



Piano Triennale per la transizione digitale 2024-2026 dell'Istituto Superiore di Sanità

Riferimento al Piano Triennale per l'informatica 2024-
2026 (aggiornamento 2025) pubblicato da AGID



PTTD_2024-2026

Rev.0 del 04/06/2025

	DATA	DA
EMESSO		Duilio Luca Bacocco ⁵
VERIFICATO		N/A
APPROVATO		<ul style="list-style-type: none"> • Dott. Corrado Di Benedetto² • Dott. Piergiorgio Faraglia⁶ • Dott.ssa Daniela Felici³ • Dott.ssa Claudia Mastrocola⁴
IN VIGORE		Approvato dal CDA ISS
¹ Area Risorse Strumentali e Tecnologie Informatiche – Ufficio I Affari Generali ² Responsabile Area Risorse Strumentali e Tecnologie Informatiche – Ufficio I Affari Generali ³ Direttore Ufficio I - Affari Generali ⁴ Direttore Centrale Affari Generali ⁵ Responsabile per la Transizione al Digitale – Ufficio I Affari Generali ⁶ Referente per la Cybersicurezza - Area Risorse Strumentali e Tecnologie Informatiche – Ufficio I Affari Generali		

STORIA DELLA REVISIONE

REV	Del	Modifiche apportate
0	04/06/2025	Prima emissione

Sommario

1. INTRODUZIONE.....	5
1.1. PREMESSA	5
1.1.1. L'Istituto Superiore di Sanità: contesto e organizzazione	5
1.2. RUOLO DEL RESPONSABILE PER LA TRANSIZIONE AL DIGITALE.....	7
1.3. CONTESTO STRATEGICO.....	8
1.4. OBIETTIVI DEL PIANO TRIENNALE	9
2. PARTE PRIMA – COMPONENTI STRATEGICHE	11
2.1. Capitolo 1 – Organizzazione e gestione del cambiamento	11
2.1.1. Contesto normativo e obiettivi.....	11
2.1.2. Roadmap delle linee d'azione	11
2.1.3. Strumenti per l'attuazione del piano e risorse e fonti di finanziamento	12
2.2. Capitolo 2 - Il procurement per la trasformazione digitale.....	13
2.2.1. Contesto normativo e obiettivi.....	13
2.2.2. Roadmap delle linee d'azione	13
3. PARTE SECONDA – COMPONENTI TECNOLOGICHE.....	15
3.1. Capitolo 3 – Servizi	15
3.1.1. Contesto normativo e obiettivi.....	15
3.1.2. Roadmap delle linee d'azione	16
3.2. Capitolo 4 – Piattaforme.....	18
3.2.1. Contesto normativo e obiettivi.....	18
3.2.2. Roadmap delle linee d'azione	20
3.2.3. Strumenti per l'attuazione del piano e risorse e fonti di finanziamento	23
3.3. Capitolo 5 – Dati e intelligenza artificiale	23
3.3.1. Contesto normativo e obiettivi.....	23
3.3.2. Roadmap delle linee d'azione	25
3.4. Capitolo 6 – Infrastrutture	32



3.4.1. Contesto normativo e obiettivi.....	32
3.4.2. Roadmap delle linee d'azione	33
3.4.3. Strumenti per l'attuazione del piano e risorse e fonti di finanziamento	36
3.5. Capitolo 7 – Sicurezza informatica.....	36
3.5.1. Contesto normativo e obiettivi.....	36
3.5.2. Roadmap delle linee d'azione	37

1. INTRODUZIONE

1.1. PREMESSA

Attraverso il presente documento, l'Istituto Superiore di Sanità stabilisce la propria strategia relativamente alla tematica della trasformazione digitale per il triennio 2024-2026, così come previsto nel Piano Triennale per l'Informatica nella Pubblica Amministrazione di AGID all'ultima versione per il periodo di riferimento.

La redazione di questo documento è effettuata dal Responsabile per la Transizione Digitale dell'Istituto, che è funzionalmente parte dell'Ufficio I Affari Generali e si avvale, per lo svolgimento delle attività legate alla transizione digitale, del supporto funzionale dell'Area Risorse Strumentali e Tecnologie Informatiche del medesimo Ufficio I Affari Generali, cui compete la gestione dell'infrastruttura informatica dell'Istituto.

Il presente documento è strutturato secondo le raccomandazioni di AGID in merito, condividendo la strutturazione in capitoli del Piano Triennale relativo al triennio cui si riferisce.

1.1.1. L'Istituto Superiore di Sanità: contesto e organizzazione

Come indicato negli Articoli 1 e 2 del proprio Statuto, l'Istituto Superiore di Sanità (di seguito anche ISS, o Istituto) è organo tecnico-scientifico del Servizio Sanitario Nazionale e persegue la tutela della salute pubblica, in particolare attraverso lo svolgimento delle funzioni di ricerca, controllo, consulenza, regolazione e formazione. Di esso si avvalgono il Ministero della Salute, le Regioni e le Province autonome di Trento e Bolzano, ed è ricompreso tra gli enti di ricerca di cui al d.lgs. 25 novembre 2016, n. 218, operando come ente pubblico di ricerca con autonomia scientifica, organizzativa, amministrativa e contabile, sottoposto alla vigilanza del Ministero della Salute. L'Istituto esercita le proprie funzioni nei limiti delle proprie disponibilità finanziarie attraverso:

- a. la genesi di conoscenza;
- b. la produzione di evidenze;
- c. il trasferimento della conoscenza e delle evidenze;
- d. l'effettuazione di controlli ovvero il rilascio di valutazioni, pareri, certificazioni e altre valutazioni di conformità;
- e. il trasferimento tecnologico;
- f. la collaborazione con Agenzie nazionali ed europee nonché con ogni altro soggetto nazionale o estero, pubblico o privato;
- g. il supporto alle attività di preparazione e risposta ai problemi emergenti;

- h. la promozione, il supporto ed il coordinamento di reti ed infrastrutture;
- i. lo svolgimento, su richiesta del Ministero della Salute o delle Regioni e delle Province autonome di Trento e Bolzano, di ogni intervento che si rendesse necessario nell'interesse pubblico;
- j. lo svolgimento di ogni altro compito attribuitogli dalle vigenti disposizioni.

L'Istituto, inoltre:

- a. svolge direttamente attività di ricerca e promuove, partecipa e coordina programmi di studio e ricerca di interesse nazionale ed internazionale;
- b. svolge attività di sorveglianza e cura la predisposizione e la tenuta di registri e di sistemi informativi su eventi rilevanti per la salute pubblica;
- c. svolge attività di certificazione CE dei dispositivi medici;
- d. effettua controlli analitici, valutazioni e ispezioni, anche ai fini autorizzativi, su articoli, biocidi, cosmetici, diagnostici in vitro, dispositivi medici, mangimi, materiali, matrici ambientali e biologiche, miscele o preparati pericolosi e non, presidi medico chirurgici, prodotti alimentari, prodotti fitosanitari, sostanze, ambienti di vita e di lavoro, agenti biologici, chimici e fisici, benessere animale e su quanto previsto dalle normative;
- e. effettua il controllo e la valutazione di medicinali biologici e chimici, anche in qualità di laboratorio ufficiale per il controllo dei medicinali;
- f. fornisce consulenza al Ministero della Salute, al Governo, alle Regioni ed alle Province autonome di Trento e di Bolzano, agli Enti locali ed alle Organizzazioni europee ed internazionali;
- g. promuove, partecipa e coordina in ambito nazionale ed internazionale attività e programmi di formazione, collaborazione, perfezionamento ed aggiornamento attraverso l'utilizzo degli appositi strumenti previsti dalle norme vigenti;
- h. appronta ed aggiorna l'inventario nazionale delle sostanze chimiche e dei preparati; i. predispone, aggiorna e gestisce banche dati, piattaforme informatiche e di documentazione per obiettivi di sanità pubblica e sicurezza;
- i. esercita altre funzioni previste dai piani triennali per esigenze di supporto all'adeguamento del servizio sanitario nazionale.

Per l'espletamento delle proprie funzioni e di ogni attività connessa l'Istituto può, anche con risorse proprie, e nei limiti delle proprie disponibilità finanziarie:

- a. stipulare convenzioni, accordi e contratti con soggetti pubblici o privati, nazionali ed internazionali;
- b. partecipare o costituire associazioni, consorzi, fondazioni o società con soggetti pubblici e privati, nazionali ed internazionali, nel rispetto delle vigenti disposizioni in materia e secondo le procedure individuate da apposito regolamento.

Come previsto dagli Articoli 13 e 14 del medesimo Statuto, il disegno organizzativo dell'Istituto si articola nei seguenti livelli funzionali:

- a) la Presidenza, cui compete l'esercizio delle funzioni strategiche di indirizzo e programmazione;
- b) la Direzione generale, cui è affidata la responsabilità della gestione complessiva delle attività;
- c) l'Area operativa tecnico-scientifica, cui è attribuita la funzione di garantire la realizzazione di quanto contenuto nel piano triennale di attività e di quant'altro disposto dal Presidente;
- d) l'Area operativa amministrativa, cui è attribuita la funzione di garantire il supporto alla Presidenza, alla Direzione generale ed all'Area operativa tecnico-scientifica.

All'Area Operativa Tecnico-Scientifica afferiscono:

- a) i Dipartimenti;
- b) i Centri;
- c) i Servizi Tecnico-scientifici;
- d) il Centro Nazionale Sangue;
- e) il Centro Nazionale Trapianti;

I Servizi tecnico scientifici, disciplinati con apposito regolamento, svolgono compiti di supporto trasversale alle attività dell'Istituto.

1.2. RUOLO DEL RESPONSABILE PER LA TRANSIZIONE AL DIGITALE

Ai sensi di quanto previsto dalla normativa vigente, l'Istituto Superiore di Sanità ha individuato un Responsabile per la Transizione Digitale (RTD) cui sono attribuiti i compiti di cui all'art. 17 del CAD, nonché:

- a) il potere di costituire tavoli di coordinamento con gli altri dirigenti dell'amministrazione e/o referenti nominati da questi ultimi;
- b) il potere di costituire gruppi tematici per singole attività e/o adempimenti;
- c) il potere di proporre l'adozione di circolari e atti di indirizzo sulle materie di propria competenza;
- d) l'adozione dei più opportuni strumenti di raccordo e consultazione con le altre figure coinvolte nel processo di digitalizzazione della pubblica amministrazione (responsabili per la gestione, responsabile per la conservazione documentale, responsabile per la prevenzione della corruzione e della trasparenza, responsabile per la protezione dei dati personali);

- e) la competenza in materia di predisposizione del Piano triennale per l'informatica della singola amministrazione, nelle forme e secondo le modalità definite dall'Agenzia per l'Italia digitale;
- f) la predisposizione di una relazione annuale sull'attività svolta dall'Area "Transizione Digitale" da trasmettere al Presidente;

Da un punto di vista funzionale e organizzativo, la figura del Responsabile per la Transizione Digitale dell'ISS è parte dell'Ufficio I Affari Generali, pertanto, nello svolgimento delle proprie attività, risponde primariamente al Dirigente dell'Ufficio I Affari Generali e al Direttore Centrale degli Affari Generali, cui riferisce circa l'andamento dell'attività svolta e segnala eventuali anomalie di gestione. Il RTD inoltre collabora, per quanto di competenza ed in relazione alle rispettive responsabilità, con il Responsabile dell'Area Risorse Strumentali e Tecnologie Informatiche e con il Referente per la cybersicurezza dell'ISS;

1.3. CONTESTO STRATEGICO

Il processo di transizione digitale all'interno dell'ISS va inevitabilmente ad impattare profondamente con le attività che caratterizzano sia la sua parte amministrativa che quella scientifica, per le quali l'attuazione degli obiettivi individuati da AGID introduce inevitabilmente dei cambiamenti, che hanno su ciascuna delle due parti ripercussioni specifiche rispetto alla tipologia di attività svolta.

I cambiamenti, per loro natura, incontrano resistenza, soprattutto in realtà dove le modalità di lavoro sono fortemente radicate e collaudate, ma l'obiettivo è quello di superare queste resistenze mediante la collaborazione e il dialogo con gli interlocutori interni all'Ente, al fine di mostrare che l'utilizzo di strumenti innovativi e di modalità di lavoro diverse non deve essere visto come una minaccia, bensì come un modo di rendere più semplice, efficiente e tutelato l'operato di ognuno.

Nel corso dell'anno 2024, in ISS sono state introdotte importanti novità in ambito di transizione digitale. Sempre nel rispetto della struttura proposta dal Piano Triennale per l'Informatica nella PA di AGID:

- Relativamente alla parte *Servizi*:
 - Per ciò che riguarda l'*Interoperabilità*, sono state gettate le fondamenta affinché l'Ente possa usufruire dei servizi offerti tramite la Piattaforma Digitale Nazionale Dati (PDND) nonché erogarne di propri, attivando l'adesione alla piattaforma in questione.
- Relativamente alla parte *Piattaforme*:
 - È stata formalizzata l'adesione all'App IO, aprendo quindi la possibilità per l'ente di comunicare coi cittadini attraverso questa piattaforma usando applicazioni che potranno essere eventualmente sviluppate o attività.

- Per quanto riguarda l'utilizzo di identità digitali, l'infrastruttura di Single Sign-On ISS è stata accreditata per consentire agli utenti di autenticarsi, sulle applicazioni che lo supportano, tramite CIE, CNS e EIDAS oltre a SPID.
- Nell'ambito dell'adesione alla cosiddetta *soluzione avanzata* di NoiPA, sono progredite le attività relative alla migrazione delle attività di gestione delle presenze verso il sistema NoiPA.
- È stato avviato il processo di migrazione integrale della gestione delle procedure di selezione del personale dalla piattaforma SelezioniOnline on-premise al portale InPA del Dipartimento della Funzione Pubblica.
- L'ISS, quale ente iscritto all'Albo del Servizio Civile Universale istituito presso il Dipartimento per le politiche giovanili e il servizio civile universale della Presidenza del Consiglio dei Ministri, è stato registrato presso la piattaforma Sistema Unico SCU Helios-Futuro per la gestione e la presentazione di programmi e progetti inerenti al servizio civile universale.
- Relativamente alla parte *Dati e Intelligenza Artificiale*:
 - Per quanto riguarda l'Open Data, è stata effettuata una prima selezione di 10 dataset che sono stati presentati ad AGID per la pubblicazione sui portali dati.gov.it e data.europa.eu ed è stato attivato un portale istituzionale, <https://dati.iss.it> dove le basi di dati aperte dell'Istituto sono elencate e fruibili.
- Relativamente alla parte *Infrastrutture*:
 - In conformità con quanto previsto dal Piano Triennale per l'Informatica nella PA di AGID, l'ISS ha avviato il processo di migrazione di alcuni servizi ritenuti *critici* dalla propria infrastruttura verso quella del Polo Strategico Nazionale, con l'obiettivo di completare la migrazione entro il 31/07/2025.
- Relativamente alla parte *Sicurezza Informatica*:
 - Nel mese di dicembre 2024, il perimetro relativo all'esercizio dell'infrastruttura informatica dell'ISS è stato certificato ISO.27001. Questo ha comportato l'introduzione, in Istituto, di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) che imposta una gestione informatica basata su un modello di governance ben preciso il quale gestisce a sua volta procedure operative indirizzate all'esercizio in sicurezza dei servizi informatici.

1.4. OBIETTIVI DEL PIANO TRIENNALE

Nell'ambito della propria transizione verso la modalità di lavoro digitale, l'ISS intende allinearsi, strategicamente, ai principi guida considerati nel Piano Triennale per l'Informatica nella PA di AGID.

Di seguito i suddetti principi guida:

- **Digital & mobile first:** per i servizi di nuova attivazione, si darà precedenza alle modalità di lavoro completamente digitali, sfruttando le prime occasioni utili per aggiornare le modalità di lavoro che caratterizzano i servizi ancora basati su modalità *legacy*.
- **Cloud first:** dove possibile, per i progetti si valuterà, in via preferenziale, l'adozione di servizi cloud, utilizzando esclusivamente infrastrutture e servizi cloud qualificati da ACN.
- **API-first:** qualora fossero avviati progetti di interoperabilità tra amministrazioni o servizi, questi saranno gestiti in via preferenziale tramite integrazioni via API (con preferenza verso il paradigma REST).
- **Digital identity only:** sui servizi pubblici dove è richiesta l'autenticazione, l'ISS integrerà l'intero set di sistemi di autenticazione tramite identità pubblica (SPID, CIE, CNS e EIDAS).
- **User-centric:** nell'ambito dell'attivazione di servizi pubblici e la manutenzione di quelli esistenti, vengono perseguite by design e by default accessibilità e usabilità ai sensi delle normative vigenti.
- **Open data by design e by default:** il processo di apertura dei dati dell'Istituto, iniziato nel 2024, continuerà con la pubblicazione di nuove basi di dati che saranno disponibili nel tempo (nuove o già esistenti)
- **Data protection by design e by default:** allo stato attuale, per tutti i servizi pubblici che vengono attivati o aggiornati vengono effettuati preliminarmente controlli relativi alle attività trattamentali svolte da parte del DPO di ISS.
- **Once only:** sfruttando PDND saranno valutate, nel corso della reingegnerizzazione dei processi istituzionali, integrazioni con altre amministrazioni e servizi per perseguire la finalità ultima del *once-only*.
- **Openness:** dove disponibili soluzioni in riuso, queste vengono valutate come possibili candidate per supportare gli scenari dell'amministrazione, mentre per il codice sorgente delle applicazioni sviluppate per ISS da terzi viene richiesta *obbligatoriamente* la consegna per effettuare i test di sicurezza statici e dinamici, propedeutici al passaggio in produzione.
- **Sostenibilità digitale:** il ciclo di vita dei servizi è già considerato nell'ambito della sicurezza informatica, come conseguenza della certificazione ISO 27001 del perimetro informatico dell'ente.
- **Sussidiarietà, proporzionalità e appropriatezza della digitalizzazione.**

2. PARTE PRIMA – COMPONENTI STRATEGICHE

2.1. Capitolo 1 – Organizzazione e gestione del cambiamento

2.1.1. Contesto normativo e obiettivi

Tra i fattori abilitanti dei processi di trasformazione digitali è di fondamentale importanza l'insieme delle *competenze digitali*, ovvero tutte quelle conoscenze, attitudini e capacità che permettono di operare in un'ambiente digitale. Nell'ambito della pubblica amministrazione, il fabbisogno di competenze digitali riguarda tutti i dipendenti, a tutti i livelli e le linee d'azione in questo senso sono rivolte verso il potenziamento di queste competenze su larga scala.

2.1.1.1. Obiettivi e linee d'azione applicabili

Nell'ambito di questa sezione dedicata ai Servizi vengono considerati i seguenti obiettivi e le relative linee d'azione applicabili:

- **Obiettivo 1.2 – Diffusione competenze digitali nel Paese e nella PA:** Roadmap delle linee d'azione

2.1.2. Roadmap delle linee d'azione

Nell'ambito dell'obiettivo di cui sopra (Obiettivo 1.2 – Diffusione competenze digitali nel Paese e nella PA), di seguito un riepilogo delle linee d'azione applicabili per l'ente:

Obiettivo 1.2 – Diffusione competenze digitali nel Paese e nella PA		
<i>Linea d'azione</i>	<i>Deadline e piano dei tempi</i>	<i>Strutture responsabili della linea d'azione</i>
CAP1.PA.07 - 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.	Triennio 2024-2026 , organizzazione ed erogazione della formazione prevista sulla base di un fabbisogno di formazione annuale.	Ufficio Reclutamento, Borse di Studio e Formazione

<p>CAP1.PA.08 - Le PA aderiscono all’iniziativa “Syllabus per la formazione digitale” e promuovono la partecipazione alle iniziative formative sulle competenze digitali 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</p>	<p>Triennio 2024-2026. L’ISS ha aderito a Syllabus nel 2022 e ha esteso a tutti i dipendenti l’accessibilità ai corsi disponibili. Vengono altresì assegnati nuovi corsi di formazione non appena questi sono disponibili, sulla base della pertinenza alle attività dell’ente.</p> <p>Viene effettuato monitoraggio periodico della formazione in piattaforma dei dipendenti (percorsi iniziati/conclusi) e periodicamente vengono inviati reminder per favorire la partecipazione alle iniziative di formazione.</p> <p>Previsti entro il 2025:</p> <ul style="list-style-type: none"> • L’attivazione di un portale Intranet descrittivo delle iniziative formative in essere; • L’attivazione di un portale di e-learning interno dove distribuire materiale formativo. 	<ul style="list-style-type: none"> • Ufficio Reclutamento, Borse di Studio e Formazione • Area Governo Strategico della Tecnologia dell’Informazione e della Transizione Digitale (Ufficio RTD)
---	--	---

2.1.3. Strumenti per l’attuazione del piano e risorse e fonti di finanziamento

Le fonti di finanziamento delle attività di formazione vengono stanziati dall’Ente stesso in funzione del fabbisogno formativo di cui alla linea d’azione CAP1.PA.07.

2.2. Capitolo 2 - Il procurement per la trasformazione digitale

2.2.1. Contesto normativo e obiettivi

La trasformazione digitale della Pubblica Amministrazione, intesa come reingegnerizzazione profonda dei processi per migliorarne efficienza e qualità dei servizi erogati, dipende da risorse e strumenti sia interni che esterni all'amministrazione stessa. Il *procurement* è il processo tramite cui l'amministrazione può approvvigionarsi di prodotti e servizi esterni e per questo motivo va realizzato con efficacia ed efficienza. Per questo motivo, negli ultimi anni è stata forte, a livello nazionale, la spinta verso una riorganizzazione dei processi legati al procurement per il settore pubblico, che ha avuto importanti ripercussioni anche sulle singole amministrazioni.

2.2.1.1. Obiettivi e linee d'azione applicabili

Nell'ambito di questa sezione dedicata ai Servizi vengono considerati i seguenti obiettivi e le relative linee d'azione applicabili:

Obiettivo 2.1 – Rafforzare l'ecosistema nazionale di approvvigionamento digitale

2.2.2. Roadmap delle linee d'azione

Nell'ambito dell'obiettivo di cui sopra (Obiettivo 1.2 – Diffusione competenze digitali nel Paese e nella PA), di seguito un riepilogo delle linee d'azione applicabili per l'ente:

Obiettivo 2.1 – Rafforzare l'ecosistema nazionale di approvvigionamento digitale		
<i>Linea d'azione</i>	<i>Deadline e piano dei tempi</i>	<i>Strutture responsabili della linea d'azione</i>
<i>RA2.1.1 - Diffusione del processo di certificazione delle piattaforme di approvvigionamento digitale</i>		
CAP2.PA.02 - Le stazioni appaltanti devono digitalizzare la fase di esecuzione dell'appalto.	Giugno 2025 A partire da gennaio 2024, l'ISS in conformità col Codice degli Appalti utilizza la piattaforma di e-procurement certificata Appalti&Contratti di Maggioli, che, in qualità di gestore certificato, la fornisce come servizio all'Istituto. La	Direzione Risorse Umane ed Economiche



	<p>piattaforma in questione digitalizza la fase di esecuzione dell'appalto come richiesto e viene aggiornata regolarmente per mantenere la compliance normativa.</p>	
--	--	--

3. PARTE SECONDA – COMPONENTI TECNOLOGICHE

3.1. Capitolo 3 – Servizi

3.1.1. Contesto normativo e obiettivi

La digitalizzazione è una parte fondamentale del processo di innovazione dei servizi pubblici, al fine di migliorarne l'efficienza, la trasparenza e la qualità. Alla base del concetto di digitalizzazione vi è quello di interoperabilità, ovvero la collaborazione e cooperazione tra enti e realtà diverse che condividono e riusano processi e risorse perseguendo il principio *once-only*. La strada tracciata per stabilire interoperabilità è quella di adottare, per la condivisione di servizi, l'architettura a microservizi, che vengono condivisi tramite la Piattaforma Digitale Nazionale Dati (PDND).

Altro aspetto chiave nel processo di digitalizzazione dei servizi pubblici è quello che riguarda il miglioramento della qualità e dell'inclusività dei servizi stessi, considerandone gli aspetti di accessibilità e usabilità, ma anche monitorandone l'adozione e l'utilizzo da parte dei cittadini.

A queste tematiche si aggiunge quella della dematerializzazione degli archivi cartacei e in generale quella della corretta formazione, gestione e conservazione dei documenti informatici, per cui tutte le Pubbliche Amministrazioni vengono chiamate a rispettare quanto indicato nelle Linee Guida sulla Formazione, Gestione e Conservazione dei Documenti Informatici dell'Agenzia per l'Italia Digitale.

Nell'ottica della digitalizzazione l'Ente, l'esigenza rappresentata dal Centro nazionale controllo e valutazione farmaci, che ad ottobre 2025 sarà sottoposto ad audit nell'ambito della certificazione di qualità ISO 17025, ha dato impulso all'aggiornamento della c.d. "Procedura Campioni", che definisce le attività di gestione dei campioni dalla loro ricezione in Istituto fino alla consegna all'unità tecnico-scientifica destinataria. Si è reso necessario aggiornare il precedente testo, ormai risalente nel tempo, tramite un'opera di miglioramento dei processi e di loro reingegnerizzazione in chiave digitale con l'obiettivo di ottimizzare e razionalizzare la gestione dei campioni. L'esperienza maturata nella reingegnerizzazione del processo servirà come base per la reingegnerizzazione di altri processi interni all'Ente.

3.1.1.1. Obiettivi e linee d'azione applicabili

Nell'ambito di questa sezione dedicata ai Servizi vengono considerati i seguenti obiettivi e le relative linee d'azione applicabili:

- **Obiettivo 3.1: Migliorare la capacità di erogare e-service**
- **Obiettivo 3.2: Migliorare la capacità di generare ed erogare servizi digitali**

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

3.1.2. Roadmap delle linee d'azione

Obiettivo 3.1: Migliorare la capacità di erogare e-service		
<i>Linea d'azione</i>	<i>Deadline e piano dei tempi</i>	<i>Strutture responsabili della linea d'azione</i>
<i>RA3.1.1 - Incremento del numero di "e-service" registrati sul Catalogo Pubblico PDND</i>		
CAP3.PA.01 - Le PA cessano di utilizzare modalità di interoperabilità diverse da PDND per le nuove implementazioni.	<p>Da gennaio 2024</p> <p>Allo stato attuale, l'ISS pur essendo accreditato presso la PDND non fruisce di servizi in interoperabilità.</p> <p>In conformità alle linee guida, comunque, ogni possibile necessità di interoperabilità tra amministrazioni sarà gestita mediante la piattaforma PDND.</p> <p>È allo studio, per il 2025, la possibilità di impiegare le API PDND dell'ANPR (Anagrafe Nazionale Popolazione Residente) per supportare le attività di alcuni registri e sorveglianze.</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
CAP3.PA.02 – Le Amministrazioni possono iniziare la migrazione dei servizi erogati in interoperabilità dalle attuali modalità alla PDND.		
CAP3.PA.03 – Le PA continuano a popolare il Catalogo delle API conformi alle "Linee guida sull'interoperabilità tecnica delle pubbliche amministrazioni"		
CAP3.PA.05 – Le PA centrali siglano accordi per l'erogazione di API su PDND		
<i>RA3.1.2 - Aumento del numero di Richieste di Fruizione Autorizzate su PDND</i>		
CAP3.PA.06 – Le PA utilizzano le API presenti sul Catalogo	<p>Da gennaio 2024</p> <p>Nel corso 2024 l'ISS è accreditato per utilizzare i servizi PDND. In ottemperanza a quanto previsto nell'obiettivo RA3.1.1, le necessità</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche

	di interoperabilità verranno soddisfatte, dove possibile, adottando servizi a catalogo ed esponendone di nuovi.	(gestione servizi IT) <ul style="list-style-type: none"> Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
CAP3.PA.07 – Le PA effettuano richieste di fruizione dei servizi erogati da privati	Da gennaio 2025 In ottemperanza a quanto previsto nell'obiettivo RA3.1.1, le necessità di interoperabilità con privati verranno soddisfatte, dove possibile, adottandone i servizi a catalogo.	
Obiettivo 3.2: Migliorare la capacità di generare ed erogare servizi digitali		
<i>RA3.2.2 - Incremento dell'accessibilità dei servizi digitali</i>		
CAP3.PA.13 – Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web	Marzo 2025 <i>COMPLETATO (marzo 2025)</i>	<ul style="list-style-type: none"> Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
CAP3.PA.14 – Le PA pubblicano, entro il 23 settembre, esclusivamente tramite l'applicazione <i>form.agid.gov.it</i> la dichiarazione di accessibilità per ciascuno dei propri siti <i>web</i> e App mobili.	Settembre 2025	
CAP3.PA.15 – Le PA pubblicano gli obiettivi di accessibilità sul proprio sito web	Marzo 2026	
CAP3.PA.16 – Le PA pubblicano, entro il 23 settembre, esclusivamente tramite l'applicazione <i>form.agid.gov.it</i> la dichiarazione di accessibilità per ciascuno dei propri siti <i>web</i> e App mobili.	Settembre 2026	

Obiettivo 3.3: Consolidare l'applicazione delle Linee guida per la formazione, gestione e conservazione documentale		
<i>RA3.3.1 - Monitorare l'attuazione delle Linee guida</i>		
CAP3.PA.17 – 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	Giugno 2025 <i>IN CORSO</i> Entro giugno 2025 l'ISS nominerà un Responsabile della gestione documentale e predisporrà il Manuale di gestione documentale, pubblicando quanto richiesto in Amministrazione trasparente.	<ul style="list-style-type: none"> • Ufficio I Affari Generali • Ufficio Anticorruzione e trasparenza
CAP3.PA.18 – Le PA devono verificare che in “Amministrazione trasparente” sia pubblicato il Manuale di conservazione e la nomina del Responsabile della conservazione	Giugno 2026 <i>IN CORSO</i> Entro giugno 2026 l'ISS pubblicherà su Amministrazione trasparente il Manuale di conservazione e la nomina del Responsabile della conservazione	

3.2. Capitolo 4 – Piattaforme

3.2.1. Contesto normativo e obiettivi

Le piattaforme della Pubblica Amministrazione sono un supporto fondamentale nella digitalizzazione di processi e servizi della PA, offrendo funzionalità sia alle amministrazioni stesse che ai cittadini. L'adozione di queste piattaforme rappresenta quindi un fattore abilitante al processo di digitalizzazione. Nel caso dell'ISS, si analizzerà l'adesione a PagoPA, AppIO, SEND, SPID e CIE, NoiPA.

3.2.1.1. PagoPA

PagoPA è la piattaforma che consente ai cittadini di effettuare pagamenti in modalità digitale verso la pubblica amministrazione, utilizzando diversi metodi di pagamento elettronici, con l'obiettivo di standardizzare e rendere più semplici ed efficienti i processi di pagamento verso la PA, favorendo inoltre la riduzione dell'uso del contante.

3.2.1.2. AppIO

L'App IO è un'applicazione per smartphone che, in ottemperanza all'art. 64bis del Codice dell'Amministrazione Digitale, istituisce un punto di accesso unico per tutti i servizi digitali delle pubbliche amministrazioni. Attraverso l'App IO, le pubbliche amministrazioni possono quindi contattare il cittadino, così come il cittadino può a sua volta interagire con i servizi che le pubbliche amministrazioni mettono a disposizione tramite l'App (es. pagamenti pagoPA).

3.2.1.3. SEND

La piattaforma SEND (Servizio Notifiche Digitali) che permette di recapitare notifiche a valore legale sulla piattaforma stessa oppure sull'App IO, sollevando gli enti dagli adempimenti legati alla gestione dell'invio delle comunicazioni a valore legale oltre a minimizzare la possibilità che il destinatario possa non essere reperibile.

3.2.1.4. SPID e CIE

SPID e CIE sono servizi di identità digitale che permettono di accedere ai servizi online della pubblica amministrazione fornendo al contempo ai servizi dati identificativi dell'utente *certificati*. Mentre SPID viene rilasciato ai cittadini da un insieme di soggetti pubblici e privati accreditati da AgID, l'identità digitale CIE è sviluppata e gestita dall'Istituto Poligrafico e Zecca dello Stato e costituisce una rappresentazione digitalizzata dei dati identificativi registrati al momento del rilascio della Carta di Identità Elettronica.

3.2.1.5. NoiPA

NoiPA è la piattaforma dedicata alle pubbliche amministrazioni per la gestione integrata dei processi in ambito risorse umane, inclusi quelli legati agli adempimenti previsti dalla normativa vigente.

3.2.1.6. Obiettivi e linee d'azione applicabili

Nell'ambito di questa sezione dedicata ai Servizi vengono considerati i seguenti obiettivi e le relative linee d'azione applicabili:

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

3.2.2. Roadmap delle linee d'azione

Nell'ambito dell'obiettivo di cui sopra (Obiettivo 4.1 – Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA), di seguito un riepilogo delle linee d'azione applicabili per l'ente:

Obiettivo 4.1 – Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA		
<i>Linea d'azione</i>	<i>Deadline e piano dei tempi</i>	<i>Strutture responsabili della linea d'azione</i>
<i>RA4.1.1 – Incremento dei servizi sulla piattaforma pagoPA</i>		
CAP4.PA.01 – 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)	Dicembre 2026 <i>IN CORSO</i> Nel corso del 2025 è previsto il completo rifacimento della piattaforma E-commerce ISS, utilizzata per pagamento all'ente dei servizi a terzi mediante pagoPA. In concomitanza al rifacimento della piattaforma, sarà aumentato anche il numero dei servizi offerti mediante la piattaforma stessa per il pagamento tramite pagoPA.	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD) • Direzione Risorse Umane ed Economiche
<i>RA4.1.2 – Incremento dei servizi sulla Piattaforma IO (l'App dei servizi pubblici)</i>		
CAP4.PA.02 – Le PA aderenti ad 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)	Dicembre 2026	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della

		<p>Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)</p> <ul style="list-style-type: none"> • Ufficio I Affari Generali
<p><i>RA4.1.3 – Incremento degli enti che usano SEND</i></p>		
<p>CAP4.PA.03 – Le PA centrali e i Comuni, in linea con i target sopra descritti e secondo la roadmap di attuazione prevista dal Piano Nazionale di Ripresa e Resilienza (PNRR), si integreranno a SEND</p>	<p>Dicembre 2026</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD) • Ufficio I Affari Generali
<p><i>RA4.1.4 – Incremento dell'adozione e dell'utilizzo di SPID e CIE da parte delle Pubbliche Amministrazioni</i></p>		
<p>CAP4.PA.04 – 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.</p>	<p>COMPLETATO</p> <p>L'ISS dispone di un sistema di IAM basato su tecnologia Microsoft Azure AD B2C che integra, in un singolo portale che può essere richiamato dalle applicazioni, i servizi di autenticazione tramite SPID, CIE, CNS e EIDAS (da marzo 2025)</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia

<p>CAP4.PA.05 – Le PA e i gestori di pubblici servizi interessati cessano il rilascio di credenziali proprietarie a cittadini databili di SPID e/o CIE.</p>	<p><i>IN CORSO</i></p> <p>In fase di progettazione delle applicazioni che offrono servizi al pubblico vengono effettuate tutte le valutazioni</p>	<p>dell'Informazione e della Transizione Digitale (Ufficio RTD)</p>
<p>CAP4.PA.06 – 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 o 3 devono anche adottare il “Login with EIDAS” per l’accesso transfrontaliero ai propri servizi</p>	<p>propedeutiche a determinare quali sistemi di autenticazione tramite identità pubblica digitale debbano essere integrati.</p> <p>È prevista, per alcuni servizi aventi utenti su scala europea, l’attivazione dell’autenticazione tramite EIDAS.</p>	
<p>CAP4.PA.07 – Le PA devono adeguarsi alle evoluzioni previste dall’ecosistema SPID</p>	<p><i>IN CORSO</i></p> <p>Il sistema di IAM e single sign-on dell’ISS verrà mantenuto conforme all’evoluzione delle specifiche SPID.</p>	
<p><i>RA4.1.5 – Promuovere l’adesione ai servizi della piattaforma NoiPA per supportare l’azione amministrativa nella gestione del personale</i></p>		
<p>CAP4.PA.08 – Le PA che intendono aderire a NoiPA esprimono manifestazione di interesse e inviano richiesta</p>	<p><i>IN CORSO</i></p> <p>Nel 2023 l’ISS ha aderito alla <i>soluzione estesa</i> di NoiPA affinché anche la gestione presenze del personale ISS potesse essere gestita mediante la piattaforma. La migrazione sarà completata entro il 2025 e comporterà, oltre allo spostamento dei carichi di lavoro legati alla gestione presenze del</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione

	personale verso la piattaforma NoiPA, anche la formazione del personale incaricato di gestire le presenze mediante la piattaforma.	Digitale (Ufficio RTD) <ul style="list-style-type: none">• Direzione Risorse Umane ed Economiche
--	--	--

3.2.3. Strumenti per l’attuazione del piano e risorse e fonti di finanziamento

Relativamente alla linea d’azione CAP4.PA.01, l’ISS ha presentato la propria candidatura per l’AVVISO PUBBLICO per la presentazione di domande di partecipazione a valere su PIANO NAZIONALE DI RIPRESA E RESILIENZA - MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.4 “SERVIZI E CITTADINANZA DIGITALE” MISURA 1.4.3 “ADOZIONE PIATTAFORMA PAGOPA” ALTRI ENTI (Regioni/Province autonome, Aziende sanitarie locali e ospedaliere, Università, Enti di ricerca e AFAM - MAGGIO 2024) per un importo pari a 75030€, da utilizzarsi per l’attivazione di ulteriori servizi di pagamento e il rifacimento del portale E-commerce.

3.3. Capitolo 5 – Dati e intelligenza artificiale

3.3.1. Contesto normativo e obiettivi

Nel contesto tecnologico attuale, i dati rivestono un’importanza considerevole poiché sono alla base dell’economia moderna (data economy), oltre a rivestire un fattore chiave nel raggiungere gli obiettivi definiti nella Strategia europea in materia di dati, abilitare l’attivazione di servizi digitali di valore per cittadini, imprese, portatori di interesse e supportare i vertici decisionali di processi organizzativi e/o produttivi tramite strumenti data-driven.

A questi scenari si aggiungono inoltre quelli legati all’Intelligenza Artificiale, le cui capacità dipendono prevalentemente dai dati a supporto e dalla loro qualità.

Affinché i dati possano supportare gli scenari di cui sopra, devono essere disponibili per gli utilizzatori e questo si traduce nell’Interoperabilità e nella pubblicazione in formato aperto. In generale, vista l’importanza dei dati, questi dovranno essere gestiti dalle amministrazioni in maniera organica, per mezzo di una *data governance* che segua principi, regole e procedure appropriate all’ambito in oggetto.

Per quanto riguarda l’Intelligenza Artificiale, nell’ambito di questa trattazione consideriamo tutti quei sistemi automatici in grado di generare output come previsioni, contenuti, raccomandazioni o

suggerimenti decisionali sulla base di deduzioni ottenute a partire da una serie di input. Nell'ambito della pubblica amministrazione e, più in generale dei servizi pubblici, l'utilizzo di sistemi di intelligenza artificiale può risultare utile per modernizzare e migliorare l'efficienza e l'efficacia dei vari processi mediante, ad esempio:

- L'automatizzazione di alcune attività ripetitive di ricerca e analisi di informazioni, permettendo di dedicare il tempo ad attività a maggior valore per l'ente o la collettività;
- La possibilità di supportare i processi decisionali o predittivi utilizzando i dati;
- La personalizzazione dei servizi per i singoli utenti.

Nell'ambito della *mission* dell'Istituto Superiore di Sanità, ovvero l'essere organo tecnico-scientifico del Servizio Sanitario Nazionale che persegue la tutela della salute pubblica, in particolare attraverso lo svolgimento delle funzioni di ricerca, controllo, consulenza, regolazione e formazione, l'uso dell'Intelligenza Artificiale, soprattutto a supporto delle attività di ricerca, rappresenta un fattore abilitante al raggiungimento di obiettivi che richiedano il processamento di enormi quantità di dati. A tal fine, con deliberazione del Consiglio di Amministrazione n.9 allegata al Verbale n. 72 del CdA del 24/10/2024, è stato dedicato un centro all'Intelligenza artificiale denominato "Centro Nazionale Intelligenza Artificiale, HTA e Tecno-assistenza", la cui mission consiste nel promuovere il miglioramento dello stato di salute pubblica attraverso la ricerca, lo sviluppo, l'ottimizzazione e la valutazione di tecnologie innovative, utilizzando competenze multidisciplinari quali l'impiego della intelligenza artificiale, l'applicazione delle metodologie di pratica e ricerca connesse all'Health Technology Assessment, l'utilizzazione della telemedicina e la ricerca legata alla biomedicina spaziale e subacquea.

3.3.1.1. Obiettivi e linee d'azione applicabili

Nell'ambito di questa sezione dedicata ai Dati e all'Intelligenza Artificiale vengono considerati i seguenti obiettivi e le relative linee d'azione applicabili:

- **Obiettivo 5.1 - Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese**
- **Obiettivo 5.2 - Aumentare la qualità dei dati e dei metadati**
- **Obiettivo 5.3 - Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati**
- **Obiettivo 5.4 - Aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale**
- **Obiettivo 5.5 - Dati per l'intelligenza artificiale**

3.3.2. Roadmap delle linee d'azione

Nell'ambito degli obiettivi di cui sopra, di seguito un riepilogo delle linee d'azione applicabili per l'ente:

Obiettivo 5.1 - Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese		
<i>Linea d'azione</i>	<i>Deadline e piano dei tempi</i>	<i>Strutture responsabili della linea d'azione</i>
<i>RA5.1.1 - Aumento del numero di dataset aperti di tipo dinamico in coerenza con quanto previsto dalle Linee guida Open Data</i>		
CAP5.PA.01 – Le PA adeguano i metadati relativi ai dati geografici all'ultima versione delle specifiche nazionali e documentano i propri dataset nel Catalogo nazionale <i>geodati.gov.it</i>	Dicembre 2026 L'ISS sta progressivamente censendo e aprendo le proprie basi dati. Nell'ambito di questa attività, se saranno individuati dataset di questo tipo, saranno pubblicati in conformità alle linee d'azione previste.	<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD) • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT)
CAP5.PA.02 – Le PA adeguano i metadati relativi ai dati non geografici alle specifiche nazionali e documentano i propri dataset nel Catalogo nazionale <i>dati.gov.it</i>		<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD) • Area Risorse Strumentali e Tecnologie

		<p>Informatiche (gestione servizi IT)</p>
<p>CAP5.PA.03 – Le PA partecipano, in funzione delle proprie necessità, a interventi di formazione e sensibilizzazione sulle politiche <i>open data</i></p>		<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD) • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT)
<p><i>RA5.1.2 - Aumento del numero di dataset resi disponibili attraverso i servizi di rete di cui al framework creato con la Direttiva 2007/2/EC (INSPIRE) e relativi Regolamenti attuativi, con particolare riferimento ai dati di elevato valore di cui al Regolamento di esecuzione (UE) 2023/138</i></p>		
<p>CAP5.PA.04 – Le PA attuano le indicazioni sui dati di elevato valore presenti nel Regolamento di esecuzione (UE) 2023/138, nelle Linee guida Open Data nonché nella specifica guida operativa</p>	<p>Da giugno 2024</p> <p>L'ISS sta progressivamente censendo e aprendo le proprie basi dati. Nell'ambito di questa attività, se saranno individuati dataset di questo tipo, saranno pubblicati in conformità alle linee d'azione previste.</p>	<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD) • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT)
<p>Obiettivo 5.2 – Aumentare la qualità dei dati e dei metadati</p>		

<p>RA5.2.1 – Aumento del numero di dataset con metadati di qualità conformi agli standard di riferimento europei e nazionali</p>		
<p>CAP5.PA.05 – Le PA pubblicano i metadati relativi ai dati di elevato valore, secondo le indicazioni presenti nel Regolamento di esecuzione (UE) e nelle Linee guida sui dati aperti e relativa guida operativa, nei cataloghi nazionali <i>dati.gov.it</i> e <i>geodati.gov.it</i></p>	<p>Da giugno 2024</p>	<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD) • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT)
<p>RA5.2.3 – Aumento del numero di amministrazioni non ancora presenti nel catalogo dati.gov.it che rendono disponibili dataset di tipo aperto</p>		
<p>CAP5.PA.08 – Ogni Comune con popolazione > 250.000 abitanti, ogni Regione ed ogni altro ente territoriale regionale, ogni Università, Ente e centro di ricerca (non ancora presenti nel catalogo <i>dati.gov.it</i>) pubblicano e documentano nel catalogo almeno 10 dataset</p>	<p>Dicembre 2024</p> <p>COMPLETATO</p> <p>A dicembre 2024 è stato attivato il portale istituzionale <i>dati.iss.it</i> e sono stati pubblicati sul suddetto portale, ma anche su <i>dati.gov.it</i> gli Open Data relativi allo <i>Stato dei corpi di acqua dolce in Italia</i>.</p>	<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD) • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT)
<p>CAP5.PA.13 – Ogni Comune con popolazione > 250.000 abitanti, ogni Regione ed ogni altro ente territoriale regionale, ogni Università, Ente e centro di</p>	<p>Dicembre 2025</p> <p>L'ISS sta progressivamente censendo e aprendo le proprie basi dati. Nell'ambito di questa attività, nel corso del 2025</p>	<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della

<p>ricerca (non ancora presenti nel 2024 catalogo <i>dati.gov.it</i>) pubblicano e documentano nel catalogo almeno 15 dataset</p>	<p>saranno individuate saranno individuate basi di dati per la pubblicazione in formato aperto in numero almeno sufficiente al raggiungimento dell'obiettivo.</p>	<p>Transizione Digitale (Ufficio RTD)</p> <ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT)
<p>CAP5.PA.18 – Ogni Comune con popolazione > 250.000 abitanti, ogni Regione ed ogni altro ente territoriale regionale, ogni Università, Ente e centro di ricerca (non ancora presenti nel 2024 catalogo <i>dati.gov.it</i>) pubblicano e documentano nel catalogo almeno 30 dataset</p>	<p>Dicembre 2026</p> <p>L'ISS sta progressivamente censendo e aprendo le proprie basi dati. Nell'ambito di questa attività, nel corso del 2026 saranno individuate basi di dati per la pubblicazione in formato aperto in numero almeno sufficiente al raggiungimento dell'obiettivo.</p>	<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD) • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT)
<p>Obiettivo 5.3 – Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati</p>		
<p><i>RA5.3.1 – Aumento del numero di dataset di tipo aperto documentati nel portale dati.gov.it che adottano le licenze previste dalle Linee guida Open Data</i></p>		
<p>CAP5.PA.20 – Le PA attuano le Linee guida contenenti regole tecniche per l'implementazione del Decreto Legislativo n.36/2006 relativamente ai requisiti e alle raccomandazioni su licenze e condizioni d'uso</p>	<p>Da gennaio 2024</p> <p>L'ISS sta progressivamente censendo e aprendo le proprie basi dati. Nell'ambito di questa attività, i dati saranno pubblicati, dove possibile, dando priorità all'utilizzo della licenza Creative Commons Attribuzione 4.0</p>	<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD) • Area Risorse Strumentali e

		Tecnologie Informatiche (gestione servizi IT)
Obiettivo 5.4 - Aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale		
<i>RA5.4.1 – Linee guida per promuovere l'adozione dell'IA nella Pubblica Amministrazione</i>		
CAP5.PA.21 – Le PA adottano le Linee per promuovere l'adozione dell'IA nella Pubblica Amministrazione	Dicembre 2025	<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD) • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT)
<i>RA5.4.2 – Linee guida per il procurement di IA nella Pubblica Amministrazione</i>		
CAP5.PA.22 – Le PA adottano le Linee guida per il procurement di IA nella Pubblica Amministrazione	Dicembre 2025	<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD) • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT)

RA5.4.3 – Linee guida per lo sviluppo di applicazioni di IA per la Pubblica Amministrazione		
CAP5.PA.23 – Le PA adottano le Linee guida per lo sviluppo di applicazioni di IA nella Pubblica Amministrazione	Dicembre 2025	<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD) • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT)
RA5.4.4 – Realizzazione di applicazioni di IA a valenza nazionale		
CAP5.PA.24 – Le PA adottano le applicazioni di IA a valenza nazionale	Dicembre 2026	<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD) • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT)
RA5.5.1 – Basi di dati nazionali strategiche		
CAP5.PA.25 – Le PA adottano le basi di dati nazionali strategiche	Dicembre 2026	<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della



		<p>Transizione Digitale (Ufficio RTD)</p> <ul style="list-style-type: none">• Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT)
--	--	--

3.4. Capitolo 6 – Infrastrutture

3.4.1. Contesto normativo e obiettivi

La strategia *Cloud Italia*, pubblicata a settembre 2021 dal Dipartimento per la Trasformazione Digitale e dall'Agenzia per la Cybersicurezza Nazionale ha come obiettivi principali l'autonomia tecnologica del Paese, il controllo sui dati e l'aumento della resilienza dei servizi digitali, con il fine ultimo di guidare le pubbliche amministrazioni verso un ambiente cloud sicuro. La strategia, infatti, nasce dalla considerazione che molte infrastrutture della PA non assicurano adeguati livelli di sicurezza e affidabilità oltre ad essere carenti dai punti di vista strutturale ed organizzativo. Questo scenario pone quindi le basi per il processo di razionalizzazione e migrazione delle infrastrutture descritto nella strategia che, prevede:

- Un approccio *cloud-first*, per cui le Amministrazioni sono tenute a valutare l'adozione del cloud in fase di definizione di un nuovo progetto o di attivazione di nuovi servizi, in via prioritaria rispetto a qualsiasi altra tecnologia, motivando un eventuale esito negativo della valutazione. In caso di disponibilità all'interno del Catalogo dei servizi cloud per la PA qualificati da ACN di una soluzione SaaS aderente alle esigenze, deve essere valutata la migrazione o l'adozione della soluzione SaaS rispetto a soluzioni IaaS o PaaS.
- La realizzazione di un'infrastruttura ad alta affidabilità, localizzata sul territorio nazionale, denominata Polo Strategico Nazionale (PSN) destinata ad accogliere i servizi oggetto di razionalizzazione e consolidamento presso le pubbliche amministrazioni.
- La migrazione, per le amministrazioni centrali (di cui l'ISS fa parte), nel rispetto dei principi di efficienza, efficacia ed economicità dell'azione amministrativa, dei loro Centri per l'elaborazione delle informazioni (CED) e relativi sistemi informatici, privi dei requisiti fissati dalla Circolare AGID 1/2019 e, successivamente, dal regolamento di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179 (di seguito Regolamento cloud e infrastrutture), verso l'infrastruttura del PSN o verso altra infrastruttura propria già esistente e in possesso dei requisiti fissati dalla Circolare AGID 1/2019 e, successivamente, dal Regolamento cloud e infrastrutture. Le amministrazioni centrali, in alternativa, possono migrare i propri servizi verso soluzioni cloud qualificate, nel rispetto di quanto previsto dal Regolamento cloud e infrastrutture;
- L'impossibilità, per le amministrazioni, di investire nella costruzione di *nuovi* data center, per ottimizzare l'utilizzo delle risorse economiche pubbliche, mentre è ammesso il consolidamento dei data center ai sensi di quanto previsto dall'articolo 33-septies del Decreto-legge 179/2012 e dal Regolamento di cui al comma 4 del citato articolo 33-septies.

Da questo punto di vista, l'ISS ha adottato una strategia combinata: al percorso pluriennale, in via di completamento, per il consolidamento della propria infrastruttura già avviato nell'ambito di progressi investimenti tecnologici, si è affiancata la migrazione dei servizi classificati come *critici*

sull’infrastruttura del Polo Strategico Nazionale. Inoltre, di base, nell’attivazione di nuovi servizi, viene data la precedenza all’adozione di soluzioni cloud certificate ACN già esistenti, evitando, se possibile in generale l’utilizzo di soluzioni cloud non certificate.

3.4.1.1. Obiettivi e linee d’azione applicabili

Nell’ambito di questa sezione dedicata ai Dati e all’Intelligenza Artificiale vengono considerati i seguenti obiettivi e le relative linee d’azione applicabili:

- **Obiettivo 6.1 – Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la strategia “Cloud Italia” e migrando verso infrastrutture e servizi cloud qualificati (incluso PSN)**
- **Obiettivo 6.2 – Garantire alle amministrazioni la disponibilità della connettività SPC**

3.4.2. Roadmap delle linee d’azione

Nell’ambito degli obiettivi di cui sopra, di seguito un riepilogo delle linee d’azione applicabili per l’ente:

Obiettivo 6.1 – Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni attuando la strategia “Cloud Italia” e migrando verso infrastrutture e servizi cloud qualificati (incluso PSN)		
<i>Linea d’azione</i>	<i>Deadline e piano dei tempi</i>	<i>Strutture responsabili della linea d’azione</i>
<i>RA6.1.1 – Numero di amministrazioni migrate</i>		
CAP6.PA.01 – Le PA proprietarie di data center di gruppo B richiedono l’autorizzazione ad AGID per le spese in materia di data center nelle modalità stabilite dalla Circolare AGID 1/2019 e prevedono in tali contratti, qualora autorizzati, una durata massima coerente con i tempi strettamente necessari a completare il percorso di migrazione previsto nei propri piani di migrazione	Dicembre 2025 <i>IN CORSO</i> L’ISS completerà, entro il 2025, il percorso di consolidamento della propria infrastruttura e contestualmente avvierà l’iter per la qualificazione della propria infrastruttura per consentire l’erogazione di servizi classificabili come <i>critici</i>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell’Informazione e della Transizione Digitale (Ufficio RTD)

<p>CAP6.PA.03 – Le PA avviano il percorso di migrazione verso il cloud in coerenza con quanto previsto dalla Strategia Cloud Italia</p>	<p>Febbraio 2024</p> <p><i>COMPLETATO</i></p> <p>La migrazione dei servizi critici verso l’infrastruttura del PSN è stata avviata nel mese di febbraio 2024 con la firma del contratto d’utenza tra ISS e PSN.</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
<p>CAP6.PA.04 – Le PA continuano ad applicare il principio cloud first e ad acquisire servizi cloud solo se qualificati o adeguati ai sensi del Regolamento cloud</p>	<p><i>IN CORSO</i></p> <p>Nel processo di attivazione di nuovi servizi e nel procurement è obbligatorio verificare che, i servizi cloud che si intenda adottare siano qualificati ACN ovvero presenti nel catalogo cloud. Nella scelta di eventuali servizi da adottare, tra eventuali alternative disponibili viene data la precedenza ai servizi qualificati</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
<p>CAP6.PA.05 – 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</p>	<p>Settembre 2025 (a partire da)</p> <p>L’attuale classificazione è stata completata nel Settembre 2023 ed è stata la base per il piano di migrazione al cloud attualmente seguito nell’ambito della migrazione a PSN. La classificazione sarà revisionata a partire dalla data di cui sopra per</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione

	allineare il quadro dei servizi allo stato dell'ente.	e della Transizione Digitale (Ufficio RTD)
CAP6.PA.06 – Le PA, ove richiesto dal Dipartimento per la Trasformazione Digitale o da AGID, trasmettono le informazioni relative allo stato di avanzamento dell'implementazione dei piani di migrazione	<p>Da settembre 2024</p> <p><i>IN CORSO</i></p> <p>Nell'ambito dell'asseverazione dei servizi migrati secondo il piano di migrazione al PSN, l'ISS ha fornito al DTD informazioni relative allo stato di avanzamento del piano stesso. Ulteriori informazioni saranno fornite su richiesta e comunque nell'ambito dell'asseverazione finale del progetto di migrazione</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
CAP6.PA.10 – 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	<p>Giugno 2025</p> <p><i>IN CORSO</i></p> <p>La conclusione del processo di migrazione dei servizi critici al cloud del PSN è prevista entro la data di cui sopra.</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
Obiettivo 6.2 – Garantire alle amministrazioni la disponibilità della connettività SPC		
<i>RA6.2.1 – Rete di connettività</i>		
CAP6.PA.11 – Sulla base delle proprie esigenze, le pubbliche	Da ottobre 2025	<ul style="list-style-type: none"> • Area Risorse Strumentali e

<p>amministrazioni iniziano la fase di migrazione della loro infrastruttura di rete utilizzando i servizi resi disponibili dalla nuova gara di connettività SPC</p>	<p>L'attività, per la parte telefonia, sarà avviata alla prima scadenza utile successiva all'aggiudicazione da parte di CONSIP della nuova gara di connettività SPC.</p>	<p>Tecnologie Informatiche (gestione servizi IT)</p> <ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
---	--	--

3.4.3. Strumenti per l'attuazione del piano e risorse e fonti di finanziamento

Relativamente alle linee d'azione CAP6.PA.03 e CAP.6.PA.10, l'ISS ha presentato la propria candidatura per l'AVVISO PUBBLICO la presentazione di domande di partecipazione a valere su PIANO NAZIONALE DI RIPRESA E RESILIENZA - MISSIONE 1 - COMPONENTE 1 INVESTIMENTO 1.1 "INFRASTRUTTURE DIGITALI" ALTRE PAC (GIUGNO 2023) FINANZIATO DALL'UNIONE EUROPEA – NextGenerationEU per un importo pari a 1.079.416€, da dedicarsi all'attuazione del piano di migrazione dei servizi verso il PSN. L'importo è stato finanziato con Decreto n. 104-3/2023 – PNRR del Dipartimento per la trasformazione digitale del 2/11/2023.

3.5. Capitolo 7 – Sicurezza informatica

3.5.1. Contesto normativo e obiettivi

La transizione al digitale, oltre a modificare profondamente la struttura dei processi interni alle varie amministrazioni, sta evidenziando l'esistenza di nuovi rischi per le realtà in fase di trasformazione, legati principalmente alla possibilità di eventuali attacchi cyber. La sicurezza e la resilienza delle reti e dei sistemi, che rappresentano le fondamenta dei servizi digitali, rappresenta quindi un obiettivo cardine per garantire sia la sicurezza del Paese, che il suo sviluppo nel tempo. Per questo motivo, a livello nazionale sono stati individuate le seguenti necessità:

- Adottare dei modelli di gestione centralizzati della cybersicurezza;

- Definire e adottare processi di gestione e mitigazione del rischio cyber, sia interno che associato ai rapporti con le terze parti;
- Migliorare la cultura *cyber* nelle amministrazioni.

3.5.1.1. Obiettivi e linee d'azione applicabili

Nell'ambito di questa sezione dedicata alla Sicurezza Informatica vengono considerati i seguenti obiettivi e le relative linee d'azione applicabili:

- **Obiettivo 7.1 – Adottare una governance della cybersicurezza diffusa nella PA**
- **Obiettivo 7.2 – Gestire i processi di approvvigionamento IT coerentemente con i requisiti di sicurezza definiti**
- **Obiettivo 7.3 – Gestione e mitigazione del rischio cyber**
- **Obiettivo 7.4 – Potenziare le modalità di prevenzione e gestione degli incidenti informatici**
- **Obiettivo 7.5 – Implementare attività strutturate di sensibilizzazione cyber del personale**
- **Obiettivo 7.6 – Contrastare il rischio cyber attraverso attività di supporto proattivo alla PA**

3.5.2. Roadmap delle linee d'azione

Nell'ambito degli obiettivi di cui sopra, di seguito un riepilogo delle linee d'azione applicabili per l'ente:

Obiettivo 7.1 – Adottare una governance della cybersicurezza diffusa nella PA		
<i>Linea d'azione</i>	<i>Deadline e piano dei tempi</i>	<i>Strutture responsabili della linea d'azione</i>
<i>RA7.1.1 – Identificazione di un modello, con ruoli e responsabilità, di gestione della cybersicurezza</i>		
CAP7.PA.01 – Le singole PA definiscono il modello unitario, assicurando un coordinamento centralizzato a livello dell'istituzione, di governance della cybersicurezza	<p>Da settembre 2024</p> <p><i>COMPLETATO (dicembre 2024)</i></p> <p>L'ISS è certificato ISO 27001 dal 20/12/2024. Nell'ambito del processo di certificazione, è stata formalizzata la strutturazione interna dedicata alla governance della cybersicurezza</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della

		Transizione Digitale (Ufficio RTD)
CAP7.PA.02 – Le PA adottano un modello di governance della cybersicurezza	<p>Da dicembre 2024</p> <p><i>COMPLETATO (dicembre 2024)</i></p> <p>L'ISS è certificato ISO 27001 dal 20/12/2024. Nell'ambito dell'organizzazione necessaria alla gestione del Sistema di Gestione della Sicurezza delle Informazioni previsto dalla certificazione, è stato adottato un modello di governance formalizzato in apposite procedure operative.</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
CAP7.PA.03 – Le PA nominano i Responsabili della Cybersicurezza e delle loro strutture organizzative di supporto	<p>Da dicembre 2024</p> <p><i>COMPLETATO (gennaio 2025)</i></p> <p>Nel mese di gennaio 2025 l'ISS ha provveduto alla nomina del proprio <i>referente per la cybersicurezza</i> ai sensi di quanto stabilito nella Legge 90/2024 e Decreto Legge 138/2024, individuando nell'Area Risorse Strumentali e Tecnologie Informatiche dell'Ufficio I Affari Generali la struttura competente in materia di cybersicurezza.</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
RA7.1.2 – Definizione del framework documentale a supporto della gestione cyber		

<p>CAP7.PA.04 – Le PA formalizzano i processi e le procedure inerenti alla gestione della cybersicurezza</p>	<p>Da dicembre 2024</p> <p><i>COMPLETATO (dicembre 2024)</i></p> <p>Il processo di certificazione ISO 27001, concluso il 20/12/2024 ha portato alla formalizzazione di procedure per la gestione della cybersicurezza all'interno del Sistema di Gestione della Sicurezza delle Informazioni.</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
<p>Obiettivo 7.2 – Gestire i processi di approvvigionamento IT coerentemente con i requisiti di sicurezza definiti</p>		
<p><i>RA7.2.1 – Definizione del framework documentale a supporto del processo di approvvigionamento IT</i></p>		
<p>CAP7.PA.05 – Le PA definiscono e approvano i requisiti di sicurezza relativi al processo di approvvigionamento IT</p>	<p>Da giugno 2024</p> <p><i>IN CORSO</i></p> <p>A partire dal 2022, l'ISS adotta un formato standard per quanto riguarda la redazione di allegati tecnici relativi a fornitura di servizi di sviluppo software e cloud. Il formato è componibile poiché ad una serie di requisiti di sicurezza standard richiesti affianca una serie di requisiti variabili, da inserirsi sulla base del punteggio di criticità ottenuto dalla specifica fornitura. I requisiti sono ottenuti a partire dalle <i>Linee guida</i></p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)

	<p><i>sicurezza nel procurement ICT di AGID.</i></p> <p>È prevista, per il 2025, un'evoluzione di questo concetto per estendersi a tutti i progetti di fornitura in ambito ICT, da inserirsi nell'ambito delle attività di miglioramento del Sistema di Gestione della Sicurezza delle Informazioni ISO 27001.</p>	
<p>CAP7.PA.06 – 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</p>	<p>Da dicembre 2024</p> <p><i>IN CORSO</i></p> <p>Sono in fase di elaborazione procedure di gestione del rischio su fornitori e terze parti con particolare attenzione a quello che riguarda la sicurezza informatica. L'ISS essendo una pubblica amministrazione è comunque tenuto ad approvvigionarsi di beni e servizi in ambito IT sfruttando i canali previsti per le PA. La contrattualistica per i fornitori e le terze parti standardizzata, già adottata per alcune tipologie di progetti in ambito IT, sarà estesa a tutti i progetti in questo ambito.</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
<p><i>RA7.2.2 – Definizione delle modalità di monitoraggio del processo di approvvigionamento IT</i></p>		

<p>CAP7.PA.07 – Le PA realizzano le attività di controllo definite nel Piano di <i>audit</i> e verifica verso i fornitori e terze parti IT</p>	<p>Da dicembre 2025</p> <p>Dal 2022 sono definite le modalità di organizzazione di audit nei confronti di fornitori e terze parti IT, che saranno attualizzate e potenziate nel corso del 2025 nell’ambito del processo di miglioramento del Sistema di Gestione della Sicurezza delle Informazioni ISO 27001</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
<p>Obiettivo 7.3 – Gestione e mitigazione del rischio cyber</p>		
<p><i>RA7.3.1 – Definizione del framework per la gestione del rischio cyber</i></p>		
<p>CAP7.PA.08 – Le PA definiscono e formalizzano il processo di <i>cyber risk management</i> e <i>security by design</i>, coerentemente con gli strumenti messi a disposizione da ACN</p>	<p>Da dicembre 2024</p> <p><i>COMPLETATO</i></p> <p>Il processo di cyber risk management e security by design è formalizzato all’interno delle procedure operative che costituiscono il Sistema di Gestione della Sicurezza delle Informazioni ISO 27001</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
<p>CAP7.PA.09 – Le PA promuovono il censimento dei dati e servizi della PA, identificandone la rilevanza e quindi le modalità per garantirne la continuità operativa</p>	<p>Dicembre 2025</p> <p><i>IN CORSO</i></p> <p>Dati e servizi dell’ISS sono censiti dal punto di vista informatico e ad essi sono associati una classificazione di</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT)

	<p>criticità intrinseca affiancata ad una criticità operativa, per la determinazione delle misure idonee e necessarie alla continuità operativa. Le procedure di business continuity sono descritte nel corpo documentale del Sistema di Gestione della Sicurezza delle Informazioni ISO 27001.</p>	<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
<p>CAP7.PA.10 – 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</p>	<p>Dicembre 2025</p> <p><i>IN CORSO</i></p> <p>Il piano pluriennale di miglioramento degli aspetti di integrità, confidenzialità e disponibilità di servizi e dati dell'Istituto è in via di completamento e ne è prevista la conclusione entro dicembre 2025</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
<p>CAP7.PA.11 – Le PA integrano le attività di monitoraggio del rischio <i>cyber</i>, come definito dal relativo Piano, nelle normali attività di progettazione, analisi, conduzione e dismissione di applicativi e sistemi informatici</p>	<p>Dicembre 2026</p> <p><i>IN CORSO</i></p> <p>Il monitoraggio del rischio <i>cyber</i> è elemento stabile delle attività di progettazione, analisi, conduzione e dismissione di applicativi e sistemi informatici dell'ISS, nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni ISO 27001. Si tratta comunque di un</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione

	elemento in fase di continua evoluzione nell'ambito del miglioramento continuo del sistema stesso.	Digitale (Ufficio RTD)
RA7.3.2 – Definizione delle modalità di monitoraggio del rischio cyber		
CAP7.PA.12 – 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	Da dicembre 2025 Vedi linea d'azione CAP7.PA.11	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
Obiettivo 7.4 – Potenziare le modalità di prevenzione e gestione degli incidenti informatici		
RA7.4.1 – Definizione del framework documentale relativo alla gestione degli incidenti		
CAP7.PA.13 – Le PA definiscono i presidi per la gestione degli eventi di sicurezza, formalizzandone i processi e le procedure	Da giugno 2024 <i>COMPLETATO (dicembre 2024)</i> I presidi per la gestione di eventi di sicurezza sono definiti nelle procedure operative che compongono il Sistema di Gestione della Sicurezza delle Informazioni ISO 27001, dove vengono anche formalizzati i relativi processi e procedure in essere	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)

<p>CAP7.PA.14 – Le PA formalizzano ruoli, responsabilità e processi, nonché le capacità tecnologiche a supporto della prevenzione e gestione degli incidenti informatici</p>	<p>Da dicembre 2024</p> <p><i>COMPLETATO (dicembre 2024)</i></p> <p>Ruoli, responsabilità, processi e capacità tecnologiche sono definiti nelle procedure operative che compongono il Sistema di Gestione della Sicurezza delle Informazioni ISO 27001, dove vengono anche formalizzati i relativi processi e procedure in essere</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
<p><i>RA7.4.2 – Definizione delle modalità di verifica e aggiornamento dei piani di risposta agli incidenti</i></p>		
<p>CAP7.PA.15 – Le PA definiscono le modalità di verifica dei Piani di risposta a seguito di incidenti informatici</p>	<p>Da dicembre 2024</p> <p><i>COMPLETATO (dicembre 2024)</i></p> <p>I piani di risposta agli incidenti informatici sono definiti nelle procedure operative che compongono il Sistema di Gestione della Sicurezza delle Informazioni ISO 27001, nell'ambito del quale avviene anche la verifica degli stessi e gli aggiornamenti periodici</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
<p>CAP7.PA.16 – Le PA definiscono le modalità di aggiornamento dei Piani di risposta e ripristino a seguito dell'accadimento di incidenti informatici</p>	<p>Da dicembre 2025</p> <p><i>COMPLETATO (dicembre 2024)</i></p> <p>I piani di risposta agli incidenti informatici sono definiti nelle procedure operative che compongono il Sistema di</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT)

	Gestione della Sicurezza delle Informazioni ISO 27001, nell'ambito del quale avviene anche la verifica degli stessi e gli aggiornamenti periodici	<ul style="list-style-type: none"> Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
Obiettivo 7.5 – Implementare attività strutturate di sensibilizzazione cyber del personale		
<i>RA7.5.1 – Definizione dei piani di formazione in ambito cyber</i>		
CAP7.PA.17 – Le PA promuovono l'accesso e l'utilizzo di attività strutturate di sensibilizzazione in ambito cybersicurezza	<p>Da giugno 2024</p> <p><i>IN CORSO</i></p> <p>Dal 2024, il corso sulla cybersicurezza erogato dalla piattaforma Syllabus è assegnato a tutti i dipendenti ISS, al fine di raggiungere una cybersecurity awareness diffusa. La frequenza del corso viene monitorata e si inviano al personale reminder periodici in merito.</p>	<ul style="list-style-type: none"> Ufficio Reclutamento, Borse di Studio e Formazione Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
CAP7.PA.18 – Le PA definiscono piani di formazione inerenti alla cybersecurity, diversificati per ruoli, posizioni organizzative e attività delle risorse dell'organizzazione	<p>Da dicembre 2024</p> <p><i>IN CORSO</i></p>	<ul style="list-style-type: none"> Ufficio Reclutamento, Borse di Studio e Formazione Area Risorse Strumentali e Tecnologie Informatiche

		<p>(gestione servizi IT)</p> <ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
<p>CAP7.PA.19 – Le PA realizzano iniziative per verificare e migliorare la consapevolezza del proprio personale</p>	<p>Da dicembre 2025 <i>IN CORSO</i></p>	<ul style="list-style-type: none"> • Ufficio Reclutamento, Borse di Studio e Formazione • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
<p>Obiettivo 7.6 – Contrastare il rischio cyber attraverso attività di supporto proattivo alla PA</p> <p><i>RA7.6.1 – Distribuzione di Indicatori di Compromissione alle PA</i></p>		
<p>CAP7.PA.20 – Le PA, di cui all’art. 2 comma 2 del CAD dovranno accreditarsi al CERT-AGID ed aderire al flusso di Indicatori di compromissione (Feed IoC) del CERT-AGID per la protezione della propria</p>	<p>Da dicembre 2024 <i>COMPLETATO (ottobre 2024)</i></p> <p>ISS ha aderito al flusso di Indicatori di compromissione del CERT-AGID</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT)

<p>Amministrazione da minacce Malware e Phishing</p>		<ul style="list-style-type: none"> • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
<p><i>RA7.6.2 – Fornitura di strumenti funzionali all'esecuzione dei piani di autovalutazione dei sistemi esposti</i></p>		
<p>CAP7.PA.21 – Le PA dovranno usufruire degli strumenti per la gestione dei rischi <i>cyber</i> messi a disposizione dal CERT-AGID</p>	<p>Da dicembre 2024</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della Transizione Digitale (Ufficio RTD)
<p><i>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</i></p>		
<p>CAP7.PA.22 – Le PA, sulla base delle proprie esigenze, partecipano ai corsi di formazione base ed avanzato erogati dal CERT-AGID</p>	<p>Da dicembre 2025</p>	<ul style="list-style-type: none"> • Area Risorse Strumentali e Tecnologie Informatiche (gestione servizi IT) • Area Governo Strategico della Tecnologia dell'Informazione e della



		Transizione Digitale (Ufficio RTD)
--	--	--