

PIANO TRIENNALE PER L'INFORMATICA
CONSIGLIO NOTARILE DI MODENA
2024 – 2026

INDICE

I. Introduzione

Premessa

Contesto strategico

Contesto esterno

Contesto interno

Spesa complessiva prevista per ogni annualità del piano

II. Organizzazione per la trasformazione digitale

Governare la trasformazione digitale

Leve per l'innovazione

III. Componenti tecnologiche

Servizi

Dati e Intelligenza artificiale

Piattaforme

Infrastrutture

Interoperabilità

Sicurezza informatica

PARTE I

INTRODUZIONE

1. Premessa

Come noto, il Piano triennale per l'informatica nella PA, elaborato dall'Agenzia per l'Italia digitale descrive le linee strategiche definite dal Governo e detta indirizzi generali per tutte le pubbliche amministrazioni.

Sulla base della strategia nazionale ogni Ente realizza il proprio Piano Triennale e lo aggiorna annualmente.

Con riferimento all'aggiornamento di quest'anno, la programmazione è relativa al triennio 2024-2026 e tiene in considerazione il peculiare contesto all'interno del quale la stessa si inserisce.

Le sfide dei prossimi anni concernono la gestione del cambiamento accelerato dalla pandemia da Covid-19 nel mondo sociale e professionale, richiedendo una netta trasformazione verso nuovi orizzonti in termini di digitalizzazione, transizione ecologica, mobilità sostenibile, istruzione, inclusione e coesione sociale e salute. Tali obiettivi sono, peraltro, previsti dalle linee di sviluppo e investimento individuate dall'UE per il rilancio dell'economia e della vita in Europa.

In particolare, il Piano Nazionale di Ripresa e Resilienza (PNRR) è lo strumento che, grazie ai fondi del Next Generation EU (NGEU), prevede un'azione ingente di investimento di oltre 190 miliardi di euro in risposta alla crisi pandemica.

Tale portata di investimenti produrrà nei prossimi anni una ulteriore forte accelerazione nei processi di innovazione in atto e le linee tracciate dal Piano Triennale assumeranno progressivamente una rilevanza maggiore e renderanno ancora più sfidante il quadro delineato.

Nella componente del PNRR denominata "Digitalizzazione, innovazione e sicurezza nella PA", sono previsti investimenti pari a 9,75 miliardi di euro. La quota di investimento più rilevante in questa componente è rappresentata da "Digitalizzazione PA" alla quale sono destinati 6,14 miliardi di euro: all'interno di questa misura rientrano diversi investimenti che riguardano alcune delle tematiche affrontate nei successivi capitoli del presente aggiornamento del Piano Triennale. Questa misura contribuirà in maniera determinante a supportare la strategia di digitalizzazione in corso, erogando finanziamenti per progetti specifici, finalizzati all'attuazione di quanto previsto nel CAD e nell'ulteriore normativa di riferimento.

Attraverso il Piano Triennale per l'informatica il Consiglio Notarile di Modena (d'ora in avanti anche solo "**Consiglio**"), partendo dallo stato dell'arte dei processi di digitalizzazione, fissa degli obiettivi di miglioramento dell'organizzazione per la trasformazione digitale e delle singole componenti tecnologiche.

Tra gli obiettivi sostanziali del Piano vi è la semplificazione del rapporto con gli iscritti e la realizzazione delle infrastrutture e delle piattaforme abilitanti.

2. Contesto strategico

Il 12 febbraio 2024 è stato pubblicato sul sito dell'Agenzia per l'Italia Digitale (AgID) il nuovo Piano Triennale per l'informatica nella Pubblica Amministrazione 2024-2026, il documento di indirizzo strategico ed economico che dovrà guidare operativamente le Amministrazioni nella trasformazione digitale.

L'ultimo aggiornamento del Piano triennale per l'informatica nella PA 2024-2026 arriva in un momento cruciale per il processo di transizione digitale della pubblica amministrazione.

La digitalizzazione, infatti, rappresenta uno dei tre assi strategici attorno a cui ruota il Piano Nazionale di Ripresa e Resilienza (PNRR), il piano straordinario di riforme e investimenti del Governo che si colloca nell'ambito del programma europeo Next Generation EU e che si pone l'obiettivo di superare le conseguenze socio economiche derivanti dalla crisi pandemica.

Il PNRR, dunque, produrrà nei prossimi anni necessariamente un'ulteriore forte accelerazione nei processi di innovazione in atto.

Il nuovo Piano Triennale per l'informatica è stato redatto da un gruppo di lavoro formato dal personale di AgID, del Dipartimento per la trasformazione digitale e di PagoPA S.p.A. e ha visto la collaborazione di numerosi stakeholders.

Si tratta del sesto aggiornamento del Piano, che costituisce l'aggiornamento delle precedenti edizioni (2017-2019, 2019-2021, 2020-2022, 2021-2023, 2022- 2024). Di conseguenza, il documento non si discosta molto dai percorsi già intrapresi, con l'intento dichiarato di assicurare continuità alle azioni di trasformazione già avviate e, dunque, di non disperdere quanto di buono realizzato finora.

Il documento, definitivamente approvato con decreto del Presidente del Consiglio dei Ministri, come previsto dal Codice dell'Amministrazione Digitale, tiene conto del mutato contesto legato all'attuazione del Piano Nazionale di Ripresa e Resilienza - PNRR in materia di trasformazione digitale e considera la necessità di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana in coerenza con l'Agenda digitale europea, assicurando, altresì, lo svolgimento dei compiti necessari per l'adempimento degli obblighi internazionali assunti in materia di innovazione tecnologica e digitale.

Dal punto di vista strutturale, il Piano presenta alcuni cambiamenti rispetto alle edizioni precedenti; oltre a fornire alcuni approfondimenti per sostenere in modo efficace le pubbliche amministrazioni

In particolare, il documento si compone di tre parti, articolate in 7 capitoli tematici:

1. la **prima parte** suddivisa in due capitoli e denominata "Componenti strategiche per la trasformazione digitale", descrive le leve tecnologiche strategiche su cui le pubbliche amministrazioni dovranno investire per accelerare il processo di trasformazione digitale;

2. la **seconda parte** suddivisa in 5 capitoli e denominata “Componenti tecnologiche”, è dedicata, rispettivamente a servizi, piattaforme, dati e intelligenza artificiale, infrastrutture e sicurezza; il tema dell’interoperabilità è, invece, trasversale a tutte le componenti;

3. la **terza parte** denominata “Strumenti” costituisce una novità dell’ultimo aggiornamento ed è dedicata agli strumenti che le amministrazioni possono prendere a riferimento come modelli di supporto, esempi di buone pratiche e check-list per pianificare i propri interventi.

L'aggiornamento 2024-2026 del Piano è, inoltre, caratterizzato da una maggiore enfasi sulla governance e da un approccio fortemente incentrato sui servizi digitali, che devono essere interoperabili e sempre più accessibili per cittadini e imprese.

Inoltre, come nella precedente edizione del PTI, l’attuale aggiornamento consiste nella presenza, sempre più pervasiva, del Piano Nazionale di Ripresa e Resilienza, quale straordinaria opportunità di accelerazione della fase di esecuzione della trasformazione digitale della PA attraverso, ad esempio, il riferimento ai target e alle linee di azione del PNRR, oltre all’indicazione degli Investimenti e degli Avvisi pubblicati nell’ambito della Missione 1.

Pur assicurando la continuità con le azioni di trasformazione già intraprese, il Piano triennale per l’informatica nella PA 2024-2026 si caratterizza per alcune importanti novità.

Tra le novità del Piano triennale per l’informatica nella pubblica amministrazione 2024- 2026, vi è una “rinnovata” attenzione al tema della gestione documentale che torna ad essere trattato all’interno del documento.

In particolare l’obiettivo previsto dal Piano è quello di “Consolidare l’applicazione delle Linee guida per la formazione, gestione e conservazione documentale” che sono in vigore dall’inizio del 2022 e che delineano i necessari adeguamenti organizzativi e funzionali richiesti alle pubbliche amministrazioni in questo ambito.

Il Piano, inoltre, prosegue nel percorso di evoluzione e consolidamento delle **piattaforme** previste dalle norme (es. SPID, pagoPA, AppIO, CIE, FSE, NoiPA ecc.), distinguendole in due macro categorie:

- Piattaforme nazionali che erogano servizi a cittadini/imprese o ad altre PA, tra cui, oltre le già note AppIO, PagoPA, SPID, CIE, NoiPA, SUAP e SUE e Fascicolo Sanitario Elettronico, si aggiunge la piattaforma SEND. Tale piattaforma “SEND- Servizio Notifiche Digitali”, ha l’obiettivo di rendere più veloce, economico e sicuro l’invio e la ricezione delle notifiche a valore legale.
- Piattaforme che attestano attributi, ovverosia ANPR, ANIST e ANIS.

Nell’ambito delle **Infrastrutture** (capitolo VI), viene data continuità all’azione intrapresa con l’edizione precedente del Piano sulla razionalizzazione data center. Come è noto, nel 2019 è stato portato a termine il Censimento del Patrimonio ICT della PA, intrapreso da AgID a partire dalla

Circolare n. 5/2017, con l'obiettivo di classificare i data center in mano pubblica sulla base di criteri di efficienza, sicurezza e affidabilità delle strutture.

Tre le differenti classificazioni di data center: Poli Strategici Nazionali (PSN), Gruppo A e Gruppo B, quest'ultimi destinati a essere dismessi il prima possibile e conseguente migrazione dei servizi verso i PSN o verso i servizi cloud qualificati per la pubblica amministrazione. Detta classificazione, che da ultimo era stata confermata nella Circolare AgID n. 1/2019, oggi deve ritenersi non più attuale. Il Capitolo VI del Piano Triennale 2024-2026, infatti, ribadisce (come già previsto dall'edizione precedente) l'accorpamento dei PSN e dei data center di Gruppo A nell'unitaria categoria "A", nonché la possibilità per le amministrazioni titolari di infrastrutture del Gruppo B di stringere accordi per consolidare le infrastrutture e i servizi all'interno dei data center "A".

Inoltre, nel delineare il processo di razionalizzazione delle infrastrutture, il nuovo Piano triennale continua a considerare come propria parte integrante il documento di indirizzo strategico sul cloud intitolato "Strategia Cloud Italia", pubblicato nel settembre del 2021 dal Dipartimento per la Trasformazione Digitale e dall'Agenzia per la cybersicurezza nazionale (istituita ai sensi dell'art. 5, D.l. n. 82/2021, conv. con mod. dalla L. n. 109/2021). In ossequio a quanto previsto dalla Strategia, le attività di migrazione dovranno essere precedute dal necessario censimento e classificazione, non solo degli applicativi in uso, ma anche dei dati oggetto di migrazione. Il piano, infatti, prevede che le pubbliche amministrazioni centrali e locali sono tenute a trasmettere all'Agenzia per la cybersicurezza nazionale l'elenco e la classificazione dei dati e dei servizi digitali, per poi provvedere al consolidamento delle proprie infrastrutture o alla migrazione verso soluzioni cloud (cfr. nel Piano OB.4.1 e OB.4.2). In tal senso, occorre segnalare altresì la recente adozione del Regolamento in materia di servizi cloud, approvato con determinazione del D.G. dell'AgID del 15 dicembre 2021, n. 628.

Tale obiettivo viene altresì perseguito dalla Strategia Nazionale di Cybersicurezza 2022-2026 e dal relativo Piano di implementazione, che contemplano una serie di azioni volte a rafforzare la cybersecurity delle PA, 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. In tale prospettiva il PTI 2024-2026 introduce il concetto di cloud federato dandone una definizione coerente con la ISO/IEC 22123-1: 2023: "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".

Tali accordi possono essere posti in essere dalle "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". In ogni caso, tale Cloud federato si affianca all'infrastruttura del Polo Strategico Nazionale (PSN).

In linea con i principi enunciati e in continuità con le azioni avviate con i Piani precedenti, il nuovo Piano inoltre 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, per finalità commerciali e non, secondo il paradigma degli open data. Un asset fondamentale tra i dati gestiti dalle pubbliche amministrazioni 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. In tale contesto, però, il nuovo piano introduce per la prima volta, nel capitolo V, il tema dell'utilizzo di sistemi di intelligenza artificiale nell'attività amministrativa. Si sostiene, in particolare, che l'IA possa rispondere alla crescente necessità di migliorare l'efficienza e l'efficacia nella gestione dei servizi pubblici, specialmente negli enti locali. Le potenzialità dell'IA includono l'automazione di attività di ricerca e di analisi di informazioni semplici e ripetitive, l'aumento delle capacità predittive finalizzate a migliorare il processo decisionale basato sui dati e il supporto alla personalizzazione dei servizi orientata all'utente. Il documento sottolinea l'importanza di tener conto dei futuri impatti della regolamentazione in materia (AI Act) di prossima applicazione, definendo obiettivi e azioni concrete per la corretta gestione degli strumenti di IA nel settore pubblico mediante un approccio basato sul rischio.

Il Piano inoltre recepisce le innovazioni della riforma nazionale del procurement pubblico introdotta dal nuovo Codice dei Contratti pubblici (D.Lgs. n. 36 del 31 marzo 2023), soprattutto con riferimento alla Parte II dello stesso, "Della digitalizzazione del ciclo di vita dei contratti", introducendo un profondo percorso di trasformazione digitale degli acquisti della pubblica amministrazione volto alla semplificazione, velocizzazione delle procedure e maggiore trasparenza, in cui un ruolo fondamentale è rivestito dalla Piattaforma Digitale Nazionale dei Dati (PDND).

Sempre nell'ambito della governance della trasformazione digitale, il nuovo aggiornamento consolida l'importanza del monitoraggio sul raggiungimento degli obiettivi predefiniti: viene aggiornata la roadmap delle Linee d'Azione da porre in essere e si richiede ai Responsabili per la Transizione Digitale (RTD) di ciascun ente di rilasciare ad AgID le informazioni sullo stato di avanzamento nella roadmap mediante un Format PT per le PA, così da rendere possibile la costruzione e l'alimentazione di una base dati informativa relativa all'attuazione del Piano. Infine, Il Piano 2024-2026 introduce, nella parte terza, una sezione verticale contenente 5 strumenti operativi come esempi di buone pratiche e *tools*, utili per pianificare gli interventi delle PA. Tale introduzione rappresenta una novità del Piano di quest'anno e, in particolare, gli strumenti operativi messi a disposizione riguardano: Procurement ICT, gestione associata delle funzioni ICT, servizi prioritari da sviluppare, smart area e servizi digitali territoriali, buone prassi su IA nella PA.

3. Contesto esterno

L'analisi del contesto esterno ha come duplice obiettivo quello di evidenziare come le caratteristiche strutturali e congiunturali dell'ambiente nel quale l'amministrazione si trova ad operare possano influire sulle attività dell'Ente e, al tempo stesso, condizionare la dell'idoneità delle strategie e il monitoraggio delle misure poste in essere.

Si tratta di una fase preliminare indispensabile, se opportunamente realizzata, in quanto consente a ciascuna amministrazione di definire la propria strategia di transizione al digitale anche tenendo conto delle caratteristiche del territorio e dell'ambiente in cui opera. In particolare, l'analisi del contesto esterno consiste nell'individuazione e descrizione delle caratteristiche culturali, sociali ed economiche del territorio o del settore specifico di intervento nonché delle relazioni esistenti con gli stakeholder e di come queste ultime possano influire sull'attività dell'amministrazione.

Da un punto di vista operativo, l'analisi del contesto esterno è riconducibile sostanzialmente a due tipologie di attività: 1) l'acquisizione dei dati rilevanti; 2) l'interpretazione degli stessi ai fini della individuazione delle possibili non conformità alla normativa e degli interventi migliorativi.

Inserire informazioni relative a:

- digitalizzazione a livello locale (ad es. programmi, protocolli d'intesa, infrastrutture, accordi)
- rapporto con l'utenza e stakeholders (ad es. alfabetizzazione digitale, statistiche di utilizzo dei servizi, ecc.)

4. Contesto interno

L'Ufficio RTD del Consiglio notarile sulla base della relazione di assessment relativa agli obblighi di transizione al digitale ed allo stato di digitalizzazione dell'ente, procede alla redazione del piano triennale per l'informatica dell'ente, adeguato ai contenuti del Piano Triennale dell'AgID 2022-2024, in cui confluiscono tutte le attività relative all'attuazione della transizione digitale che richiedono programmazione (adempimenti, acquisti informatici, migrazione dei servizi, formazione del personale, etc.). Il Piano così predisposto viene condiviso con l'organo di vertice competente a deliberarne l'approvazione.

Una volta adottato, il Piano deve essere pubblicato sul sito istituzionale del Consiglio nella sezione "Amministrazione trasparente", sottosezione "Atti generali".

5. Spesa complessiva prevista per ogni annualità del piano

<i>Schema di riferimento per redazione dei contenuti</i>		
<i>identificare obiettivi di spesa ICT per il triennio di riferimento</i>	<i>Inserire sintesi illustrazione obiettivi di spesa</i>	
	<i>Annualità</i>	<i>Spesa complessiva</i>
	<i>Anno 2024</i>	<i>3.000,00</i>
	<i>Anno 2025</i>	<i>1.500,00</i>
	<i>Anno 2026</i>	<i>1.500,00</i>

PARTE II

ORGANIZZAZIONE PER LA TRASFORMAZIONE DIGITALE

1. Il ruolo del RTD nel governo della trasformazione digitale

Come noto, il CAD impone a ciascuna pubblica amministrazione di dotarsi di un'adeguata organizzazione, nominando un *“Responsabile per la transizione alla modalità digitale”* la cui figura è descritta nell'art. 17 del D.lgs. n. 82/2005, così come modificato dal D.lgs. n. 217/2017.

Al RTD – che deve essere inquadrato come un ufficio, con a capo un dirigente o una figura apicale – è affidata: *“la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità”*. La norma dispone, anzitutto, di dare attuazione al Piano Triennale per l'informatica nella PA tramite la costituzione di una rete di RTD, vale a dire un gruppo di lavoro permanente diffuso sul territorio per supportare le amministrazioni nella transizione al digitale.

In questo modo, sarà possibile stimolare il confronto, valorizzare le migliori esperienze, la condivisione di conoscenze e di progettualità e la promozione di azioni di coordinamento tra le Pubbliche amministrazioni, sia nell'ambito dei progetti e delle azioni del Piano triennale per l'informatica nella PA, sia nell'ambito di nuove iniziative che maturino dai territori.

Una volta nominato, spetta al responsabile per la transizione digitale l'impulso e il coordinamento di tutte le attività legate al rispetto delle norme in materia di digitalizzazione.

1.1. Consolidare il ruolo dell'Ufficio del Responsabile per la Transizione al Digitale del Consiglio

Con deliberazione dell'11 luglio 2022 sono state affidate le funzioni e i compiti del Responsabile per la transizione digitale al Presidente Notaio Antonio Nicolini.

Rispetto agli obiettivi definiti nel presente Piano, il RTD è in parte soggetto attuatore (per gli atti formali necessari) e per altro verso *“propulsore”* (per il rispetto delle scadenze) dell'attività che deve essere svolta dalle altre strutture amministrative del Consiglio.

La realizzazione degli obiettivi del Piano, però, richiede il coinvolgimento di tutti gli uffici e, pertanto, si ritiene necessario rafforzare le funzioni di indirizzo e coordinamento dell'Ufficio RTD, nonché la capacità di supervisione e monitoraggio dello stato di attuazione del Piano.

2. Le leve per l'innovazione

2.1. Rafforzare le leve per l'innovazione

Le “leve per l'innovazione” rappresentano gli strumenti che accompagnano il processo di trasformazione digitale della PA, migliorando l'efficacia dell'attuazione dei diversi interventi ICT.

La pubblica amministrazione può rivelarsi un importante catalizzatore di innovazione, soprattutto per il territorio, per il tessuto economico e sociale e in ultima istanza per tutti i cittadini. I bisogni digitali di tutti questi soggetti emergono e possono essere soddisfatti attraverso l'interazione continua tra Comuni, Regioni, AGID, Ministeri, mondo accademico e della ricerca e soggetti privati in grado di fornire soluzioni innovative, grazie anche a progetti specifici di ricerca e sviluppo.

Innovazione e trasformazione digitale sono strettamente interconnessi e sono tra i principali aspetti che il presente Piano triennale e quelli successivi si accingono ad affrontare.

L'innovazione guidata dalla domanda pubblica passa attraverso tre fasi di seguito sintetizzate:

1. La **generazione dell'innovazione**: innovation procurement ed open innovation.

2. La **sperimentazione e lo sviluppo dell'innovazione**:

- Nodi Territoriali di Competenza (NTC), che assumono la funzione di hub locale del CdCT (Centro di Competenza Territoriale);
- Smart community.

Il programma Smarter Italy, avviato dal Ministero dello Sviluppo Economico, in collaborazione con AGID, MID e MIUR, intende sperimentare nuove soluzioni tecnologiche, accanto a meccanismi di open innovation e appalto innovativo (Smart procurement) per i territori.

3. La **diffusione dell'innovazione con le gare strategiche**: AGID, Dipartimento per la Trasformazione Digitale e Consip assicurano una governance unitaria multi-stakeholder e una struttura organizzativa omogenea affinché gli obiettivi dei contratti stipulati nell'ambito delle gare strategiche rispondano pienamente a quanto indicato nel Piano.

Per quanto riguarda la digitalizzazione delle procedure di appalto e la messa a punto dell'infrastruttura digitale a supporto del Piano strategico nazionale di trasformazione digitale degli acquisti pubblici (Public e-procurement) coerente con gli obiettivi del Mercato Unico Digitale, la piattaforma di e-procurement per gli appalti di innovazione prevede la digitalizzazione “end to end” dell'intero processo di acquisto pubblico al fine di assicurare l'interoperabilità e l'interscambio dei dati e delle informazioni con le piattaforme di e-procurement esistenti (nazionali ed europee), sulla base degli standard di settore e di soluzioni tecniche emergenti. In materia di procurement come leva di innovazione rileva, inoltre, quanto previsto dal D.lgs. 36/2023 recante “Codice dei contratti pubblici” che prevede, tra l'altro, un impulso alla digitalizzazione delle procedure di acquisto e alla promozione delle procedure di partenariato per l'innovazione.

2.2. Competenze digitali

Un importante profilo è quello relativo alle competenze digitali per la Pubblica Amministrazione, descritte dettagliatamente nel Syllabus realizzato dal Dipartimento della funzione pubblica della Presidenza del Consiglio dei Ministri, nell'ambito dell'iniziativa "Competenze digitali per la PA", il quale rappresenta uno strumento di riferimento per la predisposizione di attività di assessment delle competenze e di percorsi formativi mirati destinati ai dipendenti della pubblica amministrazione italiana. Esso si concentra esclusivamente sugli aspetti pertinenti alle competenze digitali complementari richieste ad un dipendente pubblico che lavora in ambienti digitali, le quali rappresentano un prerequisito per operare in modo adeguato in una PA sempre più digitale.

Il Consiglio intende rafforzare le competenze digitali, non solo dei propri dipendenti, ma anche dei cittadini, attraverso iniziative formative di valutazione e di valorizzazione.

Le azioni da intraprendere in tal senso devono riguardare anzitutto il personale interno dell'ente e vanno calibrate sulla base delle diverse funzioni esercitate. In tal caso, le competenze digitali richieste possono essere di base, specialistiche e/o complementari. In secondo luogo, il rafforzamento delle competenze digitali deve essere destinato ai cittadini, per dare luogo ad una cittadinanza digitale inclusiva e consentire, così, di superare le diseguaglianze legate al *digital divide*.

PARTE III

COMPONENTI TECNOLOGICHE

1. SERVIZI

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

Come noto, la normativa prevede che, nella progettazione e nello sviluppo di un servizio online le pubbliche amministrazioni debbano tenere in considerazione le reali esigenze degli utenti, basandosi sui risultati di apposite rilevazioni e momenti di confronto.

A tal fine, l'Ufficio RTD deve assicurare l'organizzazione di attività, sia preventive che successive, di confronto e informazione con gli utenti rispetto all'attivazione di un servizio e assicurare che tramite il sito web istituzionale dell'ente siano fornite adeguate informazioni sul funzionamento del servizio.

I servizi online, inoltre, devono essere progettati e sviluppati nel rispetto delle disposizioni normative, degli standard e dei livelli di qualità individuati e periodicamente aggiornati dall'AgID

con proprie Linee guida, tenuto conto anche dell'evoluzione tecnologica. In tal senso, l'amministrazione deve garantire:

- a) la fruibilità online tutti i servizi, che devono essere accessibili, sia attraverso il sito web istituzionale, che attraverso applicazioni mobili;
- b) l'integrazione dei servizi online con i sistemi di autenticazione SPID e CIE, nonché con l'applicazione mobile IO e il sistema di pagamento pagoPA;
- c) che gli utenti possano accedere al servizio tramite un'esperienza semplice e standardizzata da un punto di vista funzionale ed estetico, assicurando l'accessibilità agli utenti portatori di disabilità;
- d) la rilevazione del grado di soddisfazione degli utenti e la predisposizione di canali di assistenza.

2. DATI E INTELLIGENZA ARTIFICIALE

Al fine di valorizzare il proprio patrimonio informativo, le pubbliche amministrazioni, nel rispetto della normativa sulla protezione dei dati personali e degli altri limiti previsti dalla normativa vigente, devono rendere disponibili i propri dati, in forma aperta e interoperabile, alle altre amministrazioni, ai cittadini e alle imprese.

In particolare, la fornitura dei *dataset* deve avvenire preferenzialmente attraverso API (interfacce per programmi applicativi) nel rispetto delle Linee guida sull'Interoperabilità (ModI), le quali devono essere documentate attraverso i metadati (ontologie e vocabolari controllati) presenti nel Catalogo Nazionale Dati per l'interoperabilità semantica ed essere registrate sul catalogo API della PDND (Piattaforma Digitale Nazionale Dati).

Occorre, dunque, effettuare un censimento delle banche dati e dei rispettivi metadati e definire una strategia per la valorizzazione del proprio patrimonio informativo, in conformità alla strategia nazionale in materia di dati e nel rispetto delle pertinenti linee guida dell'Agenzia per l'Italia Digitale.

A tal fine è necessario:

- definire ruoli e responsabilità per l'attuazione della strategia e istituire un Gruppo di lavoro dedicato, anche avvalendosi di esperti;
- elaborare la Strategia per la valorizzazione del patrimonio informativo comunale;
- richiedere, nell'acquisizione di software, funzionalità che consentano la pubblicazione automatica dei documenti e dei dati per cui sussiste un obbligo di pubblicazione, nonché degli ulteriori dati individuati nella Strategia, in conformità agli standard e alle linee guida vigenti;
- prevedere, negli atti relativi all'affidamento di servizi in concessione, l'obbligo del concessionario di rendere disponibili tutti i dati, acquisiti e generati nell'ambito del servizio, come dati di tipo aperto e formati nel rispetto della normativa vigente;

- formare, raccogliere e conservare dati in modo da consentirne la fruizione come dati di tipo aperto e di permetterne lo scambio con le altre pubbliche amministrazioni e il riutilizzo da parte dei privati, definendo la tipologia di licenza aperta con cui i dati sono rilasciati (preferibilmente CC BY 4.0);
- individuare, nell'ambito della Strategia, nel caso in cui sussistano vincoli tecnologici, economici o normativi che impediscano la pubblicazione delle informazioni come dati di tipo aperto, le eccezioni ed eventualmente definire i diritti e le tariffe per l'accesso e la rielaborazione dei dati.

Il Piano inoltre introduce per la prima volta una sezione dedicata all'intelligenza artificiale per la pubblica amministrazione. L'intelligenza artificiale ha il potenziale per essere una tecnologia estremamente utile, o addirittura dirompente, per la modernizzazione del settore pubblico. 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.

3. PIATTAFORME

Le Piattaforme attraverso i loro strumenti consentono di ridurre il carico di lavoro delle pubbliche amministrazioni, sollevandole dalla necessità di dover realizzare *ex novo* funzionalità, riducendo i tempi e i costi di attuazione dei servizi, garantendo maggiore sicurezza informatica e alleggerendo la gestione dei servizi della pubblica amministrazione; e che quindi in ultima analisi nascono per supportare la razionalizzazione dei processi di *back-office* o di *front-end* della PA e sono disegnate per interoperare in modo organico in un'ottica di ecosistema.

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.

La strategia nazionale, in conformità con gli anni passati, prosegue nel percorso di evoluzione e consolidamento delle piattaforme esistenti (es. SPID, pagoPA, AppIO, CIE, NoiPA ecc.) e individua una serie di azioni volte a promuovere i processi di adozione, ad aggiungere nuove funzionalità e ad adeguare costantemente la tecnologia utilizzata e i livelli di sicurezza.

La strategia promuove inoltre l'avvio di nuove piattaforme che consentono di razionalizzare i servizi per le amministrazioni ed i cittadini, quali:

- INAD che gestisce l'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, che assicura l'attuazione della Linea guida sul domicilio digitale del cittadino.
- Piattaforma Notifiche Digitali che 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 e per cittadini, imprese e PA.
- Piattaforma Digitale Nazionale Dati (PDND) che permette di aprire canali tra le PA e, così, farle dialogare, realizzando l'interoperabilità, attraverso l'esposizione di API. La Piattaforma concretizza il principio "*once-only*" e in futuro, dovrà consentire anche l'analisi dei *big data* prodotti dalle amministrazioni, resi disponibili nel *data lake*, per l'elaborazione di politiche *data-driven*.
- Piattaforma Gestione Deleghe (SDG) che consentirà ai cittadini di delegare altra persona fisica per agire presso le pubbliche amministrazioni attraverso una delega.

4. INFRASTRUTTURE

Lo sviluppo delle infrastrutture è parte integrante della strategia di modernizzazione del settore pubblico poiché queste sostengono l'erogazione sia di servizi pubblici a cittadini e imprese sia di servizi essenziali per il Paese.

Tali infrastrutture devono essere affidabili, sicure, energeticamente efficienti ed economicamente sostenibili. Tuttavia, molte infrastrutture della PA risultano prive dei requisiti di sicurezza e di affidabilità necessari e, inoltre, sono carenti sotto il profilo strutturale e organizzativo.

Alla luce dello scenario delineato la strategia manifesta l'esigenza immediata di attuare un percorso di razionalizzazione delle infrastrutture e di dismissione di quelle classificate come gruppo B, mediante la migrazione di dati e servizi erogati tramite le stesse verso *data center* più sicuri e verso infrastrutture e servizi *cloud* qualificati, ovvero conformi a standard di qualità, sicurezza, performance e scalabilità, portabilità e interoperabilità.

Per quanto concerne le amministrazioni in possesso di infrastrutture carenti dei requisiti individuati dalla normativa vigente, occorre pianificare le attività di migrazione. Secondo quanto previsto dal Regolamento dell'AgID in materia di infrastrutture e cloud (adottato con det. D.G. AgID del 15 dicembre 2021, n. 628/2021) il processo di migrazione si articola nelle seguenti macro-fasi:

- **predisposizione dell'elenco dei dati e servizi digitali dell'ente**, classificati secondo il Modello predisposto dall'Agenzia per la Cybersicurezza Nazionale (ACN), che prevede una caratterizzazione di dati e servizi in tre classi: ordinari, critici e strategici. L'elenco deve

essere trasmesso ad ACN entro il 18 luglio 2022, che provvede alla validazione. Successivamente l'elenco deve essere costantemente aggiornato;

- **predisposizione del piano di migrazione**, sulla base della classificazione dei dati e dei servizi, che potrà avvenire verso altre infrastrutture della PA ovvero verso soluzioni cloud qualificate, purché siano rispettati i requisiti previsti per la specifica classe di dati e servizi. Il piano di migrazione deve essere trasmesso ad Dipartimento per la Trasformazione Digitale entro il 28 febbraio 2023, che provvede alla verifica sugli obblighi di migrazione;
- **esecuzione del piano di migrazione**, le cui attività dovranno essere completate entro giugno 2026.

Fino alla conclusione delle attività di migrazione, resta ferma la possibilità di effettuare sulle proprie infrastrutture digitali interventi ordinaria manutenzione, volti a garantire la continuità operativa e di servizio.

Per quanto concerne, poi, i profili tecnici delle attività di migrazione verso soluzioni cloud, punto di riferimento resta il *Manuale di abilitazione al Cloud* predisposto nell'ambito del *Programma nazionale di abilitazione al cloud*.

Per realizzare un'adeguata evoluzione tecnologica e supportare il paradigma *cloud*, favorendo altresì la razionalizzazione delle spese per la connettività delle pubbliche amministrazioni, è necessario anche aggiornare il modello di connettività. Tale aggiornamento, inoltre, renderà disponibili alle pubbliche amministrazioni servizi di connettività avanzati, atti a potenziare le prestazioni delle reti delle PA e a soddisfare l'esigenza di garantire lo svolgimento del lavoro agile in sicurezza. In questo contesto, il PTI nazionale prevede l'implementazione del Sistema Pubblico di Connettività (SPC) che garantisce sia l'interscambio di informazioni in maniera riservata che la realizzazione di una infrastruttura di comunicazione propria dell'Ente.

Infine, la gestione dei servizi in *cloud* deve essere presidiata dall'ente in tutto il ciclo di vita degli stessi confermando ancora una volta il necessario e competente presidio dell'Ufficio RTD. In tale ottica il PTI nazionale 2024-2026 per la piena abilitazione al cloud richiede "l'evoluzione del parco applicativo software" verso la logica *as a service* (c.d. architettura a micro-servizi) delle applicazioni esistenti per poter sfruttare le possibili soluzioni offerte dalle moderne piattaforme computazionali e dagli algoritmi di intelligenza artificiale.

5. INTEROPERABILITÀ

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

Le Linee Guida sul *Modello di Interoperabilità per la PA* (“ModI”), adottate dall’AgID con det. D.G. n. 547 del 1° ottobre 2021, individuano gli standard e le loro modalità di utilizzo per l’implementazione delle API, favorendo:

- l’aumento dell’interoperabilità tra PA e tra queste e cittadini/imprese;
- la qualità e la sicurezza delle soluzioni realizzate;
- la de-duplicazione e la co-creazione delle API.

Il ModI individua 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 profili utilizzati dalle PA.

Le amministrazioni, dunque, progettano, sviluppano e implementano i servizi pubblici in modo da funzionare in modalità integrata e senza interruzioni, garantendo l’interoperabilità tecnica dei sistemi informatici in conformità al ModI e favorendo logiche aperte e il ricorso a standard condivisi.

6. SICUREZZA INFORMATICA

La sicurezza informatica riveste un ruolo fondamentale per le amministrazioni in quanto garantisce la disponibilità, l’integrità e la riservatezza delle informazioni. Essa è inoltre direttamente collegata ai principi previsti dall’ordinamento giuridico in materia di protezione dei dati personali.

Per quanto concerne la sicurezza, una delle attività principali del RTD è rappresentata dall’adeguamento alle misure minime contenute alla Circolare AgID n. 2/2017 alla quale le pubbliche amministrazioni erano tenute a dare puntuale attuazione entro il 31 dicembre 2017.

Le Misure, che si articolano nell’attuazione di controlli di natura tecnologica, organizzativa e procedurale, prevedono tre livelli di attuazione. Il livello minimo è quello al quale ogni organizzazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme. I livelli successivi rappresentano situazioni evolutive in grado di fornire livelli di protezione più completi e dovrebbero essere adottati fin da subito dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visti come obiettivi di miglioramento da parte di tutte le altre organizzazioni.

Il Piano Nazionale di Ripresa e Resilienza (PNRR), l’istituzione della nuova Agenzia per la Cybersicurezza nazionale e il decreto attuativo del perimetro di sicurezza nazionale cibernetica pongono la cybersecurity a fondamento della digitalizzazione della Pubblica Amministrazione e del Sistema Italia. In tale contesto sono necessarie infrastrutture tecnologiche e piattaforme in grado di offrire ai cittadini e alle imprese servizi digitali efficaci, sicuri e resilienti. È necessario quindi per tutte le PA un cambio di approccio in cui la cybersecurity non deve essere vista come un costo o

un mero adempimento normativo ma come un'opportunità per la crescita e la trasformazione digitale sia della Pubblica Amministrazione che dell'intero Paese.

Per quanto riguarda la sicurezza della trasformazione digitale, il nuovo Piano pone, inoltre, particolare attenzione al coordinamento dei propri obiettivi con quelli previsti dal Piano Nazionale di Ripresa e Resilienza e dalla Strategia Nazionale di Cybersicurezza 2022-2026 e dal relativo Piano di implementazione, nell'ottica di un innalzamento dei livelli di cybersecurity delle reti e dei sistemi informativi di tutti gli Stati membri, come dimostra l'esperienza nazionale di distribuzione delle competenza tra AgID e ACN.

Fondamentali in questo senso sono le tematiche relative al Cyber Security Awareness, in quanto da tale consapevolezza possono derivare le azioni organizzative necessarie a mitigare il rischio connesso alle potenziali minacce informatiche e alle evoluzioni degli attacchi informatici. Del resto, nel corso degli ultimi due anni sono stati registrati numerosi attacchi, anche con finalità estorsiva, ai danni di molte pubbliche amministrazioni che peraltro hanno trovato nuove e più invasive forme nel contesto dell'emergenza sanitaria, nel corso della quale anche le modalità di lavoro a distanza hanno aumentato la vulnerabilità delle infrastrutture pubbliche.

Il PTI 2024- 2026 individua, in tale contesto, specifiche aree di miglioramento in favore delle pubbliche amministrazioni. In particolare lo stesso si sofferma sulla necessità di prevedere dei modelli di gestione centralizzati della cybersicurezza, coerentemente con il ruolo trasversale associato, definire processi di gestione e mitigazione del rischio cyber, sia interni sia legati alla gestione delle terze parti di processi IT e per l'appunto, promuovere attività legate al miglioramento della cultura cyber delle Amministrazioni.

ALLEGATO 1
CRONOPROGRAMMA
LE AZIONI 2024-2026

	giugno 24	luglio 24	agosto 24	settembre 24	ottobre 24	novembre 24
GOVERNARE LA TRASFORMAZIONE DIGITALE (ORGANIZZAZIONE)	consolidare ufficio RTD e organizzazione					
LEVE PER L'INNOVAZIONE (FORMAZIONE)	elaborazione piano	formazione				
SERVIZI E PIATTAFORME	pagoPA, SPID, CIE, Login, IO	attività fascicolazione e conservazione	attività fascicolazione e conservazione	attività fascicolazione e conservazione	rilevazione soddisfazione e pubblicazione	comunicazione
INFRASTRUTTURE, CLOUD, APPLICATIVI	classificazione, predisposizione elenco, trasmissione ACN					
SICUREZZA					miglioramento misure minime	configurazione https
DATI E IA						
ACCESSIBILITÀ				assessment e dichiarazione accessibilità		

	dicembre 24	gennaio 25	febbraio 25	marzo 25	aprile 25	maggio 25
GOVERNARE LA TRASFORMAZIONE DIGITALE (ORGANIZZAZIONE)				aggiornamento piano triennale		
LEVE PER L'INNOVAZIONE (FORMAZIONE)						
SERVIZI E PIATTAFORME						
INFRASTRUTTURE, CLOUD, APPLICATIVI	Valutare la migrazione	Valutare migrazione				
SICUREZZA						
DATI E IA	censimento dataset	opendata				
ACCESSIBILITÀ				elaborazione e pubblicazione obiettivi		