



Comune di Castelfranco Piandiscò

PIANO TRIENNALE PER L'INFORMATICA 2024-2026

Aggiornamento 2026



INDICE

INDICE.....	II
CRONOLOGIA REVISIONI E SINTESI MODIFICHE.....	1
ACRONIMI E DEFINIZIONI	2
RIFERIMENTI NORMATIVI	4
PREMESSA	7
INTRODUZIONE	9
OBIETTIVI PREFISSATI DA AGID	13
STATO ATTUALE DELL'ENTE	15
SINTESI DEL PIANO E CRONO PROGRAMMA	17



CRONOLOGIA REVISIONI E SINTESI MODIFICHE

Data	Versione	Provvedimento di Approvazione	Sintesi delle modifiche
30/06/2026			



ACRONIMI E DEFINIZIONI¹

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

ANAC: Autorità nazionale anticorruzione.

AOO: Area Organizzativa Omogenea.

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

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

BDNCP: Banca dati nazionale dei contratti pubblici, istituita presso ANAC.

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

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

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

Consip SpA: centrale di acquisto nazionale che offre strumenti e soluzioni di *e-procurement* per la digitalizzazione degli acquisti di amministrazioni e imprese.

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

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

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

DDT: Documento di trasporto (digitale).

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

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

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

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

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

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

¹ Fonte piano_triennale_per_informatica_nella_pa_2024-2026 aggiornamento 2025



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

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

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

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

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

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

- **Privacy by design e by default:** Principio per cui i servizi pubblici devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali.

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

- **RUP:** Responsabile Unico di Progetto a seguito del d.lgs. 36/2023, già Responsabile Unico di Procedimento.

- **SDI:** Sistema di interscambio, è un sistema informatico in grado di: ricevere le fatture sotto forma di file con le caratteristiche della FatturaPA; effettuare controlli sui file ricevuti; inoltrare le fatture verso le amministrazioni pubbliche destinatarie, o verso cessionari/committenti privati (B2B e B2C).

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

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

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



RIFERIMENTI NORMATIVI²

Di seguito un elenco delle principali fonti, raccomandazioni e norme sugli argomenti trattati a cui le amministrazioni devono attenersi.

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.64-bis c.1-bis CAD art.64-bis 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

² Fonte piano_triennale_per_informatica_nella_pa_2024-2026



Principi guida	Definizioni	Riferimenti normativi
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.50-quater e art.52 c.2 CAD D.Lgs 36/2006 Art.24-quater c.2 DL90/2014
7. concepito per la sicurezza e la protezione dei dati personali (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"
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	Art.5, 117 e 118 Costituzione Art.14 CAD



	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.	
--	--	--



PREMESSA

La presente relazione fornisce un quadro analitico e storico del processo di trasformazione digitale del Comune di Castelfranco Piandiscò nel periodo compreso tra il 2020 e il primo semestre del 2026. L'analisi si basa sul confronto dei successivi aggiornamenti dei Cronoprogrammi del Piano Triennale per l'Informatica nella PA (AgID) e sullo stato di consistenza del parco applicativi dell'Ente.

Il monitoraggio evidenzia tre macro-fasi: una prima fase di adeguamento normativo minimo ed emergenziale (2020-2021), una seconda fase di accelerazione strutturale abilitata dai fondi europei (2022-2024), e una terza fase di consolidamento, sicurezza e interoperabilità avanzata (2025-2026).

Il percorso di digitalizzazione è stato mappato aggregando gli obiettivi AgID in quattro macro-aree tecnologiche e procedurali, analizzandone l'evoluzione temporale dal 2020 ad oggi.

- Servizi ai Cittadini e Identità Digitale (SPID, CIE, PagoPA, App IO) Nel biennio 2020-2021 l'Ente registrava un'attivazione parziale dei canali digitali. PagoPA copriva soltanto i servizi scolastici e le sanzioni del codice della strada, mentre l'integrazione con l'App IO risultava rallentata da barriere tecnologiche dei software gestionali allora in uso. Tra il 2022 e il 2024, in coincidenza con l'attivazione della Misura 1.4.3 del PNRR, si è assistito a una convergenza di tutti i moduli di pagamento e alla pubblicazione di oltre 30 servizi comunali sulla piattaforma App IO. Nel report aggiornato a giugno 2026, l'integrazione risulta completata con successo, includendo l'autenticazione esclusiva tramite SPID/CIE per il 100% dei servizi online.
- Infrastrutture immateriali e Migrazione in Cloud I primi cronoprogrammi (2020-2022 e 2021-2023) mostravano il persistere di server fisici locali (on-premise) per la gestione dell'Anagrafe, dei Tributi e della Contabilità Finanziaria. La pianificazione originaria prevedeva una transizione graduale verso infrastrutture cloud entro il 2024, ma i target subivano sistematici rinvii. La svolta strategica si colloca nel Cronoprogramma 22_24 con il finanziamento della Misura 1.2 PNRR ("Abilitazione al Cloud per le PA Locali"). Tale risorsa ha azzerato i tempi morti: i dati correnti del registro applicativi 2026 confermano che l'intero ecosistema software dell'Ente è ospitato su data center qualificati ACN (Agenzia per la Cybersicurezza Nazionale) in modalità SaaS (Software as a Service).
- Interoperabilità e Valorizzazione del Patrimonio Informativo (PDND) Fini al 2022 la condivisione dei dati tra i settori interni (es. Urbanistica, Tributi, Demografici) e verso l'esterno avveniva tramite cooperazioni applicative artigianali e flussi batch asincroni. L'adozione della Piattaforma Digitale Nazionale Dati (PDND - Misura 1.3.1), introdotta programmaticamente a partire dal ciclo 2024-2026, ha imposto uno standard rigoroso. Ad oggi, l'Ente scambia dati demografici e fiscali in tempo reale mediante API (Application Programming Interface) certificate, azzerando le richieste cartacee.
- Sicurezza Informatica (Cybersecurity) e Continuità Operativa Inizialmente limitata alle Misure Minime di Sicurezza AgID (LOG di accesso, antivirus tradizionali, backup su nas locale), la cybersecurity ha subito una radicale evoluzione. Nei cronoprogrammi aggiornati al 2025 e 2026, l'Ente ha recepito i dettami della Direttiva NIS2, spostando il focus sul



monitoraggio proattivo degli endpoint, sulla crittografia dei flussi documentali e sulla formazione continua del personale in materia di ingegneria sociale e phishing.

Il giudizio finale sul percorso di digitalizzazione del Comune di Castelfranco Piandiscò, alla luce dell'analisi dei cronoprogrammi dal 2020 ad oggi (giugno 2026), è pienamente positivo, delineando il profilo di un Ente virtuoso che ha saputo trasformare un obbligo normativo in una reale opportunità di ammodernamento strutturale.

Il percorso può essere sintetizzato secondo i seguenti giudizi di merito:

- Ottima capacità di intercettazione e messa a terra dei fondi L'Ente ha mostrato una reattività straordinaria a partire dal 2022. Se la prima fase (2020-2021) era caratterizzata da una digitalizzazione frammentata e rallentata dai vincoli di bilancio locali, l'introduzione del PNRR è stata sfruttata al massimo potenziale. Le scadenze ministeriali stringenti non hanno ingessato il Comune, ma hanno fatto da volano, azzerando gli storici slittamenti temporali.
- Radicale evoluzione dell'infrastruttura. Il passaggio da un modello on-premise (basato su server fisici locali dislocati nei vari uffici) a un ecosistema interamente in Cloud qualificato ACN (SaaS) rappresenta il traguardo più significativo. Questo non solo garantisce una drastica riduzione dei costi di manutenzione hardware, ma assicura una continuità operativa (business continuity) precedentemente complessa da mantenere.
- Maturità nei servizi al cittadino e interoperabilità L'Ente non si è limitato ad adempimenti di facciata. L'estensione di PagoPA a oltre 45 tassonomie, la migrazione massiva su App IO, l'adozione della piattaforma SEND per le notifiche digitali e l'apertura degli e-service sulla PDND (Piattaforma Digitale Nazionale Dati) dimostrano il raggiungimento di un livello di interoperabilità nativa e matura, abbattendo i tempi di attesa per l'utenza e applicando concretamente il principio del Once-Only.
- Visione lungimirante e sicurezza. L'adeguamento tempestivo alle direttive di Cybersecurity (come la NIS2) e l'inserimento del personale nei piani di formazione obbligatoria tramite la piattaforma Syllabus dimostrano che la governance dell'Ente comprende che la transizione digitale non è un processo esclusivamente tecnologico, ma culturale e di protezione del patrimonio informativo.



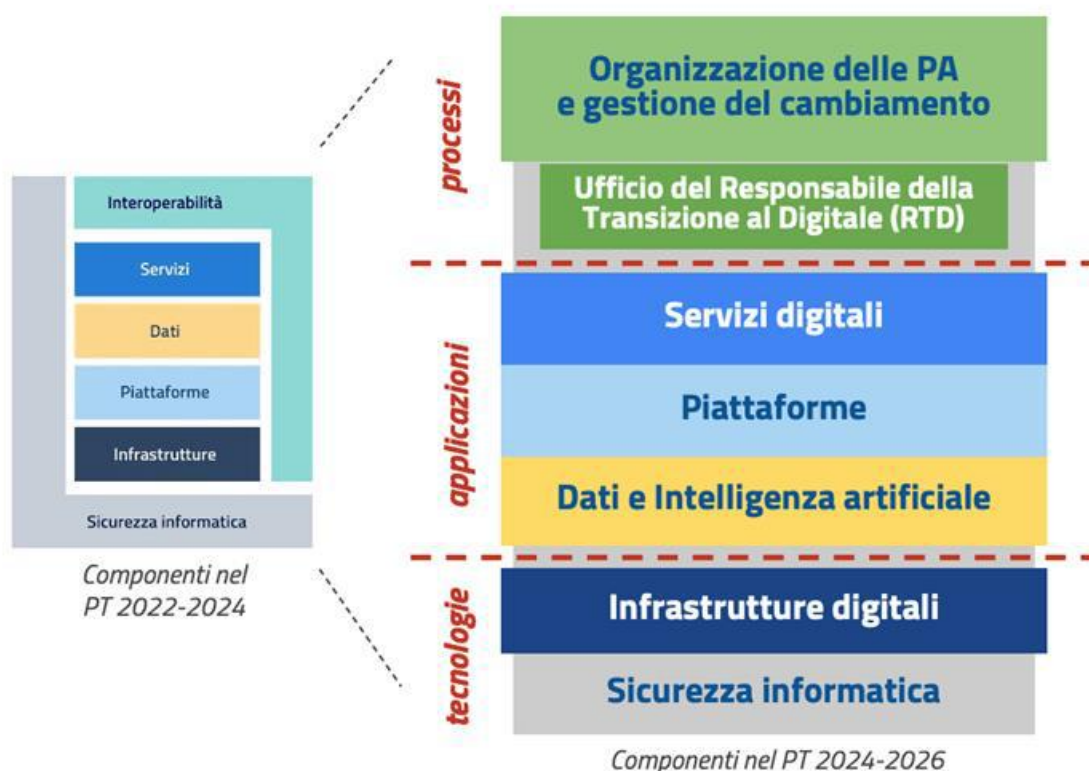
INTRODUZIONE

Il Piano triennale 2024-2026 come il passato Piano 2022 – 2024, detta indirizzi specifici per le amministrazioni e contiene elementi orientati fortemente alla responsabilizzazione delle PA.

Il Piano emanato da AgID è costituito sulla base di un Modello strategico di evoluzione del sistema informativo della Pubblica Amministrazione ed indirizza le PA nel raggiungimento dei risultati attesi presentando la visione a medio/lungo termine verso la quale la PA deve tendere per sfruttare al meglio i benefici derivanti dall'uso delle tecnologie digitali.

Il Piano triennale 2024-26 classifica non solo le sfide tecnologiche ma soprattutto le sfide organizzative che le amministrazioni devono affrontare. Il modello, quindi, viene integrato con la gestione dei processi

MODELLO 2022-2024 VS MODELLO 2024-2026



L'obiettivo è quello di sottolineare l'importanza di indirizzamento delle sfide legate sia al funzionamento del sistema informativo, sia al funzionamento del sistema organizzazione degli enti.

L'aggiornamento 2025 del piano triennale come la versione 2024-2026 è organizzato 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**. Include quindi obiettivi e strategie per il miglioramento della gestione del cambiamento, il procurement digitale e l'organizzazione dei processi.

Parte seconda – Componenti tecnologiche: 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 così come il capitolo "Dati" è integrato da una sezione nuova dedicata all'intelligenza artificiale.

Parte terza – 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. Offre strumenti pratici per supportare la trasformazione digitale, tra cui vademecum, linee guida e check-list operative. Questo aggiornamento mantiene una visione di lungo periodo, allineata con gli obiettivi del decennio digitale 2030 dell'unione europea, e punta a creare una pa più moderna, efficiente e sostenibile.

Al fine di fornire informazioni e riferimenti operativi di supporto alle amministrazioni destinatarie del Piano è stato inserito un paragrafo alla fine di ciascun capitolo concernente le **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

Da sempre la strategia del Piano Triennale per l'informatica nella Pubblica è quella fondamentale di promuovere la trasformazione digitale del Paese attraverso la trasformazione della Pubblica Amministrazione italiana attraverso i principi guida³ rilevabili in maniera esplicita fin dal 2022:

Digital & Mobile First (digitale e mobile come prima opzione): le pubbliche amministrazioni devono realizzare servizi primariamente digitali;

Digital Identity Only (accesso esclusivo mediante identità digitale): le PA devono adottare in via esclusiva sistemi di identità digitale definiti dalla normativa assicurando almeno l'accesso tramite SPID;

Cloud First (cloud come prima opzione): le pubbliche amministrazioni, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano primariamente il paradigma cloud, tenendo conto della necessità di prevenire il rischio di lock-in;

Servizi Inclusivi E Accessibili: le pubbliche amministrazioni devono progettare servizi pubblici digitali che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori;

³ piano_triennale_per_linformatica_nella_pa_2022-2024



Dati Pubblici Un Bene Comune: 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;

Interoperabile By Design: i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e senza interruzioni in tutto il mercato unico esponendo le opportune API;

Sicurezza E Privacy By Design: i servizi digitali devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali;

User-Centric, Data Driven E Agile: le amministrazioni sviluppano i servizi digitali, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo.

Once Only: le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite;

Transfrontaliero By Design (concepito come transfrontaliero): le pubbliche amministrazioni devono rendere disponibili a livello transfrontaliero i servizi pubblici digitali rilevanti;

Codice Aperto: le pubbliche amministrazioni devono prediligere l'utilizzo di software con codice aperto e, nel caso di software sviluppato per loro conto, deve essere reso disponibile il codice sorgente.

L'Aggiornamento 2026 introduce cinque novità sostanziali di contenuto rispetto al 2025:

1. AgID Academy

Avvio delle attività legate alla realizzazione dell'AgID Academy, struttura di formazione per il personale pubblico su trasformazione digitale, governance ICT e sicurezza.

2. IT-WALLET⁴.

Inserimento e consolidamento dell'IT-Wallet tra le piattaforme nazionali abilitanti, in sinergia con SPID e CIE, per l'erogazione di servizi digitali a cittadini e imprese.

3. Intelligenza Artificiale nella PA

Aggiornamento delle linee di azione sull'uso dell'AI nella gestione dei procedimenti e nei servizi pubblici, con focus su analisi del rischio, uso responsabile e formazione specifica del personale.

4. Cloud e infrastrutture digitali

Revisione dei contenuti in coerenza con la normativa aggiornata e con le indicazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN), per rafforzare la sicurezza dei dati e la sovranità digitale.

⁴ Il Sistema di Portafoglio digitale italiano (Sistema IT-Wallet) è l'ecosistema di soluzioni pubbliche e private che permettono a tutti i cittadini di disporre e gestire in maniera efficace della propria identità digitale e dei propri documenti e attestazioni, attraverso applicazioni mobile. Ha l'obiettivo di rendere più semplice, accessibile, sicuro e trasparente il processo di presentazione dei propri dati e l'accesso ai servizi erogati da pubbliche amministrazioni e soggetti privati, sia nel mondo fisico che in quello digitale, mettendo al centro il cittadino secondo i principi di self-sovereignty, once-only e data minimization. Il Sistema IT-Wallet si colloca nel più ampio contesto europeo dell'European Digital Identity Framework, un insieme di regole contenute all'interno del Regolamento (UE) n. 2024/1183 (c.d. "eIDAS 2")



5. Nuovi strumenti operativi

Inserimento di sei nuove schede operative nella Parte Terza – Strumenti, portando il totale a 22 strumenti (erano 16 nel 2025).

I nuovi strumenti riguardano temi come gestione associata ICT, modelli organizzativi tipo per Uffici Transizione Digitale, strategie nei PIAO, e intelligenza artificiale nella PA



OBIETTIVI PREFISSATI DA AGID

Per quanto riguarda i risultati attesi a livello nazionale si rimanda alla lettura del Piano AgID; per gli obiettivi sono così riassumibili suddivisi per Capitoli del Piano AgID

CAP1- Organizzazione gestione del cambiamento

Obiettivo 1.1

Migliorare i processi di trasformazione digitale della PA

Obiettivo 1.2

Diffusione competenze digitali nel Paese e nella PA

Obiettivo 1.3

Monitorare e analizzare lo stato di digitalizzazione del paese

CAP2 - Il procurement per la trasformazione digitale

Obiettivo 2.1

Rafforzare l'ecosistema nazionale di approvvigionamento digitale

Obiettivo 2.2

Diffondere l'utilizzo degli appalti innovativi

Obiettivo 2.3

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

CAP3 - Servizi

Obiettivo 3.1

Migliorare la capacità di erogare e-service

Obiettivo 3.2

Migliorare la capacità di generare ed erogare servizi digitali

Obiettivo 3.3

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

Obiettivo 3.4

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

CAP4 - Piattaforme

Obiettivo 4.1

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

Obiettivo 4.2

Ottenere la piena interoperabilità tra le piattaforme

Obiettivo 4.3

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

CAP5 - 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

Obiettivo 5.2

Aumentare la qualità dei dati e dei metadati

Obiettivo 5.3



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

Obiettivo 5.4

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

Obiettivo 5.5

Dati per l'intelligenza artificiale

CAP6 - 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)

Obiettivo 6.2

Garantire alle amministrazioni la disponibilità della connettività SPC

CAP7 - Sicurezza informatica

Obiettivo 7.1

Adottare una governance della cybersicurezza diffusa nella PA

Obiettivo 7.2

Gestire i processi di approvvigionamento IT coerentemente con i requisiti di sicurezza definiti

Obiettivo 7.3

Gestione e mitigazione del rischio cyber

Obiettivo 7.4

Potenziare le modalità di prevenzione e gestione degli incidenti informatici

Obiettivo 7.5

Implementare attività strutturate di sensibilizzazione cyber del personale

Obiettivo 7.6

Contrastare il rischio cyber attraverso attività di supporto proattivo alla PA



STATO ATTUALE DELL'ENTE

Il Comune di Castelfranco Piandiscò si presenta a metà del 2026 come un modello di eccellenza per le amministrazioni locali di medio-piccole dimensioni.

Il Comune intende consolidare il proprio livello di maturità digitale, promuovendo un modello amministrativo innovativo, inclusivo e sostenibile, orientato alla qualità dei servizi, alla trasparenza e all'accessibilità. Il programma definito dal Servizio RTD individua obiettivi concreti e progressivi nei principali ambiti di sviluppo: competenze digitali, infrastrutture sicure e sostenibili, digitalizzazione dei servizi e supporto alla trasformazione del tessuto economico locale.

Il Piano delinea un obiettivo strategico di lungo periodo e prevede un'attuazione graduale delle misure, calibrata in funzione delle priorità operative, delle risorse disponibili e della capacità organizzativa dell'Ente, secondo un approccio flessibile e orientato ai risultati.

L'Ente ha completato con successo la transizione infrastrutturale ed è ora pronto per affrontare le sfide di seconda generazione del Piano Triennale AgID (consolidamento dei dati, monitoraggio avanzato dei KPI di adozione e approccio pionieristico all'Intelligenza Artificiale).

I prossimi passi strategici e operativi per l'Ente in linea con il Piano Triennale AgID 2024-2026 si articolerebbero su diverse macro-aree di consolidamento, sicurezza e innovazione:

1. Interoperabilità e Valorizzazione dei Dati (PDND e Open Data)

- Piena operatività sulla PDND: Dopo l'attivazione dei primi e-service sulla Piattaforma Digitale Nazionale Dati, l'Ente deve proseguire nello scambio e nell'integrazione di dati in tempo reale tramite API certificate con le altre amministrazioni (es. per l'allineamento dei flussi demografici e fiscali), applicando in modo rigoroso il principio del Once-Only (evitare di chiedere al cittadino dati già in possesso della PA).
- Adeguamento Open Data e Metadati: È programmato l'adeguamento dei metadati sia per i dati geografici (da documentare nel catalogo geodati.gov.it) sia per i dati non geografici (su dati.gov.it), allineandoli alle più recenti specifiche nazionali. Questo processo avverrà in sinergia con i partner tecnologici e i sistemi gestionali in uso (es. l'ecosistema Sicraweb EVO).

2. Sicurezza Informatica e Resilienza (Cybersecurity)

- Adempimenti NIS2 e Monitoraggio Proattivo: Il passo successivo prevede l'innalzamento della postura di sicurezza dell'Ente tramite l'adozione di politiche di Identity Access Management (IAM) avanzate, la crittografia dei flussi documentali e il monitoraggio degli endpoint attraverso soluzioni evolute collegate a cruscotti di controllo
- Gestione del Rischio e Cooperazione con il CERT-AGID: L'Ente prevede di usufruire in modo continuativo degli strumenti per la gestione e la mitigazione dei rischi cyber messi a disposizione dalle strutture centrali (come l'Agenzia per la Cybersicurezza Nazionale e il CERT-AGID) per contrastare proattivamente le minacce informatiche.

3. Servizi ai Cittadini, Accessibilità e Piattaforme Nazionali

- Consolidamento e Monitoraggio KPI (App IO e Sito Web): Con oltre 30 servizi già integrati su App IO e un sito web istituzionale completamente aggiornato secondo i modelli Design Italia, l'obiettivo a regime è il monitoraggio costante dell'adozione da parte della cittadinanza



- Piattaforma Notifiche Digitali (SEND): Estensione dell'uso e della digitalizzazione integrale delle notifiche a valore legale tramite la piattaforma SEND per l'invio automatizzato di sanzioni amministrative, violazioni e atti tributari, riducendo drasticamente i costi e i tempi di spedizione cartacea.
- Dichiarazioni e Obiettivi di Accessibilità: Monitoraggio e aggiornamento periodico, esclusivamente tramite l'applicazione ministeriale dedicata, delle dichiarazioni di accessibilità per il portale web e le applicazioni mobili dell'Ente, con pubblicazione annuale degli obiettivi di miglioramento per l'inclusività informatica.

4. Competenze Digitali, Formazione e Intelligenza Artificiale

- Piano di Formazione su Piattaforma Syllabus: Per sostenere lo sviluppo del capitale umano (target PNRR), l'Ente ha formalizzato l'adesione all'iniziativa nazionale "Syllabus per la formazione digitale". I prossimi passi prevedono il coinvolgimento strutturato e obbligatorio dei dipendenti in corsi di formazione focalizzati sulle competenze digitali di base, sulla sicurezza informatica (cyber-hygiene) e sull'uso corretto e sicuro delle piattaforme cloud.
- Consapevolezza e Sperimentazione sull'Intelligenza Artificiale (AI): In coerenza con i nuovi obiettivi del Piano Triennale (Obiettivo 5.4), l'Ente inizierà a valutare e monitorare l'introduzione di tecnologie basate sull'Intelligenza Artificiale per l'ottimizzazione dell'azione amministrativa e l'analisi dei dati, partecipando a iniziative di sensibilizzazione nazionali per un uso etico e conforme.

5. Governance e Transizione Organizzativa

- Consolidamento dell'Ufficio RTD (anche in forma associata): Tra le attività da monitorare ed eventualmente implementare, vi è la partecipazione a tavoli di confronto e laboratori territoriali (es. tramite le reti digitali regionali/locali) per sperimentare modelli organizzativi avanzati per il Responsabile della Transizione Digitale (RTD) e l'Ufficio per la Transizione Digitale (UTD), valutando sinergie e scambi di buone pratiche anche con altre realtà locali dell'Unione dei Comuni.

L'ente attende così il piano Agid del prossimo Triennio per indirizzare al meglio le attività come fatto in passato.



SINTESI DEL PIANO E CRONO PROGRAMMA

La presente sezione costituisce un estratto del file in atti, in formato xls (*Allegato – PIANO_TRIENNALE_24_26_aggiornamento_2026.xls*) e contiene, in formato tabellare, l'elenco delle azioni e delle attività da intraprendere nel periodo di validità del presente piano corredate da una previsione temporale circa la loro esecuzione.

Le azioni compaiono nella tabella in ordine cronologico per priorità.

La “Descrizione” contiene una descrizione delle attività da svolgere e si riferisce ad una o più descrizioni delle attività che compare nelle tabelle sopracitate.

Il riferimento indica la funzione a cui è indirizzata l'attività

Sono riportate le attività prioritarie estrapolate dal cronoprogramma generale valido fino al 2026 a disposizione dell'Ente

Priorità 1: attività in corso

Priorità 2: attività da iniziare

Priorità 3: attività da chiudere nel 2026

Nel Piano Triennale AGID 2024–2026, quando per una linea di azione o per una attività viene indicata una data di inizio, questo ha un significato tecnico molto preciso e NON è una scadenza generica.

Rappresenta il momento in cui l'Ente deve dimostrare di aver intrapreso concretamente qualcosa e diventa obbligatorio aprire il relativo ciclo di attuazione nel proprio Piano Triennale.

Quando nel Piano Triennale AGID è indicata una data di inizio, significa che entro quella data il Comune deve aver avviato formalmente l'attività, con evidenze documentali, inserendola nel proprio Piano Triennale e iniziando il monitoraggio del relativo avanzamento.



**PRIORITA' 1:
ATTIVITA IN CORSO**

Cod.	Rif. Temp. da PT	OBIETTIVO	STATO	Descrizione	STATO AVANZAMENTO LAVORI ENTE
CAP1.PA.01	da marzo 2024	COMMUNIT Y	OPZIONALE DA VALUTARE	Le Amministrazioni e gli Enti interessati possono proporre ad AGID l'attivazione di una comunità digitale tematica/territoriale su retedigitale.gov.it	I tavoli di incontro risultano fondamentali per raggiungere l'obiettivo di supportare i processi di trasformazione digitale nelle Amministrazioni locali e non solo. L'Ente incentiva l'approccio proattivo nel condividere dati, esperienze, proposte.
CAP2.PA.02	entro giugno 2025	ACQUISTI e PIANIFICAZI ONE FABBISOGN I DI INNOVAZIO NE	DA MONITORARE	Le stazioni appaltanti devono digitalizzare la fase di esecuzione dell'appalto	Va notato che, con il nuovo Codice dei Contratti (D.Lgs. 36/2023), a partire da gennaio 2024 è previsto che le stazioni appaltanti digitalizzino l'intero ciclo di vita dei contratti (inclusa la fase di esecuzione) attraverso piattaforme di approvvigionamento digitale. il Comune svolge funzioni di stazione appaltante. Utilizza una piattaforma telematica. La fase di gara (affidamento) è digitalizzata, con caricamento di atti, interscambio elettronico, uso di piattaforme telematiche. il livello di digitalizzazione della fase di esecuzione dell'appalto (controllo tecnico, contabilità durante l'esecuzione, varianti, rapporti digitali con l'operatore economico, rendicontazione, atti di collaudo) è migliorabile e sempre in itinere.



CAP5.PA.03	Da gennaio 2021	FORMAZIONE	ATTIVITA CONTINUATIVE	Le PA partecipano, in funzione delle proprie necessità, a interventi di formazione e sensibilizzazione sulle politiche open data	si procede in tal senso
CAP7.PA.17	Da giugno 2024	FORMAZIONE	ATTIVITA CONTINUATIVE	Le PA promuovono l'accesso e l'utilizzo di attività strutturate di sensibilizzazione e formazione in ambito cybersicurezza	si procede verso attività strutturate di sensibilizzazione e formazione in ambito cybersicurezza
CAP7.PA.22	entro dicembre 2025	FORMAZIONE	ATTIVITA CONTINUATIVE	Le PA, sulla base delle proprie esigenze, partecipano ai corsi di formazione base ed avanzato erogati dal CERT-AGID	L'Ente è già iscritto a Syllabus si procederà con la valutazione del piano delle competenze e target raggiunti per poi procedere con i corsi erogati dal CERT-AGID



PRIORITA' 2:

ATTIVITA' DA INIZIARE

Cod.	Rif. Temp. da PT	OBIETTIVO	STATO	Descrizione	STATO AVANZAMENTO LAVORI ENTE
CAP1.PA.12	da settem bre 2025	MONITORAG GIO	DA FINALIZZA RE	Gli Enti locali partecipano alla seconda fase della raccolta dati, garantendo l'accuratezza e la completezza delle informazioni (RA1.3.2 - Acquisizione ed elaborazione di informazioni analitiche da Enti locali; RA1.3.3 - Aumento delle tipologie e delle fonti dati integrate all'interno dell'Osservatorio)	Nel contesto della raccolta dati menzionata si riferisce tipicamente ai dati utilizzati per supportare le attività di monitoraggio, analisi e pianificazione nell'ambito della trasformazione digitale e dei servizi pubblici. Scopi della raccolta dati: - Migliorare la comprensione delle necessità territoriali. - Analizzare lo stato attuale dei servizi pubblici per individuare aree di miglioramento. - Favorire la condivisione di buone pratiche tra enti locali. - Ampliamento delle fonti di dati per una visione più completa e multidimensionale. - Integrazione di dati provenienti da diverse tipologie di enti locali, settori, e strumenti tecnologici. Ecco una panoramica dei dati coinvolti e del loro contesto: <u>Dati amministrativi e gestionali:</u> Informazioni relative ai servizi offerti dagli enti locali (es. servizi online, modalità di accesso, qualità). Informazioni sulle infrastrutture tecnologiche utilizzate (es. reti, piattaforme, sistemi informativi).



					<u>Dati analitici e statistici:</u> Indicatori relativi all'efficienza e all'efficacia dei servizi pubblici. Statistiche d'uso dei servizi digitali (es. numero di utenti, tempo medio di risposta). Analisi sui fabbisogni territoriali o settoriali. <u>Dati socio-economici:</u> Dati relativi alla popolazione servita, con informazioni demografiche e geografiche. Informazioni sull'impatto sociale ed economico della digitalizzazione a livello locale. <u>Dati relativi a normative e compliance:</u> Stato di adozione delle linee guida AgID e altre normative relative alla digitalizzazione. Rispetto degli standard di interoperabilità e sicurezza.
CAP5.PA.21	da dicembre 2025	A.I.	DA INIZIARE	Le PA adottano le Linee per promuovere l'adozione dell'IA nella Pubblica Amministrazione	È possibile consultare il documento completo e partecipare alla consultazione pubblica attraverso la piattaforma Forum Italia Le linee guida per promuovere l'adozione dell'Intelligenza Artificiale (IA) nella Pubblica Amministrazione (PA) sono attualmente in fase di consultazione pubblica fino al 20 marzo 2025. Queste linee guida, adottate dall'Agenzia per l'Italia Digitale (AgID) con la Determinazione n. 17/2025, mirano a fornire un quadro chiaro su come integrare le tecnologie IA nel settore pubblico, garantendo conformità normativa, trasparenza, sicurezza ed etica. Il documento si articola in principi chiave e



					raccomandazioni che mirano a garantire un quadro normativo chiaro e trasparente per l'utilizzo dell'IA e assicurare che i sistemi di IA siano accurati, affidabili e sicuri. I punti principali si basano su: promuovere un'IA che rispetti i diritti fondamentali e non discrimini oltre a incentivare l'uso dell'IA per migliorare i servizi pubblici e promuovere la sostenibilità.
CAP5.PA.22	da dicembre 2025	A.I.	DA INIZIARE	Le PA adottano le Linee guida per il procurement di IA nella Pubblica Amministrazione	Nei bandi gara IT si dovrà far riferimento alle Linee Guida AGID. Sarà sufficiente raccogliere le Linee Guida AgID ed eventualmente preparare una circolare/linea guida e/o aggiornare le procedure con le ultime normative.
CAP5.PA.23	da dicembre 2025	A.I.	DA INIZIARE	Le PA adottano le Linee guida per lo sviluppo di applicazioni di IA nella Pubblica Amministrazione	È possibile consultare il documento completo e partecipare alla consultazione pubblica attraverso la piattaforma Forum Italia Le linee guida per promuovere l'adozione dell'Intelligenza Artificiale (IA) nella Pubblica Amministrazione (PA) sono attualmente in fase di consultazione pubblica fino al 20 marzo 2025. Queste linee guida, adottate dall'Agenzia per l'Italia Digitale (AgID) con la Determinazione n. 17/2025, mirano a fornire un quadro chiaro su come integrare le tecnologie IA nel settore pubblico, garantendo conformità normativa, trasparenza, sicurezza ed etica. Il documento si articola in principi chiave e raccomandazioni che mirano a garantire un quadro normativo chiaro e trasparente per



					l'utilizzo dell'IA e assicurare che i sistemi di IA siano accurati, affidabili e sicuri. I punti principali si basano su: promuovere un'IA che rispetti i diritti fondamentali e non discrimini oltre a incentivare l'uso dell'IA per migliorare i servizi pubblici e promuovere la sostenibilità.
CAP6.PA.11	da marzo 2026	CLOUD	OPZIONAL E DA VALUTARE	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	https://www.consip.it/bandi/gara-spc-connettivita Per connettività “fisica” si intende l'infrastruttura che consente il collegamento tangibile tra i sistemi. Mentre la connettività “logica” si riferisce alle applicazioni che permettono e ottimizzano lo scambio di informazioni tra i sistemi. Il Sistema pubblico di connettività (Spc) è l'infrastruttura telematica che collega le pubbliche amministrazioni offrendo servizi di trasporto dati, interoperabilità e cooperazione applicativa. Servizi di Connettività nell'ambito del Sistema Pubblico di Connettività (SPC) In questa categoria rientrano tutti i servizi mirati a soddisfare le esigenze di connettività e interconnessione delle amministrazioni, centrali e locali, che aderiscono all'SPC.
CAP7.PA.01	da settembre 2024	SICUREZZA	IN CORSO	Le singole PA definiscono il modello unitario, assicurando un coordinamento centralizzato a livello dell'istituzione, di governance della cybersicurezza	data la dimensione dell'ente, i risultati attesi saranno in linea con specifici interventi realizzati dall'Ente con l'obiettivo di allinearsi a modelli di gestione centralizzati della cybersicurezza e definire processi di gestione e mitigazione del rischio cyber



CAP7.PA.02	da dicem bre 2024	SICUREZZA	IN CORSO	Le PA adottano un modello di governance della cybersicurezza	data la dimensione dell'ente si valuterà la definizione di un modello di governance della cybersicurezza
CAP7.PA.03	da dicem bre 2024	SICUREZZA	IN CORSO	Le PA nominano i Responsabili della cybersicurezza e delle loro strutture organizzative di supporto	data la dimensione dell'ente si valuterà la definizione di un modello di governance della cybersicurezza
CAP7.PA.04	da dicem bre 2024	SICUREZZA	IN CORSO	Le PA formalizzano i processi e le procedure inerenti alla gestione della cybersicurezza	data la dimensione dell'ente si valuterà la definizione di un modello di governance della cybersicurezza con eventuale formalizzazione di processi e le procedure
CAP7.PA.05	Da giugno 2024	SICUREZZA	IN CORSO	Le PA definiscono e approvano i requisiti di sicurezza relativi al processo di approvvigionamento IT	Il processo di approvvigionamento sarà definito anche in termini di requisiti di sicurezza
CAP7.PA.06	Da dicem bre 2024	SICUREZZA	IN CORSO	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	Il processo di approvvigionamento sarà definito anche in termini di requisiti di sicurezza per le terze parti
CAP7.PA.07	Da dicem bre 2025	SICUREZZA	IN CORSO	Le PA realizzano le attività di controllo definite nel Piano di audit e verifica verso i fornitori e terze parti IT	necessario impostare un processo di audit molto semplice dato le dimensioni dell'ente
CAP7.PA.08	Da dicem bre 2024	SICUREZZA	IN CORSO	Le PA definiscono e formalizzano il processo di cyber risk management e security by design,	data la dimensione dell'ente si valuterà la definizione di un modello di governance della cybersicurezza e la formalizzazione del processo di cyber risk management e security



				coerentemente con gli strumenti messi a disposizione da ACN	by design, coerentemente con gli strumenti messi a disposizione
CAP7.PA.10	entro Dicembre 2025	SICUREZZA	IN CORSO	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	si adeguerà la privacy
CAP7.PA.12	da dicembre 2025	SICUREZZA	IN CORSO	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	data la dimensione dell'ente si valuterà la definizione di un modello di governance della cybersicurezza con eventuale formalizzazione di processi e le procedure
CAP7.PA.13	Da giugno 2024	SICUREZZA	IN CORSO	Le PA definiscono i presidi per la gestione degli eventi di sicurezza, formalizzandone i processi e le procedure	data la dimensione dell'ente si valuterà la definizione di un modello di governance della cybersicurezza con eventuale formalizzazione di processi e le procedure
CAP7.PA.14	Da dicembre 2024	SICUREZZA	IN CORSO	Le PA formalizzano ruoli, responsabilità e processi, nonché le capacità tecnologiche a supporto della prevenzione e gestione degli incidenti informatici	data la dimensione dell'ente si valuterà la definizione di un modello di governance della cybersicurezza con eventuale formalizzazione di processi e le procedure
CAP7.PA.15	Da dicembre 2024	SICUREZZA	IN CORSO	Le PA definiscono le modalità di verifica dei Piani di risposta a seguito di incidenti informatici	data la dimensione dell'ente si valuterà la definizione di un modello di governance della cybersicurezza con eventuale formalizzazione di processi e le procedure



CAP7.PA.16	Da dicem bre 2025	SICUREZZA	IN CORSO	Le PA definiscono le modalità di aggiornamento dei Piani di risposta e ripristino a seguito dell'accadimento di incidenti informatici	Il piano di Business continuity e disaster recovery sarà definito
CAP7.PA.18	Da dicem bre 2024	SICUREZZA	IN CORSO	Le PA definiscono piani di formazione inerenti alla cybersecurity, diversificati per ruoli, posizioni organizzative e attività delle risorse dell'organizzazione	data la dimensione dell'ente, i risultati attesi saranno in linea con specifici interventi realizzati dall'Ente con l'obiettivo di allinearsi a modelli di gestione centralizzati della cybersicurezza e definire processi di gestione e mitigazione del rischio cyber
CAP7.PA.19	Da dicem bre 2025	FORMAZIONE	ATTIVITA CONTINUE	Le PA realizzano iniziative per verificare e migliorare la consapevolezza del proprio personale	L'Ente ha già provveduto all'iscrizione; si valuteranno iniziative per migliorare la consapevolezza in base alle competenze
CAP7.PA.20	Da febbraio 2024 Da dicem bre 2024	SICUREZZA	IN CORSO	Le PA dovranno dotarsi degli strumenti idonei all'acquisizione degli IoC ed accreditarsi al CERT-AGID	Il Comune valuterà se dotarsi degli strumenti necessari per l'acquisizione degli Indicatori di Compromissione (IoC) e ad accreditarsi presso il CERT-AGID. Il CERT-AGID offre gratuitamente alle PA un flusso di IoC per proteggere le proprie infrastrutture da minacce come malware e phishing. Per accedere a questo servizio, è necessario compilare il modulo di accreditamento disponibile sul sito del CERT-AGID e inviarlo all'indirizzo e-mail indicato. Una volta accreditato, il Comune potrà integrare il flusso IoC nei propri sistemi di sicurezza informatica, migliorando la capacità di individuare e mitigare le minacce cibernetiche. Il CERT-AGID fornisce supporto



					tecnico per l'integrazione del feed IoC nei sistemi delle PA, offrendo indicazioni su come configurare i firewall e altri strumenti di sicurezza per utilizzare efficacemente gli indicatori forniti.
CAP7.PA.21	Da ottobre 2024 Da dicembre 2024	SICUREZZA	DA AGGIORNARE	Le PA dovranno usufruire degli strumenti per la gestione dei rischi cyber messi a disposizione dal CERT-AGID	si procederà in tal senso utilizzando gli strumenti per la gestione dei rischi cyber messi a disposizione dal CERT-AGID
CAP1.PA.14	da ottobre 2025	COMMUNITY	OPZIONALE DA VALUTARE	RTD e il personale degli UTD delle PA possono partecipare alle attività di rafforzamento delle competenze e scambio sul tema AI proposte da AgID	I tavoli di incontro risultano fondamentali per raggiungere l'obiettivo di supportare i processi di trasformazione digitale nelle Amministrazioni locali e non solo. L'Ente incentiva l'approccio proattivo nel condividere dati, esperienze, proposte. L'attivazione di una comunità digitale è anche un'opportunità di partecipazione territoriale e co-progettazione di servizi pubblici.



PRIORITA' 3

ATTIVITA' DA CHIUDERE NEL 2026

Cod.	Rif. Temp. da PT	OBIETTIVO	STATO	Descrizione	STATO AVANZAMENTO LAVORI ENTE
CAP2.PA.06	entro Settemb re 2026	ACQUISTI e PIANIFICAZION E FABBISOGNI DI INNOVAZIONE	DA PIANIFICARE	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 2027	Si procederà in tal senso
CAP3.PA.16	entro settemb re 2026	SITO WEB	DA PIANIFICARE	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	il Comune ha sviluppato il sito web istituzionale in osservanza delle prescrizioni della l. n. 4 del 2004. L'ente ha provveduto al rilascio della Dichiarazione di accessibilità relativa al sito web in uso. Procederà secondo le scadenze
CAP5.PA.24	entro dicembr e 2026	A.I.	DA PIANIFICARE	Le PA adottano le applicazioni di IA a valenza nazionale	L'ente procederà in tal senso
CAP5.PA.25	entro dicembr e 2026	A.I.	DA PIANIFICARE	Le PA adottano le basi dati nazionali strategiche	L'ente procederà in tal senso
CAP7.PA.11	entro Dicembr e 2026	SICUREZZA	IN CORSO	Le PA integrano le attività di monitoraggio del rischio cyber, come definito dal relativo Piano, nelle normali attività di progettazione, analisi,	data la dimensione dell'ente si valuterà la definizione di un modello di governance della cybersicurezza con eventuale formalizzazione di processi e le procedure



				conduzione e dismissione di applicativi e sistemi informativi	
CAP1.PA.13	da gennaio 2026	COMMUNITY	OPZIONALE DA VALUTARE	Le PA che partecipano alla community su ReTe Digitale incentrata sull'AI condividono pratiche, soluzioni e fabbisogni	I tavoli di incontro risultano fondamentali per raggiungere l'obiettivo di supportare i processi di trasformazione digitale nelle Amministrazioni locali e non solo. L'Ente incentiva l'approccio proattivo nel condividere dati, esperienze, proposte. L'attivazione di una comunità digitale è anche un'opportunità di partecipazione territoriale e co-progettazione di servizi pubblici.
CAP2.PA.08	entro giugno 2026	ACQUISTI e PIANIFICAZIONI E FABBISOGNI DI INNOVAZIONE	DA VALUTARE	Le amministrazioni entrano nel programma delle consultazioni di mercato	• Implementare indicatori di monitoraggio: % gare digitalizzate, % adesione a gare strategiche, % fornitori qualificati. • Preparare report interno annuale sull'avanzamento del procurement digitale.
CAP2.PA.09	entro giugno 2026	ACQUISTI e PIANIFICAZIONI E FABBISOGNI DI INNOVAZIONE	DA VALUTARE	Le amministrazioni che hanno avviato appalti di innovazione completano la fase di aggiudicazione e di esecuzione	• Verificare la linea nel documento ufficiale. • Se concerne innovazione negli acquisti (es. appalti innovativi, PMI/start-up), predisporre criteri interni: clausole di partecipazione PMI, appalti pre-commerciali, criteri sostenibili/green.
CAP5.PA.26	da gennaio 2026	A.I.	DA INIZIARE	Le PA documentano i propri dati rientranti nelle categorie di cui all'art. 3 del Regolamento (UE)	• Verificare la linea nel documento ufficiale.



				2022/868 (DGA) nello sportello unico reso disponibile da AgID	
CAP5.PA.27	da luglio 2026	A.I.	DA INIZIARE	Le PA trasmettono periodicamente all'AgID i dati fondamentali delle iniziative nell'ambito delle tecnologie di IA	• Se concerne innovazione negli acquisti (es. appalti innovativi, PMI/start-up), predisporre criteri interni: clausole di partecipazione PMI, appalti pre-commerciali, criteri sostenibili/green.