Piano Triennale per la transizione digitale 2023 - 2025

Ente di Gestione delle Aree Protette **del Monviso**

Riferimento al Piano Triennale per l'informatica 2022-2024 pubblicato da AGID

Sommario

PARTE Iª - IL PIANO TRIENNALE **4**
Introduzione e contesto operativo **4**
Ruolo del Responsabile per la Transizione al Digitale **4**
Contesto Strategico **5**
Servizi e banche dati **5**
Sedi e principali infrastrutture **6**
Obiettivi e spesa complessiva prevista **6**
PARTE IIa – LE COMPONENTI TECNOLOGICHE **9**
CAPITOLO 1. Servizi **10**
Contesto normativo e strategico 11
Obiettivi e risultati attesi 12
Cosa deve fare l'Amministrazione 12
Esperienze acquisite 16
CAPITOLO 2. Dati **17**
Contesto normativo e strategico 17
Obiettivi e risultati attesi 19
Cosa deve fare l'amministrazione 19
CAPITOLO 3. Piattaforme **22**
Contesto normativo e strategico 22
Obiettivi e risultati attesi 25
Cosa deve fare l'Amministrazione 26
Esperienze acquisite 27
CAPITOLO 4. Infrastrutture **28**
Contesto normativo e strategico 30
Obiettivi e risultati attesi 31
Cosa deve fare l'Amministrazione 31
Esperienze acquisite 31
CAPITOLO 5. Interoperabilità **32**
Contesto normativo e strategico 33
Obiettivi e risultati attesi 34
Cosa deve fare l'Amministrazione 34
Esperienze acquisite 34
CAPITOLO 6. Sicurezza informatica **35**
Contesto normativo e strategico 35
Obiettivi e risultati attesi 36

Cosa deve fare l'Amministrazione 37
Esperienze acquisite 38
PARTE IIIa - La governance 39
CAPITOLO 8. Governare la trasformazione digitale 39
Obiettivi e risultati attesi 39
Cosa deve fare l'Amministrazione 39
APPENDICE 1. Acronimi 40

PARTE Iª - IL PIANO TRIENNALE

Introduzione e contesto operativo

Gli Enti di gestione delle Aree protette sono enti strumentali della Regione Piemonte costituiti con Legge regionale 29 giugno 2009, n. 19 (Testo Unico sulla tutela delle aree naturali e della biodiversità) e s.m.i.
Redigere il piano triennale dell'informatica per l'EGAP comporta da una parte comprendere le linee guida del Piano triennale della Pubblica Amministrazione redatto da Agid (Agenzia per l'Italia digitale) e dalla altra parte calarsi nella realtà dell'informatica esistente e ciò che è stata fatto nella direzione indicata da Agid. Si riprende, per meglio comprenderne le finalità, la definizione iniziale del Piano triennale Agid nella sua guida dinamica: "Il Piano triennale, nel proseguire il percorso intrapreso col Piano precedente, prevede un importante coinvolgimento delle pubbliche amministrazioni che dovranno recepire ed utilizzare le indicazioni e gli strumenti messi a disposizione da AGID. Le pubbliche amministrazioni sono al centro del processo di trasformazione digitale del Paese in quanto costituiscono lo snodo principale in grado di abilitare la cultura dell'innovazione tra imprese e cittadini. In quest'ottica, il Piano detta indirizzi su temi specifici che le amministrazioni potranno utilizzare per costruire i loro piani di trasformazione digitale all'interno di una cornice condivisa, definita da AGID".
Il piano vuole essere anche una guida operativa, una strada da seguire per ottemperare all'evoluzione del sistema informativo e per condurre, di concerto con il piano strategico dell'amministrazione, ad una strategia di sviluppo allargato in campo digitale.
Il piano infine vuole essere uno strumento aperto, suscettibile di continui miglioramenti ed adeguamenti finalizzato a far crescere la qualità dei servizi all'interno dell'amministrazione e di conseguenza di quelli forniti ai cittadini, promuovendo e sollecitando la partecipazione allargata ed attiva dei cittadini.
Il contesto dell'EGAP oggi non prevede una figura dedicata all'informatica e agli applicativi, lo sviluppo del sistema è avvenuto per gli applicativi di contabilità e protocollo e dotare i tecnici degli strumenti di produttività individuale indispensabili allo svolgimento della loro professione.
La connettività è garantita da una connessione commerciale mentre la telefonia è gestita dalla Regione.
Questo progetto rappresenta la continuazione di un percorso che abbiamo cominciato a tracciare con l'approvazione del primo piano triennale avvenuto con Deliberazione del Consiglio n. 46 del 28/12/2021, e che continueremo a percorrere per identificare e costruire un sistema informativo integrato che ci consenta di operare in maniera efficace attuando le indicazioni AGID e rispettando la normativa in vigore.

Ruolo del Responsabile per la Transizione al Digitale

Questa rappresenta la seconda versione del PTTD, ma il nostro lavoro è cominciato qualche tempo fa con i primi incontri formativi in cui abbiamo acquisito la consapevolezza che oltre ai singoli adempimenti in parte conosciuti esisteva un quadro complessivo più dettagliato e più complesso.
Abbiamo compreso che per definire un'evoluzione del sistema informativo è indispensabile fotografare ed identificare gli elementi oggi presenti nel nostro ente, rapportarli con le indicazioni e costruire un percorso evolutivo di adeguamento.
Nel nostro ruolo di Enti strumentali della Regione Piemonte abbiamo identificato un consulente comune a cui abbiamo conferito un incarico professionale attraverso il Mercato della PA affinché svolga i seguenti ruoli:

- aiuto nella comprensione, razionalizzazione ed adeguamento alla realtà del nostro ente delle indicazioni AGID
- condivisione delle esperienze tra enti simili
- dialogo e consulenza per la scelta delle nuove soluzioni e per la selezione dei nuovi servizi/fornitori nel rispetto delle regole previste dal piano.

Il nostro team per la transizione al digitale:

- **Molinari Vincenzo Maria**: Direttore dell'ente
- **Paseri Maurilio**: Responsabile del servizio tecnico
- **Cavallo Paola**: segreteria di direzione

Per poter progettare un percorso è indispensabile identificare lo stato di fatto dei servizi informatici: componenti tecnologiche, infrastrutturali, applicative, le basi dati ed i servizi in essere, valutando inoltre il livello di sicurezza applicativa ed infrastrutturale ed il grado di interoperabilità oggi raggiunto.

Contesto Strategico

Come descritto in premessa si tratta di un ente strumentale della Regione Piemonte; pertanto, i riferimenti strategici sono quelli istituzionali, Legge regionale 29 giugno 2009, n. 19 s.m.i.

Servizi e banche dati

Attraverso la compilazione del questionario di PADigitale2026 abbiamo definito una prima classificazione dei servizi e delle banche dati, è importante evidenziare come l'ente da oltre 2 anni grazie alla collaborazione con SISCOM opera con tecnologia SAAS, possiamo pertanto affermare che la securizzazione dei dati applicativi è avvenuta con largo anticipo sulle tempistiche AGID:

funzione	applicativo	produttore	ubicazione	utenti	Attivo
Protocollo	Egisto - Olimpo	Siscom	Cloud Siscom	5	03/2021
Atti	Venere	Siscom	Cloud Siscom	15	03/2021
Albo pretorio		Siscom	Cloud Siscom	3	03/2021
Trasparenza		Siscom	cloud	2	
Bilancio	Giove	Siscom	Cloud Siscom	3	03/2021
Fatture elettroniche	Giove	Siscom	Cloud Siscom	3	03/2021
Stipendi	Alma	Alma		2	01/2018
Presenze	Mercurio	Siscom	Cloud Siscom	3	03/2021
Sito internet		Frequenze		3	07/2019
Sportello Forestale	Regione Piemonte				

Sono inoltre attivi:

Office 365 (file server):
Piattaforma di file server che consente l'utilizzo in locale ed il backup e la fruizione dei file anche in modalità cloud.

Conservazione Sostitutiva parzialmente attiva per i seguenti archivi:

funzione		Integrazione	Token su applicativo	periodicità
Protocollo	Registro giornaliero	Si	Non presente	giornaliera
Atti	Determine Delibere ….	NO	Non presente	N.A.
Fatture	attive passive	NO	Non presente	N.A.
Contratti		NO	Non presente	N.A.
Documenti firmati	Egisto - Olimpo	NO	Non presente	N.A.

Sedi e principali infrastrutture

Attualmente l'ente opera prevalentemente nella sede di Saluzzo con una connettività commerciale Telecom dotata di backup su LTE.

Criticità conosciute e gestite:
L'Ente dispone di una banda internet adeguata agli standard SAAS, tuttavia sono da verificare gli standard di sicurezza relativi alla protezione della rete e delle postazioni di lavoro: oggi l'ente non è dotato di uno strumento di verifica degli endpoint (pdl) e dei presidi richiesti dalle misure minime di sicurezza AGID.

Titolo	***0.1 – Analisi Misure minime di sicurezza***
Descrizione di dettaglio	*Analisi e stima dei principali presidi di sicurezza previste dalle specifiche*
Tempistiche di realizzazione e deadline	*entro il 31/03/2024*
Strutture responsabili e attori coinvolti	*RTD* *Tecnico est. supporto al Responsabile della Transizione al Digitale*
Capitolo di spesa/Fonte di finanziamento	*Da definire*

Obiettivi e spesa complessiva prevista

Il piano rappresenta un'importante occasione per progettare la trasformazione dell'ente sulla base delle indicazioni AGID, la progettazione delle attività parte dall'identificazione degli elementi di informatizzazione ora presenti nell'ente e spesso frutti di scelte dei singoli settori o dettate dalla necessità di rispondere alle vigenti normative e la trasformazione di questi elementi spesso disgiunti in un sistema informativo.
Dobbiamo necessariamente partire da un asset inventory sia delle componenti hardware che di quelle software per comprendere e misurare i singoli componenti, anche in termini contrattuali per identificare lo stato attuale: "as-is" e definire un progetto di armonizzazione ed integrazione dei componenti per poter identificare il "to-be". All'interno

del progetto dobbiamo inserire un'importante componente di crescita delle persone attraverso un progetto di formazione e stimolo continuo, non solo per gli uffici di transizione al digitale ma per l'intero ente al fine di rendere efficace e condiviso il cambiamento.
Ad oggi la connettività Internet rappresenta ancora un problema non completamente risolto per la ridotta banda disponibile e la mancata ridondanza della sede di Lerma; pertanto, una parte della nostra progettazione sarà rivolta alla ricerca di soluzioni al problema.

Strategie:

- Aumentare la digitalizzazione dell'ente per favorire lo sviluppo di una società digitale, per consentire l'accesso ai servizi di cittadini ed imprese
- promuovere lo sviluppo sostenibile, etico ed inclusivo, attraverso l'innovazione e la digitalizzazione al servizio delle persone, delle comunità e dei territori, nel rispetto della sostenibilità ambientale.
- contribuire alla diffusione delle nuove tecnologie digitali nel tessuto produttivo italiano, incentivando la standardizzazione, l'innovazione e la sperimentazione nell'ambito dei servizi pubblici.

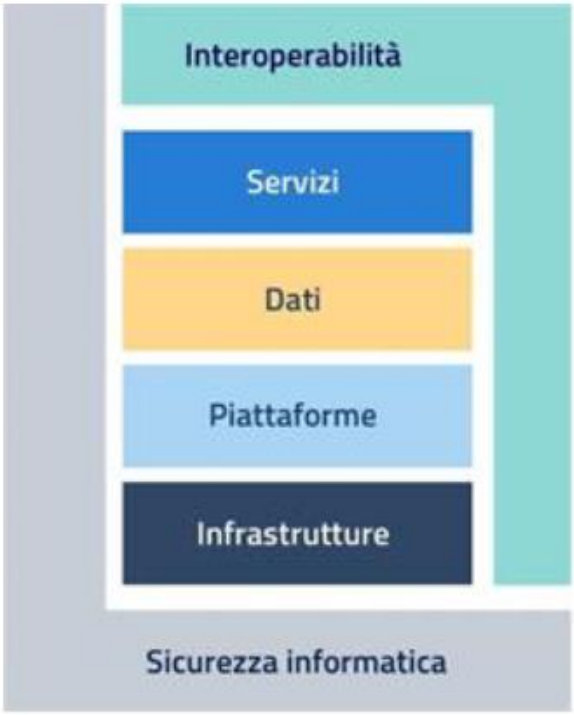
Principi guida:

- digital & mobile first (digitale e mobile come prima opzione): le pubbliche amministrazioni devono realizzare servizi primariamente digitali;
- digital identity only (accesso esclusivo mediante identità digitale): le pubbliche amministrazioni devono adottare in via esclusiva sistemi di identità digitale definiti dalla normativa;
- cloud first (cloud come prima opzione): le pubbliche amministrazioni, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano primariamente il paradigma cloud, tenendo conto della necessità di prevenire il rischio di lock-in;
- servizi inclusivi e accessibili: le pubbliche amministrazioni devono progettare servizi pubblici digitali che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori;
- dati pubblici un bene comune: il patrimonio informativo della pubblica amministrazione è un bene fondamentale per lo sviluppo del Paese e deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile;
- interoperabile by design: i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e senza interruzioni in tutto il mercato unico esponendo le opportune API;
- sicurezza e privacy by design: i servizi digitali devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali;
- user-centric, data driven e agile: le amministrazioni sviluppano i servizi digitali, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo;
- once only: le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite;
- **transfrontaliero by design** (concepito come transfrontaliero): le pubbliche amministrazioni devono rendere disponibili a livello transfrontaliero i servizi pubblici digitali rilevanti;
- **codice aperto**: le pubbliche amministrazioni devono prediligere l'utilizzo di software con codice aperto e, nel caso di software sviluppato per loro conto, deve essere reso disponibile il codice sorgente

Spesa ICT per il triennio 2023-2025	
Annualità	Spesa complessiva
Anno 2023	Euro 22.200,00 (IVA Compresa)
Anno 2024	Euro 20.500,00 (IVA Compresa)
Anno 2025	Euro 20.500,00 (IVA Compresa)

PARTE IIa – LE COMPONENTI TECNOLOGICHE

Schema delle componenti tecnologiche:



CAPITOLO 1. Servizi

Per migliorare la qualità e l'utilizzo dei servizi digitali è indispensabile un approccio multidisciplinare che coniughi l'adozione di metodologie e tecniche interoperabili per la progettazione di un servizio. La semplificazione dei processi interni alle PA, coordinata dal Responsabile per la transizione al digitale, con il necessario supporto di efficienti procedure digitali è la strategia più efficace per ridisegnare i processi.
Fornire servizi completamente digitali, progettati sulla base delle semplificazioni di processo abilitate dalle piattaforme ministeriali di cui al Capitolo 3, del principio cloud first, sia in termini tecnologici, sia in termini di acquisizione dei servizi di erogazione in forma SaaS ove possibile, da preferirsi alla conduzione diretta degli applicativi.
Valutazione e comparazione delle soluzioni open source per massimizzare il riuso del software sviluppato per conto della PA, riducendo i casi di sviluppo di applicativi utilizzati esclusivamente da una singola PA.

Agire su più livelli per generare ed erogare servizi di qualità attraverso:

- un utilizzo più consistente di soluzioni SAAS, (Software as a Service) esistenti e presenti sul marketplace di AGID;
- il riuso e la condivisione di software e competenze tra le diverse amministrazioni;
- 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.

Consultazione preliminare per l'identificazione di soluzioni a disposizione delle amministrazioni:

- le linee guida emanate ai sensi dell'art. 71 del CAD (v. paragrafo "Contesto normativo e strategico");
- Designers Italia;
- Developers Italia;
- Forum Italia.

La progettazione e scelta dei servizi deve essere guidata dalla semplificazione dell'esperienza d'uso e dell'inclusività, in modo che si adattino ai dispositivi degli utenti, senza alcuna competenza pregressa da parte dei cittadini, nel pieno rispetto delle norme riguardanti l'accessibilità e il Regolamento generale sulla protezione dei dati.
Il monitoraggio dei servizi avverrà con l'integrazione di Web Analytics Italia, la piattaforma nazionale open source che offre rilevazioni statistiche su indicatori utili al miglioramento continuo dell'esperienza utente.
Per semplificare e agevolare l'utilizzo del servizio 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 indicato nel capitolo 5.
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 **SPID**. Allo stesso modo, se è richiesto un pagamento, tale servizio dovrà essere reso disponibile anche attraverso il sistema di pagamento **pagoPA**. Da questo punto di vista è da considerare quanto specificato per le Piattaforme già messe a disposizione a livello nazionale per la gestione dei servizi di base (autenticazione, pagamenti, notifiche) nel Capitolo 3 – Piattaforme; l'adozione di queste ultime non solo rende rapida l'implementazione dei servizi necessari, ma accelera il processo di standardizzazione nella PA.
Risulta infine particolarmente rilevante evidenziare lo sviluppo che avrà nel triennio di competenza del presente Piano Triennale **il passaggio dalla PEC alla realizzazione pratica dei SERQ (servizi elettronici di recapito certificato qualificati), in conformità degli articoli 43 e 44 del Regolamento eIDAS n. 910/2014, con l'obiettivo di garantire l'identità di mittente e destinatario e l'interoperabilità dei suddetti servizi a livello europeo.**

Nell'agosto 2022 AGID ha adottato le Regole tecniche per i servizi di recapito certificato qualificato a norma del regolamento eIDAS n. 910/2014 - Criteri di adozione standard ETSI - REM-Policy- IT 1.0, che rappresenta il primo step del percorso che porterà all'adeguamento dalla PEC a SERQ, a seguito dell'approvazione di un apposito DPCM.

Contesto normativo e strategico

Riferimenti normativi italiani:

- Legge 9 gennaio 2004, n. 4 "Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici"
- Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3"
- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (in breve CAD), art. 7, 17, 23, 53, 54, 68, 69 e 71
- Decreto della Presidenza del Consiglio dei Ministri – Dipartimento per l'Innovazione e le Tecnologie del 2 novembre 2005 "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata"
- Decreto Legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla Legge 17 dicembre 2012, n. 221 "Ulteriori misure urgenti per la crescita del Paese"
- Decreto Legge 14 dicembre 2018, n. 135, convertito con modificazioni dalla Legge 11 febbraio 2019, n. 12 "Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione"
- Decreto Legge 9 giugno 2021, n. 80, convertito con modificazioni dalla Legge 6 agosto 2021, n. 113 "Misure urgenti per il rafforzamento della capacità amministrativa delle pubbliche amministrazioni funzionale all'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per l'efficienza della giustizia"
- Decreto Legge 30 aprile 2022, n. 36, convertito con modificazioni dalla Legge 29 giugno 2022, n. 79 "Ulteriori misure urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR)", art. 30 e 32
- Linee Guida AGID su acquisizione e il riuso del software per la Pubblica Amministrazione (2019)
- Linee Guida AGID sull'accessibilità degli strumenti informatici (2020)
- Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici (2021)
- Linee Guida AGID di design per i siti internet e i servizi digitali della PA (2022)
- Circolare AGID n.2/2018, Criteri per la qualificazione dei Cloud Service Provider per la PA
- Circolare AGID n.3/2018, Criteri per la qualificazione di servizi SaaS per il Cloud della PA
- Manuale di abilitazione al cloud AGID (2022)
- Regolamento AGID, 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);
- Determinazione ACN in attuazione al precedente Regolamento n. 306/2022 (con allegato).
- Determinazione ACN in attuazione al precedente Regolamento n. 307/2022 (con allegato).
- Regole tecniche per i servizi di recapito certificato a norma del regolamento eIDAS n. 910/2014 – Criteri di adozione standard ETSI – REMPolicy-IT (2022)
- Piano Nazionale di Ripresa e Resilienza:
    - Investimento 1.3: "Dati e interoperabilità"
    - Investimento 1.4: "Servizi digitali e cittadinanza digitale"

Riferimenti normativi europei:

- Direttiva UE 2016/2102 del Parlamento Europeo e del Consiglio del 26 ottobre 2016 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici

- Regolamento (UE) n. 910/2014 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (eIDAS), art. 43-44
- Regolamento (UE) 2018/1724 del Parlamento Europeo e del Consiglio del 2 ottobre 2018 che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE)

Obiettivi e risultati attesi

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

- R.A.1.1a - Diffusione del modello di riuso di software tra le amministrazioni in attuazione delle Linee Guida AGID sull'acquisizione e il riuso del software per la Pubblica Amministrazione
- R.A.1.1d - Diffusione del monitoraggio, da parte delle Amministrazioni, della fruizione dei servizi digitali

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

- R.A.1.2a - Incremento e diffusione dei modelli standard per lo sviluppo di siti, disponibili in Designers Italia
- R.A.1.2b - Diffusione dei test di usabilità nelle amministrazioni per agevolare il *feedback* e le valutazioni da parte degli utenti
- R.A.1.2c - Incremento dell'accessibilità dei servizi digitali della PA, secondo quanto indicato dalle Linee guida sull'accessibilità degli strumenti informatici

OB.1.3 - Piena applicazione del Regolamento Europeo EU 2018/1724 (Single Digital Gateway)

- R.A.1.3a - Aumento del livello di fruizione delle informazioni, spiegazioni e istruzioni, di cui agli art. 2, 9 e 10 del Regolamento EU 2018/1724
  Target 2023 - Pubblicazione del 100% delle informazioni, spiegazioni e istruzioni rese accessibili dalle autorità municipali
- R.A.1.3b - Realizzazione delle procedure e del sistema tecnico di cui agli art. 6, 13, 14 e 15 del Regolamento EU 2018/1724
  Target 2023 - 100% delle procedure adeguate secondo le specifiche tecniche del Single Digital Gateway

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

- R.A.1.4a - Migrazione dalla PEC ai servizi SERQ
  Target 2023 - 100% PA effettuano il riconoscimento del titolare delle PEC oggetto di migrazione
  Target 2024 - 100% PA migrate su nuovi servizi

Cosa deve fare l'Amministrazione

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

Pubblicazione delle statistiche di utilizzo dei propri siti web e adesione a Web Analytics Italia per migliorare il processo evolutivo dei propri servizi online

Linee di azione ancora vigenti

- Le PA pubblicano le statistiche di utilizzo dei propri siti web e possono, in funzione delle proprie necessità, aderire a Web Analytics Italia per migliorare il processo evolutivo dei propri servizi online - CAP1.PA.LA01
- Le PA dichiarano, all'interno del catalogo di Developers Italia, quali software di titolarità di un'altra PA hanno preso in riuso - CAP1.PA.LA03 → non applicabile

- Le PA che sono titolari di software devono apporre una licenza aperta sul software con le modalità indicate nelle Linee guida su acquisizione e riuso di software in ottemperanza degli articoli 68 e 69 del CAD - CAP1.PA.LA07 → non applicabile

Linee di azione 2022-2024

- Entro ottobre 2022 - Le PA adeguano le proprie procedure di procurement alle Linee Guida di AGID sull'acquisizione del software e al CAD (artt. 68 e 69) - CAP1.PA.LA04
- Entro dicembre 2022 - Le amministrazioni coinvolte nell'attuazione nazionale del Regolamento sul Single Digital Gateway attivano Web Analytics Italia per tutte le pagine da loro referenziate sul link repository europeo - CAP1.PA.LA18
- Entro dicembre 2023 - Almeno i Comuni con una popolazione superiore a 15.000 abitanti, le Città metropolitane, le Province le Università e istituti di istruzione universitaria pubblici, le Regioni e Province autonome attivano uno strumento di rilevazione delle statistiche di utilizzo dei propri siti web che rispetti adeguatamente le prescrizioni indicate dal GDPR - CAP1.PA.LA19

Attività Operative:

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

Linee di azione ancora vigenti:

- Le PA comunicano ad AGID, tramite apposito form online, l'uso dei modelli per lo sviluppo web per i propri siti istituzionali - CAP1.PA.LA14
- Le PA effettuano test di usabilità e possono comunicare ad AGID, tramite l'applicazione form.agid.gov.it, l'esito dei test di usabilità del proprio sito istituzionale - CAP1.PA.LA10
- Le PA devono seguire i principi delle Linee guida di design per i siti internet e i servizi digitali della PA - CAP1.PA.LA26

Linee di azione 2022-2024:

- Entro dicembre 2022 - Le Amministrazioni adeguano i propri siti web rimuovendo, tra gli altri, gli errori relativi a 2 criteri di successo più frequentemente non soddisfatti, come pubblicato sul sito di AGID - CAP1.PA.LA21
- Entro marzo 2023 - Entro 31 marzo 2023 le PA devono pubblicare gli obiettivi di accessibilità sul proprio sito - CAP1.PA.LA16
- Da giugno 2023 - Le PA comunicano al DTD la realizzazione dei siti in adesione agli avvisi della misura 1.4.1 del PNRR - CAP1.PA.LA27
- Entro settembre 2023 - Le PA pubblicano, entro il 23 settembre 2023, tramite l'applicazione form.agid.gov.it, una dichiarazione di accessibilità per ciascuno dei propri siti web e APP mobili - CAP1.PA.LA28
- Entro dicembre 2023 - Le PA comunicano ad AGID, tramite l'applicazione form.agid.gov.it, l'esito dei test di usabilità del proprio sito istituzionale - CAP1.PA.LA23
- Entro dicembre 2023 - Le PA risolvono gli errori relativi al criterio di successo "2.1.1 Tastiera (Livello A)", come rilevato nel campione di siti web monitorato da AGID nel 2021 - CAP1.PA.LA22
- Entro marzo 2024 - Entro il 31 marzo 2024 le PA devono pubblicare gli obiettivi di accessibilità sul proprio sito - CAP1.PA.LA29
- Entro settembre 2024 - Le PA pubblicano, entro il 23 settembre 2024, tramite l'applicazione form.agid.gov.it, una dichiarazione di accessibilità per ciascuno dei propri siti web e APP mobili - CAP1.PA.LA30
- Entro dicembre 2024 - Le PA risolvono gli errori relativi al criterio di successo "4.1.3 Messaggi di stato (Livello AA)", come rilevato nel campione di siti web monitorato da AGID nel 2021 - CAP1.PA.LA31

OB.1.3 - Piena applicazione del Regolamento Europeo EU 2018/1724 (Single Digital Gateway)

(non applicabile alla nostra tipologia di Ente - vedi casi pag. 17 linee guida)

Linee di azione 2022-2024:

- Entro dicembre 2022 - Le Pubbliche amministrazioni competenti rendono accessibili le informazioni, spiegazioni e istruzioni, di cui agli art. 2, 9 e 10 del Regolamento EU 2018/1724, secondo le specifiche tecniche di implementazione - CAP1.PA.LA24
- Entro dicembre 2023 - Le Pubbliche Amministrazioni competenti per i dati necessari all'esecuzione dei procedimenti amministrativi ricompresi nelle procedure di cui all'Allegato II del Regolamento UE 2018/1724, mettono a disposizione dati strutturati ovvero dati non strutturati in formato elettronico secondo ontologie e accessibili tramite API nel rispetto delle specifiche tecniche del Single Digital Gateway. Nel caso di Pubbliche Amministrazioni che rendono disponibili i dati non strutturati, le stesse amministrazioni predispongono la pianificazione di messa a disposizione degli stessi dati in formato strutturato prevedendo il completamento dell'attività entro dicembre 2025 - CAP1.PA.LA25
- Entro dicembre 2023 - Le Pubbliche Amministrazioni competenti per i procedimenti amministrativi relativi alle procedure di cui all'Allegato II del Regolamento UE 2018/1724 adeguano i propri procedimenti amministrativi alle specifiche tecniche di implementazione del Single Digital Gateway - CAP1.PA.LA32

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

Linee di azione 2022-2024:

- Entro dicembre 2023 - Le PA effettuano test per l'integrazione delle applicazioni in uso (ad esempio il protocollo) sul nuovo sistema. Per tali integrazioni si raccomanda alle amministrazioni di utilizzare al meglio i fondi PNRR alla data disponibili - CAP1.PA.LA33
- Entro aprile 2024 - Le PA si rendono pronte all'esercizio delle applicazioni sui nuovi sistemi - CAP1.PA.LA34

Titolo	***1.1 - WAI: adesione a Web Analytics Italia***
Descrizione di dettaglio	*Tutti i siti dell'ente devono integrare le componenti statistiche di WAI*
Tempistiche di realizzazione e deadline	*Wai già integrato nel sito istituzionale*
Strutture responsabili e attori coinvolti	*Servizio Promozione* *Curatore sito internet Frequenze*
Capitolo di spesa/Fonte di finanziamento	*Attraverso risorse interne*

Titolo	***1.2.1 – Migliorare l'esperienza d'uso e l'accessibilità dei servizi***
Descrizione di dettaglio	*L'ente ha effettuato negli scorsi anni un progetto di restyling del sito per aumentare la rispondenza ai criteri sopraesposti; tuttavia, in ragione delle nuove linee guida di design verranno analizzati ulteriori possibili miglioramenti rispetto al sito istituzionale.* *Il progetto deve prevedere la compatibilità con i portali tematici del settore parchi.*
Tempistiche di realizzazione e deadline	*Verifica dei criteri di usabilità attraverso analisi di WAI* *Analisi e rispondenza rispetto alle linee guida di design* *Entro il 30/06/2024 Verranno definiti i criteri di avvio attività* *Entro il 31/12/2024 Verrà rilasciata la prima versione del portale*
Strutture responsabili e attori coinvolti	*Direzione* *Servizio Promozione* *Fornitore del servizio* *Tecnico est. supporto al Responsabile della transizione digitale*
Capitolo di spesa/Fonte di finanziamento	*Infrastrutture e definizione della piattaforma: Progetto finanziato dal Settore parchi della regione Piemonte* *Alimentazione dei contenuti: risorse interne*

Titolo	***1.3 – Piena applicazione del Regolamento Europeo – EU 2018/1724***
Descrizione di dettaglio	*Analisi degli adempimenti relativi al single digital gateway di competenza dell'ente*
Tempistiche di realizzazione e deadline	*Non sono previsti adempimenti per la nostra tipologia di Ente*
Strutture responsabili e attori coinvolti	*Tecnico est. Supporto al Responsabile della transizione digitale*
Capitolo di spesa/Fonte di finanziamento	*Nessun costo previsto*

Titolo	***1.4 – Adeguamento servizi di recapito qualificato a norma EIDAS***
Descrizione di dettaglio	*Analisi degli applicativi che utilizzano la pec, per definire con i relativi fornitori i tempi di adeguamento alle nuove caratteristiche*
Tempistiche di realizzazione e deadline	*Analisi adempimento ed applicativi fruitori entro il 31/03/2024* *Eventuale pianificazione delle attività inerenti all'adempimento 30/06/2024*
Strutture responsabili e attori coinvolti	*Ufficio amministrativo* *Tecnico est. Supporto al Responsabile della transizione digitale*
Capitolo di spesa/Fonte di finanziamento	*Analisi degli adempimenti: contratto con il supporto RTD* *Censimento degli applicativi fruitori: risorse interne* *Pianificazione e relative attività saranno stimate e finanziate a seguito degli esiti di cui ai punti precedenti*

Esperienze acquisite

L'Ente, ormai da 2 anni opera con gli applicativi in cloud, questa esperienza ha consentito di limitare gli investimenti in infrastrutture e di securizzare i dati in modalità cloud ormai da molti anni.

CAPITOLO 2. Dati

La valorizzazione del patrimonio informativo pubblico è un obiettivo strategico per la Pubblica Amministrazione per affrontare efficacemente le nuove sfide dell'economia basata sui dati (data economy), supportare gli obiettivi definiti dalla Strategia europea in materia di dati, garantire la creazione di servizi digitali a valore aggiunto per cittadini, imprese e, in generale, tutti i portatori di interesse e fornire ai policy maker strumenti data-driven da utilizzare nei processi decisionali e/o produttivi.
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, attuato con il Decreto Legislativo n. 200/2021, che ha modificato il Decreto Legislativo n. 36/2006, tale obiettivo strategico può essere perseguito attraverso l'implementazione delle nuove regole tecniche definite con le Linee Guida sui dati aperti.

Sarà inoltre necessario abilitare, attraverso la definizione di una data governance coerente con la Strategia europea, le azioni volte al raggiungimento degli obiettivi definiti attraverso l'utilizzo degli strumenti e delle piattaforme previste dal Piano Nazionale di Ripresa e Resilienza nel sub-investimento M1C1-1.3: la PDND (Piattaforma Digitale Nazionale Dati) e NDC (National Data Catalog - Catalogo Nazionale Dati).

In particolare, la fornitura dei dataset, con riferimento in via prioritaria alle tipologie di dati identificate dalla Direttiva Open Data (come dati dinamici, dati di elevato valore e dati della ricerca), avviene preferenzialmente attraverso API (interfacce per programmi applicativi). Tali dataset devono essere coerenti con i requisiti e le raccomandazioni definiti dalle Linee Guida sui dati aperti che prevedono, tra l'altro, che le relative API:

- rispettino le Linee guida sull'Interoperabilità (ModI);
- siano documentate attraverso i metadati, ontologie e vocabolari controllati, presenti nel Catalogo Nazionale Dati (NDC) per l'interoperabilità semantica;
- siano registrate sul catalogo API della PDND.

In linea con i principi enunciati e in continuità con le azioni avviate con i Piani precedenti, il presente Piano Triennale mira ad assicurare maggiore efficacia all'attività amministrativa in tutti i processi che coinvolgono l'utilizzo dei dati, sia con riferimento alla condivisione dei dati tra pubbliche amministrazioni per finalità istituzionali, sia con riferimento al riutilizzo dei dati, per finalità commerciali e non, secondo il paradigma degli open data.

Un asset fondamentale tra i dati gestiti dalle pubbliche amministrazioni è rappresentato dalle Banche dati di interesse nazionale (art. 60 del CAD) per le quali rimane forte l'esigenza di favorirne l'accesso e la fruibilità, che si concretizzerà attraverso l'implementazione e l'utilizzo della PDND.

Ove applicabile, per l'attuazione delle linee di azione definite di seguito, le PA di piccole dimensioni, come i comuni al di sotto di 5.000 abitanti, possono sfruttare meccanismi di sussidiarietà (ad esempio attraverso le Regioni e Province Autonome, i Comuni capoluogo di provincia, le Unioni dei Comuni, le Città Metropolitane e le Province anche tramite i relativi uffici associati tra quelli esistenti).

A tal proposito, si richiamano le funzioni di raccolta ed elaborazione dati attribuite dalla Legge n. 56 del 2014 alle Province e alle Città Metropolitane, a servizio degli enti locali del territorio.

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 2003/98/CE relativa al riutilizzo di documenti nel settore pubblico
- 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 18 maggio 2015, n.102 - Attuazione della direttiva 2013/37/UE relativa al riutilizzo di documenti nel settore pubblico
- Decreto-legge 16 luglio 2020, n. 76 come convertito dalla Legge 11 settembre 2020, n. 120
- Decreto-legge 31 maggio 2021, n. 77 - Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure.
- Decreto della Presidenza del Consiglio dei Ministri 10 novembre 2011 - Regole tecniche per la definizione del contenuto del Repertorio nazionale dei dati territoriali, nonché delle modalità di prima costituzione e di aggiornamento dello stesso
- Linee guida per la definizione e l'aggiornamento del contenuto del Repertorio Nazionale dei Dati territoriali (in corso di adozione)
- Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico
- Linee guida per i cataloghi dati
- Linee guida per l'implementazione della specifica GeoDCAT-AP
- Manuale RNDT - Guide operative per la compilazione dei metadati RNDT
- Piano Nazionale di Ripresa e Resilienza - Investimento 1.3: "Dati e interoperabilità"

Riferimenti normativi europei:

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

- Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni COM (2020) del 19 febbraio 2020 – Una strategia europea per i dati

Obiettivi e risultati attesi

OB.2.1 - Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese

- R.A.2.1a - Aumento del numero di basi di dati di interesse nazionale che espongono API coerenti con il modello di interoperabilità e con i modelli di riferimento di dati nazionali ed europei
- R.A.2.1b - Aumento del numero di dataset aperti di tipo dinamico in coerenza con quanto previsto dalla Direttiva (UE) 2019/1024, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico, con particolare riferimento alla loro pubblicazione in formato interoperabile tramite API
- R.A.2.1c - Aumento del numero di dataset resi disponibili attraverso i servizi di dati territoriali di cui alla Direttiva 2007/2/EC (INSPIRE)

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

- R.A.2.2a - Aumento del numero di dataset con metadati di qualità conformi agli standard di riferimento europei e nazionali
- R.A.2.2b - Aumento del numero di dataset di tipo aperto resi disponibili dalle pubbliche amministrazioni

OB.2.3 - Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati

- R.A.2.3b - Aumento del numero di dataset di tipo aperto che adottano le licenze previste dalle Linee Guida sui dati aperti

Cosa deve fare l'amministrazione

OB.2.1 - Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese

Linee di azione ancora vigenti

- Le PA e i gestori di servizi pubblici individuano i dataset di tipo dinamico da rendere disponibili in open data coerenti con quanto previsto dalla Direttiva documentandoli nel catalogo nazionali dei dati aperti - CAP2.PA.LA01
- Le PA rendono disponibili i dati territoriali attraverso i servizi di cui alla Direttiva 2007/2/EC (INSPIRE) - CAP2.PA.LA02.
- Le PA titolari di Banche di dati di interesse nazionale avviano l'adeguamento al modello di interoperabilità e ai modelli di riferimento di dati nazionali ed europei delle basi di dati della PA e le documentano nel relativo catalogo delle API - CAP2.PA.LA14
- Le PA documentano le API coerenti con il modello di interoperabilità nei relativi cataloghi di riferimento nazionali - CAP2.PA.LA05

Linee di azione 2022-2024

- Da gennaio 2023 - Le PA attuano le linee guida contenenti regole tecniche per l'implementazione del Decreto Legislativo n. 36/2006 - CAP2.PA.LA17

- Da gennaio 2024 - Le PA attuano le indicazioni presenti nella guida operativa sui dati di elevato valore per l'attuazione del relativo Regolamento di esecuzione (UE) e delle Linee Guida sui dati aperti - CAP2.PA.LA18

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

Linee di azione ancora vigenti

- Le PA adeguano i metadati relativi ai dati geografici all'ultima versione delle specifiche nazionali e documentano i propri dataset nel catalogo nazionale geodati.gov.it - CAP2.PA.LA06
- Le PA adeguano i metadati relativi ai dati non geografici alle specifiche nazionali e documentano i propri dataset nel catalogo nazionale dati.gov.it - CAP2.PA.LA07
- Le PA pubblicano i metadati relativi ai propri dati di tipo aperto attraverso il catalogo nazionale dei dati aperti dati.gov.it - CAP2.PA.LA08

Linee di azione 2022-2024

- Da marzo 2023 - Le PA pubblicano i loro dati aperti tramite API nel catalogo PDND e le documentano anche secondo i riferimenti contenuti nel National Data Catalog per l'interoperabilità semantica - CAP2.PA.LA15
- Da gennaio 2024 - Le PA pubblicano i loro dati aperti ad elevato valore tramite API utilizzando la piattaforma PDND come da Linee Guida sui dati aperti e il riutilizzo dell'informazione del settore pubblico - CAP.PA.LA19
- Da gennaio 2024 - Le PA pubblicano i metadati relativi ai dati di elevato valore, secondo le indicazioni presenti nel Regolamento di esecuzione (UE) e nelle Linee Guida sui dati aperti e relativa guida operativa, nei cataloghi nazionali dati.gov.it e geodati.gov.it - CAP.PA.LA20

OB.2.3 - Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati

Linee di azione ancora vigenti

- Le PA adottano la licenza aperta CC BY 4.0, documentandola esplicitamente come metadato - CAP2.PA.LA09
- Le PA possono, in funzione delle proprie necessità, partecipare a interventi di formazione e sensibilizzazione sulle politiche open data - CAP2.PA.LA11

Linee di azione 2022-2024

- Da gennaio 2023 - 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 - CAP2.PA.LA16
- Da gennaio 2024 - Le PA attuano il Regolamento di esecuzione (UE) relativo ai dati di elevato valore e le relative indicazioni presenti nella guida operativa nazionale per quanto riguarda le disposizioni su licenze e condizioni d'uso da applicare a tale tipologia di dati - CAP2.PA.LA21

Titolo	***2.1 Formazione***
Descrizione di dettaglio	*Acquisizione delle competenze relative al contesto dei dati*
Tempistiche di realizzazione e deadline	*Entro il 2023*
Strutture responsabili e attori coinvolti	*Tutti* *Tecnico est. supporto al Responsabile della transizione digitale*
Capitolo di spesa/Fonte di finanziamento	*Piattaforma Syllabus delle competenze digitali*

Titolo	***2.2 Analisi preliminare delle banche dati in uso e dei procedimenti***
Descrizione di dettaglio	*Censimento dei progetti e delle principali categorie di dati gestiti*
Tempistiche di realizzazione e deadline	*Entro il 31/12/2024*
Strutture responsabili e attori coinvolti	*Servizi competenti in relazione al progetto* *Tecnico est. supporto al Responsabile della transizione digitale*
Capitolo di spesa/Fonte di finanziamento	*Non applicabile*

Esperienze acquisite

Attualmente vengono alimentate le seguenti banche dati:

- https://www.inaturalist.org/
- https://servizi.regione.piemonte.it/catalogo/banche-dati-naturalistiche-bdn
- https://www.regione.piemonte.it/web/temi/ambiente-territorio/montagna/patrimonio-outdoor/recupero-valorizzazione-patrimonio-escursionistico-piemonte-lr-122010
- https://www.dati.piemonte.it/#/catalogodetail/geoportale_regione_csw_isotc211_geoportale_regione_piemonte_r_piemon:af2f6ba1-3093-4160-8cc7-d004c4f5f962

CAPITOLO 3. Piattaforme

Nel capitolo vengono analizzate le piattaforme della Pubblica Amministrazione, che offrono funzionalità fondamentali nella digitalizzazione dei processi e dei servizi della PA.
Le Piattaforme nascono per supportare la razionalizzazione dei processi di back-office o di front-end della PA e sono disegnate per interoperare in modo organico.
Attraverso i loro strumenti, consentono di ridurre il carico di lavoro delle pubbliche amministrazioni, favorendo l'integrazione e l'interoperabilità tra sistemi, sollevandole dalla necessità di dover realizzare ex novo funzionalità, riducendo tempi e costi di attuazione dei servizi e garantendo una maggiore sicurezza informatica.
Le Piattaforme favoriscono la realizzazione di processi distribuiti e la standardizzazione dei flussi di dati tra amministrazioni, nonché la creazione e la fruizione di servizi digitali più semplici e omogenei.
Negli ultimi anni le iniziative intraprese dai vari attori coinvolti nell'ambito del Piano, hanno favorito una importante accelerazione nella diffusione di alcune delle principali piattaforme abilitanti, in termini di adozione da parte delle PA e di fruizione da parte degli utenti. Tra queste la piattaforma dei pagamenti elettronici pagoPA, le piattaforme di identità digitale SPID e CIE, nonché la Piattaforma IO che offre un unico punto d'accesso, tramite un'applicazione mobile, ai servizi pubblici locali e nazionali.
Il Piano, quindi, prosegue nel percorso di evoluzione e consolidamento delle piattaforme previste dalle norme (es. SPID, pagoPA, AppIO, CIE, FSE, NoiPA ecc.) e individua una serie di azioni volte a promuovere i processi di adozione, in forma diretta o intermediata, ad aggiungere nuove funzionalità e ad adeguare costantemente la tecnologia utilizzata e i livelli di sicurezza. Il Piano descrive inoltre lo sviluppo di nuove piattaforme che consentono di razionalizzare i servizi per le amministrazioni e di semplificare tramite l'utilizzo delle tecnologie digitali l'interazione tra cittadini e PA (per la Piattaforma Digitale Nazionale Dati – PDND, si rimanda al Capitolo 5 "Interoperabilità"):
l'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi professionali o nel Registro Imprese (INAD), è l'elenco pubblico contenente i domicili digitali eletti, destinati alle comunicazioni aventi valore legale con la PA.
la Piattaforma Notifiche Digitali (PND) permette la notificazione e la consultazione digitale degli atti a valore legale. In particolare, la piattaforma ha l'obiettivo, per gli enti, di centralizzare la notificazione verso il cittadino o le imprese utilizzando il domicilio digitale eletto e creando un cassetto delle notifiche sempre accessibile (via mobile e via web o altri punti di accesso) con un risparmio di tempo e costi per cittadini, imprese e PA.
il Sistema Gestione Deleghe (SGD) consentirà ai cittadini di delegare l'accesso a uno o più servizi a un soggetto titolare dell'identità digitale.
Una ulteriore piattaforma che entrerà in esercizio nel 2024 è la Piattaforma digitale per l'erogazione di benefici economici concessi dalle amministrazioni pubbliche (denominata IDPay) che ha l'obiettivo di razionalizzare ed efficientare l'attuale gestione delle molteplici iniziative di welfare centrali e locali. Grazie a un sistema di verifica di diritto ai bonus immediato e sicuro, permetterà ai cittadini l'accesso alle agevolazioni al momento dell'acquisto di un bene e servizio con strumenti di pagamento elettronici, mediante terminali fisici o virtuali.

Contesto normativo e strategico

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

Generali:

- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (CAD)
- Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"
- Piano Nazionale di Ripresa e Resilienza:
  - Investimento 1.3: "Dati e Interoperabilità"
  - Investimento 1.4: "Servizi digitali e cittadinanza digitale"

Riferimenti normativi europei:

- Regolamento (UE) n. 910/2014 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (eIDAS)
- Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR)
- Linee Guida CE in materia di Data Protection Impact Assessment (2017)

SPID:

- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (CAD), art.64
- Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014 recante la Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle 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" (2021)
- Linee guida AGID per la fruizione dei servizi SPID da parte dei minori (2022)
- Linee guida AGID recanti le regole tecniche dei gestori di attributi qualificati (2022)

CIE:

- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (CAD), art.66
- Legge 15 maggio 1997, n. 127 "Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e di controllo"
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"
- Decreto Legge 31 gennaio 2005, n. 7, convertito con modificazioni dalla L. 31 marzo 2005, n. 43 "Disposizioni urgenti per l'università e la ricerca, per i beni e le attività culturali, per il completamento di grandi opere strategiche, per la mobilità dei pubblici dipendenti, (e per
- semplificare gli adempimenti relativi a imposte di bollo e tasse di concessione, nonché altre misure urgenti)"
- Decreto Ministeriale del Ministero dell'Interno 23 dicembre 2015 "Modalità tecniche di emissione della Carta d'identità elettronica"
- Regolamento (UE) n. 1157 del 20 giugno 2019 sul rafforzamento della sicurezza delle carte d'identità dei cittadini dell'Unione e dei titoli di soggiorno rilasciati ai cittadini dell'Unione e ai loro familiari che esercitano il diritto di libera circolazione

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, comma 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)

SIOPE+:

- Legge 11 dicembre 2016 "Bilancio di previsione dello Stato per l'anno finanziario 2017 e bilancio pluriennale per il triennio 2017-2019, art. 1, comma 533

INAD:

- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (CAD), art. 3-bis e 6-quater
- Decreto Legge 6 novembre 2021, n. 152, convertito con modificazioni dalla Legge 29 dicembre 2021, n. 233 "Disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per la prevenzione delle infiltrazioni mafiose"
- Linee guida AGID sull'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese (2022)

IO, l'app dei servizi pubblici:

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

Sistema Gestione Deleghe (SGD):

- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (CAD), art. 64-ter
- Decreto della Presidenza del Consiglio dei Ministri – Dipartimento per la trasformazione digitale, 30 marzo 2022, Disciplina delle modalità di funzionamento del Sistema di Gestione Deleghe («SGD»)

Piattaforma Notifiche Digitali:

- Decreto Legge 14 dicembre 2018, n. 135, convertito con modificazioni dalla Legge 11 febbraio 2019, n. 12 "Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione", art. 8
- Legge n. 160 del 2019 "Bilancio di previsione dello Stato per l'anno finanziario 2020 e bilancio pluriennale per il triennio 2020-2022" art. 1, commi 402 e 403
- Decreto Legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 "Misure urgenti per la semplificazione e l'innovazione digitale"
- Decreto Legge 31 maggio 2021, n. 77 "Governance del Piano nazionale di rilancio e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure", art. 38

Obiettivi e risultati attesi

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

- R.A.3.1a - Incremento del livello di alimentazione e digitalizzazione del Fascicolo Sanitario Elettronico con i documenti sanitari da parte delle strutture sanitarie territoriali (ASL/AO/IRCCS) → non applicabile
- R.A.3.1c - Incremento del numero di amministrazioni servite in NoiPA ed estensione del numero di servizi offerti dalla piattaforma (fiscale, previdenziale ecc.) utilizzati → non applicabile

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

- R.A.3.2a - Incremento dell'adozione e dell'utilizzo di SPID e CIE da parte delle Pubbliche Amministrazioni
- R.A.3.2c - Incremento dei servizi sulla piattaforma pagoPA
- R.A.3.2d - Incremento del numero di Amministrazioni scolastiche la cui spesa è consultabile online attraverso SIOPE+ → non applicabile

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

- R.A.3.3a - Incremento dei servizi sulla Piattaforma IO (l'App dei servizi pubblici)
- R.A.3.3b - Realizzazione della Piattaforma Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi professionali o nel Registro Imprese (INAD)
- R.A.3.3d – Realizzazione del Sistema Gestione Deleghe (SGD) digitali al fine di agevolare la fruizione dei servizi online attraverso soggetti delegati
- R.A.3.3e – Realizzazione della Piattaforma Notifiche Digitali (PND)

Cosa deve fare l'Amministrazione

OB.3.1 - Favorire l'evoluzione delle piattaforme esistenti → non applicabile (Fascicolo Sanitario Elettronico – NoiPA)

OB.3.2 – Aumentare il grado di adozione e utilizzo delle piattaforme abilitanti esistenti da parte delle pubbliche amministrazioni

Le linee d'azione rappresentano un elemento cardine del piano triennale. Per ognuna di esse: inserire il titolo; inserire le caratteristiche minime comuni, ossia le attività operative, le dipendenze e la propedeuticità con altre linee; definire lo stato avanzamento della linea d'azione; indicare un orizzonte temporale in cui si intende realizzare la linea d'azione specifica, anche in coerenza con i target e le tempistiche del Piano Triennale di AGID; indicare le strutture o gli uffici responsabili delle attività previste; indicare, se possibile, il capitolo di spesa di riferimento oppure inserire un'indicazione qualitativa della fonte di finanziamento (nazionale/europea) in cui rientrano le attività della specifica linea d'azione.

Linee di azione ancora vigenti:

- Le PA e i gestori di pubblici servizi proseguono il percorso di adesione a SPID e CIE e dismettono le altre modalità di autenticazione associate ai propri servizi online - CAP3.PA.LA07
- 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. - CAP3.PA.LA13
- Le PA devono adeguarsi alle evoluzioni previste dall'ecosistema SPID (tra cui OpenID Connect, servizi per i minori e gestione degli attributi qualificati) - CAP3.PA.LA20

Linee di azione 2022-2024

- Entro dicembre 2023 - Le PA aderenti a pagoPA e App IO assicurano per entrambe le piattaforme 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) - CAP3.PA.LA21
- Entro dicembre 2024 - Le PA aderenti a pagoPA e App IO assicurano per entrambe le piattaforme 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) - CAP3.PA.LA25

OB.3.3 - Incrementare il numero di piattaforme per le amministrazioni ed i cittadini

Linee di azione 2022-2024

● Entro dicembre 2023 - Le PA centrali e i Comuni, in linea con i target sopra descritti e secondo la roadmap di attuazione prevista dal Piano Nazionale di Ripresa e Resilienza (PNRR), dovranno integrarsi alla Piattaforma Notifiche Digitali - CAP3.PA.LA22

● Entro dicembre 2024 - Le PA centrali e i Comuni, in linea con i target sopra descritti e secondo la roadmap di attuazione prevista dal Piano Nazionale di Ripresa e Resilienza (PNRR), dovranno integrarsi alla Piattaforma Notifiche Digitali - CAP3.PA.LA26

Linee di azione:

Titolo	**3.3.1 Censimento servizi oggetto di autenticazione**
Descrizione di dettaglio	Analisi preliminare dei servizi oggetto di autenticazione con raccolta degli elementi minimali: normativa, modulistica, Tipologia, frequenza, ecc.
Tempistiche di realizzazione e deadline	*Entro il 30/06/2024*
Strutture responsabili e attori coinvolti	*Direttore* *Ufficio Amministrativo, Tecnico, Vigilanza* *RTD* *Tecnico est. supporto al Responsabile della transizione digitale*
Capitolo di spesa/Fonte di finanziamento	*Risorse interne*

Titolo	**3.3.2 Notifiche Digitali**
Descrizione di dettaglio	Censimento dei servizi oggetto di autenticazione, raccolta dei moduli, Tipologia, frequenza, fruitori, ecc.
Tempistiche di realizzazione e deadline	*Analisi delle modalità di adesione alla piattaforma - Entro il 30/06/2024* *Eventuale adesione alla piattaforma – entro il 30/06/2025*
Strutture responsabili e attori coinvolti	*Area Vigilanza – Regione Piemonte* *Tecnico est. supporto al Responsabile della transizione digitale*
Capitolo di spesa/Fonte di finanziamento	*Analisi: attraverso Risorse interne* *Adesione alla piattaforma: da definire*

Esperienze acquisite

Sono state attivate e fruite dall'ente le seguenti piattaforme:

- AcquistiretePA (CONSIP – MePA)
- SINTEL
- Piattaforme Regione Piemonte (Servizi SIAP)
- PagoPA

CAPITOLO 4. Infrastrutture

Lo sviluppo delle infrastrutture digitali è parte integrante della strategia di modernizzazione del settore pubblico; esse devono essere affidabili, sicure, energeticamente efficienti ed economicamente sostenibili e garantire l'erogazione di servizi essenziali per il Paese.
L'evoluzione tecnologica espone, tuttavia, i sistemi a nuovi e diversi rischi, anche con riguardo alla tutela dei dati personali. L'obiettivo di garantire una maggiore efficienza dei sistemi non può essere disgiunto dall'obiettivo di garantire contestualmente un elevato livello di sicurezza delle reti e dei sistemi informativi utilizzati dalla Pubblica amministrazione.
Tuttavia, come già rilevato a suo tempo da AGID attraverso il Censimento del Patrimonio ICT della PA, molte infrastrutture della PA risultano prive dei requisiti di sicurezza e di affidabilità necessari e, inoltre, sono carenti sotto il profilo strutturale e organizzativo. Ciò espone il Paese a numerosi rischi, tra cui quello di interruzione o indisponibilità dei servizi e quello di attacchi cyber, con conseguente accesso illegittimo da parte di terzi a dati (o flussi di dati) particolarmente sensibili o perdita e alterazione degli stessi dati.
Lo scenario delineato pone l'esigenza immediata di attuare un percorso di razionalizzazione delle infrastrutture per garantire la sicurezza dei servizi oggi erogati tramite infrastrutture classificate come gruppo B, mediante la migrazione degli stessi verso infrastrutture conformi a standard di qualità, sicurezza, performance e scalabilità, portabilità e interoperabilità.

Con il presente documento, in coerenza con quanto stabilito dall'articolo 33-septies del decreto-legge 18 ottobre 2012, n. 179, si ribadisce che:

- con riferimento alla classificazione dei data center di cui alla Circolare AGID 1/2019 e ai fini della strategia di razionalizzazione dei data center, le categorie "infrastrutture candidabili ad essere utilizzate da parte dei PSN" e "Gruppo A" sono rinominate "A";
- al fine di tutelare l'autonomia tecnologica del Paese, consolidare e mettere in sicurezza le infrastrutture digitali delle pubbliche amministrazioni di cui all'articolo 2, comma 2, lettere a) e c) del decreto legislativo 7 marzo 2005, n. 82, garantendo, al contempo, la qualità, la sicurezza, la scalabilità, l'efficienza energetica, la sostenibilità economica e la continuità operativa dei sistemi e dei servizi digitali, il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei ministri promuove lo sviluppo di un'infrastruttura ad alta affidabilità localizzata sul territorio nazionale, anche detta Polo Strategico Nazionale (PSN), per la razionalizzazione e il consolidamento dei Centri per l'elaborazione delle informazioni (CED) destinata a tutte le pubbliche amministrazioni;
- le amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, nel rispetto dei principi di efficienza, efficacia ed economicità dell'azione amministrativa, migrano i loro Centri per l'elaborazione delle informazioni (CED) e i relativi sistemi informatici, privi dei requisiti fissati dalla Circolare AGID 1/2019 e, successivamente, dal regolamento di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179 (di seguito Regolamento cloud e infrastrutture), verso l'infrastruttura del PSN o verso altra infrastruttura propria già esistente e in possesso dei requisiti fissati dalla Circolare AGID 1/2019 e, successivamente, dal Regolamento cloud e infrastrutture. Le amministrazioni centrali, in alternativa, possono migrare i propri servizi verso soluzioni cloud qualificate, nel rispetto di quanto previsto dalle Circolari AGID n. 2 e n. 3 del 2018 e, successivamente, dal Regolamento cloud e infrastrutture;
- le amministrazioni locali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, nel rispetto dei principi di efficienza, efficacia ed economicità dell'azione amministrativa, migrano i loro Centri per l'elaborazione delle informazioni (CED) e i relativi sistemi informatici, privi dei requisiti fissati dalla Circolare AGID 1/2019 e, successivamente, dal regolamento cloud e infrastrutture, verso l'infrastruttura PSN o verso altra infrastruttura della PA già esistente in possesso dei requisiti fissati dallo stesso regolamento cloud e infrastrutture. Le amministrazioni locali, in alternativa, possono migrare i propri servizi verso soluzioni cloud qualificate nel rispetto di quanto previsto dalle Circolari AGID n. 2 e n. 3 del 2018 e, successivamente, dal Regolamento cloud e infrastrutture;

- le amministrazioni non possono investire nella costruzione di nuovi data center per ridurre la frammentazione delle risorse e la proliferazione incontrollata di infrastrutture con conseguente moltiplicazione dei costi. È ammesso il consolidamento dei data center nel rispetto di quanto previsto dall'articolo 33-septies del DL 179/2012 e dal Regolamento di cui al comma 4 del citato articolo 33-septies.

Nel delineare il processo di razionalizzazione delle infrastrutture è necessario considerare che, nel settembre 2021, il Dipartimento per la Trasformazione Digitale e l'Agenzia per la Cybersicurezza Nazionale (ACN) hanno pubblicato il documento di indirizzo strategico sul cloud intitolato "Strategia Cloud Italia". Tale documento si sviluppa lungo tre direttrici fondamentali: i) la creazione del PSN, la cui gestione e controllo di indirizzo siano autonomi da fornitori extra UE, destinato ad ospitare sul territorio nazionale principalmente dati e servizi strategici la cui compromissione può avere un impatto sulla sicurezza nazionale, in linea con quanto previsto in materia di perimetro di sicurezza nazionale cibernetica dal Decreto Legge 21 settembre 2019, n. 105 e dal DPCM 81/2021; ii) un percorso di qualificazione dei fornitori di cloud pubblico e dei loro servizi per garantire che le caratteristiche e i livelli di servizio dichiarati siano in linea con i requisiti necessari di sicurezza, affidabilità e rispetto delle normative rilevanti e iii) lo sviluppo di una metodologia di classificazione dei dati e dei servizi gestiti dalle Pubbliche Amministrazioni, per permettere una migrazione di questi verso la soluzione cloud più opportuna (PSN o adeguata tipologia di cloud qualificato).
Con riferimento al punto i) creazione del PSN, si è conclusa a luglio 2022 la fase di aggiudicazione della gara europea per l'individuazione dell'operatore economico concessionario mediante partenariato pubblico-privato che si occuperà di realizzare e gestire l'infrastruttura PSN. Inoltre, ad agosto 2022 è stato stipulato il contratto tra il Dipartimento e la nuova società costituita dal RTI aggiudicatario. Le amministrazioni che intendono avviare il percorso di migrazione verso il PSN sono tenute a consultare la documentazione di gara disponibile sul sito cloud.italia.it e contattare il Dipartimento mediante i contatti pubblicati sul medesimo sito.
Con riferimento ai punti ii) qualificazione e iii) classificazione a dicembre 2021 sono stati pubblicati il regolamento cloud e infrastrutture e a gennaio 2022 i relativi atti successivi. Inoltre, la Circolare AGID 1/2022 ha chiarito che in attesa del perfezionamento del trasferimento di competenza ed attribuzioni all'Agenzia per la Cybersicurezza Nazionale (ACN), le attività per la qualificazione dei 39 Cloud Service Provider (CSP) e dei servizi cloud IaaS, PaaS e dei servizi SaaS continueranno a essere svolte da AGID. La classificazione di dati e servizi rappresenta il primo passo operativo per le amministrazioni necessario per identificare la corretta tipologia di cloud verso la quale migrare tali dati e servizi in accordo con la Strategia Cloud Italia e il Regolamento cloud.

Le amministrazioni che devono attuare il processo di migrazione potranno avvalersi dei seguenti strumenti:

- i finanziamenti previsti nel PNRR per un ammontare complessivo di 1,9 miliardi di euro, nello specifico con i due investimenti che mirano all'adozione dell'approccio Cloud first da parte della PA, ovvero "Investimento 1.1: Infrastrutture digitali" (PA Centrali, ASL e Aziende Ospedaliere) e "Investimento 1.2: Abilitazione e facilitazione migrazione al cloud" (Comuni, Scuole, ASL e Aziende Ospedaliere);
- il Manuale di abilitazione al Cloud nell'ambito del Programma nazionale di abilitazione al cloud;
- le Gare strategiche ICT di Consip (es. Accordo Quadro Public Cloud) e gli altri strumenti Consip (MEPA e SDAPA). In particolare, l'Accordo Quadro Public Cloud consentirà alle PA di ridurre, in modo significativo, i tempi di approvvigionamento di servizi public cloud IaaS e PaaS e di servizi professionali per le PA che necessitano di reperire sul mercato le competenze necessarie per attuare quanto previsto nel manuale di abilitazione al cloud. È possibile consultare lo stato di attivazione di questa e di altre gare strategiche ICT attraverso la pagina pubblicata da Consip sul sito Acquisti in Rete PA. Inoltre, con riferimento al MEPA è stata attivata una sezione dedicata alle amministrazioni individuate come soggetti attuatori dell'investimento 1.2.

Per realizzare un'adeguata evoluzione tecnologica e supportare il paradigma cloud, favorendo altresì la razionalizzazione delle spese per la connettività delle pubbliche amministrazioni, è stato aggiornato il modello di connettività. Tale aggiornamento renderà disponibili alle Pubbliche Amministrazioni servizi di connettività avanzati,

atti a potenziare le prestazioni delle reti delle PA e a soddisfare la più recente esigenza di garantire lo svolgimento del lavoro agile in sicurezza.

Contesto normativo e strategico

Riferimenti normativi nazionali:

- Decreto legislativo 7 marzo 2005, n. 82, "Codice dell'amministrazione digitale", 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)
- Piano Nazionale di Ripresa e Resilienza:
    - Investimento 1.1: "Infrastrutture digitali"
    - Investimento 1.2: "Abilitazione e facilitazione migrazione al cloud"

Riferimenti normativi 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 Tof the Council on European data governance (Data Governance Act) (2020)

Obiettivi e risultati attesi

OB.4.1 - Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la strategia "Cloud Italia" e migrando verso infrastrutture e servizi cloud qualificati (incluso PSN)

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

Cosa deve fare l'Amministrazione

Indicatori: Non attuabili
Linee di azione:

Titolo	***4.1 Analisi di Eventuali servizi attivabili in cloud***
Descrizione di dettaglio	L'ente ha sempre utilizzato servizi in cloud, tuttavia verranno effettuate ulteriori analisi per capire se possono essere adottate ulteriori soluzioni in cloud per migliorare la sicurezza.
Tempistiche di realizzazione e deadline	*31/03/2024*
Strutture responsabili e attori coinvolti	*RTD* *Tecnico est. supporto al Responsabile della transizione digitale*
Capitolo di spesa/Fonte di finanziamento	*Analisi dei servizi attraverso risorse interne* *Eventuali costi di migrazione da definire*

Esperienze acquisite

Come specificato nei capitoli precedenti l'Ente adottato soluzioni in cloud per i servizi.

CAPITOLO 5. Interoperabilità

L'interoperabilità permette la collaborazione e l'interazione digitale tra pubbliche amministrazioni, cittadini e imprese, favorendo l'attuazione del principio once only e recependo le indicazioni dell'European Interoperability Framework.
Questo capitolo si concentra sul livello di interoperabilità tecnica e si coordina con gli altri sui restanti livelli: giuridico, organizzativo e semantico. Per l'interoperabilità semantica si consideri il Capitolo 2 "Dati" e il Capitolo 3 "Piattaforme", e per le tematiche di sicurezza il Capitolo 6 "Sicurezza informatica".

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

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

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

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

Nell'ambito del Sub-Investimento **M1C1_1.3.1 "Piattaforma nazionale digitale dei dati**" del Piano Nazionale di Ripresa e Resilienza, sarà realizzata la Piattaforma Digitale Nazionale Dati (PDND). La PDND permette di autorizzare e autenticare le PA alla comunicazione tra i loro sistemi informativi e alla condivisione dei dati a loro disposizione, realizzando l'interoperabilità attraverso l'esposizione di servizi digitali implementati dalle necessarie API. La Piattaforma contribuisce alla realizzazione del principio once only e in futuro, dovrà consentire anche l'accesso ai big data prodotti dalle amministrazioni l'elaborazione di politiche data-driven.
Le PA nell'attuazione del Modello d'interoperabilità devono esporre i propri servizi tramite API conformi alle Linee Guida e registrate sul Catalogo delle API, reso disponibile dalla Piattaforma Digitale Nazionale Dati.

Allo scopo di sviluppare servizi integrati e centrati sulle esigenze di cittadini e imprese, il Dipartimento per la Trasformazione Digitale supporta le PA nell'adozione del Modello di Interoperabilità pianificando e coordinando iniziative di condivisione e accompagnamento per le pubbliche amministrazioni, anche attraverso protocolli d'intesa ed accordi per:

- la costituzione di tavoli e gruppi di lavoro;
- l'avvio di progettualità congiunte;
- la capitalizzazione delle soluzioni realizzate dalla PA in open source ecc.

Si tratta di iniziative di raccordo operativo per abilitare l'interoperabilità tra le PA e per supportare:

- la reingegnerizzazione dei processi e la digitalizzazione di procedure analogiche, la progettazione di nuovi sistemi e servizi;
- il processo di diffusione e adozione delle piattaforme abilitanti di livello nazionale, nonché la razionalizzazione delle piattaforme esistenti;
- l'attuazione del Modello di Interoperabilità in specifici contesti in cui le Pubbliche Amministrazioni interagiscono tramite API.

In attuazione del DPR 160/2010 è stato infine attivato un gruppo tecnico per la stesura delle "specifiche tecniche SUAP" che attuano il Modello di Interoperabilità al contesto dei SUAP definendo le modalità telematiche per la comunicazione e il trasferimento dei dati tra lo Sportello Unico Attività Produttive (SUAP) e tutti gli enti coinvolti nei procedimenti attivati dallo stesso SUAP.

Contesto normativo e strategico

Riferimenti normativi italiani:

- Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"
- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (in breve CAD), artt. 12, 15, 50, 50-ter, 73, 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 Dati per l'interoperabilità dei sistemi informativi e delle basi di dati (2021)
- Decreto 12 novembre 2021 del Ministero dello sviluppo economico di modifica dell'allegato tecnico del decreto del Presidente della Repubblica 7 settembre 2010, n. 160
- Piano Nazionale di Ripresa e Resilienza:
    - Investimento M1C1 1.3: "Dati e interoperabilità"
    - Investimento M1C1 2.2: "Task Force digitalizzazione, monitoraggio e performance"

Riferimenti normativi europei:

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

Obiettivi e risultati attesi

OB.5.1 - Favorire l'applicazione della Linea Guida sul Modello di Interoperabilità da parte degli erogatori di API

OB.5.2 - Adottare API conformi al Modello di Interoperabilità

OB.5.3 - Modelli e regole per l'erogazione integrata di servizi interoperabili

Cosa deve fare l'Amministrazione

Verificare con i riferimenti regionali se sussistono linee di azione per l'Ente

Indicatori: Non attuabili nel piano

Linee di azione:

Titolo	**5.1 Formazione**
Descrizione di dettaglio	Formazione sull'argomento utilizzando la piattaforma Syllabus delle competenze
Tempistiche di realizzazione e deadline	*L'ente è già attivo sulla piattaforma* *Entro il 30/06/2024*
Strutture responsabili e attori coinvolti	*Tutti i settori dell'ente*
Capitolo di spesa/Fonte di finanziamento	*La piattaforma è gratuita*

Esperienze acquisite

Nel 2023 l'Ente ha svolto in collaborazione con il supporto RTD una formazione preliminare sul syllabus e sulla classificazione dei dati, in cui veniva condiviso anche il percorso relativo al PTTD. I riscontri sono stati positivi sia in ragione della partecipazione che negli esiti dei test valutativi.

CAPITOLO 6. Sicurezza informatica

La Direttiva NIS 2, di prossima pubblicazione sulla Gazzetta Ufficiale dell''UE e destinata ad abrogare la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, pone particolare rilevanza all'innalzamento dei livelli di cybersecurity delle reti e dei sistemi informativi degli Stati membri includendo, nel suo ambito di applicazione, le Pubbliche Amministrazioni Centrali – salvo alcune eccezioni tra le quali Banche Centrali, Parlamenti ed Enti operanti in ambito giudiziario – nonché le Amministrazioni regionali, sulla base, per quest'ultime, di una valutazione del rischio e laddove forniscano servizi la cui interruzione potrebbe avere un impatto significativo su attività critiche, sociali ovvero economiche. Benché alle citate Amministrazioni, centrali e regionali, non si applichino le sanzioni previste dalla Direttiva, esse sono soggette agli stessi obblighi previsti per gli altri soggetti essenziali/importanti contemplati dalla Direttiva NIS 2.
Tale obiettivo viene altresì perseguito dalla Strategia Nazionale di Cybersicurezza 2022-2026 e dal relativo Piano di implementazione, attualmente in fase di definizione relativamente al modello di misurazione dell'implementazione delle tempistiche e dei target delle misure, che contemplano una serie di azioni volte a rafforzare la cybersecurity delle PA, sia intervenendo a livello tecnico, sia accrescendo la consapevolezza e le competenze dei pubblici dipendenti e degli utenti dei servizi pubblici.
Appare infatti essenziale garantire servizi digitali non solo efficienti e facilmente accessibili, ma anche sicuri e resilienti sotto il profilo informatico, così da accrescerne l'affidabilità e l'utilizzo anche da parte di utenti meno avvezzi all'impiego di tecnologie digitali. La crescente risonanza e copertura mediatica data ad incidenti e ad attacchi cyber, se da un lato contribuisce ad accrescere il livello di consapevolezza sui rischi dello spazio cibernetico, dall'altro può ingenerare un senso di insicurezza nell'impiego dello strumento digitale.
Per superare tali timori è quindi essenziale un approccio olistico alla cybersecurity, attraverso una gestione continuativa ed automatizzata del rischio cyber, che contempli un'architettura "zero trust", per la cui implementazione è essenziale la collaborazione degli utenti, interni ed esterni alla PA, ma anche dei fornitori di beni e servizi ICT.
A partire dall'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN), è tuttora in fase di revisione l'architettura nazionale cyber, tramite il progressivo trasferimento di competenze dai soggetti che ne esercitavano le funzioni alla stessa ACN: per tale motivo, come meglio descritto in seguito, i target e le linee di azione relative al triennio di competenza del Piano potranno essere integrati a seguito della definizione di appositi indicatori del Piano di implementazione della Strategia Nazionale di Cybersicurezza 2022-2026.

Contesto normativo e strategico

Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (in breve CAD), art.51
- Decreto Legislativo 18 maggio 2018, n. 65 - Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione
- Decreto del Presidente del Consiglio dei Ministri 8 agosto 2019 - Disposizioni sull'organizzazione e il funzionamento del computer security incident response team - CSIRT italiano
- Decreto Legge 21 settembre 2019, n. 105 - Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica
- Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del Decreto Legge 21 settembre 2019, n.105, convertito,

con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misura volte a garantire elevati livelli di sicurezza
- Decreto Legge 14 giugno 2021 n. 82 – Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la Cybersicurezza Nazionale
- Decreto del Presidente del Consiglio dei Ministri 17 maggio 2022 - Adozione della Strategia nazionale di cybersicurezza 2022-2026 e del Piano di implementazione 2022-2026
- Linee guida sulla sicurezza nel procurement ICT (2020)
- Misure minime di sicurezza ICT per le pubbliche amministrazioni
- Piano Nazionale per la Protezione Cibernetica 2017
- Piano Nazionale di Ripresa e Resilienza - Investimento 1.5: "Cybersecurity"

Riferimenti normativi europei:

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

Obiettivi e risultati attesi

Come ricordato nell'introduzione, il trasferimento all'Agenzia per la Cybersicurezza Nazionale (ACN), ai sensi del Decreto Legge n. 82/2021, di tutte le competenze in materia di cybersicurezza e cyber resilience, ha determinato una profonda revisione dell'Architettura Nazionale Cyber, e, di conseguenza, del presente capitolo, anche alla luce dell'adozione, il 17 maggio 2022, della Strategia Nazionale di Cybersicurezza 2022-2026 e dell'annesso Piano di implementazione.
Al riguardo, le principali misure che si applicano alle Pubbliche Amministrazioni sono quelle numero 6, 10, 11, 14, 19, 20, 55, 58, 59, 70 e 71 del citato Piano. Gli obiettivi da raggiungere sono definiti in un apposito documento – in fase di elaborazione da parte dell'ACN, con il contributo delle Amministrazioni responsabili per la concreta implementazione delle citate misure – nel quale sono individuate metriche e indicatori di misurazione, sulla base dei quali saranno calcolati, per ciascuna misura, i Key Performance Indicator (KPI), i quali saranno misurati a partire dal secondo anno di esercizio (2023). Ciò, in attuazione della misura numero 82 del Piano di implementazione. Obiettivi ed indicatori saranno contemplati nel prossimo aggiornamento del Piano triennale.
Nel presente paragrafo e nei successivi sono quindi descritti gli obiettivi e i relativi risultati attesi, le linee di azione da parte dei soggetti owner con competenza sulla cybersicurezza, e quelle da parte delle PA, con riferimento temporale massimo al 2022.

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

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

Cosa deve fare l'Amministrazione

Linee di azione:

Titolo	**6.1 – Formazione Competenze digitali**
Descrizione di dettaglio	Syllabus. Piattaforma telematica sviluppata dal Dipartimento della Funzione Pubblica che eroga una formazione personalizzata, in modalità e-learning, al personale dell'Ente registrato, al fine di rafforzare le conoscenze, svilupparne di nuove, la produttività e la capacità digitale nelle amministrazioni.
Tempistiche di realizzazione e deadline	*30/06/2024*
Strutture responsabili e attori coinvolti	*Tutti i settori dell'ente*
Capitolo di spesa/Fonte di finanziamento	*https://www.syllabus.gov.it/syllabus/offerta-formativa/*

Titolo	***6.2 – Formazione Cyber security***
Descrizione di dettaglio	*Fruizione della specifica sezione del portale Syllabus, piattaforma telematica sviluppata dal Dipartimento della Funzione Pubblica che eroga una formazione personalizzata, in modalità e-learning, al personale dell'Ente registrato, al fine di rafforzare le conoscenze, svilupparne di nuove, la produttività e la capacità digitale nelle amministrazioni. Fruizione di una formazione frontale preparatoria al modulo e specifica per Enti Parco.*
Tempistiche di realizzazione e deadline	*Formazione frontale introduttiva a cura del Tecnico est. supporto al Responsabile della transizione digitale svolta nel 2023* *Fruizione piattaforma Syllabus entro 30/06/2024*
Strutture responsabili e attori coinvolti	*Tutti i settori dell'ente* *Tecnico est. supporto al Responsabile della transizione digitale*
Capitolo di spesa/Fonte di finanziamento	*https://www.syllabus.gov.it/syllabus/offerta-formativa/*

Titolo	***6.3 – Formazione su Linee guida EPDB su incident e data breach***
Descrizione di dettaglio	*Formazione frontale sulle linee guida EPDB e definizione dei registri e dei procedimenti*
Tempistiche di realizzazione e deadline	*30/06/2024*
Strutture responsabili e attori coinvolti	*Tutti i settori dell'ente* *Tecnico est. supporto al Responsabile della transizione digitale*
Capitolo di spesa/Fonte di finanziamento	*https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf*

Titolo	***6.4 Misurazione del livello di rischio***
Descrizione di dettaglio	*Analisi del rischio attraverso questionari*
Tempistiche di realizzazione e deadline	*30/06/2024*
Strutture responsabili e attori coinvolti	*Servizio Tecnico* *RTD* *Tecnico est. supporto al Responsabile della transizione digitale*
Capitolo di spesa/Fonte di finanziamento	*Risorse interne – supporto RTD*

Titolo	**6.5 Progettazione ed analisi degli interventi per ridurre il livello di rischio**
Descrizione di dettaglio	In ragione delle risultanze dell'analisi di cui al punto 6.4 verranno progettati e schedulati interventi per ridurre il fattore di rischio
Tempistiche di realizzazione e deadline	*31/12/2024*
Strutture responsabili e attori coinvolti	*Direzione* *RTD*
Capitolo di spesa/Fonte di finanziamento	*Risorse interne – supporto RTD*

Esperienze acquisite

L'ente non ha ancora acquisito una piattaforma SIEM, (Security Information and Event Management), per centralizzare registri e altre informazioni relative alla sicurezza dei sistemi.

PARTE IIIa - La governance

CAPITOLO 8. Governare la trasformazione digitale

La terza sezione è dedicata alla «Governance», in cui descrivere i soggetti coinvolti, le modalità di interazione, gli strumenti/interventi per il coinvolgimento del territorio e dove dettagliare le modalità di governance adottate dal RTD e dal team per la gestione e il monitoraggio dello sviluppo delle linee d'azione.
In base a quanto descritto nella Guida per la redazione format del Piano triennale per le pubbliche amministrazioni, le iniziative di governance, in generale, si focalizzano su diversi ambiti tra cui:

- Monitoraggio, dello stato di attuazione delle iniziative proposte nel PT di riferimento;
- Rafforzamento delle competenze, attraverso iniziative formative di valutazione e di valorizzazione delle competenze digitali dei dipendenti;
- Mentre gli obiettivi sono:
  - Rafforzare gli strumenti dell'Amministrazione per l'attuazione del Piano, costruendo un sistema condiviso di obiettivi e di indicatori di performance;
  - Individuare le azioni e gli strumenti di raccordo con il territorio e di interazione con tutti gli stakeholder;
  - Sviluppare il capitale umano, attraverso il rafforzamento delle competenze;

Obiettivi e risultati attesi

Nella prima definizione del piano verranno raccolti gli obbiettivi presenti nei vari capitoli e costituiranno un puntuale riferimento delle attività da svolgere ed il relativo monitoraggio.

Cosa deve fare l'Amministrazione

Titolo	**8.1 Definizione di un riepilogo degli obiettivi**
Descrizione di dettaglio	Realizzazione di un riepilogo degli obbiettivi con gestione temporale degli stessi (Gantt)
Tempistiche di realizzazione e deadline	*31/12/2023*
Strutture responsabili e attori coinvolti	*Tecnico est. supporto al Responsabile della transizione digitale*
Capitolo di spesa/Fonte di finanziamento	*Non sono previsti costi da sostenere*

APPENDICE 1. Acronimi

- **AGID**: è l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizza-zione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica;
- **API**: un insieme di procedure (in genere raggruppate per strumenti specifici) atte all'espletamento di un dato compito;
- **Amministratori di sistema**: soggetti deputati a intervenire per garantire l'efficienza e la funzionalità di un determinato sistema informatico, aventi la possibilità di accedere a dati personali qualora l'accesso sia assolutamente necessario per raggiungere le finalità proprie del ruolo ricoperto; secondo le misure minime di sicurezza gli amministratori di sistema devono accedere con le proprie utenze amministrative e solo in casi particolari e documentati possono accedere con l'utenza Administrator generica;
- **ANPR**: Anagrafe nazionale della popolazione residente, è il registro anagrafico centrale del Ministero dell'interno della Repubblica Italiana;
- **Antivirus**: Programma in grado di riconoscere un virus presente in un file e di eliminarlo o di renderlo inoffensivo;
- **Apparati attivi**: apparecchiature hardware collegate alla rete che ne permettono il funzionamento;
- Aree condivise: spazi di memorizzazione messi a disposizione degli utenti sui sistemi centralizzati per la condivisione e lo scambio di files;
- **Attachment**: (attaccamento) File allegato: può essere un allegato alla posta elettronica o a qualsiasi software di gestione dei file;
- **Backup**: procedura per la duplicazione dei dati su un supporto esterno o distinto da quello sul quale sono memorizzati, in modo da garantirne una copia di riserva;
- **Banda**: Quantità di dati per unità di tempo che può viaggiare su una connessione. Nella banda ampia la velocità varia da 64 Kbps a 1,544 Mbps. Nella banda larga la comunicazione avviene a velocità superiori a 1,544 Mbps;
- **CAD**: Codice dell'amministrazione digitale: norma che riunisce in sé diverse norme emanate tra il 1997 e il 2005 riguardanti l'informatizzazione della pubblica amministrazione, ed in particolare il documento informatico, la firma elettronica e la firma digitale, delle quali stabilisce l'equivalenza con il documento cartaceo e con la firma autografa;
- **CERT_PA**: Computer Emergency Readiness/Response Team. In sostanza, si tratta di una speciale squadra attiva per dare subito risposta in caso di emergenze informatiche all'interno della pubblica amministrazione. CERT-PA opera all'interno dell'AgID, l'Agenzia per l'Italia Digitale;
- **CONSIP**: è la centrale acquisti della pubblica amministrazione italiana; è una società per azioni il cui unico azionista è il Ministero dell'economia e delle finanze del governo italiano ed opera nell'esclusivo interesse dello Stato;
- **Cookie**: Tradotto letteralmente significa biscotto. È un file memorizzato sul proprio computer che identifica il computer quando è collegato ad alcuni siti Internet;
- **Classificazione Data Center**:
    - **Gruppo A** - Data center di qualità che non sono stati eletti a Polo strategico nazionale, oppure con carenze strutturali o organizzative considerate minori. Come indicato in seguito, queste strutture potranno continuare ad operare ma non potranno essere effettuati investimenti per l'ampliamento o l'evoluzione. Dovranno comunque garantire continuità dei servizi e disaster recovery, fino alla completa migrazione, avvalendosi dei servizi disponibili con il Contratto quadro SPC Cloud lotto 1 o messi a disposizione dai Poli strategici nazionali;
    - **Gruppo B** - Data center che non garantiscono requisiti minimi di affidabilità e sicurezza dal punto di vista infrastrutturale e/o organizzativo, o non garantiscono la continuità dei servizi. Queste

infrastrutture dovranno essere rapidamente consolidate verso uno dei Poli strategici nazionali o verso il cloud tramite i servizi disponibili con il Contr. quadro SPC Cloud lotto 1;

- **Cloud**: indica un paradigma di erogazione di servizi offerti on demand da un fornitore ad un cliente finale attraverso la rete Internet. Il cloud è un modello che consente di disporre, tramite internet, di un insieme di risorse di calcolo (ad es. reti, server, storage, applicazioni e servizi) che possono es-sere erogate come un servizio;
- **Cloud Market Place AgID**: è la piattaforma che espone i servizi e le infrastrutture qualificate da AgID secondo quanto disposto dalle Circolari AgID n. 2 e n.3 del 9 aprile 2018. All'interno del Cloud Marketplace è possibile visualizzare la scheda tecnica di ogni servizio che mette in evidenza le caratteristiche tecniche, il modello di costo e i livelli di servizio dichiarati dal fornitore in sede di qualificazione;
- **CIE**: La carta d'identità elettronica italiana è un documento di riconoscimento previsto in Italia dalla legge. Ha sostituito la carta d'identità in formato cartaceo nella Repubblica Italiana. La carta di identità elettronica attesta l'identità del cittadino;
- **CSIRT**: Computer security incident response team) Il CSIRT Italiano è stato istituito presso il Dipartimento delle informazioni per la Sicurezza della Presidenza del Consiglio dei Ministri (DIS) con l'obiettivo di ottimizzare l'efficacia della prevenzione e della risposta del Paese a fronte di eventi di natura cibernetica a danno di soggetti pubblici e privati;
- **CSP**: Cloud Service Provider – Fornitori di servizi in cloud;
- **Data breach**: incidente di sicurezza in cui dati sensibili, riservati, protetti vengono consultati, copiati, trasmessi, rubati o utilizzati da soggetti non autorizzati;
- **Dati personali**: dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale, dati inerenti lo stile di vita la situazione economica, finanziaria, patrimoniale, fiscale, dati di connessione: indirizzo IP, login, altro, dati di localizzazione: ubicazione, GPS, GSM, altro;
- **DNS** (Domain Name System): Sistema che gestisce gli indirizzi dei domini Internet;
- **DPIA**: Data Protection Impact Assessment" oppure "Valutazione d'impatto sulla protezione dei dati" è una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali;
- **EGAP**: Ente di Gestione delle Aree Protette;
- **Firewall**: apparato di rete hardware o software che filtra tutto il traffico informatico in entrata e in uscita e che di fatto evidenzia un perimetro all'interno della rete informatica e contribuisce alla sicurezza della rete stessa;
- **Garante Privacy o GPGP**: il Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996 n. 765, quale autorità amministrativa pubblica di controllo indipendente;
- **Indirizzamento**: attività di assegnazione di indirizzi logici ad apparati attivi;
- **Integrità**: la protezione contro la perdita, la modifica, la creazione o la replica non autorizzata delle informazioni ovvero la conferma che i dati trattati siano completi;
- **IP**: Indirizzo che permette di identificare in modo univoco un computer collegato in rete. Si suddivide in due parti, la prima individua la rete dove si trova il computer, la seconda individua il computer all'interno di quella rete;
- **Interoperabilita**: caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi;
- **IPSEC Internet Protocol Security:** è una collezione di protocolli implementati che fornisce un metodo per garantire la sicurezza del protocollo IP, sia esso versione 4 sia 6, e dei protocolli di livello superiore (come ad

esempio UDP e TCP), proteggendo i pacchetti che viaggiano tra due sistemi host, tra due security gateway (ad esempio router o firewall) oppure tra un sistema host e una security gateway;

- **Linee guida o policy**: regole operative tecniche e/o organizzative atte a guidare i processi lavorativi, decisionali e attuativi;
- **Log**: file che registra attività di base quali l'accesso ai computer e che è presente sui server della rete informatica;
- **Logging**: attività di acquisizione cronologica di informazioni attinenti all'attività effettuata sui sistemi siano essi semplici apparati o servizi informatici;
- **Misure minime di sicurezza**: le misure minime di sicurezza ICT emanate dall'AgID, sono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti;
- **NAS**: Network Attached Storage è un dispositivo collegato alla rete la cui funzione è quella di consentire agli utenti di accedere e condividere una memoria di massa, in pratica costituita da uno o più dischi rigidi, all'interno della propria rete. In ambiente NetApp tale dispositivo prende il nome di FAS;
- **Office automation**: software di produttività individuale quali ad esempio Microsoft office o Libreoffice: videoscrittura, foglio elettronico, presentazioni e database;
- **Open data**: formato aperto: un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi;
- **PagoPA**: é un sistema di pagamenti elettronici realizzato per rendere più semplice, sicuro e trasparente qualsiasi pagamento verso la Pubblica Amministrazione;
- **Policy**: modello di configurazione e adattamenti da riferirsi a gruppi di utenti o a uso del software;
- **Policy di riferimento**: documento tecnico che descrive lo stato attuale delle policy in uso, aggiorna-to periodicamente in funzione dell'evoluzione tecnologica/organizzativa;
- **Postazione di lavoro o pdl**: dispositivo (personal computer, notebook, thin/fat client, ecc.) che consente l'accesso al proprio ambiente di lavoro informatico;
- **Protocollo**: insieme di regole che definisce il formato dei messaggi scambiati tra due unità informatiche e che consente loro di comunicare nonché di comprendere la comunicazione;
- **PSN**: Poli strategici nazionali: il soggetto titolare dell'insieme di infrastrutture IT (centralizzate o distribuite), ad alta disponibilità, di proprietà pubblica, eletto a Polo Strategico Nazionale dalla Presidenza del Consiglio dei Ministri e qualificato da AgID ad erogare, in maniera continuativa e sistematica, ad altre amministrazioni;
- **Responsabile del trattamento**: il Dirigente/Responsabile P.O., oppure il soggetto pubblico o priva-to, che tratta dati personali per conto del Titolare del trattamento;
- **RDP** (Remote Desktop Protocol): è un protocollo di rete proprietario sviluppato da Microsoft, che permette la connessione remota da un computer a un altro in maniera grafica;
- Responsabile per la protezione dati – **RPD** o Data Protection Officer - **DPO**: il dipendente della struttura organizzativa del Comune, il professionista privato o impresa esterna, incaricati dal Titolare o dal Responsabile del trattamento;
- **Registri delle attività di trattamento**: elenchi dei trattamenti in forma cartacea o telematica tenuti dal Titolare e dal Responsabile del trattamento secondo le rispettive competenze;
- **Rete dati**: insieme dell'infrastruttura passiva (cavi, prese, ecc.) e degli apparati attivi (modem, router, ecc.) necessari alla interconnessione di apparati informatici;
- **Sandbox**: è un processo di rete che consente di inviare i file a un dispositivo separato, da ispezionare senza rischiare la sicurezza della rete. Ciò consente il rilevamento di minacce che potrebbero aggirare altre misure di sicurezza, comprese le minacce zero-day;
- **SIOPE+:** è la nuova infrastruttura che intermedierà il colloquio tra pubbliche amministrazioni e banche tesoriere con l'obiettivo di migliorare la qualità dei dati per il monitoraggio della spesa pubblica e per rilevare i tempi di pagamento delle Pubbliche Amministrazioni nei confronti delle imprese fornitrici;

- **Software web-based**: ha interfaccia web e non ha prerequisiti e dipendenze obbligatorie (ad esempio plug-in sul dispositivo) ed è mobile first;
- **SPC**: Sistema Pubblico di Connettività e cooperazione (SPC) è una cornice nazionale di interoperabilità: definisce, cioè, le modalità preferenziali che i sistemi informativi delle pubbliche amministra-zioni devono adottare per essere tra loro interoperabili;
- **SPC2**: Sistema pubblico di connettività e cooperazione fase 2;
- **SPCCloud**: Sistema pubblico di connettività e cooperazione in cloud per l'erogazione di servizi a favore della Pubblica amministrazione;
- **SPID**: Sistema Pubblico di Identità Digitale, è la soluzione che ti permette di accedere ai servizi on-line della Pubblica Amministrazione e dei soggetti privati aderenti con un'unica Identità Digitale (username e password) utilizzabile da computer, tablet e smartphone;
- **SSL**: Secure Sockets Layer: protocollo crittografico usato nel campo delle telecomunicazioni e dell'informatica che permette una comunicazione sicura dalla sorgente al destinatario (end-to-end) su reti TCP/IP (ad esempio Internet) fornendo autenticazione, integrità dei da-ti e confidenzialità operando al di sopra del livello di trasporto;
- **Titolare del trattamento**: l'autorità pubblica (il Comune o altro ente locale) che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali;
- **URL (Uniform Resource Locator)**: Identifica in modo univoco le informazioni presenti su Internet, un indirizzo dal quale si richiamano le informazioni;
- **Utente**: persona fisica autorizzata ad accedere ai servizi informatici dell'Ente;
- **VOIP**: (Voice over IP) tecnologia che rende possibile effettuare una comunicazione telefonica sfruttando il protocollo IP della rete dati;
- **VPN**: Virtual Private Network, è una rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico, condiviso e sicuro attraverso la rete internet.