Istituto Zooprofilattico Sperimentale
del Lazio e della Toscana - M. Aleandri

Piano Triennale per la transizione digitale 2026 - 2028 dell'IZSLT

Riferimento al Piano Triennale per l'Informatica 2025 - 2027 pubblicato da AGID

Data di pubblicazione

Istituto Zooprofilattico Sperimentale del Lazio e della Toscana "M. Aleandri"
Via Appia Nuova, 1411 – 00178 Roma
Telefono: 0679099400
Pec: izslt@legalmail.it

Sommario

Introduzione

Il *Piano Triennale per la Transizione Digitale 2026-2028* (di seguito "Piano Triennale" o semplicemente "Piano") costituisce un documento strategico di riferimento per le Pubbliche Amministrazioni (PA) italiane, orientando il percorso di digitalizzazione e innovazione tecnologica in tutti i settori, inclusi sanità, sicurezza e ricerca scientifica.

Per l'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana (di seguito "IZSLT" o "Istituto"), il Piano non rappresenta soltanto un obbligo normativo, ma un'opportunità per incrementare l'efficienza, la qualità dei servizi e la collaborazione interistituzionale attraverso l'adozione di soluzioni tecnologiche avanzate.

L'obiettivo principale del Piano Triennale per l'IZSLT è favorire una transizione digitale che renda l'Istituto più efficiente, innovativo e competitivo. La digitalizzazione dei processi, dei flussi informativi e della gestione dei dati è essenziale per affrontare le sfide attuali legate alla salute animale e pubblica, alla tracciabilità degli alimenti e al controllo dei focolai epidemici.

In particolare, gli obiettivi specifici per l'IZSLT sono:

- **Incremento dell'efficienza operativa**, attraverso l'automazione dei processi, la gestione digitale dei dati e l'integrazione dei diversi sistemi informatici in uso.
- **Gestione evoluta dei dati sanitari**, mediante piattaforme interoperabili che favoriscano la comunicazione e la collaborazione con altri enti sanitari, amministrazioni pubbliche e partner scientifici.
- **Innovazione nella ricerca e nella diagnostica**, grazie all'impiego di tecnologie emergenti quali intelligenza artificiale, big data e Internet of Things (IoT) applicati alla sanità pubblica veterinaria.
- **Tutela e sicurezza dei dati**, garantendo la conformità alle normative sulla protezione dei dati e la difesa da minacce informatiche.

Quadro Normativo e Aggiornamenti del Piano Triennale per la Transizione Digitale 2026-2028

1. Quadro Normativo di Riferimento

Il **Piano Triennale per la Transizione Digitale 2026-2028** si fonda su un insieme di norme europee e nazionali che ne definiscono obiettivi e priorità strategiche. Le principali fonti sono:

- **Decisione (UE) 2022/2481 – Digital Decade 2030**
  - Obiettivi articolati in quattro dimensioni:
    - Competenze digitali
    - Servizi pubblici digitali
    - Digitalizzazione delle imprese
    - Infrastrutture sicure e sostenibili
  - Introduzione di un modello di governance con monitoraggio annuale e obiettivi misurabili.
- **Regolamento (UE) 2018/1724 – Single Digital Gateway**
  - Garantisce un accesso semplice e uniforme ai servizi pubblici digitali in tutta l'Unione Europea.
  - Favorisce interoperabilità e semplificazione delle procedure amministrative.
- **Linee guida AGID**
  - Definiscono standard tecnici per:
    - Interoperabilità
    - Sicurezza informatica
    - Accessibilità
    - Gestione documentale
    - Open data

2. Aggiornamenti 2025

- Introduzione di **16 nuovi strumenti operativi**, tra cui:
  - **ITWallet** per l'identità digitale evoluta
  - **Data Quality** per la governance dei dati
  - Soluzioni per la **dematerializzazione documentale** e l'integrazione dell'ecosistema dei dati sanitari
- Rafforzamento della **governance digitale** con tavoli di concertazione permanenti e strumenti di supporto (modelli, checklist, buone pratiche).
- A livello europeo, il **rapporto "State of the Digital Decade 2025"** evidenzia progressi su:
  - Infrastrutture (5G, edge computing, cloud)
  - Intelligenza artificiale
  - Servizi digitali

    Ma sottolinea la necessità di accelerare su competenze digitali e digitalizzazione dei servizi pubblici.

---

3. Aggiornamenti 2026

- **Ampliamento della cassetta degli attrezzi** a **22 strumenti operativi**, con modelli e best practice per la gestione documentale e l'adozione di tecnologie emergenti.
- **Introduzione di progetti dedicati all'Intelligenza Artificiale** e consolidamento dell'ITWallet come strumento chiave per l'identità digitale.
- **Istituzione dell'AgID Academy** per la formazione e il potenziamento delle competenze digitali del personale pubblico.
- Avvio della programmazione **2027-2029**, con focus su ecosistemi digitali sicuri, interoperabili e inclusivi, in linea con il PNRR e le priorità europee.

---

4. Implicazioni per l'IZSLT

- Maggiore interoperabilità dei sistemi informativi sanitari.
- Adozione di strumenti per la gestione avanzata dei dati e la sicurezza informatica.
- Opportunità di innovazione nella ricerca e diagnostica tramite IA e big data.
- Rafforzamento delle competenze digitali del personale attraverso percorsi formativi dedicati.

Il Ruolo Strategico della Transizione Digitale in IZSLT

Visione Strategica

La transizione digitale presso l'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana (IZSLT) non costituisce soltanto un aggiornamento tecnologico, ma un profondo cambiamento organizzativo e culturale. La digitalizzazione va intesa come un percorso che coinvolge persone, processi e strumenti, promuovendo un approccio partecipativo, inclusivo e continuo.

Governance e Ruolo del Responsabile alla Transizione Digitale (RTD)

Il Responsabile per la Transizione Digitale (RTD) è la figura centrale per il coordinamento delle iniziative tecnologiche, la promozione di innovazione e la gestione del cambiamento organizzativo. In base alle Linee Guida AGID, il RTD assume il compito di costituire e guidare un Ufficio per la Transizione Digitale (UTD), valorizzando forme di collaborazione anche interistituzionale.

Il Piano Triennale 2026-2028 definisce una governance digitale integrata, in cui le politiche ICT sono strettamente allineate con le esigenze scientifiche e operative dell'Istituto. Il coinvolgimento attivo del personale nella formazione digitale è una priorità strutturale.

Obiettivi Operativi

Efficienza e Automazione

- Ottimizzazione dei processi interni: adozione di workflow digitali per informatizzare la diagnostica di laboratorio, la gestione delle risorse e dei dati.
- Automazione della gestione dei dati sanitari: implementazione di software e piattaforme per raccolta, archiviazione e analisi in tempo reale, garantendo elevata accuratezza, velocità e sicurezza nelle informazioni relative a salute animale e sicurezza alimentare.

Semplificazione Amministrativa

- Dematerializzazione documentale: digitalizzazione della gestione dei documenti amministrativi, pianificazione delle risorse e accesso alle informazioni sia internamente che verso cittadini e istituzioni.
- Adozione di soluzioni user-centriche basate su modelli e checklist introdotti dall'AGID.

Interoperabilità e Integrazione

Implementazione di soluzioni interoperabili, che assicurino il flusso sicuro di dati tra dipartimenti interni, ASL, Ministero della Salute e autorità sanitarie locali, in linea con le raccomandazioni AGID.

Innovazione nella Ricerca e Diagnostica

Intelligenza Artificiale e Machine Learning

Applicazione di sistemi di IA per diagnosi predittiva, analisi automatizzata e identificazione di pattern, riducendo tempi di risposta e migliorando la precisione dei test diagnostici.

Big Data e Analytics

Gestione di elevate mole di dati da laboratori e sistemi di monitoraggio epidemiologico per supportare modelli predittivi nella gestione delle malattie zoonotiche e ottimizzare le campagne di sorveglianza sanitaria.

IoT (Internet of Things)

Utilizzo di sensori IoT in allevamenti, laboratori e ambienti di lavoro per il monitoraggio in tempo reale della salute animale, della qualità alimentare e delle condizioni operative.

Strumenti e Competenze 2026

- AGID ha ampliato al 2026 la cassetta degli attrezzi delle PA a 22 strumenti operativi, includendo modelli, best practice checklist per la gestione documentale, IT-Wallet e IA.
- È stata istituita l'AgID Academy, con l'obiettivo di rafforzare le competenze digitali del personale con corsi strutturati su transizione digitale, gestione dati e IA.

Principi Guida del Piano Triennale 2026-2028 (aggiornati al 2026)

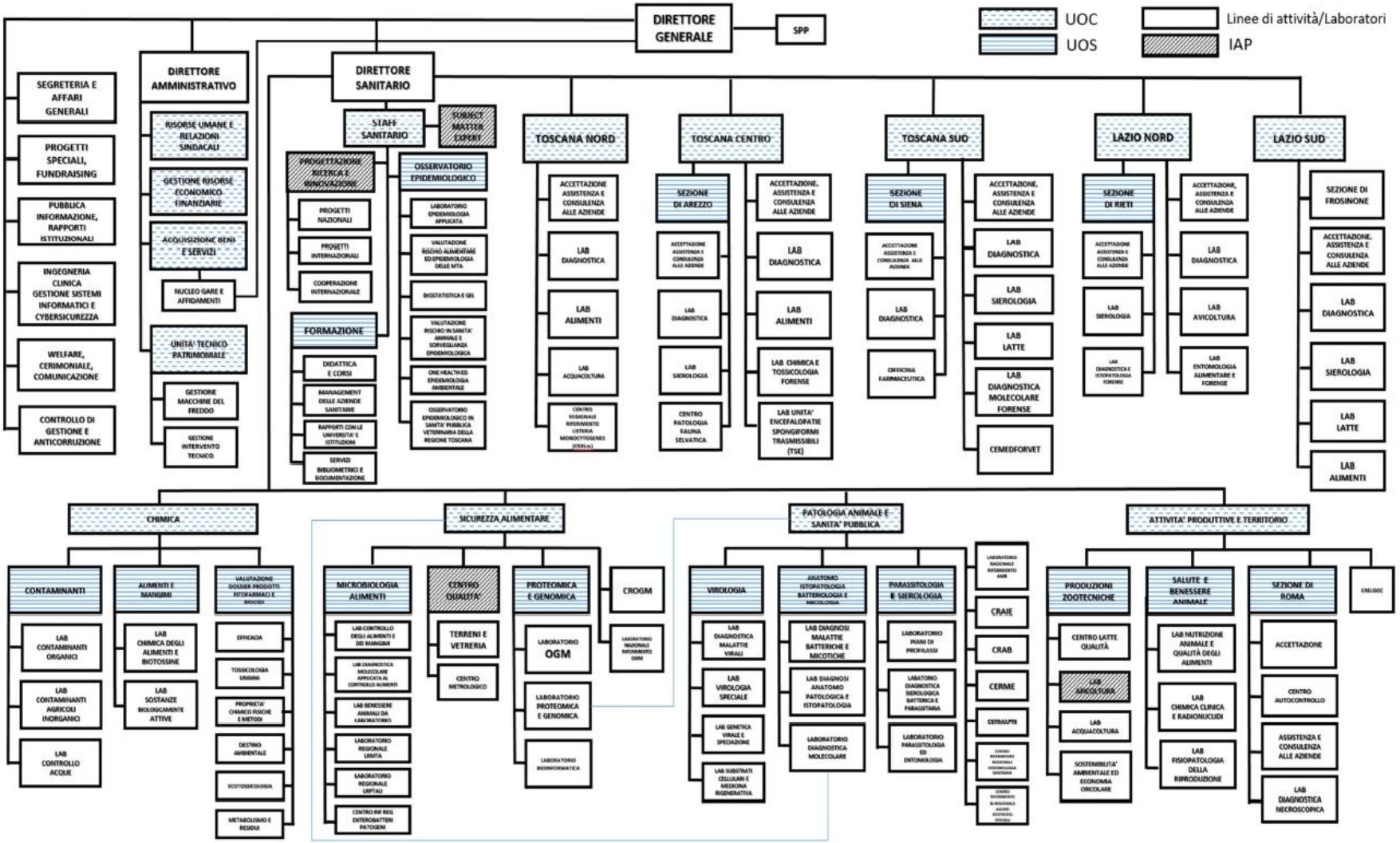
Il Piano Triennale per la Transizione Digitale 2026-2028 si basa su undici principi guida, fondamentali per orientare l'attuazione delle politiche digitali nell'ambito dell'IZSLT e della Pubblica Amministrazione. La tabella seguente sintetizza i principi, le loro definizioni e i riferimenti normativi principali.

Principio Guida	**Definizione**	**Riferimenti Normativi**
Digitale e mobile first	I servizi pubblici devono essere progettati prioritariamente in formato digitale e accessibili da dispositivi mobili. Soluzioni alternative solo se residuali, con semplificazione e reingegnerizzazione dei processi.	Art.3-bis Legge 241/1990; Art.1 c.1 lett. a) D.Lgs.165/2001; Art.15 CAD; Art.1 c.1 lett. b) Legge 124/2015; Art.6 c.1 DL 80/2021
Cloud first	Nuovi progetti e servizi devono adottare il paradigma cloud, utilizzando strutture e servizi qualificati secondo l'AGID e il SPC.	Art.33-septies Legge 179/2012; Art.73 CAD
Interoperabile by design & default (API-first)	I servizi devono essere progettati fin da subito per l'integrazione e il funzionamento collegato, esponendo API prima di definire canali di fruizione.	Art.43 c.2 DPR 445/2000; Art.2 c.1 lett.c) D.Lgs 165/2001; Art.50 c.2; art.50-ter; art.64-bis c.1-bis CAD
Digital identity only	L'accesso ai servizi pubblici deve avvenire esclusivamente tramite identità digitale conforme alle normative vigenti.	Art.64 CAD; Art.24 c.4 DL 76/2020; Regolamento EU 2014/910 eIDAS
User centric	I servizi devono essere inclusivi, centrati sull'esperienza dell'utente, con miglioramento continuo basato su misurazione di prestazioni e utilizzo.	Legge 4/2004 Art.2 c.1, art.7; art.53 CAD; Art.8 c.1 lett.c) e lett.e), art.14 c.4-bis D.Lgs 150/2009
Open data by design & default	I dati pubblici sono un bene comune: devono essere aperti, interamente accessibili e valorizzati per promuovere trasparenza e innovazione.	Art.50 c.1; c.2-bis; art.50-quater; art.52 c.2 CAD; D.Lgs 36/2006; Art.24-quater c.2 DL90/2014
Data protection & security by design & default	I servizi pubblici devono essere progettati per garantire la sicurezza e la protezione dei dati personali fin dall'origine.	Regolamento EU 2016/679 GDPR; DL 65/2018 NIS; DL 105/2019 PNSC; DL 82/2021 ACN
Once-only & transfrontaliero	Le informazioni già fornite non devono essere richieste nuovamente; i servizi devono essere interoperabili anche a livello transfrontaliero.	Art.43, 59, 64, 72 DPR 445/2000; Art.15 c.3; art.41; art.50 c.2; c.2-ter; art.60 CAD; Regolamento EU 2018/1724 Single Digital Gateway; Com.EU (2017) 134 EIF
Openness	Prevenire lock-in tecnologico: favorire software open source, condividere il codice sorgente e le buone pratiche tecnologiche e amministrative.	Art.9; art.17 c.1; art.68-69 CAD; Art.1 c.1 D.Lgs 33/2013; Art.30 D.Lgs 36/2023
Sostenibilità digitale	I servizi devono essere sostenibili dal punto di vista economico, ambientale, sociale e territoriale per tutto il loro ciclo di vita.	Art.15 c.2-bis CAD; Art.21 D.Lgs 36/2023; Regolamento EU 2020/852 principio DNSH

Sussidiarietà, proporzionalità, appropriatezza	Le iniziative digitali devono essere intraprese secondo criteri di efficacia rispetto alla competenza territoriale ottimale, evitando duplicazioni e assicurando coordinamento.	Art.5, 117, 118 Costituzione; Art.14 CAD

Contesto Organizzativo

Di seguito la rappresentazione grafica della struttura organizzativa dell'IZSLT:



Indice dei domicili digitali (IPA) www.indicepa.gov.it

L'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi [art. 6-ter del CAD], di seguito indicato con l'acronimo IPA, è l'elenco pubblico di fiducia contenente i domicili digitali da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti validi a tutti gli effetti di legge tra le pubbliche amministrazioni, i gestori di pubblici servizi e i privati. Il Decreto del Ministero dell'Economia e delle Finanze n. 55/2013, individua l'IPA come anagrafe di riferimento per la fatturazione elettronica delle amministrazioni pubbliche.

Aree Organizzative Omogenee

Le informazioni indicate nella tabella sottostante riportano le Aree Organizzative Omogenee (AOO) dell'IZSLT, presenti in IPA. Esse identificano gli uffici di protocollo che gestiscono tutte le comunicazioni che l'ente riceve (documenti in entrata) e quelle che invia ad altri enti, cittadini ed imprese (documenti in uscita). Sono costituite dall'insieme di funzioni e di strutture che operano su tematiche omogenee e che hanno esigenze di gestione della documentazione unitarie e coordinate.

Codice_IPA	Denominazione_ente	Codice_fiscale_ente	Codice_uni_aoo	Denominazione_aoo	Data istituzione	Nome responsabile	Cognome responsabile
izsrl_	Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri	00422420588	AE2TXP7	Direzione Strategica	2026-21-01	Stefano	Palomba

Ruolo del Responsabile per la Transizione al Digitale

Ai fini dell'attuazione del Piano Triennale, l'IZSLT si avvale delle seguenti componenti organizzative:

- **Responsabile per la Transizione Digitale**;
- **Ufficio per la Transizione Digitale**.

Il **Responsabile per la Transizione Digitale** (di seguito RTD) ha un ruolo cruciale nel coordinare e guidare la trasformazione digitale. Questa figura dirigenziale è incaricata di garantire l'implementazione delle strategie digitali e di promuovere l'adozione di tecnologie innovative all'interno dell'organizzazione.

Il RDT svolge principalmente attività di:

- **Coordinamento**: coordina le attività di digitalizzazione tra le diverse strutture dell'IZSLT, assicurando che tutte le iniziative siano allineate con il Piano Triennale per la Transizione Digitale.
- **Collaborazione**: stabilisce e mantiene rapporti di collaborazione con altre figure dirigenziali, come il Responsabile della gestione documentale, il Responsabile della protezione dei dati personali e il Responsabile della prevenzione della corruzione e della trasparenza.
- **Formazione e Supporto**: promuove la formazione continua del personale sulle nuove tecnologie e supporta le diverse unità nell'adozione di strumenti digitali.
- **Monitoraggio e Valutazione**: supervisiona l'implementazione delle soluzioni digitali e valuta l'efficacia delle iniziative intraprese, apportando eventuali miglioramenti.

Il RTD collabora strettamente con tutte le strutture dell'IZSLT per garantire una transizione digitale armoniosa e integrata: interagisce con i Sistemi Informativi per assicurare l'interoperabilità e la sicurezza delle infrastrutture digitali; coinvolge le diverse Unità Operative nella progettazione e implementazione dei servizi digitali, assicurando che le soluzioni adottate rispondano alle esigenze specifiche di ciascuna area; mantiene una comunicazione aperta e trasparente con tutte le parti interessate, inclusi i cittadini e le imprese, per garantire che i servizi digitali siano accessibili e utilizzabili da tutti.

Responsabile per la Transizione al Digitale (RTD), il Dr. Stefano Palomba, Commissario Straordinario dell'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri, conferendo contestualmente alla Sig.ra Iole Faita, dipendente dell'Ente con la qualifica di Assistente Tecnico – programmatore, l'incarico di referente del RDT (iole.faita@izslt.it) Delibera 278/25

Per lo svolgimento delle sue mansioni, il RDT è supportato dall'**Ufficio per la Transizione Digitale** (UDT) le cui funzioni principali sono:

Coordinamento Strategico:

- coordina lo sviluppo dei sistemi informativi e delle telecomunicazioni, garantendo l'efficienza e l'economicità dei servizi digitali;
- supervisiona l'implementazione delle strategie digitali e assicura la conformità alle normative vigenti.

Sicurezza Informatica:

- pianifica e monitora la sicurezza dei dati, dei sistemi e delle infrastrutture digitali;
- implementa misure di sicurezza per proteggere i dati e le infrastrutture digitali dell'istituto.

Accessibilità:

- promuove l'accesso agli strumenti informatici per tutti gli utenti, inclusi i soggetti disabili;
- garantisce che i servizi digitali siano interoperabili e accessibili a tutti gli utenti.

Analisi e Miglioramento:

- valuta periodicamente la coerenza tra l'organizzazione dell'amministrazione e l'uso delle tecnologie digitali per migliorare la qualità dei servizi;
- monitora i progressi dei progetti di digitalizzazione e apporta eventuali correzioni per garantire il raggiungimento degli obiettivi.

Responsabile per la transizione digitale indicato sul portale indicepa.gov.it (IPA)

Denominazione	Codice Fiscale	Nome Categoria	Codice uni_uo	Descrizione_uo	Nome responsabile	Cognome responsabile	Mail responsabile
Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri	00422420588	Istituti Zooprofilattici Sperimentali	KXGHZG	Ufficio per la transizione al Digitale	Stefano	Palomba	izslt@legalmail.it

Obiettivi generali dell'Amministrazione

L'IZSLT (Istituto Zooprofilattico Sperimentale del Lazio e della Toscana) ha avviato un percorso strutturato di modernizzazione e rafforzamento della propria infrastruttura informatica, in linea con le direttive nazionali in materia di cybersicurezza e con gli standard richiesti dalla normativa vigente per la Pubblica Amministrazione. L'Istituto gestisce un'infrastruttura complessa che serve postazioni di lavoro distribuite su più sedi territoriali tra Lazio e Toscana, garantendo servizi per la sanità veterinaria e la ricerca scientifica.

Negli ultimi anni sono stati completati importanti interventi infrastrutturali, tra cui la migrazione completa a nuovi apparati di rete, la progettazione di un'architettura di rete segmentata in VLAN, l'implementazione di doppia connettività WAN ridondante (business e GARR), e l'adozione di soluzioni open source per l'infrastruttura server e di virtualizzazione. Per il triennio 2026-2028, l'Istituto si pone obiettivi ambiziosi che completano questo percorso di trasformazione digitale: dalla migrazione di tutti i dispositivi nelle nuove VLAN all'implementazione di sistemi IPS/IDS avanzati, dalla connessione di tutte le postazioni al dominio Active Directory alla dismissione dei sistemi obsoleti, dall'implementazione di backup geograficamente distribuiti alla valutazione della migrazione di servizi selezionati verso il Polo Strategico Nazionale.

Questi obiettivi si inseriscono in una visione strategica che privilegia sicurezza, resilienza, conformità normativa e autonomia tecnologica, mantenendo al centro la continuità dei servizi essenziali erogati dall'Istituto e la protezione dei dati sensibili gestiti, nel pieno rispetto delle linee guida AGID e delle direttive dell'Agenzia per la Cybersicurezza Nazionale.

Servizi Digitali per Cittadini e Imprese

L'IZSLT persegue l'obiettivo di ampliare progressivamente l'offerta di servizi digitali accessibili online per cittadini, imprese del territorio e stakeholder del settore veterinario e della ricerca, in coerenza con gli obiettivi di trasformazione digitale della Pubblica Amministrazione e privilegiando, ove possibile, l'adozione di soluzioni SaaS qualificate da AgID.

Obiettivo 2026: Completare il rinnovo integrale del sito web istituzionale dell'IZSLT sviluppandolo in piena conformità con:

- Linee Guida di Design per i servizi web della PA di AgID
- Requisiti di accessibilità per persone con disabilità (D. Lgs. 106/2018)
- Integrazione nativa con SPID per l'autenticazione degli utenti
- Integrazione con PagoPA per i pagamenti digitali verso la PA

Obiettivo 2026: Garantire la piena accessibilità del sito web sostituendo tutti i documenti pubblicati in formati non conformi con versioni accessibili, superando l'attuale stato di "accessibilità parziale" dichiarato ad AgID. Questo intervento riguarderà la conversione di documenti legacy e l'adozione di policy stringenti per le nuove pubblicazioni.

Obiettivo 2026-2028: Applicare il principio once only ("il cittadino deve fornire i suoi dati una sola volta"), collaborando con i fornitori di piattaforme digitali per implementare meccanismi di recupero e precompilazione dei dati già forniti in precedenza dall'utente, riducendo significativamente il carico di lavoro e migliorando l'esperienza d'uso dei servizi digitali.

Servizi e Strumenti per il Personale Interno

L'IZSLT pone particolare attenzione al miglioramento dei servizi digitali rivolti al personale interno, dalle figure apicali ai collaboratori, con l'obiettivo di aumentare l'efficienza operativa, semplificare i procedimenti amministrativi e garantire conformità normativa nella gestione degli asset ICT.

Obiettivo 2026-2028: Completare il quadro regolamentare in materia di ICT attraverso l'adozione formale di:

- Regolamento per la gestione, il funzionamento e l'utilizzo del sito internet istituzionale e dei canali social media
- Individuazione e nomina formale dei ruoli di responsabilità, tra cui:

1. Responsabile del sito web istituzionale e del procedimento di pubblicazione
2. Referenti per l'aggiornamento normativo, tecnologico e migliorativo delle applicazioni gestionali

Obiettivo 2026-2028: Avviare un progetto di reingegnerizzazione di procedimenti amministrativi selezionati, identificando i processi a maggiore impatto in termini di carico di lavoro o criticità operative, per digitalizzarli, semplificarli e automatizzarli dove possibile, riducendo tempi di esecuzione ed errori manuali.

Obiettivo 2026-2028: Avviare un progetto pilota per la conservazione digitale sostitutiva degli archivi cartacei, in conformità alle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici. Il progetto prevederà la digitalizzazione controllata di archivi selezionati, l'implementazione di un sistema di conservazione a norma e la definizione di policy per la gestione del ciclo di vita dei documenti digitali.

Obiettivo 2026-2028: Implementare un piano di formazione continua per migliorare le competenze digitali del personale interno sull'utilizzo degli applicativi gestionali dell'Istituto (sistemi amministrativi, gestionali di laboratorio, strumenti di collaborazione) e degli strumenti di lavoro quotidiani, con particolare focus sulle nuove funzionalità introdotte e sulle best practice operative.

Infrastruttura di Rete e Sicurezza Perimetrale

L'infrastruttura di rete dell'IZSLT è stata completamente rinnovata con la migrazione ad apparati Cisco Meraki, che forniscono gestione centralizzata cloud-based, visibilità completa del traffico e capacità avanzate di threat detection. La rete è stata completamente ridisegnata con una segmentazione a VLAN che separa logicamente i diversi servizi e tipologie di utenti (amministrazione, laboratori, ospiti, IoT medicale, server infrastrutturali), garantendo isolamento del traffico e maggiore controllo degli accessi.

Obiettivi 2026-2028: Completare la migrazione di tutti i circa 550 dispositivi nelle VLAN appropriate secondo la nuova architettura di rete, garantendo che ogni tipologia di dispositivo sia correttamente segmentata e che le policy di comunicazione inter-VLAN siano configurate secondo il principio del minimo privilegio necessario. In parallelo, procedere con la dismissione dei sistemi obsoleti e non più supportati, migrando verso piattaforme aggiornate e supportate dai vendor o dalle comunità open source. Questo include l'aggiornamento o la sostituzione di sistemi operativi server end-of-life, applicativi legacy e middleware non più mantenuti, secondo un piano di priorità basato sull'esposizione al rischio e sulla criticità del servizio erogato. Per quanto riguarda la connettività wireless, verranno implementate reti WiFi distinte e segregate per dipendenti e utenti esterni (ospiti, visitatori), ciascuna con policy di accesso e sicurezza appropriate al profilo utente, garantendo isolamento del traffico e protezione della rete aziendale.

L'Istituto dispone di due connettività WAN ridondanti per garantire continuità dei servizi e bilanciamento del carico:

- Connettività business fornita da operatore di telecomunicazioni
- Connettività fornita da una rete dedicata alla ricerca e istruzione (Consorzio GARR)

La sicurezza perimetrale è garantita da un firewall Cisco MX di proprietà dell'Istituto, che gestisce entrambe le connessioni WAN con policy di failover automatico e load balancing. La configurazione e la gestione del firewall sono eseguite dal personale interno con il supporto di un partner certificato Cisco.

Obiettivo 2026-2028: Implementare policy di sicurezza avanzate sul firewall perimetrale, includendo regole granulari per il controllo applicativo, geo-blocking, e filtering del traffico in uscita. Configurare e attivare completamente i sistemi IPS/IDS (Intrusion Prevention/Detection System) per il monitoraggio proattivo delle minacce, con definizione di soglie di alert e procedure di risposta agli incidenti.

Infrastruttura Server/VM

Per i servizi erogati tramite server interni presenti nel datacenter dell'Istituto, viene privilegiato l'utilizzo di soluzioni open source, sia per l'hypervisor che per i servizi applicativi. Questa scelta strategica permette di:

- Evitare il vendor lock-in e mantenere autonomia tecnologica
- Ridurre i costi di licenza software
- Garantire trasparenza e controllo completo sulle tecnologie utilizzate con possibilità di personalizzazione

L'infrastruttura di virtualizzazione si basa su Proxmox VE con configurazione cluster ad alta affidabilità, mentre i servizi applicativi utilizzano prevalentemente distribuzioni Linux e stack tecnologici open source (web server, database, middleware).

Obiettivi 2026-2028: Implementare un sistema di backup geograficamente distribuito che integri l'attuale soluzione di backup locale con replica automatica presso altre sedi territoriali dell'Istituto e/o in cloud storage qualificato. Questo garantirà disaster recovery efficace anche in caso di eventi catastrofici che coinvolgano il datacenter principale, rispettando i requisiti di business continuity richiesti dalla normativa per la PA.

Migrazione ai Servizi del Polo Strategico Nazionale

In linea con la strategia nazionale di digitalizzazione della Pubblica Amministrazione, l'IZSLT sta pianificando la migrazione di servizi selezionati verso il Polo Strategico Nazionale (PSN), l'infrastruttura cloud certificata per la PA italiana che garantisce i più alti standard di sicurezza, affidabilità e sovranità digitale.

Obiettivi 2026-2028: Avviare il processo di migrazione per i primi servizi pilota non critici. La migrazione progressiva permetterà di beneficiare di:

- Infrastruttura ad alta affidabilità con SLA garantiti
- Conformità nativa alle normative italiane ed europee su privacy e sicurezza
- Competenze specialistiche messe a disposizione dal provider qualificato PSN

I servizi che richiedono controllo diretto, personalizzazione spinta o che gestiscono dati particolarmente sensibili potranno rimanere on-premise, mantenendo un modello di cloud ibrido che ottimizzi sicurezza, costi e flessibilità operativa.

Conformità Normativa e Standard di Sicurezza

L'IZSLT si adegua costantemente alle linee guida emesse da AGID relative alle misure minime di sicurezza ICT, al decreto attuativo della legge sul Perimetro di Sicurezza Nazionale Cibernetica e alle linee guida pubblicate dall'Agenzia per la Cybersicurezza Nazionale (ACN) per lo sviluppo del modello nazionale di cybersicurezza.

Obiettivi 2026-2028: Completare l'implementazione dei controlli di sicurezza richiesti, inclusi:

- Sistemi di monitoraggio e logging centralizzato conformi alle richieste ACN con retention appropriata
- Procedure di incident response e disaster recovery documentate e testate periodicamente
- Controlli di accesso basati sul principio del "least privilege" con revisione trimestrale dei permessi
- Crittografia dei dati sensibili in transito e a riposo, con particolare attenzione ai dati sanitari e di ricerca

Servizi Cloud e Continuità Operativa

Per i servizi SaaS in cloud, l'IZSLT si affida ai sistemi di sicurezza forniti dai provider qualificati, che garantiscono disponibilità del servizio, assistenza specializzata e procedure di ripristino in caso di emergenza. La selezione dei fornitori avviene secondo i criteri di qualificazione previsti dalla normativa per la PA.

Obiettivi 2026-2028: Formalizzare i Service Level Agreement (SLA) con i provider cloud e implementare procedure di monitoraggio della conformità agli standard di sicurezza richiesti, con verifiche periodiche e audit sui fornitori strategici.

Manutenzione e Prevenzione

La manutenzione ordinaria delle policy di sicurezza, della rete logica e degli apparati rappresenta un'attività continua e prioritaria. Una configurazione "ordinata" e costantemente aggiornata permette di:

- Prevenire attacchi dall'esterno attraverso hardening dei sistemi
- Individuare rapidamente eventuali anomalie o intrusioni
- Isolare tempestivamente le minacce per evitarne la propagazione laterale
- Garantire la tracciabilità degli eventi per analisi forensi

Obiettivi 2026-2028: Implementare un processo strutturato di vulnerability management con scansioni periodiche automatizzate, classificazione dei rischi e piano di remediation basato su priorità. Stabilire procedure documentate per il patch management di tutti i sistemi critici con tempistiche definite per l'applicazione degli aggiornamenti di sicurezza.

Formazione e Consapevolezza del Personale

Contrastare le minacce informatiche è fondamentale per garantire disponibilità, integrità e riservatezza delle informazioni del sistema informativo dell'Istituto, aumentando la fiducia nei servizi digitali erogati dalla PA.

Obiettivi 2026-2028: Avviare un programma strutturato e continuativo di Cyber Security Awareness che prevede:

- Formazione obbligatoria annuale per tutto il personale con test di verifica
- Campagne trimestrali di sensibilizzazione su phishing e social engineering
- Simulazioni di attacchi phishing per misurare il livello di preparazione e identificare aree di miglioramento
- Diffusione e aggiornamento di policy e procedure di sicurezza chiare, accessibili e contestualizzate ai diversi ruoli aziendali

Previsione di spesa per ogni annualità del Piano

VOCI DI SPESA	Anno 2026	Anno 2027	Anno 2028
Reti TLC - nuovi acquisti/potenziamento	85.000	20.000	20.000
HW - nuovi acquisti/potenziamento	30.000	30.000	30.000
SW - nuovi canoni SaaS	Non previsti	Non previsti	Non previsti
SW - Progetti Sistema Lab. e Digitalizzazione Dati Sanitari	400.000	400.000	400.000
Totale nuovi acquisti	**515.000**	**450.000**	**450.000**
Reti TLC - manutenzione	50.000	50.000	50.000
HW - manutenzione	20.000	20.000	20.000
SW - Canoni esistenti - SaaS/manutenzione	40.000	40.000	40.000
Totale canoni/manutenzione	**110.000**	**110.000**	**110.000**
Servizi Professionali ICT - consulenza e assistenza	70.000	50.000	50.000
Totale	**695.000**	**610.000**	**610.000**

PARTE PRIMA – Le Componenti Strategiche

Capitolo 1 – Organizzazione e gestione del cambiamento

La trasformazione digitale richiede un processo integrato per creare ecosistemi digitali strutturati, sostenuti da organizzazioni pubbliche semplificate, trasparenti ed aperte, con servizi di qualità erogati proattivamente per anticipare le esigenze dei cittadini. Questo approccio innovativo deve affrontare sistematicamente organizzazione, processi, regole, dati e tecnologie, facilitando lo scambio di buone pratiche e promuovendo una cultura amministrativa digitale.

L'art. 6 del Decreto-legge n. 80/2021 introduce il Piano Integrato di Attività e Organizzazione (PIAO) per migliorare la qualità e la trasparenza dell'attività amministrativa e semplificare i processi. Anche se molte procedure amministrative sono già definite, possono essere reingegnerizzate con interventi di semplificazione e digitalizzazione.

La trasformazione degli enti pubblici in "**ecosistemi amministrativi digitali**" è fondamentale per migliorare l'efficienza e la qualità dei servizi offerti. Utilizzando piattaforme organizzative e tecnologiche avanzate, si può garantire che il valore pubblico sia creato in modo attivo e collaborativo da cittadini, imprese e operatori pubblici.

I "**processi digitali collettivi**" basati su *e-service* e *API* sono cruciali per implementare il principio "*once-only*", che evita la duplicazione di richieste di dati già posseduti dalla Pubblica Amministrazione. Questo approccio non solo migliora la trasparenza e la correttezza amministrativa, ma assicura anche la sicurezza informatica e la protezione dei dati personali, creando un ecosistema digitale efficiente e sicuro.

La trasformazione digitale richiede un processo integrato che coinvolga decisori pubblici, dirigenza, cittadini e imprese, promuovendo la partecipazione e la consultazione. È necessaria una collaborazione tra tutte le componenti istituzionali, inclusi Governo, Enti centrali, Regioni ed Enti locali, aperta anche al partenariato economico e sociale.

Per tutte le pubbliche amministrazioni, è fondamentale:

1. la collaborazione tra i vari livelli istituzionali per strutturare correttamente e-service integrati e interoperabili, identificando i procedimenti più richiesti da cittadini e imprese;

2. la gestione del ciclo di vita degli ***e-service***, possibile solo se si dispone di competenze specialistiche adeguate all'interno dell'Ufficio per la transizione al digitale (UDT), sia in forma singola che associata.

Consolidamento del ruolo del RDT

La strategia adottata dall'IZSLT ai fini del consolidamento del ruolo del RDT e di conseguenza dell'UDT, si può riassumere nei seguenti punti:

1. **Chiarezza di Mandato e Autonomia Decisionale**

   Il RTD deve essere supportato da una chiarificazione del proprio mandato, in modo che la sua posizione all'interno dell'organigramma dell'IZSLT sia ben definita. Questo implica anche una maggiore autonomia decisionale in ambito tecnologico e digitale, nonché l'assegnazione di risorse adeguate per implementare i progetti di trasformazione digitale. Il RTD deve appartenere a un livello strategico dell'Istituto, preferibilmente in stretto raccordo con la Direzione Generale. La sua posizione di leadership garantisce che la transizione digitale non sia delegata solo agli ambiti tecnici, ma sia vista come una priorità strategica per l'intera organizzazione.

2. **Integrazione con la *Governance* dell'IZSLT**

   Il RTD deve operare in stretta sinergia con la ***governance*** dell'Istituto, supportando la Direzione Generale nel definire le priorità e gli obiettivi digitali. Il suo ruolo deve essere integrato con gli altri vertici dell'Istituto, come il Direttore Sanitario e il Responsabile della Ricerca, per garantire che la digitalizzazione non sia limitata solo agli aspetti amministrativi, ma anche ai processi di ricerca e innovazione.

3. **Sviluppo di un Piano di Digitalizzazione a Lungo Periodo**

   Il consolidamento del ruolo del RTD implica anche lo sviluppo e la gestione del presente Piano, per la definizione delle azioni a lungo termine, degli obiettivi, delle priorità e delle tempistiche sulle iniziative digitali e, nello specifico, atte a:

   - riorganizzare ed ottimizzare i flussi operativi interni, dalla gestione dei dati di laboratorio alla gestione dei servizi di diagnostica e ricerca;

- esplorare ed integrare tecnologie innovative come, ad esempio, l'intelligenza artificiale (AI) ed i big data analytics, per il monitoraggio dell'attività istituzionale al fine di migliorarne l'efficienza operativa.

4. **Monitoraggio e Misurazione dei Risultati**

   Il RTD deve anche definire indicatori di performance per misurare l'efficacia dei progetti di digitalizzazione. Questi indicatori devono riguardare la qualità dei servizi digitali, l'efficienza dei processi, il risparmio di risorse, e la soddisfazione del personale. Il monitoraggio continuo consente di effettuare correzioni tempestive e garantire che gli obiettivi vengano raggiunti in modo efficace.

5. **Rafforzamento della Collaborazione Interistituzionale**

   Il RTD deve favorire una collaborazione attiva con altre istituzioni, sia a livello locale (ad esempio, con le ASL, le Regioni, le università) che a livello nazionale (con il Ministero della Salute, AGID, etc.). L'obiettivo è creare una rete di scambio di informazioni, dati e best practices, al fine di migliorare la gestione e la sicurezza dei dati e promuovere l'ottimizzazione e l'interoperabilità dei processi.

Competenze digitali

Nel contesto dell'IZSLT, l'obiettivo delle competenze digitali, in relazione al Piano Triennale, si inserisce in un percorso che va oltre la semplice adozione di tecnologie digitali, estendendosi a un piano di trasformazione complessivo, che include la formazione del personale, l'adeguamento delle infrastrutture e l'interoperabilità dei processi. L'IZSLT, come molte altre istituzioni pubbliche nel settore della salute animale e della sicurezza alimentare, si trova ad affrontare la necessità di aggiornare e potenziare le competenze digitali per rispondere alle sfide imposte dalla crescente digitalizzazione e innovazione tecnologica.

Competenze Digitali nel Settore Sanitario Veterinario

Gli Istituti Zooprofilattici Sperimentali sono enti di ricerca e di servizio che operano nel campo della **sanità pubblica veterinaria**, con compiti di diagnostica, sorveglianza, ricerca e formazione in ambito veterinario. In questo contesto, le competenze digitali non si limitano alla mera conoscenza degli strumenti tecnologici, ma devono anche comprendere la capacità di gestire sistemi complessi di raccolta e analisi dei dati, di utilizzare piattaforme di interoperabilità sanitaria e di adottare sistemi di telemedicina o altre tecnologie avanzate per la gestione dei dati sanitari.

Obiettivi Formativi e Strategia

Nel Piano Triennale, l'obiettivo principale per le PA come l'IZSLT, riguarda lo sviluppo di competenze digitali a più livelli, sia per il personale tecnico-scientifico che per quello amministrativo.

Gli obiettivi specifici includono:

- **Aggiornamento delle competenze in ambito digitale per il personale scientifico e tecnico**: Il personale che si occupa di ricerca e diagnostica deve essere formato per saper utilizzare avanzati strumenti digitali per la gestione dei laboratori, l'analisi dei dati sanitari, la gestione delle informazioni relative alla salute animale e la sicurezza alimentare. Gli strumenti includono software di analisi bioinformatica, piattaforme di gestione delle banche dati, e applicazioni di intelligenza artificiale per il miglioramento dei processi diagnostici.
- **Formazione continua del personale amministrativo e gestionale**: I dipendenti amministrativi devono acquisire competenze nella gestione elettronica dei documenti, nell'utilizzo di software per la gestione dei bilanci, delle risorse e dei contratti, e nell'adozione di strumenti di gestione della *governance* digitale. Questo permetterà di semplificare i processi burocratici, migliorare la trasparenza e l'efficienza operativa e rendere più accessibile la comunicazione con i cittadini e le altre istituzioni.
- **Competenze specifiche nella gestione dei dati sanitari e dell'interoperabilità**: il personale dell'IZSLT, deve sviluppare competenze nel trattare dati sanitari sensibili, nel garantire la sicurezza informatica dei sistemi utilizzati e nell'assicurare la collaborazione con altre strutture sanitarie e amministrazioni pubbliche, sia a livello regionale che nazionale. Questo comprende l'adozione di standard di interoperabilità, come il FHIR (*Fast Healthcare Interoperability Resources*), e l'integrazione di piattaforme per il monitoraggio delle malattie, la tracciabilità degli alimenti e la gestione dei focolai epidemici.
- **Promozione di una cultura digitale orientata all'innovazione**: un altro obiettivo importante è la creazione di una cultura digitale all'interno dell'Istituto, che vada oltre la semplice acquisizione di strumenti. Ciò implica incentivare il personale a essere proattivo nell'adottare e sperimentare nuove tecnologie, come

ad esempio, l'analisi predittiva dei focolai zoonotici o l'utilizzo di sensori IoT per il monitoraggio in tempo reale della salute animale.

Implementazione delle Competenze Digitali

Per raggiungere questi obiettivi, l'IZSLT si sta adoperando per adottare una serie di azioni concrete, come:

- Corsi di formazione continua e aggiornamenti periodici per il personale tecnico e amministrativo, su piattaforme e strumenti digitali, per la gestione dei dati sanitari, la cybersecurity e l'aggiornamento su nuove tecnologie.
- Creazione di un team di esperti, dedicato alla trasformazione digitale che si occupi della gestione dei progetti di digitalizzazione, dal miglioramento delle infrastrutture tecnologiche alla gestione dei cambiamenti organizzativi legati all'adozione delle nuove tecnologie.
- Collaborazione con università e istituti di ricerca per sviluppare e implementare nuove soluzioni tecnologiche, partecipare a progetti di ricerca innovativi e promuovere la condivisione di conoscenze e *best pratice*.
- Sistemi di monitoraggio e valutazione per il monitoraggio delle competenze digitali del personale, per valutare l'efficacia dei programmi di formazione e per identificare le aree in cui sono necessari ulteriori sviluppi.

AgID Academy

Una delle principali innovazioni introdotte nell'aggiornamento 2026 del Piano è **l'AgID Academy**. Questa piattaforma rappresenta un pilastro strategico per lo sviluppo delle competenze digitali nella PA italiana. La sua creazione risponde all'esigenza di rafforzare la preparazione del personale pubblico affinché possa governare in modo consapevole ed efficace le tecnologie emergenti e i nuovi strumenti messi a disposizione dall'ecosistema digitale nazionale. Dal punto di vista operativo, l'AgID Academy offre percorsi formativi che coprono diversi ambiti strategici. Tra questi rientrano le competenze digitali di base e avanzate, la conoscenza delle piattaforme nazionali — con particolare attenzione al nuovo **IT-Wallet**, descritto nel Piano 2026 come una delle aree su cui verranno consolidate progettualità e linee di azione — e l'approfondimento sull'adozione responsabile dell'intelligenza artificiale.

La Academy dedica inoltre una particolare attenzione a settori critici per l'evoluzione dell'amministrazione digitale, come la gestione documentale, la dematerializzazione, la sicurezza informatica, la *governance* del dato e il corretto utilizzo delle infrastrutture e piattaforme nazionali (ad esempio la Piattaforma Digitale Nazionale Dati).

Dal punto di vista strategico, l'AgID Academy non solo consolida il processo di digitalizzazione della PA, ma apre la strada alla nuova programmazione 2027–2029. In questo scenario, la Academy assume il ruolo di infrastruttura formativa cruciale per garantire continuità nella crescita delle competenze e per preparare la PA italiana ad affrontare le sfide tecnologiche dei prossimi anni.

Contesto normativo

Riferimenti normativi nazionali:

- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (in breve CAD) art. 14-bis lettera c).
- Circolare n. 3 del 1° ottobre 2018 del Ministro per la Pubblica Amministrazione sul Responsabile per la transizione al digitale.

Riferimenti normativi europei:

- Ministerial Declaration on eGovernment - Tallinn declaration - 6 ottobre 2017;
- Regolamento (UE) 2018/1724 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) 1024/2012;
- Berlin Declaration on Digital Society and Value-based Digital Government – 8 dicembre 2020;
- Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al comitato delle regioni Bussola per il digitale 2030: il modello europeo per il decennio digitale;

- Decisione (EU) 2022/2481 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 che istituisce il programma strategico per il Decennio Digitale 2030;
- Decisione di esecuzione (ue) della Commissione Europea del 30 giugno 2023 che definisce gli indicatori chiave di prestazione per misurare i progressi compiuti verso il conseguimento degli obiettivi digitali di cui all'articolo 4, paragrafo 1, della decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio;
- Raccomandazione del Consiglio del 22 maggio 2018 relativa alle competenze chiave per l'apprendimento permanente (GU 2018/C 189/01);
- Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni COM (2020) 67 final del 19 febbraio 2020 - Plasmare il futuro digitale dell'Europa;
- Decisione del Parlamento Europeo e del Consiglio relativa a un Anno Europeo delle Competenze 2023 COM (2022) 526 final 2022/0326.

Obiettivi e Risultati attesi

1.2 - Diffusione competenze digitali nel Paese e nella PA

RA1.2.1 - Diffusione competenze digitali di base per cittadini e imprese

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA, in funzione delle proprie necessità, partecipano alle iniziative pilota, alle iniziative di sensibilizzazione e a quelle di formazione di base e specialistica per il proprio personale, come previsto dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali. **CAP1.PA.07**	ATTUALMENTE VIGENTE	ATTUALMENTE VIGENTE
Le PA aderiscono all'iniziativa "Syllabus per la formazione digitale" e promuovono la partecipazione alle iniziative formative sulle competenze di base da parte dei dipendenti pubblici, concorrendo al conseguimento dei target del PNRR in tema di sviluppo del capitale umano della PA e in linea con il Piano strategico nazionale per le competenze digitali. **CAP1.PA.08**	ATTUALMENTE VIGENTE	ATTUALMENTE VIGENTE

RA1.2.2 - Diffusione competenze digitali di base nella PA

LINEE DI AZIONE	**SCADENZA PT**	**SCADENZA IZSLT**
I RTD e il personale degli UTD delle PA possono partecipare alle attività di rafforzamento delle competenze e scambio sul tema AI proposte da AgID. **CAP1.PA.14**	Ottobre 2025	Dicembre 2025

Capitolo 2 - Il procurement per la trasformazione digitale

Il *procurement* per la trasformazione digitale è un elemento cruciale per garantire che l'IZSLT possa implementare con successo le soluzioni tecnologiche necessarie a modernizzare i suoi processi, migliorare l'efficienza operativa ed apportare innovazioni nella ricerca scientifica e nella diagnostica. Poiché la transizione digitale non si limita all'acquisizione di software e hardware, ma coinvolge anche la selezione di soluzioni integrative, servizi e competenze, un approccio strategico al *procurement* è fondamentale per assicurare la qualità e la sostenibilità dei progetti.

Il processo di *procurement* deve rispondere non solo alle esigenze tecnologiche e scientifiche dell'IZSLT ma anche alle normative pubbliche in materia di appalti, all'efficienza nell'uso delle risorse pubbliche e al rispetto delle linee guida fornite dal Piano Triennale. La digitalizzazione delle funzioni dell'Istituto richiede un'attenta selezione di soluzioni innovative ma anche la capacità di integrarle efficacemente nei processi esistenti.

Gli obiettivi principali del *procurement* nell'IZSLT possono essere riassunti in:

- **Innovazione tecnologica**: garantire l'acquisizione di soluzioni digitali all'avanguardia che supportino la modernizzazione dei laboratori, la gestione dei dati sanitari e zooprofilattici e le attività di ricerca scientifica.
- **Efficienza operativa**: ottimizzare i flussi di lavoro interni e migliorare la gestione delle risorse attraverso l'adozione di tecnologie che automatizzino i processi, riducano i tempi di risposta e migliorino la qualità dei servizi.
- **Interoperabilità**: assicurarsi che le soluzioni digitali siano interoperabili con altri sistemi informatici regionali, nazionali e internazionali, migliorando la comunicazione e la collaborazione con altre istituzioni pubbliche e private.
- **Sostenibilità e scalabilità**: selezionare tecnologie che possano crescere con l'Istituto, supportando l'adozione di nuove soluzioni future e garantendo un buon rapporto costi-benefici.
- **Conformità alle normative**: rispetto delle normative di sicurezza dei dati e sicurezza informatica per garantire la protezione delle informazioni sensibili trattate dall'IZSLT.

Prima di avviare qualsiasi procedura di acquisto, è fondamentale che l'IZSLT definisca chiaramente le proprie esigenze tecnologiche e i requisiti funzionali. Ciò implica un'analisi approfondita delle necessità dell'Istituto in ambito digitale e l'elaborazione di un piano di digitalizzazione che identifichi le aree critiche da migliorare. Per questo si rendono necessari il coinvolgimento delle funzioni operative, dei laboratori, del personale amministrativo e dei ricercatori e per ogni

area del progetto di digitalizzazione, l'indicazione chiara dei requisiti tecnici (ad esempio, compatibilità con sistemi esistenti, capacità di scalabilità) e dei requisiti funzionali (ad esempio, velocità di elaborazione, facilità d'uso, interfaccia utente). L'approccio deve essere trasparente e competitivo, rispettando le normative italiane ed europee sugli appalti pubblici. Allo stato attuale, Smarter Italy è il principale programma di sperimentazione di appalti di innovazione.

A seconda dell'entità degli investimenti, l'IZSLT opta per diverse modalità di gara. I fornitori che offrono soluzioni innovative, vengono identificati sulla base con una comprovata esperienza nel settore pubblico e sanitario. Il processo di selezione tiene conto non solo dei costi ma anche della qualità delle soluzioni proposte, della reputazione dei fornitori e della capacità di assistenza post-vendita. Le offerte ricevute vengono valutate in base a criteri oggettivi, che includano l'affidabilità delle tecnologie, la compatibilità con i sistemi esistenti, la sicurezza informatica e il rispetto delle normative di protezione dei dati. Una volta selezionati i fornitori, il passo successivo è l'implementazione delle soluzioni tecnologiche. Questo è un momento cruciale, poiché implica la personalizzazione e l'integrazione delle tecnologie nei processi operativi dell'IZSLT:

- **Progetto pilota**: è consigliabile avviare un progetto pilota per testare l'efficacia delle soluzioni in un contesto controllato, prima della piena implementazione su scala più ampia. Questo permette di identificare eventuali problematiche e di apportare modifiche prima di un'adozione totale.
- **Formazione del personale**: parallelamente all'implementazione delle soluzioni digitali, sarà fondamentale organizzare sessioni di formazione per il personale coinvolto, in modo che possa utilizzare efficacemente le nuove tecnologie.
- **Monitoraggio delle performance**: durante la fase di implementazione e successivamente, è fondamentale monitorare i risultati per valutare se le soluzioni adottate stanno soddisfacendo i requisiti prefissati. Ciò include la raccolta di feedback dagli utenti finali, l'analisi dei tempi di risposta, della sicurezza e della qualità dei dati.
- **Contratti di manutenzione**: dovranno essere stipularti contratti di assistenza tecnica e manutenzione per garantire che le soluzioni digitali rimangano operative e aggiornate nel tempo, minimizzando eventuali disservizi.
- **Aggiornamenti e miglioramenti**: il procurement deve includere la possibilità di aggiornamenti software e di integrazione di nuove funzionalità nel corso del tempo, per rispondere alle mutevoli esigenze dell'Istituto.
- **Analisi costi-benefici:** ogni fase del progetto dovrebbe essere accompagnata da un'accurata analisi costi-benefici, per garantire che l'investimento tecnologico porti un ritorno tangibile in termini di risparmio sui costi operativi, efficienza dei processi e miglioramento dei servizi.

- **Monitoraggio delle risorse:** un controllo rigoroso dei costi associati all'acquisto, implementazione e gestione delle soluzioni digitali deve essere previsto per evitare sprechi e garantire che le risorse siano impiegate in modo ottimale.

Contesto normativo

Riferimenti normativi nazionali:

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

Riferimenti normativi europei:

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

Obiettivi e Risultati attesi

2.1 - Rafforzare l'ecosistema nazionale di approvvigionamento digitale

RA2.1.1 - Diffusione del processo di certificazione delle piattaforme di approvvigionamento digitale

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le stazioni appaltanti devono digitalizzare la fase di esecuzione dell'appalto. **CAP2.PA.02**	Giugno 2025	Dicembre 2026

2.2 - Diffondere l'utilizzo degli appalti innovativi

RA2.2.1 - Incremento della partecipazione di PMI e start up agli appalti di innovazione

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le amministrazioni entrano nel programma delle consultazioni di mercato - **CAP2.PA.08**	Da Dicembre 2026	Da Dicembre 2026

RA2.2.2 - Incremento della diffusione degli appalti di innovazione nelle PA

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le amministrazioni che hanno avviato appalti di innovazione completano la fase di aggiudicazione e di esecuzione **- CAP2.PA.09**	Giugno 2026	Giugno 2026

2.3 - Favorire e monitorare l’utilizzo dei servizi previsti dalle Gare strategiche

RA2.3.1 - Incremento del livello di trasformazione digitale mediante la disponibilità di Gare strategiche allo scopo definite

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA, nel proprio piano acquisti, programmano i fabbisogni di adesione alle iniziative strategiche disponibili per il perseguimento degli obiettivi del Piano triennale per l’anno 2025. **CAP2.PA.04**	Settembre 2024	Settembre 2024
Le PA programmano i fabbisogni di adesione alle iniziative strategiche per il perseguimento degli obiettivi del Piano triennale per l’anno 2026. **CAP2.PA.05**	Settembre 2025	Settembre 2025
Le PA programmano i fabbisogni di adesione alle iniziative strategiche per il perseguimento degli obiettivi del Piano triennale per l’anno 2027. **CAP2.PA.06**	Settembre 2026	Settembre 2026

PARTE SECONDA – Le Componenti Tecnologiche

Capitolo 3 – Servizi

Negli ultimi anni, la digitalizzazione ha rivoluzionato i servizi pubblici, con gli enti locali al centro di questo cambiamento. L'adozione di tecnologie digitali è cruciale per migliorare l'efficienza, aumentare la trasparenza e garantire la qualità dei servizi offerti ai cittadini. Un *framework* di riferimento è essenziale per guidare le scelte tecnologiche e l'architettura a microservizi emerge come una soluzione agile e scalabile per standardizzare i processi digitali e facilitare il change management.

Il Piano Triennale promuove l'evoluzione del modello di **interoperabilità**, passando dalla condivisione dei dati alla condivisione dei servizi. L'interoperabilità facilita l'interazione digitale tra Pubbliche Amministrazioni (PA), cittadini e imprese, seguendo l'*European Interoperability Framework* e il principio "*once only*", che evita di richiedere dati già posseduti dalla PA.

Per raggiungere la completa interoperabilità dei *dataset* e dei servizi chiave tra PA centrali e locali, è stata creata la **Piattaforma Digitale Nazionale Dati** (PDND) nell'ambito del Piano Nazionale di Ripresa e Resilienza. La PDND gestisce autenticazione, autorizzazione e conservazione delle informazioni sugli accessi e le transazioni, semplificando gli accordi di interoperabilità e riducendo oneri amministrativi. Le amministrazioni possono pubblicare *e-service* conformi alle Linee Guida tramite **API**, registrate nel Catalogo pubblico degli *e-service*. Il Dipartimento per la Trasformazione Digitale supporta le PA nell'adozione del Modello di interoperabilità, pianificando e coordinando iniziative di condivisione attraverso protocolli d'intesa e accordi, costituzione di tavoli di lavoro, progettualità congiunte e capitalizzazione di soluzioni *open source.*

Gli strumenti per la condivisione di conoscenza e di soluzioni a disposizione delle amministrazioni sono:

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

Contesto normativo

Riferimenti normativi nazionali:

- Decreto legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”;
- Decreto legislativo 7 marzo 2005, n. 82 “Codice dell'amministrazione digitale” (CAD);
- Decreto del Presidente della Repubblica 7 settembre 2010, n. 160 “Regolamento per la semplificazione ed il riordino della disciplina sullo sportello unico per le attività produttive, ai sensi dell'articolo 38, comma 3, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133”;
- Decreto-legge 14 dicembre 2018, n. 135, convertito con modificazioni dalla Legge 11 febbraio 2019, n. 12 “Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la Pubblica Amministrazione”;
- Decreto-legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 “Misure urgenti per la semplificazione e l'innovazione digitale”;
- Decreto-legge 31 maggio 2021, n. 77, convertito con modificazioni dalla Legge 29 luglio 2021, n. 108 “Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure”;
- Linee Guida AGID per transitare al nuovo modello di interoperabilità (2017);
- Linee Guida AGID sull’interoperabilità tecnica delle Pubbliche Amministrazioni (2021);
- Linee Guida AGID sull’infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l’interoperabilità dei sistemi informativi e delle basi di dati (2021);
- Linee Guida Tecnologie e standard per la sicurezza dell’interoperabilità tramite API dei sistemi informatici;
- Decreto 12 novembre 2021 del Ministero dello sviluppo economico di modifica dell'allegato tecnico del decreto del Presidente della Repubblica 7 settembre 2010, n. 160;
- Decreto 22 settembre 2022 della Presidenza Del Consiglio Dei Ministri;
- Piano Nazionale di Ripresa e Resilienza:
    - Investimento M1C1 1.3: “Dati e interoperabilità”;
    - Investimento M1C1 2.2: “Task Force digitalizzazione, monitoraggio e performance”.

Riferimenti normativi europei:

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

Obiettivi e Risultati attesi

3.1 - Migliorare la capacità di erogare e-service

RA3.1.1 - Incremento del numero di “e-service” registrati sul Catalogo Pubblico PDND

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA cessano di utilizzare modalità di interoperabilità diverse da PDND. **CAP3.PA.01**	Da gennaio 2024	Da gennaio 2026
Le Amministrazioni iniziano la migrazione dei servizi erogati in interoperabilità dalle attuali modalità alla PDND. **CAP3.PA.02**	Da gennaio 2024	Da gennaio 2026

RA3.1.2 - Aumento del numero di Richieste di Fruizione Autorizzate su PDND

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA utilizzano le API presenti sul Catalogo - **CAP3.PA.06**	Da gennaio 2024	Da gennaio 2026
Le PA effettuano richieste di fruizione di servizi erogati da privati - **CAP3.PA.07**	Da luglio 2025	Da luglio 2026

RA3.1.3 - Ampliamento del numero delle amministrazioni coinvolte nell'evoluzione delle Linee guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA evidenziano le esigenze che non trovano riscontro nella "Linee guida sull'interoperabilità tecnica delle pubbliche amministrazioni" e partecipano alla definizione di pattern e profili di interoperabilità per l'aggiornamento delle stesse - **CAP3.PA.08**	Da gennaio 2024	Da gennaio 2026

Progettazione dei servizi: accessibilità e design

La progettazione dei servizi digitali riveste un ruolo fondamentale per garantire che tutte le risorse, i dati e le interazioni siano accessibili e fruibili da una vasta gamma di utenti. L'accessibilità e il design sono due pilastri centrali che devono orientare lo sviluppo di tutte le soluzioni digitali, per assicurare che rispondano alle esigenze di tutti gli utenti, inclusi quelli con disabilità o con competenze digitali limitate.

L'**accessibilità** si riferisce alla progettazione di servizi digitali che possano essere utilizzati senza barriere da tutti gli utenti, indipendentemente dalle loro capacità fisiche, sensoriali, cognitive o tecnologiche. In linea con le normative italiane ed europee, l'IZSLT si impegna a sviluppare e implementare servizi che rispettino i più alti standard di **accessibilità digitale**.

Il **design** dei servizi digitali è il processo di progettazione che si concentra sull'esperienza utente, sulla facilità di utilizzo e sulla creazione di soluzioni esteticamente piacevoli ma anche funzionali. Il design deve rispondere alle esigenze degli utenti, rendendo i servizi facili da usare, intuitivi e accessibili. Per garantire che i servizi digitali abbiano un chiaro valore per l'utente, è indispensabile adottare un approccio multidisciplinare. Questo significa integrare diverse metodologie e tecniche nella progettazione dei servizi.

Per migliorare la capacità di erogare servizi di qualità, l'IZSLT si è attivato verso un miglioramento continuo rispetto alle seguenti attività:

- Adozione di modelli e strumenti validati.
- Monitoraggio costante dei servizi online.
- Incremento dell'accessibilità dei servizi.
- Scambio di buone pratiche tra amministrazioni.
- Riuso e condivisione di software e competenze.

l design dei servizi digitali deve rispettare le normative sulla protezione dei dati personali, garantendo che l'accesso ai dati sensibili, come quelli sanitari e diagnostici, avvenga in modo sicuro e conforme. I design delle interfacce devono includere meccanismi chiari per l'informativa sulla privacy, l'autorizzazione al trattamento dei dati e la gestione dei consensi.

Dal 2022, l'IZSLT utilizza *Web Analytics* Italia, una piattaforma nazionale *open source* che, oltre a consentire il monitoraggio dei servizi online presenti sul proprio sito web, offre rilevazioni statistiche su indicatori utili al miglioramento continuo dell'esperienza utente.

Contesto normativo

Riferimenti normativi nazionali:

- Legge 241/1990, Nuove norme sul procedimento amministrativo.
- DPR 445/2000, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

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

Riferimenti normativi europei:

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

Obiettivi e risultati attesi

3.2 - Migliorare la capacità di generare ed erogare servizi digitali

RA3.2.2 - Incremento dell'accessibilità dei servizi digitali

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA pubblicano, entro il 23 settembre, esclusivamente tramite l'applicazione form.AGID.gov.it, la dichiarazione di accessibilità per ciascuno dei propri siti web e APP mobili - **CAP3.PA.14**	Settembre 2025	Settembre 2025
Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web - **CAP3.PA.15**	Marzo 2026	Marzo 2026
Le PA pubblicano, entro il 23 settembre, esclusivamente tramite l'applicazione form.AGID.gov.it, la dichiarazione di accessibilità per ciascuno dei propri siti web e APP mobili - **CAP3.PA.16**	Settembre 2026	Settembre 2026

Formazione, gestione e conservazione dei documenti informatici

Le Linee guida dell'AGID, sulla formazione, gestione e conservazione dei documenti informatici, entrate in vigore il 1° gennaio 2022, rappresentano un passo fondamentale nel rafforzamento e armonizzazione del quadro normativo italiano per la gestione della documentazione digitale nelle Pubbliche Amministrazioni (PA). Esse si inseriscono nell'ambito della transizione digitale in atto, mirando a semplificare, rendere più accessibile e integrare la disciplina riguardante la produzione, gestione e conservazione dei documenti informatici.

Le PA sono chiamate a implementare misure specifiche per conformarsi alle Linee guida, che prevedono principalmente:

- **Gestione corretta dei documenti sin dalla loro creazione**: ogni documento informatico deve essere creato e gestito in modo tale da garantire il rispetto degli obblighi amministrativi, giuridici e archivistici (paragrafo 1.11 delle Linee guida). Ciò significa che i documenti devono essere tracciabili, correttamente classificati e archiviati secondo le normative vigenti.
- **Gestione dei flussi documentali**: i flussi documentali devono essere organizzati in aggregazioni informatiche (paragrafo 3.3), facilitando la gestione integrata dei documenti all'interno del sistema informatico dell'amministrazione.
- **Nomina dei ruoli e delle responsabilità**: devono essere designati i responsabili per la gestione e la conservazione dei documenti (paragrafi 3.1.2 e 4.4). Questo implica la creazione di figure specifiche, come il Responsabile della gestione documentale e il Responsabile della conservazione digitale, che saranno incaricati di attuare le politiche e i processi relativi alla documentazione elettronica.
- **Adozione di manuali**: ogni amministrazione deve adottare un Manuale di gestione documentale e un Manuale di conservazione (paragrafi 3.5 e 4.7), i quali devono essere chiari, accessibili e pubblicati nell'area "Amministrazione trasparente" dell'amministrazione, come stabilito dal D.Lgs. 33/2013. Questi manuali devono descrivere dettagliatamente le procedure operative da seguire nella gestione e conservazione dei documenti.
- **Sicurezza ICT**: è obbligatorio rispettare le misure minime di sicurezza ICT indicate da AGID nella circolare del 18 aprile 2017 (n. 2/2017). Questo include l'adozione di tecnologie sicure per la gestione dei documenti elettronici e la protezione dei dati.
- **Protezione dei dati personali**: le amministrazioni devono garantire che la gestione dei documenti rispetti le normative sulla protezione dei dati personali, in particolare l'art. 32 del GDPR, che stabilisce le misure tecniche e organizzative da adottare per garantire la sicurezza dei dati.

- **Trasferimento dei documenti al sistema di conservazione**: le amministrazioni sono obbligate a trasferire i documenti al sistema di conservazione digitale, come indicato al paragrafo 4 e nell'art. 44, comma 1-bis, del Codice dell'Amministrazione Digitale (CAD).

La corretta gestione e conservazione dei documenti informatici non solo assicura l'efficienza operativa ma tutela anche la trasparenza e l'affidabilità delle informazioni nell'ambito delle pubbliche amministrazioni e delle istituzioni sanitarie come l'IZSLT.

Contesto normativo

Riferimenti normativi nazionali:

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

Riferimenti normativi europei:

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

Obiettivi e risultati attesi

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

RA3.3.1 - Monitorare l'attuazione delle linee guida

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA devono verificare che in "Amministrazione trasparente" sia pubblicato il manuale di gestione documentale, la nomina del responsabile della gestione documentale per ciascuna AOO e qualora siano presenti più AOO la nomina del coordinatore della gestione documentale - **CAP3.PA.17**	Giugno 2025	Giugno 2025
Le PA devono verificare che in "Amministrazione trasparente" sia pubblicato il manuale di conservazione e la nomina del responsabile della conservazione - **CAP3.PA.18**	Giugno 2026	Giugno 2026

Capitolo 4 – Piattaforme

Nel Piano Triennale, l'attenzione è rivolta all'evoluzione delle piattaforme nella Pubblica Amministrazione, strumenti chiave nella digitalizzazione dei processi amministrativi e dei servizi pubblici. Queste piattaforme sono ormai ben consolidate e mature, come già illustrato nei piani precedenti ma il Piano 2024-2026 si concentra sul miglioramento dei servizi erogati a cittadini, imprese e altre amministrazioni, con particolare attenzione alla continuità e all'evoluzione dei servizi descritti nel Capitolo 3, dedicato ai "Servizi".

L'obiettivo principale di tutte le piattaforme esaminate nel Piano è migliorare i servizi esistenti, attraverso l'introduzione di **innovazioni**, la **semplicità d'uso**, e il miglioramento dell'**interoperabilità** e della **sicurezza** dei sistemi. L'idea è ottimizzare l'esperienza degli utenti (cittadini, imprese e PA) rendendo i processi sempre più efficienti e trasparenti. Ogni piattaforma contribuisce a questi obiettivi in modo specifico ma il risultato complessivo è quello di **facilitare l'accesso ai servizi pubblici**, semplificare le procedure e garantire maggiore **efficacia** nelle interazioni tra amministrazioni, cittadini e imprese.

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

1. **PagoPA:** è una piattaforma digitale progettata per semplificare e rendere più sicuri i pagamenti elettronici verso la Pubblica Amministrazione, facilitando l'interazione tra cittadini, imprese e amministrazioni. L'obiettivo principale di *pagoPA* è migliorare l'efficienza dei pagamenti per i servizi pubblici, rendendo il processo più rapido, intuitivo e accessibile a tutti. La piattaforma è pensata per ridurre progressivamente l'uso del contante, incoraggiando i cittadini e le imprese ad adottare soluzioni di pagamento digitale.

2. **AppIO**: è una piattaforma digitale progettata per semplificare e centralizzare l'accesso ai servizi pubblici digitali in Italia, rappresentando un elemento fondamentale nella strategia di cittadinanza digitale del Governo italiano. Lanciata come progetto open source, l'app IO ha l'obiettivo di mettere a disposizione di cittadini e enti pubblici un unico canale di accesso per fruire di tutti i servizi digitali offerti dalla Pubblica Amministrazione. L'iniziativa si inserisce nella più ampia trasformazione digitale della PA, con l'obiettivo di rendere l'interazione con le amministrazioni pubbliche più semplice, veloce e trasparente.

3. **SEND - Servizio Notifiche Digitali**: è una piattaforma sviluppata per semplificare e rendere più efficienti le notifiche a valore legale tra le Pubbliche Amministrazioni e i cittadini o le imprese. Istituita ai sensi dell'art. 26 del decreto-legge 76/2020 (Decreto Semplificazioni), SEND rappresenta una rivoluzione nel processo di notificazione delle comunicazioni ufficiali, con l'obiettivo di velocizzare, snellire e rendere più sicuro l'invio e la ricezione di documenti legali.

4. **SPID (Sistema Pubblico di Identità Digitale):** è una delle piattaforme chiave per l'accesso ai servizi online della Pubblica Amministrazione in Italia. Consente ai cittadini e alle imprese di accedere in modo sicuro e rapido a una vasta gamma di servizi pubblici e privati tramite un'unica identità digitale, garantendo un sistema semplice ma altamente sicuro di autenticazione online. Questo sistema di autenticazione semplifica notevolmente l'interazione con la PA, migliorando l'efficienza e l'accessibilità dei servizi pubblici. Nel contesto del **PNRR** (Piano Nazionale di Ripresa e Resilienza), il sub-investimento M1C1 1.4.4 si concentra sul rafforzamento dell'adozione delle piattaforme nazionali di identità digitale, come **SPID** e **CIE** (Carta d'Identità Elettronica) e sull'Anagrafe Nazionale della Popolazione Residente (**ANPR**). Il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri, è il soggetto titolare di questo progetto che ha l'obiettivo di elevare la qualità, la sicurezza e l'interoperabilità dei servizi digitali. A tal fine, è necessario che il Sistema SPID evolva in base alle seguenti indicazioni:
   - attuazione delle "Linee guida OpenID Connect in SPID" (Determinazione del Direttore Generale di AGID n. 616/2021) comprensive dell'Avviso SPID n. 41 del 23/3/2023 versione 2.0 e il "Regolamento - SPID OpenID Connect Federation 1.0" (Determinazione del Direttore Generale di AGID n. 249/2022);
   - attuazione delle "Linee guida operative per la fruizione dei servizi SPID da parte dei minori" (Determinazione del Direttore Generale di AGID n. 133/2022);
   - attuazione delle "Linee guida recanti le regole tecniche dei Gestori di attributi qualificati" (Determinazione del Direttore Generale di AGID n. 215/2022);
   - promozione dell'utilizzo dello SPID dedicato all'uso professionale per l'accesso ai servizi online rivolti a professionisti e imprese.

5. **CIE** (**CIEId**): Carta d'Identità Elettronica (CIE) e la sua identità digitale (CIEId). Sviluppata e gestita dall'Istituto Poligrafico e Zecca dello Stato, consente la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, ai sensi del CAD, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale al momento del rilascio della CIE. La CIEId è comprovata dal cittadino attraverso l'uso della CIE o delle credenziali rilasciate dal Ministero. Come parte del continuo processo di miglioramento e digitalizzazione dei servizi, il Decreto 8 settembre 2022 ha definito alcune evoluzioni importanti per il servizio CIEId:

- Ampliamento del Set di Attributi Forniti tramite Autenticazione con CIEId: L'articolo 6 del decreto prevede l'ampliamento degli attributi identificativi che possono essere utilizzati tramite l'autenticazione digitale della CIEId. Questo include informazioni aggiuntive che possono essere usate per accedere a servizi pubblici e privati, migliorando l'efficacia dell'identità digitale e consentendo a cittadini e amministrazioni di avere informazioni più complete e verificate.
- Ampliamento delle Funzionalità del Portale del Cittadino: Come previsto dall'articolo 14, la CIE diventerà uno strumento ancora più centrale per i servizi ai cittadini. Tra le nuove funzionalità, spicca la possibilità di visualizzare, esprimere o revocare la volontà del cittadino in merito alla donazione di organi e tessuti. Questa funzione integrata nel sistema digitale della CIE consente una gestione sicura e immediata della volontà del cittadino, evitando la necessità di interventi cartacei.
- Implementazione dei Servizi Correlati al NIS (Numero Identificativo Servizi): Come stabilito dall'articolo 17, la CIEId si integrerà con un sistema che assegna un Numero Identificativo Servizi (NIS), per facilitare l'interazione con i vari servizi online e migliorare la gestione degli accessi da parte dei cittadini. Questo sistema contribuirà a migliorare la tracciabilità e l'efficienza delle transazioni elettroniche.
- Firma Elettronica Qualificata Remota: Un altro avanzamento rilevante riguarda l'implementazione della firma elettronica qualificata remota tramite l'utilizzo della CIE. Questo permetterà di firmare documenti e transazioni online in modo sicuro e legalmente valido, utilizzando la CIE come strumento per garantire l'autenticità e la validità delle firme.
- Integrazione con il Sistema ANPR: La CIEId sarà integrata con il Sistema ANPR (Anagrafe Nazionale della Popolazione Residente) per ricevere quotidianamente i dati relativi ai soggetti deceduti e per procedere al blocco tempestivo della CIEId. Questo processo garantirà che l'identità digitale dei cittadini non venga utilizzata in modo improprio e che venga aggiornato tempestivamente ogni dato relativo alla persona.
- Meccanismo di Controllo Genitoriale: La CIEId prevede anche lo sviluppo di un meccanismo di controllo genitoriale, che consentirà un accesso controllato ai servizi online da parte dei minori. Questo aspetto mira a garantire la protezione dei minori, permettendo ai genitori o tutori di monitorare e autorizzare l'accesso ai servizi digitali, in conformità con le normative di tutela e privacy.

6. **NoiPA:** è la piattaforma nazionale pensata per la **gestione del personale** della **Pubblica Amministrazione**, offrendo soluzioni avanzate e completamente digitalizzate per ottimizzare i processi **HR (Human Resources)**. Il suo obiettivo principale è garantire una gestione **integrata e flessibile** di tutte le attività

relative al personale delle pubbliche amministrazioni, sia per quanto riguarda i **servizi di gestione delle buste paga**, che per l'automazione e il monitoraggio degli **adempimenti normativi** in ambito lavorativo e retributivo.

7. **Fascicolo Sanitario Elettronico (FSE 2.0)**: rappresenta uno degli strumenti principali per la digitalizzazione del sistema sanitario nazionale e ha l'obiettivo di garantire l'accesso universale e omogeneo ai servizi di sanità digitale, sia per i cittadini che per gli operatori sanitari, su tutto il territorio italiano. Questa piattaforma, attraverso la raccolta e la gestione centralizzata delle informazioni sanitarie dei cittadini, si propone di migliorare l'efficacia e l'efficienza dei servizi sanitari, garantendo una migliore gestione delle cure e un accesso più semplice e tempestivo alle informazioni sanitarie.

8. **Sportelli Unici per le Attività Produttive (SUAP) e gli Sportelli Unici per l'Edilizia (SUE):** sono componenti fondamentali della Pubblica Amministrazione, soprattutto nell'ambito della semplificazione amministrativa e della digitalizzazione dei servizi. Questi sportelli rappresentano il punto di accesso unico per cittadini, imprese e professionisti, attraverso cui possono interagire con le amministrazioni pubbliche per adempiere agli obblighi legatile attività produttive e agli interventi edilizi. Entrambi i sistemi si inseriscono in un contesto normativo che punta a migliorare l'efficienza, la trasparenza e la tempestività dei servizi erogati dalle Pubbliche Amministrazioni.

9. **IT-Wallet**: è il portafoglio digitale pubblico italiano, progettato per permettere a cittadini e residenti di gestire in modo sicuro e immediato identità digitale, documenti e attestazioni verificate, utilizzabili sia online che nel mondo fisico. È composto da un portafoglio pubblico integrato nell'app IO e, in futuro, da portafogli privati conformi alle Linee Guida AgID e all'art. 64-quater del CAD. Il sistema consente di presentare attributi digitali già verificati, semplificando l'accesso ai servizi pubblici e privati, riducendo duplicazioni documentali e aumentando il controllo da parte dei cittadini sui propri dati.

Per quanto riguarda l'IZSLT, attualmente, vengono utilizzate le seguenti piattaforme:

- **PagoPA**, per il pagamento, ove previsto, delle prestazioni veterinarie, analisi di laboratorio e certificazioni;
- **SPID** per l'accesso al Portale degli Avvelenamenti, da parte di Medici Veterinari abilitati alla gestione informatizzata dei casi di avvelenamento, dalla denuncia del sospetto alla diagnosi definitiva.

Contesto normativo

PagoPA

Riferimenti normativi nazionali:

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

AppIO

Riferimenti normativi nazionali:

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

SEND

Riferimenti normativi nazionali:

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

SPID

Riferimenti normativi nazionali:

- Decreto legislativo 7 marzo 2005, n. 82 “Codice dell'amministrazione digitale” (CAD), art.64
- Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014 recante la Definizione delle caratteristiche del sistema pubblico per la gestione dell’identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese

- Regolamento AGID recante le regole tecniche dello SPID (2014)
- Regolamento AGID recante le modalità attuative per la realizzazione dello SPID (2014)
- Linee Guida AGID per la realizzazione di un modello di R.A.O. pubblico (2019)
- Linee guida per il rilascio dell'identità digitale per uso professionale (2020)
- Linee guida AGID recanti Regole Tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD (2020)
- Linee Guida AGID “OpenID Connect in SPID” (2021)
- Linee guida AGID per la fruizione dei servizi SPID da parte dei minori (2022)
- Linee guida AGID recanti le regole tecniche dei gestori di attributi qualificati (2022)

CIE

Riferimenti normativi nazionali:

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

Riferimenti normativi europei:

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

NoiPA

Riferimenti normativi nazionali:

- Legge 27 dicembre 2006, n. 296 “Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato” (legge finanziaria 2007) art. 1 commi 446 e 447
- Legge 23 dicembre 2009, n. 191 “Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato” (legge finanziaria 2010) art. 2, comma 197
- Decreto-legge 6 luglio 2011, n. 98, convertito con modificazioni dalla L. 15 luglio 2011, n. 11 “Disposizioni urgenti per la stabilizzazione finanziaria”
- Legge 19 giugno 2019, n. 56 “Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo”
- Decreto del Ministro dell'Economia e delle Finanze 31 ottobre 2002 “Modifiche delle norme sull'articolazione organizzativa del Dipartimento per le politiche di sviluppo e di coesione del Ministero dell’Economia e delle Finanze”
- Decreto del Ministro dell'Economia e delle Finanze 6 luglio 2012 “Contenuti e modalità di attivazione dei servizi in materia stipendiale erogati dal Ministero dell'Economia e delle Finanze”

FSE

Riferimenti normativi nazionali:

- Decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla Legge 17 dicembre 2012, n. 221 “Ulteriori misure urgenti per la crescita del Paese”
- Decreto del Presidente del Consiglio dei Ministri 29 settembre 2015, n. 178 “Regolamento in materia di fascicolo sanitario elettronico”
- Legge 11 dicembre 2016, n. 232 “Bilancio di previsione dello Stato per l'anno finanziario 2017 e bilancio pluriennale per il triennio 2017-2019”
- Decreto-legge 19 maggio 2020, n. 34, convertito con modificazioni dalla Legge 17 luglio 2020, n. 77 “Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché' di politiche sociali connesse all'emergenza epidemiologica da COVID-19”
- Decreto-legge 28 ottobre 2020, n. 137, convertito con modificazioni dalla Legge 18 dicembre 2020, n. 176 “Ulteriori misure urgenti in materia di tutela della salute, sostegno ai lavoratori e alle imprese, giustizia e sicurezza, connesse all'emergenza epidemiologica da COVID-19”
- Decreto-legge 27 gennaio 2022, n. 4, convertito con modificazioni dalla Legge 28 marzo 2022, n. 25 “Misure urgenti in materia di sostegno alle imprese e agli operatori economici, di lavoro, salute e servizi territoriali, connesse all'emergenza da COVID-19, nonché per il contenimento degli effetti degli aumenti dei prezzi nel settore elettrico”

- Decreto del Ministero dell'Economia e delle Finanze 23 dicembre 2019 "Utilizzo del Fondo per il finanziamento degli investimenti e lo sviluppo infrastrutturale - Fascicolo sanitario elettronico" (Piano di digitalizzazione dei dati e documenti sanitari)
- Decreto del Ministero della Salute 20 maggio 2022 "Adozione delle Linee guida per l'attuazione del Fascicolo sanitario elettronico" pubblicato sulla GU Serie Generale n. 160 11.07.2022
- Decreto del Ministero della Salute 7 settembre 2023 "Fascicolo sanitario elettronico 2.0" Linee Guida per l'attuazione del Fascicolo Sanitario Elettronico (2022)
- Piano Nazionale di Ripresa e Resilienza:
    - M6 - Salute C2 1.3.1 "Rafforzamento dell'infrastruttura tecnologica e degli strumenti per la raccolta, l'elaborazione, l'analisi dei dati e la simulazione (FSE)"

IT-Wallet

Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (CAD), art. 64-quater, come introdotto dal decreto-legge 2 marzo 2024, n. 19, convertito con modificazioni dalla Legge 29 aprile 2024, n. 56, art. 20, comma 1, lettera e), "Ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR)".

Riferimenti normativi europei:

- Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

Obiettivi e risultati attesi

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

RA4.1.1 - Incremento dei servizi sulla piattaforma pagoPA

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA aderenti a **pagoPA** assicurano l'attivazione di nuovi servizi in linea con i target sopra descritti e secondo le modalità attuative definite nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR) - **CAP4.PA.01**	Dicembre 2026	Dicembre 2026

RA4.1.2 - Incremento dei servizi sulla Piattaforma IO (l'App dei servizi pubblici)

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA aderenti a **App IO** assicurano l'attivazione di nuovi servizi in linea con i target sopra descritti e secondo le modalità attuative definite nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR) - **CAP4.PA.02**	Dicembre 2026	Dicembre 2026

RA4.1.4 - Incremento dell'adozione e dell'utilizzo di SPID e CIE da parte delle Pubbliche Amministrazioni

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA e i gestori di pubblici servizi proseguono il percorso di adesione a SPID e CIE, dismettendo le altre modalità di autenticazione associate ai propri servizi online e integrando lo SPID uso professionale per i servizi diretti a professionisti e imprese - **CAP4.PA.04**	ATTUALMENTE VIGENTE	ATTUALMENTE VIGENTE
Le PA e i gestori di pubblici servizi interessati cessano il rilascio di credenziali proprietarie a cittadini dotabili di SPID e/o CIE - **CAP4.PA.05**	ATTUALMENTE VIGENTE	ATTUALMENTE VIGENTE

Le PA e i gestori di pubblici servizi interessati adottano lo SPID e la CIE *by default*: le nuove applicazioni devono nascere SPID e CIE-*only* a meno che non ci siano vincoli normativi o tecnologici, se dedicate a soggetti dotabili di SPID o CIE. Le PA che intendono adottare lo SPID di livello 2 e 3 devono anche adottare il "*Login with eIDAS*" per l'accesso transfrontaliero ai propri servizi - **CAP4.PA.06**	ATTUALMENTE VIGENTE	ATTUALMENTE VIGENTE
Le PA devono adeguarsi alle evoluzioni previste dall'ecosistema SPID (tra cui OpenID Connect, uso professionale, *Attribuite Authorities*, servizi per i minori e gestione degli attributi qualificati) - **CAP4.PA.07**	ATTUALMENTE VIGENTE	ATTUALMENTE VIGENTE

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

RA4.3.1 - Incremento del numero di basi dati di interesse nazionale conformi alle regole tecniche

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA interessate avanzano la richiesta di inserimento delle proprie basi di dati nell'elenco di Basi di dati di interesse nazionale gestito da AgID secondo il processo definito - **CAP4.PA.23**	Da gennaio 2026	Da gennaio 2026

Capitolo 5 – Dati e Intelligenza Artificiale

Open Data e Data governance

Il Piano Triennale dedica particolare attenzione a due tematiche fondamentali per la trasformazione digitale della pubblica amministrazione italiana: ***Open Data*** e ***Data Governance***. Questi due ambiti sono strategici per migliorare l'efficacia, la trasparenza e l'interoperabilità dei dati pubblici, fondamentali per il buon funzionamento dei servizi pubblici e per la creazione di valore economico e sociale.

L'***Open Data*** è visto come un catalizzatore per l'innovazione, la trasparenza e la partecipazione civica. Il Piano Triennale stabilisce le linee guida per promuovere la diffusione dei dati pubblici in formati aperti con l'obiettivo di favorire l'accesso, l'utilizzo e la condivisione dei dati per sviluppare applicazioni e servizi innovativi.

Gli obiettivi del Piano Triennale, in tema di Open Data sono:

- **Rendere i dati pubblici più accessibili**. L'AGID intende aumentare la disponibilità dei dati pubblici attraverso il portale dati.gov.it e altre piattaforme di pubblicazione dei dati, mirando ad espandere il numero di dataset disponibili come Open Data. Ciò favorirà l'accesso a informazioni rilevanti per cittadini, aziende e enti pubblici.
- **Migliorare la qualità e l'interoperabilità dei dati**. I dati devono essere di alta qualità, facili da comprendere e interoperabili tra i diversi enti pubblici e sistemi, non solo da un punto di vista tecnico ma anche semantico. Per questo, il Piano prevede l'adozione di formati aperti, standard comuni e metadati che facilitino il riutilizzo dei dati.
- **Promuovere il riutilizzo dei dati**. Un altro obiettivo del Piano è incentivare l'uso dei dati da parte di terzi, come aziende, ricercatori e startup, al fine di sviluppare nuovi servizi e prodotti, stimolando così l'economia digitale e l'innovazione.
- **Garantire la sostenibilità degli Open Data**. Le amministrazioni pubbliche sono chiamate a pianificare il loro impegno continuo nell'apertura dei dati, adottando politiche che assicurino la sostenibilità nel lungo periodo (sia in termini finanziari che organizzativi).

L'IZSLT, come istituto di ricerca e controllo sanitario, ha a disposizione una grande quantità di dati scientifici e sanitari che potrebbero beneficiare di un approccio Open Data. Per rendere disponibili i propri dati all'esterno, adeguandosi agli standard di interoperabilità definiti dal Piano Triennale, l'IZSLT deve adottare formati aperti (ad esempio, CSV, XML, JSON) per la pubblicazione dei dati che facilitino l'accesso e l'uso da parte di ricercatori, professionisti sanitari e cittadini.

Questi dati potrebbero essere utilizzati per progetti di ricerca collaborativa con altre istituzioni, università, e organizzazioni pubbliche e private, contribuendo così a una maggiore trasparenza e a un uso più ampio dei dati per finalità di ricerca e di sviluppo di politiche sanitarie.

Il processo di pubblicazione dei dati deve seguire le seguenti fasi, così come indicato nelle Linee guida AGID:

1. Identificazione: individuazione dei dati da pubblicare, analisi dei vincoli, definizione delle priorità e del percorso di apertura.
2. Analisi: valutazione della qualità dei dati, bonifica e analisi dei processi di produzione.
3. Arricchimento: creazione di **vocabolari controllati** (elenchi di termini predefiniti utilizzati per garantire la coerenza nella descrizione dei dati), ontologie (insieme di concetti e delle relazioni tra di essi), **mashup** (applicazione web che combina dati o funzionalità provenienti da più fonti per creare nuovi servizi) e **LOD** (**Linking Open Data**: pubblicare dati strutturati in modo che possano essere collegati e utilizzati da altre font).
4. Modellazione e documentazione: definizione degli schemi e dei modelli dei dati, definizione delle modalità di conservazione e storicizzazione.
5. Validazione: verifica della qualità dei dati.
6. Pubblicazione: metadatizzazione, definizione delle politiche di accesso e licenza, modalità di pubblicazione.

La **Data Governance** è il processo di gestione e organizzazione dei dati pubblici, per garantire che siano sicuri, accessibili ed utilizzabili in modo efficace e conforme alle normative vigenti. Il Piano promuove un **modello di *governance* centralizzato**, in cui le amministrazioni pubbliche cooperano e condividono i dati in modo strutturato. Per far questo, l'obiettivo fondamentale è migliorare la **qualità dei dati** attraverso l'adozione di azioni atte a garantire l'accuratezza, la completezza e la chiarezza dei dati, al fine di supportare decisioni informate e politiche pubbliche efficaci.

Un ruolo fondamentale nell'ambito della gestione della Data Governance è svolto dal RTD, che attraverso la collaborazione di un Gruppo di Lavoro, ha ò la responsabilità di pianificare e implementare il processo di apertura dei dati. In questo contesto dovranno essere coinvolti referenti tematici delle singole unità organizzative, che gestiscono e trattano i dati nelle rispettive aree. La sua responsabilità si estende anche al coordinamento e al raccordo con figure cruciali come i responsabili della conservazione, della trasparenza, della protezione dei dati e della sicurezza. Infatti Il Piano Triennale stabilisce che la *governance* dei dati deve rispettare rigorosamente la normativa sulla privacy, in particolare il **GDPR** (Regolamento generale sulla protezione dei dati), per proteggere i dati sensibili e garantire che vengano trattati in modo sicuro e trasparente.

L’AGID fungerà da coordinatore nazionale, stabilendo le linee guida e gli standard a cui i diversi enti della PA devono attenersi, consentendo così una gestione più integrata e una comunicazione fluida tra i sistemi.

Contesto normativo

Riferimenti normativi nazionali:

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

- Linee Guida AGID per l'implementazione della specifica GeoDCAT-AP (2017)80
- Linee Guida AGID recanti regole tecniche per la definizione e l'aggiornamento del contenuto del Repertorio Nazionale dei Dati Territoriali (2022)
- Linee Guida AGID recanti regole tecniche per l'attuazione del decreto legislativo 24 gennaio 2006, n. 36 e s.m.i. relativo all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico adottate con Determinazione AGID n. 183/2023 del 3 agosto 2023
- Manuale RNDT - Guide operative per la compilazione dei metadati RNDT

Riferimenti normativi europei

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

Intelligenza Artificiale per la PA

Nel Piano Triennale, l'**Intelligenza Artificiale (IA)** rappresenta una delle tecnologie centrali per l'ottimizzazione dei processi amministrativi e l'innovazione nella Pubblica Amministrazione. L'adozione dell'IA è vista come uno strumento strategico per rendere la **PA** più **efficiente**, **trasparente**, **intelligente** e **orientata al cittadino**; più precisamente il suo utilizzo consentirebbe di raggiungere i seguenti obiettivi:

1. **Migliorare i Servizi Pubblici per i Cittadini e le Imprese:**
   - **Personalizzazione dei servizi**: per offrire servizi pubblici personalizzati che rispondano in modo più efficace alle esigenze dei cittadini, ad esempio tramite assistenti virtuali o chatbot.
   - **Automazione delle operazioni burocratiche**: per ridurre i tempi di attesa, semplificare la gestione delle pratiche amministrative e migliorare l'esperienza dell'utente.
2. **Aumentare l'Efficienza dei Processi Interni della PA:**
   - **Ottimizzazione dei processi amministrativi**: per migliorare la gestione dei flussi di lavoro interni alla PA, riducendo la **burocrazia** e **snellendo** i procedimenti. Questo include, ad esempio, la gestione automatica dei documenti e la digitalizzazione dei processi.
   - **Gestione dei dati e decisioni basate su dati**: I modelli di IA possono supportare le PA nell'analisi e nella gestione di grandi volumi di dati, migliorando l'efficacia decisionale.
3. **Prevenire la Corruzione e Migliorare la Trasparenza:**
   - **Monitoraggio dei flussi finanziari**: L'IA può essere utilizzata per rilevare anomalie nei dati fiscali, finanziari e amministrativi, contribuendo alla prevenzione della corruzione e migliorando la trasparenza nelle operazioni pubbliche.
   - **Analisi dei dati per la trasparenza**: Le amministrazioni possono utilizzare l'IA per generare report e analisi trasparenti delle proprie attività e per pubblicare dati aperti che siano facilmente accessibili e utilizzabili dai cittadini.
4. **Promuovere l'Innovazione e la Competitività:**
   - **Sostenere la ricerca e l'innovazione**: L'adozione di IA nella PA stimola la creazione di ecosistemi di innovazione in cui università, startup e aziende collaborano per sviluppare nuove soluzioni tecnologiche per il settore pubblico.

- **Supporto alla crescita del mercato digitale**: La PA, attraverso l'uso dell'IA, diventa un motore di crescita per le tecnologie digitali, contribuendo a costruire un mercato innovativo di **servizi digitali pubblici**.

Per promuovere l'adozione dell'IA nella Pubblica Amministrazione, il Piano Triennale prevede delle azioni strategiche:

Creazione di un Ecosistema Nazionale di IA

Il Piano promuove la creazione di un ecosistema nazionale di intelligenza artificiale, che favorisce l'interazione tra PA, università, centri di ricerca e imprese tecnologiche. Le amministrazioni pubbliche sono invitate a collaborare per sviluppare soluzioni basate su IA, condividendo best practices, esperienze e tecnologie.

Infrastrutture e Dati per l'IA

L'intelligenza artificiale si basa su dati di alta qualità. Per questo motivo, il Piano Triennale promuove l'adozione di infrastrutture centralizzate per la gestione dei dati e l'analisi intelligente:

- **Data lake e piattaforme di dati**: Implementazione di sistemi di archiviazione centralizzata dei dati, come i *data lake,* per raccogliere, conservare e rendere accessibili i dati utili all'addestramento dei modelli di IA.
- **Condivisione dei dati**: Promozione della condivisione dei dati tra le amministrazioni pubbliche e il settore privato, nel rispetto della privacy e delle normative di protezione dei dati.

Sviluppo delle Competenze e Formazione

Una delle azioni fondamentali per l'adozione dell'IA è la formazione delle competenze del personale pubblico. Il Piano prevede:

- Formazione continua: Corsi di aggiornamento per i funzionari pubblici, in particolare per i RTD e i referenti delle singole amministrazioni.
- Programmi di formazione specifica sull'IA: Creazione di programmi di formazione incentrati sulle tecniche di IA applicabili al settore pubblico, inclusi machine learning, analisi dei dati, e intelligenza artificiale etica.

Normative e Linee Guida sull'IA

Per favorire un uso etico e responsabile dell'IA, il Piano Triennale stabilisce il rispetto delle normative nazionali e internazionali. In particolare:

- Allineamento con l'**AI Act europeo**: Le amministrazioni pubbliche dovranno conformarsi all'**AI Act**, il regolamento europeo che stabilisce le linee guida per l'uso sicuro e trasparente dell'IA.
- Etica e trasparenza: Le amministrazioni dovranno adottare principi etici per l'uso dell'IA, inclusi la non discriminazione, la trasparenza nei processi decisionali automatizzati e la responsabilità nell'utilizzo delle tecnologie.

Monitoraggio e Valutazione dell'Adozione dell'IA

Il Piano prevede la creazione di sistemi di monitoraggio e valutazione per misurare l'efficacia e l'impatto dell'IA nella PA:

- Indicatori di performance: Sviluppo di indicatori chiari per monitorare l'adozione dell'IA e la qualità dei servizi pubblici.
- Audit e revisione periodica: Le amministrazioni saranno sottoposte a controlli periodici per garantire che le applicazioni di IA siano utilizzate in modo corretto, sicuro e in linea con le normative.

Per l'adozione efficace dell'IA nella Pubblica Amministrazione è essenziale creare e utilizzare **dati di alta qualità**, sviluppare una **governance solida dei dati** e seguire il quadro normativo europeo, come l'**AI Act**, che pone particolare attenzione agli aspetti qualitativi dei set di dati utilizzati per addestrare, convalidare e testare i sistemi di IA (tra cui rappresentatività, pertinenza, completezza e correttezza). La Commissione Europea ha avviato una specifica attività presso il CEN e il CENELEC per definire norme tecniche europee per rispondere a tali esigenze.

Nel Piano Triennale 2026, dati e intelligenza artificiale assumono un ruolo centrale e ampliato.

Gli aggiornamenti più rilevanti riguardano:

- Allineamento alle nuove normative europee: Data Governance Act, AI Act e strategie UE sull'IA.
- Creazione di una governance più strutturata su dati e IA, con nuovi risultati attesi e linee di azione.
- Rafforzamento della qualità dei dati, interoperabilità e sicurezza.
- Promozione dell'uso responsabile dell'IA, supportata da formazione specifica tramite AgID Academy.
- Integrazione con le piattaforme nazionali, tra cui PDND e IT-Wallet.

Il Piano 2026 chiude il triennio 2024–2026 e pone le basi normative, tecnologiche e operative per il nuovo ciclo 2027–2029.

Contesto normativo

Riferimenti normativi europei:

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

Obiettivi e risultati attesi

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

RA5.1.1 – Aumento del numero di dataset aperti di tipo dinamico in coerenza con quanto previsto dalle Linee guida Open Data

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA partecipano, in funzione delle proprie necessità, a interventi di formazione e sensibilizzazione sulle politiche open data - **CAP5.PA.03**	ATTUALMENTE VIGENTE	ATTUALMENTE VIGENTE

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

RA5.4.1 – Linee guida per promuovere l'adozione dell'IA nella Pubblica Amministrazione

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA dovranno rispettare le Linee per promuovere l'adozione dell'IA nella Pubblica Amministrazione - **CAP5.PA.21**	Da dicembre 2025	Da dicembre 2025

RA5.4.2 – Linee guida per il procurement di IA nella Pubblica Amministrazione

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA dovranno rispettare le Linee guida per il procurement di IA nella Pubblica Amministrazione - **CAP5.PA.22**	Da dicembre 2025	Da dicembre 2025

RA5.4.3 - Linee guida per lo sviluppo di applicazioni di IA per la Pubblica Amministrazione

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA dovranno rispettare le Linee guida per lo sviluppo di applicazioni di IA nella Pubblica Amministrazione - **CAP5.PA.23**	Da dicembre 2025	Da dicembre 2025
Le PA trasmettono periodicamente all'AgID i dati fondamentali delle iniziative nell'ambito delle tecnologie di IA - **CAP5.PA.27**	Da luglio 2026	Da luglio 2026

RA5.4.4 - Realizzazione di applicazioni di IA a valenza nazionale

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA adottano le applicazioni di IA a valenza nazionale - **CAP5.PA.24**	Dicembre 2026	Dicembre 2026

5.5 - Dati per l'intelligenza artificiale

RA5.5.1 - Basi di dati nazionali strategiche

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA adottano le basi dati nazionali strategiche - **CAP5.PA.25**	Dicembre 2026	Dicembre 2026

Capitolo 6 – Infrastrutture

Infrastrutture digitali e Cloud

Il "**Cloud Italia**" è una strategia nazionale pubblicata nel settembre 2021 dal Dipartimento per la Trasformazione Digitale e dall'Agenzia per la Cybersicurezza Nazionale, mirata a supportare la riorganizzazione e la digitalizzazione delle pubbliche amministrazioni italiane attraverso l'adozione del *cloud computing*. Questa strategia si inserisce nel quadro del PNRR e risponde a obiettivi chiave per la trasformazione digitale della Pubblica Amministrazione.

Gli obiettivi principali di questa strategia sono:

- Autonomia tecnologica del Paese, assicurando un maggiore controllo sulle tecnologie e sui dati.
- Controllo sui dati sensibili e la sicurezza delle informazioni trattate dalle pubbliche amministrazioni.
- Resilienza dei servizi digitali, migliorando la capacità delle infrastrutture pubbliche di fronteggiare attacchi e guasti.

Il principio *"cloud first"*, promuove l'adozione delle tecnologie **cloud** da parte della **Pubblica Amministrazione** come opzione prioritaria, in modo sicuro, controllato e conforme alle normative di **protezione della privacy** e alle raccomandazioni delle istituzioni europee e nazionali**.** Questo principio si basa sui seguenti punti:

1. **Adozione prioritaria del cloud.** Le pubbliche amministrazioni, quando definiscono nuovi progetti o sviluppano nuovi servizi, devono valutare prima l'adozione del *cloud* rispetto ad altre tecnologie.
2. **Obbligo di valutazione.** Ogni amministrazione è obbligata a effettuare una valutazione obbligatoria sull'adozione del *cloud*. Questa valutazione deve considerare se la tecnologia cloud è adatta per il progetto o servizio da sviluppare.
3. **Evoluzione tecnologica e impatto globale.** Il *cloud* è considerato una delle evoluzioni tecnologiche più significative degli ultimi anni e sta rivoluzionando tutti i sistemi informativi a livello mondiale, quindi la sua adozione rappresenta un passo fondamentale per l'aggiornamento delle infrastrutture digitali della Pubblica Amministrazione.
4. **Sicurezza e privacy.** L'adozione del *cloud* deve avvenire in modo sicuro, rispettando rigorosi standard di protezione dei dati personali e delle informazioni sensibili. Questo allineamento ai principi di sicurezza e privacy è fondamentale per garantire la protezione dei dati e la fiducia degli utenti.

L'attuazione della **Strategia Cloud Italia** e dell'articolo 33-septies del Decreto-Legge n. 179/2021 ha portato alla creazione del Polo Strategico Nazionale (PSN), un'infrastruttura promossa dal Dipartimento per la Trasformazione Digitale. Questo Polo, insieme ad altre infrastrutture digitali qualificate e sicure, offre alle amministrazioni le soluzioni tecnologiche necessarie per supportare il processo di migrazione al cloud.

Il Regolamento attuativo dell'art. 33-septies ha fissato il termine del 28 febbraio 2023 per la presentazione da parte delle amministrazioni dei piani di migrazione verso il *cloud*. Questi piani definiscono le modalità in cui le amministrazioni migreranno dati, servizi e applicativi sul *cloud*, nel rispetto della normativa e della sicurezza.

Dopo la presentazione dei piani, le amministrazioni sono tenute a **gestire il trasferimento** dei loro dati, servizi e applicativi al cloud, un processo che deve essere **concluso entro il 30 giugno 2026**. La migrazione deve essere eseguita in modo gestito e coordinato, con l'obiettivo di modernizzare l'infrastruttura IT della pubblica amministrazione, ridurre il debito tecnologico e migliorare l'efficienza dei servizi pubblici. Per realizzare al meglio il proprio piano di migrazione, le amministrazioni possono far riferimento al sito cloud.italia.it.

La migrazione al *cloud* offre vantaggi economici e operativi, ma richiede una gestione attenta delle sfide legate alla gestione dei costi operativi correnti e alla complessità dell'integrazione dei servizi digitali. Con l'aumento dei servizi *cloud* da molti fornitori diversi, la gestione del parco applicativo e l'integrazione tra i vari sistemi di uno stesso ente, diventano più difficili, compromettendo l'interoperabilità tra enti e la gestione corretta dei dati. È necessaria, quindi, una transizione verso architetture a micro-servizi per garantire una gestione più flessibile e scalabile dei servizi digitali. Un corretto approccio alla gestione del *cloud* richiede una pianificazione accurata sia da un punto di vista contrattuale che tecnologico.

Le infrastrutture digitali devono essere affidabili, sicure, energeticamente efficienti ed economicamente sostenibili, per garantire l'erogazione continua di servizi essenziali. L'evoluzione tecnologica, però, introduce nuovi rischi, specialmente legati alla protezione dei dati personali e alla sicurezza dei sistemi informativi. Molte delle infrastrutture della Pubblica Amministrazione sono ancora carenti in termini di sicurezza e affidabilità. Questo debito tecnologico può comportare interruzione o indisponibilità dei servizi pubblici ed attacchi cyber che potrebbero comportare accessi illegittimi a dati sensibili o la perdita e alterazione dei dati stessi. Per questo motivo che il miglioramento dell'efficienza tecnologica deve andare di pari passo con il rafforzamento della sicurezza delle reti e dei sistemi informativi utilizzati dalla PA.

Lo scenario delineato pone l'esigenza immediata di attuare un percorso di razionalizzazione delle infrastrutture per garantire la sicurezza dei servizi oggi erogati tramite infrastrutture classificate come gruppo B, mediante la migrazione degli stessi verso ***data center*** più sicuri e verso infrastrutture e servizi cloud qualificati, ovvero conformi a standard di qualità, sicurezza, performance e scalabilità, portabilità e interoperabilità.

Per abilitare le applicazioni esistenti al cloud, le amministrazioni dovranno intraprendere interventi come:

- **Rearchitect**: Ripensare l'architettura delle applicazioni per renderle compatibili con il cloud.
- **Replatform**: Riadattare le applicazioni a una nuova piattaforma tecnologica, ottimizzando l'uso del cloud.
- **Repurchase**: Acquistare nuove soluzioni software, magari già native del cloud, invece di mantenere le applicazioni legacy.

Inoltre, il *cloud* richiede un'evoluzione verso architetture a micro-servizi, che si caratterizzano per i seguenti aspetti:

- Autonomia: Ogni micro-servizio è indipendente, gestisce i propri dati e non dipende da altri servizi (self-contained).
- Comunicazione via API: I micro-servizi comunicano con l'esterno utilizzando API o web service senza dipendenza dallo stato precedente (stateless).
- Indipendenza tecnologica: Ogni micro-servizio può essere sviluppato utilizzando differenti linguaggi e tecnologie senza compromettere l'interoperabilità.
- Deployment indipendente: Ogni servizio può essere dispiegato e gestito autonomamente, consentendo maggiore flessibilità e scalabilità.
- Orientamento al business: I micro-servizi devono essere progettati per supportare attività amministrative specifiche, non solo con scopi tecnologici. Ogni micro-servizio deve rispondere a necessità di business legate ai procedimenti amministrativi.

L'Ufficio del RTD ha il compito di **pianificare e coordinare** la migrazione verso il cloud, considerando sia gli aspetti tecnici che quelli organizzativi ed assicurandosi che sia allineato con le strategie dell'ente e con l'adozione di nuovi modelli operativi.

La gestione dei servizi in cloud non si limita alla fase di migrazione, ma deve coprire l'intero ciclo di vita dei servizi. È necessario, a tal fine, strutturare strumenti e presidi organizzativi, includendo la pianificazione, il monitoraggio e l'ottimizzazione dei costi operativi (OPEX) relativi ai servizi in cloud. Anche in questo caso, la gestione può essere singola o associata tra diverse amministrazioni.

Nel Piano Triennale 2026, i contenuti legati al cloud vengono aggiornati per rispecchiare l'evoluzione della normativa europea e nazionale.
L'adeguamento del tema *"cloud"* alla normativa di settore comporta:

- **Allineamento alla disciplina UE sulla sovranità digitale e sicurezza** (protezione dei dati e controllo giurisdizionale).
- **Riaffermazione del principio cloud first come obbligo normativo** con valutazione obbligatoria del cloud per ogni nuovo progetto.
- **Integrazione con il nuovo Codice dei Contratti Pubblici,** che aggiorna le regole di acquisto dei servizi cloud.
- **Recepimento della Strategia Cloud Italia (DL 179/2012)** e dei meccanismi di classificazione/qualificazione dei servizi cloud.
- **Maggiore ruolo dell'ACN** nelle verifiche di sicurezza e qualificazione.
- **Transizione da adempimenti puntuali a governance continua**, con collegamento strutturale tra cloud, interoperabilità e sicurezza.

Contesto normativo

Riferimenti normativi nazionali:

- Decreto legislativo 7 marzo 2005, n. 82, "Codice dell'amministrazione digitale", articoli. 8-bis e 73;
- Decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, "Ulteriori misure urgenti per la crescita del Paese", articolo 33-septies;
- Decreto legislativo 18 maggio 2018, n. 65, "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione"
- Decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla L. 18 novembre 2019, n. 133 "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica"
- Decreto-legge 17 marzo 2020, n. 18, convertito con modificazioni dalla Legge 24 aprile 2020, n. 27 "Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19", art. 75;
- Decreto-legge 16 luglio 2020, n. 76, convertito con modificazioni dalla Legge 11 settembre 2020, n. 120 "Misure urgenti per la semplificazione e l'innovazione digitale", art. 35;

- Decreto-legge 31 maggio 2021, n. 77, convertito con modificazioni dalla Legge 29 luglio 2021, n. 108 “Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure”;
- Decreto-legge 14 giugno 2021, n. 82, convertito con modificazioni dalla Legge 4 agosto 2021, n. 109 “Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale”
- Circolare AGID n. 1/2019, del 14 giugno 2019 - Censimento del patrimonio ICT delle Pubbliche Amministrazioni e classificazione delle infrastrutture idonee all’uso da parte dei Poli Strategici Nazionali;
- Strategia italiana per la banda ultra-larga (2021);
- Strategia Cloud Italia (2021);
- Regolamento AGID, di cui all’articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la Pubblica Amministrazione e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la Pubblica Amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la Pubblica Amministrazione (2021);
- Determinazioni ACN in attuazione al precedente Regolamento n. 306/2022 (con allegato) su e n. 307/2022 (con allegato);
- Decreti direttoriali ACN prot. N. 29 del 2 gennaio 2023, n. 5489 dell’8 febbraio 2023 e n. 20610 del 28 luglio 2023;

- Piano Nazionale di Ripresa e Resilienza:
    - Investimento 1.1: “Infrastrutture digitali”
    - Investimento 1.2: “Abilitazione e facilitazione migrazione al cloud”

Riferimenti normativi europei:

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

Obiettivi e risultati attesi

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

RA6.1.1 - Numero di amministrazioni migrate

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA avviano il percorso di migrazione verso il cloud in coerenza con quanto previsto dalla Strategia Cloud Italia – **CAP6.PA.03**	ATTUALMENTE VIGENTE	ATTUALMENTE VIGENTE
Le PA continuano ad applicare il principio cloud first e ad acquisire servizi cloud solo se qualificati – **CAP6.PA.04**	ATTUALMENTE VIGENTE	ATTUALMENTE VIGENTE
Le PA aggiornano l'elenco e la classificazione dei dati e dei servizi digitali in presenza di dati e servizi ulteriori rispetto a quelli già oggetto di conferimento e classificazione come indicato nel Regolamento e di conseguenza aggiornano, ove necessario, anche il piano di migrazione – **CAP6.PA.05**	ATTUALMENTE VIGENTE	ATTUALMENTE VIGENTE
Le amministrazioni concludono la migrazione in coerenza con il piano di migrazione trasmesso ai sensi del Regolamento cloud e, ove richiesto dal Dipartimento per la Trasformazione Digitale o da AgID, trasmettono le informazioni necessarie per verificare il completamento della migrazione - **CAP6.PA.10**	Giugno 2026	Giugno 2026

6.2 - Garantire alle amministrazioni la disponibilità della connettività SPC

RA6.2.1 - Rete di connettività

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Sulla base delle proprie esigenze, le pubbliche amministrazioni iniziano la fase di migrazione della loro infrastruttura di rete utilizzando i servizi resi disponibili dalla nuova gara di connettività SPC – **CAP6.PA.11**	Da marzo 2026	Da marzo 2026

Capitolo 7 – Sicurezza Informatica

L'evoluzione delle tecnologie digitali ha reso possibile un miglioramento significativo nella gestione dei procedimenti amministrativi, con l'obiettivo di renderli più efficaci, efficienti ed economici. Questo ha spinto molte amministrazioni verso la digitalizzazione, che è ormai considerata una tappa obbligata per modernizzare e semplificare i servizi offerti ai cittadini e alle imprese. Con l'adozione di queste tecnologie, emerge, però, la crescente minaccia di attacchi informatici.

Gli attacchi cyber possono avere conseguenze devastanti, non solo per la sicurezza dei dati, ma anche per il **funzionamento dei servizi pubblici**. La protezione delle **infrastrutture critiche** e dei sistemi informativi che gestiscono questi servizi è quindi essenziale. Un attacco riuscito potrebbe compromettere la gestione di risorse fondamentali come l'energia, i trasporti, la sanità, l'acqua, e altre funzioni vitali per la vita quotidiana dei cittadini.

La **sicurezza dell'ecosistema digitale** è considerata una priorità cruciale per il corretto funzionamento del sistema Paese. In particolare, la protezione dei **beni ICT** (Information and Communication Technology), che supportano i servizi e le funzioni essenziali dello Stato, è fondamentale. Questi beni, che includono infrastrutture come server, reti, applicazioni e dispositivi, sono vulnerabili agli attacchi cyber. La crescente digitalizzazione ha reso questi beni tra i **bersagli preferiti** degli attacchi informatici, come dimostrano i recenti **rapporti di settore**.

In risposta a queste sfide, l'Italia ha adottato una serie di iniziative per rafforzare la propria capacità di difendersi dagli attacchi informatici, tra cui l'istituzione della Agenzia per la **Cybersicurezza Nazionale** (**ACN**). La creazione di questa agenzia è stata formalizzata dal Decreto-legge 14 giugno 2021, n. 82, con l'obiettivo di coordinare e gestire la sicurezza cibernetica a livello nazionale.

L'**ACN** ha il compito di sviluppare le capacità cyber nazionali, fornendo un'unica voce istituzionale per la direzione e l'azione in ambito di cybersicurezza. Ciò include la redazione e l'implementazione della **Strategia Nazionale di Cybersicurezza**, un documento fondamentale che definisce le linee guida per la protezione delle infrastrutture digitali e la gestione dei rischi informatici.

Gli **obiettivi** del Piano Triennale sono focalizzati su una serie di azioni chiave per migliorare la sicurezza informatica della Pubblica Amministrazione, in coerenza con gli interventi realizzati dall'ACN. I principali ambiti di intervento identificati nel Piano sono i seguenti:

- **Modelli di gestione centralizzati della cybersicurezza**: sviluppare modelli di gestione centralizzati della cybersicurezza, che consentano un controllo e una supervisione unificata della sicurezza delle reti, dei sistemi e dei dati in tutto il sistema pubblico. L'ACN, attraverso l'introduzione di linee guida, mira a centralizzare la gestione dei rischi e a migliorare l'efficienza nelle azioni di difesa.

- **Gestione e mitigazione del rischio cyber:** definizione di processi chiari per la gestione e la mitigazione dei rischi cyber, sia a livello interno di ogni singola amministrazione che nei confronti di terze parti coinvolte nei **processi IT**. La gestione del rischio deve essere strutturata in modo da ridurre al minimo le vulnerabilità legate a software, dispositivi e comunicazioni. I rischi derivanti dalle terze parti, come i fornitori di servizi IT e cloud, sono una preoccupazione crescente. Il Piano prevede quindi l'adozione di politiche per garantire che anche i partner esterni rispettino standard di sicurezza adeguati. Inoltre, la gestione del rischio non si limita alla protezione dai singoli attacchi informatici, ma riguarda anche la capacità di reazione rapida e la resilienza del sistema in caso di incidenti.

- **Miglioramento della cultura cyber nelle amministrazioni:** sensibilizzazione e la formazione dei dipendenti pubblici in tema di cybersicurezza. La cultura cyber è essenziale per prevenire errori umani e per garantire che ogni membro della Pubblica Amministrazione sia in grado di riconoscere e affrontare le minacce informatiche in modo efficace. Il Piano prevede attività di formazione continua per il personale delle PA, che si estenda a tutti i livelli dell'amministrazione.

- **Piattaforme e servizi per il contrasto dei rischi cyber**: l'AGID metterà a disposizione delle pubbliche amministrazioni una serie di piattaforme e servizi per il monitoraggio, l'analisi e il contrasto dei rischi informatici legati al patrimonio ICT delle amministrazioni. Questi servizi saranno erogati tramite il **CERT** (*Computer Emergency Response Team*), che fornirà supporto tecnico e operativo alle amministrazioni, per la gestione degli incidenti di sicurezza, la prevenzione delle minacce e l'analisi delle vulnerabilità. La creazione di una rete di **incident response** a livello nazionale è fondamentale per garantire una rapida reazione alle emergenze e per minimizzare i danni derivanti da attacchi informatici.

Contesto normativo

Riferimenti normativi nazionali:

- Decreto legislativo 7 marzo 2005, n. 82, "Codice dell'amministrazione digitale", articolo 51105
- Decreto del Presidente del Consiglio dei ministri 17 febbraio 2017, "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali"
- Decreto Legislativo 18 maggio 2018, n. 65, "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione"
- Decreto del Presidente del Consiglio dei ministri 8 agosto 2019, "Disposizioni sull'organizzazione e il funzionamento del *computer security incident response* team - CSIRT italiano"
- Decreto-legge 21 settembre 2019, n. 105, "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica"
- Decreto-legge 19 luglio 2020, n. 76, "Misure urgenti per la semplificazione e l'innovazione digitale"
- Decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, "Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misura volte a garantire elevati livelli di sicurezza";
- Decreto-legge 14 giugno 2021 n. 82, "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la Cybersicurezza Nazionale";
- Decreto legislativo 8 novembre 2021 n. 207, "Attuazione della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche (rifusione)";
- Decreto-legge 21 marzo 2022 n. 21, "Misure urgenti per contrastare gli effetti economici e umanitari della crisi Ucraina", articoli 27, 28 e 29;
- Decreto del Presidente del Consiglio dei ministri 17 maggio 2022, Adozione della Strategia nazionale di cybersicurezza 2022-2026 e del relativo Piano di implementazione 2022-2026;
- Misure minime di sicurezza ICT per le pubbliche amministrazioni, 18 marzo 2017;
- Linee guida sulla sicurezza nel procurement ICT, del mese di aprile 2020;
- Strategia Cloud Italia, adottata a settembre 2021
- Piano Nazionale di Ripresa e Resilienza - Investimento 1.5: "Cybersecurity";

Riferimenti normativi europei:

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

Obiettivi e risultati attesi

7.1 - Adottare una governance della cybersicurezza diffusa nella PA

RA7.1.1 - Identificazione di un modello, con ruoli e responsabilità, di gestione della cybersicurezza

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le singole PA definiscono il modello unitario, assicurando un coordinamento centralizzato a livello dell'istituzione, di governance della cybersicurezza - **CAP7.PA.01**	Da settembre 2024	Da giugno 2025
Le PA adottano un modello di governance della cybersicurezza - **CAP7.PA.02**	Da dicembre 2024	Da giugno 2025
Le PA nominano i Responsabili della cybersicurezza e delle loro strutture organizzative di supporto - **CAP7.PA.03**	Da dicembre 2024	Da giugno 2025

RA7.1.2 - Definizione del framework documentale a supporto della gestione cyber

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA formalizzano i processi e le procedure inerenti alla gestione della cybersicurezza - *CAP7.PA.04*	Da dicembre 2024	Da giugno 2025

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

RA7.2.1 - Definizione del framework documentale a supporto del processo di approvvigionamento IT

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA definiscono e approvano i requisiti di sicurezza relativi al processo di approvvigionamento IT - **CAP7.PA.05**	Da giugno 2024	Da giugno 2024
Le PA definiscono e promuovono i processi di gestione del rischio sui fornitori e terze parti IT, la contrattualistica per i fornitori e le terze parti IT, comprensive dei requisiti di sicurezza da rispettare - **CAP7.PA.06**	Da dicembre 2024	Da dicembre 2024

RA7.2.2 - Definizione delle modalità di monitoraggio del processo di approvvigionamento IT

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA realizzano le attività di controllo definite nel Piano di audit e verifica verso i fornitori e terze parti IT - **CAP7.PA.07**	Da dicembre 2025	Da dicembre 2025

7.3 - Gestione e mitigazione del rischio cyber

RA7.3.1 - Definizione del framework per la gestione del rischio cyber

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA definiscono e formalizzano il processo di cyber risk management e security by design, coerentemente con gli strumenti messi a disposizione da ACN - **CAP7.PA.08**	Da dicembre 2024	Da giugno 2025
Le PA promuovono il censimento dei dati e servizi della PA, identificandone la rilevanza e quindi le modalità per garantirne la continuità operativa - **CAP7.PA.09**	Dicembre 2025	Dicembre 2025
Le PA realizzano o acquisiscono gli strumenti atti alla messa in sicurezza dell'integrità, confidenzialità e disponibilità dei servizi e dei dati, come definito dalle relative procedure - **CAP7.PA.10**	Dicembre 2025	Dicembre 2025
Le PA integrano le attività di monitoraggio del rischio cyber, come definito dal relativo Piano, nelle normali attività di progettazione, analisi, conduzione e dismissione di applicativi e sistemi informativi - **CAP7.PA.11**	Dicembre 2026	Dicembre 2026

RA7.3.2 - Definizione delle modalità di monitoraggio del rischio cyber

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA integrano le attività di monitoraggio del rischio cyber, come definito dal relativo Piano, nelle normali attività di progettazione, analisi, conduzione e dismissione di applicativi e sistemi informativi - **CAP7.PA.12**	Da dicembre 2025	Da dicembre 2025

7.4 - Potenziare le modalità di prevenzione e gestione degli incidenti informatici

RA7.4.1 - Definizione del framework documentale relativo alla gestione degli incidenti

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA definiscono i presidi per la gestione degli eventi di sicurezza, formalizzandone i processi e le procedure - **CAP7.PA.13**	Da giugno 2024	Da dicembre 2025
Le PA formalizzano ruoli, responsabilità e processi, nonché le capacità tecnologiche a supporto della prevenzione e gestione degli incidenti informatici - **CAP7.PA.14**	Da dicembre 2024	Da dicembre 2025

RA7.4.2 - Definizione delle modalità di verifica e aggiornamento dei piani di risposta agli incidenti

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA definiscono le modalità di verifica dei Piani di risposta a seguito di incidenti informatici - **CAP7.PA.15**	Da dicembre 2024	Da dicembre 2024
Le PA definiscono le modalità di aggiornamento dei Piani di risposta e ripristino a seguito dell'accadimento di incidenti informatici - **CAP7.PA.16**	Da dicembre 2025	Da dicembre 2025

7.5 - Implementare attività strutturate di sensibilizzazione cyber del personale

RA7.5.1 - Definizione dei piani di formazione in ambito cyber

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA promuovono l'accesso e l'utilizzo di attività strutturate di sensibilizzazione e formazione in ambito cybersicurezza - **CAP7.PA.17**	Da giugno 2024	Da giugno 2024
Le PA definiscono piani di formazione inerenti alla cybersecurity, diversificati per ruoli, posizioni organizzative e attività delle risorse dell'organizzazione - **CAP7.PA.18**	Da dicembre 2024	Da dicembre 2024

RA7.5.2 - Adozione di strumenti atti alla formazione in ambito cyber

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA realizzano iniziative per verificare e migliorare la consapevolezza del proprio personale - **CAP7.PA.19**	Da dicembre 2025	Da dicembre 2025

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

RA7.6.2 - Fornitura di strumenti funzionali all'esecuzione dei piani di autovalutazione dei sistemi esposti

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA dovranno usufruire degli strumenti per la gestione dei rischi cyber messi a disposizione dal CERT-AGID - **CAP7.PA.21**	Da ottobre 2024	Da giugno 2025

RA7.6.3 - Supporto formativo e informativo rivolto alle PA e in particolare agli RTD per l'aumento del livello di consapevolezza delle minacce cyber

LINEE DI AZIONE	SCADENZA PT	SCADENZA IZSLT
Le PA, sulla base delle proprie esigenze, partecipano ai corsi di formazione base ed avanzato erogati dal CERT-AGID - **CAP7.PA.22**	Dicembre 2025	Dicembre 2025

APPENDICE – GLOSSARIO

- AgID: Agenzia per l'Italia Digitale è l'agenzia tecnica della Presidenza del Consiglio col compito di garantire la realizzazione degli obiettivi dell'Agenda digitale e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione.
- ANAC: Autorità nazionale anticorruzione.
- AOO: Area Organizzativa Omogenea.
- API: API (Application Programming Interface) è un insieme di definizioni e protocolli che consentono a software diversi di comunicare tra loro.
- API-first: Principio per cui i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e attraverso processi digitali collettivi.
- BDNCP: Banca dati nazionale dei contratti pubblici, istituita presso ANAC.
- CAD: Codice Amministrazione Digitale è un testo unico che riunisce e organizza le norme in merito all'informatizzazione della PA nei rapporti con cittadini e imprese.
- CITD: Comitato Interministeriale per la Trasformazione Digitale promuove, indirizza, coordina l'azione del Governo nelle materie dell'innovazione tecnologica, dell'attuazione dell'agenda digitale italiana ed europea, della strategia italiana per la banda ultra-larga, della digitalizzazione delle pubbliche amministrazioni e delle imprese, nonché della trasformazione, crescita e transizione digitale del Paese.
- Cloud first: Strategia che promuove l'utilizzo dei servizi cloud come prima scelta per la gestione dei dati e dei processi aziendali.
- Consip SpA: centrale di acquisto nazionale che offre strumenti e soluzioni di e-procurement per la digitalizzazione degli acquisti di amministrazioni e imprese.
- Decennio Digitale: Insieme di regole e principi guida dettati dalla Commissione Europea per guidare i Paesi Membri nel raggiungimento degli obiettivi fissati per il Decennio Digitale 2020 - 2030.
- Digital & mobile first: Principio per cui le pubbliche amministrazioni devono erogare i propri servizi pubblici in digitale e devono essere fruibili su dispositivi mobili.
- Digital identity only: Principio per cui le pubbliche amministrazioni devono erogare i propri servizi pubblici in digitale e devono essere fruibili su dispositivi mobili.
- DDT: Documento di trasporto (digitale).
- Gold plating: Fenomeno in cui un progetto viene implementato con caratteristiche o dettagli aggiuntivi che vanno oltre i requisiti richiesti, senza alcuna reale necessità o beneficio tangibile.
- Governo come Piattaforma: Approccio strategico nella progettazione e nell'erogazione dei Servizi Pubblici in cui il governo agisce come una piattaforma aperta che facilita l'erogazione di servizi da parte di entità pubbliche e private.
- ICT: Information and Communication Technology (Tecnologie dell'Informazione e della Comunicazione).

- Interoperabilità: Rende possibile la collaborazione tra Pubbliche amministrazioni e tra queste e soggetti terzi, per mezzo di soluzioni tecnologiche che assicurano l'interazione e lo scambio di informazioni senza vincoli sulle implementazioni, evitando integrazioni ad hoc.
- Lock-in: Fenomeno che si verifica quando l'amministrazione non può cambiare facilmente fornitore alla scadenza del periodo contrattuale perché non sono disponibili le informazioni essenziali sul sistema che consentirebbero a un nuovo fornitore di subentrare al precedente in modo efficiente.
- Once-only: Principio secondo cui l'amministrazione non richiede al cittadino dati e informazioni di cui è già in possesso.
- Open data by design e by default: Principio per cui il patrimonio informativo della Pubblica Amministrazione deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile.
- Openess: Principio per cui le pubbliche amministrazioni devono tenere conto della necessità di prevenire il rischio di lock-in nei propri servizi, prediligere l'utilizzo di software con codice aperto o di e-Service e, nel caso di software sviluppato per loro conto, deve essere reso disponibile il codice sorgente, nonché promuovere l'amministrazione aperta e la condivisione di buone pratiche sia amministrative che tecnologiche.
- PDND: Piattaforma Digitale Nazionale Dati (PDND) è lo strumento che abilita l'interoperabilità dei sistemi informativi degli Enti e dei Gestori di Servizi Pubblici.
- PIAO: Piano Integrato di Attività e Organizzazione è un documento unico di programmazione e governance che va a sostituire tutti i programmi che fino al 2022 le Pubbliche Amministrazioni erano tenute a predisporre, tra cui i piani della performance, del lavoro agile (POLA) e dell'anticorruzione.
- PNC: Piano Nazionale per gli investimenti complementari è il piano nazionale di investimenti finalizzato a integrare gli interventi del PNRR tramite risorse nazionali.
- PNRR: Piano Nazionale di Ripresa e Resilienza è il piano nazionale di investimenti finalizzato allo sviluppo sostenibile e al rilancio dell'economia tramite i fondi europei del Next Generation EU.
- Privacy by design e by default: Principio per cui i servizi pubblici devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali.
- RTD: Responsabile per la Trasformazione Digitale è il dirigente all'interno della Pubblica Amministrazione che garantisce operativamente la trasformazione digitale dell'amministrazione, coordinando lo sviluppo dei servizi pubblici digitali e l'adozione di nuovi modelli di relazione con i cittadini, trasparenti e aperti.
- RUP: Responsabile Unico di Progetto a seguito del d.lgs. 36/2023, già Responsabile Unico di Procedimento.
- SDI: Sistema di interscambio, è un sistema informatico in grado di: ricevere le fatture sotto forma di file con le caratteristiche della FatturaPA; effettuare controlli sui file ricevuti; inoltrare le fatture verso le amministrazioni pubbliche destinatarie, o verso cessionari/committenti privati (B2B e B2C).
- SIPA: Sistema Informativo delle Pubbliche Amministrazioni (SIPA) insieme coordinato di risorse, norme, procedure, tecnologie e dati volti a supportare la gestione informatizzata delle attività e dei processi all'interno delle pubbliche amministrazioni.

- User-centric: Principio per cui le pubbliche amministrazioni devono progettare servizi pubblici che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo.
- UTD: Ufficio per la Transizione Digitale è l'ufficio dell'amministrazione a cui viene affidato il delicato processo di transizione alla modalità operativa digitale.