Piano Triennale per la transizione digitale 2024-2026

del Consorzio Boschi Carnici

Riferimento al Piano Triennale per l'informatica nella Pubblica Amministrazione 2024-2026

Tolmezzo, 28/10/2024

Sommario

INTRODUZIONE

Premessa

Il Consorzio Boschi Carnici è un consorzio di Comuni che gestisce una vasta proprietà silvo-pastorale distribuita entro 18 Comuni della Carnia. L'attività di gestione è regolata dal Piano di Gestione forestale (PGF), valido per il periodo 2012-2023, che suddivide la proprietà in 77 particelle forestali a vocazione produttiva, protettiva o attualmente lasciate alla libera evoluzione. Negli ultimi decenni grazie a una politica di ampliamento della sua proprietà e successive acquisizioni di boschi, proprietà abbandonate, malghe e pascoli si è passati dai 1.670 ettari iniziali agli attuali 3.000 ettari complessivi. Non tutta la superficie è interessata da foreste produttive, ma sono presenti anche boschi di protezione, ad evoluzione naturale e a gestione speciale. Parallelamente si è dotato di personale tecnico e di custodia, che consente di seguire direttamente tutte le fasi di cui si compone la conduzione di una proprietà così articolata, dalla progettazione alla realizzazione degli interventi, secondo i moderni principi della gestione ambientale multifunzionale e garantendo così un'elevata qualità dei processi.

L'Ente è organizzato nelle seguenti aree:

1. Area amministrativa
2. Area contabile
3. Area tecnica

Negli ultimi anni l'ente ha provveduto ad intraprendere diverse azioni per avviare e sostenere il proprio processo di digitalizzazione:

- migrazione su Cloud regionale dei dati dell'Ente;
- implementazione del parco macchine (workstation fisse) dei dipendenti attraverso la sostituzione dei dispositivi obsoleti;
- adesione al sistema PagoPA, anche grazie all'impiego di risorse provenienti da finanziamenti del Fondo Innovazione;

Contesto Strategico

Il contesto strategico del Piano Triennale per l'informatica nella Pubblica amministrazione, e nello specifico il Piano Triennale per l'informatica del Consorzio, è costituito da una serie di fattori che hanno contribuito a definire gli obiettivi e le linee di azione del Piano stesso.

Tra i fattori più rilevanti si possono annoverare:

1. La trasformazione digitale in atto a livello globale, che sta cambiando radicalmente il modo in cui le persone interagiscono con il mondo che le circonda, anche in ambito pubblico.
2. La necessità di migliorare l'efficienza e l'efficacia della Pubblica Amministrazione, anche al fine di ridurre i costi e migliorare la qualità dei servizi offerti ai cittadini e alle imprese.
3. La necessità di garantire la sicurezza e la resilienza dei sistemi informatici della Pubblica Amministrazione, in un contesto di crescenti cyber-minacce.

In base a questi fattori, il Piano Triennale per l'informatica nella Pubblica amministrazione si pone come obiettivo generale quello di "rendere la Pubblica Amministrazione italiana più efficiente, efficace, accessibile e sicura, attraverso l'utilizzo delle tecnologie digitali".

Per raggiungere questo obiettivo, il Piano Triennale dell'Ente si concentra su quattro ambiti strategici:

1. **Semplificazione e innovazione dei servizi pubblici**: migliorare la qualità dei servizi pubblici offerti ai cittadini e alle imprese, rendendoli più semplici e accessibili.

2. **Efficienza e efficacia della Pubblica Amministrazione**: migliorare l'efficienza e l'efficacia della Pubblica Amministrazione, riducendo i costi e migliorando i processi.
3. **Sicurezza e resilienza dei sistemi informatici**: garantire la sicurezza e la resilienza dei sistemi informatici della Pubblica Amministrazione, proteggendoli dalle cyber-minacce.
4. **Valorizzazione delle competenze digitali**: valorizzare le competenze digitali dei dipendenti della Pubblica Amministrazione, attraverso la formazione e l'aggiornamento continuo.

Per implementare le linee di azione del Piano triennale per l'informatica nella pubblica amministrazione 2024-2026, l'Agenzia per l'Italia Digitale (AgID) ha definito un modello standard per la redazione dei Piani triennali delle singole amministrazioni cui il presente documento si conforma. Questo modello è finalizzato a garantire la coerenza e la sinergia tra i piani delle singole amministrazioni e il Piano Triennale nazionale.

Principi Guida

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
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.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 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

Finalità del Piano triennale

Il presente Piano Triennale per la transizione digitale, predisposto secondo il modello standard per la redazione del Piano Triennale per l'informatica da parte delle PA fornito dall'Agenzia per l'Italia Digitale (AgID) nell'apposita Guida pubblicata il 26/03/2024, in linea con il Piano Triennale per l'informatica nella Pubblica Amministrazione redatto da AgID, ha lo scopo di fornire all'Ente uno strumento di programmazione per la Transizione al Digitale e migliorare la consapevolezza sulla portata innovativa del processo di migrazione al digitale e delle disposizioni legislative contenute nel Codice dell'Amministrazione Digitale (CAD), nonché delle conseguenti linee guida e regole tecniche emanate da AgID.

La consapevolezza delle opportunità offerte dalle tecnologie per l'informazione e la comunicazione, unita agli obblighi disposti dal CAD, ha reso necessario un forte impegno dell'Amministrazione ad intraprendere un percorso di crescita culturale e di riorganizzazione sia in termini procedurali che di infrastruttura. Questo al fine di elevare il livello di digitalizzazione utile a garantire il diritto alla cittadinanza digitale, migliorare il rapporto con i propri interlocutori (cittadini, imprese e altre Pubbliche Amministrazioni) e migliorare il benessere operativo dei propri dipendenti.

Coerentemente con gli obiettivi definiti dal Legislatore e dall'Agenzia per l'Italia Digitale, e in particolare quelli del Piano Nazionale di Ripresa e Resilienza (PNRR), il presente Piano ha l'obiettivo di accelerare il processo di semplificazione amministrativa e di digitalizzazione nelle relazioni con i cittadini e le imprese. Promuove l'uso competitivo delle tecnologie dell'informazione e della comunicazione (ICT) e il miglioramento continuo dei processi interni dell'ente.

Questo Piano esprime un percorso voluto dal Consorzio, nel quale tutti i settori dell'Amministrazione, le competenze, i progetti e le risorse economiche disponibili, anche tramite specifiche linee di finanziamento, convergono per promuovere compiutamente i diritti di cittadinanza digitale, l'efficacia dell'azione amministrativa e la trasparenza dei procedimenti. Questi costituiscono l'asse fondamentale dell'azione di trasformazione digitale dell'Amministrazione.

L'adozione di soluzioni digitali consentirà all'ente di offrire servizi più accessibili e convenienti per i cittadini, migliorando complessivamente la qualità della vita all'interno della comunità. Gli obiettivi strategici da raggiungere con il Piano comprendono:

1. Modernizzazione dell'amministrazione pubblica: Promuovere l'adozione di strumenti digitali per semplificare e automatizzare i processi amministrativi, migliorando l'accessibilità e la qualità dei servizi offerti ai cittadini.
2. Digitalizzazione dei servizi: Offrire servizi pubblici online, consentendo ai cittadini di interagire con l'amministrazione in modo rapido e conveniente, riducendo la necessità di spostamenti fisici e di conseguenza generando "valore pubblico"
3. Sicurezza dei dati: Garantire la protezione dei dati sensibili dei cittadini e dell'amministrazione attraverso l'implementazione di misure di sicurezza informatica adeguate.
4. Partecipazione e trasparenza: Favorire la partecipazione dei cittadini alla vita amministrativa, fornendo strumenti per la consultazione e la condivisione di informazioni sui progetti e le decisioni dell'ente.
5. Sviluppo dell'innovazione: Promuovere la cultura dell'innovazione all'interno dell'amministrazione, incoraggiando la sperimentazione di nuove tecnologie e soluzioni digitali per migliorare i servizi offerti.

Guida alla lettura del piano

Il Piano Triennale per l'Informatica è organizzato in capitoli che contengono degli obiettivi raggiungibili attraverso delle azioni specifiche codificate chiamate "Linee d'Azione".

Per rendere più leggibile il documento, ogni unità minima codificata (linea d'azione) comprende le seguenti componenti:

- **Linea d'azione**: codice e il titolo della linea d'azione (es: CAP1.PA.01). E' un dato definito da AGID/MiD.
- **Termine adempimento**: la data ufficiale di partenza o di fine (scadenza) del progetto/attività descritta.
- **Termine predisposizione**: programmazione dell'ente rispetto alla linea d'azione specificata.
- **Stato**: stato di avanzamento della linea d'azione.
- **Descrizione**: descrizione sintetica dell'azione da compiere o della richiesta specifica indicata da AGID/MiD.
- **Dettaglio**: descrizione dell'attività programmata dall'ente per l'attuazione della linea d'azione.
- **Budget previsto:** importo stanziato o comunque preventivato dall'ente per la realizzazione dell'attività programmata.
- **Budget utilizzato:** importo impegnato al momento della redazione del piano.
- **Strutture responsabili e attori coinvolti:** Eventuali strutture interne o esterne coinvolte nel completamento della linea d'azione

PARTE PRIMA - Componenti strategiche per la trasformazione digitale

Questa sezione è articolata in due capitoli che descrivono le leve strategiche su cui investire per accelerare il processo di trasformazione digitale dell'Ente, focalizzando l'attenzione su un approccio innovativo che affronti, in maniera sistematica, gli aspetti essenziali legati a organizzazione, processi, regole, dati e tecnologie

Capitolo 1 - Organizzazione e gestione del cambiamento

L'ecosistema digitale amministrativo dell'Ente

La trasformazione digitale dell'Ente richiede la creazione di un ecosistema digitale strutturato, volto a rendere l'organizzazione più semplice, trasparente, aperta e digitalizzata, con servizi di alta qualità erogati in modo proattivo per anticipare le esigenze dei cittadini. Gli ecosistemi digitali, in questo caso, sono quindi intesi non solo come piattaforme tecnologiche, ma come un insieme integrato di processi e pratiche innovative.

È essenziale adottare un approccio sistematico che affronti tutti gli aspetti legati all'organizzazione, ai processi, alle regole, ai dati e alle tecnologie. Questo richiede strumenti per mappare tali aspetti e facilitare lo scambio di buone pratiche, promuovendo una cultura amministrativa digitale tra tutti i dipendenti di questo Ente e tra questo Ente e gli Enti per i quali svolge, a diverso titolo, funzioni o servizi.

Con l'introduzione del Piano Integrato di Attività e Organizzazione (PIAO) previsto dall'art. 6 del Decreto-legge n. 80/2021, l'Ente s'impegna a migliorare la qualità e la trasparenza dell'attività amministrativa, semplificando e reingegnerizzando continuamente i processi.

Poiché l'azione amministrativa, vista sotto questo aspetto, può essere considerata un processo collettivo, si rende necessario potenziare e introdurre nuovi strumenti di collaborazione digitale basati su e-service e API che permettano lo scambio automatico e interoperabile di dati e informazioni. Questo, oltre a facilitare il principio once-only, consentirà di generare un maggiore valore all'interno dell'amministrazione locale contribuendo ad accrescere i livelli di correttezza, trasparenza, sicurezza informatica e protezione dei dati personali.

L'Ente punta quindi all'evoluzione da una visione di "Piattaforma per Governo" a quella di "Governo come Piattaforma", come descritto nella Comunicazione EU (2021)118 sulla Bussola Digitale 2030.

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

Quella del Responsabile per la transizione al digitale (RTD) è una figura prevista dal Codice dell'Amministrazione Digitale (decreto legislativo 7 marzo 2005, n. 82) all'interno dell'amministrazione con il ruolo di guidare la PA nella quale opera a rispondere ai cambiamenti richiesti dalla digitalizzazione.

Così come esplicitato dalla circolare nr. 3 del 1 ottobre 2018 del Ministro per la Pubblica Amministrazione, il ruolo del Responsabile della Transizione al Digitale prevede il raccordo e la consultazione delle altre figure coinvolte nel processo di digitalizzazione della Pubblica Amministrazione.

Al fine di adempiere al mandato istituzionale per l'esercizio dei compiti di seguito individuati, all' RTD sono affidate le risorse economiche necessarie per raggiungere gli obiettivi del presente piano reperite in parte dai fondi europei messi a disposizione del PNRR ed in parte con risorse finanziarie proprie dell'Ente. Il RTD opererà d'intesa con il titolare e i relativi responsabili per la protezione dei dati personali, con il DPO, con

l’amministratore di rete, con il responsabile della gestione documentale e con il responsabile della conservazione.

Atteso che il Responsabile per la Transizione al Digitale ha il principale compito di impulso e coordinamento nella progettazione e coordinamento della migrazione al digitale dell’Ente, resta in capo ai rispettivi responsabili di settore il raggiungimento degli obiettivi individuati nel presente piano.

L’art 17 del CAD e la Circolare 3/2018 del Ministero della Pubblica Amministrazione, prevedono per l’RTD i compiti di:

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 mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
i) promozione delle iniziative attinenti l’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;
k) 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).

Il Responsabile per la Transizione Digitale (RTD) del Consorzio è stato individuato nel sig. Morocutti Luca, responsabile dell’Ufficio per la Transizione Digitale della Comunità di Montagna della Carnia che opera in forma associata per tutti gli enti convenzionati e che si farà carico delle attività previste per l’attuazione delle linee d’azione previste per le PA locali dall’obiettivo 1.1 *(Migliorare i processi di trasformazione digitale della PA)* del Piano triennale per l’informatica nella pubblica amministrazione 2024-2026, in particolare:

- CAP1.PA.03: Le PA partecipanti alle iniziative laboratoriali forniscono contributi e proposte di modifica e integrazione al Vademecum sulla nomina del Responsabile per la transizione al digitale e sulla costituzione dell’Ufficio per la transizione al digitale in forma associata

- CAP1.PA.04: Le PA partecipanti alle iniziative laboratoriali e che hanno adottato modelli organizzativi/operativi per l'Ufficio per la transizione al digitale condividono le esperienze, gli strumenti sviluppati e i processi implementati

Contesto normativo e strategico

Riferimenti normativi europei:

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

Obiettivo 1.2 - Diffusione competenze digitali nel Paese e nella PA

L'obiettivo di diffondere le competenze digitali punta ad aumentare il livello di alfabetizzazione digitale di cittadini e dipendenti. Questo si traduce in una serie di iniziative volte a rendere i cittadini più consapevoli e capaci nell'uso delle tecnologie digitali e a potenziare le capacità digitali del personale dell'Ente per migliorare l'efficienza dei servizi offerti. I risultati attesi dalle azioni di seguito descritte sono un miglioramento dell'inclusione digitale e della partecipazione dei cittadini ai servizi comunali, un aumento dell'efficienza e della trasparenza dell'amministrazione locale, e un generale miglioramento della qualità della vita attraverso l'uso di tecnologie smart e infrastrutture digitali avanzate.

Linea d'azione	**CAP1.PA.07 - Competenze digitali - Sensibilizzazione**
Termine adempimento	Dal 01/09/2024
Termine predisposizione	31/12/2024
Stato	In preparazione
Descrizione	Le PA, in funzione delle proprie necessità, partecipano alle iniziative pilota, alle iniziative di sensibilizzazione e a quelle di formazione di base e specialistica per il proprio personale, come previsto dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali
Dettaglio	Il PIAO dell'Ente sarà adeguato al fine di contenere indicazioni specifiche relative alla formazione del personale sul tema della transizione digitale.
Budget previsto	0,00 €
Budget utilizzato	0,00 €
Strutture responsabili e attori coinvolti	Ufficio Personale in collaborazione con l'Ufficio Informatica. Nel progetto formativo tutti gli uffici sono coinvolti

Linea d'azione	**CAP1.PA.08 - Competenze digitali - Syllabus**
Termine adempimento	Dal 01/09/2024

Termine predisposizione	31/12/2024
Stato	In preparazione
Descrizione	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.
Dettaglio	Il PIAO dell'Ente sarà adeguato al fine di contenere indicazioni specifiche relative alla formazione del personale sul tema della transizione digitale, in particolare attraverso la piattaforma Syllabus a cui l'ente ha già aderito come previsto dalla Direttiva DFP-0020099-P-23/03/2023 del Ministro per la Pubblica Amministrazione.
Budget previsto	0,00 €
Budget utilizzato	0,00 €
Strutture responsabili e attori coinvolti	Ufficio Personale coadiuvato dall'Ufficio per la transizione digitale. Nel progetto formativo tutti gli uffici sono coinvolti

Capitolo 2 - Il procurement per la trasformazione digitale

Il *procurement* per la trasformazione digitale

In un contesto in cui settori chiave come la salute, la giustizia, la protezione dei consumatori, la mobilità, il monitoraggio ambientale, l'istruzione e la cultura sono fondamentali per il benessere della comunità, la digitalizzazione dei servizi pubblici non solo semplifica le procedure, ma stimola anche la diffusione di modelli organizzativi di open innovation. Questo approccio promuove la collaborazione tra amministrazioni, cittadini e imprese, creando un ecosistema dinamico e interconnesso.

La concreta attuazione della trasformazione digitale richiede la disponibilità di risorse professionali e strumentali, sia interne che esterne all'amministrazione, e un'efficace gestione degli acquisti pubblici. La recente riforma del procurement pubblico, introdotta dal Codice dei Contratti Pubblici, rappresenta un passo significativo verso la digitalizzazione del ciclo di vita dei contratti.

Questo Ente è per tanto pienamente consapevole dell'importanza cruciale della digitalizzazione degli appalti pubblici come parte integrante del processo di trasformazione digitale. Questo percorso non solo migliorerà l'efficienza e la trasparenza delle procedure di acquisto, ma contribuirà anche a una gestione più efficace delle risorse pubbliche. Per affrontare questa sfida, il nostro ente intende attuare una serie di iniziative strategiche, delineate come segue:

1. **Implementazione delle Normative Vigenti:** piena attuazione delle disposizioni del nuovo Codice dei Contratti Pubblici (Decreto legislativo n. 36 del 31 marzo 2023) in materia di digitalizzazione del ciclo di vita dei contratti attraverso l'adozione di una piattaforma per la gestione delle procedure di appalto, dalla pianificazione all'esecuzione, garantendo maggiore trasparenza e velocità nei processi.
2. **Formazione e Sviluppo delle Competenze:** potenziamento della formazione del personale addetto agli appalti, affinché acquisisca le competenze necessarie per utilizzare efficacemente gli strumenti digitali. Questo includerà corsi di aggiornamento su normative, tecnologie emergenti e best practice nella gestione digitale degli appalti.
3. **Utilizzo di Strumenti Digitali Avanzati:** ricorso a Convenzioni, Accordi quadro, Mercato Elettronico e Sistema Dinamico di Acquisizione, per facilitare l'acquisto di beni e servizi. Questi strumenti permetteranno di semplificare e velocizzare le procedure di acquisto, migliorando la qualità delle forniture e dei servizi.
4. **Focus su Innovazione e Intelligenza Artificiale:** nei piani di acquisto, verrà data priorità a soluzioni innovative e tecnologie data-driven, inclusi sistemi di intelligenza artificiale. Questo al fine di migliorare l'efficienza dei processi di appalto e di sperimentare nuove modalità di gestione e monitoraggio dei contratti.
5. **Sicurezza Informatica e Protezione dei Dati:** i sistemi utilizzati per la digitalizzazione degli appalti dovranno rispettare gli standard di sicurezza informatica e protezione dei dati personali, in conformità con le normative europee e nazionali in vigore.
6. **Monitoraggio e Valutazione:** dovrà essere implementato un sistema di monitoraggio continuo per valutare l'efficacia delle iniziative di digitalizzazione degli appalti promosse dall'Ente. Questo permetterà di identificare aree di miglioramento e di apportare le necessarie correzioni in tempo reale.

Attraverso queste azioni, l'Ente mira a diventare un modello di eccellenza nella gestione digitale degli appalti pubblici, migliorando la trasparenza, l'efficienza e la qualità dei servizi offerti ai cittadini. La digitalizzazione degli appalti rappresenta una componente fondamentale dell'impegno di questo Ente verso una pubblica amministrazione più moderna, efficiente e innovativa.

Contesto normativo e strategico

Riferimenti normativi italiani:

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

Riferimenti normativi europei:

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

Obiettivo 2.1 - Rafforzare l'ecosistema nazionale di approvvigionamento digitale

L'obiettivo della digitalizzazione della fase di esecuzione degli appalti è quello di automatizzare e rendere più trasparenti tutte le fasi di gestione dei contratti pubblici, dalla stipula alla conclusione. I risultati attesi dalle azioni programmate dall'Ente sono una maggiore trasparenza e tracciabilità dei processi, una riduzione dei tempi e dei costi amministrativi, e un miglioramento della qualità e dell'efficienza nella gestione degli approvvigionamenti

Linea d'azione	**CAP2.PA.02 - Digitalizzazione della fase di esecuzione degli appalti**
Termine adempimento	Dal 01/01/2024
Termine predisposizione	31/12/2024
Stato	Raggiunto
Descrizione	Le stazioni appaltanti devono digitalizzare la fase di esecuzione dell'appalto.

Dettaglio	L'Ente si avvale di piattaforme PAD come e-APPALTI FVG o MePA e assolve agli obblighi di pubblicazione previsti dalla normativa. Il CIG viene acquisito fino al 30/09/2024 anche mediante PCP per affidamenti fino a 5.000,00
Budget previsto	0,00 €
Budget utilizzato	0,00 €
Strutture responsabili e attori coinvolti	Tutti i settori

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.

Capitolo 3 – Servizi

E-service in interoperabilità tramite PDND

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

La PDND è lo strumento per gestire l'autenticazione, l'autorizzazione e la raccolta e conservazione delle informazioni relative agli accessi e alle transazioni effettuate suo tramite. La Piattaforma fornisce un insieme di regole condivise per semplificare gli accordi di interoperabilità snellendo i processi di istruttoria, riducendo oneri e procedure amministrative.

Progettazione dei servizi: accessibilità e design

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

Nell'attuale processo di trasformazione digitale dell'Ente è essenziale che i servizi abbiano un chiaro valore per l'utente; questo obiettivo richiede un approccio multidisciplinare nell'adozione di metodologie e tecniche interoperabili per la progettazione di un servizio. La qualità finale, così come il costo complessivo del servizio, non può infatti prescindere da un'attenta analisi dei molteplici layer, tecnologici e organizzativi interni, che strutturano l'intero processo della prestazione erogata, celandone la complessità sottostante. Ciò implica anche la necessità di un'adeguata semplificazione dei procedimenti e un approccio sistematico alla gestione dei processi interni, sotto il coordinamento del Responsabile per la transizione al digitale, e con il fondamentale coinvolgimento delle altre figure responsabili dell'organizzazione e del controllo strategico.

Si richiama quindi l'importanza di fornire servizi completamente digitali, servendosi delle piattaforme abilitanti descritte nel proseguo del presente documento e, nel rispetto del principio cloud first, su "Infrastrutture" qualificate. È cruciale inoltre il rispetto degli obblighi del CAD in materia di open source e accessibilità, al fine di massimizzare il riuso del software sviluppato di cui PA è titolare, riducendo i casi di sviluppo di applicativi utilizzati esclusivamente da una singola PA.

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

- il riuso e la condivisione di software e competenze tra le diverse amministrazioni;
- un utilizzo più consistente di soluzioni Software as a Service già esistenti;
- l'adozione di modelli e strumenti validati e a disposizione di tutti;

- il costante monitoraggio da parte delle PA dei propri servizi online;
- l'incremento del livello di accessibilità dei servizi erogati tramite siti web e app mobile
- lo scambio di buone pratiche tra le diverse amministrazioni, da attuarsi attraverso la definizione, la modellazione e l'organizzazione di comunità di pratica.

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

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

Nel caso il servizio richieda un accesso da parte del cittadino è necessario che sia consentito attraverso un sistema di autenticazione previsto dal CAD, assicurando l'accesso tramite l'identità digitale. Allo stesso modo, se è richiesto un pagamento, tale servizio dovrà essere reso disponibile anche attraverso il sistema di pagamento pagoPA. L'adozione di queste ultime non solo rende rapida l'implementazione dei servizi necessari, ma accelera il processo di standardizzazione nella PA.

Per il monitoraggio dei propri servizi, l'Ente utilizza Web Analytics Italia, la piattaforma nazionale open source che offre rilevazioni statistiche su indicatori utili al miglioramento continuo dell'esperienza utente.

Contesto normativo

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

Riferimenti normativi italiani:

- Decreto legislativo 30 giugno 2003, n. 196 «Codice in materia di protezione dei dati personali»
- Decreto legislativo 7 marzo 2005, n. 82 «Codice dell'amministrazione digitale» (in breve CAD), artt. 12, 15, 50, 50-ter, 73, 75
- Decreto del Presidente della Repubblica 7 settembre 2010, n. 160 «Regolamento per la semplificazione ed il riordino della disciplina sullo sportello unico per le attività produttive, ai sensi dell'articolo 38, comma 3, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133»
- Decreto-legge 14 dicembre 2018, n. 135, convertito con modificazioni dalla Legge 11 febbraio 2019, n. 12 «Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la Pubblica Amministrazione», art. 8, comma 3
- Decreto-legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 «Misure urgenti per la semplificazione e l'innovazione digitale», art. 34
- Decreto-legge 31 maggio 2021, n. 77, convertito con modificazioni dalla Legge 29 luglio 2021, n. 108 «Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure», art. 39
- Linee Guida AGID per transitare al nuovo modello di interoperabilità (2017)
- Linee Guida AGID sull'interoperabilità tecnica delle Pubbliche Amministrazioni (2021)
- Linee Guida AGID sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale per l'interoperabilità dei sistemi informativi e delle basi di dati (2021)
- Linee Guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici

- Decreto 12 novembre 2021 del Ministero dello sviluppo economico di modifica dell'allegato tecnico del decreto del Presidente della Repubblica 7 settembre 2010, n. 160
- DECRETO 22 settembre 2022 della Presidenza Del Consiglio Dei Ministri
- Piano Nazionale di Ripresa e Resilienza:
    - Investimento M1C1 1.3: «Dati e interoperabilità»
    - Investimento M1C1 2.2: «Task Force digitalizzazione, monitoraggio e performance»

Riferimenti normativi europei:

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

Obiettivo 3.1 – Migliorare la capacità di erogare e-service

L'obiettivo di migliorare la capacità di erogare e-service per l'interoperabilità dei dati è quello garantire che i vari sistemi informatici utilizzati da questo Ente possano comunicare e scambiare dati tra loro e con altre pubbliche amministrazioni in modo efficace e sicuro. I risultati attesi dalle azioni già poste in essere o in fase di programmazione, anche grazie ai finanziamenti previsti dal PNRR, sono una maggiore efficienza nella fornitura dei servizi digitali, una riduzione dei tempi di gestione delle pratiche, e una migliore esperienza per i cittadini grazie all'integrazione dei dati tra diversi enti pubblici.

Linea d'azione	**CAP3.PA.01 - Piattaforma PDND**
Termine adempimento	Dal 31/12/2024
Termine predisposizione	31/12/2024
Stato	Raggiunto
Descrizione	Le PA cessano di utilizzare modalità di interoperabilità diverse da PDND.
Dettaglio	L'Ente ha aderito alla PDND ma non ha ancora individuato i set di dati da rendere disponibili per la fruizione mediante pubblicazione di API in erogazione sulla piattaforma. Nel corso del 2024 si provvederà ad individuare i set di dati da rendere possibilmente disponibile e ad avviare eventuali attività per lo sviluppo, anche servendosi del supporto di Insiel o di altri operatori esterni, delle API di erogazione da pubblicare sulla PDND.
Budget previsto	0,00 €
Budget utilizzato	0,00 €
Strutture responsabili e attori coinvolti	Ufficio informatica e Responsabile per la transizione digitale

Linea d'azione	**CAP3.PA.02 - Migrazione dei servizi erogati in interoperabilità dalle attuali modalità alla PDND.**
Termine adempimento	30/06/2026

Termine predisposizione	31/12/2024
Stato	In preparazione
Descrizione	Le Amministrazioni iniziano la migrazione dei servizi erogati in interoperabilità dalle attuali modalità alla PDND
Dettaglio	L'Ente non ha ancora pubblicato alcun e-service di erogazione su PDND ma provvederà ad analizzare i propri flussi di dati per programmare lo sviluppo delle relative API per la condivisione su PDND
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio Informatica in accordo con il Responsabile per la Transizione Digitale

Linea d'azione	**CAP3.PA.04 - Adesione ai bandi pubblicati per finanziare l'erogazione di API su PDND**
Termine adempimento	Dal 01/01/2024
Termine predisposizione	31/12/2024
Stato	Raggiunto
Descrizione	Le PA locali rispondono ai bandi pubblicati per l'erogazione di API su PDND.
Dettaglio	L'Ente non ha aderito all'avviso per la realizzazione delle attività finanziate dalla misura 1.3.1 del PNRR, in quanto non rientrava tra gli enti beneficiari, ma monitorerà eventuali ulteriori bandi che possano rendere possibili le attività di migrazione API.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio Informatica in accordo con il Responsabile per la Transizione Digitale

Linea d'azione	**CAP3.PA.06 - Utilizzo delle API presenti sul Catalogo della PDND**
Termine adempimento	Dal 01/01/2025
Termine predisposizione	31/12/2024
Stato	In preparazione
Descrizione	Le PA utilizzano le API presenti sul Catalogo
Dettaglio	L'Ente provvederà a valutare quali servizi presenti nel Catalogo della PDND possano essere impiegati per il miglioramento delle proprie attività amministrative.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio Informatica in accordo con il Responsabile per la Transizione Digitale e con i responsabili degli uffici competenti per i servizi che verranno individuati.

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

L'obiettivo di migliorare la capacità di generare ed erogare servizi digitali è quello sviluppare e implementare soluzioni tecnologiche avanzate per offrire servizi pubblici in modo efficiente e accessibile. I risultati attesi includono un miglioramento dell'accessibilità ai servizi digitali da parte dei cittadini, una riduzione dei costi amministrativi associati alla gestione delle pratiche cartacee, e una maggiore soddisfazione dell'utenza grazie all'automazione dei processi e all'uso innovativo delle tecnologie digitali.

Linea d'azione	**CAP3.PA.09 - Pubblicazione obiettivi di accessibilità sul sito web istituzionale**
Termine adempimento	31/03/2024
Termine predisposizione	31/03/2024
Stato	Raggiunto
Descrizione	Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web.
Dettaglio	L'Ente ha pubblicato i propri obiettivi di Accessibilità per l'anno 2024 entro il termine previsto.
Budget previsto	0,00 €
Budget utilizzato	0,00 €
Strutture responsabili e attori coinvolti	Ufficio Informatica in accordo con il Responsabile per la Transizione Digitale

Linea d'azione	**CAP3.PA.11 - Trasmissione e pubblicazione del link alla dichiarazione di accessibilità**
Termine adempimento	23/09/2024
Termine predisposizione	01/09/2024
Stato	In preparazione
Descrizione	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
Dettaglio	La dichiarazione di accessibilità verrà redatta entro la scadenza prevista.
Budget previsto	0,00 €
Budget utilizzato	0,00 €
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP3.PA.12 - Attivazione di Web Analytics Italia per le statistiche di utilizzo del sito web istituzionale**
Termine adempimento	31/12/2024

Termine predisposizione	31/12/2024
Stato	In preparazione
Descrizione	Tutte le Regioni, le Province autonome, le Città metropolitane, i Comuni capoluogo delle Città metropolitane attivano Web Analytics Italia per la rilevazione delle statistiche di utilizzo del proprio sito web istituzionale presente su IndicePA.
Dettaglio	L'Ente non rientra tra quelli tenuti ad attivare tale azione, ma intende comunque aderire a WebAnalytics Italia per la rilevazione delle statistiche di utilizzo del proprio sito web istituzionale e per la pubblicazione dei risultati.
Budget previsto	0,00 €
Budget utilizzato	0,00 €
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP3.PA.13 - Pubblicazione obiettivi di accessibilità sul sito web istituzionale**
Termine adempimento	31/03/2025
Termine predisposizione	
Stato	In preparazione
Descrizione	Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web.
Dettaglio	Gli obiettivi di accessibilità per l'anno 2025 saranno pubblicati sul sito web entro il 31 marzo 2025.
Budget previsto	0,00 €
Budget utilizzato	0,00 €
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP3.PA.14 - Trasmissione e pubblicazione del link alla dichiarazione di accessibilità**
Termine adempimento	23/09/2025
Termine predisposizione	01/09/2025
Stato	In preparazione
Descrizione	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.
Dettaglio	La dichiarazione di accessibilità sarà pubblicata entro la scadenza prevista.
Budget previsto	0,00 €
Budget utilizzato	0,00 €
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP3.PA.15 - Pubblicazione obiettivi di accessibilità sul sito web istituzionale**
Termine adempimento	31/03/2026
Termine predisposizione	01/03/2026
Stato	In preparazione
Descrizione	Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web.
Dettaglio	Gli obiettivi di accessibilità per l'anno 2026 saranno pubblicati sul sito web entro la scadenza prevista
Budget previsto	0,00 €
Budget utilizzato	0,00 €
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP3.PA.16 - Trasmissione e pubblicazione del link alla dichiarazione di accessibilità**
Termine adempimento	23/09/2026
Termine predisposizione	01/09/2026
Stato	In preparazione
Descrizione	Le PA pubblicano, entro il 23 settembre, tramite l'applicazione form.AGID.gov.it, la dichiarazione di accessibilità per ciascuno dei propri siti web e APP mobili.
Dettaglio	La dichiarazione di accessibilità sarà pubblicata entro la scadenza prevista
Budget previsto	0,00 €
Budget utilizzato	0,00 €
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Formazione, gestione e conservazione dei documenti informatici

Le Linee guida sulla formazione, gestione e conservazione dei documenti informatici, emanate dall'Agenzia per l'Italia Digitale (AgID) e in vigore dal 1 gennaio 2022, costituiscono un passo cruciale per il rafforzamento e l'armonizzazione del quadro normativo in materia di gestione documentale digitale. Queste linee guida, adottate ai sensi dell'art. 71 del Codice dell'Amministrazione Digitale (CAD), mirano a semplificare e rendere più accessibile la normativa, integrandola e consolidandola in un unico documento sistematico di pratico utilizzo. Esse rappresentano una premessa fondamentale per l'azione amministrativa in ambiente digitale, in linea con gli obiettivi di semplificazione, trasparenza, partecipazione, economicità, efficacia ed efficienza già prescritti dalla Legge n. 241/1990.

Il nostro ente, già in linea con le normative vigenti, intende rafforzare ulteriormente i propri processi di gestione documentale untando alla massima applicazione delle Linee guida, assicurando così la conformità giuridica e l'ottimizzazione dei processi interni al fine di consolidare l'impegno nella trasformazione digitale e assicurare un servizio efficiente, trasparente e sicuro per i cittadini e le imprese. La corretta implementazione di tali misure contribuirà a rafforzare l'efficacia operativa dell'ente, incrementando al contempo la qualità dei servizi offerti.

Contesto normativo

Riferimenti normativi italiani:

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

Riferimenti normativi europei:

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

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

L'obiettivo di consolidare l'applicazione delle Linee guida per la formazione, gestione e conservazione documentale è garantire un'adozione uniforme e efficace delle normative riguardanti la formazione, la gestione e la conservazione dei documenti all'interno dell'amministrazione. I risultati attesi sono una migliore organizzazione e accessibilità dei documenti, una riduzione dei rischi legati alla gestione documentale, e un aumento della trasparenza e della conformità normativa nell'archiviazione e conservazione dei dati.

Linea d'azione	**CAP3.PA.17 - Manuale di gestione documentale e nomina del responsabile per la gestione documentale**
Termine adempimento	30/06/2025
Termine predisposizione	---
Stato	In preparazione
Descrizione	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

Dettaglio	L'ente non ha ancora adottato il manuale di gestione documentale per tanto prevede di procedere secondo i seguenti step: • Redazione del Manuale di Gestione Documentale: L'ente si impegna a elaborare il Manuale di Gestione Documentale, attualmente non adottato. • Definizione del titolario di classificazione: L'ente programma la definizione del titolario di classificazione, finalizzato a una migliore organizzazione documentale. • Adozione e pubblicazione: L'ente provvederà all'adozione e alla pubblicazione del Manuale di Gestione Documentale entro il termine previsto.
Budget previsto	0,00 €
Budget utilizzato	0,00 €
Strutture responsabili e attori coinvolti	Ufficio amministrativo con il supporto del Responsabile per la transizione digitale

Linea d'azione	**CAP3.PA.18 - Manuale di conservazione documentale e nomina del responsabile della conservazione**
Termine adempimento	30/06/2025
Termine predisposizione	---
Stato	In preparazione
Descrizione	Le PA devono verificare che in Amministrazione Trasparente sia pubblicato il manuale di conservazione e la nomina del responsabile della conservazione.
Dettaglio	Il piano di conservazione verrà adottato come allegato al manuale di Conservazione e successivamente pubblicato nella sezione di Amministrazione Trasparente dedicata gli atti generali.
Budget previsto	0,00 €
Budget utilizzato	0,00 €
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Capitolo 4 – Piattaforme

Le piattaforme della Pubblica Amministrazione sono piattaforme tecnologiche che offrono funzionalità fondamentali, trasversali, abilitanti e riusabili nella digitalizzazione dei processi e dei servizi della PA. Esse favoriscono la realizzazione di processi distribuiti e la standardizzazione dei flussi di dati tra amministrazioni, nonché la creazione e la fruizione di servizi digitali più semplici e omogenei.

Le principali piattaforme già attive sono SPID, pagoPA, AppIO, ANPR, CIE, FSE, NoiPA, SEND, INAD è inoltre prevista l'attivazione di nuove piattaforme quali SDG.

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

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

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

- **Piattaforma Notifiche Digitali (SEND)** che permette la notificazione e la consultazione digitale degli atti a valore legale. In particolare, la piattaforma ha l'obiettivo, per gli enti, di centralizzare la notificazione verso il cittadino o le imprese utilizzando il domicilio digitale eletto e creando un cassetto delle notifiche sempre accessibile (via mobile e via web o altri punti di accesso) con un risparmio di tempo e costi e per cittadini, imprese e PA;

- **Piattaforma Digitale Nazionale Dati (PDND)** che permette di aprire canali tra le PA e, così, farle dialogare, realizzando l'interoperabilità, attraverso l'esposizione di API. La Piattaforma concretizza il principio "once-only" e in futuro, dovrà consentire anche l'analisi dei big data prodotti dalle amministrazioni, resi disponibili nel data lake, per l'elaborazione di politiche data-driven.

- **Piattaforma Gestione Deleghe (SDG)** che consentirà ai cittadini di delegare altra persona fisica per agire presso le pubbliche amministrazioni attraverso una delega.

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

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

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

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

Contesto normativo e strategico

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

Riferimenti normativi italiani

PagoPA

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

AppIO

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

SEND

- Decreto-legge 14 dicembre 2018, n. 135, convertito con modificazioni dalla Legge 11 febbraio 2019, n. 12 «Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la Pubblica Amministrazione», art. 8.
- Legge n. 160 del 2019 «Bilancio di previsione dello Stato per l'anno finanziario 2020 e bilancio pluriennale per il triennio 2020-2022» art. 1, commi 402 e 403.
- Decreto-legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 «Misure urgenti per la semplificazione e l'innovazione digitale».

- Decreto-legge 31 maggio 2021, n. 77 «Governance del Piano nazionale di rilancio e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure», art. 38.

SPID

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

NoiPA

- Legge 27 dicembre 2006, n. 296 «Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato» (legge finanziaria 2007) art. 1, commi 446 e 447.
- Legge 23 dicembre 2009, n. 191 «Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato» (legge finanziaria 2010) art. 2, comma 197.
- Decreto-legge 6 luglio 2011, n. 98, convertito con modificazioni dalla L. 15 luglio 2011, n. 111 «Disposizioni urgenti per la stabilizzazione finanziaria».
- Legge 19 giugno 2019, n. 56 «Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo».
- Decreto del Ministro dell'Economia e delle Finanze 31 ottobre 2002 «Modifiche delle norme sull'articolazione organizzativa del Dipartimento per le politiche di sviluppo e di coesione del Ministero dell'Economia e delle Finanze».
- Decreto del Ministro dell'Economia e delle Finanze 6 luglio 2012 «Contenuti e modalità di attivazione dei servizi in materia stipendiale erogati dal Ministero dell'Economia e delle Finanze».

FSE

- Decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla Legge 17 dicembre 2012, n. 221 «Ulteriori misure urgenti per la crescita del Paese».
- Decreto del Presidente del Consiglio dei Ministri 29 settembre 2015, n. 178 «Regolamento in materia di fascicolo sanitario elettronico».
- Legge 11 dicembre 2016, n. 232 «Bilancio di previsione dello Stato per l'anno finanziario 2017 e bilancio pluriennale per il triennio 2017-2019».
- Decreto-legge 19 maggio 2020, n. 34, convertito con modificazioni dalla Legge 17 luglio 2020, n. 77 «Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché politiche sociali connesse all'emergenza epidemiologica da COVID-19».

- Decreto-legge 28 ottobre 2020, n. 137, convertito con modificazioni dalla Legge 18 dicembre 2020, n. 176 «Ulteriori misure urgenti in materia di tutela della salute, sostegno ai lavoratori e alle imprese, giustizia e sicurezza, connessi all'emergenza epidemiologica da COVID-19».
- Decreto-legge 27 gennaio 2022, n. 4, convertito con modificazioni dalla Legge 28 marzo 2022, n. 25 «Misure urgenti in materia di sostegno alle imprese e agli operatori economici, di lavoro, salute e servizi territoriali, connesse all'emergenza da COVID-19, nonché per il contenimento degli effetti degli aumenti dei prezzi nel settore elettrico».
- Decreto del Ministero dell'Economia e delle Finanze 23 dicembre 2019 «Utilizzo del Fondo per il finanziamento degli investimenti e lo sviluppo infrastrutturale - Fascicolo sanitario elettronico (Piano di digitalizzazione dei dati e documenti sanitari)».
- Decreto del Ministero della Salute 20 maggio 2022 «Adozione delle Linee guida per l'attuazione del Fascicolo sanitario elettronico pubblicato sulla GU Serie Generale n. 160 del 11.07.2022».
- Decreto del Ministero della Salute 7 settembre 2023 «Fascicolo sanitario elettronico 2.0».
- Linee Guida per l'attuazione del Fascicolo Sanitario Elettronico (2022).
- Piano Nazionale di Ripresa e Resilienza: M6 - Salute C21.3.1 «Rafforzamento dell'infrastruttura tecnologica e degli strumenti per la raccolta, l'elaborazione, l'analisi dei dati e la simulazione (FSE)».

CIE

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

Riferimenti normativi europei:

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

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

L'obiettivo di migliorare e aumentare l'adozione di servizi erogati da piattaforme nazionali a cittadini, imprese e altre PA, come PagoPA, SEND, App IO, mira a promuovere l'uso diffuso di strumenti digitali standardizzati per migliorare l'efficienza e la facilità di accesso ai servizi pubblici. I risultati attesi dalle azione programmate dall'amministrazione includono una semplificazione delle procedure per cittadini e imprese, una maggiore integrazione e interoperabilità tra diverse piattaforme digitali, e un miglioramento complessivo nella fruizione dei servizi pubblici attraverso soluzioni innovative e integrate.

Linea d'azione	**CAP4.PA.01 - Attivazione di nuovi servizi Pago PA**
Termine adempimento	31/12/2025

Termine predisposizione	31/12/2024
Stato	In preparazione
Descrizione	Le PA aderenti a PagoPA assicurano l'attivazione di nuovi servizi in linea con i target sopra descritti e secondo le modalità attuative definite nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR).
Dettaglio	L'Ente ha aderito già all'attivazione di servizi di pagamento tramite PagoPA. Verrà eseguito un monitoraggio sui possibili servizi specifici da attivare in coerenza con le attività svolte.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP4.PA.06 - Adozione del "Login with eIDAS"**
Termine adempimento	31/12/2025
Termine predisposizione	31/07/2025
Stato	Raggiunto
Descrizione	Le PA e i gestori di pubblici servizi interessati adottano lo SPID e la CIE by default: le nuove applicazioni devono nascere SPID e CIE-only a meno che non ci siano vincoli normativi o tecnologici, se dedicate a soggetti dotabili di SPID o CIE. Le PA che intendono adottare lo SPID di livello 2 e 3 devono anche adottare il «Login with eIDAS» per l'accesso transfrontaliero ai propri servizi.
Dettaglio	Alle applicazioni ed ai servizi utilizzati dall'Ente è possibile accedere tramite mediante riconoscimento dell'identità digitale con SPID, CIE e eIDAS.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP4.PA.07 - Adeguamento alle evoluzioni previste dall'ecosistema SPID**
Termine adempimento	31/12/2025
Termine predisposizione	31/07/2025
Stato	Raggiunto
Descrizione	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).
Dettaglio	Alle applicazioni ed ai servizi utilizzati dall'Ente è possibile accedere tramite mediante riconoscimento dell'identità digitale con SPID, CIE e eIDAS.
Budget previsto	n.a.
Budget utilizzato	n.a.

Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Capitolo 5 - Dati e Intelligenza Artificiale

La costruzione di un'economia dei dati è un obiettivo dell'Unione Europea. La Pubblica Amministrazione è la fonte di una rilevante quantità di dati che possono diventare una miniera di informazioni solo se condivisi tra i diversi enti pubblici, sia a livello tecnico che semantico. L'intelligenza artificiale sostiene proprio questo tipo di processo: garantisce la comprensione del significato dei dati.

Open data e data governance

Con il recepimento della Direttiva Europea (UE) 2019/1024 (cosiddetta Direttiva Open Data) sull'apertura dei dati e il riutilizzo dell'informazione del settore pubblico, attuata con il D.Lgs. n.200/2021, che ha modificato il D.Lgs. n.36/2006, l'obiettivo strategici sopra delineato può essere perseguito attraverso l'attuazione delle nuove regole tecniche definite con le Linee Guida sui dati aperti. Tale documento, adottato da Agid con determinazione n.183/2023 è finalizzato a supportare le pubbliche amministrazioni e gli altri soggetti coinvolti nel processo di apertura dei dati e, quindi, favorire l'aumento dell'offerta di dati pubblici ai fini del loro riutilizzo.

In questo contesto il Consorzio si impegna nel processo di formazione e pubblicazione dei propri dati secondo lo schema proposto dalle suddette Linee Guida che si compone delle seguenti fasi:

1. identificazione (ricognizione, analisi dei vincoli, priorità e percorso di apertura dei dati);
2. analisi (analisi della qualità, bonifica, analisi di processo);
3. arricchimento (vocabolari controllati, ontologie, mashup e linking nei linked open data);
4. validazione (qualità dei dati);
5. pubblicazione (meta datazione, politiche di accesso e licenza, modalità di pubblicazione).

Contesto normativo e strategico

Riferimenti normativi italiani:

- Decreto legislativo 30 giugno 2003, n. 196 «Codice in materia di protezione dei dati personali».
- Decreto legislativo 7 marzo 2005, n. 82 «Codice dell'amministrazione digitale» (in breve CAD), artt. 50, 50-ter., 51, 52, 59, 60.
- Decreto legislativo 24 gennaio 2006, n. 36 «Attuazione della direttiva (UE) 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico che ha abrogato la direttiva 2003/98/CE».
- Decreto legislativo 27 gennaio 2010, n. 32 «Attuazione della direttiva 2007/2/CE, che istituisce un'infrastruttura per l'informazione territoriale nella Comunità europea (INSPIRE)».
- Decreto legislativo 14 marzo 2013, n. 33 «Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni» (Decreto trasparenza).
- Decreto legislativo 10 agosto 2018, n. 101 «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE» (regolamento generale sulla protezione dei dati).
- Decreto-legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 «Misure urgenti per la semplificazione e l'innovazione digitale».
- Decreto-legge 31 maggio 2021, n. 77, convertito con modificazioni dalla Legge 29 luglio 2021, n. 108 «Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure».
- Linee Guida AGID per i cataloghi dati (2017).
- Linee Guida AGID per l'implementazione della specifica GeoDCAT-AP (2017).

- Linee Guida AGID recanti regole tecniche per la definizione e l'aggiornamento del contenuto del Repertorio Nazionale dei Dati Territoriali (2022).
- Linee Guida AGID recanti regole tecniche per l'attuazione del decreto legislativo 24 gennaio 2006, n. 36 e s.m.i. relativo all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico adottate con Determinazione AGID n. 183/2023 del 3 agosto 2023.
- Manuale RNDT - Guide operative per la compilazione dei metadati RNDT.
- Piano Nazionale di Ripresa e Resilienza - Investimento 1.3: «Dati e interoperabilità».

Riferimenti normativi europei:

- Direttiva 2007/2/CE del Parlamento europeo e del Consiglio, del 14 marzo 2007, che istituisce un'Infrastruttura per l'informazione territoriale nella Comunità europea (INSPIRE).
- Regolamento (CE) n. 1205/2008 del 3 dicembre 2008 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda i metadati.
- Regolamento (CE) n. 976/2009 della Commissione, del 19 ottobre 2009, recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda i servizi di rete.
- Regolamento (UE) 2010/1089 del 23 novembre 2010 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda l'interoperabilità dei set di dati territoriali e dei servizi di dati territoriali.
- Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (in breve GDPR).
- Direttiva (UE) 2019/1024 del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.
- Decisione (UE) 2019/1372 del 19 agosto 2019 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda il monitoraggio e la comunicazione.
- Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati).
- Regolamento di esecuzione (UE) 2023/138 della Commissione del 21 dicembre 2022 che stabilisce un elenco di specifiche serie di dati di elevato valore e le relative modalità di pubblicazione e riutilizzo.
- Comunicazione della Commissione 2014/C 240/01 del 24 luglio 2014 - Orientamenti sulle licenze standard raccomandate, i dataset e la tariffazione del riutilizzo dei documenti.
- Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni COM (2020) del 19 febbraio 2020 - Una strategia europea per i dati.

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

La condivisione e il riutilizzo dei dati tra le PA e utilizzo e la fruibilità di tali dati da parte di cittadini e imprese mira a creare ambiente integrato e accessibile che faciliti lo scambio di informazioni tra diversi enti pubblici e i soggetti privati anche per lo sviluppo di progetti innovativi. I risultati attesi prevedono, oltre al miglioramento della trasparenza amministrativa, una maggiore consapevolezza ed efficienza nei processi decisionali e amministrativi, e un aumento dell'innovazione e dell'interazione con la comunità locale grazie all'accesso semplificato ai dati pubblici.

Linea d'azione	**CAP5.PA.03 - Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese**
Termine adempimento	31/12/2025
Termine predisposizione	31/07/2025
Stato	In preparazione

Descrizione	Le PA partecipano, in funzione delle proprie necessità, a interventi di formazione e sensibilizzazione sulle politiche open data.
Dettaglio	L'Ente valuterà in futuro eventuali azioni di diffusione formazione e sensibilizzazione sugli open data presso la propria popolazione
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

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

L'obiettivo di aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati è promuovere la comprensione e l'adozione delle strategie volte a valorizzare e gestire in modo efficace le risorse informative pubbliche. I risultati attesi includono una migliore gestione del patrimonio informativo, una maggiore partecipazione dei cittadini e delle imprese nella creazione e nel riutilizzo dei dati pubblici, e una promozione dell'innovazione e dello sviluppo economico attraverso l'uso strategico delle informazioni pubbliche.

Linea d'azione	**CAP5.PA.20 - Implementazione del Decreto Legislativo n. 36/2006 relativamente ai requisiti e alle raccomandazioni su licenze e condizioni d'uso**
Termine adempimento	Dal 01/01/2024
Termine predisposizione	31/12/2024
Stato	Raggiunto
Descrizione	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
Dettaglio	I dati degli atti dell'Ente sono pubblicati nella sezione Amministrazione Trasparente del sito istituzionale. I dati territoriali sono gestiti da Regione o da altri enti. Si approfondirà nel corso del triennio come operare per la corretta pubblicazione degli Open Data
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Intelligenza artificiale per la Pubblica Amministrazione

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

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

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

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

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

1. **Miglioramento dei servizi e riduzione dei costi**. Le pubbliche amministrazioni concentrano l'investimento in tecnologie di intelligenza artificiale nell'automazione dei compiti ripetitivi connessi ai servizi istituzionali obbligatori e al funzionamento dell'apparato amministrativo. Il conseguente recupero di risorse è destinato al miglioramento della qualità dei servizi anche mediante meccanismi di proattività.
2. **Analisi del rischio**. Le amministrazioni pubbliche analizzano i rischi associati all'impiego di sistemi di intelligenza artificiale per assicurare che tali sistemi non provochino violazioni dei diritti fondamentali della persona o altri danni rilevanti. Le pubbliche amministrazioni adottano la classificazione dei sistemi di IA secondo le categorie di rischio definite dall'AI Act.
3. **Trasparenza, responsabilità e informazione**. Le pubbliche amministrazioni pongono particolare attenzione alla trasparenza e alla interpretabilità dei modelli di intelligenza artificiale al fine di garantire la responsabilità e rendere conto delle decisioni adottate con il supporto di tecnologie di intelligenza artificiale. Le amministrazioni pubbliche forniscono informazioni adeguate agli utenti al fine di consentire loro di prendere decisioni informate riguardo all'utilizzo dei servizi che sfruttano l'intelligenza artificiale.
4. **Inclusività e accessibilità**. Le pubbliche amministrazioni sono consapevoli delle responsabilità e delle implicazioni etiche associate all'uso delle tecnologie di intelligenza artificiale. Le pubbliche amministrazioni assicurano che le tecnologie utilizzate rispettino i principi di equità, trasparenza e non discriminazione.
5. **Privacy e sicurezza**. Le pubbliche amministrazioni adottano elevati standard di sicurezza e protezione della privacy per garantire che i dati dei cittadini siano gestiti in modo sicuro e responsabile. In particolare, le amministrazioni garantiscono la conformità dei propri sistemi di IA con la normativa vigente in materia di protezione dei dati personali e di sicurezza cibernetica.
6. **Formazione e sviluppo delle competenze**. Le pubbliche amministrazioni investono nella formazione e nello sviluppo delle competenze necessarie per gestire e applicare l'intelligenza artificiale in modo efficace nell'ambito dei servizi pubblici. A tale proposito si faccia riferimento agli obiettivi individuati nel Capitolo 1.
7. **Standardizzazione**. Le pubbliche amministrazioni tengono in considerazione, durante le fasi di sviluppo o acquisizione di soluzioni basate sull'intelligenza artificiale, le attività di normazione tecnica in corso a

livello internazionale e a livello europeo da CEN e CENELEC con particolare riferimento ai requisiti definiti dall'AI Act.

8. **Sostenibilità**: Le pubbliche amministrazioni valutano attentamente gli impatti ambientali ed energetici legati all'adozione di tecnologie di intelligenza artificiale e adottando soluzioni sostenibili dal punto di vista ambientale.

9. **Foundation Models** (Sistemi IA «ad alto impatto»). Le pubbliche amministrazioni, prima di adottare foundation models «ad alto impatto», si assicurano che essi adottino adeguate misure di trasparenza che chiariscono l'attribuzione delle responsabilità e dei ruoli, in particolare dei fornitori e degli utenti del sistema di IA.

10. **Dati.** Le pubbliche amministrazioni, che acquistano servizi di intelligenza artificiale tramite API, valutano con attenzione le modalità e le condizioni con le quali il fornitore del servizio gestisce di dati forniti dall'amministrazione con particolare riferimento alla proprietà dei dati e alla conformità con la normativa vigente in materia di protezione dei dati e privacy.

Contesto normativo e strategico

Riferimenti normativi europei:

- Comunicazione della Commissione al Parlamento Europeo e al Consiglio, «Piano Coordinato sull'Intelligenza Artificiale», COM (2021) 205 del 21 aprile 2021.
- «Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale» (AI Act), COM (2021) 206, del 21 aprile 2021.
- Decisione della Commissione «on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence» C (2023) 3215 del 22 maggio 2023.

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

L'obiettivo di aumentare la consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale include anche la promozione e l'adozione di apposite linee guida per l'acquisizione e lo sviluppo di applicativi basati sull'AI. Questo per garantire un'implementazione responsabile, etica e trasparente delle tecnologie avanzate. I risultati attesi sono un miglioramento dell'efficienza operativa attraverso l'automazione dei processi complessi, una maggiore capacità di previsione e pianificazione basata sui dati, e una promozione di servizi pubblici più personalizzati e orientati alle necessità dei cittadini, nel rispetto dei principi di sicurezza dei dati e inclusione sociale.

Linea d'azione	**CAP5.PA.22 - Adozione delle linee guida per il procurement di IA nella Pubblica Amministrazione**
Termine adempimento	31/12/2025
Termine predisposizione	31/07/2025
Stato	In preparazione
Descrizione	Le PA adottano le Linee guida per il procurement di IA nella Pubblica Amministrazione.

Dettaglio	L'Ente provvederà a comprendere come applicare alle proprie attività gli applicativi basati sull'intelligenza artificiale e ad adottare le Linee guida per il procurement di IA nelle proprie attività.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP5.PA.23 - Adozione delle linee guida per lo sviluppo di applicazioni di IA nella Pubblica**
Termine adempimento	31/12/2025
Termine predisposizione	31/07/2025
Stato	In preparazione
Descrizione	Le PA adottano le Linee guida per lo sviluppo di applicazioni di IA nella Pubblica Amministrazione.
Dettaglio	L'Ente provvederà a comprendere come sviluppare applicativi di IA nelle proprie attività e ad adottare
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP5.PA.24 - Adozione delle applicazioni di IA a valenza nazionale**
Termine adempimento	31/12/2026
Termine predisposizione	01/01/2026
Stato	In preparazione
Descrizione	Le PA adottano le applicazioni di IA a valenza nazionale
Dettaglio	L’Ente valuterà le applicazioni di IA a valenza nazionale disponibili con l'intento di comprendere quali possano essere utili alle attività dell'ente.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Capitolo 6 - Infrastrutture

Infrastrutture digitali e Cloud

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

Con l'applicazione del principio cloud first, si vuole favorire l'adozione sicura, controllata e completa delle tecnologie cloud da parte dell'ente, in linea con i principi di tutela della privacy e con le raccomandazioni delle istituzioni europee e nazionali. In particolare, nella fase di definizione di un nuovo progetto, e/o di sviluppo di nuovi servizi, in via prioritaria dovrà essere valutata l'adozione del paradigma cloud prima di qualsiasi altra tecnologia.

L'adozione del paradigma cloud è inoltre un modo per:

- Mitigare il rischio di lock-in verso i fornitori di sviluppo e manutenzione applicativa;
- Incrementare la sicurezza delle reti, dei dati e delle informazioni e per proteggere l'ente dai rischi cyber.

Altro aspetto da considerare è quello dei costi operativi correnti. Con la migrazione al cloud, siprevede la possibilità di risparmio economico subordinato, tuttavia, ad una corretta gestione dei costi cloud, sia da un punto di vista contrattuale che tecnologico.

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

Approfondimento tecnologico per il RTD

1) La piena abilitazione al cloud richiede l'evoluzione del parco applicativo software verso la logica as a service delle applicazioni esistenti, andando oltre il mero lift-and-shift dei server, progettando opportuni interventi di rearchitect, replatform o repurchase per poter sfruttare le possibilità offerte oggi dalle moderne piattaforme computazionali e dagli algoritmi di intelligenza artificiale. In tal senso, occorre muovere verso architetture a «micro-servizi» le cui caratteristiche sono, in sintesi, le seguenti:

- ogni servizio non ha dipendenze esterne da altri servizi e gestisce autonomamente i propri dati (self-contained)
- ogni servizio comunica con l'esterno attraverso API/webservice e senza dipendenza da stati pregressi (lightweight/stateless)
- ogni servizio può essere implementato con differenti linguaggi e tecnologie, in modo indipendente dagli altri servizi (implementation-indipendent)
- ogni servizio può essere dispiegato in modo automatico e gestito indipendentemente dagli altri servizi (indipendently deployable)
- ogni servizio implementa un insieme di funzioni legate a procedimenti e attività amministrative, non ha solo scopo tecnologico (business-oriented):

2) È compito dell'Ufficio RTD curare sia gli aspetti di pianificazione della migrazione/abilitazione al cloud che l'allineamento dello stesso con l'implementazione delle relative opportunità di riorganizzazione dell'ente offerte dall'abilitazione al cloud e dalle nuove architetture a micro-servizi.

3) La gestione del ciclo di vita dei servizi in cloud dell'amministrazione richiede la strutturazione di opportuni presidi organizzativi e strumenti tecnologici per il cloud-cost-management, in forma singola o associata.

Contesto normativo e strategico

Riferimenti normativi nazionali:

- Decreto legislativo 7 marzo 2005, n. 82, «Codice dell'amministrazione digitale» articoli 8-bis e 73;
- Decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, «Ulteriori misure urgenti per la crescita del Paese», articolo 33-septies;
- Decreto legislativo 18 maggio 2018, n. 65, «Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione»;
- Decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla L. 18 novembre 2019, n. 133 «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica»;
- Decreto-legge 17 marzo 2020, n. 18, convertito con modificazioni dalla Legge 24 aprile 2020, n. 27 «Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19», art. 75;
- Decreto-legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 «Misure urgenti per la semplificazione e l'innovazione digitale», art. 35;
- Decreto-legge 31 maggio 2021, n. 77, convertito con modificazioni dalla Legge 29 luglio 2021, n. 108 «Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure»;
- Decreto-legge 14 giugno 2021, n. 82, convertito con modificazioni dalla Legge 4 agosto 2021, n. 109 «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale»;
- Circolare AGID n. 1/2019 del 14 giugno 2019 - Censimento del patrimonio ICT delle Pubbliche Amministrazioni e classificazione delle infrastrutture idonee all'uso da parte dei Poli Strategici Nazionali;
- Strategia italiana per la banda ultra-larga (2021);
- Strategia Cloud Italia (2021);
- Regolamento AGID, di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la Pubblica Amministrazione e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la Pubblica Amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la Pubblica Amministrazione (2021);
- Determinazioni ACN in attuazione al precedente Regolamento n. 306/2022 (con allegato) su e n. 307/2022 (con allegato);
- Decreti direttoriali ACN prot. N. 29 del 2 gennaio 2023, n. 5489 dell'8 febbraio 2023 e n. 20610 del 28 luglio 2023;
- Piano Nazionale di Ripresa e Resilienza:
    - Investimento 1.1: «Infrastrutture digitali»;
    - Investimento 1.2: «Abilitazione e facilitazione migrazione al cloud».

Riferimenti europei:

- European Commission Cloud Strategy, Cloud as an enabler for the European Commission Digital Strategy, 16 May 2019;
- Strategia europea sui dati Commissione Europea 19.2.2020 COM (2020) 66 final Data Governance and data policy at the European Commission, July 2020 Regulation of the European Parliament and of the Council on European data governance (Data Governance Act - 2020).

Obiettivo 6.1 – Migliorare la qualità e la sicurezza dei servizi digitali erogati dall'amministrazione attuando la strategia «Cloud Italia» e migrando verso infrastrutture e servizi cloud qualificati.

L'obiettivo di migliorare la qualità e la sicurezza dei servizi digitali erogati dall'amministrazione proseguendo nell'attuazione della strategia «Cloud Italia» e completando la migrazione dei dati e dei servizi verso infrastrutture e servizi cloud qualificati mira a modernizzare e potenziare i sistemi informatici dell'Ente. I risultati attesi sono una maggiore affidabilità e sicurezza dei servizi digitali offerti ai cittadini, una riduzione dei costi operativi attraverso l'uso di soluzioni cloud scalabili ed efficienti, e una maggiore resilienza delle infrastrutture IT, garantendo continuità operativa e protezione dei dati.

Linea d'azione	**CAP6.PA.03 -Migrazione al cloud**
Termine adempimento	30/06/2026
Termine predisposizione	01/01/2025
Stato	In preparazione
Descrizione	Le PA avviano il percorso di migrazione verso il cloud in coerenza con quanto previsto dalla Strategia Cloud Italia.
Dettaglio	I gestionali utilizzati presso questo Ente sono già in Cloud. Saranno valutate attivazioni di nuovi servizi attraverso i finanziamenti a valere sulla misura 1.2 del PNRR non appena verrà pubblicato il nuovo avviso.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP6.PA.04 -Applicazione del principio "Cloud first"**
Termine adempimento	Dal 31/07/2024
Termine predisposizione	31/07/2024
Stato	Raggiunto
Descrizione	Le PA continuano ad applicare il principio cloud first e ad acquisire servizi cloud solo se qualificati.
Dettaglio	I servizi più recentemente acquistati dall'Ente sono tutti forniti da provider presenti sul catalogo ACN dei fornitori di servizi cloud qualificati.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio Informatica in accordo con il Responsabile per la Transizione Digitale

Capitolo 7 - Sicurezza informatica

Sicurezza informatica

La necessità di migrare verso il digitale per ottimizzare i procedimenti amministrativi porta con sé nuovi rischi cyber. La riforma dell'architettura nazionale cyber, con l'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN), mira a sviluppare e rafforzare le capacità cyber nazionali attraverso la Strategia nazionale di cybersicurezza. Con il supporto del Piano Nazionale di Ripresa e Resilienza, sono state allocate risorse significative per migliorare la sicurezza cibernetica della Pubblica Amministrazione. Gli interventi previsti includono modelli di gestione centralizzata della cybersicurezza, processi di gestione del rischio, e promozione della cultura cyber. L'AGID fornirà piattaforme e servizi per contrastare i rischi cyber. Il Consorzio si focalizza su metodologie proattive come vulnerability assessment, penetration test e website security scanner, e partecipa a progetti di formazione sulla sicurezza informatica

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

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

Per l'attuazione delle linee d'azione l'ente si servirà delle piattaforme e dei servizi che AGID metterà a disposizione della Pubblica Amministrazione e che verranno erogati tramite il CERT, finalizzati alla conoscenza e al contrasto dei rischi cyber legati al patrimonio ICT della PA .
Il Consorzio intende investire su strumenti proattivi utilizzati per individuare e proteggere gli asset più esposti agli attacchi usando le seguenti metodologie:

- Vulnerability assessment
- Penetration test
- Website security scanner

Ha inoltre aderito al progetto "Progetto PNRR Cybersecurity FVG – Training & Awareness: Formazione e sensibilizzazione sui temi della Sicurezza informatica".

Contesto normativo e strategico

Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82, «Codice dell'amministrazione digitale», articolo 51
- Decreto del Presidente del Consiglio dei ministri 17 febbraio 2017, «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali»
- Decreto Legislativo 18 maggio 2018, n. 65, «Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello elevato di sicurezza delle reti e dei sistemi informativi nell'Unione»
- Decreto del Presidente del Consiglio dei ministri 8 agosto 2019, «Disposizioni sull'organizzazione e il funzionamento del computer security incident response team - CSIRT italiano»

- Decreto-legge 21 settembre 2019, n. 105, «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica»
- Decreto-legge 19 luglio 2020, n. 76, «Misure urgenti per la semplificazione e l'innovazione digitale»
- Decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, «Regolamento in materia di cybersecurity di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misura volte a garantire elevati livelli di sicurezza»
- Decreto-legge 14 giugno 2021 n. 82, «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la Cybersicurezza Nazionale»
- Decreto legislativo 8 novembre 2021 n. 207, «Attuazione della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche (rifusione)»
- Decreto-legge 21 marzo 2022 n. 21, «Misure urgenti per contrastare gli effetti economici e umanitari della crisi Ucraina», articoli 27, 28 e 29
- Decreto del Presidente del Consiglio dei ministri 17 maggio 2022, Adozione della Strategia nazionale di cybersicurezza 2022-2026 e del relativo Piano di implementazione 2022-2026
- Misure minime di sicurezza ICT per le pubbliche amministrazioni, 18 marzo 2017
- Linee guida sulla sicurezza nel procurement ICT, del mese di aprile 2020
- Strategia Cloud Italia, adottata a settembre 2021
- Piano Nazionale di Ripresa e Resilienza - Investimento 1.5: «Cybersecurity»

Riferimenti normativi europei:

- Direttiva 6 luglio 2016 n. 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
- Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»).
- Direttiva 14 dicembre 2022 n. 2022/2555/UE relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (Testo rilevante ai fini del SEE).

Obiettivo 7.1 – Adottare una governance della cybersicurezza diffusa nella PA

L'obiettivo di adottare una governance della cybersicurezza dell'Ente mira a strutturare e implementare un sistema organizzato e coordinato per la gestione della sicurezza informatica. Questo include la definizione di politiche e procedure, l'adozione di tecnologie di sicurezza avanzate, e la formazione continua del personale. I risultati attesi sono un rafforzamento della protezione contro le minacce informatiche, una maggiore resilienza operativa in caso di incidenti di sicurezza, e una maggiore fiducia da parte dei cittadini nella capacità dell'ente di salvaguardare i dati e i servizi digitali.

Linea d'azione	**CAP7.PA.01 - Definizione di un modello unitario dell'ente per la governance della cybersicurezza**
Termine adempimento	Dal 01/09/2024
Termine predisposizione	31/12/2024
Stato	Raggiunto

Descrizione	Le singole PA definiscono il modello unitario, assicurando un coordinamento centralizzato a livello dell'istituzione, di governance della cybersicurezza.
Dettaglio	I gestionali in Cloud, forniti in convenzione Regionale e gestiti tramite fornitore Insiel e i gestionali di fornitori terzi sono adeguati agli standard AgID.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP7.PA.02 - Adozione del modello di governance della cybersicurezza dell'ente**
Termine adempimento	Dal 01/12/2024
Termine predisposizione	31/12/2024
Stato	Raggiunto
Descrizione	Le PA adottano un modello di governance della cybersicurezza.
Dettaglio	I gestionali in Cloud, forniti in convenzione Regionale e gestiti tramite fornitore Insiel e i gestionali di fornitori terzi sono adeguati agli standard AgID.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP7.PA.03 - Nomina del Responsabili della cybersicurezza**
Termine adempimento	Dal 01/12/2024
Termine predisposizione	31/12/2024
Stato	In preparazione
Descrizione	Le PA nominano i Responsabili della cybersicurezza e delle loro strutture organizzative di supporto.
Dettaglio	L'Ente non ha ancora nominato un responsabile della cybersicurezza, avendo nominato esclusivamente il RTD, provvederà ad individuare la figura più idonea per tale funzione.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP7.PA.04 - Formalizzazione dei processi inerenti alla cybersicurezza**
Termine adempimento	Dal 01/12/2024
Termine predisposizione	31/12/2024
Stato	In preparazione
Descrizione	Le PA formalizzano i processi e le procedure inerenti alla gestione della cybersicurezza.
Dettaglio	Non appena nominato il responsabile della cybersicurezza, l'Ente provvederà a formalizzare le procedure di cybersecurity.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

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

L'obiettivo di gestire i processi di approvvigionamento IT coerentemente con i requisiti di sicurezza definiti a livello di governance, mira a garantire che tutte le acquisizioni di tecnologie e servizi informatici rispettino rigorosi standard di sicurezza. Questo comporta la valutazione e selezione di fornitori e soluzioni IT che soddisfino i criteri di sicurezza individuati, la redazione di contratti che includano clausole specifiche per la protezione dei dati e la sicurezza informatica, e il monitoraggio continuo delle conformità. I risultati attesi sono un miglioramento della sicurezza delle infrastrutture IT dell'ente, la riduzione dei rischi associati agli approvvigionamenti tecnologici lungo tutta la catena di fornitura, e l'assicurazione che tutti i sistemi e servizi implementati contribuiscano alla protezione dei dati e alla continuità operativa dell'Ente.

Linea d'azione	**CAP7.PA.05 - Approvazione dei requisiti di sicurezza dei processi di approvvigionamento IT**
Termine adempimento	Dal 01/06/2024
Termine predisposizione	31/12/2024
Stato	Raggiunto
Descrizione	Le PA definiscono e approvano i requisiti di sicurezza relativi al processo di approvvigionamento IT.
Dettaglio	L'Ente osserva le indicazioni contenute nelle Linee guida sulla sicurezza nel procurement ICT emanate da AGID a maggio 2020 e provvederà a formalizzare tali indicazioni tecnico-amministrative per garantire, all'interno delle proprie procedure per l'approvvigionamento di beni e servizi informatici, la rispondenza ad adeguati livelli di sicurezza.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio Informatica in accordo con il Responsabile per la Transizione Digitale

Linea d'azione	**CAP7.PA.06 - Gestione dei rischi su fornitori e terze parti nei processi di approvvigionamento IT**
Termine adempimento	Dal 01/12/2024
Termine predisposizione	31/12/2024
Stato	Raggiunto
Descrizione	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.
Dettaglio	L'Ente osserva le indicazioni contenute nelle Linee guida sulla sicurezza nel procurement ICT emanate da AGID a maggio 2020. Una volta formalizzate tali indicazioni tecnico-amministrative per garantire, all'interno delle procedure per l'approvvigionamento di beni e servizi informatici dell'ente, la rispondenza ad adeguati livelli di sicurezza, provvederà a strutturare i processi di gestione del rischio derivante dalla compromissione della catena di fornitura.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP7.PA.07 - Realizzazione di attività di audit e verifica verso i fornitori e le terze parti**
Termine adempimento	Dal 01/12/2025
Termine predisposizione	31/07/2025
Stato	Raggiunto
Descrizione	Le PA realizzano le attività di controllo definite nel Piano di audit e verifica verso i fornitori e terze parti IT.
Dettaglio	L'Ente osserva le indicazioni contenute nelle Linee guida sulla sicurezza nel procurement ICT emanate da AGID a maggio 2020. Una volta formalizzate tali indicazioni tecnico-amministrative per garantire, all'interno delle procedure per l'approvvigionamento di beni e servizi informatici dell'ente, la rispondenza ad adeguati livelli di sicurezza, provvederà a definire il pano di audit nei confronti dei fornitori e delle terze parti interessate e ad attuare le attività in esso previste.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Obiettivo 7.3 – Gestione e mitigazione del rischio cyber

L'obiettivo di gestione e mitigazione del rischio cyber mira a definire e attuare misure in grado di identificare, valutare e ridurre le minacce informatiche che possono compromettere la sicurezza delle infrastrutture IT e dei dati gestiti dall'ente locale. Questo implica l'implementazione di un programma di gestione del rischio che includa l'analisi periodica delle vulnerabilità, l'adozione di misure preventive e correttive, e lo sviluppo di piani di risposta agli incidenti. I risultati attesi sono una riduzione dell'esposizione alle minacce cyber, una maggiore capacità di prevenire e rispondere rapidamente agli attacchi informatici, e la protezione continua delle risorse digitali e dei dati sensibili dell'ente, assicurando così la continuità e la fiducia nei servizi offerti ai cittadini.

Linea d'azione	**CAP7.PA.08 - Definizione del processo di Cyber risk management e security by design**
Termine adempimento	Dal 01/12/2024
Termine predisposizione	31/12/2024
Stato	In preparazione
Descrizione	Le PA definiscono e formalizzano il processo di cyber risk management e security by design, coerentemente con gli strumenti messi a disposizione da ACN.
Dettaglio	Non appena nominato il responsabile della cybersicurezza, l'Ente provvederà a definire e formalizzare il processo di cyber risk management e security by design, coerentemente con le esigenze determinate dalle peculiarità della propria attività con gli strumenti messi a disposizione da ACN.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP7.PA.09 - Censimento dei dati e dei servizi dell'ente**
Termine adempimento	31/12/2025
Termine predisposizione	31/07/2025
Stato	In preparazione
Descrizione	Le PA promuovono il censimento dei dati e servizi della PA, identificandone la rilevanza e quindi le modalità per garantirne la continuità operativa.
Dettaglio	Non appena nominato il responsabile della cybersicurezza, l'Ente provvederà ad eseguire il censimento dei dati e dei servizi erogati, identificandone la rilevanza con particolare riguardo alla possibile perdita di dati ed al loro ripristino per la definizione delle modalità operative per garantirne la continuità.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP7.PA.10 - Attuazione delle procedure operative di cybersicurezza**
Termine adempimento	31/12/2025
Termine predisposizione	31/07/2025
Stato	In preparazione
Descrizione	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
Dettaglio	Non appena nominato il responsabile della cybersicurezza, si provvederà a gestire l'azione, in particolare in connessione alla messa in sicurezza dell'integrità, confidenzialità e disponibilità dei servizi e dei dati.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP7.PA.11 - Integrazione delle attività di monitoraggio del rischio cyber nella gestione dei sistemi**
Termine adempimento	31/12/2026
Termine predisposizione	01/01/2026
Stato	In preparazione
Descrizione	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.
Dettaglio	Non appena nominato il responsabile della cybersicurezza, l'Ente provvederà a integrare 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.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

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

L'obiettivo di potenziare le modalità di prevenzione e gestione degli incidenti informatici mira a rafforzare le capacità dell'Ente di anticipare, rilevare e rispondere efficacemente agli attacchi informatici. Questo include l'adozione di tecnologie avanzate di monitoraggio e rilevamento delle minacce, la formazione continua del personale sulla sicurezza informatica, e lo sviluppo di protocolli chiari per la gestione degli incidenti. I risultati attesi sono una maggiore prevenzione degli attacchi attraverso il monitoraggio proattivo, una risposta più rapida ed efficace agli incidenti, e una riduzione dell'impatto delle violazioni di sicurezza, garantendo così la protezione delle infrastrutture IT, dei servizi e dei dati.

Linea d'azione	**CAP7.PA.13 - Definizione dei presidi per la gestione degli eventi di sicurezza**
Termine adempimento	Dal 01/06/2024
Termine predisposizione	31/12/2024
Stato	In preparazione
Descrizione	Le PA definiscono i presidi per la gestione degli eventi di sicurezza, formalizzandone i processi e le procedure.
Dettaglio	Non appena nominato il responsabile della cybersicurezza, l'Ente provvederà a definire i presidi per la gestione degli eventi di sicurezza, formalizzandone i processi e le procedure.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio Informatica in accordo con il Responsabile per la Transizione Digitale

Linea d'azione	**CAP7.PA.14 - Formalizzazione di ruoli, responsabilità e processi nella gestione degli incidenti informatici**
Termine adempimento	Dal 01/12/2024
Termine predisposizione	31/12/2024
Stato	In preparazione
Descrizione	Le PA formalizzano ruoli, responsabilità e processi, nonché le capacità tecnologiche a supporto della prevenzione e gestione degli incidenti informatici.
Dettaglio	Non appena nominato il responsabile della cybersicurezza, l'Ente provvederà a formalizzare ruoli, responsabilità e processi, nonché le capacità tecnologiche a supporto della prevenzione e gestione degli incidenti informatici.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP7.PA.15 - Definizione modalità di verifica della risposta agli incidenti informatici**
Termine adempimento	Dal 01/12/2024
Termine predisposizione	31/12/2024
Stato	In preparazione
Descrizione	Le PA definiscono le modalità di verifica dei Piani di risposta a seguito di incidenti informatici.

Dettaglio	Non appena nominato il responsabile della cybersicurezza, l'Ente provvederà a definire le modalità di verifica dei Piani di risposta a seguito di incidenti informatici.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP7.PA.16 - Definizione modalità di aggiornamento dei piani di risposta agli incidenti informatici**
Termine adempimento	Dal 01/12/2025
Termine predisposizione	31/07/2025
Stato	In preparazione
Descrizione	Le PA definiscono le modalità di aggiornamento dei Piani di risposta e ripristino a seguito dell'accadimento di incidenti informatici.
Dettaglio	Non appena nominato il responsabile della cybersicurezza, l'Ente provvederà a definire le modalità di aggiornamento dei Piani di risposta e ripristino a seguito dell'accadimento di incidenti informatici.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Obiettivo 7.5 – Implementare attività strutturate di sensibilizzazione cyber del personale

L'obiettivo di implementare attività strutturate di sensibilizzazione cyber del personale mira a educare e formare continuamente i dipendenti dell'ente locale sulle pratiche di sicurezza informatica e sulla consapevolezza delle minacce cyber. Questo include la realizzazione di programmi di formazione periodici, workshop, simulazioni di attacchi informatici e campagne informative. I risultati attesi sono un aumento della consapevolezza e delle competenze del personale in materia di sicurezza informatica, una riduzione del rischio di errori umani che possono compromettere la sicurezza, e una cultura organizzativa più attenta e proattiva nella protezione delle risorse digitali.

Linea d'azione	**CAP7.PA.17 - Formazione e sensibilizzazione in ambito cybersicurezza**
Termine adempimento	Dal 01/06/2024
Termine predisposizione	31/12/2024
Stato	In preparazione
Descrizione	Le PA promuovono l'accesso e l'utilizzo di attività strutturate di sensibilizzazione e formazione in ambito cybersicurezza.

Dettaglio	Non appena nominato il responsabile della cybersicurezza, l'Ente provvederà a definire e attuare le modalità per la promozione di attività strutturate di sensibilizzazione e formazione in ambito cybersicurezza.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio Informatica in accordo con il Responsabile per la Transizione Digitale

Linea d'azione **CAP7.PA.18 - Definizione piani di formazione specifici inerenti alla cybersicurezza**

Termine adempimento	Dal 01/12/2024
Termine predisposizione	31/12/2024
Stato	In preparazione
Descrizione	Le PA definiscono piani di formazione inerenti alla cybersecurity, diversificati per ruoli, posizioni organizzative e attività delle risorse dell'organizzazione.
Dettaglio	Non appena nominato il responsabile della cybersicurezza, l'Ente provvederà alla definizione di piani formativi sul tema della cybersicurezza diversificati in base ai ruoli, posizioni organizzative e attività delle risorse dell'organizzazione.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione **CAP7.PA.19 - Miglioramento della consapevolezza del personale in tema di cybersicurezza**

Termine adempimento	Dal 01/12/2025
Termine predisposizione	31/07/2025
Stato	In preparazione
Descrizione	Le PA realizzano iniziative per verificare e migliorare la consapevolezza del proprio personale.
Dettaglio	Non appena nominato il responsabile della cybersicurezza, l'Ente provvederà, anche in considerazione delle linee d'azione precedenti, a verificare e migliorare il libello di consapevolezza del proprio personale sul tema della cybersicurezza.
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

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

L'obiettivo di contrastare il rischio cyber attraverso attività di supporto proattivo all'operatività dell'ente mira a fornire assistenza continua e preventiva per proteggere le infrastrutture digitali e i dati sensibili. Questo include la collaborazione con esperti di sicurezza informatica e di strutture e servizi erogati a livello nazionale come il CertA-GID per monitorare le minacce, effettuare valutazioni periodiche delle vulnerabilità, e implementare misure preventive avanzate. I risultati attesi sono una riduzione delle probabilità di attacchi informatici, una capacità di risposta più rapida ed efficace in caso di incidenti, e un ambiente IT più sicuro e resiliente per la PA, garantendo la continuità dei servizi e la fiducia dei cittadini.

Linea d'azione	**CAP7.PA.20 - Accreditamento dell'ente al Cert-AGID**
Termine adempimento	31/12/2025
Termine predisposizione	31/07/2025
Stato	In preparazione
Descrizione	Le PA dovranno dotarsi degli strumenti idonei all'acquisizione degli IoC ed accreditarsi al CERT-AGID.
Dettaglio	L'Ente provvederà a valutare e pianificare le attività dell'azione, approfondendo a mezzo di consulenza specialistica
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP3.PA.10 - Test automatico di accessibilità del sito web**
Termine adempimento	Dal 01/10/2024
Termine predisposizione	31/12/2025
Stato	In preparazione
Descrizione	Le PA dovranno usufruire degli strumenti per la gestione dei rischi cyber messi a disposizione dal CERT-AGID.
Dettaglio	Non appena nominato il responsabile della cybersicurezza ed effettuato l'accreditamento al Cert-AGID verranno valutati i servizi di cui l'ente potrebbe usufruire
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Linea d'azione	**CAP7.PA.22 - Fruizione dei servizi offerti dal Cert-AGID**
Termine adempimento	31/12/2025

Termine predisposizione	31/07/2025
Stato	In preparazione
Descrizione	Le PA, sulla base delle proprie esigenze, partecipano ai corsi di formazione base ed avanzato erogati dal CERT-AGID.
Dettaglio	l'Ente provvederà ad effettuare una ricognizione delle esigenze formative interne e a formare opportunamente il personale anche usufruendo dei corsi erogati dal Cert-AGID
Budget previsto	n.a.
Budget utilizzato	n.a.
Strutture responsabili e attori coinvolti	Ufficio informatica in collaborazione con il Responsabile per la transizione digitale

Conclusioni

L'inclusione di questi obiettivi nel piano triennale per l'informatica dell'ente rappresenta un impegno concreto verso la modernizzazione e la sicurezza dei servizi digitali offerti. La digitalizzazione dei processi, l'adozione di tecnologie avanzate come l'intelligenza artificiale e il cloud, e la gestione rigorosa della cybersicurezza garantiranno un miglioramento significativo dell'efficienza, della trasparenza e della resilienza operativa. Inoltre, la formazione continua del personale e la sensibilizzazione sulla sicurezza informatica contribuiranno a creare una cultura organizzativa proattiva e attenta alla protezione dei dati. Questi sforzi collettivi non solo miglioreranno la qualità dei servizi offerti ai cittadini, ma rafforzeranno anche la fiducia nella capacità dell'ente di gestire le sfide digitali del futuro.

Glossario

AGID

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

API

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

API-first

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

CAD

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

CITD

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

Cloud first

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

Decennio Digitale

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

Digital & mobile first

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

Digital identity only

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

Gold plating

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

Governo come Piattaforma

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

ICT

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

Interoperabilità

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

Lock-in

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

Once-only

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

Open data by design e by default

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

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

SIPA

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

User-centric

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

UTD

Ufficio Informatica è l'ufficio dell'amministrazione a cui viene affidato il delicato processo di transizione alla modalità operativa digitale.