gestione dei lavoratori e accesso al lavoro autonomo
 - accesso e fruizione di servizi privati essenziali e di servizi e prestazioni pubbliche
 - pubblica sicurezza
 - migrazione, asilo e controllo delle frontiere
 - interpretazione giuridica e applicazione della legge.

Tutti i sistemi di IA ad alto rischio dovranno essere valutati sia prima di essere immessi sul mercato sia durante il loro ciclo di vita.

Nel corso dell'iter di definizione del regolamento sono stati anche introdotti alcuni requisiti minimi di trasparenza per l'IA generativa, che dovrebbero:

- rivelare che il contenuto è stato generato dall'IA;

- progettare il modello per evitare che generi contenuti illegali;
- pubblicare riepiloghi dei dati protetti da diritto di autore e utilizzati per l'addestramento.

Secondo l'AI Act i sistemi di IA a rischio limitato dovrebbero soddisfare requisiti minimi di trasparenza che consentano agli utenti di prendere decisioni informate. Dopo aver interagito con le applicazioni, l'utente può decidere se continuare a utilizzarle. In generale, gli utenti devono essere informati quando interagiscono con l'IA. Ciò include i sistemi di IA che generano o manipolano contenuti di immagini, audio o video.

1.17. LA VISIONE DEL LABORATORIO ARTIFICIAL INTELLIGENCE AND INTELLIGENT SYSTEMS (AIIS) DEL CINI

Un'adozione efficace e conforme alla normativa di strumenti di Intelligenza Artificiale (AI) all'interno della Pubblica Amministrazione (PA) richiede un'attenta navigazione nel panorama legislativo corrente e una previsione strategica delle evoluzioni future in questo ambito.

Il contesto normativo attuale mostra un crescente interesse e una serie di iniziative di regolamentazione dell'AI ancora in divenire. Con l'avvento di tecnologie sempre più avanzate, si rende necessario un quadro normativo che ne guidi l'uso responsabile e etico.

Normative come l'imminente AI Act, e il GDPR (*General Data Protection Regulation*), rappresentano elementi imprescindibili in questo percorso, ponendo delle basi per la gestione dei dati e l'uso delle tecnologie AI.

Strategicamente, l'adozione dell'AI nella PA deve essere allineata con gli obiettivi a lungo termine dell'amministrazione digitale, che includono la digitalizzazione dei servizi, l'aumento dell'efficienza amministrativa e la promozione di una governance trasparente e accessibile. L'AI può giocare un ruolo cruciale in queste aree, migliorando la capacità di analisi dei dati, automatizzando processi e offrendo nuovi servizi ai cittadini. Per raggiungere questi risultati, la PA deve garantire che i sistemi di AI adottati siano affidabili, controllati da adeguate procedure di gestione del rischio, privi di implicazioni etiche e sociali negative.

1.18. POSSIBILI OBIETTIVI

Tenuto conto delle incertezze e della rapida evoluzione del contesto, nel breve periodo occorre partire da una fase di acquisizione sistematica di conoscenze che poi dovrà essere seguita negli anni successivi da un approccio operativo. In questa ottica, vengono individuati tre obiettivi principali.

1.18.1. ACQUISIZIONE DI CONOSCENZE E STRUMENTI PER L'ANALISI DEL RISCHIO NELL'ADOZIONE DI STRUMENTI DI AI

L'acquisizione di conoscenze e strumenti per l'analisi del rischio nell'adozione di strumenti di Intelligenza Artificiale (AI) è un pilastro fondamentale per la Pubblica Amministrazione nel contesto attuale, dove l'AI Act e altre normative emergenti pongono l'accento sulla gestione dei rischi associati all'utilizzo dell'AI. Questo impegno si concentra non solo sulla comprensione dei potenziali pericoli, ma anche sulle modalità di interazione con questi sistemi avanzati, riconoscendo che il carattere dei rischi può variare significativamente a seconda delle specifiche applicazioni dell'AI.

L'analisi del rischio nell'AI, in linea con le direttive dell'AI Act, prevede un'attenta valutazione che va oltre la semplice identificazione delle criticità. Questo processo richiede una comprensione approfondita delle diverse categorie di rischio stabilite dalla normativa, che a loro volta implicano diversi livelli di controllo e monitoraggio. L'essenza di questo approccio risiede nel riconoscere che

ogni applicazione dell'AI possiede caratteristiche uniche e, di conseguenza, richiede una strategia su misura per gestire i rischi ad essa associati.

Un elemento chiave per il raggiungimento di questo obiettivo è la formazione e l'aggiornamento continuo delle competenze all'interno delle amministrazioni pubbliche. Ciò implica non solo dotare i dipendenti delle conoscenze tecniche necessarie per comprendere e gestire i rischi dell'AI, ma anche sviluppare una cultura organizzativa che promuova la consapevolezza e la responsabilità nei confronti di questi nuovi sistemi tecnologici. In questo senso, l'analisi del rischio diventa un processo dinamico, che evolve con il progresso tecnologico e l'accumulo di nuove esperienze e conoscenze nel campo dell'AI.

1.18.2. ACQUISIZIONE DI CONOSCENZE SUI PRINCIPALI STANDARD INTERNAZIONALI APPLICABILI A PRODOTTI E SERVIZI BASATI SU AI

L'AI è un campo in rapida evoluzione, e con esso, anche gli standard internazionali che ne governano l'uso. È fondamentale che le amministrazioni siano consapevoli di questi standard per assicurare che i prodotti e i servizi che adottano o sviluppano siano ad essi conformi. In particolare, gli standard su AI del CEN-CENELEC, l'organismo europeo di standardizzazione, specificheranno i criteri di conformità, anche in relazione all'AI Act.

Inoltre, è fondamentale la conoscenza anche degli standard internazionali come ISO/IEC 20546 (*Big Data - Overview and Vocabulary*) e ISO/IEC 22989 (*AI - Artificial Intelligence Concepts and Terminology*). L'attuazione di procedure di valutazione e di revisione standardizzate sono elementi imprescindibili per assicurare che le soluzioni AI rispettino gli standard internazionali e siano eticamente responsabili.

1.18.3. ANALISI E GESTIONE DEI DATI DA UTILIZZARE IN APPLICAZIONI BASATE SU AI

I dati rappresentano l'elemento centrale per la realizzazione di applicazioni basate su metodi di apprendimento automatico. Per ottenere strumenti che rispondano alle esigenze e la cui introduzione sia sicura ed affidabile sia sotto il profilo strettamente tecnico, che sotto il profilo sociale, i dati che alimentano il sistema di AI devono soddisfare dei requisiti di qualità.

Conoscere tali requisiti è un presupposto fondamentale per affrontare lo sviluppo di sistemi AI. Diversi sono gli aspetti da considerare per garantire la qualità dei dati, che sono fortemente legati al contesto applicativo e pertanto richiedono da parte delle PA un approfondimento che consenta di calare, nel proprio dominio operativo, indicazioni di carattere generale come Analisi di Rappresentatività dei Dati, Prevenzione e Identificazione dei Bias, Protezione della Privacy, ecc. Queste indicazioni si aggiungono alle indicazioni da seguire per qualsiasi applicazione informatica e che includono, tra l'altro, la standardizzazione della raccolta dati, la loro affidabilità e coerenza, e la verifica e pulizia, ottenuta attraverso processi volti ad eliminare errori e inesattezze.

1.19. SUGGERIMENTI PER LE AZIONI DIRETTE ALLE PA

1.19.1. PREDISPOSIZIONE DI STRUMENTI PER L'ANALISI DEL RISCHIO

In un'era dove l'Intelligenza Artificiale (AI) si sta rapidamente integrando nelle strutture della Pubblica Amministrazione (PA), la predisposizione di strumenti efficaci per l'analisi del rischio diventa un aspetto cruciale. AGID, DTD e altri soggetti istituzionali sono chiamati a svolgere un ruolo fondamentale in questo processo, fornendo alle amministrazioni gli strumenti necessari per navigare con sicurezza nel complesso panorama dell'AI.

Questa missione richiede non solo la creazione di risorse adatte, ma anche l'attuazione di una formazione mirata e di un supporto continuo. La sfida sta nel bilanciare innovazione e sicurezza, garantendo che l'adozione dell'AI nella PA avvenga in un ambiente controllato e consapevole dei potenziali rischi e benefici.

Alcune possibili azioni includono:

- **Creazione di strumenti per l'analisi del rischio:** tali strumenti dovranno includere modelli, linee guida e best practices. Gli strumenti in questione devono essere adattabili alle esigenze di diverse dimensioni e tipologie di PA.
- **Formazione e Supporto:** Sulla base di questi strumenti, offrire formazione e supporto tecnico alle amministrazioni per un loro uso efficace.
- **Aggiornamento Continuo:** Mantenere gli strumenti aggiornati con le ultime ricerche e sviluppi nel campo dell'AI.

1.19.2. SVILUPPO DI METODOLOGIE E PROCEDURE DI VALUTAZIONE PER APPLICAZIONI AI

L'implementazione di metodologie e procedure di valutazione per le applicazioni AI rappresenta un tassello fondamentale nella strategia di digitalizzazione della PA. A seguito dell'introduzione dell'AI Act, si dovrà assicurare che le PA siano pienamente equipaggiate per valutare e gestire le applicazioni AI in conformità con le normative vigenti. Questo compito richiede una profonda comprensione dei principi etici e legali che governano l'uso dell'AI, oltre alla capacità di tradurre queste conoscenze in pratiche operative concrete.

L'obiettivo è di creare un ambiente in cui l'AI possa essere utilizzata in modo efficace e responsabile, massimizzando i benefici per la società pur rispettando rigorosi standard di sicurezza e etica.

Alcune possibili azioni includono:

- **Guida sull'AI Act:** Fornire una guida chiara e dettagliata sull'applicazione dell'AI Act, aiutando le amministrazioni a comprendere e aderire ai requisiti normativi.
- **Workshop e Seminari:** Organizzare incontri formativi per discutere l'interpretazione e l'implementazione dell'AI Act ai diversi settori della PA.
- **Strumenti di Autovalutazione:** Creare strumenti che permettano alle amministrazioni di condurre valutazioni interne.

1.19.3. ASSICURARE LINEE GUIDA SULLA RACCOLTA E IL TRATTAMENTO DI DATI FINALIZZATI ALL'UTILIZZO IN SISTEMI AI

Creare e implementare un insieme di linee guida robuste per la raccolta e il trattamento dei dati all'interno della Pubblica Amministrazione. Queste linee guida dovranno mirare a garantire che i dati utilizzati come training per sistemi di Intelligenza Artificiale (AI) siano di alta qualità, privi di bias, rappresentativi della popolazione e trattati nel pieno rispetto della privacy.

1.19.4. PROGETTAZIONE E ADOZIONE DI UN PIANO DI COMPETENZE PER L'AI

I.1. Mappatura delle competenze necessarie

- Eseguire una dettagliata analisi delle competenze necessarie per implementare e gestire efficacemente l'AI nella PA.
- Identificare specifiche abilità tecniche, gestionali ed etiche richieste.

- **Differenziazione tra competenze in-house e esternalizzate**
 - Valutare quali competenze possono essere sviluppate internamente e quali richiedono l'apporto di esperti esterni.
 - Stabilire un equilibrio tra le risorse interne e l'outsourcing per ottimizzare l'efficienza e l'efficacia.
- **Messa in atto di un programma di upskilling**
 - Implementare programmi formativi per aggiornare le competenze del personale esistente.
 - Organizzare workshop, corsi di formazione e partnership con istituzioni accademiche e aziende del settore.

1.19.4.1. COMPETENZE CHIAVE DA COPRIRE:

- Innovation manager esperto di AI: professionista con visione strategica e competenze tecniche per guidare l'introduzione dell'AI.
- Ethics officer: specialista incaricato di assicurare che l'uso dell'AI sia conforme ai principi etici e legali.
- Esperto di apprendimento automatico e Intelligenza Artificiale: tecnico qualificato per lo sviluppo e la gestione di soluzioni basate su AI.
- Esperto di dati: professionista focalizzato sulla gestione, analisi e sicurezza dei dati.

1.19.5. PROGETTAZIONE E ADOZIONE DI UN PIANO DEI FABBISOGNI

- Individuazione dei servizi e dei processi da valorizzare con sistemi di AI
 - Identificare aree specifiche dove l'AI può migliorare l'efficienza, la precisione e l'efficacia dei servizi pubblici.
 - Priorizzare i processi che possono trarre maggior beneficio dall'integrazione con l'AI.
- Individuazione dei dati e verifica della qualità
 - Selezionare set di dati pertinenti per le applicazioni AI.
 - Assicurare che i dati siano di alta qualità, rappresentativi e privi di bias.
- Individuazione delle implicazioni etiche e legali
 - Analizzare le implicazioni etiche e legali dell'uso dell'AI nei servizi pubblici.
 - Assicurare che ogni implementazione sia in linea con le normative vigenti e rispetti i principi etici fondamentali.

1.20. L'ESPERIENZA DI INAIL

In un contesto in continua evoluzione, l'adozione di tecnologie basate sull'intelligenza Artificiale da parte dell'Istituto Nazionale contro gli Infortuni sul Lavoro (INAIL) si presenta come un obiettivo strategico di primaria importanza sia per migliorare la propria organizzazione interna che per erogare servizi avanzati ai cittadini.

In questo capitolo sono analizzate come INAIL le sfide, le opportunità e i benefici derivanti dai progetti di IA dell'INAIL, quali siano le prospettive future in questo ambito e i progetti attualmente in corso. Nel contesto dell'organizzazione e dei processi, INAIL si è dotata di un modello maturo di Open Innovation per gestire le innovazioni e i cambiamenti che avverranno nei prossimi mesi, anche dal punto di vista legislativo. L'introduzione dell'AI Act, infatti, comporterà adeguamenti normativi per l'INAIL sia come fornitore che come utente di soluzioni IA. Per questo è prevista l'integrazione di un framework di governance dell'IA all'esistente quadro di governance del dato e la revisione di processi e

prassi già esistenti per garantire la conformità legale ed etica lungo tutto il ciclo di vita delle soluzioni IA.

1.20.1. IL PERCORSO DI INAIL NEL MONDO DELL'IA

L'Intelligenza Artificiale (IA) sta rivoluzionando il mondo grazie alla rapida e immediata disponibilità di soluzioni che permettono di automatizzare ed efficientare un'ampia gamma di processi. Anche INAIL ha avviato da tempo un percorso di adozione di tali tecnologie, nell'ottica di abilitare nuove opportunità e benefici.

Le soluzioni di IA dell'INAIL coprono una vasta gamma di ambiti e settori, di conseguenza le scelte di applicazione dell'IA sono state effettuate con una specifica coerenza strategica rispetto agli obiettivi prefissati. Gli ambiti coperti variano quindi dall'assistenza virtuale ad utenti esterni attraverso l'impiego di chatbot ad hoc, ai servizi di monitoraggio e analisi dei ticket, a strumenti avanzati per la selezione di pubblicazioni scientifiche e la raccolta automatica di dati provenienti da repository specializzati. La presenza di applicativi predittivi che analizzano dati su rischi e incidenti, inoltre, sottolinea la chiara missione dell'INAIL nella promozione e sensibilizzazione sui temi della sicurezza sul lavoro e del benessere dei lavoratori. In generale, l'INAIL si è focalizzato sul valorizzare al meglio il proprio patrimonio informativo potenziando le capacità di analisi e ricerca sui dati e sviluppando di conseguenza soluzioni custom mediante linguaggi come *Phyton*, in integrazione a prodotti di mercato.

Si riportano di seguito, aggregate in funzione dei principali benefici per area di riferimento, le più significative attività progettuali in corso.

1. Miglioramento dell'Efficienza Operativa e Pianificazione

L'IA può automatizzare processi operativi complessi, migliorando l'efficienza nella gestione dei dati, nelle operazioni quotidiane e nelle pratiche amministrative. Ciò consente di risparmiare tempo e risorse, ridistribuendo le attività in modo più adeguato. In tale contesto, INAIL ha avviato numerosi progetti volti ad introdurre l'IA per migliorare l'operatività. Si citano l'utilizzo di sistemi analitico-predittivi per la definizione di un modello di *what-if analysis* focalizzato sulle politiche del personale e l'utilizzo di analoghi strumenti per la gestione del bilancio tecnico attuariale, mediante una soluzione che consente di produrre il bilancio di previsione dell'INAIL per un periodo futuro fino a 30-50-90 anni.

2. Sensibilizzazione, formazione e analisi dei Dati per la Prevenzione degli Infortuni

L'analisi predittiva basata sull'IA può essere utilizzata per esaminare grandi dataset e identificare modelli che potrebbero prevedere potenziali rischi di infortuni. Questo può dunque contribuire a sviluppare strategie di sensibilizzazione, formazione e prevenzione più efficaci o interventi mirati in ambito; in tale ottica sono stati avviati progetti che prevedono l'adozione di sistemi cognitivi per l'analisi dei dati afferenti agli infortuni mortali, i quasi incidenti e gli infortuni su strada.

3. Gestione delle Richieste e dei Reclami

Chatbot addestrati dall'IA attraverso tecniche di Machine Learning sono in fase di implementazione per gestire le richieste e i reclami degli utenti, fornendo loro risposte immediate e migliorandone l'esperienza complessiva; tali strumenti abilitano altresì la riqualificazione dell'attività del personale interno, favorendone la riallocazione verso attività a maggior valore aggiunto.

4. Automazione nell'Elaborazione delle Prestazioni e nella gestione dei Bandi

L'IA viene utilizzata per automatizzare la gestione dei bandi e delle prestazioni, accelerando i processi e riducendo gli errori manuali. Si cita in tal senso l'utilizzo di sistemi cognitivi e di IA

per facilitare ed efficientare i processi interni ed esterni delle procedure dei Bandi ISI attraverso l'implementazione di un Assistente Personale verso gli utenti, l'Analisi dei documenti amministrativi e tecnici ISI, e la classificazione documentale per fornire *alert* alle imprese in fase di caricamento.

5. Analisi dei Dati Medici

L'IA può essere applicata all'analisi dei dati medici per migliorare la valutazione delle condizioni di salute dei lavoratori, contribuendo a una valutazione più accurata delle richieste di indennizzo. Per trarre il beneficio sono in corso di sviluppo un modello di Machine Learning che supporta il medico nella valutazione del danno rispetto ai dati relativi all'infortunio, ed un sistema cognitivo per la ricerca di pareri simili secondo entità e concetti presenti nei referti. È inoltre attiva una progettualità legata all'utilizzo di sistemi cognitivi e di IA per la lavorazione dei pareri della Consulenza tecnica in materia di valutazione dei fattori di rischio correlati all'insorgenza e al riconoscimento delle malattie professionali.

6. Rilevamento di Frodi

L'IA può essere impiegata per identificare modelli sospetti o anomalie nei dati, contribuendo alla prevenzione delle frodi legate alle richieste di indennizzo. Anche in questo caso l'INAIL ha avviato e completato, fra gli altri, un progetto per la revisione delle anomalie nel flusso di gestione delle pratiche, attraverso suggerimenti intelligenti via Machine Learning, allo scopo di identificare e prevenire attività fraudolente e individuare anomalie di processo.

7. Evoluzione e Personalizzazione dei Servizi in funzione della customer experience

Per intercettare al meglio le esigenze e il livello di soddisfazione degli utenti, è da anni utilizzata l'IA per realizzare un modello di classificazione, annotazione ed estrazione di entità ai fini dell'analisi dei feedback, e la loro classificazione utile ad indirizzare azioni evolutive o di personalizzazione dei servizi per specifiche necessità individuate in funzione delle classi di utenti (imprese, medici, cittadini).

Per implementare soluzioni di IA, è inoltre importante considerare anche le implicazioni etiche, la sicurezza dei dati e la conformità normativa. L'interazione con gli stakeholder e la formazione del personale sono inoltre cruciali per garantire una transizione efficace verso l'utilizzo dell'IA all'interno di un'organizzazione come INAIL. Su questi ultimi aspetti è importante sottolineare come la collaborazione con istituti di ricerca e università sia un fattore di accelerazione di innovazione e di trasferimento tecnologico che permette costantemente all'Istituto di meglio raggiungere i propri obiettivi. Su questo punto INAIL ha forti connessioni ed esperienze, come quella relativa al Rehab Technologies Lab nato dall'accordo con l'Istituto Italiano di Tecnologia.

1.20.2. PROGETTI FUTURI

L'INAIL, in linea con i suoi obiettivi strategici ed evolutivi, ha definito nel suo futuro a breve e medio termine un percorso di consolidamento, evoluzione ed arricchimento delle sue soluzioni di IA.

Il principale focus vede l'INAIL concentrato nel potenziamento, attraverso una soluzione basata sulle tecnologie IA generativa (attualmente in prototipazione), del *knowledge management*, semplificando il processo di acquisizione, distribuzione e utilizzo efficace delle conoscenze di una organizzazione. La sperimentazione in corso si concentra su un sistema di ricerca avanzato che risponda a domande fornite dagli utenti in relazione ad informazioni contenute sia in specifici documenti in ambito Istituzionale (concordati e acquisiti durante le attività di sperimentazione), sia all'interno del portale web www.inail.it. La sperimentazione permette di interrogare il perimetro informativo attraverso un

chatbot, col quale l'utente interagisce per ricercare le informazioni e dal quale riceve le risposte alle domande formulate.

Rimanendo nell'ambito della gestione del patrimonio informativo, è in corso la sperimentazione di un prototipo di *legal AI discovery* per analizzare la documentazione legale. Il sistema permette l'indicizzazione e una migliore consultazione delle informazioni e della documentazione, fornendo un'esperienza avanzata di ricerca su documenti e contenuti non strutturati. In particolare, viene data all'utente la possibilità di ricercare per concetti, entità, parole semanticamente simili, citazioni, riferimenti legislativi, ottenendo risultati accurati e veloci, attraverso la capacità degli strumenti di IA di comprendere il significato della frase o dei termini chiave inseriti.

Con riferimento all'applicazione dell'IA per il potenziamento dell'operatività dell'INAIL, si ritiene utile citare una sperimentazione da avviare a breve, dedicata alla realizzazione di un algoritmo di Machine Learning volto a garantire l'efficientamento del modello di IT Costing mediante la normalizzazione e classificazione dei dati. Nello specifico, l'utilizzo di tecniche di *ML* e *text analytics* per l'analisi delle iniziative è finalizzato al suggerimento automatico della classificazione in termini di servizio, componente di servizio e natura di costo.

Inoltre, nell'ottica di proseguire nel percorso di potenziamento del suo modello di prossimità digitale verso l'utenza, sono già previsti e parzialmente avviati specifici servizi attraverso tecnologie innovative quali il metaverso, la realtà aumentata e l'IA generativa.

1.20.3. ORGANIZZAZIONE E PROCESSI DI INNOVAZIONE

L'INAIL ha da poco rinnovato la sua organizzazione e i suoi processi di gestione delle innovazioni, al fine di adeguarsi alle richieste degli utenti nella cosiddetta nuova normalità post pandemica, e alle rapide evoluzioni delle tendenze tecnologiche. La necessità di innovare può infatti essere dettata dall'evoluzione delle esigenze degli utenti ma anche dal cambiamento dell'ecosistema circostante.

Per garantire il corretto focus sull'IA, e in generale sulle innovazioni, interpretando correttamente le opportunità potenzialmente derivanti dalle nuove tecnologie, l'INAIL si è organizzato per attivare nei processi di gestione dell'innovazione figure specialistiche in organico, o attraverso consulenze dei partner, che abbiano competenze verticali e approfondite sui principali temi innovativi, con prioritario focus sulle soluzioni IA. L'obiettivo di queste figure è quello di svolgere un ruolo specialistico mirato nella valutazione di soluzioni innovative in grado di rafforzare il ruolo di INAIL come istituzione orientata all'innovazione per il business. Come illustrato nelle sezioni precedenti, particolare attenzione è posta sulle soluzioni di IA, nell'ottica di valorizzare l'eterogeneo patrimonio informativo dell'INAIL e fornire all'utenza servizi sempre più completi ed evoluti.

L'obiettivo del rinnovato processo di *innovation management* è dunque la creazione di valore per il business dell'INAIL attraverso l'introduzione di soluzioni innovative, sfruttando le competenze tecnologiche, di business e di design proprie degli specialisti dell'Istituto, nonché dei suoi partner.

In questo senso, sono stati identificati diversi driver che hanno guidato il rinnovamento dell'organizzazione e del processo di Innovation Management:

- Avvicinarsi progressivamente ad un modello maturo di "Open Innovation" che sia in grado di aumentare la ricettività dell'Istituto agli stimoli innovativi interni (idee e soluzioni proposte dalle Direzioni di business esterni) attraverso attività di Scouting Tecnologico.
- Coinvolgere nel processo di innovazione competenze prevenienti da diverse aree funzionali per le rispettive competenze.
- Supportare il processo con idonei strumenti (ad esempio la Scheda di valutazione Innovatività) in grado di fornire informazioni complete e standardizzate a tutti gli attori coinvolti nelle valutazioni, semplificando le fasi di analisi e di benchmark tra le soluzioni presentate.

- Integrare la gestione delle innovazioni nel più ampio scenario operativo dell'INAIL, evitando sovrapposizioni con altri processi aziendali incaricati di raccogliere e analizzare le esigenze.

La nuova Organizzazione vede quindi tre attori principali, fra loro complementari, a guidare il processo di Innovation Management:

- CIT: Struttura dedicata alla Consulenza e Innovazione Tecnologica, composta da specialisti in campo Innovation e nuovi trend tecnologici.
- Innovation Team: Team con specifiche competenze verticali che vengono costituiti ad hoc in funzione delle soluzioni innovative da valutare.
- Innovation Board: Comitato multidisciplinare composto da referenti delle diverse aree funzionali e, alternativamente, da ulteriori partecipanti opzionali sulla base di specifiche esigenze o tematiche.

L'Innovation Board ha il compito di:

- presidiare la governance dell'innovazione.
- promuovere e definire gli indirizzi strategici e le linee guida di innovazione.
- valutare la coerenza con gli indirizzi strategici e la fattibilità delle iniziative proposte, attraverso gli strumenti organizzativi e tecnici più opportuni (Innovation team, Proof of Concept, Progetti pilota, ...).

1.20.4. GOVERNANCE DEI DATI E DELL'IA

Nella sezione precedente sono descritti i processi e l'organizzazione che INAIL ha instaurato per la gestione dell'innovazione.

Questo approccio è alla base di un percorso evolutivo che l'INAIL ha individuato per la gestione strutturata dell'innovazione, specialmente quella derivante dall'introduzione dell'IA. In questa sezione, quindi, ci si focalizza sull'obiettivo dell'INAIL di adottare una più matura strategia di *innovation management*, attraverso un percorso incrementale. L'approccio incrementale è spesso utilizzato per gestire la complessità del cambiamento e risulta particolarmente adeguato alla gestione dei rischi associati all'implementazione di soluzioni di IA in entità strutturate, perché permette flessibilità e risposta rapida ai cambiamenti, con una *vision* di tipo evolutivo. Questa strategia si colloca dunque in un quadro di lungo termine, dove vengono elaborati piani d'azione dettagliati per conseguire gli obiettivi specifici che l'INAIL si è proposto e che fungono da viatico per tutte le decisioni di *business* che intraprende.

Il primo passo verso questo approccio passa anzitutto per l'adozione di un'opportuna Governance dei dati a cui si integra la Governance dell'IA. La priorità dell'INAIL è infatti quella di favorire un uso sostenibile ed etico dei dati, e quindi di sviluppare sistemi di IA che siano non solo perfettamente conformi alle normative vigenti e quelle imminenti (cfr. paragrafo 3.1), ma che incarnino tutti i principi etici di *Trustworthy AI* definiti dall'*High-Level Expert Group on AI*. La visione a lungo termine è quindi quella di dotarsi di un framework di governance dei dati e dell'IA che permetta ad INAIL di incrementare la propria maturità nella gestione dei dati e dell'IA in modo sistemico, etico e sostenibile.

Ci sono al momento specifici progetti che stanno definendo i principi guida di gestione e un framework di governance dei dati a 360°, sulla base delle best practice di mercato e in linea con l'approccio ESG dell'INAIL e delle linee guida delle istituzioni europee. La definizione dei principi guida detterà, chiaramente, una nuova linea per i processi di sviluppo di sistemi e applicativi di IA nell'Istituto, con una presa in carico dell'intero ciclo di vita degli stessi. L'impegno dell'INAIL verso questa direzione è di lungo corso: in passato, infatti, INAIL si è già dotata di un primo framework di Governance delle soluzioni di IA, che standardizza la pipeline di sviluppo di soluzioni di IA e identifica dei punti di

controllo e delle azioni dettate da tali principi etici. Questo approccio verrà ulteriormente integrato dalle attività relative alla governance dei dati e dell'IA attualmente in corso, considerando anche l'imminente approvazione del Regolamento AI Act (COM/2021/206 final), sul quale è stato raggiunto un accordo provvisorio lo scorso 9 Dicembre 2023 che risulta prodromico all'approvazione del Regolamento stesso. Si terrà inoltre conto anche delle evoluzioni in ambito di IA generativa.

L'istituzione del framework verrà necessariamente accompagnata da azioni di formazione sui dipendenti con lo scopo di creare e diffondere una aggiornata cultura del dato e un'appropriata conoscenza delle tematiche di *data & AI ethics*. Data la visione a lungo termine di adozione "diffusa" dell'IA, è fondamentale che tutti i dipendenti siano adeguatamente preparati a lavorare in modo responsabile ed etico, sia per aderire alle normative in vigore che per rappresentare un modello virtuoso all'interno del panorama europeo e nazionale. È stato già effettuato un primo inventario di competenze, che si ispira al *Syllabus* e a *e-CF*, i due framework principali adottati nelle PA italiane che evidenziano le competenze più importanti di chi si occupa di gestione del dato a vario titolo.

Sulla base di questa premessa, saranno definiti nel dettaglio gli elementi del modello organizzativo di governance attraverso un progetto che contempla la creazione di ruoli specifici da inserire nell'organigramma dell'Istituto. A tali ruoli si affiancheranno figure specializzate in governance ed etica dell'IA. Grazie a queste nuove designazioni, sarà possibile delineare chiaramente diritti e responsabilità in relazione ai dati e all'IA. Ciò consentirà all'INAIL di gestire in modo strutturato e organico l'intero ciclo di vita dell'IA.

Difatti, l'approccio incrementale prevede anche che si definiscano adeguati KPI per valutare la performance delle applicazioni e dei sistemi di IA, al fine di correggere eventuali cause di rischio e mantenere ogni sistema conforme ai principi etici e alla conformità normativa (su questo punto, cfr. approfondimento in paragrafo 3.1). La valutazione della performance va attuata secondo specifici obiettivi, elaborati anche di accordo con i numerosi fornitori presenti nell'Istituto, per poter assicurare un congruo *follow-up* al lancio dell'applicativo sia dal punto di vista funzionale/di business che infrastrutturale, tecnico e di sicurezza. Questo è quanto mai importante data la necessità di indirizzare, anche per questioni di *compliance*, eventuali rischi causati dalle applicazioni di IA, che possono manifestarsi sia al lancio di nuovi sistemi, che per cambiamenti legislativi futuri. È necessario, quindi, un monitoraggio continuo che valuti l'efficacia della governance e introduca miglioramenti, garantendo così un adeguato risk management.

L'implementazione progressiva di questi step di processo e l'interazione del framework di data governance e governance dell'IA sono al centro di specifiche raccomandazioni elaborate all'interno di un progetto su *ESG e sostenibilità*, che si sta occupando proprio di analizzare i processi dell'INAIL al fine di orientarli verso un iter etico e sostenibile.

La necessità di adottare un approccio evolutivo incrementale diventa particolarmente urgente e rilevante, soprattutto considerando l'imminente entrata in vigore dell'AI Act. In virtù di quest'ultimo, l'INAIL sarà chiamato a conformarsi non solo a nuove normative di conformità, ma anche a nuovi metodi di gestione. La necessità di attuare un tale processo evolutivo, però, non viene solo dall'esigenza legislativa e di *compliance*, ma anche dal ruolo e dalla responsabilità sociale che l'INAIL assolve nell'ecosistema italiano. Infatti, contrariamente a quanto avviene in una società o organizzazione privata, il ruolo di una pubblica amministrazione è quello di affrontare certe tematiche con un riguardo maggiore verso i cittadini e i loro diritti, con l'obiettivo di rafforzare il rapporto di fiducia con essi, andando oltre ai requisiti minimi di *compliance* ai dettami legislativi.

1.20.5. COME AFFRONTARE L'AI ACT

L'impatto più tangibile e articolato dell'AI Act sarà quello relativo alla conformità normativa. In quanto fornitore, l'INAIL dovrà adeguarsi ai requisiti imposti dalla nuova legge, prevedendo di adeguare i propri sistemi - sviluppati internamente o con il supporto di partner - alle nuove norme, specie per quanto riguarda i sistemi classificati come ad alto rischio secondo la stratificazione prevista dal Regolamento Europeo. La nostra mappatura delle applicazioni rileva che al momento non ci sono sistemi di IA che rientrano in questa categoria, ma è bene che l'Istituto tenga ben presenti gli obblighi che essi comportano e che si monitori nel tempo la rischiosità delle proprie applicazioni e le evoluzioni delle prescrizioni regolamentari. Su questo punto, si prevede l'istituzione di un catalogo delle applicazioni che permetta un monitoraggio centralizzato e continuato nel tempo, supportando così la *compliance* dell'Istituto. La centralizzazione del catalogo permetterà di agire in modo tempestivo e uniforme qualora dovessero esserci modifiche alla regolamentazione, e di verificare che le applicazioni in utilizzo siano o meno ad alto rischio. Inoltre, si faciliterebbe il monitoraggio del rispetto dei requisiti regolamentari, come per esempio il tipo di dati utilizzato, se l'applicazione utilizza sistemi di identificazione biometrica remota, se regola l'accesso ad alcuni prestazioni e servizi pubblici e servizi privati essenziali, oppure se interagisce in modo diretto con gli esseri umani e di conseguenza è necessario che la persona ne sia informata.

Considerando l'INAIL sia nel ruolo di utente che di fornitore di soluzioni di IA, la conformità normativa sarà di fondamentale importanza e si prevede lo sviluppo di specifiche checklist per facilitare l'identificazione del livello di rischio rispetto all'AI Act e dei conseguenti requisiti normativi. In questo sarà fondamentale la collaborazione tra gli uffici che sviluppano o utilizzano applicazioni di IA e le funzioni di controllo. Inoltre, come precedentemente anticipato (cfr. Paragrafo 3) si dovranno prevedere sistemi di monitoraggio delle performance dei sistemi di IA in utilizzo al fine di assicurarsi, durante tutto il ciclo di vita dei sistemi, il rispetto dei requisiti come affidabilità, non discriminazione, accuratezza, robustezza e cybersicurezza, sorveglianza umana e qualità dei dati. Infatti, tutti fornitori e gli utenti di sistemi di IA ad alto rischio devono garantire la conformità ai requisiti sopracitati, ma soprattutto disporre di un sistema di gestione della qualità e del rischio, che in caso di applicazioni ad alto rischio, avvii un processo di monitoraggio iterativo e continuo. Anche i dataset utilizzati devono essere pertinenti, rappresentativi, esenti da errori e completi. Come già sottolineato, l'INAIL sta valutando quali dei requisiti obbligatori per le applicazioni di IA ad alto rischio siano comunque da implementare per assicurare un livello di governance maggiore che vada oltre la *compliance* ma verso un rapporto più di fiducia con i propri utenti e i cittadini.

Sul tema di IA generativa, data la forte spinta innovativa e la volontà di investire in tali tecnologie, già in uso all'interno dell'Istituto, INAIL vuole strutturarsi fin da ora per gestire adeguatamente questo processo di adozione al fine di assicurare i giusti livelli di supervisione, controllo e rispetto dei requisiti non solo legali, ma etici. Infatti, l'IA generativa pone diversi rischi, tra cui risultati *biased* e discriminatori, che generano preoccupazioni sulla sicurezza delle informazioni e la loro affidabilità. Il meccanismo di governo di questi sistemi non è ancora definito, ma al momento si prevede sicuramente l'adozione di Codici di Condotta e *model cards*, che includano le informazioni rilevanti per comprendere il funzionamento del modello, le sue capacità e i suoi limiti. Quando l'AI Act sarà in vigore, questo comporterà principalmente un controllo sui propri fornitori e la corretta interazione con l'AI Office europeo che verrà istituito.

Il framework di governance dei dati e dell'IA che è in corso di definizione cercherà di indirizzare tutti questi requisiti regolamentari, ma cercherà inoltre di formalizzare una governance che vada anche oltre alla *compliance*. In questo senso, il framework permetterà di migliorare l'efficienza e l'efficacia delle soluzioni di IA in adozione nell'Istituto e di implementare anche i requisiti etici di cui l'AI Act è portatore.

L'adozione dell'AI Act rappresenterà un nuovo corso per l'INAIL, che non potrà soffermarsi solo sulle necessità di *compliance*, seppur centrali. Le pubbliche amministrazioni, infatti sono spinte ad andare oltre la *compliance* dato il ruolo sociale che esercitano e alla necessità di rafforzare il rapporto di fiducia con i cittadini. L'adozione di un *framework* di *governance* a 360° garantirà ad INAIL di andare oltre i dettami legislativi verso una visione etica e responsabile della tecnologia, come richiesto ad un attore pubblico e socialmente rilevante quale l'INAIL.

Il complesso iter di revisione di processi e prassi interne che l'INAIL dovrà intraprendere per raggiungere gli ambiziosi obiettivi fin qui esposti, sono al centro di una serie di raccomandazioni che, come precedentemente anticipato, indirizzeranno l'implementazione del cambiamento da un punto di vista organizzativo e culturale. Le raccomandazioni terranno in considerazione i diversi gradi di maturità dei processi già presenti all'interno dell'Istituto e prevederanno, se necessario, lo *scouting* di strumenti tecnologici a supporto delle nuove metodologie da integrare nei processi esistenti.

1.21. L'ESPERIENZA DI INPS

L'INPS ha maturato una significativa esperienza in materia di Intelligenza Artificiale (IA) e IA generativa. Le dimostrazioni pratiche fornite dall'INPS hanno illustrato in modo tangibile i miglioramenti che l'implementazione di questa tecnologia può apportare nel settore pubblico.

Di seguito si riportano gli elementi fondamentali di alcuni dei principali progetti ideati e implementati dall'INPS con l'obiettivo di potenziare i servizi offerti all'utenza mediante l'impiego dell'intelligenza artificiale.

1.21.1. I PROGETTI

1.21.1.1. CLASSIFICAZIONE E SMISTAMENTO AUTOMATICO DELLA POSTA ELETTRONICA CERTIFICATA (PEC)

Si prevede che l'INPS riceverà nel 2023 un volume di oltre 6 milioni di PEC, con una media superiore a 16.000 PEC al giorno. La corretta individuazione dell'argomento trattato e la successiva assegnazione all'ufficio competente richiederebbero un notevole impiego di risorse umane, con un elevato numero di addetti dedicati esclusivamente allo smistamento delle PEC. La soluzione sviluppata dall'INPS, basata su IA, consente uno smistamento automatizzato e rapido delle PEC in arrivo, senza richiedere l'intervento umano.

Questo processo permette all'INPS di liberare circa 40.000 ore di lavoro annue, che possono essere impiegate per compiti di diretto servizio all'utenza, compresa la lavorazione della voluminosa mole di comunicazioni in ingresso. Con questo progetto l'INPS ha ricevuto un prestigioso riconoscimento da parte di IRCAl, Centro di Ricerca Internazionale per l'Intelligenza Artificiale sotto l'egida UNESCO, posizionandosi tra i 10 migliori progetti mondiali in ambito di Intelligenza Artificiale che supportano i 17 SDGs (Obiettivi di Sviluppo Sostenibile) dell'ONU.

1.21.1.2. GESTIONE DELLE RICHIESTE AL CUSTOMER SERVICE

Il progetto, in fase di rilascio previsto per il primo trimestre del 2024, è rivolto alla gestione ottimizzata delle richieste web che vengono rivolte al *Customer Service* di INPS, il quale riceve circa 2,5 milioni di richieste l'anno. Attualmente, ogni istanza viene presa in carico da un operatore di primo livello, il quale è in grado di rispondere correttamente nel 40% dei casi. Nel restante 60%, l'operatore deve inoltrare l'istanza ad un operatore specializzato nell'area della richiesta ricevuta, definito di secondo livello.

La soluzione basata su IA che INPS ha sviluppato, consente di indirizzare correttamente oltre un terzo delle richieste direttamente all'operatore di secondo livello, consentendo un notevole risparmio di lavoro umano da parte dell'operatore di primo livello. L'INPS è stato selezionato come vincitore con il progetto in questione durante il convegno "Premi Agenda Digitale" che si è tenuto a gennaio 2023, dedicato alle PA, PMI e startup che si sono distinte per progetti di digitalizzazione in ambito pubblico.

1.21.1.3. ASSISTENTE VIRTUALE

INPS sta utilizzando tecnologie di intelligenza artificiale al fine di migliorare drasticamente le capacità dell'Assistente Virtuale unificato dell'INPS, che sarà presto in grado di dare una risposta automatizzata all'utente vagliando una vasta mole di dati di pubblico dominio, tra cui normativa, messaggi e circolari dell'INPS, al fine di fornire una risposta immediata ed automatizzata.

A marzo 2022 INPS ha avviato un progetto PNRR denominato *Chatbot* intelligente conclusosi a febbraio 2023 con il rilascio in produzione di un assistente virtuale su Portale internet di tipo generalista.

Attualmente l'architettura di riferimento dell'Assistente Virtuale unico è su due livelli:

- **Masterbot generalista**, con l'obiettivo di:
 - Fornire un rapido accesso ai *chatbot* verticali (carosello oppure *routing / integration*);
 - Guidare il cittadino alla prestazione / area di prestazione di interesse, se possibile rispondendo già alla domanda, utilizzando AI generativa per classificare la domanda;
- **Skillbot specializzato** (*chatbot* verticale) con l'obiettivo di rispondere alla domanda puntualmente.

L'architettura su due livelli ha già permesso l'indirizzamento delle nuove chatbot verticali su servizi comuni, nonché il riuso delle chatbot già sviluppate in INPS, adottando apposite linee guida di integrazione.

A marzo 2023 INPS ha avviato una nuova iniziativa legata all'AI di tipo generativo, tutt'ora in corso. Una prima sperimentazione è stata già rilasciata ad agosto 2023 (durata 4 settimane) per migliorare l'esperienza utente sul motore di ricerca (scenario 1) e per rispondere a domande utente riguardanti la prestazione "opzione donna" (scenario 2 – verticale). Successivamente è stata rilasciata in novembre 2023 un secondo scenario verticale, per la prestazione "Supporto per la formazione ed il Lavoro".

La soluzione già realizzata con AI di tipo generativo ha prodotto un cambio di paradigma non solo nell'esperienza utente ma anche nel processo di produzione delle chatbot, mettendo in evidenza l'efficienza di un modello scalabile che permette, a valle dell'acquisizione dei contenuti validati dagli SME, strutturati seguendo apposite linee guida fornite dalla DC Informatica alle altre DC di prodotto, l'esecuzione di pochi passaggi per la configurazione applicativa e la pubblicazione dello "Skillbot specializzato" all'interno del Portale internet di INPS. Attività chiave sono il prompt engineering di tuning ed i test utente.

1.21.1.4. ALTRI PROGETTI

Oltre ai progetti menzionati sopra, INPS si sta specializzando anche nel portare avanti iniziative di AI nell'ambito contenzioso e legale. In questo contesto, è da evidenziare che allo stato attuale le comunicazioni non strutturate in ambito legale pervengono all'INPS in forma digitale tramite PEC. I dipendenti di INPS applicano metadati a queste comunicazioni inserendo nell'applicativo di interesse le informazioni di contesto necessarie (parti in causa, tribunale, ecc.) presenti nella documentazione

specifica. In questo contesto, il progetto ha lo scopo di utilizzare un sistema di Intelligenza Artificiale in grado di elaborare le comunicazioni digitali estraendo automaticamente le informazioni di contesto dai documenti di interesse, in modo da ridurre notevolmente il tempo richiesto per l'inserimento dei dati e rendere più efficiente il processo di data-entry.

Un progetto simile, relativo sempre all'estrazione dei dati dai documenti è "Smart Prof" per il quale l'INPS prevede di efficientare i processi di pagamento per il bonus asilo nido.

1.21.2. LE SFIDE LEGATE ALL'IA GENERATIVA

Grazie alla diffusione ed alla notorietà delle tecnologie legate all'intelligenza artificiale generativa il periodo attuale emerge come uno dei più dinamici e rivoluzionari nel settore specifico relativo all'Intelligenza Artificiale. L'ampia diffusione ed applicabilità delle soluzioni basate sull'intelligenza artificiale generativa hanno reso immediatamente evidenti (su vasta scala) i vantaggi che tale tecnologia può apportare nell'immediato e nella quotidianità delle persone, data la notevole semplicità di utilizzo.

La corsa verso gli "human-like-bot" ha generato un notevole impatto in tutti i settori sia privato che pubblici. Infatti, la ricerca su questi modelli di intelligenza artificiale generativa continua a progredire, portando a costanti evoluzioni ed aggiornamenti sulle architetture e sui modelli coinvolti, noti come LLM (Large Language Model).

In particolare, sono già emersi (e continuano a progredire) anche LLM Open Source. Questo consente di evitare la dipendenza da prodotti sì avanzati ma chiusi e controllati da compagnie private straniere, e allo stesso tempo permette di sfruttare al meglio le competenze delle comunità globali.

Allo stato attuale esistono due modalità per poter usufruire dell'intelligenza artificiale generativa: affidarsi a un fornitore cloud oppure adottare un modello "Open Source" su un'infrastruttura interna ("on premise"). L'aspetto vincolante, in questa scelta, è la complessità di tali modelli, i quali necessitano di infrastrutture ad elevate prestazioni, fattore che giustifica il ricorso a modelli basati su cloud

Tuttavia, l'utilizzo dei modelli cloud presenta un problema di fondo: essi sono continuamente addestrati e migliorati senza alcun controllo da parte dell'utilizzatore, compromettendo la chiarezza nell'utilizzo dei dati nel processo di addestramento/training, in contrasto con il concetto di trasparenza e spiegabilità sostenuto dall'AI Act.

In aggiunta, l'utilizzo dei modelli cloud pone un interrogativo importante sulla gestione dei dati sensibili, come quelli presenti nella pubblica amministrazione e in enti governativi. A prescindere dalle rassicurazioni legali, fornire tali dati ai cloud vendor pone seri rischi presenti e futuri riguardo la salvaguardia della privacy del cittadino e la confidenzialità dei dati.

1.21.3. LEZIONI APPRESE

L'esperienza di INPS fornisce alcuni punti di attenzione ed elementi di riflessione per tutte le pubbliche amministrazioni in procinto di adottare soluzioni basate su intelligenza artificiale.

- La scelta del modello di intelligenza artificiale è determinante per ottenere risultati in linea con le specifiche esigenze. La Pubblica Amministrazione dovrebbe valutare:
 - modelli predittivi non linguistici (e.g. Machine learning *supervised* o *unsupervised*);
 - modelli linguistici per la comprensione ed il confronto di contenuti;
 - modelli linguistici per la generazione di contenuti.

Le tre categorie di modelli hanno costi, complessità e maturità diverse.

- Le pubbliche amministrazioni dovrebbero prediligere modelli predittivi non linguistici quando i dati sono strutturati ed i predittori della risposta sono un numero molto elevato e di tipologia eterogenea (e.g., controlli antifrode); dovrebbe invece prediligere modelli linguistici per la comprensione ed il confronto di contenuti in scenari di disambiguazione (e.g., instradamento di un problema, classificazione di un testo, estrazione di testo da un documento); infine, i modelli linguistici per la generazione di contenuti in scenari di conversazione con l'utenza (e.g., assistenti virtuali) e nel supporto decisionale (e.g., raccomandazione). Alcuni algoritmi potrebbero essere più indicati di altri in base al ruolo nella soluzione, di conseguenza è opportuno valutare il livello di personalizzazione e di flessibilità fin dall'inizio.
- Le pubbliche amministrazioni che intendono realizzare servizi di tipo chat/voice bot basati su intelligenza artificiale di tipo generativo devono prevedere un processo di analisi documentale ed un'infrastruttura di raccolta dei documenti (base di conoscenza), che permetta di governarne in modo efficace, anche sotto il profilo organizzativo, l'acquisizione, l'aggiornamento, la "metadattazione" e la validazione dei contenuti, coinvolgendo gli esperti della materia in ogni fase del ciclo di vita del modello "linguistico" utilizzato.
- Le pubbliche amministrazioni che intendono avvalersi di intelligenza artificiale di tipo generativo dovranno porre attenzione alla qualità dei contenuti, per ridurre al minimo il fattore aleatorio di "interpretabilità" del significato dei testi, mai del tutto neutralizzabile, l'effetto di "dispersione" dell'informazione, dipendente dalla ridondanza dei concetti, l'uso di termini e sigle tipiche di un contesto tematico, rischiose se non ben inquadrati. L'effettiva presenza delle informazioni all'interno delle fonti è determinante per la generazione di una risposta; la presenza di terminologia specialistica o assente dal vocabolario (es. acronimi, neologismi, forme letterarie particolarmente articolate o inusuali) va ridotta o adeguatamente tradotta in linguaggio aderente ai modelli linguistici su cui è addestrata l'intelligenza artificiale di tipo generativo (foundation model). Per fare un esempio, se l'addestramento del modello è stato eseguito su documenti dove il termine "pensione" è legato alle rendite da polizza ed il contesto di utilizzo del modello è la Previdenza Sociale risulterà di particolarmente importante "correggere" nella soluzione (tipicamente nel prompt engineering, durante la fase di tuning) come il termine "pensione" va utilizzato.
- I contenuti utilizzati dall'intelligenza artificiale di tipo generativo devono essere autorizzati da fonti autorevoli e competenti, ovvero deve essere esplicitamente inibita (tipicamente nel *prompt engineering*) ogni forma di "creatività" cui tendenzialmente mirano i modelli linguistici di tipo generativo, poiché questi hanno, in generale, l'obiettivo di ricostruire un senso compiuto e realistico di una conversazione, non quello di riportare la realtà dei fatti. Opportuno, inoltre, che le fonti siano riportate direttamente nella risposta fornita dalla chatbot/voice bot, oppure siano tracciate dietro le quinte, e nel caso recuperabili.
- Le Pubbliche Amministrazioni che intendono avvalersi di intelligenza artificiale di tipo generativo devono costruire un proprio Framework di Valutazione della bontà delle "Risposte", basato su un numero significativo di "Domande", suddivise per tematica, ed un numero di indicatori puntuali di valutazione di tipo sia qualitativo che quantitativo. Parte di tale Framework di Valutazione è il meccanismo attraverso cui sono raccolti i feedback dal Cittadino, utili a stabilire il grado di affidabilità dei risultati ed a migliorare il modello.

- Per ridurre il rischio di lock-in dai servizi offerti dal mercato è raccomandato che la soluzione adottata sia basata su modelli aperti e componenti intercambiabili e interoperabili, nello specifico è raccomandato adottare modelli più maturi e meno costosi per realizzare le componenti della soluzione più stabili e semplici di funzionamento, quindi isolare le componenti della soluzione sulle quali confrontare tra loro modelli diversi, applicando la competizione tra tecnologie sui compiti più complessi e sfidanti, coinvolgendo anche produttori di AI generativa di nicchia.
- Nel presentare al Cittadino una soluzione di Assistente Virtuale basata su intelligenza artificiale di tipo generativo il Cittadino deve essere informato su alcuni aspetti:
 - o Il Cittadino deve essere informato che la qualità della risposta dipende dalla qualità della sua domanda. Domande corte e poco contestualizzate metteranno in difficoltà l'assistente virtuale che, in prima battuta, ha necessità di recuperare il contesto.
 - o Il Cittadino deve essere informato che le risposte potrebbero contenere errori e, lì dove si siano già raccolti dei feedback, fornendo la percentuale statistica.
- Nel processo di interazione tra Cittadino e Assistente Virtuale basato su intelligenza artificiale di tipo generativo deve essere applicata una strategia di comunicazione che permetta al Cittadino di interloquire per avere risposte personalizzate, usando un contesto di risposta che, nel corso della conversazione, deve potersi arricchire di informazioni. Rispetto ai chat/voice bot tradizionali, che sono basati su flussi di dialogo "rigidi" (what if) in questo caso sono necessarie metodologie per orientare il dialogo prevedendo punti di consolidamento (congestion), dove può essere l'Assistente virtuale a porre domande e suggerimenti.

1.22. L'ESPERIENZA DI ISTAT

Istat ha attivato diversi progetti per esplorare le potenzialità dell'IA nell'ambito delle proprie attività istituzionali.

Da anni ISTAT utilizza tecniche di IA attraverso l'uso delle ontologie per modellare i dati. Infatti, il linguaggio logico delle ontologie è in grado di abilitare il "ragionamento automatico" (reasoner) per il controllo della qualità dei dati, recuperando eventuali incoerenze sui dati e fornendo nuove informazioni non direttamente ottenibili dalle analisi dei dati stessi.

Recentemente, ISTAT sta esplorando una possibile soluzione attraverso l'uso di algoritmi di AI generativa per produrre ontologie partendo da una descrizione in linguaggio naturale del contesto semantico che si vuole modellare. La necessaria interazione con gli specialisti consente sia l'addestramento degli algoritmi che il miglioramento della qualità della modellazione. Una possibile applicazione di tali tecniche generative può essere utilizzata nell'ambito della gestione dei dati delle Pubbliche Amministrazioni, per rendere i dati amministrativi interoperabili attraverso le tecniche del semantic web, ottimizzando l'impegno - di risorse con competenze specialistiche elevate.

Altri casi di studio, in corso di verifiche, riguardano la produzione dei dati statistici, dalla loro raccolta alla diffusione.

Nell'ambito della raccolta dati si ipotizza l'utilizzo di un assistente virtuale per supportare gli utenti nella compilazione dei questionari di indagine.

Per la fase di diffusione dei dati statistici sono allo studio diversi casi d'uso:

- Utilizzo di una chat bot per aiutare gli utenti a trovare, tra i documenti e i comunicati stampa disponibili sul sito istituzionale, le informazioni statistiche desiderate.
- Abilitazione della ricerca semantica sui contenuti del sito istituzionale
- Assistente virtuale per rispondere alle richieste inviate dagli utenti al Contact Centre
- Utilizzo di IA per la creazione di query per l'interrogazione di repository (DB relazionali, NoSQL, asset semantici, Linked Open Data) utilizzando il linguaggio naturale.

Infine, anche per gli utenti interni si intende sperimentare l'utilizzo di IA generativa per la richiesta di informazioni su procedure amministrative interne (delibere, regolamentazioni, compilazione di modulistica per il personale)