



Ministero delle Imprese e del Made in Italy

DIREZIONE GENERALE PER LE RISORSE, L'ORGANIZZAZIONE, I SISTEMI INFORMATIVI E IL BILANCIO
DIVISIONE V – SISTEMI INFORMATIVI E TRASFORMAZIONE DIGITALE

Piano Triennale per la transizione digitale 2023-2025 del Ministero delle Imprese e del Made in Italy

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

Il Responsabile della Transizione Digitale

Aurelio La Corte

0 INDICI

Indice delle sezioni

0	INDICI	2
1	SCOPO E PREMESSA DEL DOCUMENTO	5
2	INTRODUZIONE	6
3	IL CONTESTO DI RIFERIMENTO.....	7
3.1	Missione istituzionale del Ministero	7
3.2	Modello Organizzativo del Ministero.....	8
3.3	Ruolo del Responsabile per la Transizione al Digitale.....	11
3.4	Organigramma del Ministero	14
3.5	Visione strategica trasversale	14
4	VISIONE DELL'AMMINISTRAZIONE.....	15
5	APPROCCIO METODOLOGICO	16
6	IL PIANO TRIENNALE IT	18
6.1	Componenti tecnologiche AgID	18
6.1.1	A. Servizi	19
6.1.1.1	Obiettivi AgID.....	19
6.1.1.2	Definizione AS-IS.....	20
6.1.2	B. Dati	21
6.1.2.1	Obiettivi AgID.....	22
6.1.2.2	Definizione AS-IS.....	22
6.1.3	C. Piattaforma	23
6.1.3.1	Obiettivi AgID.....	23
6.1.3.2	Definizione AS-IS.....	24
6.1.4	D. Infrastruttura	25
6.1.4.1	Obiettivi AgID.....	25
6.1.4.2	Definizione AS-IS.....	26
6.1.5	E. Interoperabilità.....	27
6.1.5.1	Obiettivi AgID.....	28
6.1.5.2	Definizione AS-IS.....	29
6.1.6	F. Sicurezza Informatica	29

6.1.6.1	Obiettivi AgID	30
6.1.6.2	Definizione AS-IS	31
6.2	Introduzione alle Linee Programmatiche	32
6.2.1	Linea programmatica: Workspace e Digital Adoption	33
6.2.2	Linea programmatica: Razionalizzazione del catalogo dei servizi	34
6.2.3	Linea programmatica: Migrazione al Cloud	35
6.2.4	Linea Programmatica: Miglioramento delle modalità di erogazione del Servizio	36
6.2.5	Linea programmatica: Sicurezza informatica e <i>disaster recovery</i>	38
6.2.6	Linea programmatica: Dematerializzazione e conservazione sostitutiva	39
6.2.7	Linea programmatica: Definizione di un nuovo modello e pratiche di <i>Data Governance</i>	41
6.2.8	Linea programmatica: Razionalizzazione del parco applicativo	42
6.2.9	Linea programmatica: Razionalizzazione e ridisegno del Modello Operativo IT (Processi, procedure e standard)	43
7	ROADMAP DEL PIANO ICT	45
8	MODELLO DI GOVERNANCE	45
9	INIZIATIVE IN CORSO	46
10	APPENDICE A – Normativa e linee guida di riferimento	47
10.1	Normativa di riferimento sui Servizi	47
10.2	Normativa di riferimento sui Dati	48
10.3	Normativa di riferimento sulle Piattaforme.....	49
10.4	Normativa di riferimento Infrastrutture	52
10.5	Normativa di riferimento Interoperabilità	52
10.6	Normativa di riferimento sulla Sicurezza Informatica	53
11	APPENDICE 1 – Elenco acronimi	55

Indice delle figure

Figura 1: organigramma del MIMIT (aggiornamento del 22.03.2022)	14
Figura 2: componenti del Piano	16
Figura 3: schema dell'approccio matriciale adottato per la redazione del Piano	17
Figura 4: componenti tecnologiche AgID.....	18
Figura 5: modello iniziale di Governance del PIANO	45

Indice delle tabelle

1 SCOPO E PREMESSA DEL DOCUMENTO

Il Piano Triennale per l'Informatica rappresenta uno strumento essenziale volto a delineare le linee evolutive e gli obiettivi di trasformazione digitale delle Amministrazioni Pubbliche¹.

Considerata la rilevanza di tale strumento programmatico, il MIMIT ha avviato le attività di ricognizione interna al fine di definire gli interventi che caratterizzeranno le attività ICT del prossimo triennio. Il presente documento è dunque da considerarsi quale prima struttura del Piano Strategico ICT dell'Amministrazione all'interno del quale sono stati individuati e descritti i primi macro-ambiti di intervento. Pertanto, il perimetro della presente versione si limita alla presentazione delle Linee Programmatiche individuate e delle intersezioni delle stesse con le componenti tecnologiche. Fornisce inoltre una indicazione degli interventi in corso e pianificati nel breve termine all'interno del MIMIT, in linea con il presente Piano Strategico.

Su tale base, questa versione verrà poi completata ed integrata con la presentazione degli obiettivi strategici e delle specifiche iniziative progettuali nel corso del 2023, via via che viene definita e conclusa la strategia di migrazione in cloud. A tal proposito, la migrazione verso il cloud è un percorso obbligato, specialmente per quei dati e servizi che devono essere ospitati nel Polo Strategico Nazionale e per quei dati e servizi che rivestono una particolare importanza per le missioni istituzionali del ministero. Infatti il Dipartimento per la trasformazione digitale (DTD) e l'Agenzia per la Cybersicurezza Nazionale (ACN) hanno pubblicato, il 7 settembre 2021, la strategia Cloud Italia². L'ACN, inoltre, ha successivamente pubblicato, in data 25 maggio 2022, la strategia Nazionale per la Cybersicurezza³. L'Agenzia per l'Italia Digitale (AgID) il 15 dicembre 2021 ha inoltre adottato, con la determinazione n. 628/2021, il Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA 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 amministrazione⁴.

Il presente documento viene redatto dal Responsabile per la Transizione al Digitale (RTD) del MIMIT, che *ha tra le principali funzioni quella di garantire operativamente la trasformazione digitale ... coordinandola nello sviluppo dei servizi pubblici digitali e nell'adozione di modelli di relazione trasparenti e aperti*⁵.

¹ [Piano Triennale per l'informatica | Agenzia per l'Italia digitale \(agid.gov.it\)](https://www.agid.gov.it/pt)

² <https://innovazione.gov.it/dipartimento/focus/strategia-cloud-italia/>

³ https://www.acn.gov.it/ACN_Strategia.pdf ; https://www.acn.gov.it/ACN_Implementazione.pdf

⁴

https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/2134818431400_0628+DT+DG+628+-+15+dic+2021+-+Regolamento+servizi+cloud.pdf

https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/2134818432500_0Regolamento+servizi+cloud.pdf

⁵ [Responsabile per la transizione al digitale | Agenzia per l'Italia digitale \(agid.gov.it\)](https://www.agid.gov.it/rt)

L'articolo 17 del Codice dell'Amministrazione Digitale obbliga tutte le amministrazioni a individuare un ufficio per la transizione alla modalità digitale - il cui responsabile è il RTD - a cui competono le attività e i processi organizzativi ad essa collegati e necessari alla realizzazione di un'amministrazione digitale e all'erogazione di servizi fruibili, utili e di qualità.

Nel seguito al presente documento, intitolato "Piano Triennale per la transizione digitale 2023-2025 del Ministero delle Imprese e del Made in Italy", inteso anche come "Piano Strategico per l'informatica" o come "Piano strategico ICT" del MIMIT, ci si riferirà per brevità come "PIANO".

2 INTRODUZIONE

Il presente documento rappresenta lo strumento tramite il quale si intende promuovere la propria trasformazione digitale. In tal senso, si incardina all'interno della più ampia strategia delineata all'interno del Piano Triennale per l'informatica della Pubblica Amministrazione (Piano ICT), redatto dall'Agenzia per l'Italia Digitale (AgID), come risultato della collaborazione tra suddetta Agenzia e il Dipartimento per la Trasformazione Digitale.

In tale contesto si innesca anche il piano Digital Compass 2030, sviluppato dalla Commissione Europea, che compie un passo fondamentale e altamente strategico rispetto alla centralità del tema delle competenze digitali.

Il presente PIANO è finalizzato a disegnare un processo di efficientamento della missione e delle funzioni istituzionali del Ministero oltre che di miglioramento della qualità dei servizi offerti nel rispetto delle prerogative di tutti i principali stakeholder coinvolti (imprese, cittadini, enti locali, regioni, agenzie ecc.). Nasce, inoltre, con la prospettiva di andare incontro in modo efficace alle sfide che questa Amministrazione dovrà affrontare nel prossimo futuro strutturando un percorso in grado di favorire la realizzazione degli obiettivi specifici ad esse correlati. In tal senso il documento è incentrato sulla progettazione e personalizzazione delle componenti tecnologiche definite dall'AgID mediante l'adozione di linee programmatiche che hanno lo scopo di adattare le prime alle specifiche esigenze e necessità del MIMIT.

Quanto sopra non può prescindere dal rispetto dei principi guida definiti dall'AgID, i quali fungono da direttrici di un approccio metodologico basato sullo studio del contesto di riferimento, l'analisi del modello organizzativo del MIMIT, la sua missione istituzionale e i legittimi interessi dell'Amministrazione e degli stakeholder inseriti nei principali processi ministeriali.

L'impianto generale vede questo PIANO organizzato in 5 parti principali, la cui sintesi è di seguito riportata.

- 1) Una prima parte introduttiva (1 - SCOPO E PREMESSA DEL DOCUMENTO; 2 - INTRODUZIONE).
- 2) Una seconda parte focalizzata sull'analisi del contesto di riferimento (3 - IL CONTESTO DI RIFERIMENTO), sulla declinazione degli obiettivi generali che l'Amministrazione intende perseguire (4 - VISIONE DELL'AMMINISTRAZIONE) nonché sulla definizione dell'approccio

metodologico adottato (5 - APPROCCIO METODOLOGICO) nell'ottica di applicazione del modello *to-be* ottimale per l'adozione della strategia di trasformazione digitale.

- 3) Una terza parte (6 - IL PIANO TRIENNALE IT) finalizzata a descrivere ed approfondire le componenti tecnologiche individuate dall'AgID: 1. Servizi, 2. Dati, 3. Piattaforma, 4. Infrastrutture, 5. Interoperabilità e 6. Sicurezza Informatica. Ciascuna componente è approfondita esplicitandone le principali caratteristiche e funzioni, definendone gli obiettivi così come identificati da AgID ed infine fornendo una descrizione del contesto attuale del Ministero rispetto alle singole componenti tecnologiche, funzionale all'individuazione del percorso innovativo da intraprendere. I riferimenti normativi, presentati per ciascuna componente e raccolti in APPENDICE A – Normativa e linee guida di riferimento in conclusione al piano, saranno il punto cardine di tutte le analisi e le valutazioni esposte poiché rappresentano il quadro nazionale e comunitario a cui l'Amministrazione dovrà attenersi. Integrando il contenuto di cui sopra, inoltre, questa parte del PIANO introduce le linee programmatiche, le quali corrispondono alla personalizzazione delle indicazioni AgID rispetto alle necessità riscontrate dal Ministero, ulteriormente declinate in obiettivi specifici e progettualità.
- 4) Una quarta parte dedicata alla proposta di una road-map per la messa in pratica del PIANO (7 - ROADMAP DEL PIANO ICT) definita nell'ambito di un modello di governance ben preciso e quanto più affine al contesto in cui l'Amministrazione opera (8 - MODELLO DI GOVERNANCE).
- 5) Una quinta parte (9- INIZIATIVE IN CORSO) che riporta indicazioni su attività ed interventi in corso e pianificati nel breve termine all'interno del MIMIT, in linea con il presente PIANO. In tale sezione viene anche riportato per grandi linee il dimensionamento economico previsto nel triennio.

3 IL CONTESTO DI RIFERIMENTO

3.1 Missione istituzionale del Ministero

Il Ministero delle imprese e del Made in Italy (MIMIT), dicastero del governo italiano, è incaricato della formulazione e attuazione di politiche e strategie per lo sviluppo del sistema produttivo nazionale finalizzate ad incentivare una crescita duratura e continuativa nel tempo.

Il Ministero interviene attraverso il suo operato in aspetti essenziali delle principali sfide contemporanee a livello globale, quali la digitalizzazione, l'innovazione, l'internalizzazione del sistema economico, la comunicazione, la difesa dei consumatori e la tutela della proprietà intellettuale, valorizzando e promuovendo il *made in Italy* in Italia e nel mondo.

Nello specifico, il suo mandato istituzionale prevede la promozione di politiche finalizzate al miglioramento della competitività a livello internazionale, la formulazione di strategie volte a promuovere la trasparenza e l'efficacia della concorrenza nei diversi settori produttivi, la

salvaguardia degli approvvigionamenti energetici e l'incentivazione ad una transizione verso un'economia digitale di sistema.

Attualmente, anche in conseguenza delle criticità originatesi nel corso della crisi pandemica globale che hanno avuto un ampio impatto sul contesto economico nazionale e mondiale, gli incarichi e le funzioni del Ministero risultano, in una nuova prospettiva, strettamente legati sia alle strategie di tutela e mantenimento del tessuto sociale, produttivo e occupazionale adottate dal Governo che agli interventi strutturali nel sistema produttivo promossi dal Piano Nazionale di Ripresa e Resilienza (PNRR). Di conseguenza, le funzioni istituzionali così come attribuite al Ministero dal Decreto legislativo 30 luglio 1999, n.300 e s.m.i si estendono verso la formulazione di strategie volte alla crescita occupazionale, all'incremento degli investimenti privati, alla promozione della digitalizzazione, della ricerca e dello sviluppo sostenibile.

3.2 Modello Organizzativo del Ministero

Il modello organizzativo attuale del Ministero è la conseguenza di interventi normativi finalizzati alla creazione di una struttura amministrativa funzionale ed efficace.

Attraverso il Decreto del Presidente del Consiglio dei ministri 29 luglio 2021, n.149 è stato adottato il Regolamento di organizzazione del Ministero, in attuazione decreto-legge marzo 2021, n.22 convertito con modificazione della legge 22 aprile 2021, n.55.

Il citato decreto ha portato ad una riorganizzazione interna del Ministero definendo un'articolazione in nove Uffici di livello dirigenziale generale, coordinati da un Segretario Generale. Inoltre, la Direzione Generale per l'approvvigionamento, l'efficienza e la competitività energetica (DGAECE) e la Direzione generale per le infrastrutture e la sicurezza dei sistemi energetici e geominerari (DGISSEG) sono transitate al Ministero della transizione ecologica (oggi Ministero dell'Ambiente e della Sicurezza Energetica).

È stata altresì prevista la creazione di una struttura tecnica di missione al fine di coordinare le politiche e gli interventi strutturali del PNRR, e un'unità per la sorveglianza dei prezzi per verificare e arginare i fenomeni speculativi.

Il Segretariato Generale è al suo interno composto da 5 divisioni e svolge la funzione di coordinamento delle attività del Ministero in tutte le materie di competenza, con particolare riferimento alla programmazione economico-finanziaria, al bilancio e al controllo di gestione, e all'attivazione di sinergie con gli enti vigilati.

Il Ministero è stato riorganizzato, con il DPCM 29.07.2021, il DM 26.10.2021 ed il DM 19.11.2021, in 9 Direzioni Generali, di seguito riportati in una visione sintetica:

1. Direzione Generale per la politica industriale, l'innovazione e le PMI (DGPIIPM), composta da 7 divisioni e con la funzione di formulare strategie finalizzate allo sviluppo della competitività del sistema imprenditoriale, attraverso attività come la promozione della ricerca e dell'innovazione, dello sviluppo e circolazione delle tecnologie digitali e della sostenibilità ambientale;

2. Direzione Generale per la tutela della proprietà industriale - Ufficio italiano brevetti e marchi (DGTPI-UIBM), con 9 divisioni e la funzione di elaborare e promuovere politiche per la lotta alla contraffazione, e di portare all'attuazione interventi per la valorizzazione dei titoli di proprietà industriale;
3. Direzione Generale per gli incentivi alle imprese (DGLAI), costituita da 9 divisioni e con l'incarico di gestire i Fondi per la crescita sostenibile e di garanzia per le piccole imprese e di elaborare politiche per la finanza d'impresa;
4. Direzione Generale per le tecnologie delle comunicazioni e la sicurezza informatica - Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (DGTCSI-ISCTI), con 8 divisioni incaricate, tra le varie funzioni loro attribuite, dell'aggiornamento del piano nazionale di ripartizione delle frequenze e al coordinamento e pianificazione delle frequenze sia a livello nazionale che internazionale;
5. Direzione Generale per i servizi di comunicazione elettronica, di radiodiffusione e postali (DGSCERP), formata da 21 divisioni che si occupano dell'elaborazione di studi sulle prospettive future di reti, servizi di comunicazione elettronica e radiodiffusione e della predisposizione della regolamentazione dei settori delle comunicazioni elettroniche e della radiodiffusione;
6. Direzione Generale per la Riconversione Industriale e Grandi Filiere Produttive (DGRIGFP), composta da 6 divisioni con l'incarico di formulare politiche relative all'aerospazio e alla ricerca aerospaziale e programmi per la reindustrializzazione dei settori maggiormente colpiti dalla crisi e per l'integrazione delle politiche ambientali;
7. Direzione Generale per il mercato, la concorrenza, la tutela del consumatore e la normativa tecnica (DGMCTCNT), comprendente 12 divisioni, che ha l'obiettivo di tutelare e promuovere la concorrenza e formulare proposte normative inerenti alla liberalizzazione;
8. Direzione Generale per la Vigilanza sugli enti cooperativi e sulle società (DGVECS), con 7 divisioni e il compito di vigilare sul sistema cooperativo, su albi delle società cooperative e sulle gestioni commissariali;
9. Direzione Generale per le Risorse, l'Organizzazione, i Sistemi Informativi e il Bilancio (DGROSIB), composta da 8 divisioni, che svolge funzioni di coordinamento degli uffici e delle attività di formazione di bilancio e previsione della spesa e della progettazione di sistemi informativi e gestione delle banche dati.

All'interno del Ministero sono presenti due datacenter di competenza della DGROSIB – Divisione V nelle due sedi centrali di Roma, che forniscono tutti i servizi generali (sistema di posta elettronica, sistema documentale, servizi web intranet ed internet, ecc) e le infrastrutture di rete in tutte le sedi del ministero. Ci sono, inoltre, altri datacenter di competenza di altre Direzioni Generali e da queste gestite autonomamente:

- CED UIBM: datacenter di competenza della Direzione Generale Ufficio Italiano Brevetti e Marchi, L'infrastruttura utilizza la connettività fino al livello di firewall fornita dalla DGROSIB.
- CED DGLAI: datacenter di competenza della Direzione Generale Incentivi Alle Imprese. Ha connettività propria e i servizi sono erogati in maniera indipendente. I flussi tra il CED DGLAI ed il CED della DGROSIB sono regolati da firewall policy. I client e i server non sono di

competenza della DGROSIB ma usufruiscono solo dei servizi di posta elettronica e del Documentale Informatico.

- CED ISCTI: datacenter di competenza della Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica - Istituto superiore delle comunicazioni e delle tecnologie dell'informazione. Connesso ad uno dei datacenter della DGROSIB, l'infrastruttura utilizza la connettività fornita dalla DGROSIB e i servizi vengono pubblicati tramite l'infrastruttura ADC della DGROSB. La competenza della DGROSIB si ferma al firewall che interconnette i due datacenter.

Allo stato attuale nel MISE sono presenti 80 sedi territoriali: 72 sedi connesse tramite VPN IPSec, 8 interconnesse tramite rete MPLS. In 15 delle 72 sedi sono presenti server, utilizzati come fileserver locali, ad uso esclusivo della sede in cui sono installati:

- ISPCMP: Ispettorato Campania
- ISPFVG: Ispettorato Friuli-Venezia Giulia
- ISPLMB: Ispettorato Lombardia
- ISPLZA: Ispettorato Lazio
- ISPMRU: Ispettorato Marche e Umbria
- ISPMRU: Ispettorato Marche e Umbria
- ISPPGB: Ispettorato Puglia e Basilicata
- ISPPVA: Ispettorato Piemonte e Valle d'Aosta
- ISPSCL: Ispettorato Sicilia
- ISPSRD: Ispettorato Sardegna:
- ISPTAA: Trentino-Alto Adige
- ISPTSC: Ispettorato Toscana
- ISPVNT: Ispettorato Veneto

A fronte di un perimetro infrastrutturale e di servizi notevolmente ampio e con una organizzazione del ministero che richiede servizi a volte notevolmente eterogenei, il coordinamento, la pianificazione e il supporto per le tematiche della digitalizzazione sono in carico alla Divisione V "Sistemi informativi e trasformazione digitale" della DGROSIB. Infatti le competenze di tale Divisione, così come previste dal citato DM 19 novembre 2021, sono:

- Pianificazione, programmazione e gestione di: a) fabbisogni del patrimonio, beni e servizi informatici per il funzionamento a valere sui capitoli in gestione diretta e su quelli in gestione unificata; b) procedure ad evidenza pubblica per i fabbisogni di beni e servizi relativi alle attività di competenza e per le categorie su delega; c) procedure per l'acquisizione di beni e servizi sul mercato elettronico per le materie di competenza e per le categorie su delega
- Rapporti con l'autorità per la vigilanza sui contratti pubblici di lavori, servizi e forniture
- Assolvimento, in qualità di centro di competenza del Ministero, dei compiti stabiliti, dalla vigente normativa, per il responsabile dei sistemi informativi ai sensi dell'articolo 17 del decreto legislativo 7 marzo 2005, n. 82

- Definizione degli standard tecnici per lo sviluppo dei sistemi informativi, di telecomunicazione e fonia
- Predisposizione, aggiornamento, attuazione e vigilanza sul rispetto del piano di sicurezza informatica del Ministero
- Progettazione e coordinamento per l'erogazione di servizi in rete a cittadini e imprese
- Predisposizione e implementazione di accordi di servizio in compartecipazione con le pubbliche amministrazioni
- Promozione di iniziative per l'attuazione di direttive per l'innovazione tecnologica impartite dalla Presidenza del Consiglio dei Ministri
- Pianificazione, promozione e coordinamento dell'utilizzo dei sistemi di posta elettronica, firma digitale e mandato informatico
- Gestione e sviluppo dell'infrastruttura informatica in tema di gestione documentale e dell'applicativo per la gestione del protocollo informatico unificato
- Gestione delle infrastrutture, anche software, legate agli accessi e alla rilevazione delle presenze
- Progettazione, sviluppo e controllo dei sistemi informativi
- Controllo e implementazione dell'intera rete e della connettività interna e verso i sistemi esterni al Ministero e gestione della fonia
- Programmazione e coordinamento degli investimenti e delle forniture di beni e servizi informatici bilanciando le esigenze con risorse, sostenibilità tecnica e sicurezza informatica
- Studi di fattibilità e redazione dei capitolati tecnici relativi ai sistemi informativi
- Assistenza per progettazione e sviluppo o individuazione ed acquisto di sistemi informativi dedicati
- Predisposizione e gestione dei contratti e delle forniture di beni e servizi informatici
- Supporto, pareri e consulenze in materia informatica
- Regolamentazione e gestione tecnica del portale web Internet ed intranet
- Servizio di consegnatario dei beni informatici ai sensi del decreto del Presidente della Repubblica n. 254/2002
- Supporto informatico per le attività connesse e in tema di trattamento e protezione dei dati, ai sensi del Regolamento Europeo 2016 n. 679 e rapporti con la struttura di supporto al responsabile protezione dati (DPO)

3.3 Ruolo del Responsabile per la Transizione al Digitale

Il ruolo del Responsabile per la Transizione Digitale è assunto dal dirigente pro-tempore della sopra richiamata Divisione V "Sistemi informativi e trasformazione digitale" della DGROSIB, che quindi costituisce la struttura e l'organizzazione di supporto al Responsabile della Transizione Digitale.

La Divisione V è suddivisa in quattro Aree Funzionali, all'interno delle quali sono individuate una o più Unità Organizzative Omogenee coordinate da un referente.

- AREA DI STAFF – Monitoraggio, pianificazione e programmazione strategica, con 1 Unità Organizzativa denominata “U.O. Monitoraggio, pianificazione e programmazione strategica”. L’attività svolta riguarda supporto alla dirigenza nel monitoraggio e nella pianificazione di progetti strategici, nella gestione dei progetti trasversali alle aree, nella programmazione e coordinamento degli investimenti e delle forniture di beni e servizi informatici. Assistenza alla dirigenza nelle attività riguardanti la misura ed il miglioramento delle performance, nelle attività di verifica dei carichi di lavoro e degli adempimenti connessi al Piano Triennale Prevenzione e Corruzione. Collaborazione con il dirigente nella gestione delle comunicazioni interne ed esterne alla Divisione.
- AREA INFRASTRUTTURE, SISTEMI E SICUREZZA, con 1 Unità Organizzativa denominata “UO Infrastrutture, sistemi informativi e sicurezza”. L’attività svolta riguarda: gestione sistemistica di tutti gli asset informatici, delle infrastrutture info-telematiche e dei servizi di telecomunicazione; definizione degli standard tecnici e delle linee guida per utilizzo asset informatici, sviluppo dei sistemi informativi e dei sistemi e servizi di telecomunicazione. Gestione ed assistenza delle utenze e delle postazioni di lavoro; predisposizione, aggiornamento, attuazione e vigilanza sul rispetto del piano di sicurezza informatica del Ministero; assicurare l’evoluzione dei sistemi informativi del Ministero; assicurare il corretto, celere e puntuale processo di gestione dei flussi procedurali sia sul piano formale che sostanziale; assicurare il rispetto delle tempistiche; assolvimento, in qualità di centro di competenza del Ministero, dei compiti stabiliti, dalla vigente normativa, per il Responsabile dei Sistemi Informativi ai sensi dell’articolo 17 del decreto legislativo 7 marzo 2005, n. 82; supporto, pareri e consulenze in materia informatica; assistenza al Segretariato, alle Direzioni generali e agli Uffici di diretta collaborazione per progettazione e sviluppo, od individuazione ed acquisto, di sistemi informativi dedicati; progettazione, sviluppo e controllo dei sistemi informativi; promozione di iniziative per l’attuazione di direttive per l’innovazione tecnologica; progettazione e coordinamento per l’erogazione di servizi in rete a cittadini e imprese; studi di fattibilità e redazione dei capitolati tecnici relativi ai sistemi informativi; supporto informatico per le attività connesse e in tema di trattamento e protezione dei dati, ai sensi del Regolamento Europeo 2016 n. 679 e rapporti con la struttura di supporto al Responsabile Protezione Dati (DPO); promozione open data; regolamentazione e gestione tecnica del portale web internet ed intranet.
All’interno dell’UO è incardinato l’ufficio del consegnatario dei beni informatici.
- AREA SERVIZI/SISTEMI GESTIONALI, con 3 Unità Organizzative.
 - UO Servizi – L’attività svolta riguarda supporto, coordinamento per il raggiungimento degli obiettivi degli uffici presenze e documentale; garantire la corretta configurazione dei capitoli di bilancio ai dirigenti delegati; gestione delle utenze e delle configurazioni di altri sistemi gestionali, pianificazione; gestione delle infrastrutture, anche software, legate agli accessi e alla rilevazione delle presenze.

- UO Documentale – L'attività riguarda gestione documentale, conservazione digitale e protocollo; gestione del protocollo informatico unificato; pianificazione, promozione e coordinamento dell'utilizzo dei sistemi di posta elettronica certificata, firma digitale, aggiornare (o proporre la modifica) del manuale di gestione documentale. Pianificazione, promozione e coordinamento dell'utilizzo dei sistemi di posta elettronica certificata e di firma digitale. Gestione e sviluppo dell'infrastruttura informatica in tema di gestione documentale e dell'applicativo per la gestione del protocollo informatico unificato.
- UO Ufficio Unico Presenze – L'attività riguarda la gestione del personale di tutte le DDGG e del Segretariato generale; supporto totale alle DDGG per le attività di gestione sul Time@Work di tutto il Personale MIMIT; trasmissione dei dati per la produttività annuale (FUA); trasmissione su portale Perla-PA della Funzione Pubblica delle assenze mensili e trimestrali di tutto il Personale MIMIT e dei permessi sindacali del Personale MIMIT avente diritto; raccolta dei prospetti per gli ordinativi dei buoni pasto; predisposizione della documentazione delle malattie e degli straordinari e invio della documentazione agli uffici competenti; collaborazione con gli uffici competenti in merito alla concessione di autorizzazioni ai parcheggi e utilizzo del sistema Check & In per il controllo accessi dei Garage ministeriali; collaborazione con l'ufficio Badge di Via Molise per il personale applicato presso la sede di Viale America; gestione dell'iter per la comunicazione unica in merito all'adesione dei dipendenti agli scioperi del personale dell'Amministrazione Pubblica; redazione dei dati del Conto Annuale per la DGROSIB da consegnare all'ufficio incaricato entro i termini di legge.
- AREA AMMINISTRAZIONE, con 1 unità organizzativa denominata "UO Amministrazione". L'attività svolta riguarda acquisizione di beni e servizi informatici; gestione economica e finanziaria; gestione contratti di telefonia fissa e mobile, gestione dei contratti dei circuiti per trasmissione dati; predisposizione e gestione amministrativa dei contratti e delle forniture di beni e servizi informatici; gestione amministrativa delle utenze di fonia fissa e mobile; predisposizione e implementazione di accordi di servizio in compartecipazione con le Pubbliche Amministrazioni; procedimento contabile dei contratti dell'intera divisione (impegno e pagamento); adempimenti in materia di anticorruzione e trasparenza.

Per lo svolgimento delle attività di propria competenza la Divisione V si avvale anche del supporto di personale esterno, suddiviso in quattro specifici gruppi:

- Assistenza informatica;
- Supporto Sistemi infrastrutturali;
- Sistemisti di network;
- Sistemisti di sicurezza.

3.4 Organigramma del Ministero

L’organigramma in forma grafica del MIMIT è riportato all’indirizzo [Organigramma grafico \(mimit.gov.it\)](https://mimit.gov.it). L’aggiornamento alla data attuale è riportato nella seguente figura.

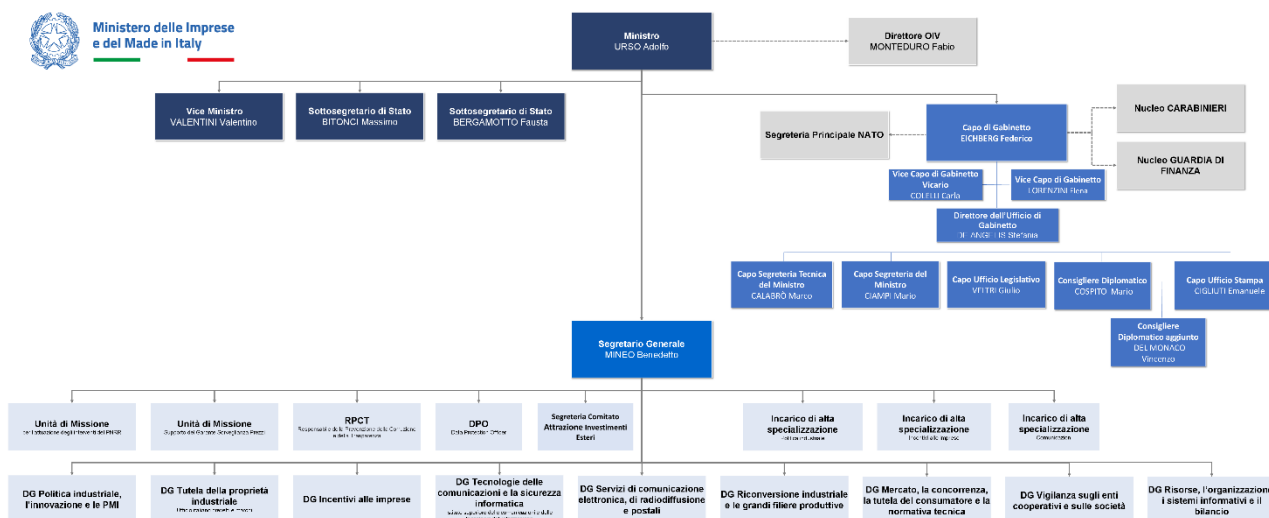


Figura 1: organigramma del MIMIT (aggiornamento del 22.03.2022)

3.5 Visione strategica trasversale

La strategia ed i principi guida adottati nella redazione del presente piano sono in linea con la strategia indicata dall’AGID nell’ultima versione del Piano Triennale per l’informatica nella Pubblica Amministrazione. In aggiunta, nel pensare a contribuire allo sviluppo di una società digitale, si pensa a servizi e soluzioni tecnologiche che siano in grado non solo di mettere al centro i cittadini e le imprese, ma anche l’essere umano in sé, pensando quindi a modelli di innovazione nel campo digitale che abbiano come effetto il miglioramento della vita, inteso questo in termini generali e secondo una visione che guarda a molteplici aspetti, permettendo la condivisione di valori e conoscenza.

Al contempo, non può essere trascurato l’impatto che questa continua integrazione tra mondo cibernetico e mondo fisico sui rischi che ne derivano. L’insorgenza di nuove problematiche dovute alla sensibilità delle informazioni in transito sulle reti e sui dispositivi per digitalizzare l’amministrazione, rende la tutela dei sistemi ICT ancora più determinante. Ne consegue che la messa in sicurezza di tutti i sistemi informativi diventa una strategia dominante e trasversale a qualsiasi iniziativa di transizione digitale, specialmente in un contesto quale quello attuale nel quale gli attacchi informatici sono sempre più frequenti e i relativi moventi possono essere i più svariati, da quelli legati agli interessi economici a quelli di lesione della reputazione di organizzazioni e persone. La sicurezza cibernetica assume rilevanza strategica nella realizzazione di qualsiasi iniziativa, divenendo, dunque, non solo un requisito imprescindibile, ma una strategia da perseguire con continuità.

A tal fine, uno degli obiettivi, trasversale a tutte le iniziative intraprese e che verranno intraprese, è realizzare una omogeneizzazione di sistemi e informazioni per arrivare ad una gestione centralizzata della sicurezza di tutto l'eco-sistema dell'ICT del Ministero, dotandosi di infrastrutture e soluzioni tecnologiche che permettono di garantire adeguati livelli di sicurezza cibernetica.

4 VISIONE DELL'AMMINISTRAZIONE

Nel contesto del presente documento, l'obiettivo primario del MIMIT è quello di avviare un percorso verso la propria trasformazione digitale, in risposta ad un contesto esterno che sta cambiando rapidamente e che pone il Ministero stesso di fronte a nuove sfide e importanti opportunità di crescita e rinnovamento.

In tale ottica, si sottolineano le necessità di rendere più efficiente il modello organizzativo e il modello di governo interni e di ripensare agli standard dei propri processi in coerenza con le aumentate aspettative del contesto in continua evoluzione. L'organizzazione e i processi sono centrali alla trasformazione digitale, secondo un cambiamento armonizzato con l'evoluzione del sistema informativo. A tendere, tale impostazione avrà il compito di rendere efficiente la sinergia tra cambiamento organizzativo e innovazione digitale a servizio di tutte le divisioni del MIMIT al fine di collaborare alla diffusione di una nuova cultura interna e alla formazione di nuove competenze e agevolare l'integrazione di un'offerta di servizi digitali sempre più fruibili ed efficienti per cittadini e imprese.

Si ricerca, in tal senso, di dotare il MIMIT di metodologie e strumenti in grado di garantire un governo e una gestione efficace delle informazioni sia al personale interno che agli utenti esterni, valorizzando il patrimonio informativo e culturale. Il tutto da realizzare con l'ausilio e il rispetto degli obiettivi delineati dalle linee guida AgID declinati a seguire in ciascun paragrafo per componente tecnologica e coerenti al quadro normativo di riferimento.

Il processo di digitalizzazione della Pubblica Amministrazione impatterà sul Ministero attraverso interventi tecnologici ad ampio raggio accompagnati da significative riforme strutturali. Il supporto della migrazione al cloud delle amministrazioni centrali e locali e la piena interoperabilità delle banche dati richiedono lo sviluppo e l'acquisizione di nuove competenze per il personale della PA e una semplificazione e sburocratizzazione delle procedure chiave.

In questo quadro generale, il comparto ICT è chiamato a contribuire alla realizzazione degli obiettivi perseguiti dall'Amministrazione, supportando l'assolvimento delle diverse funzioni attribuite e mettendosi al servizio delle esigenze espresse dagli utenti coinvolti nei processi del MIMIT, siano essi interni o esterni all'amministrazione.

Allo stesso tempo, le opportunità offerte dalle tecnologie e dalla loro rapida evoluzione accrescono l'importanza strategica della funzione ICT all'interno del MIMIT, come motore dell'innovazione in termini più generali e traino per raggiungere sempre più elevati livelli di efficienza ed efficacia dell'azione amministrativa.

In questo contesto emerge con particolare rilevanza il tema della corretta gestione delle informazioni rilevanti per l'assolvimento delle funzioni istituzionali assegnate alle strutture del Ministero. La necessaria integrazione e trasversalità dell'informazione all'interno dell'Amministrazione non può infatti prescindere dalla specifica definizione dei ruoli e delle responsabilità connesse alle diverse fasi del processo di produzione, acquisizione, trattamento, elaborazione e valorizzazione dei dati, anche attraverso la definizione di opportuni protocolli e standard per la messa in condivisione delle informazioni.

Solo attraverso l'individuazione dei profili di responsabilità connessi è possibile garantire un reale monitoraggio e un'effettiva valutazione della qualità dei dati prodotti e rilasciati sia sotto il profilo della completezza che sotto quello dell'affidabilità, che garantiscano in primo luogo le strutture interne della Amministrazione e di conseguenza, i soggetti esterni con cui le informazioni vengono poi condivise.

In coerenza con quanto sopra richiamato, il piano triennale riportato nel presente documento descrive il percorso di evoluzione e trasformazione digitale del MIMIT.

5 APPROCCIO METODOLOGICO

Nei precedenti paragrafi è stato illustrato il contesto all'interno del quale opera il Ministero. In coerenza con le *Best practices* in ambito *IT Governance*, è stato individuato un approccio metodologico alla predisposizione del Piano suddiviso in vari livelli come descritti nella seguente figura.

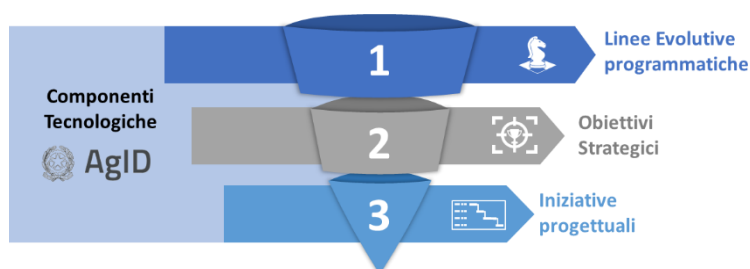


Figura 2: componenti del Piano

Le componenti individuate sono volte ad illustrare la base del percorso evolutivo intrapreso dal Ministero. In particolare, i tre livelli programmatici e operativi sono stati definiti tenendo costantemente in considerazione i principali input forniti dall'Agenzia per l'Italia Digitale (AgID) in tema di componenti tecnologiche di riferimento sulla base delle quali orientare i percorsi evolutivi delle Pubbliche Amministrazioni.

Con specifico riferimento al percorso evolutivo definito dal MIMIT, la piramide programmatica prevede:

1. L'individuazione di "Linee Evolutive Programmatiche", volte a riconoscere e definire le principali macro-argomentazioni/settori sui quali il Ministero concentrerà le attività di innovazione;
2. L'identificazione di "Obiettivi Strategici" associati a ciascuna linea programmatica e che si intende perseguire nel corso del triennio di competenza;
3. La pianificazione delle specifiche "Iniziativa Progettuali" volte al perseguimento degli obiettivi di cui sopra e alla definizione delle attività operative di dettaglio da intraprendere.

Come anticipato, il percorso evolutivo delineato ha previsto un'analisi delle componenti tecnologiche AgID, finalizzata ad individuare le intersezioni con le Linee Programmatiche individuate dall'Amministrazione e sottolineare la coerenza del percorso in fase di avviamento, con le direttive nazionali in tema di digitalizzazione. Sulla base di tali premesse, il Piano è stato dunque sviluppato in base all'approccio matriciale di seguito rappresentato.



		 Componenti Tecnologiche					
		SERVIZI	DATI	PIATTAFORME	INFRASTRUTTURA	INTEROPERABILITA'	SICUREZZA INFORMATICA
Linee Evolutive programmatiche	Workspace e Digital Adoption	✓		✓			
	Realizzazione del catalogo dei servizi	✓		✓		✓	
	Migrazione al Cloud	✓			✓		
	Miglioramento dell'erogazione dei servizi				✓		✓
	Sicurezza informatica e Disaster Recovery						✓
	Dematerializzazione e conservazione sostitutiva	✓	✓				
	Nuovo modello e pratiche di Data Governance		✓		✓		
	Razionalizzazione del parco applicativo	✓	✓		✓		
	Razionalizzazione e ridisegno del modello Operativo IT	✓	✓	✓	✓	✓	✓

Figura 3: schema dell'approccio matriciale adottato per la redazione del Piano

All'interno delle sezioni successive del presente documento verranno espone in dettaglio le linee programmatiche. Saranno presenti dei navigatori che mostreranno per ognuna quali sono le componenti tecnologiche intersecate. I colori di ogni componente tecnologica verranno mostrati nei paragrafi dedicati alla loro analisi.

Infine, con lo scopo di garantire un costante monitoraggio delle attività, saranno previste nell'arco del triennio più fasi di revisione degli obiettivi, così da garantire aggiornamenti puntuali nel caso in cui il contesto interno o esterno venga assoggettato a modifiche quali: aggiornamento delle normative, nuove attribuzioni di funzioni, modifiche organizzative, richieste di cambiamento eccezionali da parte degli stakeholder.

6 IL PIANO TRIENNALE IT

6.1 Componenti tecnologiche AgID

All'interno del Piano Triennale per l'informatica, l'AgID definisce le seguenti componenti tecnologiche che costituiscono i principali pilastri del percorso di digitalizzazione verso il quale le Pubbliche Amministrazioni devono tenere. In particolare:

1. Servizi;
2. Dati;
3. Piattaforma;
4. Infrastrutture;
5. Interoperabilità;
6. Sicurezza Informatica.

Il focus del presente documento è rappresentato dalla progettazione e personalizzazione di tali componenti rispetto alle specifiche necessità individuate dal MIMIT. A tal proposito, il primo passo per andare incontro alle esigenze del Ministero è stato delineare specifiche Linee Programmatiche che definiscono i principali temi su cui sarà incentrato il percorso di innovazione. A ciascuna di esse, inoltre, è associata una pluralità di obiettivi strategici ben definiti, da raggiungere nel corso del triennio di competenza e declinati in specifiche progettualità che esplicitano le attività operative da intraprendere.

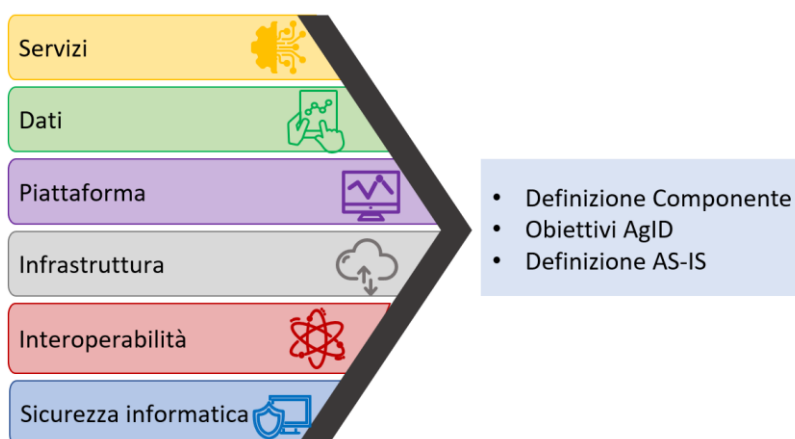


Figura 4: componenti tecnologiche AgID

Nei seguenti paragrafi ciascuna componente è approfondita in tre sottosezioni che offrono una descrizione delle caratteristiche, una spiegazione degli obiettivi presenti nel documento AgID e, infine, una fotografia del contesto attuale del Ministero, necessaria alla definizione degli obiettivi da perseguire nel triennio.

I seguenti paragrafi che approfondiscono le sei componenti tecnologiche individuate dall'AgID sono stati redatti seguendo i riferimenti normativi riuniti nell'APPENDICE 1 presente alla fine del documento.



6.1.1 A. Servizi

Avere dei servizi pubblici digitali efficienti permette alle PPAA di alleggerire il carico burocratico e procedurale di molteplici processi interni. Al fine di sfruttare al massimo il potenziale dei servizi digitali è necessario l'intervento su aspetti tecnologici e organizzativi, puntando prettamente sulla semplificazione dei processi e sulla razionalizzazione degli elementi tecnologici, hardware e software, in forza alle amministrazioni per ridurre la frammentazione che porta inevitabilmente ad un ritardo nella maturità dei servizi.

Nello specifico, le PPAA dovranno costruire il nuovo modello dei servizi in un'ottica di:

- **miglioramento della capacità di generare ed erogare servizi digitali:** attraverso la diffusione del modello di riuso di software tra le PA, l'acquisizione e il riuso del software, l'adozione del paradigma cloud, nonché il monitoraggio continuo dei servizi;
- **miglioramento dell'esperienza d'uso e dell'accessibilità dei servizi,** tra cui l'aderenza dei servizi ai modelli standard per lo sviluppo di siti disponibili in Designers Italia, la diffusione dei test di usabilità per agevolare il feedback e le valutazioni da parte degli utenti interni.

6.1.1.1 Obiettivi AgID

Il Piano AgID indica l'insieme delle metodologie, delle tecniche e dei principi che perseguono il miglioramento della qualità dei servizi pubblici digitali. Al fine di allineare i propri standard con le direttive AgID, è necessario per le Pubbliche Amministrazioni agire su più livelli per migliorare la qualità dei servizi erogati, tra questi:

- **incrementare il livello di accessibilità dei servizi erogati tramite siti web e app mobile:** prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo;
- **garantire l'inclusività e accessibilità dei servizi:** progettando servizi pubblici digitali che siano per definizione accessibili, inclusivi e che vengano incontro alle diverse esigenze dei cittadini e delle imprese presenti sul territorio nazionale, rendendo disponibili i servizi pubblici digitali rilevanti;
- **gestione del dato in un'ottica "once only":** il dato dell'utente, fornito alle PPAA, costituisce la *single source of truth* da condividere con l'intero ecosistema nazionale della PA. In tal modo, cittadini e imprese presentano le informazioni una sola volta e usufruiscono di più servizi senza dover fornire nuovamente i propri dati personali;

- **adozione del paradigma cloud nella realizzazione di nuovi servizi:** attraverso l'utilizzo, in via prioritaria, di soluzioni SaaS (*Software as a Service*), il riuso, la condivisione di software e competenze tra le diverse amministrazioni.

Dunque, la strategia di trasformazione digitale della PA, indirizzata dal Piano Triennale AgID, vede al centro della trasformazione tutte quelle azioni, strumenti e metodi per il miglioramento dei servizi e della loro erogazione, ponendo le basi per la definizione delle politiche interne dell'evoluzione della Pubblica Amministrazione attraverso la declinazione di «obiettivi strategici» sui quali le PPAA dovranno costruire il nuovo modello di servizi. Tra questi:

- **migliorare la capacità di generare ed erogare servizi digitali:** attraverso la diffusione del modello di riuso di software tra le amministrazioni, l'acquisizione e il riuso del software per la Pubblica Amministrazione, l'adozione del paradigma cloud e il conseguente ampliamento dell'offerta del Catalogo dei servizi cloud qualificati nonché il monitoraggio continuo dei servizi;
- **migliorare l'esperienza d'uso e l'accessibilità dei servizi,** tra cui l'incremento e diffusione dei modelli standard per lo sviluppo di siti disponibili in Designers Italia, la diffusione dei test di usabilità nelle amministrazioni per agevolare il feedback e le valutazioni da parte degli utenti interni, l'incremento dell'accessibilità dei servizi digitali della PA, secondo quanto indicato dalle Linee guida sull'accessibilità degli strumenti informatici.

6.1.1.2 Definizione AS-IS

In tale contesto, il Ministero presenta un certo grado di frammentazione dell'attuale catalogo servizi, dovuto principalmente alla necessità di dover sopperire alle molteplici richieste da parte di fattori esterni, come normative e adeguamenti, e da parte degli utenti interni, i quali necessitano sempre più di soluzioni ICT per erogare servizi ed espletare i propri compiti. Tale frammentazione è alimentata dalla mancata presenza di standard procedurali, a livello ministeriale, per la gestione del ciclo di vita del servizio, che causa di conseguenza una gestione inefficiente sia delle risorse hardware/software a disposizione che dell'*effort* delle risorse preposte alla loro gestione. Inoltre, l'attuale sistema informativo del Ministero non è dotato delle componenti tecnologiche adeguate agli standard tecnologici di altre PAC, come ad esempio il DWH, per abilitare logiche di *Data Quality* e *Data Analytics*, o soluzioni di CRM, per l'acquisizione ed esposizione di dati strutturati verso i *touchpoint* e per l'analisi del comportamento degli utenti in relazione al servizio. All'interno del Ministero, risulta complesso raccogliere e analizzare i dati degli utenti finali al fine di poter utilizzare gli stessi nel processo decisionale volto al miglioramento dei servizi e dell'esperienza utente.

Alla luce di tali criticità, preliminarmente analizzate e che saranno oggetto di ulteriori approfondimenti, è evidente la necessità del Ministero di adattare il proprio modello di servizio alle linee guida AgID e agli standard di mercato nazionali ed europei, attuando una rivisitazione e un miglioramento dell'attuale modello di erogazione dei servizi. Tale processo è focalizzato due principali direttrici o linee guida programmatiche:

- **Razionalizzazione del catalogo dei servizi**, attraverso la reingegnerizzazione dei processi sottesi alla creazione, mantenimento dei servizi e all’ottimizzazione delle relative modalità di erogazione. In tale contesto, rientrano tutti gli interventi che vedono la realizzazione di nuovi modelli organizzativi, procedure di design del servizio e modalità di monitoraggio delle performance in un’ottica di *continuous improvement*; Le progettualità che verranno identificate interverranno in tutte le fasi di ideazione, progettazione e realizzazione del servizio, garantendo standard avanzati di flessibilità ed efficacia di erogazione;
- **Miglioramento delle modalità di erogazione del Servizio**, attraverso il disegno di un nuovo modello architeturale, a livello *enterprise*, che possa supportare l’erogazione dei servizi e che permetta di delineare indirizzi strategici comuni e condivisi, al fine di costruire un “ecosistema dei servizi” innovativo. In tale contesto rientrano tutti gli interventi volti al miglioramento dei “*touchpoint*” digitali, all’adozione di componenti tecnologiche, piattaforme strategiche nazionali e al monitoraggio continuo, garantendo il soddisfacimento dei *needs* degli utenti, imprese e cittadini, secondo un approccio proattivo.



6.1.2 B. Dati

I dati custoditi dalle PA devono essere gestiti con particolare cura in modo da ridurre al minimo i rischi di distruzione, perdita o accesso non autorizzato. Un importante obiettivo per le PA è sicuramente la creazione e pubblicazione di un *dataset* di qualità, generando interesse riguardo i dati pubblicati. A tal proposito la Presidenza del Consiglio dei ministri attraverso la Piattaforma Digitale Nazionale Dati (PDND) punta a favorire la conoscenza, la condivisione e l’utilizzo del patrimonio informativo detenuto. Si tratta di un’infrastruttura tecnologica che rende possibile l’interoperabilità dei sistemi informativi e delle basi di dati delle pubbliche amministrazioni e dei gestori di servizi pubblici, mediante l’accreditamento, l’identificazione e la gestione dei livelli di autorizzazione dei soggetti abilitati ad operare sulla stessa.

La valorizzazione del patrimonio informativo pubblico riguarda sia la condivisione dei dati tra pubbliche amministrazioni per finalità istituzionali che il riutilizzo dei dati, secondo il paradigma degli open data. L’importanza di tali obiettivi viene definita all’interno del CAD, del Piano Triennale per l’Informatica nella Pubblica Amministrazione e nel quadro delineato dalla Direttiva europea sull’apertura dei dati e il riutilizzo dell’informazione del settore pubblico.

I dati di tipo aperto, con riferimento all’articolo 1 del CAD, presentano le seguenti caratteristiche:

- Sono disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l’utilizzo da parte di chiunque, anche per finalità commerciali;
- Sono accessibili attraverso le tecnologie dell’informazione e della comunicazione in formati aperti e provvisti dei relativi metadati;
- Sono resi disponibili gratuitamente, o ai costi marginali sostenuti per la loro riproduzione e divulgazione, attraverso le tecnologie dell’informazione e della comunicazione.

I dati custoditi dalle PA devono essere gestiti con particolare cura in modo da ridurre al minimo i rischi di distruzione, perdita o accesso non autorizzato. Provvedere all'apertura dei dati non significa operare una condivisione automatica e sistematica di ogni informazione o documento ma di permettere l'accesso alle informazioni sempre nel rispetto della loro riservatezza, necessaria a creare e mantenere la fiducia dei cittadini nelle istituzioni.

6.1.2.1 Obiettivi AgID

Il Piano Triennale, redatto dall' Agenzia per l'Italia Digitale (AgID), definisce una serie di obiettivi concreti e linee d'azione a cui le amministrazioni devono fare riferimento nel merito della pianificazione del proprio piano di digitalizzazione. In particolar modo, il capitolo dedicato ai dati si occupa di definire gli obiettivi sui quali le PA devono focalizzarsi per una gestione efficace dei dati per migliorare la capacità di generare ed erogare servizi digitali e di qualità, in particolare:

- **Favorire la condivisione e il riutilizzo dei dati** tra le PA e il riutilizzo da parte di cittadini e imprese, aumentando il numero di basi di dati di interesse nazionale che espongono API coerenti con i modelli di riferimento di dati nazionali ed europei; aumentando il 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; aumentando il numero di *dataset* resi disponibili attraverso i servizi di dati territoriali di cui alla Direttiva 2007/2/EC (*INSPIRE*).
- **Aumentare la qualità dei dati e dei metadati**, aumentando il numero di dataset con metadati di qualità conformi agli standard di riferimento europei e nazionali ed il numero di *dataset* di tipo aperto resi disponibili dalle pubbliche amministrazioni.
- Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati, aumentando il numero di *dataset* di tipo aperto che adottano la licenza CC BY 4.0.

6.1.2.2 Definizione AS-IS

Nella società odierna grazie ad un costante aumento della quantità di dati generati dai singoli cittadini, rivestono sempre una maggiore importanza attività legate alla raccolta, all'analisi e alla protezione dei dati. Le tendenze mostrano come il volume dei dati prodotti a livello mondiale è in rapida crescita. In generale la gestione di banche dati, necessitano di un'accurata programmazione che dia conto di tutte le fasi del processo generativo. Inoltre, i dati, una volta prodotti, rappresentano un patrimonio che va correttamente gestito al fine della sua preservazione nel tempo.

Rispetto agli input suggeriti da AgID, nel contesto dell'Amministrazione, si riscontra una diffusa frammentarietà del patrimonio informativo in molteplici basi di dati non collegate tra di loro, causando ridondanza di informazioni e assenza di una catalogazione delle stesse. A tal proposito, l'obiettivo primario è quello di creare un catalogo dati a prescindere dall'*ownership* degli stessi accompagnato dalla definizione di un processo di aggiornamento.

Per quanto concerne il tema interoperabilità, ad oggi non vi è alcun tipo di interlocuzione strutturata tra i diversi sistemi e le rispettive basi dati. L'obiettivo, dunque, è il perseguimento delle indicazioni fornite da AgID dello sviluppo di API e servizi orientati al popolamento della PDND.

In tale ottica, si propone nei paragrafi seguenti una linea evolutiva per la definizione di un modello di dati condiviso e di Data Governance strutturata al fine di: includere un generale efficientamento nell'utilizzo dei dati e delle informazioni che risultano ad oggi sparse e poco utilizzate; garantire servizi migliori agli interlocutori; migliorare l'interoperabilità tra i servizi interni.



6.1.3 C. Piattaforma

Sempre più rilevanti all'interno del contesto pubblico, le piattaforme rappresentano soluzioni volte ad offrire agli stakeholder funzionalità fondamentali, trasversali, abilitanti e riusabili che da un lato aumentano il grado di digitalizzazione dei processi e servizi della PA, dall'altro, forniscono ai propri interlocutori servizi omogenei uniformando le modalità di erogazione.

Uno dei principali vantaggi dell'utilizzo delle piattaforme è, in ottica di efficientamento, la riduzione del carico di lavoro in seno alle PA, garantendo una maggiore sicurezza informatica e consentendo al contempo una razionalizzazione dei processi *front* e *back-end* oltre che una standardizzazione dei flussi di dati scambiati tra le amministrazioni, al fine di velocizzarne i processi. Tali soluzioni si caratterizzano per un impatto a due principali livelli, in quanto svolgono una fondamentale funzione esterna di raccordo tra le varie istituzioni e tra istituzioni e cittadini, tramite servizi condivisi e facilmente leggibili.

In tale contesto, le Linee Guida definite a livello nazionale in materia di digitalizzazione, sponsorizzano l'utilizzo delle piattaforme abilitanti al fine di migliorare la capacità nell'interscambio delle informazioni tra le istituzioni, ad oggi rallentata principalmente da un'elevata eterogeneità nella ricezione, archiviazione e condivisione dei dati.

La funzione di raccordo di cui sopra, pertanto, nell'ottica di garantire la piena attuazione del piano triennale AgID, è supportata, a titolo esemplificativo, dall'utilizzo di strumenti di raccolta dei servizi a livello regionale e provinciale sotto piattaforme nazionali (AppIO).

Sulla base di tali premesse, nell'ottica di garantire la piena attuazione delle indicazioni fornite dall'Agenzia, numerose amministrazioni, tra cui anche il MIMIT, hanno intrapreso un percorso volto ad una sempre maggiore adozione delle piattaforme a disposizione – quali pagoPA, SPID e CIE ecc.

6.1.3.1 Obiettivi AgID

Analizzato il Piano Triennale redatto dall'AgID, sono state individuate le seguenti direttrici di azione a cui l'Amministrazione potrà ispirarsi per l'attuazione del proprio piano di digitalizzazione, in particolare:

- **Favorire l'evoluzione delle piattaforme già in uso.** Le PA dovranno aderire alle piattaforme nazionali abilitanti quali SPID (Sistema Pubblico di Identità Digitale), pagoPA (sistema di pagamenti alla PA), AppIO (app per interagire con tutti i servizi nazionali e territoriali), ANPR (Anagrafe Nazionale della Popolazione Residente), CIE (Carta d'Identità Elettronica), NoiPA (consultazione documenti stipendiali del personale pubblico), e continuarne l'adeguamento ai nuovi avanzamenti tecnologici e in materia di sicurezza.
- **Aumentare il grado d'adozione e utilizzo delle piattaforme da parte di PA e cittadini,** sia in termini di utenze che di flusso di dati. A tal fine dovranno essere ampiamente adottati i sistemi di identificazione digitale SPID e CIE, a sostituzione, o a supporto dei vecchi sistemi basati su credenziali proprietarie (nome utente e password). Previste nel piano sono anche le piattaforme pagoPA, per la gestione dello stipendio del personale; AppIO per la raccolta di servizi dislocati sul territorio.
- **Incrementare e razionalizzare il numero di piattaforme per le amministrazioni al fine di semplificare i servizi ai cittadini.** Tramite l'incremento del numero di piattaforme a disposizione delle PA e dei cittadini, e l'aumento dei servizi su quelle preesistenti, come AppIO. Verranno inoltre creati nuovi sistemi che fungeranno da raccordo tra i sistemi territoriali e nazionali oltre che tra le PA (per esempio per favorire lo scambio di dati tra le amministrazioni nazionali). Tra queste, si citano a titolo esemplificativo e non esaustivo: INAD (Indice Nazionale Domicili Digitali), PND (Piattaforma Notifiche Digitali, un sistema di notifiche elettroniche a sostituzione della raccomandata), PDND (Piattaforma Digitale Nazionale Dati e interoperabilità, per la condivisione di informazioni tra enti e istituzioni), SDG (Sistema Gestione Deleghe, che permette di digitalizzare le deleghe).

6.1.3.2 Definizione AS-IS

Sulla base degli obiettivi AgID, con particolare riferimento all'evoluzione delle piattaforme esistenti, il Ministero ha adottato i servizi NoiPA e pagoPA, quest'ultimo attivo dal 2018, con aggiornamenti alla versione web effettuati a febbraio del 2020, entrambi utilizzati a pieno regime. Ha inoltre aderito all'applicazione AppIO, che, adottata esclusivamente per il lancio e l'erogazione del "bonus decoder", dovrà essere pienamente integrata nel loro parco applicativo. Infine, il Ministero ha realizzato la piena implementazione di un riconoscimento Single Sign On basato sulle piattaforme SPID, CNS e EIDAS, il cui uso sarà dunque incluso nel presente Piano.

Da un'analisi effettuata sul parco applicativo del Ministero, è stato riscontrato un progresso parziale nel grado di adozione delle piattaforme abilitanti. Il Ministero offre in totale più di 80 servizi che sono rivolti al cittadino e alle altre Direzioni interne al Ministero. Di questi, circa 30, che corrispondono al 34% dei servizi, è dotato di almeno un sistema di accesso (SPID/CIE e/o credenziali proprietarie). Dei circa 30, soltanto 10 sono stati aggiornati al nuovo sistema SPID/CIE (il 34.5% del totale). Tra l'altro, molti dei servizi aggiornati utilizzano SPID e CIE congiuntamente al vecchio sistema di credenziali per garantire un servizio anche agli utenti al di fuori della CE. I restanti 20 servizi circa necessitano di un aggiornamento ai nuovi sistemi di identificazione.

L'analisi effettuata rappresenterà il punto di partenza per avviare un processo di razionalizzazione, necessario per il Ministero al fine di valutare lo stato del proprio parco applicativo oltre che l'adozione delle Linee Guida AgID.



6.1.4 D. Infrastruttura

L'implementazione di una Infrastruttura Digitale che sia in grado di garantire un elevato livello di efficienza dei servizi offerti dalla Pubblica Amministrazione ai *Dipendenti stessi*, ai *Cittadini* e alle *Imprese*, è diventata un elemento indispensabile nello sviluppo di una strategia digitale efficace e coerente con gli obiettivi stabiliti. Il Piano Triennale per l'informatica nella Pubblica Amministrazione, emanato da AgID, nel suo ultimo aggiornamento, con l'intento di guidare le PA nello sviluppo delle proprie Infrastrutture Digitali, ha individuato l'insieme di azioni necessarie per l'ammodernamento dei Data Center afferenti alle PA al fine di soddisfare tutti gli standard nazionali ed europei.

Il nuovo Piano Triennale (aggiornamento 2022-2026), in continuità con il precedente, ha messo in evidenza la necessità di applicare l'approccio "**Cloud First**" a tutti i progetti di digitalizzazione delle infrastrutture afferenti alle Amministrazioni Nazionali. Pertanto, a supporto di tale approccio, con il Piano Nazionale di Ripresa e Resilienza (PNRR) sono stati espressamente previsti degli investimenti al fine di accelerare ed agevolare la transizione al Cloud (nello specifico con i due investimenti: "Investimento 1.1: Infrastrutture digitali" e "Investimento 1.2: Abilitazione e facilitazione migrazione al cloud").

Secondo il principio *Cloud first*, quanto oggi è *on-premises*, necessita di essere migrato su infrastrutture Cloud al fine di migliorare la qualità e la sicurezza dei servizi che le Amministrazioni locali sono in grado di offrire ai cittadini e alle imprese, oltre che ai dipendenti stessi. Qualora si effettui la definizione di un nuovo progetto e/o sviluppo di un servizio, le Amministrazioni devono valutare in via prioritaria l'adozione del paradigma Cloud.

Di conseguenza, in relazione a tale contesto di riferimento, l'Amministrazione, in armonia con il *Digital Europe Programme* e dell'attuale Piano Triennale per l'informatica nella Pubblica Amministrazione, deve avviare un insieme di specifiche iniziative volte a garantire, sia per la propria infrastruttura locale che per tutti i settori di interesse pubblico, una infrastruttura ICT affidabile, sicura, energicamente efficiente ed economicamente sostenibile.

6.1.4.1 Obiettivi AgID

Il capitolo riservato alle infrastrutture si occupa di definire gli obiettivi sui quali le PA devono focalizzarsi al fine di potenziare le infrastrutture per migliorare la capacità di generare ed erogare servizi digitali e di qualità, in linea con il Piano Triennale, redatto dall'Agenzia per l'Italia digitale (AgID). In particolare:

- **Migliorare la qualità e la sicurezza dei servizi digitali** erogati dalle Amministrazioni locali, migrandone gli applicativi *on-premise* (data center Gruppo B) verso infrastrutture e servizi cloud qualificati, aumentando il numero di amministrazioni locali migrate (#1.064 è il target 2023).
- **Migliorare la qualità e la sicurezza dei servizi digitali** erogati dalle Amministrazioni centrali migrandone gli applicativi *on-premise* (data center Gruppo B) verso infrastrutture e servizi cloud qualificati, **incluso PSN**, aumentando il numero di amministrazioni locali migrate (#30 è il target 2023).
- **Migliorare la fruizione dei servizi digitali per cittadini ed imprese** tramite il potenziamento della connettività per le PA, verificando la disponibilità di servizi di connettività Internet a banda larga e ultra-larga per le PA locali e aggiornando i servizi di connettività a banda ultra-larga nel contratto SPC connettività.

6.1.4.2 Definizione AS-IS

L'attuale struttura delle infrastrutture ICT (centro elaborazione dati, reti/connettività, etc.) è stata, nel tempo, guidata dalle diverse esigenze delle singole direzioni o uffici, per cui si riscontra, oggi, mancanza di omogeneità nella struttura con conseguente necessità di razionalizzazione e consolidamento delle stesse (es. dismissione dei data center obsoleti e inefficienti), che sono attualmente categorizzate – secondo il "Censimento del patrimonio ICT della Pubblica Amministrazione"- come gruppo B, in altre parole necessitano di essere migrate verso servizi cloud qualificati e data center più sicuri.

Pertanto, l'infrastruttura attuale può essere considerata di tipo tradizionale, si costituisce di componenti tecnologicamente superate che espongono a diversi rischi (es. *downtime*, *sicurezza*) e impattano in termini di performance, con ripercussioni inevitabili sull'erogazione e la qualità dei servizi offerti, oltreché che sulla produttività del lavoro dei dipendenti (es. scarsa capacità di accesso ai dati, tempi di attesa più lunghi ecc.).

Non è presente documentazione a supporto dell'attuale disegno dell'Infrastruttura.

Non ultimo si evidenzia la necessità di potenziamento, soprattutto in termini di connettività, per cui non dispone, ad oggi, di un'adeguata capacità di banda (talvolta, le sedi dell'Amministrazione del MIMIT dispongono di una copertura pari a 2048/512 kbps, sono pochissimi i casi in cui si superano i 10 mbps), con conseguenti impatti:

- sulla possibilità di soddisfare le necessità interne e di cooperazione;
- sui flussi di lavoro: difficoltà nel passare da pratiche tradizionali a procedimenti digitalizzati;
- sulla produttività e fruizione dei servizi digitali sia per i dipendenti dell'Amministrazione che per i cittadini e le imprese.

L'infrastruttura ICT corrente rimarca, in aggiunta, il bisogno di conformità, in termini di connettività, ai livelli di sicurezza, agli standard internazionali e alle raccomandazioni del CERT-PA e di monitoraggio dell'intera infrastruttura fisica per intervenire tempestivamente in caso di necessità.

In tale contesto appare quindi evidente come uno degli obiettivi a cui l'Amministrazione debba puntare sia il consolidamento e miglioramento sia in termini di efficienza operativa che di prestazioni dei servizi, mediante la migrazione verso il Cloud, che abilita ad una maggiore flessibilità, affidabilità, scalabilità e sicurezza dei servizi, in particolare per quei servizi che sono critici o strategici.

In coerenza con gli obiettivi dell'Amministrazione e tenendo conto dei target e delle tempistiche del piano Triennale AgID, l'Amministrazione:

- trasmetterà, al DTD e all'AgID, il proprio piano di migrazione verso infrastrutture e servizi cloud qualificati, mediante una piattaforma dedicata messa a disposizione dal DTD come indicato nei Regolamenti - CAP4.PA.LA16 e CAP4.PA.LA22, entro febbraio 2023.
- potrà acquistare i servizi della nuova gara di connettività SPC.



6.1.5 E. Interoperabilità

In linea generale, il concetto di interoperabilità⁶, che è relativo all'interazione ed all'interscambio in diversi ambiti, compreso quello informatico, misura il grado di sinergia in diversi ambiti e tra sistemi diversi per facilitare lo scambio e il riutilizzo delle informazioni.

Con l'obiettivo di favorire l'interoperabilità tra le Pubbliche Amministrazioni, le direttive al livello nazionale individuano alcuni punti di sviluppo riguardanti specifiche iniziative di raccordo operativo, in un'ottica sia interna alle amministrazioni che esterna rivolta quindi al cittadino.

Tali linee di sviluppo saranno caratterizzate dalle seguenti attività:

- la reingegnerizzazione dei processi e la digitalizzazione delle procedure, includendo come dettagliato nei successivi paragrafi, la progettazione di nuovi sistemi e servizi;
- il processo di diffusione e l'adozione delle piattaforme abilitanti di livello nazionale, nonché la razionalizzazione di quelle già esistenti;
- la definizione di tecniche di interoperabilità da individuare per specifici domini.

Sebbene focalizzato sulla sfera tecnica dell'interoperabilità, come previsto dalle Linee Guida AgID, il presente paragrafo ne prevede anche il riferimento al livello giuridico, organizzativo e semantico.

⁶ Si specifica che, sebbene focalizzato sulla sfera tecnica dell'interoperabilità, come previsto dalle Linee Guida AgID, il presente paragrafo ne prevede anche il riferimento al livello giuridico, organizzativo e semantico. Per un approfondimento ai concetti di "interoperabilità semantica" e di "sicurezza" si rimanda rispettivamente al Capitolo 2 – Dati e al Capitolo 6 – Sicurezza informatica del Piano Triennale per l'informatica 2021 – 2023 rilasciato da AgID.

6.1.5.1 Obiettivi AgID

Gli obiettivi definiti da AgID in materia di interoperabilità sono orientati a favorire un sistema collaborativo e di interscambio tra amministrazioni e tra amministrazioni ed enti terzi, maggiormente efficace ed efficiente.

L'interesse espresso dall'Amministrazione rimanda a quanto prescritto da AgID riguardo lo sviluppo di API e servizi orientati al popolamento della Piattaforma Digitale Nazionale Dati (PDND).

La PDND, essenziale per favorire la conoscenza e l'utilizzo del patrimonio informativo detenuto, nonché per la condivisione dei dati con diritto di accesso, rende possibile l'interoperabilità dei sistemi informativi mediante l'accreditamento, l'identificazione e la gestione dei livelli di autorizzazione dei soggetti abilitati ad operare sulla stessa. In aggiunta, la PDND consente la raccolta e la conservazione delle informazioni relative agli accessi e alle transazioni effettuate suo tramite.

Le indicazioni fornite da AgID e riguardanti il Modello di Interoperabilità per la PA individuano standard e modalità di utilizzo per l'implementazione delle *Application Programming Interface* (API) favorendo in tal modo:

- l'aumento dell'interoperabilità tra PA comprendendo anche un'evoluzione nel rapporto con cittadini ed imprese del territorio;
- la qualità e la sicurezza delle soluzioni realizzate;
- la de-duplicazione e la co-creazione delle API.

Tali risultati si declinano in maniera ancor più specifica nei seguenti obiettivi rintracciabili all'interno delle Linee Guida AgID:

- **Favorire l'applicazione della Linea Guida da parte degli erogatori di API** tramite il loro incremento sul catalogo Developers Italia e la registrazione delle amministrazioni sullo stesso sito. In tal modo, le PA potranno adottare il modello interoperabilità di AgID e realizzare API conformi.
- **Adottare API conformi al Modello suggerito da AgID** tramite l'incremento del numero di PA registrate sul catalogo PDND e fruitrici di API. Le PA registreranno sul catalogo i servizi conformi al modello.
- **Adottare modelli e regole per l'erogazione integrata di servizi interoperabili** tramite l'ampliamento del numero di PA coinvolte nell'adozione del Modello AgID, che dovrà tuttavia essere in parte personalizzato indicando eventuali discrepanze con le specifiche esigenze.

Si potrà, in particolare, fare riferimento agli obiettivi AgID, esponendo i propri servizi tramite API conformi registrandole sul catalogo reso disponibile dalla PDND, quale componente unica e centralizzata realizzata per favorire la ricerca e l'utilizzo delle medesime.

6.1.5.2 Definizione AS-IS

In maniera complementare a quanto descritto nel Cap.2 “Dati” del Piano Triennale per l’informatica, la componente relativa all’interoperabilità non è stata fino ad ora oggetto di una dedicata analisi da parte del MIMIT.

L’attuale patrimonio informativo dell’Amministrazione presenta un elevato grado di frammentazione che non ne permette la gestione centralizzata da parte di un’unica entità. Allo stesso tempo, il suo valore è elevato sia in termini di varietà dei dati presenti che di utilità degli stessi per le altre istituzioni pubbliche e i cittadini.

Da una prima analisi effettuata sui servizi riconducibili al Ministero, sono emersi alcuni database che potrebbero apportare un valore aggiunto all’efficienza dell’attività di tutta la Pubblica Amministrazione una volta resi parte integrante del piano di interoperabilità che la coinvolgerà. Tra questi, le informazioni sui dati di trasparenza presenti sul portale del MIMIT (che raccoglie albi, liste di incarichi e altri dati di competenza del Ministero). A questi si possono aggiungere dati relativi al registro nazionale degli aiuti di stato e banca di enti controllati dal MIMIT (ad esempio, la banca dati Infratel sulle reti internet e la banca dati SINFI sulla banda ultra-larga).

Risulta, quindi, fondamentale da parte del Ministero continuare a seguire il percorso tracciato nel documento AgID per l’implementazione di un numero crescente API per questi ed altri servizi, per popolare il catalogo reso disponibile dalla PDND, essenziale per perseguire l’obiettivo dell’interoperabilità.



6.1.6 F. Sicurezza Informatica

L’innovazione tecnologica dell’ultimo decennio ha comportato il bisogno di un’accelerazione nella definizione dei processi di digitalizzazione della Pubblica Amministrazione. Questo processo simboleggia una valida occasione di crescita e sviluppo, nonché di miglioramento della vita dei cittadini e del Paese in ambito internazionale. Tuttavia, queste dinamiche hanno contribuito all’aumento del rischio di esposizione della PA a vulnerabilità e minacce di tipo cibernetico, impattanti su tutto il patrimonio informativo dei sistemi pubblici con una conseguente perdita di dati e relativi danni di natura economica e/o reputazionale. Tale rischio viene accentuato dalla mancanza di adeguati strumenti di difesa nei confronti delle minacce emergenti; primo fra tutti è quello hacker attraverso i *ransomware*, software malevoli che sfruttano le vulnerabilità della rete per entrare nei sistemi operativi criptando file sensibili.

Per assicurare il coordinamento tra i soggetti pubblici e la realizzazione di azioni volte a garantire la sicurezza e la resilienza cibernetica per lo sviluppo digitale del Paese, nel 2021 è stata istituita l’Agenzia Nazionale per la Cybersecurity (ACN) che ha elaborato la Strategia Nazionale di Cybersicurezza (2022-2026) e l’annesso Piano di implementazione, con lo scopo di “pianificare,

coordinare e attuare misure tese a rendere il Paese più sicuro e resiliente anche nel dominio digitale”.

In un’ottica di prevenzione di tali scenari, la strategia di sicurezza cibernetica nazionale colloca nel proprio perimetro l’ACN nel ruolo di “Autorità” a tutela degli interessi nazionali e della resilienza dei servizi e delle funzioni essenziali dello Stato contro le minacce cibernetiche.

6.1.6.1 Obiettivi AgID

Il Piano Triennale, redatto dall’ Agenzia per l’Italia digitale (AgID), definisce una serie di obiettivi concreti e linee d’azione in ambito di sicurezza informatica, tramite un approccio orientato alla sicurezza come opportunità di crescita, proponendo la realizzazione di un ecosistema ICT sicuro e resiliente per offrire ai cittadini e alle imprese servizi digitali efficaci in completa sicurezza. Vengono individuate le seguenti direttrici di azione a cui l’Amministrazione potrà ispirarsi:

- Aumentare la consapevolezza del rischio *cyber* (*Cyber Security Awareness*) nelle PA con il seguente *risultato atteso*:
 - Incremento del livello di Cyber Security Awareness misurato tramite questionari di self-assessment ai RTD (Responsabile per la Transizione al Digitale). Dovendo fornire servizi sicuri ed affidabili ai cittadini, è molto importante che all’interno delle pubbliche amministrazioni venga sviluppata la Cyber Security Awareness, ovvero la conoscenza di minacce, rischi e delle best practices nell’ambito della sicurezza IT all’interno delle organizzazioni. È fondamentale che tale consapevolezza risulti diffusa a tutti i livelli organizzativi, da quelli apicali a quelli operativi. Al fine di valutare e di incrementare il grado di conoscenza in materia di sicurezza informatica degli RTD (Responsabile per la Transizione Digitale), figura chiave per la trasformazione digitale della pubblica amministrazione, verranno somministrati dei questionari di auto valutazione con l’obiettivo di erogare corsi di formazione mirati a colmare eventuali divari.
- Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione con i seguenti *risultati attesi*:
 - Incremento del numero dei portali istituzionali che utilizzano il protocollo HTTPS only, misurato tramite tool di analisi specifico. Ad ogni cittadino/utente che utilizzi un portale istituzionale della Pubblica Amministrazione, dev’essere garantito un determinato standard di sicurezza che consenta la fornitura di servizi efficaci, sicuri ed affidabili. A tal fine verrà implementato sui portali della PA il protocollo HyperText Transfer Protocol over Secure Socket Layer (HTTPS), tramite il quale la comunicazione su Internet viene criptata attraverso crittografia asimmetrica, consentendo un alto livello di sicurezza. L’adozione di tale protocollo verrà monitorata utilizzando uno strumento di analisi specifico sviluppato dal Computer Emergency Response Team (CERT) di AgID.
 - Massimizzare il numero dei Content Management System (CMS) non vulnerabili utilizzati nei portali istituzionali delle PA, misurato tramite tool di analisi specifico. I

portali istituzionali della pubblica amministrazione necessitano dell'ausilio di Content Management System (CMS), software che permettono ad un operatore, con qualsiasi formazione, di gestire i contenuti da pubblicare su un sito web. Per aumentare il livello di sicurezza dei portali istituzionali è necessario ridurre al minimo i CMS vulnerabili ad attacchi e minacce cibernetiche. La vulnerabilità di tali software verrà monitorata utilizzando uno strumento di analisi specifico sviluppato dal Computer Emergency Response Team (CERT) di AgID.

A supporto degli obiettivi AgID, la Strategia Nazionale di Cybersicurezza 2022-2026, ispirata ad un approccio "whole-of-society" che vede la collaborazione sinergica di tutta la società, punta ad affrontare cinque sfide chiave quali:

- il rafforzamento della resilienza nella transizione digitale del sistema Paese;
- il conseguimento dell'autonomia strategica nella dimensione cibernetica;
- l'anticipazione dell'evoluzione della minaccia cyber;
- la gestione di crisi cibernetiche;
- il contrasto della disinformazione online.

Per affrontare tali sfide vengono individuati obiettivi strategici, ciascuno dei quali è declinato su più aree tematiche, in funzione di specifiche misure ("obiettivi attuativi") che l'Agenzia intende raggiungere entro il 2026.

6.1.6.2 Definizione AS-IS

Il Ministero delle Imprese e del Made in Italy opera sulla sicurezza informatica attraverso tre strumenti principali:

- Normativo: con le "Politiche di sicurezza e conduzione dei sistemi informativi del Ministero delle Imprese e del Made in Italy" (c.d. Policy di Sicurezza) e le Misure minime di sicurezza AgID, che delineano le linee guida mandatorie in termini di sicurezza e le medesime strategie ad alto livello;
- Tecnico: attraverso l'ausilio di molteplici tecnologie ed apparati che vanno dalla sicurezza perimetrale (firewall, apparati di segmentazione della rete, accesso remoto tramite SSL-VPN, sistemi per la *multifactor authentication*) ad avanzati sistemi di monitoraggio (PRTG, SIEM) passando per infrastrutture di *content filtering* (proxy, sandbox, antispam, anti malware centralizzato) e per finire con strumenti a protezione dei PC, basati su agent (antivirus, EDR, *agent siem, application control, Vulnerability Management*);
- Organizzativo: attraverso servizi professionali in ambito cyber security (ad esempio, tramite l'introduzione di un *Security Operation Center* interno (SOC), ovvero un meccanismo di gestione e governance degli strumenti tecnici e normativi).

I ruoli e le responsabilità individuate per la gestione delle attività di cybersecurity relative al MIMIT, ed in capo alla Divisione V – Sistemi Informativi e trasformazione digitale, fanno riferimento alle seguenti strutture/unità organizzative:

- CSO – Chief Security Officer;
- ULS – Unità Locale di Sicurezza;
- SOC MIMIT– Presidio SOC interno al MIMIT;
- Sistemi Informativi – Gruppi operativi che hanno in carico tutto l’IT (ad eccezione di quanto in carico al SOC MIMIT) del Ministero.

Nello specifico è il CSO che definisce, sulla base del mandato istituzionale, gli obiettivi e le strategie di Sicurezza. È il diretto responsabile della definizione degli standard tecnici per lo sviluppo dei sistemi informativi, di telecomunicazione e fonia e per la predisposizione, aggiornamento, attuazione e vigilanza sul rispetto del piano di sicurezza informatica del Ministero.

Sul piano della gestione della continuità aziendale, avendo le Amministrazioni un’operatività sempre più legata ad un patrimonio informativo dematerializzato e affidando a supporti virtuali la maggior parte delle funzioni essenziali, risultano soggetti a guasti e rapida obsolescenza. Per tale motivo, diventa cruciale pianificare processi e ricorrere a soluzioni in grado di prevedere la problematica e porre rimedio agli attacchi o agli eventi disastrosi che danneggiano o distruggono i supporti di raccolta dei dati.

Nel contesto del Ministero, partendo dagli indicatori di qualità operativi riferiti alla disponibilità dei sistemi e dei servizi dell’Amministrazione è possibile caratterizzare i servizi in due fasce, A per i servizi di maggior importanza e B per quelli di importanza ordinaria. Ognuna di queste due aree a sua volta si declina in altre due sottocategorie che prendono in considerazione i relativi valori di RTO (intervallo temporale ammissibile di indisponibilità dei sistemi in seguito ad un evento malevolo) e di RPO (ammontare massimo di dati che possono essere persi in seguito ad un evento malevolo). In quest’ottica è possibile classificare i servizi del Ministero su quattro livelli di criticità:

- A1 - Altissima: in questa categoria rientrano i servizi che hanno RPO = 0 ed RTO = 0 e che in pratica non possono essere interrotti e che non possono tollerare alcuna perdita di dati;
- A2 - Alta: in questa categoria rientrano i servizi che hanno RPO = 0 ma RTO > 0 (ed inferiore ad un’ora);
- B1 - Media: in questa categoria rientrano i servizi con RPO > 0 (ma inferiore ad un’ora) ed RTO > 0 (ed inferiore a 4 ore);
- B2 - Bassa: in questa categoria rientrano i servizi con RPO > 0 (ed inferiore ad un giorno) ed RTO > 0 (ed inferiore ad un giorno).

6.2 Introduzione alle Linee Programmatiche

In coerenza con il focus del Piano Strategico, incentrato sulla progettazione e sulla personalizzazione delle componenti tecnologiche definite dall’AgID, il presente paragrafo ripercorre le Linee Programmatiche individuate e contestualizzate all’interno del contesto ministeriale.



6.2.1 Linea programmatica: Workspace e Digital Adoption

La trasformazione digitale delle PA non si basa solo sull'introduzione di nuove soluzioni tecnologiche, ma richiede che i cambiamenti e l'innovazione siano accompagnati da un'evoluzione delle conoscenze e delle competenze degli individui e generino una nuova consapevolezza nei singoli.

In tale contesto, la presente linea programmatica intende introdurre il percorso di evoluzione dell'esperienza del dipendente verso il Digital Working, basandosi sui capisaldi del *change management*, che consentono di mettere in evidenza l'importanza di una cultura lavorativa per obiettivi e di una comunicazione e collaborazione agile, digitale e trasversale che permette di superare le barriere dei singoli uffici (divisioni/direzioni) e i confini logistici (es. ispettorati diffusi su tutto il territorio nazionale).

Tale percorso tiene conto anche dello svolgimento del "Lavoro Flessibile", prevedendo formazione attiva e specifica sull'adozione e utilizzo dei tool digitali e definendo anche processi adeguati, con conseguenti benefici in termini di ottimizzazione dei processi interni stessi ed efficientamento nell'erogazione dei servizi.

La linea programmatica si articola in tre fasi:

- **Lancio:** per creare consapevolezza sul cambiamento e sulle evoluzioni nella modalità di lavoro, attraverso un piano di comunicazione dell'alto management verso i dipendenti delle diverse divisioni/direzioni del MIMIT.
- **Sperimentazione:** creazione di gruppi pilota per adottare il modello e valutarne la rispondenza, studiando i risultati e gli effetti sul lavoro.
- **Estensione:** il modello è stato esteso a tutti i dipendenti, implementando strategie di formazione e fornendo assistenza in modo personalizzato.

Al termine di questo percorso è utile avviare una fase di rinforzo, per monitorare la situazione e intervenire con azioni disegnate ad hoc sulle specifiche esigenze, coinvolgendo anche i dipendenti dislocati presso sedi regionali con eventi "open day" e "workshop".

A tal fine, saranno previsti, nel presente Piano, differenti interventi:

- Scouting e adozione di strumenti/piattaforme di collaborazione più idonee e in linea con le esigenze dell'Amministrazione.
- Abilitare la possibilità di lavorare sia in sede, sia in mobilità sia in remoto avendo a disposizione sempre tutti gli strumenti di cui si necessita per svolgere le proprie attività.
- Investimento nell'innovazione anticipando il cambiamento, al fine di essere pronti per le trasformazioni.
- Accompagnare l'investimento tecnologico con iniziative di *change management* per agevolare il cambiamento organizzativo e culturale.

- Evolvere le professionalità coerentemente con le nuove modalità lavorative, al fine di massimizzare il potenziale e accrescere il benessere delle persone.

Tale linea programmatica favorisce sia un miglioramento della qualità e della produttività del lavoro dei dipendenti sia un miglioramento della qualità dei servizi forniti dall'amministrazione al dipendente, al cittadino e alle imprese, oltreché una riduzione dei costi.



6.2.2 Linea programmatica: Razionalizzazione del catalogo dei servizi

Il Ministero ha la necessità di rinnovarsi continuamente al fine di rispondere alla richiesta di servizio dell'utenza e ai sempre maggiori compiti assegnati dal Legislatore. Le esigenze dell'utenza, interna ed esterna, sono in rapido cambiamento, per via del processo di trasformazione delle imprese, iniziato in parte con il PNRR, e per i numerosi servizi che il Ministero deve garantire, caratterizzati molto spesso da velocità di realizzazione ed erogazione.

Il Ministero necessita di razionalizzare i servizi e le attività correlate al fine di soddisfare le aspettative dei diversi segmenti di utenza, puntando su una personalizzazione del servizio e sulla proattività nell'erogazione dello stesso. Tale necessità impone, come *starting point*, una razionalizzazione dell'attuale catalogo dei servizi, identificando per ciascuno il proprio segmento di utenza.

In tale contesto, la linea programmatica *Razionalizzazione del catalogo dei servizi* ha l'obiettivo di reingegnerizzare ed ottimizzare i servizi del Ministero. In questa, rientrano tutte le attività che permettono di identificare le modalità di costruzione del catalogo dei servizi e il mantenimento dello stesso, permettendo in tal modo di poter intervenire facilmente sull'aggiornamento e rinnovamento del "ecosistema dei servizi" del Ministero.

Al fine di poter garantire un pieno soddisfacimento dei *needs* dell'utenza, il Ministero deve intervenire sia sugli utenti interni, intesi come funzionari del Ministero e le altre direzioni, che sugli utenti esterni, cittadini, imprese e media. A tal fine, saranno previsti, nel Piano, differenti interventi per ciascun segmento identificato:

- Razionalizzare il catalogo dei servizi per gli utenti esterni, attraverso:
 - la **definizione del ciclo di vita del servizio nel Ministero**, inteso come la definizione delle modalità di creazione, le policy interne per la gestione e i criteri minimi che il servizio deve garantire per un'erogazione efficiente dello stesso;
 - la **definizione del "catalogo as-is"**, da utilizzare come base per l'evoluzione del modello dei servizi del Ministero, identificando i servizi "*core*" e i servizi a supporto del cittadino e imprese;
 - la definizione del "**catalogo dei servizi to-be**", comprensivo dei nuovi servizi del Ministero e dei servizi esistenti evoluti e/o reingegnerizzati;

- **l'identificazione di metriche di monitoraggio** interne, per misurare l'efficienza nell'implementazione del servizio, ed esterne, per monitorare la *customer satisfaction* dell'utente finale, imprese e cittadini;
- **l'adozione di sistemi di monitoraggio e improvement avanzato**, come *Artificial Intelligence* per migliorare la *user experience* e *analytics* per l'ottimizzazione delle prestazioni;
- definizione del catalogo dei servizi TO-Be, reingegnerizzazione di alcuni dei servizi esistenti e sviluppo di nuovi servizi
- Razionalizzare il catalogo dei servizi per gli utenti interni, attraverso:
 - la **definizione delle policy di realizzazione dei servizi interni**, funzionali a standardizzare l'accesso al servizio e definire le modalità di creazione dello stesso;
 - la **definizione del catalogo dei servizi interni**, prettamente IT, con il dettaglio del perimetro, delle modalità di ingaggio della Divisione V e gli standard per garantire aderenza alle strategie, tecnologiche e procedurali, del Ministero;
 - la **reingegnerizzazione delle piattaforme** esistenti e **l'implementazione di nuove piattaforme** a supporto del nuovo modello di servizio del Ministero;
 - la **piena adozione del catalogo dei servizi IT**, abilitando in tal modo un processo strutturato per l'approvvigionamento di soluzioni tecnologiche all'interno del Ministero;
 - l'implementazione di piattaforme a supporto dei nuovi servizi e razionalizzazione delle piattaforme esistenti.

La linea programmatica "Razionalizzazione del catalogo dei servizi" si pone dunque l'obiettivo di rendere la Divisione V **punto di riferimento del Ministero per tutte le tematiche relative al ICT**. Tali interventi permetteranno un efficientamento di tutte le procedure di realizzazione dei servizi, per gli utenti esterni, e il soddisfacimento dei *needs* strettamente IT per gli utenti interni al Ministero.



6.2.3 Linea programmatica: Migrazione al Cloud

La presente linea programmatica permette all'Amministrazione di fornire servizi digitali e di disporre di infrastrutture tecnologiche sicure, efficienti ed affidabili, in linea con i principi di tutela della privacy, con le raccomandazioni delle istituzioni europee e nazionali, mantenendo le necessarie garanzie di autonomia tecnologica dell'Amministrazione, di sicurezza e controllo sui dati e aumentare la resilienza dei propri servizi digitali.

Il ricorso al Cloud permette di raggiungere tali obiettivi contribuendo, inoltre, ad aumentare l'efficienza energetica anche nell'ottica della sostenibilità ambientale.

Questo paragrafo si pone l'obiettivo di definire una strategia di indirizzo per l'adozione del Cloud Computing nell'Amministrazione (può essere implementata tramite un'infrastruttura pubblica, privata, ibrida o multi-cloud), alla luce delle sfide e dei rischi emergenti.

In linea con la Strategia Cloud Italia, per la definizione della linea programmatica, in merito alle scelte da compiere rispetto le diverse soluzioni di migrazione in cloud, l'Amministrazione terrà conto della classificazione e qualificazione dei dati e dei servizi per guidare e supportare il processo di migrazione.

Nel Piano Strategico ICT 23-25, saranno previsti diversi interventi:

- Adozione di una soluzione cloud mediante attuazione della *Cloud Adoption Roadmap*, costituita da tre *workstream*:
 - o *program enablement*: definizione del piano attuativo di migrazione (Masterplan) e ingaggio di tutti gli stakeholder coinvolti. La definizione ed elaborazione del piano è eseguita classificando dati e servizi sulla base del danno che una loro compromissione in termini di confidenzialità, integrità e disponibilità provocherebbe (dati e servizi strategici, critici e ordinari).
 - o *foundational*: progettazione e setup dell'ambiente cloud target che accoglierà i workload applicativi ed infrastrutturali.
 - o *workload migration*: progettazione esecutiva architettura target servizi applicativi e infrastrutturali e migrazione degli stessi, seguendo i principi e i canoni per la costruzione di una struttura cloud su approccio CI/CD (*Continuous Improvement/Continuous Development*), che prevede il continuo sviluppo e il continuo miglioramento dei processi.
- Definizione di un modello di *Cloud Adoption Governance* che preveda un re-design dei processi di gestione e ICT secondo un approccio agile, in grado di rispondere in maniera rapida ai cambiamenti introdotti dall'innovazione tecnologica e dall'adozione del Cloud.
- Rafforzamento delle competenze digitali e specialistiche in materia Cloud.

La realizzazione della linea programmatica favorisce l'Amministrazione attraverso:

- maggiore efficienza nella gestione di soluzioni tecnologiche e servizi digitali;
- la creazione di un'offerta più vasta e migliore di servizi digitali, sia per i dipendenti delle divisioni del MIMIT che per i cittadini e imprese;
- agilità nella gestione delle infrastrutture sfruttando un modello scalabile basato su servizi a consumo;
- miglioramento dell'efficienza energetica delle infrastrutture e maggiore sostenibilità ambientale grazie alla dismissione dei data center meno efficienti.



6.2.4 Linea Programmatica: Miglioramento delle modalità di erogazione del Servizio

La trasformazione digitale della PA richiede di disegnare, realizzare ed esporre servizi sempre più digitalizzati, garantendo un'interazione "proattiva" con l'utenza tramite tutti i *touchpoint* a

disposizione. La *customer journey* dell'utente diviene in tal modo fulcro nell'erogazione del servizio e tutte le PPAA devono mettere in campo soluzioni innovative volte a massimizzare l'esperienza utente e garantire la fruizione snella ed efficace del servizio.

Il Ministero necessita di intervenire su tale linea attraverso una customizzazione «*data driven*» dell'esperienza utente e implementando al contempo tutti i mezzi, hardware e software, per garantire l'accesso al servizio da parte degli utenti esterni, tra cui la connettività tra le sedi, propedeutica ad efficientare l'erogazione del servizio per gli utenti interni.

In tale contesto, la linea programmatica **miglioramento delle modalità di erogazione del Servizio**, si pone l'obiettivo di disegnare un nuovo modello di erogazione dei servizi, basato sull'ottimizzazione della *customer experience* dell'utente, e sulla costruzione di un "ecosistema dei servizi" in cui è prevalente la centralità dell'utente. Attraverso questa linea di intervento, sarà possibile adottare un approccio proattivo in grado di prevedere i *needs* degli utenti, imprese e cittadini.

In coerenza con le precedenti linee guida programmatiche, il Ministero dovrà intervenire sugli utenti interni ed esterni, garantendo in tal modo il soddisfacimento dei bisogni specifici per ciascun segmento di utenza:

- Miglioramento delle modalità di erogazione del servizio verso gli utenti esterni, attraverso:
 - **l'assessment delle modalità di erogazione del servizio**, potendo sfruttare gli output delle altre attività del presente Piano Strategico, con l'obiettivo di identificare la rispondenza degli attuali servizi con i criteri definiti da AgID, mappare le interdipendenze tra servizi e/o tra componenti tecnologiche a supporto del servizio e identificare spunti di miglioramento ed efficientamento anche nell'ottica della migrazione Cloud del parco applicativo del Ministero;
 - la **definizione del modello dei servizi to-be**, inteso come la definizione delle componenti tecnologiche abilitanti, a supporto dell'erogazione del servizio, e alla creazione di una Enterprise Architecture del Ministero. Tali progettualità permetteranno di sfruttare soluzioni di CRM, per l'ottimizzazione del *customer journey*, *Artificial Intelligence*, per il miglioramento del servizio in termini di *front-end* e *back-end*, e Data Analytics, per il monitoraggio attivo delle prestazioni dei servizi;
 - la **definizione degli interventi necessari alla trasformazione delle modalità di erogazione del servizio del Ministero**, attraverso l'identificazione dei gap architettonici e applicativi, e la prioritizzazione degli investimenti necessari per colmare tali gap al fine di raggiungere gli obiettivi delle linee guida programmatiche.
- Miglioramento delle modalità di erogazione del servizio verso gli utenti interni, attraverso:
 - il **potenziamento della rete e infrastruttura**, in coerenza con la linea programmatica identificata, al fine di rendere maggiormente inclusivo il servizio e sopperire a potenziali inefficienze dovute alla connettività;
 - la **reingegnerizzazione dei touch point** per l'utente interno, sfruttando pienamente le piattaforme nazionali per l'accesso, il pagamento e la fruizione del servizio;

- la **creazione di servizi “mobile first”** che permettano la fruizione dei servizi maggiormente utilizzati dagli utenti interni direttamente da remoto, tramite dispositivi mobili, al fine di snellire l'intero processo di erogazione degli stessi.

La linea programmatica “Miglioramento delle modalità di erogazione del Servizio” si pone dunque l'obiettivo di **trasformare l'attuale paradigma di erogazione del servizio del Ministero**, migliorando l'esperienza dell'utente esterno, ed efficientare tutti i processi interni per la creazione, erogazione e mantenimento del nuovo “ecosistema dei servizi”. Al contempo, la linea guida programmatica individuata ha l'obiettivo di migliorare l'esperienza degli utenti interni, abilitando l'accesso inclusivo ai servizi e migliorando la fruibilità degli stessi, abilitando in tal modo efficienze e sinergie di lungo termine.



6.2.5 Linea programmatica: Sicurezza informatica e *disaster recovery*

Il Ministero dell'Impresa e del Made in Italy, consapevole dei rischi in ambito sicurezza informatica che derivano dalla transizione digitale, intende impostare la digitalizzazione facendo riferimento non solo alla linea definita da AgID, ma, come già delineato in precedenza, anche al principale interlocutore istituzionale in ambito **sicurezza informatica**, ossia **l'Agenzia per la Cybersicurezza Nazionale** (ACN). Nel merito della realtà organizzativa del MIMIT, le attività di gestione del rischio possono tradursi in controlli di natura tecnologica, organizzativa e procedurale utili a valutare il livello di sicurezza informatica e volti a contrastare le minacce informatiche più frequenti, all'interno di un percorso continuo di monitoraggio e miglioramento.

Il presente Piano farà ampio riferimento a tale strategia, costituendo una linea guida che il Ministero intende adottare per il consolidamento degli aspetti di sicurezza centrali per la protezione del proprio patrimonio informativo e tecnologico, nell'ottica di una sinergica e strutturata interazione dei principi di **Risk Management, Business Continuity e Cybersecurity**.

Essendo la gestione del rischio informatico una parte fondamentale della progettazione e della gestione continuativa del sistema informativo, nell'ottica dei principi di **security by design**, già nella fase di definizione dei requisiti, la progettazione di un servizio deve prevedere una **valutazione del rischio**. Tale valutazione deve permettere di appurare la necessità di proteggere il servizio stesso e analizzare quanto una soluzione tecnica faciliti o, al contrario, ostacoli l'adozione di controlli adeguati.

Anche a fronte di un considerevole aumento di incidenti informatici o azioni ostili volti a compromettere il corretto funzionamento dei sistemi informativi o dei servizi erogati, le iniziative di AgID sono volte ad agevolare un sistema di prevenzione e di risposta efficiente delle singole amministrazioni.

Nel Piano Strategico ICT 23-25, saranno previsti diversi interventi:

- Definire un processo di analisi del rischio per poter ottenere, nel medio termine, una stima del **livello di rischio cyber** cui è esposta ciascuna PA;
- Rendere **autonomo** il Ministero nella pianificazione di interventi per **il trattamento del rischio** al fine di ridurlo ad un livello **ritenuto accettabile** (*risk appetite*);
- Ricondurre tali interventi a **convenzioni** già attive nell'ambito dei contratti quadro;
- Consentire il monitoraggio dell'implementazione di tali interventi al Ministero una volta affrontata **l'analisi del rischio**;
- Creare uno strumento di **monitoraggio** AgID esteso a tutti i dipartimenti;
- Diffondere tra tutti gli **stakeholders** coinvolti la **cultura** della **gestione del rischio cyber**.

Nello specifico, le macro-attività che verranno attivate per il MIMIT saranno delineate su due filoni principali:

1. Modello di Governo del Rischio, caratterizzato dalle seguenti attività:

- Definizione modello di **Maturity Assessment Cyber** (CMA) e strumento a supporto;
- **Assessment ISO27001** per la definizione di un SGSI e la valutazione delle misure di sicurezza implementate tramite rielaborazione e mapping di recenti attività di *assessment* svolte;
- Definizione modello organizzativo di **gestione del rischio**;
- Definizione e formalizzazione di **ruoli e responsabilità**;
- Definizione dei **flussi** e degli **output** di comunicazione del modello.

2. Dimensionamento Struttura di Governo del Rischio, caratterizzato dalle seguenti attività:

- Benckmarking funzioni IT *Security*;
- Benckmarking funzioni Privacy;
- Valutazione delle **competenze** presenti e mancanti ai fini del nuovo modello di gestione del rischio;
- Definizione piano di **dimensionamento** nel tempo della struttura di governo del rischio.

In particolare, la realizzazione della linea programmatica mira a migliorare e potenziare l'Amministrazione attraverso la diffusione della cultura del rischio *cyber*, con riferimento a:

- **Sviluppo sicuro** dei servizi, sulla base della rispondenza alle linee guida sullo sviluppo sicuro del software ed all'utilizzo del tool di risk assessment di AgID;
- **Familiarità** con i principi dell'analisi dinamica (DAST) e statica (SAST) del software;
- Introduzione all'approccio del **privacy/security by design**.
-



6.2.6 Linea programmatica: Dematerializzazione e conservazione sostitutiva

Nel percorso di modernizzazione dell'Amministrazione, anche la sfera della raccolta documentaria è stata influenzata. Dematerializzazione e conservazione sostitutiva, infatti, vanno avanti di pari passo alla digitalizzazione. Il processo di reingegnerizzazione dei procedimenti

dell'Amministrazione, compresi i servizi resi ai cittadini e alle imprese, si coniuga inevitabilmente con la conversione definitiva dei documenti dal formato cartaceo a quello digitale.

In tale contesto, la presente linea programmatica intende introdurre l'adozione di un percorso di gestione documentale digitale, nell'ambito del sistema informativo dell'Amministrazione, che garantisce la tracciabilità complessiva dei procedimenti, attraverso il trattamento elettronico di tutte le informazioni attinenti.

Questo percorso costituisce lo strumento essenziale per attuare il processo di dematerializzazione ai fini della conservazione sostitutiva, rendendo più economico, rapido e protetto l'invio di documenti e consentendo allo stesso tempo di ottimizzare i processi organizzativi.

In coerenza con il regolamento tecnico in materia, redatto dall'AgID, su deroga del Codice dell'Amministrazione Digitale (CAD), che stabilisce i requisiti tecnologici del sistema di conservazione - necessari a garantire la validità legale del documento stesso - la linea programmatica pone l'attenzione sugli aspetti più sensibili delle quattro fasi del percorso di gestione documentale digitale:

- Creazione: i documenti (digitale nativo o digitalizzati), all'atto della creazione, devono rispettare i canoni stabiliti dalla normativa. La corretta creazione del documento digitale garantisce l'autenticità originaria dello stesso prima del suo trasferimento al sistema di conservazione e alla sua successiva archiviazione.
- Versamento: passaggio del documento digitale dal sistema che lo ha generato al sistema di conservazione; questo passaggio è caratteristico in quanto richiede, come indicato dall'AgID, una serie di accortezze tecniche e tecnologiche ulteriori al semplice salvataggio del documento all'interno di spazio di archiviazione riservato (es. hard disk dedicato, spazio in cloud ecc). Tramite il versamento viene garantita l'integrità del documento all'interno dell'archivio digitale.
- Archiviazione: una volta che è versato, è quindi archiviato nel sistema di conservazione sostitutiva. L'obiettivo dell'archiviazione è quello di garantire l'affidabilità, la leggibilità e la reperibilità del documento digitale nel lungo periodo, in ottemperanza a quanto prescritto dalle norme civilistiche e fiscali in materia di conservazione della documentazione contabile.
- Distribuzione: la fase finale del processo di gestione documentale digitale consiste nella messa a disposizione, da parte del sistema di conservazione, dei documenti conservati ai soggetti che ne fanno richiesta. Questo passaggio del processo garantisce al soggetto che prende visione del documento tutte le caratteristiche proprie del documento digitale conservato a norma di legge: autenticità, integrità, affidabilità, leggibilità e reperibilità.

Nel PIANO saranno previsti interventi per la creazione del processo di Gestione Documentale tramite un insieme complesso di strumenti che permettono di svolgere e semplificare le procedure di archiviazione di documenti digitali indispensabili in questo contesto, in cui è imprescindibile la presenza e la produzione di documentazioni e la loro conseguente archiviazione. In particolare, la gestione elettronica dei documenti avverrà tramite software o piattaforme *opensource* che grazie

ad algoritmi specifici, consentono di registrare, ordinare, catalogare, semplificare la lettura e la trasmissione di dati nonché la loro conservazione

La realizzazione della linea programmatica facilita e velocizza lo svolgimento di certe attività lavorative dell'Amministrazione, snellisce alcune procedure burocratiche o amministrative e, garantisce una maggiore trasparenza delle banche dati nonché una buona tutela della privacy. Inoltre, garantisce ai dipendenti, ai cittadini e alle imprese servizi più rapidi, efficaci e sicuri, anche da remoto, e la riduzione generale dei costi legati alla stampa e all'archiviazione dei documenti cartacei e degli spazi fisici occupati, infine, permette una conservazione dei documenti più sicura e riduzione degli errori (legati alla ridondanza).



6.2.7 Linea programmatica: Definizione di un nuovo modello e pratiche di *Data Governance*

In un mondo in cui la velocità di acquisizione delle informazioni è sempre più cruciale, è necessaria l'elaborazione di sistemi di raccolta, di analisi e di tutela dei dati, che rappresenta un presupposto essenziale per l'implementazione di strumenti di analisi che migliorino il processo decisionale. Di conseguenza, risulta necessario l'investimento mirato ad una visione collaborativa ed integrata all'interno dell'ecosistema del Ministero dell'Impresa e del Made in Italy, per facilitare e ottimizzare la gestione dei dati provenienti dalle attività di una moltitudine di Unità Operative.

L'identificazione dei dati della PA come "patrimonio informativo" fornisce l'idea del grande valore che essi possiedono e delle potenzialità derivanti dal loro utilizzo strategico. La valorizzazione di tale patrimonio informativo pubblico rappresenta quindi un obiettivo cruciale per tutte le PPAA, tramite cui i dati possono diventare un'importante risorsa al fine di strutturare soluzioni strategiche al funzionamento efficiente della PA.

In particolare, per il contesto del Ministero dell'Impresa e del Made in Italy, è necessario adottare una strategia volta all'implementazione di un framework di *Data Governance* che permetta l'accentramento dei dati che oggi risultano sparsi e poco utilizzati, garantire servizi migliori agli interlocutori e agli utilizzatori degli stessi, migliorare l'interoperabilità dei servizi interni all'Amministrazione attraverso l'adozione di politiche e standard condivisi e ben strutturati.

L'obiettivo della linea programmatica è, quindi, garantire accessibilità, disponibilità e affidabilità dei dati sia all'interno dell'Amministrazione che verso gli utenti esterni in ottica di *Open Data*. Si articola nei principali interventi di seguito proposti:

- Definizione del framework di ***Data Governance Office*** individuando i ruoli organizzativi e le relative responsabilità necessari alla corretta gestione delle procedure di governo del dato e dei flussi informativi;
- Riorganizzazione del patrimonio informativo per indirizzare le esigenze del *core-business* e degli applicativi tramite attività di ***Data Modeling***;

- Automatizzazione dei controlli ed efficientamento della fase di “*ingestion*” e censimento delle informazioni all’interno degli applicativi tramite metodologie e tool di **Data Quality** supportate da sistemi di monitoraggio;
- Definizione di **Data Policy, Standard e Processi** adatti alla corretta gestione degli asset informativi tramite strumenti messi a disposizione dei diversi Uffici del Ministero dell’Impresa e del Made in Italy;
- Adozione di soluzioni di Intelligenza Artificiale e Machine Learning che permettono di processare, estrarre informazioni, analizzare e mettere in relazione dati eterogenei in modo più efficiente e più attendibile;
- Definizione di un *Service Business Layer* per aumentare la disponibilità e la fruibilità dei dati.

Diffondere la cultura del dato a tutte le direzioni del Ministero coinvolte nei processi di valorizzazione del dato, è un passaggio fondamentale per instradare gli interventi proposti al fine di eliminare la ridondanza del dato, aumentarne la qualità, incrementare l’interoperabilità e la condivisione delle informazioni sia interna che esterna.



6.2.8 Linea programmatica: Razionalizzazione del parco applicativo

Come per la maggior parte delle Pubbliche Amministrazioni, centrali e locali, il parco applicativo del Ministero delle Imprese e del Made in Italy risulta attualmente costituito da una pluralità di applicativi caratterizzati da interventi eseguiti nel tempo da soggetti interni ed esterni. La frammentazione della funzione IT che ha caratterizzato l’attività del Ministero negli ultimi anni, ha comportato un’oggettiva difficoltà di accentramento della conoscenza delle applicazioni in tema di necessità, utilizzo/utilità effettiva e necessità di aggiornamento.

L’eterogeneità delle applicazioni, la frammentazione e la necessità di avere un unico centro di responsabilità in materia IT, hanno spinto l’Amministrazione ad individuare la “Razionalizzazione del parco applicativo” quale ambito strategico fondamentale sul quale pianificare e avviare degli interventi nel corso del prossimo triennio.

Tale linea programmatica prevede l’adozione da parte dell’Amministrazione di una visione di lungo periodo basata su tre diverse **direttrici**, che possono essere identificate nelle seguenti fasi:

- Mappatura dei sistemi attualmente a disposizione, che, in qualità di attività propedeutica alle successive azioni, rappresenta il punto di partenza per conoscere lo stato del proprio parco applicativo ed individuare in maniera puntuale le principali cause di inefficienza;
- Analisi di dettaglio delle singole applicazioni per acquisire informazioni rilevanti, come ad esempio quali sono i soggetti che le utilizzano (interni o esterni al MIMIT) oltre che la percentuale e le modalità di impiego; qual è il valore che l’utente vi attribuisce;
- Razionalizzazione dell’attuale parco applicativo, che, sulla base delle evidenze emerse nelle fasi precedenti, potrà prevedere:
 - Acquisizione di nuove applicazioni;

- Laddove utile, integrazione di alcune delle applicazioni esistenti (soprattutto per quelle ritenute “core”) prevedendo un aggiornamento per la generazione di nuove funzionalità;
- Dismissione delle applicazioni inutilizzate poiché non più utili oppure basate su tecnologie ormai obsolete, anche nell’ottica di favorire l’ammodernamento delle infrastrutture.

Tale linea programmatica favorisce considerevoli ritorni in termini di benefici, più nello specifico incentrati su una **riduzione dei costi** di esercizio e di *application management*, la **semplificazione della gestione operativa**, **riduzione dei tempi** di risoluzione dei malfunzionamenti, l’**aumento dell’efficienza** dell’azione amministrativa, la **flessibilità** e la **sicurezza delle applicazioni**, agendo su quelle non più giustificate in termini di costi e utilità.



6.2.9 Linea programmatica: Razionalizzazione e ridisegno del Modello Operativo IT (Processi, procedure e standard)

Com’è noto, la gestione dell’ICT nel settore pubblico ha un ruolo chiave poiché concorre allo sviluppo dell’economia digitale di ogni Nazione. Se ben organizzata, infatti, favorisce il ripensamento dei processi che concorrono alla realizzazione delle Linee Guida AgID, che a loro volta facilitano la digitalizzazione della Pubblica Amministrazione, fattori imprescindibili per la crescita dell’economia. Il processo di trasformazione digitale attualmente in corso ha reso i sistemi informatici sempre più centrali nella gestione dei processi, delle procedure e degli standard della Pubblica Amministrazione centrale e locale.

Per questo motivo la definizione di un modello operativo IT è ormai di rilevanza strategica poiché deriva dalla necessità che questa Amministrazione si doti di una struttura in grado di rispondere alle richieste e alle aspettative degli *stakeholder*, facendo leva sullo sfruttamento delle nuove tecnologie e sulla loro integrazione con i sistemi esistenti.

In sinergia con quanto previsto dall’Obiettivo 4 – Evoluzione e disegno dei processi di *IT Governance*, la “Razionalizzazione e ridisegno del Modello Operativo IT” risponde all’esigenza espressa dal Ministero di progettare e implementare un modello che definisca, in modo chiaro, i processi abilitanti all’erogazione di servizi in ambito IT che documentino le modalità di interazione tra tutti gli *stakeholder* coinvolti oltre che le tecnologie adoperate. A questo fine, interviene sulla frammentarietà dei flussi organizzativi, attualmente distribuiti tra molteplici soggetti (interni ed esterni al MIMIT) che, per la loro molteplicità, necessitano di essere coordinati richiedendo una vera e propria *IT Governance*.

Tale linea programmatica prevede 3 diverse **direttrici**, che possono essere identificate nelle seguenti fasi:

- **Analisi**, basata sull’identificazione dei processi attualmente vigenti, al fine di rilevarne e descrivere tutti gli elementi che li caratterizzano per comprendere in modo preciso quali

sono gli attori a vario titolo coinvolti e quali ruoli rivestono nel complesso dell'organizzazione ministeriale;

- **Razionalizzazione** di quanto precedentemente individuato e analizzato che, coerentemente con la missione istituzionale del Ministero ed in linea con gli obiettivi che questa Amministrazione si propone di raggiungere nel periodo di competenza del Piano; è funzionale alla successiva fase;
- Definizione di un **disegno di evoluzione** dei processi attuali nonché di identificazione di nuovi per ottimizzare la gestione e l'implementazione delle soluzioni applicative.

Tali fasi/direttrici individuate potranno essere adottate dall'Amministrazione per intervenire puntualmente nelle aree che necessitano in maniera preponderante di una evoluzione e standardizzazione dei processi. In particolare:

- Gestione della domanda dei servizi IT;
- Gestione operativa dell'infrastruttura IT (*event, incident, problem, ecc*);
- Gestione e ottimizzazione della spesa IT;
- Gestione e aggiornamento del ciclo di vita dell'applicazione;
- Gestione del cambio release delle applicazioni e delle funzionalità;
- Program & Project Management.

La Linea Programmatica si articola principalmente nei seguenti interventi:

- Identificazione delle opportune **leve tecnologiche e organizzative** in risposta alle esigenze di evoluzione richieste;
- Azioni mirate sulla frammentarietà dei dati e sull'infrastruttura sempre più estesa e in evoluzione;
- Sviluppo di una **visione d'insieme** relativa ai dettagli tecnici e finanziari per consentire una corretta pianificazione delle risorse disponibili evitando, in tal modo, sprechi e costi non preventivati.

La realizzazione di questa linea programmatica favorisce l'Amministrazione attraverso una maggiore efficacia ed efficienza nella gestione della domanda alla distribuzione di processi e delle soluzioni applicative. Consente, inoltre, lo sviluppo dei sistemi IT per renderli in grado di soddisfare le aspettative e le tecnologie in evoluzione. La razionalizzazione e il ridisegno del Modello Operativo IT, inoltre, consentirà al Ministero di ottimizzare gli inutilizzi anche attraverso una più corretta preparazione del budget e allocazione dei costi tra le diverse Divisioni, compresa la pianificazione degli acquisti e dei rinnovi contrattuali. Potrà inoltre essere garantita la verifica di compliance ed una più frequente distribuzione dei software con rilasci continui degli aggiornamenti per migliorare la qualità di utilizzo degli applicativi.

7 ROADMAP DEL PIANO ICT

In relazione agli obiettivi strategici e alle linee progettuali definite nel presente piano, al fine di attuare le direttrici evolutive individuate dall'Amministrazione nel triennio di competenza, verrà identificata in dettaglio la roadmap attuativa del piano strategico ICT nel corso dell'anno. Tale roadmap infatti dipende da alcune iniziative in corso rivolte a delineare un quadro di dettaglio delle attività rivolte alla trasformazione digitale del MIMIT. Quanto riportato nella sezione 9 INIZIATIVE IN CORSO permette comunque di individuare una roadmap attuativa nel breve termine.

8 MODELLO DI GOVERNANCE

La corretta attuazione e il monitoraggio dei contenuti presentati all'interno di questo PIANO non possono prescindere dalla definizione di un adeguato **Modello di Governance** che sia volto a definire i ruoli e le responsabilità degli *stakeholder* a vario titolo coinvolti nei processi oltre che gli ambiti di intervento sui quali agire.

A tal fine, può essere delineato un modello iniziale strutturato su tre macro-livelli. Il primo designato alla definizione della strategia di alto livello per la realizzazione del PIANO, ed i successivi due responsabili della definizione, implementazione e monitoraggio degli obiettivi strategici declinati in iniziative progettuali.

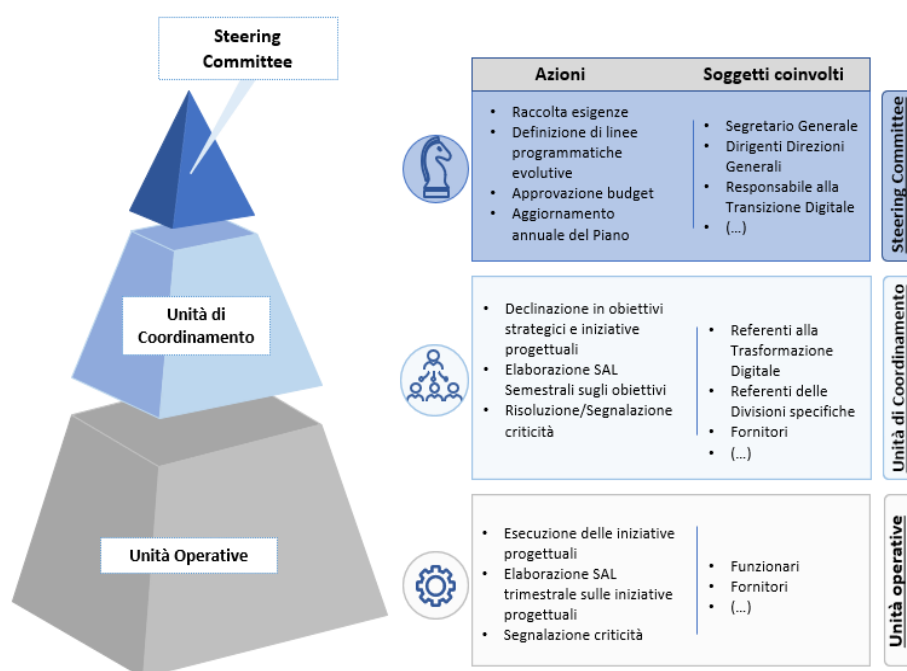


Figura 5: modello iniziale di Governance del PIANO

Nello specifico, la *Steering Committee*, appositamente nominata, avrà la funzione di raccolta delle esigenze provenienti dalle Direzioni Generali definendo successivamente la strategia **high level** per l'attuazione del piano declinando le Linee Programmatiche.

In funzione di questo primo livello di responsabilità, la definizione, l'implementazione e il monitoraggio degli obiettivi strategici e la declinazione degli stessi in specifiche iniziative progettuali saranno affidati alle Unità di Coordinamento.

Successivamente, le Unità Operative composte da funzionari e tecnici, metteranno in atto il piano nelle sue declinazioni pratiche mediante l'attuazione delle iniziative progettuali definite in precedenza dall'Unità di Coordinamento.

Infine, il processo di monitoraggio verrà attuato mediante un approccio che prevede la segnalazione di eventuali criticità da parte delle Unità Operative, la risoluzione delle quali è affidata alle Unità di Coordinamento. Nell'ipotesi in cui non si riuscisse a individuare una soluzione, tali criticità verranno segnalate alla *Steering Committee*, che avrà il ruolo di allineare le Linee Programmatiche alle esigenze specifiche dell'Amministrazione.

Si profila dunque non solo un approccio **Top-Down** volto a declinare la strategia in attività operative, ma anche **Bottom-Up** della *Governance*, grazie ad un continuo processo di segnalazione e riallineamento volto all'ottimizzazione dei processi.

In conclusione, si specifica che tale modello definito ad alto livello verrà successivamente declinato in funzioni, responsabilità e iniziative progettuali specifiche.

9 INIZIATIVE IN CORSO

Il seguente capitolo riporta in modo sintetico le principali iniziative in corso previste nell'attuale pianificazione biennale di beni e servizi in ambito ICT identificate dalle varie Direzioni Generali del MIMIT e collegati agli obiettivi strategici e linee programmatiche sopra descritte, con la stima di massima del fabbisogno finanziario. In tale fase di stesura del presente Piano la descrizione delle iniziative ed il relativo budget previsto risulta essere trasversale alle varie linee programmatiche, in successive revisioni verranno associate previsioni di costo con visione di dettaglio sulle singole linee programmatiche.

Iniziativa programmata	Periodo	Importo programmato
Servizi per Digital Transformation rivolti a definizione strategia della trasformazione digitale ed alla digitalizzazione dei processi in ottica riduzione del rischio cyber	2023-2025	15.100.000
Servizi per attuazione piano Triennale ICT	2023-2025	8.600.000
Servizi e forniture per sicurezza perimetrale e gestione dei processi IT	2023-2025	4.300.000
Servizi professionali per SOC e reingegnerizzazione servizi in ottica cloud	2023-2025	5.000.000
Potenziamento infrastrutture per servizi in ambito cloud	2023-2025	2.600.000
Realizzazione infrastrutture iperconvergente per microservi e potenziamento infrastruttura di rete DGIAI	2023	990.000
Potenziamento protezione infrastruttura UIBM	2023	130.000
Piattaforma software a sostegno dei servizi dell'Ufficio Italiano Brevetti e Marchi	2023-2025	11.000.000

10 APPENDICE A – Normativa e linee guida di riferimento

10.1 Normativa di riferimento sui Servizi

Riferimenti normativi italiani

- [1] Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (in breve CAD), art. 7, 17, 23, 53, 54, 68, 69 e 71
- [2] 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
- [3] Decreto Legislativo 10 agosto 2018, n. 106 - Attuazione della direttiva (UE) 2016/2102 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici
- [4] Decreto-legge 18 ottobre 2012, n. 179 - Ulteriori misure urgenti per la crescita del Paese, art. 9, comma 7
- [5] Linee Guida AgID per il design dei servizi digitali della Pubblica Amministrazione (in fase di consultazione)
- [6] Linee Guida AgID sull'accessibilità degli strumenti informatici
- [7] Linee Guida AgID sull'acquisizione e il riuso del software per la Pubblica Amministrazione
- [8] Circolare AgID n.2/2018, Criteri per la qualificazione dei Cloud Service Provider per la PA
- [9] Circolare AgID n.3/2018, Criteri per la qualificazione di servizi SaaS per il Cloud della PA
- [10] Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici
- [11] Piano Nazionale di Ripresa e Resilienza:
 - Sub-Investimento 1.3.2: *“Single Digital Gateway”*
 - Sub-Investimento 1.4.1: *“Citizen experience - Miglioramento della qualità e dell'usabilità dei servizi pubblici digitali”*
 - Sub-Investimento 1.4.2: *“Citizen inclusion - Miglioramento dell'accessibilità dei servizi pubblici digitali”*

Riferimenti normativi europei:

- [12] 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)
- [13] 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

Progetti di riferimento finanziati:

- [14] Programma operativo Nazionale “Governance e Capacità istituzionale” 2014-2020 Italia Login - La casa del cittadino
- [15] European Union’s Horizon 2020: Wadcher (Web Accessibility Directive Decision Support Environment)

10.2 Normativa di riferimento sui Dati

Riferimenti normativi italiani:

- [16] Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali
- [17] Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (in breve CAD) artt. 50, 50-ter., 51, 52, 59, 60
- [18] Decreto legislativo 24 gennaio 2006, n.36 - Attuazione della direttiva 2003/98/CE relativa al riutilizzo di documenti nel settore pubblico
- [19] 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)
- [20] 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)
- [21] Decreto legislativo 18 maggio 2015, n.102 - Attuazione della direttiva 2013/37/UE relativa al riutilizzo di documenti nel settore pubblico
- [22] Decreto-legge 16 luglio 2020, n. 76 come convertito dalla Legge 11 settembre 2020, n. 120;
- [23] 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
- [24] 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
- [25] Linee guida per la definizione e l'aggiornamento del contenuto del Repertorio Nazionale dei Dati Territoriali (in corso di adozione)
- [26] Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico
- [27] Linee guida per i cataloghi dati
- [28] Linee guida per l'implementazione della specifica GeoDCAT-AP
- [29] Manuale RNDT - Guide operative per la compilazione dei metadati RNDT
- [30] Piano Nazionale di Ripresa e Resilienza - Investimento 1.3: "Dati e interoperabilità"
- [31] Legge Regionale n.14 del 13 settembre 2013 – Disposizioni in materia di trasparenza amministrativa e di valorizzazione dei dati di titolarità regionale

Riferimenti normativi europei:

- [32] Regolamento (CE) 2008/1205 del 3 dicembre 2008 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda i metadati
- [33] 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
- [34] Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (in breve GDPR)
- [35] Direttiva (UE) 2019/1024 del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico

- [36] 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
- [37] 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

10.3 Normativa di riferimento sulle Piattaforme

Generali:

- [38] Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (CAD), artt.5, 6- quater, 50-ter, 62, 62-ter, 64, 64bis, 66Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali
- [39] Regolamento europeo in materia di protezione dei dati personali n. 679/2016 General Data Protection Regulation (GDPR)
- [40] Piano Nazionale di Ripresa e Resilienza:
 - Sub-Investimento 1.3.1: "Piattaforma nazionale digitale dei dati"
 - Sub-Investimento 1.4.3: "Servizi digitali e cittadinanza digitale - piattaforme e applicativi"
 - Sub-Investimento 1.4.4: "Estensione dell'utilizzo delle piattaforme nazionali di Identità Digitale (SPID, CIE) e dell'anagrafe nazionale digitale (ANPR)"
 - Sub-Investimento 1.4.5: "Piattaforma Notifiche Digitali"

Riferimenti normativi europei:

- [41] 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)
- [42] Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR)
- [43] WP 29 "Linee Guida in materia di Data Protection Impact Assessment"

NoiPA:

- [44] Legge 27 dicembre 2006, n. 296 - Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2007) art. 1, commi 446 e 447
- [45] Legge 23 dicembre 2009, n. 191 - Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2010) art. 2, comma 197
- [46] Legge 19 giugno 2019, n. 56 - Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo
- [47] Decreto-legge 06 luglio 2011, n. 98 - Disposizioni urgenti per la stabilizzazione finanziaria, art. 11, comma 9, convertito con modificazioni dalla legge 15 luglio 2011, n. 111, e s.m.
- [48] Decreto Ministeriale del Ministro dell'Economia e delle Finanze del 31 ottobre 2002 - Modifiche delle norme sull'articolazione organizzativa del Dipartimento per le politiche di sviluppo e di coesione del Ministero dell'Economia e delle Finanze

- [49] Decreto Ministeriale del Ministro dell'Economia e delle Finanze del 6 luglio 2012 - Contenuti e modalità di attivazione dei servizi in materia stipendiale erogati dal Ministero dell'Economia e delle Finanze

Progetti di riferimento finanziati:

- [50] Programma di trasformazione digitale Cloudify NoiPA finalizzato all'evoluzione del sistema NoiPA e realizzato attraverso il cofinanziamento dell'Unione Europea
- [51] Programma Operativo Nazionale Governance e Capacità Istituzionale 2014 - 2020 FSE/FESR, gestito dal Dipartimento della Funzione Pubblica

SPID:

- [52] Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014 in materia 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
- [53] Regolamento AgID recante le regole tecniche dello SPID
- [54] Regolamento AgID recante le modalità attuative dello SPID
- [55] Schema di convenzione per l'ingresso delle PA nello SPID

CIE:

- [56] Legge 15 maggio 1997, n. 127- Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e di controllo 26
- [57] Decreto-legge 31 gennaio 2005, n. 7 - Disposizioni urgenti per l'università e la ricerca, per i beni e le attività culturali, per il completamento di grandi opere strategiche, per la mobilità dei pubblici dipendenti, (e per semplificare gli adempimenti relativi a imposte di bollo e tasse di concessione, nonché altre misure urgenti)
- [58] Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
- [59] Decreto Ministeriale del Ministro dell'Interno 23 dicembre 2015 - Modalità tecniche di emissione della Carta d'identità elettronica
- [60] 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:

- [61] Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (CAD), art. 5
- [62] Art. 15, comma 5 bis, del decreto-legge 18 ottobre 2012, n. 179 - Ulteriori misure urgenti per la crescita del Paese
- [63] Art. 65, comma 2, del Decreto legislativo 13 dicembre 2017, n. 217 - Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche

- [64] Decreto Legislativo 14 dicembre 2018, n. 135 Art. 8, comma 2 e 3, Piattaforme Digitali - Disposizioni urgenti in materia di sostegno e semplificazione
- [65] Art. 24 comma 2, lettera a) del Decreto Semplificazioni n. 76 del 16 luglio 2020 (convertito, con modificazioni, dalla Legge n. 120 dell'11 settembre 2020)
- [66] Linee Guida per l'Effettuazione dei Pagamenti Elettronici a favore delle Pubbliche Amministrazioni e dei Gestori di Pubblici Servizi (G.U. n. 153 del 03/07/2018)
- [67] Art. 24 comma 2, lettera a) del Decreto Semplificazioni n. 76 del 16 luglio 2020 (convertito, con modificazioni, dalla Legge n. 120 dell'11 settembre 2020)
- [68] Linee Guida per l'Effettuazione dei Pagamenti Elettronici a favore delle Pubbliche Amministrazioni e dei Gestori di Pubblici Servizi (G.U. n. 153 del 03/07/2018)

PDND (Piattaforma Digitale Nazionale Dati):

- [69] Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (CAD), art. 50-ter
- [70] Decreto Legislativo 14 dicembre 2018, n. 135 Art. 8, commi 2 e 3, Piattaforme Digitali - Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione - Convertito con modificazioni dalla legge n. 12 dell'11 febbraio 2019
- [71] Art. 34 del Decreto Semplificazioni n. 76 del 16 luglio 2020 (convertito, con modificazioni, dalla Legge n. 120 dell'11 settembre 2020)
- [72] Art. 39 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

IO, l'app dei servizi pubblici:

- [73] Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (CAD), art. 64-bis
- [74] Decreto legislativo 14 dicembre 2018, n. 135 Art. 8 Piattaforme Digitali - Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione -Convertito con modificazioni dalla legge n.12 dell'11 febbraio 2019
- [75] Art. 24 lettera f) 2 del Decreto Semplificazioni n. 76 del 16 luglio 2020 (convertito, con modificazioni, dalla Legge n. 120 dell'11 settembre 2020)
- [76] Art. 42 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
- [77] Linee guida per accesso telematico ai servizi della Pubblica Amministrazione - In fase di emanazione

Sistema Gestione Deleghe (SDG):

- [78] Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (CAD), art. 64-ter, introdotto dal Decreto-legge 31 maggio 2021, n. 77

Piattaforma Notifiche Digitali:

- [79] Decreto Legislativo 14 dicembre 2018, n. 135 Art. 8, commi 2 e 3, Piattaforme Digitali - Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la

pubblica amministrazione - Convertito con modificazioni dalla legge n. 12 dell'11 febbraio 2019

- [80] Legge di bilancio 160 del 2019 - Art. 1, commi 402 e 403
- [81] Art. 26 del Decreto Semplificazioni n. 76 del 16 luglio 2020 (convertito, con modificazioni, dalla Legge n. 120 dell'11 settembre 2020)
- [82] Art. 38 del 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

10.4 Normativa di riferimento Infrastrutture

Riferimenti normativi italiani:

- [83] Legge 27 dicembre 2019, n. 160 articolo 1 commi 407, 610-611
- [84] Decreto legislativo 7 marzo 2005, n.82 - Codice dell'amministrazione digitale
- [85] 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
- [86] Decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221
- [87] Decreto-legge 21 settembre 2019, n. 105 Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica
- [88] Decreto-legge 17 marzo 2020, n. 18, articolo 75
- [89] 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
- [90] Strategia italiana per la banda ultralarga (http://presidenza.governo.it/GovernoInforma/Documenti/piano_banda_ultra_larga.pdf)

Riferimenti europei:

- [91] Programma europeo CEF Telecom (<https://ec.europa.eu/inea/en/connecting-europe-facility>)
- [92] Strategia europea sui dati, Commissione Europea 19.2.2020 COM (2020) 66 finale
- [93] European Commission Cloud Strategy, Cloud as an enabler for the European Commission Digital Strategy, 16 May 2019

10.5 Normativa di riferimento Interoperabilità

Riferimenti normativi italiani:

- [94] Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (in breve CAD), artt. 12, 15, 50, 50-ter, 73, 75
- [95] Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali
- [96] Determina AgID 219/2017 - Approvazione e pubblicazione delle "Linee guida per transitare al nuovo modello di interoperabilità"

- [97] Determina AgID 406/2020 - Adozione della Circolare recante le linee di indirizzo sulla interoperabilità tecnica
- [98] Piano Nazionale di Ripresa e Resilienza – Investimento 1.3: “Dati e interoperabilità

Riferimenti normativi europei:

- [99] Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (in breve GDPR)
- [100] 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)
- [101] European Interoperability Framework – Implementation Strategy
- [102] Interoperability solutions for public administrations, businesses, and citizens.

10.6 Normativa di riferimento sulla Sicurezza Informatica

Riferimenti normativi nazionali:

- [103] Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (in breve CAD), art.51
- [104] DPCM del 17 febbraio 2017 - Aggiornamento dell'architettura nazionale di sicurezza cibernetica già delineata dal DPCM del 24 gennaio 2013
- [105] 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
- [106] Decreto-legge 21 settembre 2019, n. 105 - Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica
- [107] Decreto del Presidente del Consiglio dei ministri 8 agosto 2019 - Disposizioni sull'organizzazione e il funzionamento del computer security incident response team - CSIRT italiano
- [108] Piano Nazionale per la Protezione Cibernetica 2017
- [109] Decreto-legge 16 luglio 2020, n. 76 - Misure urgenti per la semplificazione e l'innovazione digitale
- [110] Decreto-legge 14 giugno 2021, n. 82 - Definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale
- [111] Decreto-legge 21 marzo 2022, n. 21 - Ridefinizione dei poteri speciali in materia di servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G
- [112] Decreto legislativo 8 novembre 2021, n. 207 (Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018) - Istituzione del Codice europeo delle comunicazioni elettroniche
- [113] Strategia Cloud Italia - Diffusione di soluzioni basate sul Cloud computing nel circuito delle Pubbliche Amministrazioni

Riferimenti normativi europei:

- [114] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 in materia di protezione dei dati personali

- [115] Regolamento (UE) 2014/910 del Parlamento europeo e del Consiglio – Regolamento eIDAS;
- [116] Nuova strategia Cybersicurezza europea

11 APPENDICE 1 – Elenco acronimi

Acronimo	Definizione
AgID	Agenzia per l'Italia Digitale
ANPR	Anagrafe Nazionale della Popolazione Residente
API	Application Programming Interface
CAD	Codice dell'Amministrazione Digitale
CED	Centro Elaborazione Dati
CEF	Connecting Europe Facility
CERT-PA	Computer Emergency Response Team Pubblica Amministrazione
CI/CD	Continuous Improvement/Continuous Development
CIE	Carta d'Identità Elettronica
CSIRT	Computer Security Response Team
CSO	Chief Security Officer
DGAECE	Direzione Generale per l'Approvvigionamento, l'Efficienza e la Competitività Energetica
DGIAI	Direzione Generale per gli Incentivi alle Imprese
DGISSEG	Direzione Generale per le Infrastrutture e la Sicurezza dei Sistemi Energetici e Geominerari
d.lgs.	Decreto Legislativo
DGMCTCNT	Direzione Generale per il Mercato, la Concorrenza, la Tutela del Consumatore e la Normativa Tecnica
DGPIIPM	Direzione Generale per la Politica Industriale, l'Innovazione e le PMI
DGRIGFP	Direzione Generale per la Riconversione Industriale e Grandi Filiere Produttive
DGROSIB	Direzione Generale per le Risorse, l'Organizzazione, i Sistemi Informativi e il Bilancio
DGSCERP	Direzione Generale per i Servizi di Comunicazione Elettronica, di Radiodiffusione e Postali
DGTCSI-ISCTI	Direzione Generale per le Tecnologie delle Comunicazioni e la Sicurezza Informatica - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione
DGTPI-UIBM	Direzione Generale per la Tutela della Proprietà Industriale - Ufficio Italiano Brevetti e Marchi
DGVECS	Direzione Generale per la Vigilanza sugli Enti Cooperativi e sulle Società
DPCM	Decreto del Presidente del Consiglio dei Ministri
DTD	Dipartimento per la Trasformazione Digitale
eIDAS	Electronic Identification Authentication and Signature
FESR	Fondo Europeo di Sviluppo Regionale
FSE	Fascicolo Sanitario Elettronico

Acronimo	Definizione
FSE	Fondo Sociale Europeo
GDPR	Regolamento Generale sulla Protezione dei Dati
GeoDCAT - AP	Data Catalog Vocabulary Application Profile
ICT	Information and Communication Technology
INAD	Indice Nazionale dei Domicili Digitali
INSPIRE	Infrastruttura per l'Informazione Territoriale nella Comunità Europea
IO	Input/Output
IT	Information Technology
MIMIT	Ministero delle Imprese e del Made in Italy
PA	Pubblica Amministrazione
PDND	Piattaforma Digitale Nazionale Dati
PEC	Posta Elettronica Certificata
PND	Piattaforma Notifiche Digitali
PNRR	Piano Nazionale Ripresa e Resilienza
PPAA	Politica e Pubblica Amministrazione Associazione
PSN	Piano Strategico Nazionale
RNDT	Repertorio Nazionale dei Dati Territoriali
SaaS	Software as a Service
SDG	Sistema di Gestione Digitale
SIOPE	Sistema Informativo sulle Operazioni degli Enti Pubblici
SOC LDO	Security Operation Center Leonardo
SOC	Security Operation Center
SPC	Sistema Pubblico di Connettività
SPID	Sistema Pubblico di Identità Digitale
ULS	Unità Locale di Sicurezza