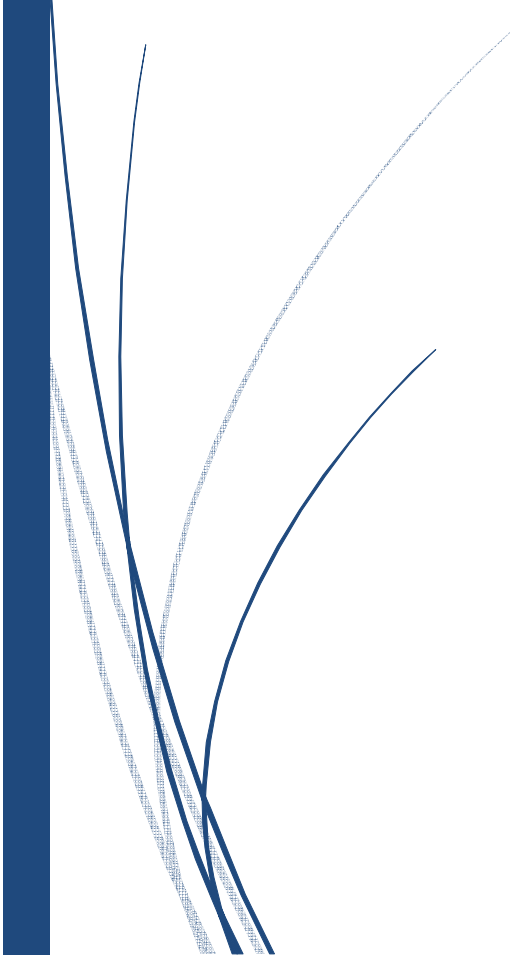




20/03/2023

PIANO TRIENNALE PER LA TRANSIZIONE DIGITALE 2023/2025

*Riferimento al Piano Triennale per l'informatica 2022/2024
pubblicato da AgID (Format AgID per la redazione)*



Ordine degli Assistenti sociali del Lazio
Largo dei Colli Albani 32 - 00179 ROMA



SOMMARIO

PARTE I - IL PIANO TRIENNALE

1. Introduzione	3
2. Ruolo dei Responsabile per la Transizione al Digitale	3
3. Contesto strategico	3
4. Strategia	4
5. Principi guida	4
6. Obiettivi e spesa complessiva prevista	5

PARTE II - LE COMPONENTI TECNOLOGICHE

Capitolo 1. - Servizi	6
- Contesto normativo e strategico	6
- Obiettivi e risultati attesi	7
- Cosa deve fare l'Amministrazione	7
Capitolo 2. - Dati	8
- Contesto normativo e strategico	8
- Obiettivi e risultati attesi	8
- Cosa deve fare l'Amministrazione	9
Capitolo 3. - Piattaforme	9
- Contesto normativo e strategico	10
- Obiettivi e risultati attesi	11
- Cosa deve fare l'Amministrazione	12
Capitolo 4. - Infrastrutture	12
- Contesto normativo e strategico	13
- Obiettivi e risultati attesi	13
- Cosa deve fare l'Amministrazione	14
Capitolo 5. - Interoperabilità	14
- Contesto normativo e strategico	14
- Obiettivi e risultati attesi	15
- Cosa deve fare l'Amministrazione	15
Capitolo 6. - Sicurezza informatica	15
- Contesto normativo e strategico	15
- Obiettivi e risultati attesi	16
- Cosa deve fare l'Amministrazione	16
Capitolo 7. - Le leve per l'innovazione	17
- Contesto normativo e strategico	17
- Obiettivi e risultati attesi	17
- Cosa deve fare l'Amministrazione	18



PARTE III - LA GOVERNANCE

Capitolo 8. - Governance	19
- Contesto normativo e strategico	19
- Obiettivi e risultati attesi	20
- Cosa deve fare l'Amministrazione	20
Capitolo 9. - Indicazioni per la PA	20
Appendice - Acronimi	24



PARTE I - IL PIANO TRIENNALE

1. Introduzione

L'Ordine degli Assistenti sociali è stato istituito con Legge 23 marzo 1993, n. 84 "Ordinamento della professione di assistente sociali e istituzione dell'albo professionale" (GU n. 76 Serie generale del 1° aprile 1993) e successivamente normato da:

- Decreto del Ministero di Grazie e Giustizia 11 ottobre 1994, n. 615 "Regolamento recante norme relative all'istituzione delle sedi regionali o interregionali dell'ordine e del consiglio nazionale degli assistenti sociali, ai procedimenti elettorali e alla iscrizione e cancellazione dall'albo professionale" (GU n. 260 del 7 novembre 1994);
- Decreto del Presidente della Repubblica 8 luglio 2005, n.169 "Regolamento per il riordino del sistema elettorale e della composizione degli organi di ordini professionali" (GU n. 198 del 26-8-2005).

La sua struttura organizzativa è composta da un Consiglio nazionale e da n. 20 consigli regionali, uno per ogni regione italiana.

Ogni Consiglio regionale, con sua capacità decisionale e deliberativa, è composto da un numero precisato di consiglieri e da un Revisore Unico.

Per quanto riguarda l'aspetto organizzativo, l'Ordine del Lazio è suddiviso in 5 macro aree:

- Amministrazione;
- Formazione;
- Supporto tecnico;
- Consiglio Territoriale di Disciplina;
- Segreteria;

ogni macro area è suddivisa in uno o più Uffici con relativo Responsabile del procedimento.

A capo delle macro aree, è stato posto l'Ufficio per la Transizione al Digitale, composto da un Funzionario amministrativo (con riconoscimento di Posizione organizzativa, come da normativa), da un consulente informatico e da un consulente legale.

Detto Ufficio, svolge funzioni di controllo, supporto e decisione rispetto alle attività del Consiglio ad esso collegate.

2. Ruolo del Responsabile per la Transizione al Digitale

Il Responsabile per la Transizione al Digitale - RTD è una figura interna a tutte le PPAA, prevista dal CAD (Codice dell'Amministrazione Digitale, D.lgs. 82/2005).

Con il Decreto Legislativo 13 dicembre 2017, n. 217 "Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche", nasce il concetto di Responsabile per la Transizione Digitale che va ad integrare i suoi compiti con il coordinamento e la diffusione dei sistemi di identità e domicilio digitale ed interoperabilità tra i sistemi della PA ed acquisti di soluzioni e sistemi informatici.

La Circolare n. 3 del 1 ottobre 2018, adottata dal Ministro per la PA, invita le PA a definire, con atto organizzativo interno e nell'ambito della dotazione organica complessiva delle posizioni di funzione dirigenziale, un RTD ed un ufficio dirigenziale, di livello generale - ove previsto nel relativo ordinamento -, cui attribuire i compiti per la transizione digitale declinati dal comma 1 dell'art. 17 del citato CAD.

Pertanto, il RTD è la figura dirigenziale che ha, tra le sue principali funzioni, quella di garantire operativamente la trasformazione digitale della PA, coordinandola nello sviluppo dei servizi pubblici digitali e nell'adozione di modelli di relazione trasparenti ed aperti con i cittadini

Sempre nella citata Circolare, si stabilisce che, laddove non siano previste posizioni dirigenziali, le funzioni per la transizione al digitale elencate dall'art. 17 del CAD, possano essere affidate ad un dipendente in posizione apicale o, in alternativa, a un titolare di posizione organizzativa.

3. Contesto Strategico

Il Piano Triennale per l'informatica nella PA (di seguito Piano Triennale o P.T.) è uno strumento fondamentale per promuovere la trasformazione digitale del Paese e, in particolare, quella della Pubblica Amministrazione Italiana.

In questo contesto in continua evoluzione, con l'accelerazione provocata dal suo maggiore utilizzo nel corso del periodo della pandemia da Covid-19, la tecnologia riveste, infatti, un ruolo di primo piano e necessita di un Piano e di una programmazione di ampio respiro, che tenga conto delle molteplici variabili sul tema e sui cambiamenti in corso.



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.

La presente edizione del Piano Triennale, in continuità con la precedente, risultandone il relativo aggiornamento, mantiene inalterata e consolida la struttura ed articolazione del documento:

- Parte I - Il Piano Triennale, composta da un'introduzione denominata *executive summary*, seguita dalla descrizione della strategia e da un approfondimento sui principi guida indicati dall'AgID.

- Parte II - Le componenti tecnologiche, suddivisa nei rispettivi capitoli corrispondenti ai livelli rappresentati nel "Modello strategico".

- Parte III - La Governance, suddivisa in 3 capitoli che descrivono la governance da attuare per la trasformazione digitale del Paese e le azioni in carico alle Amministrazioni.

I capitoli della Parte II e III hanno la seguente struttura:

breve introduzione che descrive i temi affrontati nel capitolo fornendo un raccordo con il Piano precedente ed offrendo un'anteprima degli scenari futuri;

il contesto normativo e strategico che elenca i riferimenti sia normativi che strategici a cui le Amministrazioni devono attenersi, in termini di fonti normative con link a documenti/siti ufficiali e riferimenti ad attività progettuali finanziate, compresi i riferimenti agli specifici investimenti del PNRR;

la sezione degli obiettivi e dei risultati attesi che descrive gli obiettivi prefissati e, per ciascun obiettivo, individua i risultati attesi (R.A.) e relativi target annuali. Inoltre, per ciascun risultato atteso sono riportati i risultati del monitoraggio effettuato a dicembre 2022.

Rispetto al precedente Piano Triennale 2020/2022, si dà atto dell'esecuzione di gran parte delle attività ivi previste quali l'adozione del Cloud backup, il monitoraggio periodico delle vulnerabilità informatiche, la realizzazione di un nuovo sito web basato su CMS Wordpress, la verifica dell'utilizzo dello SPID, la verifica di bandi per la digitalizzazione delle PPAA e l'analisi delle procedure per la dematerializzazione della documentazione cartacea.

Unico obiettivo programmato nel precedente Piano ed ancora da implementare, è quello della formazione in materia informatica e di data protection, il cui espletamento si reputa necessario al punto da integrare uno degli obiettivi più rilevanti per il presente Piano Triennale 2023/2025.

4. Strategia

- Favorire lo sviluppo di una società digitale, dove i servizi mettono al centro i cittadini e le imprese, attraverso la digitalizzazione della PA 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.

5. Principi Guida

- **Digital & mobile first** (digitale e mobile come prima opzione): le PPAA devono realizzare servizi primariamente digitali.
- **Digital identity only** (accesso esclusivo mediante identità digitale): le PPAA devono adottare in via esclusiva sistemi di identità digitale definiti dalla normativa.
- **Cloud first** (cloud come prima opzione): le PPAA, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano primariamente il paradigma cloud, tenendo conto della necessità di prevenire il rischio di lock-in.
- **Servizi inclusivi ed accessibili**: le PPAA devono progettare servizi pubblici digitali che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori.
- **Dati pubblici un bene comune**: il patrimonio informativo della PA è un bene fondamentale per lo sviluppo del Paese e deve essere valorizzato e reso disponibile ai cittadini ed alle imprese, in forma aperta e interoperabile.
- **Interoperabile by design**: i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e senza interruzioni in tutto il mercato unico esponendo le opportune API (Application Programming Interface).
- **Sicurezza e privacy by design**: i servizi digitali devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali.



- **User-centric, data driven e agile:** le Amministrazioni sviluppano i servizi digitali, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni ed utilizzo;
- **Once only:** le PPAA devono evitare di chiedere ai cittadini ed alle imprese informazioni già fornite;
- **Transfrontaliero by design** (concepito come transfrontaliero): le PPAA devono rendere disponibili, a livello transfrontaliero, i servizi pubblici digitali rilevanti;
- **Codice aperto:** le PPAA devono prediligere l'utilizzo di software con codice aperto e, nel caso di software sviluppato per loro conto, deve essere reso disponibile il codice sorgente.

6. Obiettivi e spesa complessiva prevista

L'Ordine, anche a seguito della pandemia da Covid-19, ha implementato e velocizzato il processo di dematerializzazione di tutti i documenti cartacei in entrata ed in uscita, già iniziato intorno agli anni 2017.

L'obiettivo finale sarà quello di arrivare alla dematerializzazione completa che potrà avvenire solo quando sarà possibile applicare marche da bollo virtuali sugli unici documenti ancora cartacei (certificati in bollo e variazioni all'Albo: iscrizioni/cancellazioni/trasferimenti).

Per quanto riguarda le spese complessive previste, seguendo il target degli obiettivi riportati nei capitoli successivi ed essendo l'Ordine una piccola PA, si demanda al Consiglio regionale la valutazione annuale della spesa che si potrà stanziare a seconda del budget disponibile.



PARTE II - LE COMPONENTI TECNOLOGICHE

Il corpo centrale del documento sarà costituito da un Capitolo per ogni componente tecnologica, in linea con le esigenze dell'Amministrazione, con le relative linee d'azione ipotizzate.

Come indicato nel format del Piano triennale dell'AgID, vengono inclusi i soli capitoli relativi alle componenti tecnologiche che effettivamente l'Ente necessita, sulla base dei principi volti alla digitalizzazione e nel rispetto delle disponibilità di budget di un Ente di ridotte dimensioni come è l'Ordine degli Assistenti sociali del Lazio.

Capitolo 1. Servizi

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 PPAA.

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 ed 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 ed 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.

Per semplificare ed agevolare l'utilizzo del servizio è necessario favorire l'applicazione del principio *once only*, richiedendo agli utenti i soli dati non conosciuti dalla PA e, per questi, assicurandone la validità ed efficacia probatoria nei modi previsti dalla norma, anche attraverso scambi di dati nei modi previsti dal Modello di Interoperabilità per la PA, indicato nel Capitolo 5. Interoperabilità.

Nel caso il servizio richieda un accesso da parte del cittadino è necessario che sia consentito attraverso un sistema di autenticazione previsto dal CAD, assicurando l'accesso tramite l'identità digitale. Allo stesso modo, se è richiesto un pagamento, tale servizio dovrà essere reso disponibile anche attraverso il sistema del PagoPA, di cui l'Ordine, già dispone.

Da questo punto di vista è da considerare quanto specificato per le Piattaforme già messe a disposizione a livello nazionale per la gestione dei servizi di base come previsto nel Capitolo 3. Piattaforme. L'adozione di queste ultime, non solo rende rapida l'implementazione dei servizi necessari, ma accelera il processo di standardizzazione nella PA.

Infine, risulta particolarmente rilevante evidenziare lo sviluppo che avrà nel triennio di competenza del presente Piano Triennale, il passaggio dalla PEC alla realizzazione pratica dei SERCQ (Servizi Elettronici di Recapito Certificato Qualificati), in conformità degli artt. 43 e 44 del Regolamento eIDAS (electronic IDentification Authentication and Signature) n. 910/2014, con l'obiettivo di garantire l'identità di mittente e destinatario e l'interoperabilità dei suddetti servizi a livello europeo.

Nell'agosto 2022 AgID ha adottato le Regole tecniche per i servizi di recapito certificato qualificato a norma del citato Regolamento eIDAS - Criteri di adozione standard ETSI - REM-Policy- IT 1.0, che rappresenta il primo step del percorso che porterà all'adeguamento dalla PEC a SERCQ, a seguito dell'approvazione di un apposito DPCM.

Contesto normativo e strategico

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

Riferimenti normativi italiani:

- 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 del Presidente della Repubblica 11 febbraio 2005, n. 68 "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3".

- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'Amministrazione Digitale" (in breve CAD), artt. 7, 17, 23, 53, 54, 68, 69 e 71.

- Decreto della Presidenza del Consiglio dei Ministri - Dipartimento per l'Innovazione e le Tecnologie del 2 novembre 2005 "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata".



- 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 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”.
- Decreto Legge 9 giugno 2021, n. 80, convertito con modificazioni dalla Legge 6 agosto 2021, n. 113 “Misure urgenti per il rafforzamento della capacità amministrativa delle PPAA funzionale all’attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per l’efficienza della giustizia”.
- Decreto Legge 30 aprile 2022, n. 36, convertito con modificazioni dalla Legge 29 giugno 2022, n. 79 “Ulteriori misure urgenti per l’attuazione del Piano nazionale di ripresa e resilienza (PNRR)”, artt. 30 e 32.
- Linee Guida AgID su acquisizione e il 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 P.A. (2022).
- Circolare AgID n. 2/2018, Criteri per la qualificazione dei Cloud Service Provider per la Pubblica Amministrazione.
- Circolare AgID n. 3/2018, Criteri per la qualificazione di servizi SaaS per il Cloud della Pubblica Amministrazione.
- Manuale di abilitazione al cloud AgID (2022).
- Regolamento AgID, recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico ed affidabilità delle infrastrutture digitali per la P.A. 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).

Obiettivi e risultati attesi

OB.1.1 - Migliorare la capacità di generare ed erogare servizi digitali:

- *R.A.1.1d - Diffusione del monitoraggio, da parte delle Amministrazioni, della fruizione dei servizi digitali*
- Target 2023: attivazione di Web Analytics Italia.

OB.1.2 - Migliorare l’esperienza d’uso e l’accessibilità dei servizi:

- *R.A.1.2a - Incremento e diffusione dei modelli standard per lo sviluppo di siti, disponibili in Designers Italia*
- Target 2024: passaggio del sito web al modello standard previsto da Designer Italia
- *R.A.1.2c - Incremento dell’accessibilità dei servizi digitali della P.A., secondo quanto indicato dalle Linee guida sull’accessibilità degli strumenti informatici*
- Target 2023-2025: monitorare e migliorare l’accessibilità del sito web per i nuovi contenuti.

OB.1.4 - Adeguamento dei servizi di recapito certificato qualificato a norma del regolamento eIDAS:

- *R.A.1.4a - Migrazione dalla PEC ai servizi SERCQ*
- Target 2025: Eseguire la migrazione delle PEC in SERCQ.

Cosa deve fare l’Amministrazione

OB.1.1 - Migliorare la capacità di generare ed erogare servizi digitali:

- settembre 2023: analisi e registrazione a Web Analytics Italia;
- dicembre 2023: introduzione del codice nel sito web e monitoraggio degli accessi.

OB.1.2 - Migliorare l’esperienza d’uso e l’accessibilità dei servizi:

- *R.A.1.2a:*
 - ottobre 2023: richiedere l’approvazione al Consiglio dell’Ordine;
 - giugno 2024: predisporre un bando per identificare un operatore economico per le attività di migrazione dei contenuti e realizzazione della nuova piattaforma web;
 - dicembre 2024: nuovo sito web online.
- *R.A.1.2c:*
 - 2023/2025: monitoraggio trimestrale dell’accessibilità del sito web, con pubblicazione dei nuovi contenuti accessibili.

OB.1.4 - Adeguamento dei servizi di recapito certificato qualificato a norma del regolamento eIDAS:

- dicembre 2024: identificazione di un fornitore qualificato AgID che disponga della tecnologia per la migrazione delle PEC;
- dicembre 2025: migrazione delle PEC dell’Ordine a SERCQ.



Capitolo 2. Dati

La valorizzazione del patrimonio informativo pubblico è un obiettivo strategico per la PA 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, tutti i portatori di interesse e fornire ai policy maker strumenti data-driven da utilizzare nei processi decisionali e/o produttivi.

In linea con i principi enunciati e in continuità con le azioni avviate con il precedente Piano, 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 PPAA per finalità istituzionali, sia con riferimento al riutilizzo dei dati, per finalità commerciali e non, secondo il paradigma degli *open data*.

Un *asset* fondamentale tra i dati gestiti dalle PPAA è rappresentato dalle Banche dati di interesse nazionale (art. 60 del CAD) per le quali rimane forte l'esigenza di favorirne l'accesso e la fruibilità, che si concretizzerà attraverso l'implementazione e l'utilizzo della PDND (Piattaforma Digitale Nazionale 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 e 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 PPAA” (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 (in attesa di adozione definitiva).
- 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).

- 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.

Obiettivi e risultati attesi

OB.2.2 - Aumentare la qualità dei dati e dei metadati:

- *R.A.2.2b - Aumento del numero di dataset di tipo aperto resi disponibili dalle PPAA*
 - Target 2023: analisi annuale sulle tipologie di dati generati dall'Ente per sottoporle al Consiglio e verificare la fattibilità di realizzare dataset per renderli pubblici.
 - Target 2024: analisi annuale sulle tipologie di dati generati dall'Ente per sottoporle al Consiglio e verificare la fattibilità di realizzare dataset per renderli pubblici.
 - Target 2025: analisi annuale sulle tipologie di dati generati dall'Ente per sottoporle al Consiglio e verificare la fattibilità di realizzare dataset per renderli pubblici.

Cosa deve fare l'Amministrazione

- dicembre 2023: verifica delle tipologie di dati da poter pubblicare nei cataloghi nazionali dati.gov.it.
- dicembre 2024: verifica delle tipologie di dati da poter pubblicare nei cataloghi nazionali dati.gov.it.
- dicembre 2025: Verifica delle tipologie di dati da poter pubblicare nei cataloghi nazionali dati.gov.it.

Capitolo 3. Piattaforme

Come per il precedente Piano, questo Piano triennale si focalizza sull'evoluzione delle piattaforme della PA, che offrono funzionalità fondamentali nella digitalizzazione dei processi e dei servizi della PA.

Le piattaforme nascono per supportare la razionalizzazione dei processi di *back-office* o di *front-end* della PA e sono disegnate per interoperare in modo organico.

Attraverso i loro strumenti, consentono di ridurre il carico di lavoro delle PPAA, favorendo l'integrazione e l'interoperabilità tra sistemi, sollevandole dalla necessità di dover realizzare ex novo funzionalità, riducendo tempi e costi di attuazione dei servizi e garantendo una maggiore sicurezza informatica.

Le piattaforme favoriscono la realizzazione di processi distribuiti e la standardizzazione dei flussi di dati tra Amministrazioni, nonché la creazione e la fruizione di servizi digitali più semplici e omogenei.

Negli ultimi anni le iniziative intraprese dai vari attori coinvolti nell'ambito del Piano, hanno favorito un'importante accelerazione nella diffusione di alcune delle principali piattaforme abilitanti, in termini di adozione da parte delle PPAA e di fruizione da parte degli utenti. Tra queste, la piattaforma dei pagamenti elettronici PagoPA di cui l'Ordine già dispone, le piattaforme di identità digitale SPID e CIE, nonché la piattaforma IO che offre un unico punto d'accesso, tramite un'applicazione mobile, ai servizi pubblici locali e nazionali.

Il Piano, quindi, prosegue nel percorso di evoluzione e consolidamento delle piattaforme previste dalle norme ed individua una serie di azioni volte a promuovere i processi di adozione, in forma diretta o intermediata, ad aggiungere nuove funzionalità e ad adeguare costantemente la tecnologia utilizzata e i livelli di sicurezza.

Il Piano descrive, inoltre, lo sviluppo di nuove piattaforme che 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, si rimanda al Capitolo 5 "Interoperabilità"):

- l'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi professionali o nel Registro Imprese (INAD), è l'elenco pubblico contenente i domicili digitali eletti, destinati alle comunicazioni aventi valore legale con la PA;

- la Piattaforma Notifiche Digitali (PND) permette la notificazione e la consultazione digitale degli atti a valore legale. In particolare, la piattaforma ha l'obiettivo, per gli enti, di centralizzare la notificazione verso il cittadino



o le imprese utilizzando il domicilio digitale eletto e creando un cassetto delle notifiche sempre accessibile (via mobile e via web o altri punti di accesso) con un risparmio di tempo e costi per cittadini, imprese e PA;

- il Sistema Gestione Deleghe (SGD) consentirà ai cittadini di delegare l'accesso a uno o più servizi a un soggetto titolare dell'identità digitale.

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.

Generali:

- Decreto legislativo 7 marzo 2005, n. 82 “Codice dell’Amministrazione Digitale” (CAD).
- Decreto legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”.
- 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) n. 910/2014 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (eIDAS).
- Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR).
- Linee Guida CE in materia di Data Protection Impact Assessment (2017).

SPID:

- 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 PPAA 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:

- Decreto legislativo 7 marzo 2005, n. 82 “Codice dell’Amministrazione Digitale” (CAD), art.66.
- 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, convertito con modificazioni dalla L. 31 marzo 2005, n. 43 “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 Ministero dell'Interno 23 dicembre 2015 “Modalità tecniche di emissione della Carta d'identità elettronica”.
- 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.

INAD:

- Decreto legislativo 7 marzo 2005, n. 82 “Codice dell’Amministrazione Digitale” (CAD), artt. 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 (2022).

IO, l’app dei servizi pubblici:

- 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).

Sistema Gestione Deleghe

- Decreto legislativo 7 marzo 2005, n. 82 “Codice dell’Amministrazione Digitale” (CAD), art. 64-ter.

- Decreto della Presidenza del Consiglio dei Ministri - Dipartimento per la trasformazione digitale, 30 marzo 2022, Disciplina delle modalità di funzionamento del Sistema di Gestione Deleghe («SGD»).

Piattaforma Notifiche Digitali:

- 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.

Obiettivi e risultati attesi

OB.3.1 - Favorire l’evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l’azione amministrativa:

- *R.A.3.1c - Inserimento dell’Ente su NoiPA*

- Target dicembre 2023: Proposta al Consiglio dell’Ordine.

- Target dicembre 2024: Registrazione ed utilizzo della piattaforma dei dipendenti della PA.

OB.3.2 - Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PPAA:

- *R.A.3.2a - Incremento dell’adozione e dell’utilizzo di SPID e CIE da parte delle PPAA*

- Target dicembre 2023: verifica delle attività che necessitano dell’accesso mediante SPID e CIE.

- Target dicembre 2024: attuazione dell’utilizzo di questa piattaforma.

- Target dicembre 2025: verifica di eventuali nuove attività da inserire in programmazione.

OB.3.3 - Incrementare e razionalizzare il numero di piattaforme per le amministrazioni al fine di semplificare i servizi ai cittadini:

- *R.A.3.3b - Utilizzo della Piattaforma Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all’iscrizione in albi professionali o nel Registro Imprese (INAD)*

- Target dicembre 2023: verifica delle funzionalità attive.

- Target dicembre 2024: utilizzo della piattaforma.

- *R.A.3.3d - Utilizzo del Sistema Gestione Deleghe (SGD) digitali al fine di agevolare la fruizione dei servizi online attraverso soggetti delegati*

- Target Dicembre 2024: verifica della funzionalità del nuovo progetto e valutazione se può essere utile l’utilizzo di tale piattaforma.

- Target Dicembre 2025: Utilizzo della piattaforma.



Cosa deve fare l'Amministrazione

OB.3.1 - Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa:

- dicembre 2023: valutazione da parte del Consiglio dell'Ordine;
- dicembre 2024: Se l'esito della valutazione è positivo per l'adesione a NoiPA dovrà esprimere manifestazione di interesse e inviare richiesta di adesione - CAP3.PA.LA01.

OB.3.2 - Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PPAA:

- dicembre 2023: l'Ordine prosegue il percorso di adesione a SPID e CIE e per i servizi che riterrà opportuni dovrà dismettere le altre modalità di autenticazione associate ai propri servizi online - CAP3.PA.LA07 ed adottare SPID e CIE.

- dicembre 2024: adozione dell'autenticazione on-line.

OB.3.3 - Incrementare e razionalizzare il numero di piattaforme per le amministrazioni al fine di semplificare i servizi ai cittadini:

- dicembre 2024: se l'Ordine risulterà in linea con i target sopra descritti e secondo la roadmap di attuazione prevista dal Piano Nazionale di Ripresa e Resilienza (PNRR), dovrà integrarsi alla Piattaforma Notifiche Digitali - CAP3.PA.LA26.

Capitolo 4. Infrastrutture

Lo sviluppo delle infrastrutture digitali 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.

Tuttavia, l'evoluzione tecnologica espone 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 PA.

Come già rilevato a suo tempo da AgID attraverso il Censimento del Patrimonio ICT della PA, molte infrastrutture della risultano prive dei requisiti di sicurezza e di affidabilità necessari e, inoltre, sono carenti sotto il profilo strutturale ed 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 ed 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.

Nel delineare il processo di razionalizzazione delle infrastrutture è necessario considerare che, nel settembre 2021, il Dipartimento per la Trasformazione Digitale e l'Agenzia per la Cybersicurezza Nazionale (ACN) hanno pubblicato il documento di indirizzo strategico sul cloud intitolato "Strategia Cloud Italia".

Tale documento si sviluppa lungo tre direttrici fondamentali:

1) la creazione del PSN (Polo Strategico Nazionale, l'infrastruttura per garantire la sicurezza e l'autonomia tecnologia sugli asset strategici del Paese), la cui gestione e controllo di indirizzo siano autonomi da fornitori extra UE, destinato ad ospitare sul territorio nazionale principalmente dati e servizi strategici la cui compromissione può avere un impatto sulla sicurezza nazionale, in linea con quanto previsto in materia di perimetro di sicurezza nazionale cibernetica dal Decreto Legge 21 settembre 2019, n. 105 e dal DPCM 81/2021;

2) un percorso di qualificazione dei fornitori di cloud pubblico e dei loro servizi per garantire che le caratteristiche e i livelli di servizio dichiarati siano in linea con i requisiti necessari di sicurezza, affidabilità e rispetto delle normative rilevanti;

3) lo sviluppo di una metodologia di classificazione dei dati e dei servizi gestiti dalle PPAA, per permettere una migrazione di questi verso la soluzione cloud più opportuna (PSN o adeguata tipologia di cloud qualificato).

Per realizzare un'adeguata evoluzione tecnologica e supportare il paradigma cloud, favorendo altresì la razionalizzazione delle spese per la connettività delle PPAA, è stato aggiornato il modello di connettività.

Tale aggiornamento renderà disponibili alle PPAA servizi di connettività avanzati, atti a potenziare le prestazioni delle reti delle PA e a soddisfare la più recente esigenza di garantire lo svolgimento del lavoro agile in sicurezza.



Contesto normativo e strategico

Riferimenti normativi nazionali:

- Decreto legislativo 7 marzo 2005, n. 82, “Codice dell’Amministrazione Digitale”, artt. 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”, art. 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 PPAA 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 PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la PA, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la PA (2021).
- Determinazioni ACN in attuazione al precedente Regolamento n. 306/2022 (con allegato) su e n. 307/2022 (con allegato).
- 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).

Obiettivi e risultati attesi

OB.4.3 - Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PPAA:

- *R.A.4.3a - Disponibilità di servizi di connettività Internet a banda larga e ultra-larga per le PA locali*
 - Target 2023: passaggio a connettività FTTH se disponibile;
 - Target 2024: passaggio a connettività FTTH se disponibile;
 - Target 2025: passaggio a connettività FTTH se disponibile.



Cosa deve fare l'Amministrazione

OB.4.3 - Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PPAA:

- da gennaio 2024 - Le PPAA possono acquistare i servizi della nuova gara di connettività SPC - CAP4.PA.LA23.

Capitolo 5. Interoperabilità

L'interoperabilità permette la collaborazione e l'interazione digitale tra PPAA, cittadini ed imprese, favorendo l'attuazione del principio *once only* e recependo le indicazioni dell'*European Interoperability Framework*.

Questo capitolo si concentra sul livello di interoperabilità tecnica e si coordina con gli altri sui restanti livelli: giuridico, organizzativo e semantico.

Per l'interoperabilità semantica si consideri il Capitolo 2 "Dati" e il Capitolo 3 "Piattaforme" e per le tematiche di sicurezza il Capitolo 6 "Sicurezza informatica".

L'insieme delle Linee Guida sull'interoperabilità costituisce il Modello di interoperabilità (ModI) ed individua gli standard e le loro modalità di utilizzo per l'implementazione delle API favorendo:

- l'aumento dell'interoperabilità tra PPAA e tra queste e cittadini/imprese;
- la qualità e la sicurezza delle soluzioni realizzate;
- la de-duplicazione e la co-creazione delle banche dati e delle relative API, migliorando il trattamento dei dati e la loro gestione.

Le "Linee guida sull'interoperabilità tecnica delle PPAA" adottate da AgID con Determinazione n. 547 del 1° ottobre 2021, individuano le tecnologie SOAP e REST da utilizzare per l'implementazione delle API e, per esse, le modalità di loro utilizzo attraverso l'individuazione di pattern e/o profili da applicarsi da parte delle PPAA e sono periodicamente aggiornate in modo da assicurare il confronto continuo con:

- le PPAA, per determinare le esigenze operative delle stesse;
- i Paesi Membri dell'Unione Europea e gli organismi di standardizzazione, per agevolare la realizzazione di servizi digitali transfrontalieri.

Nell'ambito del Sub-Investimento MIC1_1.3.1 "Piattaforma nazionale digitale dei dati" del Piano Nazionale di Ripresa e Resilienza, sarà realizzata la Piattaforma Digitale Nazionale Dati (PDND).

La PDND permette di autorizzare ed autenticare le PPAA alla comunicazione tra i loro sistemi informativi ed alla condivisione dei dati a loro disposizione, realizzando l'interoperabilità attraverso l'esposizione di servizi digitali implementati dalle necessarie API. La Piattaforma contribuisce alla realizzazione del principio *once only* ed in futuro, dovrà consentire anche l'accesso ai big data prodotti dalle amministrazioni l'elaborazione di politiche *data-driven*.

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. 12, 15, 50, 50-ter, 73 e 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 PPAA (2021).
- Linee Guida AgID sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi e delle basi di dati (2021).



- 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.
- Piano Nazionale di Ripresa e Resilienza:
 - Investimento M1C1 1.3: "Dati e interoperabilità";
 - Investimento M1C1 2.2: "Task Force digitalizzazione, monitoraggio e performance".

Riferimenti normativi europei:

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

Obiettivi e risultati attesi

OB.5.2 - Adottare API conformi al Modello di Interoperabilità:

- *R.A.5.2a - Incremento del numero delle amministrazioni registrate in PDND e fruitrici di API*

Cosa deve fare l'Amministrazione

Entro giugno 2023 il Piano Triennale dell'AgID prevede la migrazione del catalogo delle API da developers.italia a PDND - (Dipartimento per la Trasformazione Digitale) - CAP5.LA20. Pertanto, entro dicembre 2024 verrà programmata la registrazione alla piattaforma e di seguito una verifica di eventuali API utilizzabili dall'Ordine. Identicamente entro dicembre 2025 verranno verificate le nuove API disponibili e se possono essere utili all'Ordine.

Capitolo 6. Sicurezza informatica

La Direttiva NIS 2, di prossima pubblicazione sulla Gazzetta Ufficiale dell'UE e destinata ad abrogare la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, pone particolare rilevanza all'innalzamento dei livelli di cybersecurity delle reti e dei sistemi informativi degli Stati membri.

Tale obiettivo viene altresì perseguito dalla Strategia Nazionale di Cybersicurezza 2022/2026 e dal relativo Piano di implementazione, attualmente in fase di definizione, relativamente al modello di misurazione dell'implementazione delle tempistiche e dei target delle misure, che contemplano una serie di azioni volte a rafforzare la cybersecurity delle PPAA, sia intervenendo a livello tecnico, sia accrescendo la consapevolezza e le competenze dei pubblici dipendenti e degli utenti dei servizi pubblici.

Appare, infatti, essenziale garantire servizi digitali non solo efficienti e facilmente accessibili, ma anche sicuri e resilienti sotto il profilo informatico, così da accrescerne l'affidabilità e l'utilizzo anche da parte di utenti meno avvezzi all'impiego di tecnologie digitali. La crescente risonanza e copertura mediatica data ad incidenti e ad attacchi cyber, se da un lato contribuisce ad accrescere il livello di consapevolezza sui rischi dello spazio cibernetico, dall'altro può ingenerare un senso di insicurezza nell'impiego dello strumento digitale.

Per superare tali timori è, quindi, essenziale, un approccio olistico alla cybersecurity, attraverso una gestione continuativa ed automatizzata del rischio cyber, che contempli un'architettura "zero trust", per la cui implementazione è essenziale la collaborazione degli utenti, interni ed esterni alla PA, ma anche dei fornitori di beni e servizi ICT.

A partire dall'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN), è tuttora in fase di revisione, l'architettura nazionale cyber, tramite il progressivo trasferimento di competenze dai soggetti che ne esercitavano le funzioni alla stessa ACN: per tale motivo, come meglio descritto in seguito, i target e le linee di azione relative al triennio di competenza del Piano, potranno essere integrati a seguito della definizione di appositi indicatori del Piano di implementazione della Strategia Nazionale di Cybersicurezza 2022/2026.

Contesto normativo e strategico

Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale (in breve CAD), art. 51.
- 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.
- 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 del Presidente del Consiglio dei Ministri 17 maggio 2022 - Adozione della Strategia nazionale di cybersicurezza 2022-2026 e del Piano di implementazione 2022/2026.
- Linee guida sulla sicurezza nel procurement ICT (2020).
- Misure minime di sicurezza ICT per le PPAA.
- Piano Nazionale per la Protezione Cibernetica 2017.
- Piano Nazionale di Ripresa e Resilienza - Investimento 1.5: "Cybersecurity".

Riferimenti normativi europei:

- Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio - Regolamento eIDAS.
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 in materia di protezione dei dati personali.
- The EU's Cybersecurity Strategy for the Digital Decade (2020).

Obiettivi e risultati attesi

OB.6.1 - Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PPAA:

- *R.A.6.1a - Incremento del livello di Cyber Security Awareness misurato tramite questionari di self-assessment ai RTD*
 - Target 2023: esecuzione del test al RTD;
 - Target 2024: esecuzione del test al RTD;
 - Target 2025: esecuzione del test al RTD.

OB.6.2 - Aumentare il livello di sicurezza informatica dei portali istituzionali della PA:

- *R.A.6.2a - Incremento del numero dei portali istituzionali che utilizzano il protocollo HTTPS only, misurato tramite tool di analisi specifico*
 - Target 2023: monitoraggio del protocollo HTTPS;
 - Target 2024: monitoraggio del protocollo HTTPS;
 - Target 2025: monitoraggio del protocollo HTTPS.
- *R.A.6.2b - Massimizzare il numero dei Content Management System (CMS) con versione aggiornata utilizzati nei portali istituzionali delle PA, misurato tramite tool di analisi specifico*
 - Target 2023: monitoraggio aggiornamento del CMS e plugin;
 - Target 2024: monitoraggio aggiornamento del CMS e plugin;
 - Target 2025: monitoraggio aggiornamento del CMS e plugin.

Cosa deve fare l'Amministrazione

OB.6.1 - Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PPAA:

- le PPAA continuano a seguire le misure minime di sicurezza ICT per le PPAA - CAP6.PA.LA06;
- le PPAA possono definire, in funzione delle proprie necessità, all'interno dei piani di formazione del personale, interventi sulle tematiche di Cyber Security Awareness - CAP6.PA.LA05.

OB.6.2 - Aumentare il livello di sicurezza informatica dei portali istituzionali della PA

- le PPAA devono mantenere costantemente aggiornati i propri portali istituzionali ed applicare le correzioni alle vulnerabilità - CAP6.PA.LA08.
- le PPAA, in funzione delle proprie necessità, possono utilizzare il tool di self assessment per il controllo del protocollo HTTPS e la versione del CMS messo a disposizione da AgID - CAP6.PA.LA09.



Capitolo 7. Le leve per l'innovazione

Le PPAA sono chiamate ad attuare progetti ad elevato contenuto di innovazione, volti non soltanto alla razionalizzazione dei costi di gestione e allo sviluppo dei servizi in un'ottica di modernizzazione degli stessi, ma anche al rafforzamento di un processo di trasformazione dei servizi pubblici offerti a cittadini ed imprese che stimoli la domanda pubblica, accresca la competitività dei territori e punti al miglioramento qualitativo delle prestazioni fornite dal mercato.

La Pubblica Amministrazione italiana svolge ogni anno milioni di procedure di appalto. La digitalizzazione completa delle procedure promette una significativa riduzione di costi e tempi, facilita la partecipazione di tutti gli operatori economici, anche delle PMI e delle startup che dispongono di una minore capacità finanziaria.

La digitalizzazione delle procedure di appalto necessita di un'apposita piattaforma di e-procurement, costituita da un insieme coordinato e normato di servizi, banche dati e sistemi di trasmissione, su cui si appoggiano gli applicativi verticali di negoziazione ed acquisto.

Nel triennio 2022/2024 il PNRR prevede la revisione del Codice dei contratti pubblici, che avrà, come conseguenza, anche l'aggiornamento delle regole tecniche delle piattaforme di e-procurement delle singole Amministrazioni.

Gli obiettivi del Piano Triennale potranno essere raggiunti solo attraverso azioni di sensibilizzazione e di formazione che coinvolgono necessariamente i dipendenti della PA.

Il re-skilling e up-skilling su tematiche connesse alla trasformazione digitale, rappresenta uno dei pilastri dell'imponente investimento previsto nell'ambito del PNRR sul capitale umano della PA italiana e della Strategia "Riformare la PA. Persone qualificate per qualificare il Paese", promossa dal Ministro per la PA a gennaio 2022.

L'iniziativa "Syllabus per la formazione digitale" che mira a consentire a tutti i dipendenti delle amministrazioni che aderiscono all'iniziativa, l'accesso a percorsi formativi sulle competenze digitali messi a disposizione da grandi player del mondo ICT e della formazione, erogati in e-learning e personalizzati a partire da una rilevazione online, strutturata ed omogenea dei fabbisogni individuali di formazione. L'iniziativa "Syllabus per la formazione digitale", il cui impianto - ulteriormente arricchito e potenziato - si basa sul progetto del Dipartimento della Funzione Pubblica "Competenze digitali per la PA" finanziato con il PON Governance e Capacità Istituzionale 2014/2020, rientra tra gli interventi finanziati nell'ambito del sub-investimento 2.3.1 in istruzione e formazione a valere sulla Missione 1, Componente 1 del PNRR.

A questa attività si sono aggiunte iniziative "verticali": la formazione specifica sui temi della qualità dei dati, dell'accessibilità, della security awareness, del governo e della gestione dei progetti ICT, rivolta a tutti i dipendenti della PA; la formazione e l'aggiornamento sui temi della trasformazione digitale e del governo dei processi di innovazione per i Responsabili per la Transizione al digitale.

Contesto normativo e strategico

Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'Amministrazione Digitale" (in breve CAD), art. 13.
- Competenze digitali, documento AgID, 13 febbraio 2020.
- Syllabus "Competenze digitali per la PA" (2020).
- Strategia Nazionale per le competenze digitali (2020).
- Piano Operativo della Strategia Nazionale per le competenze digitali (2020).
- Guida AgID dei diritti di cittadinanza digitale (2022).
- Piano Nazionale di Ripresa e Resilienza:
 - Investimento 1.7: "Competenze digitali di base";
 - Investimento 2.3: "Competenze e capacità amministrativa" 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.
- Raccomandazione del Consiglio del 22 maggio 2018 relativa alle competenze chiave per l'apprendimento permanente (GU 2018/C 189/01).

Obiettivi e risultati attesi

OB.7.2 - Rafforzare le competenze digitali per la PA e per il Paese e favorire l'inclusione digitale:

- *R.A.7.2a - Diffusione delle competenze digitali nella PA, attraverso la promozione dell'accesso da parte dei dipendenti pubblici a percorsi formativi sulle competenze digitali in e-learning*



- Target 2023: verifica di percorsi di formazione basate sul Syllabus “Competenze digitali per la PA” che prevedono la rilevazione delle competenze possedute attraverso lo strumento di self-assessment online promosso dal Dipartimento della Funzione Pubblica e su formazione su misura mirata ad accrescere le competenze e colmare le lacune tecniche informatiche;

- Target 2024: verifica di percorsi di formazione basate sul Syllabus “Competenze digitali per la PA” che prevedono la rilevazione delle competenze possedute attraverso lo strumento di self-assessment online promosso dal Dipartimento della Funzione Pubblica e su formazione su misura mirata ad accrescere le competenze e colmare le lacune tecniche informatiche;

- Target 2025: verifica di percorsi di formazione basate sul Syllabus “Competenze digitali per la PA” che prevedono la rilevazione delle competenze possedute attraverso lo strumento di self-assessment online promosso dal Dipartimento della Funzione Pubblica e su formazione su misura mirata ad accrescere le competenze e colmare le lacune tecniche informatiche.

• *R.A.7.2c - Diffusione delle competenze digitali nella PA per l’attuazione degli obiettivi del Piano triennale*

Target 2023: verifica di corsi e-learning-blended (SNA) o webinar o MOOC (Massive Open Online Courses) per dipendenti pubblici (Formez) o privati personalizzando il percorso formativo in base all’ambito applicativo e sulla base delle lacune di ciascun dipendente;

Target 2024: verifica di corsi e-learning-blended (SNA) o webinar o MOOC (Massive Open Online Courses) per dipendenti pubblici (Formez) o privati personalizzando il percorso formativo in base all’ambito applicativo e sulla base delle lacune di ciascun dipendente;

Target 2025: verifica di corsi e-learning-blended (SNA) o webinar o MOOC (Massive Open Online Courses) per dipendenti pubblici (Formez) o privati personalizzando il percorso formativo in base all’ambito applicativo e sulla base delle lacune di ciascun dipendente.

Cosa deve fare l’Amministrazione

OB.7.2 - Rafforzare le competenze digitali per la PA e per il Paese e favorire l’inclusione digitale:

- le PPAA, in funzione delle proprie necessità, partecipano alle iniziative pilota, alle iniziative di sensibilizzazione e a quelle di formazione di base e specialistica previste dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali - CAP7.PA.LA12;

- le PPAA, in funzione delle proprie necessità, 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 - CAP7.PA.LA19;

- le PPAA, in funzione delle proprie necessità, partecipano alle attività di formazione “Monitoraggio dei contratti ICT” secondo le indicazioni fornite da AgID - CAP7.PA.LA13;

- le PPAA, in funzione delle proprie necessità, utilizzano tra i riferimenti per i propri piani di azione quanto previsto nel Piano operativo della strategia nazionale per le competenze digitali aggiornato - CAP7.PA.LA15.



PARTE III - LA GOVERNANCE

Capitolo 8. Governance

I cambiamenti che hanno investito il nostro Paese negli ultimi anni, anche a causa della crisi pandemica, sono stati accompagnati da una serie di novità normative e da nuove opportunità che hanno l'obiettivo di dare un'ulteriore spinta al processo di trasformazione digitale già iniziata. Il Piano triennale, in questo contesto, si pone come strumento di sintesi tra le differenti linee di trasformazione digitale della PA.

Tra queste va data rilevanza a quella rappresentata dal Piano Nazionale di Ripresa e Resilienza (PNRR), inserita nel programma Next Generation EU (NGEU). In particolare, la Missione 1 del PNRR si pone l'obiettivo di dare un impulso decisivo al rilancio della competitività e della produttività del Sistema Paese affidando alla trasformazione digitale un ruolo centrale. Lo sforzo di digitalizzazione ed innovazione è centrale in questa Missione, ma riguarda trasversalmente anche tutte le altre.

In questo mutato contesto, obiettivi ed azioni del Piano triennale, dunque, non possono che essere definiti ed individuati in accordo con le indicazioni del PNRR.

Da questo punto di vista, è importante evidenziare che il Decreto Legge 31 maggio 2021 n. 77 c.d. "Semplificazioni" (come convertito con la legge n. 108/2021), contiene disposizioni in ordine all'organizzazione della gestione del Piano Nazionale di Ripresa e Resilienza, definendo i ruoli ricoperti dalle diverse Amministrazioni coinvolte nonché le modalità di monitoraggio del Piano e del dialogo con le autorità europee.

In tale scenario, si rende strategico attivare e mettere a disposizione dei RTD specifici strumenti utili a favorire percorsi di incontro caratterizzati da canali di informazione, condivisione ed approfondimento su specifici temi e relative pratiche: le comunità digitali tematiche/territoriali nella community dei RTD, disponibile all'indirizzo retedigitale.gov.it, hanno questo intento e mirano a favorire forme di rafforzamento del sistema dei RTD su temi specialistici per supportare l'attuazione dei processi di trasformazione digitale in linea con la strategia nazionale e con le previsioni del presente Piano Triennale.

Il monitoraggio del Piano triennale

Il monitoraggio del Piano triennale si compone delle seguenti attività:

- misurazione dei risultati (R.A.) conseguiti dal sistema PA per ciascuna componente tecnologica e non tecnologica del Piano;
- analisi della spesa e degli investimenti pubblici in ICT delle PPAA centrali e locali componenti il relativo panel;
- avvio di una riflessione su un processo di allineamento tra gli indicatori e gli obiettivi del Piano stesso e gli strumenti di misurazione e monitoraggio già presenti nei diversi strumenti di programmazione. A tal proposito si prenderanno in considerazione:
 - gli obiettivi della Strategia Italiana sul digitale "Italia Digitale 2026";
 - il target del PNRR, con particolare riferimento con quanto previsto nella Missione 1;
 - le misure del programma europeo "Percorso per il decennio digitale", che prevede un sistema di monitoraggio strutturato, trasparente e condiviso basato sull'indice di digitalizzazione dell'economia e della società (DESI) per misurare i progressi compiuti verso ciascuno degli obiettivi per il 2030.

L'attuazione di queste azioni ha la finalità di ottenere una visione delle attività svolte dalle Amministrazioni in relazione alla loro coerenza con il Piano triennale con la possibilità di introdurre azioni correttive necessarie per il raggiungimento degli obiettivi previsti dalle strategie nazionali ed europee.

Contesto normativo e strategico

- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'Amministrazione Digitale" (in breve CAD) artt. 14-bis, lettera c e 18-bis.
- 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" artt. 1-11 e art. 41.
- Decreto Legge 30 aprile 2022, n. 36, convertito con modificazioni dalla Legge 29 giugno 2022, n. 79 "Ulteriori misure urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR)".
- Regolamento AgID recante le procedure di contestazione, accertamento, segnalazione delle violazioni in materia di transizione digitale e di esercizio del potere sanzionatorio ai sensi dell'art. 18-bis del d. lgs. 7 marzo 2005, n. 82 e successive modifiche (2021).

- Strategia “Italia Digitale 2026” (2021).
- Communication: “2030 Digital Compass: the European way for the Digital Decade” (2021).

Il monitoraggio del Piano triennale:

- Direttiva di definizione degli obiettivi dell’Agenzia per l’Italia Digitale (2022).
- Proposal for a Decision establishing the 2030 Policy Programme “Path to the Digital Decade”.
- The Digital Economy and Society Index (DESI)

Obiettivi e risultati attesi

OB.8.1 - Migliorare i processi di trasformazione digitale della PA:

- *R.A.8.1h - Rafforzamento del livello di coerenza (raccordo) delle programmazioni ICT delle PA con il Piano triennale*
 - Target 2023: verifica coerenza delle programmazioni annuali con il Piano Triennale e verifica dell’adesione alle piattaforme di community di RTD;
 - Target 2024: verifica coerenza delle programmazioni annuali con il Piano Triennale e verifica dell’adesione alle piattaforme di community di RTD;
 - Target 2025: verifica coerenza delle programmazioni annuali con il Piano Triennale e verifica dell’adesione alle piattaforme di community di RTD.

Cosa deve fare l’Amministrazione

OB.8.1 - Migliorare i processi di trasformazione digitale della PA:

- verifica annuale dell’implementazione delle attività previste nel Piano triennale ed eseguire un calendario operativo per quelle ancora da espletare;
- verifica di adesione alla piattaforma di community al fine di partecipare attivamente ai lavori - CAP8.PA.LA07.
- verifica di adesione, in base alle proprie esigenze, ad iniziative di formazione per RTD e loro Uffici, proposte da AgID - CAP8.PA.LA32.

Capitolo 9. Indicazioni per le PPA

L’aggiornamento 2023/2025 del Piano Triennale dell’Ordine, mantiene inalterata la struttura del documento consolidata nella scorsa edizione e fa riferimento al Modello strategico di evoluzione ICT della PA, che descrive, in maniera funzionale, la trasformazione digitale, attraverso due livelli trasversali relativi ad interoperabilità e sicurezza informatica e quattro livelli verticali per servizi, dati, piattaforme ed infrastrutture.

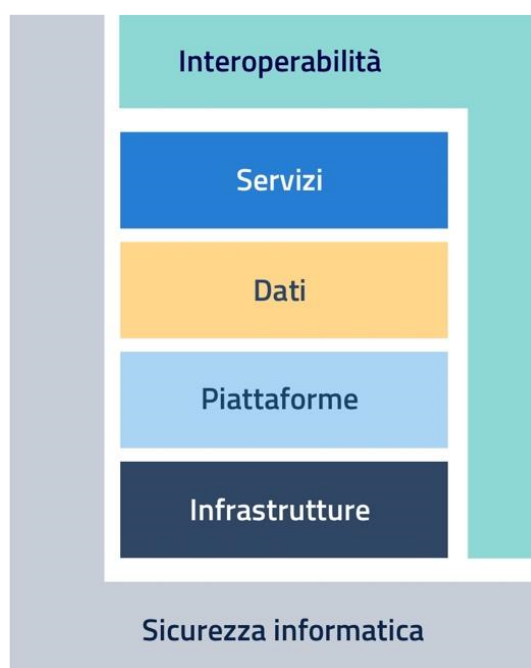


Immagine 1 - Rappresentazione del modello Strategico



In sintesi, l'aggiornamento offerto nella presente edizione, ha riguardato, in particolare:

- la revisione del contesto normativo e strategico, in linea con gli ultimi interventi legislativi e le più recenti linee guida adottate;
- l'adeguamento di obiettivi, risultati attesi e linee di azione per gli anni 2023, 2024 e 2025, sulla base degli esiti del monitoraggio 2022, con l'integrazione di riferimenti diretti a target e investimenti previsti dal PNRR;
- la riformulazione e ripianificazione delle linee di azione del Piano Triennale precedente che non hanno raggiunto la naturale conclusione.



SERVIZI

Cod. Ob.	Obiettivo PT 2023/2025	Cod. RA PT 2023/2025	Risultato atteso 2023/2025
OB.1.1	Migliorare la capacità di generare ed erogare servizi digitali	R.A.1.1d	Diffusione del monitoraggio, da parte delle Amministrazioni, della fruizione dei servizi digitali
OB.1.2	Migliorare l'esperienza d'uso e l'accessibilità dei servizi	R.A.1.2a	Incremento e diffusione dei modelli standard per lo sviluppo di siti disponibili in Designers Italia
		R.A.1.2c	Incremento dell'accessibilità dei servizi digitali della PA, secondo quanto indicato dalle Linee guida sull'accessibilità degli strumenti informatici
OB.1.4	Adeguamento dei servizi di recapito certificato qualificato a norma del regolamento eIDAS	R.A.1.4a	Migrazione dalla PEC ai servizi SERCQ

DATI

Cod. Ob.	Obiettivo PT 2023/2025	Cod. RA PT 2023/2025	Risultato atteso 2023/2025
OB.2.2	Aumento del numero di dataset di tipo aperto resi disponibili dalle PPAA	R.A.2.2b	Aumento del numero di dataset di tipo aperto resi disponibili dalle PPAA

PIATTAFORME

Cod. Ob.	Obiettivo PT 2023/2025	Cod. RA PT 2023/2025	Risultato atteso 2023/2025
OB.3.1	Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa	R.A.3.1c	Incremento del numero di Amministrazioni servite in NoiPA ed estensione del numero di servizi offerti dalla piattaforma (fiscale, previdenziale ecc.) utilizzati
OB.3.2	Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PPAA	R.A.3.2a	Incremento dell'adozione e dell'utilizzo di SPID e CIE da parte delle PPAA
OB.3.3	Incrementare e razionalizzare il numero di piattaforme per le Amministrazioni al fine di semplificare i servizi ai cittadini	R.A.3.3b	Realizzazione della Piattaforma Indice nazionale dei domicili digitali delle persone fisiche e degli altri enti di diritto privato non tenuti all'iscrizione in albi professionali o nel Registro Imprese (INAD)
		R.A.3.3d	Realizzazione del Sistema Gestione Deleghe (SGD) digitali al fine di agevolare la fruizione dei servizi online attraverso soggetti delegati

INFRASTRUTTURE

Cod. Ob.	Obiettivo PT 2023/2025	Cod. RA PT 2023/2025	Risultato atteso 2023/2025
OB.4.3	Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA	R.A.4.3a	Disponibilità di servizi di connettività Internet a banda larga e ultra larga per le PA locali



INTEROPERABILITA'

Cod. Ob.	Obiettivo PT 2023/2025	Cod. RA PT 2023/2025	Risultato atteso 2023/2025
OB.5.2	Adottare API conformi al Modello di Interoperabilità	R.A.5.2a	Incremento del numero delle Amministrazioni registrate in PDND e fruitrici di API

SICUREZZA

Cod. Ob.	Obiettivo PT 2023/2025	Cod. RA PT 2023/2025	Risultato atteso 2023/2025
OB.6.1	Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA	R.A.6.1a	Incremento del livello di Cyber Security Awareness misurato tramite questionari di self-assessment ai RTD e ai loro uffici
OB.6.2	Aumentare il livello di sicurezza informatica dei portali istituzionali della P.A.	R.A.6.2a	Incremento del numero dei portali istituzionali che utilizzano il protocollo HTTPS only, misurato tramite tool di analisi specifico
		R.A.6.2b	Massimizzare il numero dei Content Management System (CMS) con versione aggiornata utilizzati nei portali istituzionali delle PA, misurato tramite tool di analisi specifico

LEVE PER L'INNOVAZIONE

Cod. Ob.	Obiettivo PT 2023/2025	Cod. RA PT 2023/2025	Risultato atteso 2023/2025
OB.7.2	Rafforzare le competenze digitali per la PA e per il Paese e favorire l'inclusione digitale	R.A.7.2a	Diffusione delle competenze digitali nella PA, attraverso la promozione dell'accesso da parte dei dipendenti pubblici a percorsi formativi sulle competenze digitali in e-learning
		R.A.7.2c	Diffusione delle competenze digitali nella PA per l'attuazione degli obiettivi del Piano triennale



Appendice - Acronimi

ACRONIMO	DEFINIZIONE
AgID	Agenzia per l'Italia Digitale
ANPR	Anagrafe nazionale popolazione residente
API	Application Programming Interface
CAD	Codice dell'amministrazione digitale
ICT	Information and Communication Technologies
PEC	posta elettronica certificata
SERCQ	servizi elettronici di recapito certificato qualificati
DPCM	decreto del Presidente del Consiglio dei ministri
CAD	Codice dell'Amministrazione Digitale
PND	Piattaforma Notifiche Digitali
SGD	Sistema Gestione Deleghe
eIDAS	electronic IDentification Authentication and Signature
GDPR	General Data Protection Regulation
SPID	Sistema Pubblico di Identità Digitale
CIE	Carta di Identità Elettronica
INAD	Indice nazionale dei domicili digitali
ACN	Agenzia per la Cybersicurezza Nazionale
PSN	Polo Strategico Nazionale
FTTH	Fiber to the Home
SOAP	Simple Object Access Protocol
REST	REpresentational State Transfer
PDND	Piattaforma Digitale Nazionale Dati
NIS	Network and Information Security
CSIRT	Computer Security Incident Response Team
RTD	Responsabile per la Transizione al Digitale
HTTPS	Hyper Text Transfer Protocol Secure
CMS	Content Management System
SNA	Scuola Nazionale dell'Amministrazione
MOOC	Massive Open Online Courses
NGEU	Next Generation EU

Ufficio virtuale per la Transizione al Digitale

Responsabile, Alessandra Poleselli
Componente, avv. Elena Pietropaoli
Componente, ing. Mirko Tarantelli