TRANSIZIONE DIGITALE

PIANO TRIENNALE PER L'INFORMATICA COMUNALE 2024 – 2026

Comune di Montanaro

Città Metropolitana di Torino

02 APRILE 2024

REL. 1.0

Sommario

Introduzione

Il presente documento struttura il percorso di definizione del Piano Triennale del Comune per il triennio 2024-2026.

Raccoglie, nella sua evoluzione, tutti i passaggi che vengono effettuati sia per la definizione del Piano sia per le azioni che sono intraprese per il raggiungimento degli obbiettivi.

Per definire il Piano Triennale Comunale 2024-2026 sono state seguite le indicazioni del Piano Triennale per l'informatica nella Pubblica Amministrazione 2024 – 2026 elaborato dall'Agid ai sensi dell'art. 14-bis del CAD.

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

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

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

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

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

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

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

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

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

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

Finalità del Piano triennale

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

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

I. Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di uguaglianza e di non discriminazione, nonché per l'effettivo riconoscimento dei diritti dei cittadini e delle imprese di cui al presente Codice in conformità agli obiettivi indicati nel Piano triennale per l'informatica nella Pubblica Amministrazione di cui all'articolo 14-bis, comma 2, lett. b) (..)

II. Le pubbliche amministrazioni utilizzano, nei rapporti interni, in quelli con altre amministrazioni e con i privati, le tecnologie dell'informazione e della comunicazione, garantendo l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni nel rispetto delle Linee guida.

III. Le pubbliche amministrazioni operano per assicurare l'uniformità e la graduale integrazione delle modalità di interazione degli utenti con i servizi informatici (..) da esse erogati, qualunque sia il canale di erogazione, nel rispetto dell'autonomia e della specificità di ciascun erogatore di servizi. (..)

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

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

a) emanazione di Linee guida contenenti regole, standard e guide tecniche, nonché di indirizzo, vigilanza e controllo sull'attuazione e sul rispetto delle norme di cui al presente Codice, anche attraverso l'adozione di atti amministrativi generali, in materia di agenda digitale, digitalizzazione della Pubblica Amministrazione, sicurezza informatica, interoperabilità e cooperazione applicativa tra sistemi informatici pubblici e quelli dell'Unione europea;

b) programmazione e coordinamento delle attività delle amministrazioni per l'uso delle tecnologie dell'informazione e della comunicazione, mediante la redazione e la successiva verifica dell'attuazione del Piano triennale per l'informatica nella Pubblica Amministrazione contenente la fissazione degli obiettivi e l'individuazione dei principali interventi di sviluppo e gestione dei sistemi informativi delle amministrazioni pubbliche. Il predetto Piano è elaborato dall'AGID, anche sulla base dei dati e delle informazioni acquisiti dai soggetti di cui all'articolo 2, comma 2, ed è approvato dal Presidente del Consiglio dei ministri o dal Ministro delegato entro il 30 settembre di ogni anno (…)

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

Art. 1.

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

- Comma 513. L'Agenzia per l'Italia digitale (AGID) predispone il Piano triennale per l'informatica nella Pubblica Amministrazione che è approvato dal Presidente del Consiglio dei Ministri o dal Ministro delegato. Il Piano contiene, per ciascuna amministrazione o categoria di amministrazioni, l'elenco dei beni e servizi informatici e di connettività e dei relativi costi, suddivisi in spese da sostenere per innovazione e spese per la gestione corrente, individuando altresì i beni e servizi la cui acquisizione riveste particolare rilevanza strategica.

- Comma 514. Ai fini di cui al comma 512, Consip SpA o il soggetto aggregatore interessato, sentita l'AGID per l'acquisizione dei beni e servizi strategici indicati nel Piano triennale per l'informatica nella Pubblica Amministrazione di cui al comma 513, programma gli acquisti di beni e servizi informatici e di connettività, in coerenza con la domanda aggregata di cui al predetto Piano. (..) Consip SpA e gli altri soggetti aggregatori promuovono l'aggregazione della domanda funzionale all'utilizzo degli strumenti messi a disposizione delle pubbliche amministrazioni su base nazionale, regionale o comune a più amministrazioni.

Strategia

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

Modello strategico

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

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

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

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

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

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

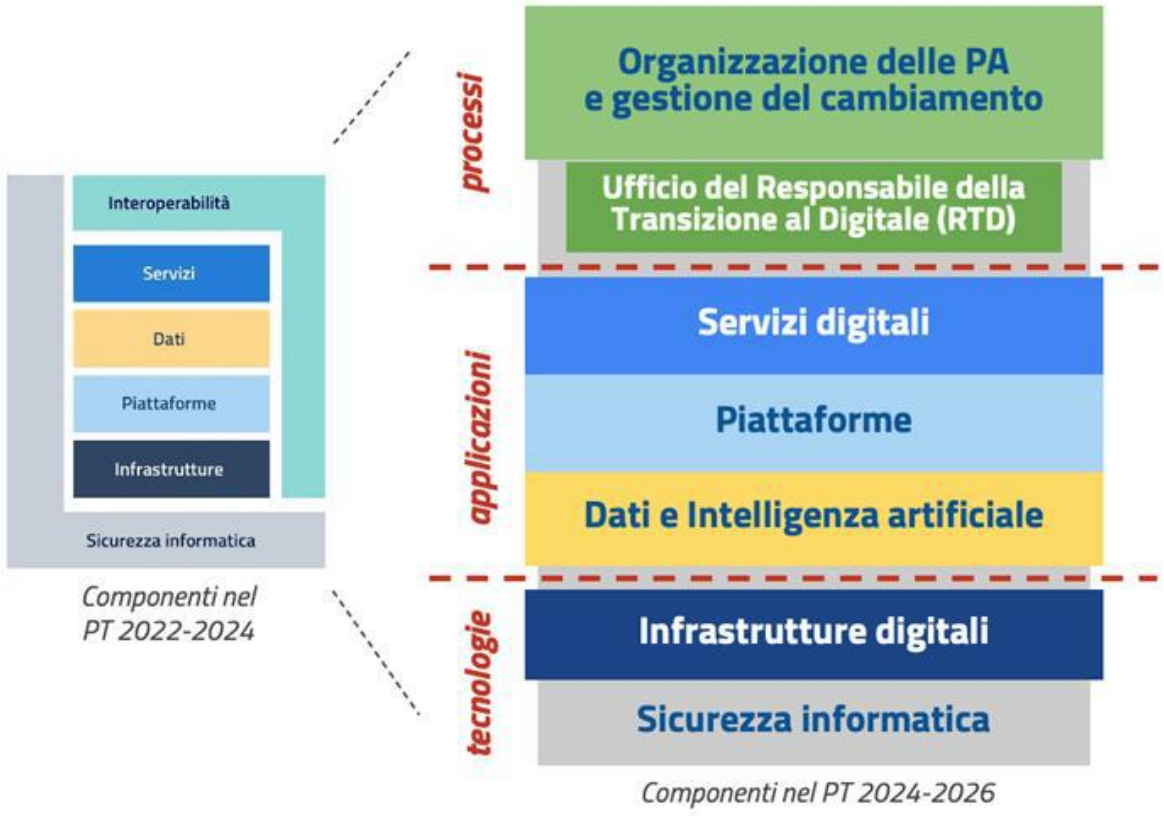
In una logica di miglioramento continuo, il modello strategico del Piano triennale 2024-26 propone una architettura organizzativa e tecnologica che ha l'obiettivo di fornire una visione

complessiva della Pubblica Amministrazione digitale che parte dal "sistema informativo" del singolo ente per arrivare a definire le relazioni con i servizi, le piattaforme e le infrastrutture nazionali erogate a livello centrale.

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

- processi
- applicazioni
- tecnologie

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



1 - Modello strategico del Piano triennale 2024-26

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

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

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

Principi guida

I principi guida emergono dal quadro normativo e sono da tenere presenti ad ogni livello decisionale e in ogni fase di implementazione, naturalmente declinandoli nello specifico della missione istituzionale di ogni ente pubblico.

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

Principi guida	**Definizioni**	**Riferimenti normativi**
1. Digitale e mobile come prima opzione (digital & mobile first)	Le pubbliche amministrazioni devono erogare i propri servizi pubblici in digitale e fruibili su dispositivi mobili, considerando alternative solo in via residuale e motivata, attraverso la "riorganizzazione strutturale e gestionale" dell'ente ed anche con una "costante semplificazione e reingegnerizzazione dei processi"	Art.3-bis Legge 241/1990 Art.1 c.1 lett. a) D.Lgs. 165/2001 Art.15 CAD Art.1 c.1 lett. b) Legge 124/2015 Art.6 c.1 DL 80/2021
2. cloud come prima opzione (cloud first)	le pubbliche amministrazioni, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano il paradigma cloud e utilizzano esclusivamente infrastrutture digitali adeguate e servizi cloud qualificati secondo i criteri fissati da ACN e nel quadro del SPC	Art.33-septies Legge 179/2012 Art. 73 CAD
3. interoperabile by design e by default (API-first)	i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e attraverso processi digitali collettivi, esponendo opportuni e-Service, a prescindere dai canali di erogazione del servizio che sono individuati logicamente e cronologicamente dopo la progettazione dell'interfaccia API;	Art.43 c.2 dPR 445/2000 Art.2 c.1 lett.c) D.Lgs 165/2001 Art.50 c2, art.50-ter e art.64bis c.1-bis CAD
4. accesso esclusivo mediante identità digitale (digital identity only)	le pubbliche amministrazioni devono adottare in via esclusiva sistemi di identità digitale definiti dalla normativa	Art.64 CAD Art. 24, c.4, DL 76/2020 Regolamento EU 2014/910 "eIDAS"
5. servizi inclusivi, accessibili e centrati sull'utente (user-centric)	le pubbliche amministrazioni devono progettare servizi pubblici che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo	Legge 4/2004 Art.2 c.1, art.7 e art.53 CAD Art.8 c.1 lettera c) e lett.e), ed art.14 c.4-bis D.Lgs 150/2009
6. dati pubblici un bene comune (open data by design e by default)	il patrimonio informativo della Pubblica Amministrazione è un bene fondamentale per lo sviluppo del Paese e deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile	Art.50 c.1 e c,2-bis, art.50quater e art.52 c.2 CAD D.Lgs 36/2006 Art.24-quater c.2 DL90/2014
7. concepito per la sicurezza e la protezione dei dati personali (data protection by design e by default)	i servizi pubblici devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali	Regolamento EU 2016/679 "GDPR" DL 65/2018 "NIS" DL 105/2019 "PNSC" DL 82/2021 "ACN"

Principi guida	Definizioni	Riferimenti normativi
8. once only e concepito come transfrontaliero	le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite, devono dare accesso ai loro fascicoli digitali e devono rendere disponibili a livello transfrontaliero i servizi pubblici rilevanti	Art.43, art.59, art.64 e art.72 DPR 445/2000 Art.15 c.3, art.41, art.50 c.2 e c.2-ter, e art.60 CAD Regolamento EU 2018/1724 "single digital gateway" Com.EU (2017) 134 "EIF"
9. apertura come prima opzione (openness)	le pubbliche amministrazioni devono tenere conto della necessità di prevenire il rischio di lock-in nei propri servizi, prediligere l'utilizzo di software con codice aperto o di e-service e, nel caso di software sviluppato per loro conto, deve essere reso disponibile il codice sorgente, nonché promuovere l'amministrazione aperta e la condivisione di buone pratiche sia amministrative che tecnologiche	Art.9, art.17 c.1 ed art.68-69 CAD Art.1 c.1 D.Lgs 33/2013 Art.30 D.Lgs 36/2023
10. sostenibilità digitale	le pubbliche amministrazioni devono considerare l'intero ciclo di vita dei propri servizi e la relativa sostenibilità economica, territoriale, ambientale e sociale, anche ricorrendo a forme di aggregazione	Art.15 c.2-bis CAD Art.21 D.lgs. 36/2023 Regolamento EU 2020/852 "principio DNSH"
11. sussidiarietà, proporzionalità e appropriatezza della digitalizzazione	I processi di digitalizzazione dell'azione amministrativa coordinati e condivisi sono portati avanti secondo i principi di sussidiarietà, proporzionalità e appropriatezza della digitalizzazione, ovvero lo Stato deve intraprendere iniziative di digitalizzazione solo se sono più efficaci di quelle a livello regionale e locale, e in base alle esigenze espresse dalle amministrazioni stesse, limitandosi negli altri casi a quanto necessario per il coordinamento informatico dei dati, e al tempo stesso le singole amministrazioni devono garantire l'appropriatezza delle iniziative di digitalizzazione portate avanti autonomamente, cioè in forma non condivisa con altri enti al livello territoriale ottimale rispetto alle esigenze preminenti dell'azione amministrativa e degli utenti dei servizi pubblici.	Art.5, 117 e 118 Costituzione Art.14 CAD

Percorso di elaborazione del Piano triennale

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

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

Il Piano triennale del Comune

Il Piano triennale comunale rappresenta un documento strategico che incarna le linee guida e le azioni previste a livello nazionale, declinandole secondo le specificità e le esigenze del territorio comunale. Questo piano si configura come uno strumento essenziale per indirizzare l'amministrazione comunale verso l'innovazione e la digitalizzazione, in linea con gli obiettivi nazionali. La strutturazione del Piano triennale comunale che hai descritto evidenzia un impegno verso una governance digitale attenta e programmata. Vediamo più da vicino i suoi componenti:

Articolazione del Piano triennale del Comune

Responsabile per la Transizione Digitale

Questa figura rappresenta il punto di riferimento per l'implementazione della strategia digitale all'interno del Comune. Le sue principali attività includono la pianificazione, la gestione e il monitoraggio delle iniziative digitali, assicurandosi che siano allineate sia con gli obiettivi nazionali che con le esigenze locali.

Contesto Strategico

Il contesto strategico fornisce una panoramica della situazione attuale del Comune in termini di risorse umane (dotazione organica) e strutturazione (organigramma), offrendo anche una sintesi del percorso di transizione digitale intrapreso fino a quel momento. Viene altresì data attenzione alle violazioni e sanzioni, come parte della valutazione dei rischi associati alla transizione digitale.

Obiettivi di Spesa Complessivi

Questa sezione del piano mette in evidenza la programmazione finanziaria per il triennio 2024-2026, partendo da un'analisi delle spese sostenute negli anni precedenti. È fondamentale per

garantire che le risorse siano allocate in modo efficiente e in linea con gli obiettivi di digitalizzazione.

Tabelle di Azione

Le specifiche tabelle di azione costituiscono il cuore operativo del Piano, dettagliando le azioni da intraprendere, i risultati attesi e lo stato di attuazione. Questo approccio mira a fornire una guida chiara per l'esecuzione del piano, facilitando il monitoraggio e la valutazione del progresso verso gli obiettivi prefissati.

Importanza del Piano

L'adozione di un Piano triennale comunale ben strutturato è cruciale per affrontare le sfide della digitalizzazione in modo coordinato e coerente. Permette di:

- Garantire che le iniziative digitali locali siano allineate con gli obiettivi più ampi definiti a livello nazionale.
- Ottimizzare l'uso delle risorse, evitando sovrapposizioni e garantendo efficienza nelle spese.
- Monitorare i progressi e adeguare le strategie in base ai risultati ottenuti e alle evoluzioni del contesto tecnologico e normativo.

L'approccio integrato e strategico del Piano triennale comunale è fondamentale per realizzare una transizione digitale efficace che risponda alle esigenze dei cittadini e contribuisca al miglioramento della qualità dei servizi offerti dal Comune.

Articolazione del Piano nazionale e guida alla lettura

Il Piano nazionale è strutturato in tre parti:

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

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

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

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

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

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

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

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

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

Il Responsabile per la Transizione Digitale

Il responsabile per la Transizione Digitale dell'Ente è il **dott. Canonico Paolo Alberto** funzionario Responsabile del Settore Qualità della vita, nominato con Delibera di Giunta Comunale n. 29 del 12 Marzo 2022.

Inoltre con Delibera di Giunta Comunale n. 35 del 23 Marzo 2022 è stata individuata, in sostituzione dell'Ufficio per la Transizione digitale, una squadra dati (Data Team) per l'attuazione del Piano Triennale dell'Informatica e pertanto

Il responsabile per la transizione è supportato da tutti i responsabili dei settori:

- ❑ Affari generali
- ❑ Finanziario
- ❑ Tecnico
- ❑ Qualità della vita
- ❑ Vigilanza

ognuno per la propria competenza, i quali sono parte attiva nella predisposizione del piano e nella sua attuazione.

La figura del Responsabile della Transizione Digitale è una figura prevista dall'art. 17 del CAD [1]che dispone che ogni pubblica amministrazione affidi ad un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, 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.

Sempre l'art 17 attribuisce al suddetto ufficio i seguenti compiti:

a) **coordinamento strategico** dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
b) **indirizzo e coordinamento dello sviluppo dei servizi**, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;
d) **accesso dei soggetti disabili** agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;
e) analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché' di ridurre i tempi e i costi dell'azione amministrativa;
f) cooperazione alla revisione della **riorganizzazione dell'amministrazione** ai fini di cui alla lettera e);
g) **indirizzo, coordinamento e monitoraggio della pianificazione** prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese[2] mediante gli strumenti della **cooperazione applicativa tra pubbliche amministrazioni**, ivi inclusa la predisposizione e

[1] Modifica prevista dal D.Lgs. n.179/2016
[2] Il D.Lgs. 26 agosto 2016, n. 179 ha disposto (con l'art. 61, comma 2, lettera d)) che l'espressione «cittadini e imprese», ovunque ricorra, si intende come «soggetti giuridici»

l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;

i) **promozione delle iniziative attinenti all'attuazione delle direttive** impartite dal Presidente del Consiglio dei ministri o dal Ministro delegato per l'innovazione e le tecnologie;

j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché' del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-bis.

j-bis) **pianificazione e coordinamento degli acquisti** di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b).

Inoltre, con l Circolare n. 3 del 1° ottobre 2018 il Ministro per la PA ha sottolineato l'urgenza di attivazione di percorsi di transizione digitali negli Enti, sotto la guida del RTD ed ha identificato, oltre ai compiti e ai poteri espressamente previsti dal CAD, anche i seguenti:

- il potere del RTD di costituire **tavoli di coordinamento** con gli altri dirigenti dell'amministrazione e/o referenti nominati da questi ultimi;
- il potere del RTD di costituire **gruppi tematici** per singole attività e/o adempimenti (ad esempio: pagamenti informatici, piena
- implementazione di SPID, gestione documentale, apertura e pubblicazione dei dati, accessibilità, sicurezza, ecc.);
- il potere del RTD di proporre l'**adozione di circolari** e atti di indirizzo sulle materie di propria competenza (ad esempio, in materia di approvvigionamento di beni e servizi ICT);
- l'adozione dei più opportuni **strumenti di raccordo e consultazione del RTD** con le altre figure coinvolte nel processo di digitalizzazione della pubblica amministrazione (responsabili per la gestione, responsabile per la conservazione documentale, responsabile per la prevenzione della corruzione e della trasparenza, responsabile per la protezione dei dati personali);
- la competenza del RTD in materia di **predisposizione del Piano triennale per l'informatica della singola amministrazione**, nelle forme e secondo le modalità definite dall'Agenzia per l'Italia digitale;
- la **predisposizione di una relazione annuale sull'attività svolta dall'Ufficio** da trasmettere al vertice politico o amministrativo che ha nominato il RTD.

Principali attività del Responsabile per la Transizione Digitale

Riassumendo le attività dell'RTD possono essere suddivise in tre categorie:

1. Strategia
2. Gestione
3. Progetto

1. <u>Strategia</u>

1.1. Definizione e coordinamento della strategia generale di trasformazione digitale dell'Ente
1.2. Individuazione, coordinamento e monitoraggio delle strategie IT e selezione delle tecnologie maggiormente idonee
1.3. Definizione della strategia di approvvigionamento IT

2. <u>Gestione ordinaria</u>

1.1. Gestione Hardware, Software, infrastruttura e reti
1.2. Sicurezza informatica
1.3. Gestione e integrazione delle banche dati
1.4. Assistenza informatica
1.5. Statistiche e Controllo di Gestione
1.6. Formazione
1.7. Gestione amministrativa (Gare e Contratti)

3. <u>Gestione Progetti</u>

1.1. Studio e sviluppo delle attività di implementazione del Piano Triennale
1.2. Definizione e monitoraggio del portafoglio progetti
1.3. Definizione di standard tecnici per i sistemi hardware, software e di rete settoriali e intersettoriali
1.4. Ideazione, promozione e realizzazione di progetti tecnologici altamente innovativi a supporto delle strutture dell'Ente e dell'efficace erogazione e gestione di servizi ai cittadini

Contesto strategico

Numero di abitanti	Al 31/12/2023 abitanti n. 5.076
Estensione	Superficie 20,9 km²

Dotazione organica dell'Ente

→ Personale in servizio e raffronto con dotazione organica al 31.12.2022

Q.F.	IN SERVIZIO NUMERO
A ora Area Operatori	0
B ora Area Operatori esperti	5
C ora Area Istruttori	13
D ora Area Funzionarie dell'Elevata qualificazione	6
Segretario comunale in Convenzione con il Comune di Foglizzo	1

→ Personale in servizio suddiviso per settori al 31.12.2022

SETTORE TECNICO/TENCNICO MANUTENTIVO	
AREA (EX Q.F.)	**N° IN SERVIZIO**
FUNZIONARI (ex cat. D)	2
ISTRUTTORI (ex cat. C)	3
OPERATORI ESPERTI (ex cat. B)	2

SETTORE FINANZIARIO	
AREA (EX Q.F.)	**N° IN SERVIZIO**
FUNZIONARI (ex cat. D)	2
ISTRUTTORI (ex cat. C)	3
OPERATORI ESPERTI (ex cat. B)	1

SETTORE AFFARI GENERALI	
AREA (EX Q.F.)	***N° IN SERVIZIO***
FUNZIONARI (ex cat. D)	1
ISTRUTTORI (ex cat. C)	3
OPERATORI ESPERTI (ex cat. B)	1

SETTORE QUALITA' DELLA VITA	
AREA (EX Q.F.)	***N° IN SERVIZIO***
FUNZIONARI (ex cat. D)	1
ISTRUTTORI (ex cat. C)	1
OPERATORI ESPERTI (ex cat. B)	0

SETTORE VIGILANZA	
AREA (EX Q.F.)	***N° IN SERVIZIO***
ISTRUTTORI (ex cat. C)	3
OPERATORI ESPERTI (ex cat. B)	1

Attualmente la suddivisione del personale in servizio con la nuova declaratoria dei profili in vigore dal 01/04/2023 è quella esplicitata nel grafico seguente:

Uffici/Organigramma dell'Ente

L'organizzazione del Comune si articola in Settori e Unità operative

Denominazione Settore

1 *Settore Qualità della Vita*

2 *Settore Finanziario*

3 *Settore Tecnico e Tecnico Manutentivo*

4 *Settore Affari generali*

5 *Settore Polizia Locale*

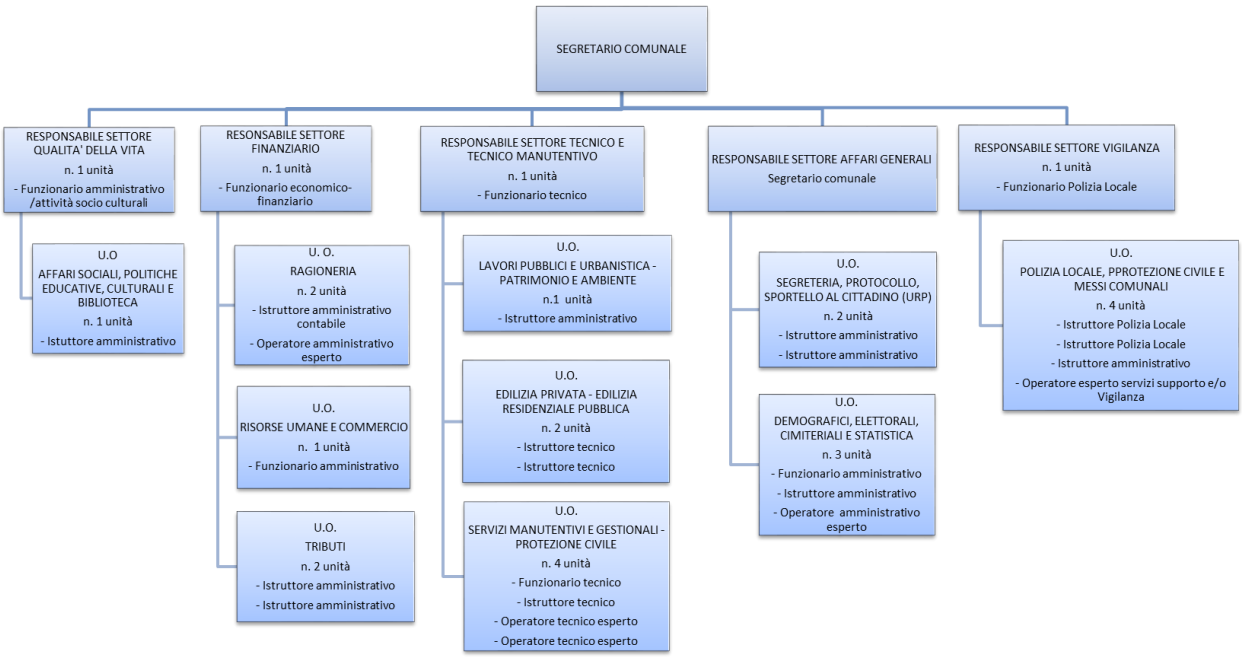
Il Settore è la struttura organizzativa di primo livello, aggregante servizi secondo criteri di omogeneità ed è coordinata e diretta da un Responsabile di Posizione Organizzativa di nomina sindacale (dal 01.04.2023 incarichi di Elevata Qualificazione).
La consistenza del personale in servizio al 01.01.2023, oltre al Segretario Generale, è di n. 24 dipendenti di ruolo.

Si evidenzia che dall' 01.04.2023 è entrato in vigore il nuovo ordinamento professionale previsto dal CCNL16/11/2022. Di conseguenza, in data 17/05/2023, con atto deliberativo della G.C. n. 63, previo confronto con la parte sindacale, sono stati definiti i nuovi profili professionali con riferimento alle nuove aree di inquadramento.

L'articolazione organizzativa del Comune di Montanaro persegue obiettivi di massima semplificazione, attraverso la riduzione al minimo del numero dei Settori, nonché di massima flessibilità, attraverso l'adattamento dell'assetto organizzativo alle mutevoli esigenze dell'Ente.

In relazione agli obiettivi e strategici individuati nel DUP ed al fine di meglio perseguire gli obiettivi di performance organizzativa, efficienza, economicità e di qualità dei servizi ai cittadini, l'attuale organizzazione dell'Ente potrà essere pertanto revisionata/modificata per adeguarsi a nuove sopraggiunte necessità.

Il Comune di Montanaro è dotato di un proprio **organigramma** nel quale sono rappresentati i Settori in capo ai rispettivi Responsabili:



Sintesi del percorso di transizione digitale intrapreso dall'Ente

Accesso ai servizi in rete - Spid

Il Sistema Pubblico per la gestione dell'Identità Digitale dei cittadini (SPID) è normato dall'art. 64 del CAD che recita: "per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese".

Il sistema SPID è quindi lo strumento principale per accedere ai servizi digitali delle pubbliche amministrazioni insieme alla CIE e alla CNS, infatti l'art. 64, comma 2-quater, del CAD dispone che: "L'accesso ai servizi in rete erogati dalle pubbliche amministrazioni che richiedono identificazione informatica avviene tramite SPID" e sempre L'art. 64, commi 2-quater e 2-nonies, del CAD dispone che siano affiancate allo SPID anche la CIE (carta d'identità elettronica) e la CNS (carta nazionale dei servizi) quali strumenti per l'accesso ai servizi in rete delle pubbliche amministrazioni.

Per questo motivo le amministrazioni devono dotarsi del sistema di accesso SPID ai propri servizi secondo le modalità definite con il DPCM 24/10/2014 (recante la "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese -SPID-, nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese).

Quindi dopo le modifiche apportate dal decreto-legge n. 76 del 16 luglio 2020, convertito con modificazioni dalla legge 11 settembre 2020 n. 120, all'articolo 64-bis del CAD, la

disciplina delle modalità di accesso ai servizi in rete prevede che dal 28 febbraio 2021 le pubbliche amministrazioni:

- facciano uso esclusivamente di "identità digitali" (SPID), carta di identità elettronica (CIE) e carta nazionale dei servizi (CNS), "ai fini dell'identificazione dei cittadini che accedono ai propri servizi in rete" (comma 3-bis dell'art. 64 del CAD);
- non possono (è vietato) "rilasciare o rinnovare credenziali per l'identificazione e l'accesso dei cittadini ai propri servizi in rete, diverse da SPID, CIE o CNS, fermo restando l'utilizzo di quelle già rilasciate fino alla loro naturale scadenza e, comunque, non oltre il 30 settembre 2021 (articolo 24, comma 4, del DL 76/2020);

Non ottemperare all'obbligo dell'uso esclusivo di SPID, CIE e CNS per l'accesso ai servizi da parte dei cittadini, "costituisce mancato raggiungimento di uno specifico risultato e di un rilevante obiettivo da parte dei dirigenti responsabili delle strutture competenti e comporta la riduzione, non inferiore al trenta per cento della retribuzione di risultato e del trattamento accessorio collegato alla performance individuale dei dirigenti competenti, oltre al divieto di attribuire premi o incentivi nell'ambito delle medesime strutture" (art. 64-bis, co. 1-quinquies, d.lgs. 82/2005).

I servizi on line rivolti ai cittadini che utilizzano sistemi di autenticazione saranno dotati anche di accesso con credenziali (SUE)

Attualmente è attivo l'accesso con SPID per i seguenti servizi accessibili dal sito istituzionale:

Sportello on line (Mosaico)

Newsletter

Sono in fase operativa le attivazioni di tali accessi legati all'Avviso PNRR Spid CIE

Pagamenti on line – pagoPA

Ai sensi dell'Art. 65 del D.L. 217/2017, modificato dal D.L DL 76/2020 – Disposizioni transitorie – comma 2, vige "l'obbligo per i prestatori di servizi di pagamento abilitati di utilizzare esclusivamente la piattaforma di cui all'articolo 5, comma 2, del decreto legislativo n. 82 del 2005 per i pagamenti verso le pubbliche amministrazioni decorre dal 28 febbraio 2021.

Al fine di consentire i pagamenti digitali da parte dei cittadini, i soggetti di cui all'articolo 2, comma 2, del decreto legislativo 7 marzo 2005, n. 82, sono tenuti, entro il 28 febbraio 2021:

- a integrare i loro sistemi di incasso con la piattaforma di cui all'articolo 5, comma 2, del decreto legislativo 7 marzo 2005, n. 82,
- ovvero ad avvalersi, a tal fine, di servizi forniti da altri soggetti di cui allo stesso articolo 2, comma 2, o da fornitori di servizi di incasso già abilitati ad operare sulla piattaforma.
- Il mancato adempimento dell'obbligo di cui al precedente periodo rileva ai fini della misurazione e della valutazione della performance individuale dei dirigenti responsabili e comporta responsabilità dirigenziale e disciplinare ai sensi degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165".

Inoltre, le "Linee Guida per l'effettuazione dei pagamenti a favore delle pubbliche amministrazioni e dei gestori di pubblici servizi" adottate dall'AgID, precisano che al sistema

PagoPA, che "rappresenta il sistema nazionale dei pagamenti elettronici in favore delle pubbliche amministrazioni e degli altri soggetti tenuti per legge all'adesione", "gli enti creditori possono affiancare esclusivamente i seguenti metodi di pagamento:

- delega unica F24 (cosiddetto modello F24) fino alla sua integrazione con il Sistema PagoPA;
- Sepa Direct Debit (SDD) fino alla sua integrazione con il Sistema PagoPA;
- eventuali altri servizi di pagamento non ancora integrati con il Sistema PagoPA e che non risultino sostituibili con quelli erogati tramite PagoPA poiché una specifica previsione di legge ne impone la messa a disposizione dell'utenza per l'esecuzione del pagamento;
- per cassa, presso il soggetto che per tale ente svolge il servizio di tesoreria o di cassa".

Quindi l'uso di PagoPA non è esclusivo ma è possibile affiancare a tale modalità anche quelle previste dalle citate linee guida.

Inoltre è necessario considerare che, l'art. 118-ter del DL 34/2020, convertito con modificazioni dalla L. 77/2020, ha disposto che gli enti territoriali possono "con propria deliberazione, stabilire una riduzione fino al venti per cento delle aliquote e delle tariffe delle proprie entrate tributarie e patrimoniali, applicabile a condizione che il soggetto passivo obbligato provveda ad adempiere mediante autorizzazione permanente

A partire dal mese di febbraio 2021 l'ente ha avviato l'attività di integrazione dei sistemi di incasso, prevedendo, per almeno due servizi erogati, la possibilità di effettuare i pagamenti mediante piattaforma pagoPA, a mezzo di emissione di Avviso di pagamento. Entro il 31/12/2021 il processo di migrazione dei servizi di incasso verso la piattaforma pagoPA è stato completato.

Inoltre per alcuni servizi (es. servizio mensa) la modalità di pagamento con PagoPA è l'unica possibile. Tale tracciabilità permette ai cittadini anche di poter usufruire di detrazione previste nell'ambito di compilazione della dichiarazione 730.

Servizi ai cittadini in modalità digitale e Punto accesso telematico – App IO

Il decreto DL 76/2020 ha novellato il CAD, d.lgs. 82/2005, con gli articoli dal 23-bis al 37-bis.

Il CAD così modificato all'art. 64-bis del CAD stabilisce che:

- (comma 1) le pubbliche amministrazioni debbano rendere "fruibili i propri servizi in rete, in conformità alle Linee guida, tramite il punto di accesso telematico attivato presso la Presidenza del Consiglio dei ministri, senza nuovi o maggiori oneri per la finanza pubblica".
- (comma 1-ter) le pubbliche amministrazioni debbano rendere "fruibili i propri servizi in rete tramite applicazione su dispositivi mobili anche attraverso il punto di accesso telematico, salvo impedimenti di natura tecnologica attestati dalla società di cui all'articolo 8, comma 2 del decreto-legge 14 dicembre 2018, n. 135, convertito, con modificazioni, dalla legge 11 febbraio 2019, n. 12".
- (comma 1-quater) le pubbliche amministrazioni debbano rendere **"fruibili tutti i loro servizi anche in modalità digitale e, al fine di attuare il presente articolo, avviano i relativi progetti di trasformazione digitale entro il 28 febbraio 2021"**.

- (comma 1-quinquies) il "mancato raggiungimento di uno specifico risultato e di un rilevante obiettivo da parte dei dirigenti responsabili delle strutture competenti" e, pertanto, comporta "la riduzione, non inferiore al trenta per cento della retribuzione di risultato e del trattamento accessorio collegato alla performance individuale dei dirigenti competenti" e il "divieto di attribuire premi o incentivi nell'ambito delle medesime strutture" in caso di violazione delle disposizioni dei precedenti commi 1-ter e 1-quater.

Quindi con la citata normativa viene disposto che i comuni debbano rendere accessibili i propri servizi attraverso la rete, sia via web che tramite applicazione su dispositivi mobili anche attraverso "il punto di accesso telematico".

Il punto di accesso telematico, attivato presso la Presidenza del Consiglio dei ministri, consiste nella applicazione IO.

L'app IO è una piattaforma nazionale, integrata a PagoPA e SPID, che viene resa disponibile a tutte le pubbliche amministrazioni per consiste loro di relazionarsi in modo personalizzato con il cittadino.

Adottano l'app IO l'ente può inviare comunicazioni ai propri utenti per fornire aggiornamenti, ricordare scadenze o richiedere pagamenti relativi a un determinato servizio.

Attualmente, in seguito alla partecipazione all'Avviso PNRR – App IO è in fase di asseverazione da parte del Dipartimento della transizione digitale l'attivazione dei seguenti servizi tramite APP IO:

Anagrafe

Attività sportive

Avviso di avvenuto pagamento

Avviso di pagamento

Biblioteche

Centri estivi e centri gioco

Comunicazione agli Amministratori Comunali

Comunicazione stranieri diciottenni nati in Italia

Comunicazioni ai cittadini residenti

Comunicazioni ai diciottenni

Comunicazioni del Sindaco

Comunicazioni elezioni

Comunicazioni giudici popolari

Comunicazioni ricorrenze matrimonio

Comunicazioni ricorrenze nascita

Contributi allo studio
Diritti di segreteria
Discariche e isole ecologiche
Disinfestazioni
Edilizia privata
Eventi e manifestazioni
Permesso di soggiorno
Registrazione contratto
Residenza
Segnalazioni, suggerimenti e reclami
Servizi Cimiteriali - Concessioni
Servizi Demografici - Albo Presidenti di seggio
Servizi Demografici - Carta d'identità
Servizi Demografici - Iscrizione Albo Scrutatori
Servizi Demografici - Tessera elettorale
Servizi Tributari - Canone unico
Servizi Tributari - IMU
Servizio Polizia Municipale - Sanzione Amministrativa
Servizio Polizia Municipale - Violazione al CDS
Traffico

Cloud First

Il piano nazionale prevede l'adozione concreta del paradigma cloud e la dismissione dei data center di fascia b), nello specifico:

1. Da settembre 2020 - Le PA continuano ad applicare i principi Cloud First - SaaS First e ad acquisire servizi cloud solo se qualificati da AGID, consultando il Catalogo dei servizi cloud qualificati da AGID per la PA - CAP1.PA.LA02
2. Entro settembre 2021 - Le PAL proprietarie di data center classificati da AGID nel gruppo B trasmettono ad AGID i piani di migrazione verso i servizi cloud qualificati da AGID e i data center di gruppo A attuando quanto previsto nel programma nazionale di abilitazione al cloud tramite il sistema PPM del Cloud Enablement Program - CAP4.PA.LA04

In data 07 Dicembre 2023 è stato possibile trasferire su cloud (Nuvola SISCOM) tutti gli applicativi interni attualmente in uso. Rimane il server interno per le cartelle di archiviazione interna ma si prevede che in un prossimo futuro anche tali documenti possano essere trasferiti in modalità cloud-

Processo di dematerializzazione dei documenti

Ai sensi dell'art. 42 del CAD – dematerializzazione dei documenti delle pubbliche amministrazioni – le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle Linee guida.

DESCRIVERE LO STATO ATTUALE

In ottemperanza del citato disposto nel corso del 2024 sarà effettuata la mappatura dei flussi documentali prendendo come base la mappatura dei processi e procedimenti per aree di rischio (art. 1 comma 16 legge 190/2012, allegato 2 del piano nazionale anticorruzione) e il registro dei trattamenti (art. 30 Regolamento (UE) 2016/679) per poter successivamente effettuare una valutazione in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle Linee guida.

È stata parallelamente avviata una valutazione circa la fattibilità economica della dematerializzazione delle pratiche dell'Ufficio Tecnico PRSENTI NELL'ARCHIVIO. DA aprile 2020 le pratiche edilizie presentate all'ut, avvengono tramite portale telematico per circa l'80%.

Misure di minime sicurezza AgID

Le misure minime di sicurezza ICT emanate dall'AgID, sono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti.

In cosa consistono le misure di sicurezza

Le misure consistono in controlli di natura tecnologica, organizzativa e procedurale e utili alle Amministrazioni per valutare il proprio livello di sicurezza informatica.

A seconda della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa dell'Amministrazione, le misure minime possono essere implementate in modo graduale seguendo tre livelli di attuazione.

Minimo: è quello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme.

Standard: è il livello, superiore al livello minimo, che ogni amministrazione deve considerare come base di riferimento in termini di sicurezza e rappresenta la maggior parte delle realtà della PA italiana.

Alto: deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.

Obiettivi delle misure minime

Le misure minime sono un importante supporto metodologico, oltre che un mezzo attraverso il quale le Amministrazioni, soprattutto quelle più piccole e che hanno meno possibilità di avvalersi di professionalità specifiche, possono verificare autonomamente la propria situazione e avviare un percorso di monitoraggio e miglioramento. Le misure minime:

- forniscono un riferimento operativo direttamente utilizzabile (checklist),
- stabiliscono una base comune di misure tecniche ed organizzative irrinunciabili;
- forniscono uno strumento utile a verificare lo stato di protezione contro le minacce informatiche e poter tracciare un percorso di miglioramento;
- responsabilizzano le Amministrazioni sulla necessità di migliorare e mantenere adeguato il proprio livello di protezione cibernetica.

Responsabilità della PA

L'adeguamento alle misure minime è a cura del responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie, come indicato nel CAD (art. 17) o, in sua assenza, del dirigente designato. Il dirigente responsabile dell'attuazione deve compilare e firmare digitalmente il "Modulo di implementazione" allegato alla Circolare 18 aprile 2017, n. 2/2017.

Secondo la circolare, le misure minime di sicurezza devono essere adottate da parte di tutte le pubbliche Amministrazioni entro il 31 dicembre 2017.

È previsto entro l'anno 2026 la redazione e l'aggiornamento del modulo di implementazione allegato alla Circolare 18 aprile 2017, n. 2/2017 (https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict) ed altresì sarà prodotto Il modulo comprensivo degli inventari dei dispositivi autorizzati e non autorizzati e dei software autorizzati e non autorizzati.

Avvisi e Bandi PNRR Digitalizzazione

In sintesi si elencano gli avvisi per i quali il Comune di Montanaro ha presentato domanda e per i quali è in attesa del decreto di liquidazione che avverrà a seguito del raggiungimento degli obbiettivi di ogni singolo bando:

Avviso Misura **1.4.1**	"Esperienza del Cittadino nei servizi pubblici"
Avviso Misura 1.4.4	"Estensione dell'utilizzo delle piattaforme nazionali di identità digitale - **SPID CIE**"
Avviso Misura 1.2	"Abilitazione al **cloud** per le PA Locali"
Avviso Misura 1.4.3	"Adozione **app IO**"
Avviso Misura 1.4.3	"Adozione piattaforma **pagoPA**"
Avviso Misura 1.3.1	"Piattaforma Digitale Nazionale Dati" Comuni Ottobre 2022

Violazioni e sanzioni

Relativamente all'attuazione del Piano strategico per l'informatica è importante rilevare che violazione di specifiche disposizioni comparta l'applicazione di rilevanti sanzioni che vengono di seguito riepilogate:

- ai sensi dell'art. 64-bis del CAD – Accesso telematico ai servizi della Pubblica Amministrazione, comma 1-quinquies, "la violazione dell'articolo 64, comma 3-bis e delle disposizioni di cui al presente articolo, costituisce mancato raggiungimento di uno specifico risultato e di un rilevante obiettivo da parte dei dirigenti responsabili delle strutture competenti e comporta la riduzione, non inferiore al 30 per cento della retribuzione di risultato e del trattamento accessorio collegato alla performance individuale dei dirigenti competenti, oltre al divieto di attribuire premi o incentivi nell'ambito delle medesime strutture", l'Ente quindi deve prevedere una riduzione di almeno del 30% della retribuzione di risultato e del trattamento accessorio collegato alla performance individuale dei dirigenti competenti, oltre al divieto di attribuire premi o incentivi nell'ambito delle medesime strutture nel caso in cui sia violato quanto disposto dall'art. 64-bis;
- ai sensi dell'Art. 65 del D.L. 217/2017, modificato dal D.L DL 76/2020 – Disposizioni transitorie – comma 2, vige "l'obbligo per i prestatori di servizi di pagamento abilitati di utilizzare esclusivamente la piattaforma di cui all'articolo 5, comma 2, del decreto legislativo n. 82 del 2005 per i pagamenti verso le pubbliche amministrazioni decorre dal 28 febbraio 2021. Anche al fine di consentire i pagamenti digitali da parte dei cittadini, i soggetti di cui all'articolo 2, comma 2, del decreto legislativo 7 marzo 2005, n. 82, sono tenuti, entro il 28 febbraio 2021, a integrare i loro sistemi di incasso con la piattaforma di cui all'articolo 5, comma 2, del decreto legislativo 7 marzo 2005, n. 82, ovvero ad avvalersi, a tal fine, di servizi forniti da altri soggetti di cui allo stesso articolo 2, comma 2, o da fornitori di servizi di incasso già abilitati ad operare sulla piattaforma. Il mancato adempimento dell'obbligo di cui al precedente periodo rileva ai fini della misurazione e della valutazione della performance individuale dei dirigenti responsabili e comporta responsabilità dirigenziale e disciplinare ai sensi degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165".

Inoltre, è altrettanto importante rilevare che con il Piano Nazionale di Ripresa e Resilienza (PNRR), inserito nel programma *Next Generation EU* (NGEU) e in particolare, nella Missione 1 del PNRR viene posto 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 e innovazione è centrale in questa Missione, ma riguarda trasversalmente anche tutte le altre.

In questo mutato contesto obiettivi e azioni del Piano triennale, dunque, non possono che essere definiti e 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.

La prima parte del decreto-legge, in particolare, ha definito, con un'articolazione a più livelli, la *governance* del Piano nazionale di ripresa e resilienza (PNRR). La responsabilità di indirizzo del Piano è assegnata alla Presidenza del Consiglio dei ministri. Viene istituita una Cabina di regia, presieduta dal Presidente del Consiglio dei ministri, alla quale partecipano di volta in volta i Ministri e i Sottosegretari competenti in ragione delle tematiche affrontate in ciascuna seduta. La Cabina di regia esercita poteri di indirizzo, impulso e coordinamento generale sull'attuazione degli interventi del PNRR.

Lo stesso decreto-legge con l'articolo 41 - introduce l'articolo 18-bis del Codice dell'amministrazione digitale - che prevede un articolato procedimento sanzionatorio per le pubbliche amministrazioni per le violazioni degli obblighi in materia di transizione digitale.

In particolare, in base all'articolo 18-bis del CAD, AgID esercita poteri di vigilanza, verifica, controllo e monitoraggio sul rispetto delle disposizioni del Codice dell'amministrazione digitale e di ogni altra norma in materia di innovazione tecnologica e digitalizzazione della pubblica amministrazione, ivi comprese quelle contenute nelle Linee guida e nel Piano triennale per l'informatica nella pubblica amministrazione, e procede, d'ufficio o su segnalazione del difensore civico digitale, all'accertamento delle relative violazioni da parte dei soggetti di cui all'articolo 2, comma 2.

Nell'esercizio dei poteri di vigilanza, verifica, controllo e monitoraggio, l'AgID richiede e acquisisce presso i soggetti di cui all'articolo 2, comma 2, dati, documenti e ogni altra informazione strumentale e necessaria.

La disciplina per la vigilanza e per l'esercizio del potere sanzionatorio previsto dall'articolo 18-bis è oggetto di apposito Regolamento adottato dall'Agenzia che disciplina le procedure di "*contestazione, accertamento, segnalazione e irrogazione delle sanzioni*" in caso di violazioni della norma.

https://trasparenza.agid.gov.it/archivio28_provvedimenti-amministrativi_0_123054_725_1.html

Obiettivi di spesa complessivi

Dati Bilancio:

Spesa corrente	
Anno (preventivo) (2024)	3.963.549,70
Anno-3 (consuntivo) 2021	3.552.002,63
Anno-2 (consuntivo) 2022	3.587.310,48
Anno-1 (consuntivo in via di predisposizione) 2023	3.714.997,69
Spesa conto capitale	
Anno (preventivo) (2024)	2.665.259,92
Anno-3 (consuntivo) 2021	547.220,52
Anno-2 (consuntivo) 2022	651.660,98
Anno-1 (consuntivo in via di predisposizione) 2023	828.157,86

Spesa corrente ICT						
Anno (preventivo) 2021 (2024)	**SW**	servizi informatici €. **0,00 (impegni ancora da effettuare)** -utilizzo beni terzi (noleggio e licenze) €.561,20; -utenze e canoni ADSL €. 2.250,90 **TOTALE €.2.812,10**	**HW**		**FORMAZIONE**	2.045,00
Anno-3 (consuntivo) 2018 (2021)	**SW**	servizi informatici €. 8.367,60; -utilizzo beni terzi (noleggio e licenze) €.14.115,80;	**HW**		**FORMAZIONE**	€ 1.288,10

		-utenze e canoni ADSL €. 2.250,90 **TOTALE €.24.734,30**				
Anno-2 (consuntivo) 2019 (2022)	**SW**	-servizi informatici €. 10.656,27; -utilizzo beni terzi (noleggio e licenze) €.9.902,74; -utenze e canoni ADSL €.2.250,90 **TOTALE €.22.809,91**	**HW**		**FORMAZIONE**	€ 2.447,00
Anno-1 (consuntivo in via di predisposizione) 2020 (2023)	**SW**	-servizi informatici €. 10.653,04; -utilizzo beni terzi (noleggio e licenze) €.9.252,48; -utenze e canoni ADSL €. 2.250,90 **TOTALE €.22.156,42**	**HW**		**FORMAZIONE**	4.185,82
Spesa in conto capitale ICT						
Anno (preventivo) 2021 (2024)	**SW**		**HW**		**FORMAZIONE**	
Anno-3 (consuntivo) 2018 (2021)	**SW**	0	**HW**	4.300,00	**FORMAZIONE**	
Anno-2 (consuntivo) 2019 (2022)	**SW**	0	**HW**	5.075,30	**FORMAZIONE**	
Anno-1 (consuntivo in via di predisposizione) 2020 (2023)	**SW**	329,4	**HW**	7.829,96	**FORMAZIONE**	

CONTRIBUTI ASSEGNATI PNRR DIGITALIZZAZIONE

Avviso Misura **1.4.1**	"Esperienza del Cittadino nei servizi pubblici"	FINANZIATA	€ 155.234,00
Avviso Misura 1.4.4	"Estensione dell'utilizzo delle piattaforme nazionali di identità digitale - **SPID CIE**"	FINANZIATA	€ 14.000,00
Avviso Misura 1.2	"Abilitazione al **cloud** per le PA Locali"	FINANZIATA	€ 121.992,00
Avviso Misura 1.4.3	"Adozione **app IO**"	FINANZIATA	€ 11.662,00
Avviso Misura 1.4.3	"Adozione piattaforma **pagoPA**"	FINANZIATA	€ 23.996,00
Avviso Misura 1.3.1	"Piattaforma Digitale Nazionale Dati" Comuni Ottobre 2022	FINANZIATA	€ 20.344,00
		TOTALE	**€ 347.228,00**
Spesa impegnata al fine di raggiungere gli obiettivi PNRR			€ 71.614,00

	importi impegnati "fuori avviso PNRR" in ambito digitalizzazione acquisto Mercurio - Programma Gestione del Personale	€ 5.500,00

L'importo di **270.114,00 €**, che verrà liquidato a questo Comune al raggiungimento di tutti gli obiettivi dichiarati, potrà essere utilizzato totalmente nell'ambito della digitalizzazione, educazione informatica, infrastrutture e strumenti digitali sia con il fine di ottimizzare e rendere più **efficiente, fruibile e trasparente** il lavoro all'interno del Comune di Montanaro sia per **facilitare l'accesso dei cittadini** ai servizi di competenza del Comune.

Di seguito si elencano alcuni punti che sono ritenuti essenziali dal R.T.D., in accordo con la "squadra dati" composta dai funzionari Responsabili di Settore.

Strategie e sviluppo "post PNRR digitalizzazione":

Per il triennio di programmazione preso in esame si punta a consolidare il livello di spesa sopra indicato, riferito agli scorsi anni, in particolare utilizzando le somme che saranno liquidate al Comune a seguito del raggiungimento degli obiettivi legati al PNRR digitalizzazione.

È stata rilevata da parte dell'RTD la necessità di indirizzare tale budget anche per sostenere un programma di **formazione** dei dipendenti necessaria per dotare l'organizzazione di competenze tecniche ed organizzative adeguate ad affrontare il cambiamento determinato dalla transizione digitale.

Inoltre, sulla base di pareri acquisiti dai diversi settori del Comune di Montanaro, il RTD elenca qui alcuni servizi per i quali sarebbe un'urgente attivazione, sia per l'ottimizzazione del lavoro interno dei diversi uffici sia per facilitare l'accesso degli utenti alla

documentazione e partecipazione pubblica (dalla consultazione di un documento del 1500 alla partecipazione ad una gara d'appalto).

- **Digitalizzazione dell'archivio UTC** (locale archivio cartaceo piano terra);
- **Digitalizzazione dell'archivio storico** e corrente atti amministrativi (scansione digitale di atti presenti come copie cartacee - in particolare atti e documenti con più di 100 anni - e possibilità di creare un Portale per la consultazione, previa registrazione dell'utente);
- **Riordino degli archivi**, parallelamente alla digitalizzazione degli stessi, valutare i locali ad oggi adibiti ad archivio, storico o corrente, e valutare la possibilità di affidare esternamente anche i servizi di deposito e archiviazione;
- Creare uno **Sportello di assistenza informatica e digitale** (assistenza, formazione, aggiornamento e sviluppo dei servizi) a favore dei cittadini, che possa fornire assistenza informatica, supporto all'utilizzo di un computer o cellulare. Supporto per la compilazione delle pratiche di accesso a bonus e altre pratiche online (esempio attivazione e gestione dell'identità digitale, richieste per "PUNTO INPS" del Comune di Montanaro, assegni di maternità dei comuni, bonus utenze, disagio fisico, copia CU, OBIS/M)".
- Proposta di conferenze e **formazione continua a favore dei cittadini**, giornate informative riguardo i temi inerenti la digitalizzazione, sensibilizzazione sul corretto utilizzo degli strumenti informatici. Predisposizione di strumenti e progetti didattici in collaborazione con le scuole presenti sul territorio per educare le giovani generazioni al corretto utilizzo degli strumenti informatici con particolare riferimento alla partecipazione pubblica (consultazione archivi, biblioteca, iscrizione a servizi, etc.).
  Particolare attenzione sarà rivolta alle persone che, per motivi anagrafici o sociali, hanno una minore propensione allo sviluppo di abilità informatiche
- Richiesta preventivi per affidamento di un servizio che offra una valutazione e **reingegnerizzazione dei processi** quale uno strumento che consente di ripensare e modificare i flussi di lavoro del Comune, per velocizzare il raggiungimento degli obiettivi e ridurre i costi a partire da un'attenta analisi dei processi in essere, delle risorse e della produttività, con riferimento particolare alla modifica di alcuni passaggi e processi in seguito ai servizi attivati per mezzo degli Avvisi PNRR Digitalizzazione;
  La digitalizzazione dei processi in alcuni casi è un passaggio essenziale per sbloccare alcune dinamiche che rendono il procedimento più lento (come è stato, per esempio, la digitalizzazione delle Cedole librarie, in precedenza cartacee con la firma di più soggetti, ad oggi digitalizzate utilizzando semplicemente con identificativo il codice fiscale)
- **Tavolo multimediale** presso la Biblioteca Civica "G. Gozzano", scrivania condivisa con la disponibilità di wifi gratuito e l'utilizzo di due pc a disposizione degli utenti, per studio, ricerca e consultazione del catalogo della Biblioteca e dello SBAM;
- **Digitalizzazione della sala del consiglio comunale** con la realizzazione di un impianto di videoconferenza e videoproiezione (anche per partecipazione delle sedute on line ed in remoto)
- Acquisto di **nuovi strumenti hardware** per gli uffici comunali, nel dettaglio:
    - un Tablet per la biblioteca, al fine di facilitare la ricerca e assistenza all'utenza presso gli scaffali;

    - fornire agli uffici che lo richiedono di un PC portatile anche al fine di adattare uffici o sale riunioni sprovvisti di tali postazioni
    - un tablet per i Vigili da utilizzare in remoto, esempio per la spunta al mercato o le sanzioni, etc);
    - aggiornamento delle postazioni di lavoro che al momento risultano obsolete perché ad esempio equipaggiate ancora con dischi rotazionali o con monitor di dimensione e risoluzione non adeguate
    - uno schermo piatto (tra 80 e 90 pollici) da inserire in un luogo adeguato sia per corsi di formazione sia per consultazione pratiche e atti, sia per facilitare e rendere più accessibile e visibile il lavoro delle diverse Commissioni comunali;
    - telefoni cellulari per l'utilizzo da parte dei dipendenti in smart working e per i Responsabili di Settore, in modo da poter ridirigere le chiamate dirette verso gli uffici comunali e non interrompere il dialogo con i cittadini;
- Provvedere alla ricerca del **software più adatto** per ciascun ufficio ed eventualmente effettuare ricerche di mercato al fine di individuare strumenti informatici specializzati e dedicati, che mirino ad ottimizzare e rendere efficace il lavoro dei diversi uffici, nella peculiarità della loro competenza, ed altresì facilitare l'accesso da parte dei cittadini/utenti/operatori economici;
- Provvedere ad aderire ad una Stazione Appaltante qualificata (ai sensi del Nuovo codice appalti (D.LGS N. 36/2023) con particolare riferimento alla **Piattaforma digitale Appalti** per gli affidamenti sopra/sotto soglia, tenendo presente da una parte l'efficacia della digitalizzazione degli appalti e dall'altra permettendo a tutti i possibili operatori economici di accreditarsi in maniera facile e trasparente al Portale individuato;
- **INFRASTRUTTURE**: adeguare i locali comunali a sistemi di connessione con banda ultra larga, fibra ottica e rete wifi;
- Redigere una versione aggiornata del **Manuale di gestione documentale e del Manuale di conservazione**, su impulso del Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi;
- **Formazione del personale interno**: costante aggiornamento, formazione e coinvolgimento del personale interno (sia dipendenti che amministrazione) in un'ottica di portare una maggiore familiarità e conoscenza degli strumenti informatici, sia per aumentare l'efficienza del lavoro svolto, sia per avvicinare i cittadini/utenti ai servizi a loro dedicati. Programmare, implementare e rafforzare la formazione e l'uso dellle nuove procedure informatizzate appena introdotte (Sportello On line/Mosaico, Mercurio software per risorse umane, firma digitale delle delibere e determine.);
- Terminare e completare il passaggio a **server Cloud**, già perfezionato per quanto riguarda gli applicativi, anche per le cartelle dati all'interno della rete interna.

LINEE DI AZIONE DEI PIANI DEGLI ANNI PRECEDENTI ANCORA VIGENTI

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
PARTE PRIMA – Componenti strategiche per la trasformazione digitale	Capitolo 1 - Organizzazione e gestione del cambiamento	Obiettivo 1.2 - Diffusione competenze digitali nel Paese e nella PA	RA1.1.0	Rafforzare Le competenze digitali per la PA e per il Paese e favorire l'inclusione digitale	Vigente	2023	PA	Sì	Sì	NA	La dimensione dell'Ente non consente all'ente di partecipare a iniziative pilota di questi tipo	Le PA aderiscono all'iniziativa "Syllabus per la formazione digitale" e promuovono la partecipazione alle iniziative formative sulle competenze di base da parte dei dipendenti pubblici, concorrendo al conseguimento dei target del PNRR in tema di sviluppo del capitale umano della PA e in linea con il Piano strategico nazionale per le competenze digitali - CAP1.PA.08
PARTE PRIMA – Componenti strategiche per la trasformazione digitale	Capitolo 1 - Organizzazione e gestione del cambiamento	Obiettivo 1.2 - Diffusione competenze digitali nel Paese e nella PA	RA1.1.0	Rafforzare Le competenze digitali per la PA e per il Paese e favorire l'inclusione digitale	Vigente	2023	PA	Sì	Sì	NA	La dimensione dell'Ente non consente all'ente di partecipare a iniziative pilota di questi tipo	Le PA, in funzione della propria missione istituzionale, realizzano iniziative per lo sviluppo delle competenze digitali dei cittadini previste dal PNRR e in linea con il Piano operativo della Strategia Nazionale per le Competenze Digitali - CAP1.PA.09
PARTE SECONDA – Componenti tecnologiche	Capitolo 4 - Piattaforme	Obiettivo 4.1 - Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA	RA4.1.4	Incremento dell'adozione e dell'utilizzo di SPID e CIE da parte delle Pubbliche Amministrazioni	Vigente	2023	PA e GPS	Sì	Sì	Ok	Ok	Le PA e i gestori di pubblici servizi proseguono il percorso di adesione a SPID e CIE, dismettendo le altre modalità di autenticazione associate ai propri servizi online e integrando lo SPID uso professionale per i servizi diretti a professionisti e imprese - CAP4.PA.04
PARTE SECONDA – Componenti tecnologiche	Capitolo 4 - Piattaforme	Obiettivo 4.1 - Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA	RA4.1.4	Incremento dell'adozione e dell'utilizzo di SPID e CIE da parte delle Pubbliche Amministrazioni	Vigente	2023	PA e GPS	Sì	Sì	Ok	Non risultano servizi online dotati di credenziali proprietarie	Le PA e i gestori di pubblici servizi interessati cessano il rilascio di credenziali proprietarie a cittadini dotabili di SPID e/o CIE - CAP4.PA.05
PARTE SECONDA – Componenti tecnologiche	Capitolo 4 - Piattaforme	Obiettivo 4.1 - Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA	RA4.1.4	Incremento dell'adozione e dell'utilizzo di SPID e CIE da parte delle Pubbliche Amministrazioni	Vigente	2023	PA e GPS	Sì	Sì	Ok	Ok	Le PA e i gestori di pubblici servizi interessati adottano lo SPID e la CIE by default: le nuove applicazioni devono nascere SPID e CIE-only a meno che non ci siano vincoli normativi o tecnologici, se dedicate a soggetti dotabili di SPID o CIE. Le PA che intendono adottare lo SPID di livello 2 e 3 devono anche adottare il

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
												"Login with eIDAS" per l'accesso transfrontaliero ai propri servizi - CAP4.PA.06
PARTE SECONDA – Componenti tecnologiche	Capitolo 4 - Piattaforme	Obiettivo 4.1 - Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA	RA4.1.4	Incremento dell'adozione e dell'utilizzo di SPID e CIE da parte delle Pubbliche Amministrazioni	Vigente	2023	PA	Sì	Sì	Ok	Ok sulla base delle disponibilità di bilancio e/o eventuali finanziamenti	Le PA devono adeguarsi alle evoluzioni previste dall'ecosistema SPID (tra cui OpenID Connect, uso professionale, Attribuite Authorities, servizi per i minori e gestione degli attributi qualificati) - CAP4.PA.07
PARTE SECONDA – Componenti tecnologiche	Capitolo 5 - Dati e Intelligenza Artificiale	Obiettivo 5.1 - Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese	RA5.1.1	Aumento del numero di dataset aperti di tipo dinamico in coerenza con quanto previsto dalle Linee guida Open Data	Vigente	2023	PA	Sì	Sì	Da approfondire	Ok sulla base delle disponibilità di bilancio e/o eventuali finanziamenti	Le PA adeguano i metadati relativi ai dati geografici all'ultima versione delle specifiche nazionali e documentano i propri dataset nel Catalogo nazionale geodati.gov.it - CAP5.PA.01
PARTE SECONDA – Componenti tecnologiche	Capitolo 5 - Dati e Intelligenza Artificiale	Obiettivo 5.1 - Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese	RA5.1.1	Aumento del numero di dataset aperti di tipo dinamico in coerenza con quanto previsto dalle Linee guida Open Data	Vigente	2023	PA	Sì	Sì	DA approfondire	Ok sulla base delle disponibilità di bilancio e/o eventuali finanziamenti	Le PA adeguano i metadati relativi ai dati non geografici alle specifiche nazionali e documentano i propri dataset nel Catalogo nazionale dati.gov.it - CAP5.PA.02
PARTE SECONDA – Componenti tecnologiche	Capitolo 5 - Dati e Intelligenza Artificiale	Obiettivo 5.1 - Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese	RA5.1.1	Aumento del numero di dataset aperti di tipo dinamico in coerenza con quanto previsto dalle Linee guida Open Data	Vigente	2023	PA	Sì	Sì	Ok	Ok monitorare gli interventi formativi	Le PA partecipano, in funzione delle proprie necessità, a interventi di formazione e sensibilizzazione sulle politiche open data - CAP5.PA.03
PARTE SECONDA – Componenti tecnologiche	Capitolo 6 - Infrastrutture	Obiettivo 6.1 - Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la	RA6.1.1	Numero di amministrazioni migrate	Vigente	2023	PA	Sì	Sì	Ok	L'ente ha migrato gli applicativi su Cloud	Le PA proprietarie di data center di gruppo B richiedono l'autorizzazione ad AGID per le spese in materia di data center nelle modalità stabilite dalla Circolare AGID 1/2019 e prevedono in tali contratti, qualora autorizzati, una durata massima coerente con i tempi strettamente

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
		strategia "Cloud Italia" e migrando verso infrastrutture e servizi cloud qualificati (incluso PSN)										necessari a completare il percorso di migrazione previsti nei propri piani di migrazione – CAP6.PA.01
PARTE SECONDA – Componenti tecnologiche	Capitolo 6 - Infrastrutture	Obiettivo 6.1 - Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la strategia "Cloud Italia" e migrando verso infrastrutture e servizi cloud qualificati (incluso PSN)	RA6.1.1	Numero di amministrazioni migrate	Vigente	2023	PA	Sì	Sì	NA	NA	Le PA proprietarie di data center classificati da AGID nel gruppo A continuano a gestire e manutenere tali data center in coerenza con quanto previsto dalla Strategia Cloud Italia e dal Regolamento cloud – CAP6.PA.02
PARTE SECONDA – Componenti tecnologiche	Capitolo 6 - Infrastrutture	Obiettivo 6.1 - Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la strategia "Cloud Italia" e migrando verso infrastrutture e servizi cloud qualificati (incluso PSN)	RA6.1.1	Numero di amministrazioni migrate	Vigente	2023	PA	Sì	Sì	Ok	L'ente ha migrato gli applicativi su Cloud	Le PA avviano il percorso di migrazione verso il cloud in coerenza con quanto previsto dalla Strategia Cloud Italia – CAP6.PA.03

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
PARTE SECONDA – Componenti tecnologiche	Capitolo 6 - Infrastruttura	Obiettivo 6.1 - Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la strategia "Cloud Italia" e migrando verso infrastrutture e servizi cloud qualificati (incluso PSN)	RA6.1.1	Numero di amministrazioni migrate	Vigente	2023	PA	Sì	Sì	Ok	L'ente ha migrato gli applicativi su Cloud	Le PA continuano ad applicare il principio cloud first e ad acquisire servizi cloud solo se qualificati – CAP6.PA.04
PARTE SECONDA – Componenti tecnologiche	Capitolo 6 - Infrastruttura	Obiettivo 6.1 - Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la strategia "Cloud Italia" e migrando verso infrastrutture e servizi cloud qualificati (incluso PSN)	RA6.1.1	Numero di amministrazioni migrate	Vigente	2023	PA A	Sì	Sì	Da attuare	Verificare se era stata trasmessa all'Agenzia per la Cybersicurezza Nazionale (ACN) la classificazione dei dati e dei servizi digitali per abilitare il processo di migrazione verso gli ambienti cloud. (essere inviata entro il 18 luglio 2022: le PA, infatti, devono) https://padigitale2026.gov.it/supporto/domande-frequenti/#03_classification-data-services/008_Entroquandodevoinviarelaclassificazionedaties Link al servizio di calssificazione: https://padigitale2026.gov.it/come-partecipare/classifica-pa/ documenti di riferimento: https://assets.innovazione.gov.it/1642693979-det_306_cloud_modclass_20220118.pdf	Le PA aggiornano l'elenco e la classificazione dei dati e dei servizi digitali in presenza di dati e servizi ulteriori rispetto a quelli già oggetto di conferimento e classificazione come indicato nel Regolamento e di conseguenza aggiornano, ove necessario, anche il piano di migrazione – CAP6.PA.05

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											https://assets.innovazione.gov.it/1642694063-det_306_all1_20220118_modello.pdf	

LINEE DI AZIONE DEL PIANO PREVISTE PER L'ANNO 2024

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
PARTE PRIMA – Componenti strategiche per la trasformazione digitale	Capitolo 1 - Organizzazione e gestione del cambiamento	Obiettivo 1.3 - Monitorare e analizzare lo stato di digitalizzazione del paese	RA1.3.2/RA1.3.3	Acquisizione ed elaborazione di informazioni analitiche da Enti locali e Aumento delle tipologie e delle fonti dati integrate all'interno dell'Osservatorio	set-24	2024	ENTI LOCALI	Sì	Sì	Da pianificare		Gli Enti locali partecipano alla prima fase della raccolta dati, garantendo l'accuratezza e la completezza delle informazioni - CAP1.PA.11
PARTE PRIMA – Componenti strategiche per la trasformazione digitale	Capitolo 2 - Il procurement per la trasformazione digitale	Obiettivo 2.3 - Favorire e monitorare l'utilizzo dei servizi previsti dalle Gare strategiche	RA2.3.1	Incremento del livello di trasformazione digitale mediante la disponibilità di Gare strategiche allo scopo definite	set-24	2024	PA	Sì	Sì	Da pianificare	Verranno programmati i fabbisogni di adesione alle iniziative strategiche per l'anno 2025: • Analizzando i propri obiettivi e fabbisogni. • Valutando le iniziative disponibili e le loro caratteristiche. • Identificando le risorse umane, finanziarie e tecnologiche necessarie per aderire alle iniziative. • Redigendo un piano acquisti che includa le iniziative a cui si intende aderire.	Le PA, nel proprio piano acquisti, programmano i fabbisogni di adesione alle iniziative strategiche disponibili per il perseguimento degli obiettivi del Piano triennale per l'anno 2025 - CAP2.PA.04
PARTE SECONDA – Componenti tecnologiche	Capitolo 3 - Servizi	Obiettivo 3.1 - Migliorare la capacità di erogare e-service	RA3.1.1	Incremento del numero di "e-service" registrati sul Catalogo Pubblico PDND	Da gennaio 2024	2024	PA	Sì	Sì	ok	Non sono attive modalità di interoperabilità diverse da PDND (Piattaforma Digitale Nazionale Dati) con altre PA	Le PA cessano di utilizzare modalità di interoperabilità diverse da PDND - CAP3.PA.01
PARTE SECONDA – Componenti tecnologiche	Capitolo 3 - Servizi	Obiettivo 3.2 - Migliorare la capacità di generare ed erogare servizi digitali	RA3.2.2	Incremento dell'accessibilità dei servizi digitali	marzo 2024	2024	PA	Sì	Sì	Ok	Sono stati pubblicati gli obiettivi di accessibilità	Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web - CAP3.PA.09
PARTE SECONDA – Componenti tecnologiche	Capitolo 3 - Servizi	Obiettivo 3.2 - Migliorare la capacità	RA3.2.2	Incremento dell'accessibilità dei servizi digitali	Settembre 2024	2024	PA	Sì	Sì	Da pianificare	Da attuare entro il 23 settembre 2024	Le PA pubblicano, entro il 23 settembre, esclusivamente tramite l'applicazione form.AGID.gov.it, la dichiarazione di accessibilità per

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
		di generare ed erogare servizi digitali										ciascuno dei propri siti web e APP mobili - CAP3.PA.11
PARTE SECONDA – Componenti tecnologiche	Capitolo 4 - Piattaforme	Obiettivo 4.2 - Ottenere la piena interoperabilità tra le piattaforme	RA4.2.1	Adesione ai nuovi servizi offerti da ANPR	febbraio 2024	2024	COMUNI	Sì	Sì	Da valutare	Il Comune deve valutare se richiedere l'adesione ai servizi di Stato civile su ANPR.	Dalla "fine dell'adozione controllata" i Comuni potranno richiedere l'adesione servizi di Stato civile su ANPR - CAP4.PA.18
PARTE SECONDA – Componenti tecnologiche	Capitolo 5 - Dati e Intelligenza Artificiale	Obiettivo 5.1 - Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese	RA5.1.2	Aumento del numero di dataset resi disponibili attraverso i servizi di rete di cui al framework creato con la Direttiva 2007/2/EC (INSPIRE) e relativi Regolamenti attuativi, con particolare riferimento ai dati di elevato valore di cui al Regolamento di esecuzione (UE) 2023/138	Da giugno 2024	2024	PA	Sì	Sì	Da valutare	Quali sono i dati di elevato valore? I dati di elevato valore sono dati che possono generare significativi benefici per la società, l'ambiente e l'economia attraverso il loro riutilizzo. Quali sono le modalità di pubblicazione dei dati di elevato valore? I dati di elevato valore possono essere pubblicati attraverso: • API: Interfacce di programmazione che permettono l'accesso automatico ai dati. • Download in blocco: Download di file completi contenenti i dati. Qual è la specifica guida operativa? La specifica guida operativa è un documento che fornisce alle PA istruzioni e supporto per la pubblicazione dei dati di elevato valore.	Le PA attuano le indicazioni sui dati di elevato valore presenti nel Regolamento di esecuzione (UE) 2023/138, nelle Linee guida Open Data nonché nella specifica guida operativa - CAP5.PA.04
PARTE SECONDA – Componenti tecnologiche	Capitolo 5 - Dati e Intelligenza Artificiale	Obiettivo 5.3 - Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna	RA5.3.1	Aumento del numero di dataset di tipo aperto documentati nel portale dati.gov.it che adottano le licenze previste dalle Linee guida Open Data	Da gennaio 2024	2024	PA	Sì	Sì	Da pianificare	Cosa si deve fare: • Adottare le linee guida per l'implementazione del Decreto Legislativo n. 36/2006. • Adeguare le proprie licenze e condizioni d'uso ai requisiti e alle raccomandazioni delle linee guida. • Assicurare la conformità alle linee guida di tutti i contratti e gli accordi con i fornitori di beni e servizi informatici.	Le PA attuano le linee guida contenenti regole tecniche per l'implementazione del Decreto Legislativo n. 36/2006 relativamente ai requisiti e alle raccomandazioni su licenze e condizioni d'uso - CAP5.PA.20

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
		economia dei dati									Quali sono i requisiti e le raccomandazioni delle linee guida? Le linee guida forniscono requisiti e raccomandazioni su: • Tipi di licenze da utilizzare per i dati e i software della PA. • Condizioni d'uso dei dati e dei software della PA. • Procedure per la concessione di licenze e la gestione delle condizioni d'uso. Come le PA possono adottare le linee guida? Le PA possono adottare le linee guida: • Emanando un atto formale (delibera, detremina, ecc.). • Redigendo un documento che descrive come le linee guida saranno applicate nella PA. • Utilizzando modelli e best practice disponibili.	
PARTE SECONDA – Componenti tecnologiche	Capitolo 6 - Infrastrutture	Obiettivo 6.1 - Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la strategia "Cloud Italia" e migrando verso infrastrutture e servizi cloud qualificati (incluso PSN)	RA6.1.1	Numero di amministrazioni migrate	Da gennaio 2024	2024	PA	Sì	Sì	Se richiesto		Le PA, ove richiesto dal Dipartimento per la Trasformazione Digitale o da AGID, trasmettono le informazioni relative allo stato di avanzamento dell'implementazione dei piani di migrazione – CAP6.PA.06
PARTE SECONDA –	Capitolo 6 - Infrastrutture	Obiettivo 6.1 - Migliorare	RA6.1.1	Numero di amministrazioni migrate	set-24	2024	AMMINI	Sì	Sì	Se richiesto		4.083 amministrazioni concludono la migrazione in coerenza con il piano di migrazione e, ove richiesto

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
Componenti tecnologiche		la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la strategia "Cloud Italia" e migrando verso infrastrutture e servizi cloud qualificati (incluso PSN)					STRAZIONI					dal Dipartimento per la Trasformazione Digitale o da AGID, trasmettono le informazioni necessarie per verificare il completamento della migrazione – CAP6.PA.09
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.1 - Adottare una governance della cybersicurezza diffusa nella PA	RA7.1.1	Identificazione di un modello, con ruoli e responsabilità, di gestione della cybersicurezza	Da settembre 2024	2024	PA	Sì	Sì	Da attuare	Cosa si intende per modello unitario di governance della cybersicurezza? Il modello unitario di governance della cybersicurezza è un insieme di regole, procedure e strumenti che le PA adottano per gestire i rischi informatici in modo coordinato e centralizzato. Quali sono i ruoli e le responsabilità dei soggetti coinvolti nella governance della cybersicurezza? I ruoli e le responsabilità dei soggetti coinvolti nella governance della cybersicurezza variano in base alle dimensioni e alla complessità della PA. In generale, i ruoli principali sono: • Responsabile della cybersicurezza: Ha la responsabilità complessiva della sicurezza informatica della PA. • CISO: Chief Information Security Officer. È il responsabile tecnico della sicurezza informatica. • Unità di sicurezza informatica: È l'unità responsabile dell'implementazione delle misure di sicurezza informatica.	Le singole PA definiscono il modello unitario, assicurando un coordinamento centralizzato a livello dell'istituzione, di governance della cybersicurezza - CAP7.PA.01

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											Quali sono le procedure per la gestione dei rischi informatici? Le procedure per la gestione dei rischi informatici includono: • Identificazione dei rischi: Identificare i potenziali rischi informatici che possono colpire la PA. • Valutazione dei rischi: Valutare la probabilità e l'impatto dei rischi informatici identificati. • Trattamento dei rischi: Adottare le misure di sicurezza adeguate per ridurre i rischi informatici. Quali sono le misure di sicurezza adeguate? Le misure di sicurezza adeguate variano in base alle dimensioni e alla complessità della PA. In generale, le misure di sicurezza di base includono: • Protezione del perimetro: Proteggere la rete informatica della PA da accessi non autorizzati. • Controllo degli accessi: Limitare l'accesso alle informazioni e ai sistemi informatici della PA ai soli utenti autorizzati. • Protezione dei dati: Proteggere i dati della PA da intrusioni, perdita o furto. • Formazione e sensibilizzazione: Fornire formazione e sensibilizzazione ai dipendenti della PA sui rischi informatici.	
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.1 - Adottare una governance della cybersicurezza diffusa nella PA	RA7.1.1	Identificazione di un modello, con ruoli e responsabilità, di gestione della cybersicurezza	Da dicembre 2024	2024	PA	Sì	Sì	Da attuare	Cosa si deve fare: • Definire un modello di governance della cybersecurity che sia chiaro, efficace e adattato alle proprie esigenze. • Identificare i ruoli e le responsabilità di tutti i soggetti coinvolti nella gestione della cybersecurity.	Le PA adottano un modello di governance della cybersicurezza - CAP7.PA.02

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											• Definire le procedure per la gestione dei rischi informatici. • Adottare le misure di sicurezza adeguate alla protezione dei dati e dei sistemi informatici. Cosa si intende per modello di governance della cybersecurity? Il modello di governance della cybersecurity è un insieme di regole, procedure e strumenti che le PA utilizzano per gestire i rischi informatici. Quali sono i componenti chiave di un modello di governance della cybersecurity? I componenti chiave di un modello di governance della cybersecurity includono: • Strategia di sicurezza informatica • Struttura organizzativa • Processi di gestione dei rischi • Misure di sicurezza • Formazione e consapevolezza • Monitoraggio e revisione	
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.1 - Adottare una governance della cybersicurezza diffusa nella PA	RA7.1.1	Identificazione di un modello, con ruoli e responsabilità, di gestione della cybersicurezza	Da dicembre 2024	2024	PA	Sì	Sì	Da attuare	Cosa si deve fare: • Nominare un RCS per ciascun ufficio o servizio. • Dotare il RCS di una struttura organizzativa di supporto adeguata. • Definire i compiti e le responsabilità Quali sono i compiti e le responsabilità del RCS? I compiti e le responsabilità del RCS includono: • Effettuare l'analisi dei rischi informatici. • Definire e implementare le misure di sicurezza adeguate. • Gestire gli incidenti informatici.	Le PA nominano i Responsabili della cybersicurezza e delle loro strutture organizzative di supporto - CAP7.PA.03

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											• Fornire formazione e sensibilizzazione ai dipendenti sui rischi informatici. • Monitorare e revisionare il sistema di gestione dei rischi informatici. Come le PA possono nominare il RCS e la sua struttura di supporto? Le PA possono nominare il RCS e la sua struttura di supporto: • Emanando un atto formale (delibera, decreto, ecc.). • Identificando le risorse umane e finanziarie necessarie. • Definendo le procedure per la selezione e la formazione del RCS. Quali sono le competenze che dovrebbe avere il RCS? Il RCS dovrebbe avere competenze in materia di: • Sicurezza informatica • Gestione dei rischi • Leadership • Comunicazione	
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.1 - Adottare una governance della cybersicurezza diffusa nella PA	RA7.1.2	Definizione del framework documentale a supporto della gestione cyber	Da dicembre 2024	2024	PA	Sì	Sì	Da attuare	Cosa si deve fare: • Definire e documentare i processi e le procedure per la gestione della cybersecurity. • Assicurare che i processi e le procedure siano adeguati ai rischi informatici specifici della PA. • Fornire formazione ai dipendenti sui processi e le procedure per la gestione della cybersecurity. Quali sono i processi e le procedure che le PA dovrebbero formalizzare? I processi e le procedure che le PA dovrebbero formalizzare includono: • Analisi dei rischi informatici • Gestione delle vulnerabilità	Le PA formalizzano i processi e le procedure inerenti alla gestione della cybersicurezza - CAP7.PA.04

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											• Controllo degli accessi • Sicurezza dei dati • Incident response • Formazione e sensibilizzazione • Monitoraggio e revisione Come le PA possono formalizzare i processi e le procedure per la gestione della cybersecurity? Le PA possono formalizzare i processi e le procedure per la gestione della cybersecurity: • Emanando un atto formale (delibera, decreto, ecc.). • Redigendo un documento che descriva i processi e le procedure. • Utilizzando modelli e best practice disponibili.	
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.2 - Gestire i processi di approvvigionamento IT coerentemente con i requisiti di sicurezza definiti	RA7.2.1	Definizione del framework documentale a supporto del processo di approvvigionamento IT	Da giugno 2024	2024	PA	Sì	Sì	Da attuare	Cosa si deve fare: • Definire i requisiti di sicurezza che i fornitori IT devono soddisfare per poter fornire beni e servizi alla PA. • Approvare i requisiti di sicurezza con un atto formale (delibera, decreto, ecc.). • Includere i requisiti di sicurezza nei documenti di gara per l'approvvigionamento IT. Quali sono i requisiti di sicurezza che le PA dovrebbero definire? I requisiti di sicurezza che le PA dovrebbero definire includono: • Sicurezza dei dati • Sicurezza dei sistemi • Sicurezza delle reti • Sicurezza delle applicazioni • Gestione delle vulnerabilità • Controllo degli accessi • Incident response	Le PA definiscono e approvano i requisiti di sicurezza relativi al processo di approvvigionamento IT - CAP7.PA.05

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											Come le PA possono definire e approvare i requisiti di sicurezza per l'approvvigionamento IT? Le PA possono definire e approvare i requisiti di sicurezza per l'approvvigionamento IT: Emanando un atto formale (delibera, decreto, ecc.). • Redigendo un documento che descriva i requisiti di sicurezza. • Utilizzando modelli e best practice disponibili.	
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.2 - Gestire i processi di approvvigionamento IT coerentemente con i requisiti di sicurezza definiti	RA7.2.1	Definizione del framework documentale a supporto del processo di approvvigionamento IT	Da dicembre 2024	2024	PA	Sì	Sì	Da attuare	Cosa si deve fare: • Definire un processo di valutazione e selezione dei fornitori e terze parti IT, basato sulla valutazione dei rischi e sulla conformità ai requisiti di sicurezza. • Definire un modello di contratto per i fornitori e terze parti IT, che includa i requisiti di sicurezza da rispettare. • Monitorare e controllare i fornitori e terze parti IT per assicurarsi che rispettino i requisiti di sicurezza. I requisiti di sicurezza che le PA dovrebbero includere nei contratti con i fornitori IT includono: • Sicurezza dei dati • Sicurezza dei sistemi • Sicurezza delle reti • Sicurezza delle applicazioni • Gestione delle vulnerabilità • Controllo degli accessi • Incident response Come le PA possono definire e promuovere i processi di gestione del rischio e la contrattualistica con i fornitori IT?	Le PA definiscono e promuovono i processi di gestione del rischio sui fornitori e terze parti IT, la contrattualistica per i fornitori e le terze parti IT, comprensive dei requisiti di sicurezza da rispettare - CAP7.PA.06

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											Le PA possono definire e promuovere i processi di gestione del rischio e la contrattualistica con i fornitori IT: • Emanando un atto formale (delibera, decreto, ecc.). • Redigendo un documento che descrive i processi di gestione del rischio e la contrattualistica. • Utilizzando modelli e best practice disponibili.	
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.3 - Gestione e mitigazione del rischio cyber	RA7.3.1	Definizione del framework per la gestione del rischio cyber	Da dicembre 2024	2024	PA	Sì	Sì	Da attuare	Cosa si deve fare: • Definire un processo per la gestione dei rischi informatici (cyber risk management). • Integrare la sicurezza informatica (security by design) fin dalle prime fasi di progettazione di nuovi sistemi e servizi. • Utilizzare gli strumenti messi a disposizione da ACN per la gestione dei rischi informatici e la security by design Come le PA possono definire e formalizzare il processo di cyber risk management e security by design? Le PA possono definire e formalizzare il processo di cyber risk management e security by design: • Effettuando un'analisi dei rischi informatici. • Identificando i controlli necessari per mitigare i rischi informatici. • Implementazione dei controlli identificati. • Monitoraggio e revisione del processo di cyber risk management e security by design. Cosa si intende per cyber risk management?	Le PA definiscono e formalizzano il processo di cyber risk management e security by design, coerentemente con gli strumenti messi a disposizione da ACN - CAP7.PA.08

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											Il cyber risk management è il processo di identificazione, valutazione e mitigazione dei rischi informatici. Cosa si intende per security by design? La security by design è l'approccio che integra la sicurezza informatica fin dalle prime fasi di progettazione di nuovi sistemi e servizi. Quali sono gli strumenti messi a disposizione da ACN? ACN mette a disposizione delle PA diversi strumenti per la gestione dei rischi informatici e la security by design, tra cui: • Linee guida • Procedure • Strumenti di valutazione • Formazione	
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.4 - Potenziare le modalità di prevenzione e e gestione degli incidenti informatici	RA7.4.1	Definizione del framework documentale relativo alla gestione degli incidenti	Da giugno 2024	2024	PA	Sì	Sì	Approfondire	Cosa si deve fare: • Definire un piano di risposta agli incidenti informatici. • Identificare i ruoli e le responsabilità di tutti i soggetti coinvolti nella gestione degli eventi di sicurezza. • Definire le procedure per la gestione degli eventi di sicurezza. • Adottare le misure di sicurezza adeguate alla prevenzione e la gestione degli incidenti informatici. Come le PA possono definire i presidi per la gestione degli eventi di sicurezza? Le PA possono definire i presidi per la gestione degli eventi di sicurezza: • Effettuando un'analisi dei rischi informatici.	Le PA definiscono i presidi per la gestione degli eventi di sicurezza, formalizzandone i processi e le procedure - CAP7.PA.13

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											• Identificando i controlli necessari per mitigare i rischi informatici. • Implementazione dei controlli identificati. • Monitoraggio e revisione dei presidi per la gestione degli eventi di sicurezza Cosa si intende per piano di risposta agli incidenti informatici? Il piano di risposta agli incidenti informatici è un documento che descrive le azioni che le PA devono intraprendere in caso di incidente informatico. Quali sono i ruoli e le responsabilità dei soggetti coinvolti nella gestione degli eventi di sicurezza? I ruoli e le responsabilità dei soggetti coinvolti nella gestione degli eventi di sicurezza variano in base alle dimensioni e alla complessità della PA. In generale, i ruoli principali sono: • Responsabile della sicurezza informatica: Ha la responsabilità complessiva della sicurezza informatica della PA. • CISO: Chief Information Security Officer. È il responsabile tecnico della sicurezza informatica. • Unità di sicurezza informatica: È l'unità responsabile dell'implementazione delle misure di sicurezza informatica. • Team di risposta agli incidenti informatici: È il team responsabile della gestione degli incidenti informatici. Quali sono le procedure per la gestione degli eventi di sicurezza? Le procedure per la gestione degli eventi di sicurezza includono:	

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											• Identificazione dell'incidente: Identificare l'incidente informatico e la sua gravità. • Contenimento dell'incidente: Limitare i danni causati dall'incidente informatico. • Ricerca e analisi dell'incidente: Identificare la causa dell'incidente informatico e le sue implicazioni. • Ripristino dei sistemi: Ripristinare i sistemi informatici danneggiati dall'incidente informatico. • Lezione appresa: Imparare dagli errori commessi per migliorare la capacità di risposta alle future minacce informatiche. Quali sono le misure di sicurezza adeguate alla prevenzione e la gestione degli incidenti informatici? Le misure di sicurezza adeguate variano in base alle dimensioni e alla complessità della PA. In generale, le misure di sicurezza di base includono: • Protezione del perimetro: Proteggere la rete informatica della PA da accessi non autorizzati. • Controllo degli accessi: Limitare l'accesso alle informazioni e ai sistemi informatici della PA ai soli utenti autorizzati. • Protezione dei dati: Proteggere i dati della PA da intrusioni, perdita o furto. • Formazione e sensibilizzazione: Fornire formazione e sensibilizzazione ai dipendenti della PA sui rischi informatici.	
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.4 - Potenziare le modalità di prevenzione e e	RA7.4.1	Definizione del framework documentale relativo alla gestione degli incidenti	Da dicembre 2024	2024	PA	Sì	Sì	Da attuare	Cosa si deve fare: • Definire un piano di risposta agli incidenti informatici (Incident Response Plan - IRP) che includa:	Le PA formalizzano ruoli, responsabilità e processi, nonché le capacità tecnologiche a supporto della prevenzione e gestione degli incidenti informatici - CAP7.PA.14

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
		gestione degli incidenti informatici									○ Ruoli e responsabilità di tutti i soggetti coinvolti nella gestione degli incidenti informatici. ○ Processi per la prevenzione, la detection, la risposta e la ripresa da un incidente informatico. ○ Capacità tecnologiche necessarie per la gestione degli incidenti informatici. • Attuare il piano di risposta agli incidenti informatici e testarlo regolarmente. • Fornire formazione a tutti i dipendenti sui loro ruoli e responsabilità nella gestione degli incidenti informatici. Quali sono i ruoli e le responsabilità che le PA dovrebbero definire? I ruoli e le responsabilità che le PA dovrebbero definire includono: • Responsabile della sicurezza informatica (CISO): responsabile per la definizione e l'implementazione della strategia di sicurezza informatica della PA. • Team di risposta agli incidenti informatici (IRT): responsabile per la gestione degli incidenti informatici. • Dipendenti: responsabili per la segnalazione di eventuali incidenti informatici. Quali sono i processi che le PA dovrebbero definire? I processi che le PA dovrebbero definire includono: • Prevenzione: identificazione e mitigazione dei rischi informatici. • Detection: identificazione tempestiva di un incidente informatico.	

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											• Risposta: azioni da intraprendere per contenere e risolvere un incidente informatico. • Ripresa: ripristino dei sistemi e dei dati dopo un incidente informatico. Quali sono le capacità tecnologiche che le PA dovrebbero implementare? Le capacità tecnologiche che le PA dovrebbero implementare includono: • Strumenti di sicurezza informatica per la prevenzione e la detection degli incidenti informatici. • Sistemi di backup e disaster recovery per la ripresa da un incidente informatico. • Procedure di logging e auditing per la tracciabilità degli eventi e la identificazione delle cause degli incidenti informatici. Come le PA possono formalizzare la gestione degli incidenti informatici? Le PA possono formalizzare la gestione degli incidenti informatici: • Emanando un atto formale (delibera, decreto, ecc.). • Redigendo un documento che descrive il piano di risposta agli incidenti informatici. • Utilizzando modelli e best practice disponibili.	
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.4 - Potenziare le modalità di prevenzione e gestione degli incidenti informatici	RA7.4.2	Definizione delle modalità di verifica e aggiornamento dei piani di risposta agli incidenti	Da dicembre 2024	2024	PA	Sì	Sì	Da attuare	Cosa si deve fare: • Definire un piano di verifica del DRP che includa: ○ Obiettivi della verifica. ○ Metodologia di verifica. ○ Strumenti da utilizzare per la verifica. ○ Frequenza della verifica. • Attuare il piano di verifica del DRP e documentare i risultati.	Le PA definiscono le modalità di verifica dei Piani di risposta a seguito di incidenti informatici - CAP7.PA.15

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											• Effettuare le necessarie correzioni al DRP in base ai risultati della verifica. Quali sono gli obiettivi della verifica del DRP? Gli obiettivi della verifica del DRP includono: • Valutare l'efficacia del DRP nel rispondere a un incidente informatico. • Identificare eventuali carenze del DRP. • Migliorare il DRP nel tempo. Qual è la metodologia di verifica del DRP? La metodologia di verifica del DRP può includere: • Revisione del DRP per verificarne la completezza e l'accuratezza. • Simulazione di un incidente informatico per testare il DRP. • Interviste ai soggetti coinvolti nella gestione del DRP. Quali sono gli strumenti da utilizzare per la verifica del DRP? Gli strumenti da utilizzare per la verifica del DRP possono includere: • Checklist per la revisione del DRP. • Scenari di simulazione di incidenti informatici. • Questionari per le interviste ai soggetti coinvolti nella gestione del DRP.	
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.5 - Implementare attività strutturate di	RA7.5.1	Definizione dei piani di formazione in ambito cyber	Da giugno 2024	2024	PA	Sì	Sì	Da attuare	Cosa si deve fare: • Promuovere la cultura della sicurezza informatica tra i propri dipendenti.	Le PA promuovono l'accesso e l'utilizzo di attività strutturate di sensibilizzazione e formazione in ambito cybersicurezza - CAP7.PA.17

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
		sensibilizzazione cyber del personale									• Organizzare attività di formazione sulla cybersicurezza per tutti i dipendenti. • Fornire ai dipendenti gli strumenti necessari per proteggersi dalle minacce informatiche. Come le PA possono promuovere la sensibilizzazione e la formazione in ambito cybersicurezza? Le PA possono promuovere la sensibilizzazione e la formazione in ambito cybersicurezza: • Organizzando corsi di formazione sulla cybersicurezza. • Inviando e-mail informative sui rischi informatici. • Pubblicando materiale informativo sul sito web della PA. • Organizzando eventi di sensibilizzazione sulla cybersicurezza. Quali sono i temi principali che dovrebbero essere trattati nei corsi di formazione sulla cybersicurezza? I temi principali che dovrebbero essere trattati nei corsi di formazione sulla cybersicurezza includono: • Le minacce informatiche più comuni • Le best practice per la sicurezza informatica • Come proteggere i dati personali e professionali • Come riconoscere e rispondere alle minacce informatiche A chi dovrebbero essere rivolti i corsi di formazione sulla cybersicurezza? I corsi di formazione sulla cybersicurezza dovrebbero essere rivolti a tutti i dipendenti delle PA, indipendentemente dal loro ruolo o livello di competenza.	

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											Quali sono gli strumenti che le PA possono fornire ai dipendenti per proteggersi dalle minacce informatiche? Le PA possono fornire ai dipendenti diversi strumenti per proteggersi dalle minacce informatiche, tra cui: • Antivirus • Antispam • Firewall • VPN	
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.5 - Implementare attività strutturate di sensibilizzazione cyber del personale	RA7.5.1	Definizione dei piani di formazione in ambito cyber	Da dicembre 2024	2024	PA	Sì	Sì	Da pianificare	Cosa si deve fare: • Sviluppare piani di formazione sulla cybersecurity specifici per ciascun ruolo, posizione organizzativa e attività svolta all'interno della PA. • Adeguare i contenuti dei piani di formazione alle esigenze specifiche di ciascun gruppo di dipendenti. • Garantire che tutti i dipendenti ricevano la formazione necessaria per svolgere il proprio lavoro in modo sicuro. Quali sono i criteri che le PA dovrebbero utilizzare per diversificare i piani di formazione sulla cybersecurity? I criteri che le PA dovrebbero utilizzare per diversificare i piani di formazione sulla cybersecurity includono: • Il livello di accesso alle informazioni e ai sistemi informatici • Il tipo di dati trattati • Le attività svolte • Le responsabilità Quali sono i contenuti che dovrebbero essere inclusi nei piani di formazione sulla cybersecurity?	Le PA definiscono piani di formazione inerenti alla cybersecurity, diversificati per ruoli, posizioni organizzative e attività delle risorse dell'organizzazione - CAP7.PA.18

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											I contenuti che dovrebbero essere inclusi nei piani di formazione sulla cybersecurity includono: • Le minacce informatiche più comuni • Le best practice per la sicurezza informatica • Come proteggere i dati personali e professionali • Come riconoscere e rispondere alle minacce informatiche Come le PA possono garantire che tutti i dipendenti ricevano la formazione necessaria? Le PA possono garantire che tutti i dipendenti ricevano la formazione necessaria: • Rendendo la formazione obbligatoria per tutti i dipendenti • Offrendo la formazione in diverse modalità (aula, online, e-learning) • Monitorando la partecipazione alla formazione • Valutando l'apprendimento dei dipendenti	
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.6 - Contrastare il rischio cyber attraverso attività di supporto proattivo alla PA	RA7.6.1	Distribuzione di Indicatori di Compromissione alle PA	Da febbraio 2024	2024	PA	Sì	Sì	Da attuare	Cosa si deve fare: • Acquisire gli strumenti necessari per ricevere e gestire gli IoC dal CERT-AGID. • Accreditarsi al CERT-AGID per poter accedere al servizio di feed di IoC. • Implementare le procedure per l'utilizzo degli IoC nella propria attività di gestione dei rischi informatici. Cosa sono gli IoC? Gli IoC (Indicatori di Compromissione) sono informazioni che possono essere utilizzate per identificare un attacco informatico in corso o imminente.	Le PA dovranno dotarsi degli strumenti idonei all'acquisizione degli IoC ed accreditarsi al CERT-AGID - CAP7.PA.20

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											Quali sono i vantaggi di acquisire gli IoC? I vantaggi di acquisire gli IoC includono: • Migliore capacità di prevenzione delle minacce informatiche. • Riduzione del tempo di risposta agli incidenti informatici. • Maggiore consapevolezza dei rischi informatici. Come si può ottenere l'accreditamento al CERT-AGID? Per ottenere l'accreditamento al CERT-AGID, le PA devono: • Compilare il modulo di accreditamento disponibile sul sito web del CERT-AGID. • Inviare la documentazione richiesta al CERT-AGID. • Superare un audit da parte del CERT-AGID.	
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.6 - Contrastare il rischio cyber attraverso attività di supporto proattivo alla PA	RA7.6.2	Fornitura di strumenti funzionali all'esecuzione dei piani di autovalutazione e dei sistemi esposti	Da ottobre 2024	2024	PA	Sì	Sì	Da attuare	Cosa si deve fare: • Implementare gli strumenti del CERT-AGID per la gestione dei rischi cyber. • Utilizzare gli strumenti per monitorare, identificare e rispondere alle minacce informatiche. • Fornire formazione ai propri dipendenti sull'utilizzo degli strumenti. Quali strumenti offre il CERT-AGID? Il CERT-AGID offre diversi strumenti per la gestione dei rischi cyber, tra cui: • Piattaforma di analisi e condivisione di informazioni sulle minacce informatiche (Cyber Threat Intelligence Platform – CTIP) • Sistema di monitoraggio delle vulnerabilità (HyperSOC)	Le PA dovranno usufruire degli strumenti per la gestione dei rischi cyber messi a disposizione dal CERT-AGID - CAP7.PA.21

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											• Servizio di early warning • Servizio di analisi forense • Formazione sulla sicurezza informatica Come le PA possono iniziare a utilizzare gli strumenti del CERT-AGID? Le PA possono iniziare a utilizzare gli strumenti del CERT-AGID: • Registrandosi al portale del CERT-AGID • Consultando la documentazione disponibile sul portale • Partecipando ai corsi di formazione erogati dal CERT-AGID • Contattando il CERT-AGID per ricevere assistenza Quali sono i vantaggi di utilizzare gli strumenti del CERT-AGID? I vantaggi di utilizzare gli strumenti del CERT-AGID includono: • Migliore capacità di prevenzione delle minacce informatiche. • Riduzione del tempo di risposta agli incidenti informatici. • Maggiore consapevolezza dei rischi informatici. • Risparmio di tempo e denaro • Accesso a competenze specialistiche Come si può ottenere assistenza per l'utilizzo degli strumenti del CERT-AGID? Le PA possono ottenere assistenza per l'utilizzo degli strumenti del CERT-AGID: • Consultando la documentazione disponibile sul portale	

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	LINEA DI AZIONE
											• Partecipando ai corsi di formazione erogati dal CERT-AGID • Contattando il CERT-AGID tramite e-mail o telefono	

LINEE DI AZIONE DEL PIANO PREVISTE PER L'ANNO 2025

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	DECRIZIONE RISULTATO ATTESO
PARTE PRIMA – Componenti strategiche per la trasformazione digitale	Capitolo 1 - Organizzazione e gestione del cambiamento	Obiettivo 1.3 - Monitorare e analizzare lo stato di digitalizzazione del paese	RA1.3.2/RA1.3.3	Acquisizione ed elaborazione di informazioni analitiche da Enti locali e Aumento delle tipologie e delle fonti dati integrate all'interno dell'Osservatorio	set-25	2025	ENTI LOCALI	Sì	Sì	Da pianificare		Gli Enti locali partecipano alla seconda fase della raccolta dati, garantendo l'accuratezza e la completezza delle informazioni - CAP1.PA.12
PARTE PRIMA – Componenti strategiche per la trasformazione digitale	Capitolo 2 - Il procurement per la trasformazione digitale	Obiettivo 2.3 - Favorire e monitorare l'utilizzo dei servizi previsti dalle Gare strategiche	RA2.3.1	Incremento del livello di trasformazione digitale mediante la disponibilità di Gare strategiche allo scopo definite	set-25	2025	PA	Sì	Sì	Da pianificare	Vedere CAP2.PA.04 anno 2024	Le PA programmano i fabbisogni di adesione alle iniziative strategiche per il perseguimento degli obiettivi del Piano triennale per l'anno 2026 - CAP2.PA.05
PARTE SECONDA – Componenti tecnologiche	Capitolo 3 - Servizi	Obiettivo 3.1 - Migliorare la capacità di erogare e-service	RA3.1.2	Aumento del numero di Richieste di Fruizione Autorizzate su PDND	Da gennaio 2025	2025	PA	Sì	Sì	Da verificare		Le PA effettuano richieste di fruizione di servizi erogati da privati - CAP3.PA.07
PARTE SECONDA – Componenti tecnologiche	Capitolo 3 - Servizi	Obiettivo 3.2 - Migliorare la capacità di generare ed erogare servizi digitali	RA3.2.2	Incremento dell'accessibilità dei servizi digitali	mar-25	2025	PA	Sì	Sì	Da pianificare		Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web - CAP3.PA.13
PARTE SECONDA – Componenti tecnologiche	Capitolo 3 - Servizi	Obiettivo 3.2 - Migliorare la capacità di generare ed erogare servizi digitali	RA3.2.2	Incremento dell'accessibilità dei servizi digitali	set-25	2025	PA	Sì	Sì	Da pianificare	Da attuare entro il 23 settembre 2025	Le PA pubblicano, entro il 23 settembre, esclusivamente tramite l'applicazione form.AGID.gov.it, la dichiarazione di accessibilità per ciascuno dei propri siti web e

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	DECRIZIONE RISULTATO ATTESO
												APP mobili - CAP3.PA.1
PARTE SECONDA – Componenti tecnologiche	Capitolo 4 - Piattaforme	Obiettivo 4.3 - Migliorare la sicurezza, accessibilità e l'interoperabilità delle basi dati di interesse nazionale	RA4.3.1	Incremento del numero di basi dati di interesse nazionale conformi alle regole tecniche	Da gennaio 2025	2025	PA	Sì	Sì	Da verificare		Le PA interessate avanzano la richiesta di inserimento delle proprie basi di dati nell'elenco di Basi di dati di interesse nazionale gestito da AGID secondo il processo definito - CAP4.PA.23
PARTE SECONDA – Componenti tecnologiche	Capitolo 4 - Piattaforme	Obiettivo 4.3 - Migliorare la sicurezza, accessibilità e l'interoperabilità delle basi dati di interesse nazionale	RA4.3.1	Incremento del numero di basi dati di interesse nazionale conformi alle regole tecniche	Da gennaio 2025	2025	PA	Sì	Sì	Da verificare		La PA titolari di basi di dati di interesse nazionale le adeguano all'aggiornamento delle regole tecniche - CAP4.PA.24
PARTE SECONDA – Componenti tecnologiche	Capitolo 5 - Dati e Intelligenza Artificiale	Obiettivo 5.2 - Aumentare la qualità dei dati e dei metadati	RA5.2.1	Aumento del numero di dataset con metadati di qualità conformi agli standard di riferimento europei e nazionali	Da giugno 2025	2025	PA	Sì	Sì	Da pianificare		Le PA pubblicano i metadati relativi ai dati di elevato valore, secondo le indicazioni presenti nel Regolamento di esecuzione (UE) e nelle Linee guida sui dati aperti e relativa guida operativa, nei cataloghi nazionali dati.gov.it e geodati.gov.it - CAP5.PA.05

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	DECRIZIONE RISULTATO ATTESO
PARTE SECONDA – Componenti tecnologiche	Capitolo 5 - Dati e Intelligenza Artificiale	Obiettivo 5.4 - Aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale	RA5.4.1	Linee guida per promuovere l'adozione dell'IA nella Pubblica Amministrazione	dic-25	2025	PA	Sì	Sì	Da verificare		Le PA adottano le Linee per promuovere l'adozione dell'IA nella Pubblica Amministrazione - CAP5.PA.21
PARTE SECONDA – Componenti tecnologiche	Capitolo 5 - Dati e Intelligenza Artificiale	Obiettivo 5.4 - Aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale	RA5.4.2	Linee guida per il procurement di IA nella Pubblica Amministrazione	dic-25	2025	PA	Sì	Sì	Da verificare		Le PA adottano le Linee guida per il procurement di IA nella Pubblica Amministrazione - CAP5.PA.22
PARTE SECONDA – Componenti tecnologiche	Capitolo 5 - Dati e Intelligenza Artificiale	Obiettivo 5.4 - Aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale	RA5.4.3	Linee guida per lo sviluppo di applicazioni di IA per la Pubblica Amministrazione	dic-25	2025	PA	Sì	Sì	Da verificare		Le PA adottano le Linee guida per lo sviluppo di applicazioni di IA nella Pubblica Amministrazione - CAP5.PA.23
PARTE SECONDA – Componenti tecnologiche	Capitolo 6 - Infrastrutture	Obiettivo 6.2 - Garantire alle amministrazioni la disponibilità della connettività SPC	RA6.2.1	Rete di connettività	Da gennaio 2025	2025	PA	Sì	Sì	Da verificare		Sulla base delle proprie esigenze, le pubbliche amministrazioni iniziano la fase di migrazione della loro infrastruttura di rete utilizzando i servizi resi disponibili dalla nuova gara di connettività SPC – CAP6.PA.11
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.2 - Gestire i processi di approvvigionamento IT coerentemente con i requisiti di sicurezza definiti	RA7.2.2	Definizione delle modalità di monitoraggio del processo di approvvigionamento IT	Da dicembre 2025	2025	PA	Sì	Sì	Da pianificare		Le PA realizzano le attività di controllo definite nel Piano di audit e verifica verso i fornitori e

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	DECRIZIONE RISULTATO ATTESO
												terze parti IT - CAP7.PA.07
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.3 - Gestione e mitigazione del rischio cyber	RA7.3.1	Definizione del framework per la gestione del rischio cyber	Da dicembre 2025	2025	PA	Sì	Sì	Da pianificare		Le PA promuovono il censimento dei dati e servizi della PA, identificandone la rilevanza e quindi le modalità per garantirne la continuità operativa - CAP7.PA.09
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.3 - Gestione e mitigazione del rischio cyber	RA7.3.1	Definizione del framework per la gestione del rischio cyber	Da dicembre 2025	2025	PA	Sì	Sì	Da pianificare		Le PA realizzano o acquisiscono gli strumenti atti alla messa in sicurezza dell'integrità, confidenzialità e disponibilità dei servizi e dei dati, come definito dalle relative procedure - CAP7.PA.10
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.3 - Gestione e mitigazione del rischio cyber	RA7.3.2	Definizione delle modalità di monitoraggio del rischio cyber	Da dicembre 2025	2025	PA	Sì	Sì	Da pianificare		Le PA integrano le attività di monitoraggio del rischio cyber, come definito dal relativo Piano, nelle normali attività di progettazione, analisi, conduzione e dismissione di applicativi e sistemi informativi - CAP7.PA.12

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	DECRIZIONE RISULTATO ATTESO
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.4 - Potenziare le modalità di prevenzione e gestione degli incidenti informatici	RA7.4.2	Definizione delle modalità di verifica e aggiornamento dei piani di risposta agli incidenti	Da dicembre 2025	2025	PA	Sì	Sì	Da pianificare		Le PA definiscono le modalità di aggiornamento dei Piani di risposta e ripristino a seguito dell'accadimento di incidenti informatici - CAP7.PA.16
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.5 - Implementare attività strutturate di sensibilizzazione cyber del personale	RA7.5.2	Adozione di strumenti atti alla formazione in ambito cyber	Da dicembre 2025	2025	PA	Sì	Sì	Da pianificare		Le PA realizzano iniziative per verificare e migliorare la consapevolezza del proprio personale - CAP7.PA.19
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.6 - Contrastare il rischio cyber attraverso attività di supporto proattivo alla PA	RA7.6.3	Supporto formativo e informativo rivolto alle PA e in particolare agli RTD per l'aumento del livello di consapevolezza delle minacce cyber	dic-25	2025	PA	Sì	Sì	Da pianificare		Le PA, sulla base delle proprie esigenze, partecipano ai corsi di formazione base ed avanzato erogati dal CERT-AGID - CAP7.PA.22

LINEE DI AZIONE DEL PIANO PREVISTE PER L'ANNO 2026

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	DECRIZIONE RISULTATO ATTESO
PARTE PRIMA – Componenti strategiche per la trasformazione digitale	Capitolo 2 - Il procurement per la trasformazione digitale	Obiettivo 2.1 - Rafforzare l'ecosistema nazionale di approvvigionamento digitale	RA2.1.1	Diffusione del processo di certificazione delle piattaforme di approvvigionamento digitale	dic-26	2026	STAZIONI APPALTANTI	Sì	Sì	Da pianificare		Le stazioni appaltanti devono digitalizzare la fase di esecuzione dell'appalto - CAP2.PA.02
PARTE PRIMA – Componenti strategiche per la trasformazione digitale	Capitolo 2 - Il procurement per la trasformazione digitale	Obiettivo 2.3 - Favorire e monitorare l'utilizzo dei servizi previsti dalle Gare strategiche	RA2.3.1	Incremento del livello di trasformazione digitale mediante la disponibilità di Gare strategiche allo scopo definite	set-26	2026	PA	Sì	Sì	Da pianificare	Vedere CAP2.PA.04 anno 2024	Le PA programmano i fabbisogni di adesione alle iniziative strategiche per il perseguimento degli obiettivi del Piano triennale per l'anno 2027 - CAP2.PA.06
PARTE SECONDA – Componenti tecnologiche	Capitolo 3 - Servizi	Obiettivo 3.2 - Migliorare la capacità di generare ed erogare servizi digitali	RA3.2.2	Incremento dell'accessibilità dei servizi digitali	mar-26	2026	PA	Sì	Sì	Da pianificare		Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web - CAP3.PA.15
PARTE SECONDA – Componenti tecnologiche	Capitolo 3 - Servizi	Obiettivo 3.2 - Migliorare la capacità di generare ed erogare servizi digitali	RA3.2.2	Incremento dell'accessibilità dei servizi digitali	set-26	2026	PA	Sì	Sì	Da pianificare	Da attuare entro il 23 settembre 2026	Le PA pubblicano, entro il 23 settembre, esclusivamente tramite l'applicazione form.AGID.gov.it, la dichiarazione di accessibilità per ciascuno dei propri siti web e APP mobili - CAP3.PA.16

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	DECRIZIONE RISULTATO ATTESO
PARTE SECONDA – Componenti tecnologiche	Capitolo 3 - Servizi	Obiettivo 3.3 - Consolidare l'applicazione delle Linee guida per la formazione, gestione e conservazione documentale	RA3.3.1	Monitorare l'attuazione delle linee guida	giu-25	2026	PA	Sì	Sì	Da pianificare		Le PA devono verificare che in "Amministrazione trasparente" sia pubblicato il manuale di gestione documentale, la nomina del responsabile della gestione documentale per ciascuna AOO e qualora siano presenti più AOO la nomina del coordinatore della gestione documentale - CAP3.PA.17
PARTE SECONDA – Componenti tecnologiche	Capitolo 3 - Servizi	Obiettivo 3.3 - Consolidare l'applicazione delle Linee guida per la formazione, gestione e conservazione documentale	RA3.3.1	Monitorare l'attuazione delle linee guida	giu-26	2026	PA	Sì	Sì	Da pianificare		Le PA devono verificare che in "Amministrazione trasparente" sia pubblicato il manuale di conservazione e la nomina del responsabile della conservazione - CAP3.PA.18
PARTE SECONDA – Componenti tecnologiche	Capitolo 4 - Piattaforme	Obiettivo 4.1 - Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA	RA4.1.1	Incremento dei servizi sulla piattaforma pagoPA	dic-26	2026	PA	Sì	Sì	Da pianificare		Le PA aderenti a pagoPA assicurano l'attivazione di nuovi servizi in linea con i target sopra descritti e secondo le modalità attuative definite nell'ambito del Piano Nazionale di Ripresa e Resilienza

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	DECRIZIONE RISULTATO ATTESO
												(PNRR) - CAP4.PA.01
PARTE SECONDA – Componenti tecnologiche	Capitolo 4 - Piattaforme	Obiettivo 4.1 - Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA	RA4.1.2	Incremento dei servizi sulla Piattaforma IO (l'App dei servizi pubblici)	dic-26	2026	PA	Sì	Sì	Da pianificare		Le PA aderenti a App IO assicurano l'attivazione di nuovi servizi in linea con i target sopra descritti e secondo le modalità attuative definite nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR) - CAP4.PA.02
PARTE SECONDA – Componenti tecnologiche	Capitolo 4 - Piattaforme	Obiettivo 4.1 - Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA	RA4.1.3	Incremento degli enti che usano SEND	dic-26	2026	PAC e COMUNI	Sì	Sì	Da pianificare		Le PA centrali e i Comuni, in linea con i target sopra descritti e secondo la roadmap di attuazione prevista dal Piano Nazionale di Ripresa e Resilienza (PNRR), si integreranno a SEND - CAP4.PA.03
PARTE SECONDA – Componenti tecnologiche	Capitolo 5 - Dati e Intelligenza Artificiale	Obiettivo 5.4 - Aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale	RA5.4.4	Realizzazione di applicazioni di IA a valenza nazionale	dic-26	2026	PA	Sì	Sì	Da verificare		Le PA adottano le applicazioni di IA a valenza nazionale - CAP5.PA.24

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	DECRIZIONE RISULTATO ATTESO
PARTE SECONDA – Componenti tecnologiche	Capitolo 5 - Dati e Intelligenza Artificiale	Obiettivo 5.4 - Aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale	RA5.5.1	Basi di dati nazionali strategiche	dic-26	2026	PA	Sì	Sì	Da verificare		Le PA adottano le basi dati nazionali strategiche - CAP5.PA.25
PARTE SECONDA – Componenti tecnologiche	Capitolo 6 - Infrastrutture	Obiettivo 6.1 - Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la strategia "Cloud Italia" e migrando verso infrastrutture e servizi cloud qualificati (incluso PSN)	RA6.1.1	Numero di amministrazioni migrate	giu-26	2026	AMMINISTRAZIONI	Sì	Sì	Ok	L'ente ha migrato gli applicativi su Cloud	Le amministrazioni concludono la migrazione in coerenza con il piano di migrazione trasmesso ai sensi del Regolamento cloud e, ove richiesto dal Dipartimento per la Trasformazione Digitale o da AGID, trasmettono le informazioni necessarie per verificare il completamento della migrazione – CAP6.PA.10
PARTE SECONDA – Componenti tecnologiche	Capitolo 7 - Sicurezza informatica	Obiettivo 7.3 - Gestione e mitigazione del rischio cyber	RA7.3.1	Definizione del framework per la gestione del rischio cyber	Da dicembre 2026	2026	PA	Sì	Sì	Da pianificare		Le PA integrano le attività di monitoraggio del rischio cyber, come definito dal relativo Piano, nelle normali attività di progettazione, analisi, conduzione e dismissione di applicativi e sistemi

PARTE	CAPITOLO	OBBIETIVI	RISULTATI ATTESI		QUANDO	ANNO	CHI	APPLICABILE AI COMUNI	APPLICABILE AL COMUNE	STATO	ATTUAZIONE	DECRIZIONE RISULTATO ATTESO
												informativi - CAP7.PA.11

Attività da focalizzare

Scadenze a breve

Gennaio 2024

- Le PA cessano di utilizzare modalità di interoperabilità diverse da PDND - CAP3.PA.01
- Le PA attuano le linee guida contenenti regole tecniche per l'implementazione del Decreto Legislativo n. 36/2006 relativamente ai requisiti e alle raccomandazioni su licenze e condizioni d'uso - CAP5.PA.20
- Le PA, ove richiesto dal Dipartimento per la Trasformazione Digitale o da AGID, trasmettono le informazioni relative allo stato di avanzamento dell'implementazione dei piani di migrazione – CAP6.PA.06

Febbraio 2024

- Dalla "fine dell'adozione controllata" i Comuni potranno richiedere l'adesione servizi di Stato civile su ANPR - CAP4.PA.18
- Le PA dovranno dotarsi degli strumenti idonei all'acquisizione degli IoC ed accreditarsi al CERT-AGID - CAP7.PA.20

Marzo 2024

- Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web - CAP3.PA.09

Da Giugno 2024

- Le PA attuano le indicazioni sui dati di elevato valore presenti nel Regolamento di esecuzione (UE) 2023/138, nelle Linee guida Open Data nonché nella specifica guida operativa - CAP5.PA.04
- Le PA definiscono e approvano i requisiti di sicurezza relativi al processo di approvvigionamento IT - CAP7.PA.05
- Le PA definiscono i presidi per la gestione degli eventi di sicurezza, formalizzandone i processi e le procedure - CAP7.PA.13
- Le PA promuovono l'accesso e l'utilizzo di attività strutturate di sensibilizzazione e formazione in ambito cybersicurezza - CAP7.PA.17

Monitoraggio

Nel piano della performance verrà inserito uno specifico obiettivo/parametro finalizzato all'attuazione delle operazioni sopra elencate.

La verifica del grado di realizzazione del suddetto obiettivo/parametro consentirà di monitorare la transizione digitale dei servizi dell'ente.

Allegati al piano

A. PIANO TRIENNALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE Edizione 2024-2026