



Piano Triennale per la Transizione Digitale 2026 dell'Università degli Studi di Firenze

Riferimento al Piano triennale per l'informatica Edizione 2024-2026

Aggiornamento 2026 pubblicato da AGID

Oltre a offrire il supporto digitale necessario alle linee d'azione del [Piano strategico di Ateneo](#) 2023-2027, il Piano Triennale rappresenta uno strumento fondamentale per assicurare uno sviluppo coerente, coordinato e conforme alle direttive nazionali e agli standard internazionali relativi ai servizi digitali, ai sistemi informatici e alle procedure operative ICT dell'Ateneo. Ciò risulta particolarmente importante anche in relazione al previsto aumento della richiesta di tali servizi, a fronte di risorse economiche e di personale limitate.

Il Piano si allinea inoltre alle linee guida nazionali definite da AgID nel Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026.

Firenze, gennaio 2026



Sommario

INTRODUZIONE	3
Strategia	4
Modello strategico	6
Principi guida.....	7
Aggiornamenti Agid 2026	9
PARTE PRIMA – Componenti strategiche	10
Capitolo 1 - Organizzazione e gestione del cambiamento	11
L’ecosistema digitale amministrativo	11
Il ruolo del Responsabile e dell’Ufficio per la transizione digitale.....	11
Capitolo 2 - Il procurement per la trasformazione digitale	16
Il procurement per la trasformazione digitale.....	16
Gli acquisti di beni e servizi standardizzati	17
L’ecosistema digitale degli acquisti pubblici.....	18
La qualificazione della Stazione appaltante.....	18
Le gare strategiche per la trasformazione digitale	20
PARTE SECONDA – Componenti tecnologiche.....	22
Capitolo 3 - Servizi.....	23
E-Service in interoperabilità tramite PDND	23
Progettazione dei servizi: accessibilità e design	28
Formazione, gestione e conservazione dei documenti informatici.....	29
Capitolo 4 - Piattaforme.....	35
Piattaforme nazionali che erogano servizi a cittadini/imprese o ad altre PA	35
Piattaforme che attestano attributi.....	43
Capitolo 5 - Dati e Intelligenza Artificiale	47
Dati e data governance	47
Intelligenza artificiale per la Pubblica Amministrazione.....	56
Dati per l’intelligenza artificiale	57
Capitolo 6 - Infrastrutture.....	61
Infrastrutture digitali e Cloud	61
Capitolo 7 - Sicurezza informatica	66
APPENDICE 1 - Glossario e Acronimi.....	78
APPENDICE 2 - Riferimenti normativi	81

INTRODUZIONE

Il Piano Triennale per l'Informatica dell'Università degli Studi di Firenze rappresenta lo strumento fondamentale di indirizzo strategico e di pianificazione operativa per la gestione e lo sviluppo dei sistemi informativi e delle tecnologie digitali dell'Ateneo. La sua redazione è un obbligo normativo sancito dal Codice dell'Amministrazione Digitale (CAD - D.Lgs. 7 marzo 2005, n. 82), che affida al Responsabile per la Transizione al Digitale (RTD) il compito di definire gli indirizzi per lo sviluppo dei sistemi informativi, in coerenza con le linee guida nazionali. Questo documento costituisce l'aggiornamento annuale per l'anno 2026 del Piano relativo al triennio 2024-2026, recependo le evoluzioni normative e tecnologiche intervenute nell'ultimo anno.

L'aggiornamento 2026 si inserisce in una fase cruciale del percorso di digitalizzazione nazionale. Se il biennio precedente è stato caratterizzato dalla messa a terra dei progetti legati al Piano Nazionale di Ripresa e Resilienza (PNRR), il 2026 rappresenta il momento del consolidamento e dell'integrazione sistemica. Per l'Università di Firenze, questo non è un mero adempimento burocratico, ma l'atto con cui l'Ateneo definisce la propria traiettoria di innovazione per garantire il funzionamento della didattica, della ricerca e dei servizi amministrativi. Per tale ragione in questo aggiornamento 2026, l'Ateneo fiorentino pone particolare enfasi su come le tecnologie emergenti possano integrarsi nel tessuto accademico. L'introduzione dell'Intelligenza Artificiale viene affrontata non solo come opportunità di automazione dei processi di back-office, ma anche come strumento di supporto alla didattica e alla ricerca, sempre all'interno di un quadro etico e regolamentare definito. Parallelamente, l'adozione di piattaforme nazionali come l'IT-Wallet e la Piattaforma Digitale Nazionale Dati (PDND) impone di ripensare ed evolvere i servizi agli studenti e ai dipendenti sia all'interno dell'Ateneo che nel rapporto con altre pubbliche amministrazioni, in Italia e in Europa.

Un aspetto centrale del nostro approccio è l'interoperabilità. L'Università di Firenze si impegna a superare la logica dei silos informativi, lavorando affinché i dati siano condivisi in modo sicuro ed efficiente tra le diverse aree dell'amministrazione e con gli enti esterni, in attuazione del principio "once-only". Questo significa progettare servizi dove l'utente non debba fornire più volte le stesse informazioni che l'amministrazione già possiede. La valorizzazione dei dati diventa, quindi, strategica e il patrimonio informativo dell'Ateneo un

asset cruciale.

La sicurezza informatica rimane un prerequisito imprescindibile. In un contesto di minacce crescenti, il Piano definisce le azioni per innalzare i livelli di protezione delle infrastrutture, dei dati personali e strategici e della proprietà intellettuale prodotta dalla ricerca, investendo non solo in tecnologie difensive, ma anche nella consapevolezza e nella formazione di tutta la comunità universitaria.

Il Piano Triennale dell'Università di Firenze è, dunque, un documento programmatico vivo che traduce la visione strategica in un portafoglio di progetti concreti, con tempi, responsabilità e indicatori di risultato definiti, garantendo che ogni investimento in tecnologia si traduca in un valore tangibile per la comunità universitaria.

Strategia

Il presente Piano è da considerare una leva operativa del piano Strategico di Ateneo che si innesta sui tre macro-obiettivi strategici dell'Ateneo:

1. Semplificazione Amministrativa: Riduzione dei tempi di risposta e abbattimento della burocrazia cartacea attraverso il completamento del passaggio al Cloud dei sistemi gestionali e l'implementazione delle dematerializzazione dei documenti.
2. Innovazione Didattica: Supporto alle nuove metodologie pedagogiche (blended learning, realtà aumentata) tramite un'infrastruttura di rete resiliente e capillare in tutti i campus.
3. Valorizzazione del Patrimonio Informativo: Trasformazione del dato da sottoprodotto amministrativo ad asset strategico per il decision-making (Business Intelligence di Ateneo).

Inoltre, occorre considerare che l'Università degli Studi di Firenze opera in un contesto dove la competitività è strettamente legata alla maturità digitale. Il contesto strategico del 2026 presenta anche sfide esterne che richiedono un adattamento rapido:

- L'avvento dell'IT-Wallet: L'integrazione dei titoli di studio e delle identità digitali universitarie nel portafoglio digitale nazionale cambierà radicalmente il modo in cui i nostri studenti interagiscono con la PA e con le istituzioni estere (progetti Erasmus+ e European Student Card).
- Sovranità Digitale e Cloud: In linea con la strategia "Cloud First" della PA, UNIFI ha già migrato i servizi critici in logica SaaS e l'adozione di cloud certificati rimane la prima

opzione per tutti i nuovi progetti, ma è necessario valutare attentamente e caso per caso rispetto alla gestione dei dati per la ricerca e derivanti dalla ricerca.

- **Cyber Resilienza:** L'Università è un bersaglio sensibile. Il contesto strategico impone il passaggio a un modello che protegga la proprietà intellettuale della ricerca e i dati di migliaia di utenti, l'Ateneo presta particolare attenzione al percorso di adeguamento alla NIS2 e collabora con gli altri atenei, con la CRUI, il MUR e CODAU
- **Intelligenza Artificiale:** le evoluzioni degli strumenti rendono indispensabile considerare con priorità e attenzione il tema delle nuove tecnologie e in particolare il tema dell'intelligenza artificiale generativa. L'Ateneo si impegna a fornire a tutta la comunità degli strumenti conformi alle normative, accompagnando l'utenza con i necessari percorsi formativi

Il presente Piano, oltre a recepire le direttrici dettate da AgID, a tenere in considerazione le sfide derivanti dal contesto sia interno che esterno, è coordinato con i requisiti di Assicurazione della Qualità previsti per le Università (D.lgs. 19/2012 e s.m.i.), che definiscono un sistema di Autovalutazione, Valutazione ed Accredimento (AVA), disciplinato da successivi decreti, di cui il più recente è il D.M. 1154/2021, istitutivo del Sistema di assicurazione della qualità definito AVA 3.0.

In relazione al percorso di Trasformazione digitale sono previsti, nell'ambito B- Gestione delle Risorse del modello AVA 3.0, i seguenti Sottoambiti per i quali sono definiti specifici punti di attenzione misurati attraverso indicatori dedicati:

- **B.4 Attrezzature e tecnologie**
 - B.4.1 Pianificazione e gestione delle attrezzature e delle tecnologie
 - B.4.2 Adeguatezza delle attrezzature e delle tecnologie
 - B.4.3 Infrastrutture e servizi di supporto alla didattica integralmente o prevalentemente a distanza
- **B.5 Gestione delle informazioni e della conoscenza**
 - B.5.1 Gestione delle informazioni e della conoscenza

L'Ateneo, rispetto al sottoambito Attrezzature e tecnologie (B.4), ha previsto:

- B.4.1 - alla luce del processo di riorganizzazione in corso nel dicembre 2025, di istituire dei settori in grado di sostenere la strategia di gestione e manutenzione delle attrezzature e delle tecnologie a supporto delle proprie missioni e attività istituzionali e gestionali. Tali

settori hanno tra i propri compiti la gestione degli asset fisici e software del sistema IT.

- B.4.2 la verifica ciclica delle attrezzature e le tecnologie in uso per lo svolgimento delle attività al fine di renderle facilmente fruibili da docenti e studenti.
- B.4.3 Per le specifiche attività di supporto alla didattica integralmente o prevalentemente a distanza l'Ateneo ha costituito un Teaching learning center e previsto nell'assetto organizzativo il Settore Digital learning.

Rispetto al sottoambito B.5-Gestione delle informazioni e della conoscenza, il presente Piano costituisce il Documento di pianificazione di Ateneo sulla gestione delle informazioni e delle conoscenze.

Modello strategico

L'evoluzione del sistema informativo di Ateneo segue il "Modello Strategico" definito da AgID, strutturato per livelli, adattato alle specificità dell'ecosistema UniFi:

- **Infrastrutture:** L'Ateneo prosegue il percorso di razionalizzazione dei propri Data Center, adottando un approccio ibrido che combina risorse on-premise per dati sensibili di ricerca con servizi Cloud qualificati per le applicazioni gestionali e i servizi web, sfruttando le connettività ad alta capacità della rete GARR.
- **Piattaforme Abilitanti:** Piena integrazione con le piattaforme nazionali (SPID/CIE per l'accesso, PagoPA per i pagamenti delle tasse universitarie, App IO per le comunicazioni istituzionali). A queste si affiancano le piattaforme di dominio specifiche per l'Higher Education (sistemi di gestione carriere studenti ESSE3, piattaforme di e-learning Moodle, sistemi di gestione della ricerca IRIS).
- **Dati e Interoperabilità:** Implementazione del modello di interoperabilità tramite API, aderendo alla Piattaforma Digitale Nazionale Dati (PDND). Questo modello garantisce che i dati fluiscano in modo sicuro tra le strutture interne e verso l'esterno (Ministero, altri Enti), valorizzando il patrimonio informativo dell'Ateneo.
- **Sicurezza Informatica:** Un livello trasversale che permea tutti gli altri, con l'adozione di politiche di "Security by design e by default" per ogni nuovo servizio rilasciato, senza trascurare i sistemi on-premise e la necessità di un monitoraggio continuo al fine di identificare prima possibile azioni potenzialmente ostili.

Principi guida

I principi guida emergono dal quadro normativo e sono da tenere presenti ad ogni livello decisionale, e in ogni fase di implementazione, naturalmente contestualizzati secondo le specificità dell'Università degli Studi di Firenze.

I principi sono riassunti nella tabella seguente, con i relativi riferimenti normativi:

Principi guida	Definizioni	Riferimenti normativi
1. Digitale e mobile come prima opzione (<i>digital & mobile first</i>)	Le pubbliche amministrazioni devono erogare i propri servizi pubblici in digitale e fruibili su dispositivi mobili, considerando alternative solo in via residuale e motivata, attraverso la "riorganizzazione strutturale e gestionale" dell'ente ed anche con una "costante semplificazione e reingegnerizzazione dei processi"	Art.3-bis Legge 241/1990 Art.1 c.1 lett. a) D.Lgs. 165/2001 Art.15 CAD Art.1 c.1 lett. b) Legge 124/2015 Art.6 c.1 DL 80/2021
2. cloud come prima opzione (<i>cloud first</i>)	le pubbliche amministrazioni, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano prioritariamente il paradigma <i>cloud</i> e utilizzano esclusivamente infrastrutture digitali adeguate e servizi <i>cloud</i> qualificati secondo i criteri fissati da ACN anche nel quadro del SPC	Art.33-septies Legge 179/2012 Art. 73 CAD
3. interoperabile by design e by default (<i>API-first</i>)	i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e attraverso processi digitali collettivi, esponendo opportuni <i>e-service</i> , a prescindere dai canali di erogazione del servizio che sono individuati logicamente e cronologicamente dopo la progettazione dell'interfaccia API	Art.43 c.2 dPR 445/2000 Art.2 c.1 lett.c) D.Lgs 165/2001 Art.50 c2, art.50-ter e art.64-bis c.1-bis CAD
4. accesso esclusivo mediante identità digitale (<i>digital identity only</i>)	le pubbliche amministrazioni devono adottare in via esclusiva sistemi di identità digitale definiti dalla normativa	Art.64 CAD Art. 24, c.4, DL 76/2020 Regolamento EU 2014/910 "eIDAS"
5. servizi inclusivi, accessibili e centrati sull'utente (<i>user-centric</i>)	le pubbliche amministrazioni devono progettare servizi pubblici che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo	Legge 4/2004 Art.2 c.1, art.7 e art.53 CAD Art.8 c.1 lettera c) e lett.e), ed art.14 c.4-bis D.Lgs 150/2009

6. dati pubblici un bene comune (<i>open data by design e by default</i>)	il patrimonio informativo della Pubblica Amministrazione è un bene fondamentale per lo sviluppo del Paese e deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile	Art.50 c.1 e c,2-bis, art.50- quater e art.52 c.2 CAD D.Lgs 36/2006 Art.24-quater c.2 DL 90/2014
7. concepito per la sicurezza e la protezione dei dati personali (<i>data protection by design e by default</i>)	i servizi pubblici devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali	Regolamento EU 2016/679 "GDPR" DL 65/2018 "NIS" DL 105/2019 "PNSC" DL 82/2021 "ACN"
8. <i>once only</i> e concepito come transfrontaliero	le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite, devono dare accesso ai loro fascicoli digitali e devono rendere disponibili a livello transfrontaliero i servizi pubblici rilevanti	Art.43, art.59, art.64 e art.72 DPR 445/2000 Art.15 c.3, art.41, art.50 c.2 e c.2-ter, e art.60 CAD Regolamento EU 2018/1724 " <i>single digital gateway</i> " Com.EU (2017) 134 "EIF"
9. apertura come prima opzione (<i>openness</i>)	le pubbliche amministrazioni devono tenere conto della necessità di prevenire il rischio di <i>lock-in</i> nei propri servizi, prediligere l'utilizzo di <i>software</i> con codice aperto o di <i>e-service</i> e, nel caso di <i>software</i> sviluppato per loro conto, deve essere reso disponibile il codice sorgente, nonché promuovere l'amministrazione aperta e la condivisione di buone pratiche sia amministrative che tecnologiche	Art.9, art.17 c.1 ed art.68- 69 CAD Art.1 c.1 D.Lgs 33/2013 Art.30 D.Lgs 36/2023
10. sostenibilità digitale	le pubbliche amministrazioni devono considerare l'intero ciclo di vita dei propri servizi e la relativa sostenibilità economica, territoriale, ambientale e sociale, anche ricorrendo a forme di aggregazione	Art.15 c.2-bis CAD Art.21 D.lgs. 36/2023 Regolamento EU 2020/852 "principio DNSH"
11. sussidiarietà, proporzionalità e appropriatezza della digitalizzazione	I processi di digitalizzazione dell'azione amministrativa coordinati e condivisi sono portati avanti secondo i principi di sussidiarietà, proporzionalità e appropriatezza della digitalizzazione, ovvero lo Stato deve intraprendere iniziative di digitalizzazione solo se sono più efficaci di quelle a livello regionale e locale, e in base alle esigenze espresse dalle amministrazioni stesse, limitandosi negli altri casi a quanto necessario per il coordinamento informatico dei dati, e al tempo	Art.5, 117 e 118 Costituzione Art.14 CAD

	stesso le singole amministrazioni devono garantire l'appropriatezza delle iniziative di digitalizzazione portate avanti autonomamente, cioè in forma non condivisa con altri enti al livello territoriale ottimale rispetto alle esigenze preminenti dell'azione amministrativa e degli utenti dei servizi pubblici.	
--	--	--

Tabella 1 - Principi guida

Aggiornamenti Agid 2026

Le principali modifiche dell'aggiornamento 2026 riguardano:

- L'introduzione delle attività connesse alla realizzazione dell'AgID Academy;
- Il consolidamento del tema *IT-Wallet* nell'ambito delle piattaforme nazionali che erogano servizi a cittadini e imprese o altre PA, nel capitolo 4 – Piattaforme;
- L'aggiornamento delle tematiche connesse all'Intelligenza Artificiale;
- L'adeguamento dei contenuti sul tema del *cloud* alla normativa di settore;
- L'introduzione di sei nuovi strumenti per i quali si rimanda al [sito dell'AGID](#).



PARTE PRIMA – Componenti strategiche

Capitolo 1 - Organizzazione e gestione del cambiamento

L'ecosistema digitale amministrativo

L'ecosistema digitale amministrativo dell'Università di Firenze è l'insieme organico delle procedure, degli applicativi e delle competenze che permettono il funzionamento della macchina organizzativa. L'obiettivo per il triennio è superare la frammentazione dei sistemi legacy. L'ecosistema si sta evolvendo verso una "Amministrazione Digitale Integrata", dove i flussi documentali sono digitali (dal protocollo informatico alla conservazione a norma) e i processi di back-office evolvono verso l'automazione per liberare risorse umane da dedicare ad attività a maggior valore aggiunto. Fondamentale è l'integrazione tra le aree amministrative centrali e le strutture periferiche (Dipartimenti, Scuole, Centri), garantita da sistemi unificati che permettono una gestione trasparente e in tempo reale delle risorse finanziarie, umane e patrimoniali.

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

In ottemperanza all'art. 17 del CAD, il Responsabile per la Transizione al Digitale (RTD) dell'Università di Firenze è il perno della governance tecnologica e organizzativa. Non limitandosi a un ruolo tecnico, l'RTD opera in stretta sinergia con la Rettore, il Direttore Generale e gli Organi di Governo per garantire che gli investimenti ICT siano coerenti con gli obiettivi strategici e l'organizzazione dell'Ateneo.

Il Responsabile per la Transizione al Digitale si avvale dell'Ufficio per la Transizione al Digitale, che ha il compito di supportarlo:

- nella redazione del Piano triennale per la Transizione Digitale;
- ad assicurare il coordinamento dello sviluppo dei sistemi informativi, di telecomunicazione e di fonia;
- ad assicurare l'allineamento tra la programmazione dei sistemi informativi di Ateneo e lo sviluppo degli applicativi e delle piattaforme, forniti dal Consorzio CINECA;
- nello sviluppo di iniziative relative alla sicurezza informatica dell'Ateneo in stretta relazione con le Strutture competenti;
- nel contribuire al miglioramento dell'accessibilità degli strumenti digitali;
- nelle analisi periodiche sulla coerenza tra l'organizzazione e l'utilizzo delle tecnologie e dei

sistemi;

- nel progettare e coordinare iniziative cooperazione applicativa tra amministrazioni;
- nella pianificazione e coordinamento processo di diffusione tecnologie e sistemi (domicilio digitale, posta elettronica, protocollo informatico, firma digitale);
- nel pianificare e coordinare l'acquisto di soluzioni e sistemi informatici;
- nell'ottimizzare i processi amministrativi attraverso l'uso delle tecnologie e di applicativi;
- nella reingegnerizzazione dei processi interni;
- nelle iniziative di transizione digitale e di innovazione tecnologica (AI);
- nella diffusione e rafforzamento delle competenze digitali

Obiettivo 1.1 - Migliorare i processi di trasformazione digitale della PA

RA1.1.1 - Rafforzare la collaborazione e lo scambio di pratiche e soluzioni tra Amministrazioni

RA1.1.2 - Individuazione e diffusione di modelli organizzativi/operativi degli Uffici Transizione digitale, anche in forma associata

Linee di azione per le PA

RA1.1.1

Da gennaio 2026 - Le PA che partecipano alla *community* su ReTe Digitale incentrata sull'AI condividono pratiche, soluzioni e fabbisogni - Codice Linea di Azione: CAP1.PA.13

Attività Operative: l'Ufficio del Responsabile per la Transizione Digitale dell'Università di Firenze parteciperà con interesse alla neonata community dedicata all'Intelligenza Artificiale di AgID. I suoi membri si sono già iscritti alla nuova community di AgID.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale

RA1.1.2

Da marzo 2024 - Le PA partecipanti alle iniziative laboratoriali e che hanno adottato modelli organizzativi/operativi per l'Ufficio per la transizione digitale condividono le esperienze, gli strumenti sviluppati e i processi implementati - Codice Linea di Azione: CAP1.PA.04

Attività Operative: l'Ufficio del Responsabile per la Transizione Digitale dell'Università di Firenze ha partecipato attivamente alle iniziative laboratoriali avviate il 16 maggio del 2024 e prendendo parte ai due incontri del Laboratorio "MODELLI ORGANIZZATIVI/OPERATIVI

DELL'UFFICIO PER LA TRANSIZIONE AL DIGITALE" organizzati nel corso del 2024 e ha inviato la scheda di rilevazione UTD entro i termini, il giorno 03/09/2024. Il RTD ha partecipato e presentato una relazione sull'esperienza dell'Università di Firenze al ForumPA del 19/05/2025.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale

Da dicembre 2025 - Le PA partecipanti alle iniziative laboratoriali sperimentano i modelli e forniscono ad AgID il *feedback* sui nuovi modelli organizzativi/operativi dell'UTD adottati - Codice Linea di Azione: CAP1.PA.06

Attività Operative: l'ufficio del Responsabile per la Transizione Digitale dell'Università di Firenze continuerà a seguire, sperimentare, fornire feedback sui modelli adottati dall'Agenzia anche nel corso del 2026. I membri dell'Ufficio RTD si sono iscritti alla nuova Community di AgID, "Intelligenza Artificiale per la PA" e partecipano ai webinar formativi sul tema.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale

Competenze digitali per il Paese e per la PA

L'Università degli Studi di Firenze riconosce che la trasformazione digitale è anche un processo di trasformazione culturale. L'efficacia degli investimenti infrastrutturali descritti in questo Piano dipende direttamente dalla capacità delle persone di utilizzare consapevolmente i nuovi strumenti. Pertanto, l'Ateneo interpreta questo capitolo del Piano Triennale secondo una duplice direttrice: come Pubblica Amministrazione che deve qualificare il proprio personale e come Istituzione formativa che deve generare competenze per il Paese.

Per il personale tecnico-amministrativo, l'Università integra nel piano di formazione continua specifiche attività mirate ad accrescere le competenze digitali. L'obiettivo è colmare il divario tra le competenze digitali necessarie e quelle possedute, con lo scopo di accompagnare l'evoluzione dei ruoli professionali. Le azioni prioritarie riguardano:

- Sicurezza informatica: Corsi periodici sulla cybersecurity awareness per prevenire minacce (phishing, social engineering e tecniche di manipolazione in genere) e garantire la protezione dei dati e degli asset istituzionali.
- Gestione del dato: Formazione specifica sull'analisi dei dati e sull'uso consapevole delle informazioni disponibili, per favorire una cultura amministrativa data-driven.
- Lavoro Agile e Collaborativo: Consolidamento delle competenze sull'uso avanzato delle

piattaforme di collaborazione e condivisione, superando la logica del lavoro individuale.

Per il corpo docente l'Ateneo, attraverso il suo Teaching Learning Center, promuove percorsi di aggiornamento sull'integrazione delle tecnologie digitali nella didattica. Non si tratta solo di strumenti per l'erogazione di didattica a distanza, ma di metodologie per la didattica aumentata e ibrida (blended learning), e sull'uso etico dell'Intelligenza Artificiale Generativa come supporto all'apprendimento e alla ricerca.

Rispetto agli Studenti l'Università di Firenze ha la responsabilità di formare i futuri professionisti e cittadini digitali. Per questo l'Ateneo si impegna a inserire moduli di competenze digitali (base e avanzate) anche nei corsi di studio non STEM.

Obiettivo 1.2 - Diffusione competenze digitali nel Paese e nella PA

RA1.2.2 - Diffusione competenze digitali di base nella PA

Linee di azione per le PA

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 - Codice Linea di Azione: CAP1.PA.07

Attività Operative: L'Ateneo attiverà, come da piano della formazione di Ateneo, delle iniziative formative dedicate al miglioramento e aggiornamento continuo delle competenze digitali del personale. Inoltre, parteciperà a eventuali iniziative nazionali.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Direzione Generale, Area Persone e organizzazione/Settore Formazione, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Digital learning e formazione informatica

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 - Codice Linea di Azione: CAP1.PA.08

Attività Operative: L'Ateneo aderisce all'iniziativa «Syllabus per la formazione digitale» e promuove la partecipazione alle iniziative formative sulle competenze digitali di base da

parte dei propri dipendenti, 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.

Tempistiche di realizzazione e deadline: 31/12/26

Strutture responsabili: Ufficio per la Transizione al Digitale, Direzione Generale, Area Persone e organizzazione/Settore Formazione, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Digital learning e formazione informatica

Le PA, in funzione della propria missione istituzionale, realizzano iniziative per lo sviluppo delle competenze digitali dei cittadini previste dal PNRR e in linea con il Piano operativo della Strategia Nazionale per le Competenze Digitali - Codice Linea di Azione: CAP1.PA.09

Attività Operative: L'Ateneo realizza iniziative per lo sviluppo delle competenze digitali dei cittadini previste dal PNRR e in linea con il Piano operativo della Strategia Nazionale per le Competenze Digitali, anche nell'ambito del progetto ALMA-DEH.

Tempistiche di realizzazione e deadline: 31/12/26

Strutture responsabili: Ufficio per la Transizione al Digitale, Direzione Generale, Area Persone e organizzazione/Settore Formazione, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Digital learning e formazione informatica.

RA1.2.2

Da ottobre 2025 – 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 - Codice Linea di Azione: CAP1.PA.14

Attività Operative: il RTD ed il personale afferente al suo Ufficio parteciperanno con interesse alle iniziative che verranno promosse da AgID sul tema cruciale dell'Intelligenza Artificiale. I membri dell'Ufficio RTD si sono iscritti alla nuova Community di AgID, "Intelligenza Artificiale per la PA" e partecipano ai webinar formativi sul tema.

Tempistiche di realizzazione e deadline: 31/12/26

Strutture responsabili: Ufficio per la Transizione al Digitale

Capitolo 2 - Il procurement per la trasformazione digitale

Il *procurement* per la trasformazione digitale

Scenario

Con l'entrata in vigore del nuovo Codice dei Contratti pubblici (il Decreto legislativo 36/2023) prima e con l'introduzione del cosiddetto "Correttivo" (il Decreto legislativo 209/2024, "Disposizioni integrative e correttive al codice dei contratti pubblici, di cui al decreto legislativo 31 marzo 2023, n.36") poi, la Pubblica Amministrazione sta andando verso la creazione di un sistema organico di e-procurement che investa tutti gli aspetti e le fasi del ciclo di vita del contratto pubblico. Più nello specifico, la Parte II del Libro I del Codice, intitolata "Della digitalizzazione del ciclo di vita dei contratti", ha introdotto un profondo percorso di trasformazione digitale degli acquisti della Pubblica Amministrazione, volto alla semplificazione, alla velocizzazione delle procedure e atto a garantire una maggiore trasparenza degli acquisti.

Il Dlgs 209/2024 -c.d. "Corretivo" ha apportato alcune modifiche, fra l'altro , proprio ad alcuni articoli di detta Parte II con l'obiettivo di rendere più efficace la digitalizzazione del ciclo di vita dei contratti pubblici.

In questo senso possono essere lette:

- le modifiche fatte all'art 24- Fascicolo Virtuale dell'Operatore Economico (FVOE)- secondo le quali è stato previsto che l'interoperabilità fra le banche dati che alimentano la Banca dati nazionale dei contratti pubblici (BDNCP), di cui l'FVOE è una sezione, e la BDNCP stessa non può essere vanificata dalle disposizioni che regolamentano le prime;
- la nuova formulazione dell'art 26" Regole tecniche", dalla cui lettura emerge una rinnovata attenzione a che la digitalizzazione sia accompagnata dalla sicurezza informatica - (art. 26)
- l'estensione anche alle stazioni appaltanti della possibilità di segnalare ad AgID le eventuali omissioni presenti in tema di informazioni o attività necessarie a garantire l'interoperabilità dei dati.

Infine, sempre nell'ottica della digitalizzazione, il correttivo ha confermato l'obbligo di utilizzare, a far data dal 1° gennaio 2025, gli strumenti di gestione informativa digitale delle costruzioni (cd. GID) di cui il sistema BIM, già introdotto dal Codice 50/2016, costituisce il

cuore operativo.

A tale proposito, si segnala che il correttivo ha innalzato a 2 milioni di euro la soglia di obbligatorietà per l'adozione degli strumenti di progettazione e gestione dell'opera pubblica sopra richiamati, con la sola esclusione degli interventi di manutenzione ordinaria e straordinaria, a meno che non riguardino opere già digitalizzate, mentre per i beni culturali (ai sensi del D.Lgs. 42/2004) l'adozione degli strumenti è obbligatoria qualora l'importo superi i 5.382.000 euro.

Gli acquisti di beni e servizi standardizzati

L'esigenza di razionalizzare gli acquisti, anche in ambito ICT, mediante una loro aggregazione e centralizzazione, al fine di monitorare in maniera puntuale le esigenze della singola amministrazione e di conseguire economie di scala stipulando contratti più vantaggiosi, riducendo il fenomeno della frammentazione degli acquisti, è molto sentito dall'Università di Firenze. La sua complessa articolazione policentrica e le peculiari richieste di acquisto che possono arrivare, per motivi di didattica e di ricerca, rende difficoltoso ridurre la suddetta frammentazione.

Tuttavia, al di là degli acquisti ICT volti al soddisfacimento di specifiche esigenze legate al mondo della ricerca che sono effettuati direttamente dalle strutture interessate, l'Ateneo tramite la propria Area ICT (Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici) centralizza gli acquisti avvalendosi, quando possibile, degli strumenti di aggregazione messi a disposizione dal mercato quali: adesione a contratti stipulati dalla Conferenza dei Rettori delle Università Italiane (CRUI) per le Università ad essa aderenti, o ad Accordi/Convenzioni quadro della centrale di committenza nazionale (Consip) o regionale (START); quando tali opportunità non sono presenti, l'Area in questione svolge comunque le funzioni di programmazione, progettazione, affidamento ed esecuzione delle risorse informatiche destinate alla collettività universitaria nel suo complesso.

Coerentemente con il dettato normativo di cui all'art.25 del D. Lgs 36/2023, gli acquisti in area ICT e non solo avvengono tramite l'utilizzo delle PAD (Piattaforme di Acquisto Digitale) quali MEPA, START e U-Buy, adottata nel corso del 2025 solo dall'area ICT per affidamenti in house al Consorzio CINECA proprietario della piattaforma in oggetto.

Con l'obiettivo di consentire la gestione integrata dell'intero ciclo di acquisto è allo studio di

CINECA il rilascio di una nuova versione che verrà testata nel corso del 2026 e, se le verifiche avranno esito positivo, sarà valutata l'adozione per tutte le strutture di Ateneo.

L'ecosistema digitale degli acquisti pubblici

Come previsto dalla Parte II del Libro I del Codice dei contratti pubblici, rubricata "Digitalizzazione del ciclo di vita dei contratti pubblici", dal primo gennaio 2024 è obbligatorio, per la Pubblica Amministrazione, effettuare gli acquisti attraverso le piattaforme di approvvigionamento digitale rese interoperabili con la Banca dati nazionale dei contratti pubblici (BDNCP) di ANAC tramite Piattaforma Digitale Nazionale dei Dati (PDND). La PDND costituisce, dunque, l'infrastruttura tecnologica abilitante per la gestione di tutte le fasi del ciclo di vita dei contratti pubblici (programmazione, progettazione, affidamento e esecuzione). Tale sistema informativo distribuito è definito dal Codice dei contratti pubblici "Ecosistema nazionale di approvvigionamento digitale" (art. 22).

In tale contesto, la PDND è centrale anche perché costituisce lo snodo per l'accesso agli e-service di ANAC, che abilitano l'operatività del ciclo di vita del *procurement*.

La qualificazione della Stazione appaltante

La qualificazione delle Stazioni appaltanti è uno strumento per attestare la capacità di gestire direttamente il ciclo di vita dei contratti pubblici secondo criteri di qualità, efficienza e professionalizzazione e nel rispetto dei principi di economicità, efficacia, tempestività e correttezza.

Nel sistema disegnato dalla versione originaria del Codice, la qualificazione era prevista per la sola fase di progettazione ed affidamento delle commesse pubbliche ed era articolata su tre livelli crescenti di qualificazione definiti all'art 63 e precisamente:

- I. qualificazione base, per servizi e forniture fino alla soglia di 750.000 euro e lavori fino a un milione di euro;
- II. qualificazione intermedia, per servizi e forniture fino a 5 milioni di euro e per lavori fino alle soglie di cui all'art 14 (soglie di rilevanza europea, dal 1° gennaio 2024 pari a 5.538.000,00 euro);
- III. qualificazione avanzata, senza limiti di importo.

Il Correttivo del 2024 ha modificato l'art 63 prevedendo l'estensione dell'obbligo di

qualificazione delle Stazioni Appaltanti (S.A.) anche alla fase esecutiva, completando in tal modo il disegno organico di riforma dell'intero ciclo dell'appalto: programmazione, progettazione, affidamento ed esecuzione.

L'obiettivo dichiarato dal legislatore è quello di innalzare il livello di competenza, efficienza e trasparenza nell'attuazione del public procurement, in linea con i principi fondamentali del Codice e gli impegni assunti nel quadro del PNRR. L'Università di Firenze in data 27/06/2025 ha acquisito la certificazione di livello massimo sia per i lavori che per servizi e forniture anche per la fase di esecuzione che si aggiunge allo stesso livello di qualificazione ottenuto per la fase di affidamento.

L'allegato II.14 del suddetto Codice, all'art. 32, stabilisce che sono considerati servizi di particolare importanza le prestazioni di importo superiore a 500.000 euro e, indipendentemente dall'importo: gli interventi particolarmente complessi sotto il profilo tecnologico, le prestazioni che richiedono l'apporto di una pluralità di competenze, gli interventi caratterizzati dall'utilizzo di componenti o di processi produttivi innovativi o dalla necessità di elevate prestazioni per quanto riguarda la loro funzionalità.

In via di prima applicazione del Codice possono essere individuati, tra i servizi di particolare importanza, quelli di telecomunicazione ed i servizi informatici.

È, quindi, sempre fortemente auspicabile che il Responsabile della transizione al digitale venga coinvolto negli acquisti ICT e per la transizione digitale.

Obiettivo 2.1 - Rafforzare l'ecosistema nazionale di approvvigionamento digitale

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

Obiettivo 2.2 - Diffondere l'utilizzo degli appalti innovativi

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

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

Linee di azione per le PA

RA2.1.1

Giugno 2025 * - Le stazioni appaltanti devono digitalizzare la fase di esecuzione dell'appalto

- Codice Linea di Azione: CAP2.PA.02

Attività Operative: L'Ateneo è attualmente impegnato sul fronte della digitalizzazione dell'intera fase di esecuzione dei contratti la quale, tuttavia, rimane condizionata dal conseguimento della piena operatività delle soluzioni tecnologiche messe a disposizione da soggetti istituzionali coinvolti dei quali si avvale.

Tempistiche di realizzazione e deadline: 31/12/26

Strutture responsabili: Tutte le strutture

RA2.2.1

Da dicembre 2026 - Le amministrazioni entrano nel programma delle consultazioni di mercato - Codice Linea di Azione: CAP2.PA.08

Attività Operative: L'Università, qualora coinvolta, parteciperà al programma.

Tempistiche di realizzazione e deadline: 31/12/26

Strutture responsabili: Tutte le strutture

Le gare strategiche per la trasformazione digitale

Scenario

Le gare strategiche ICT gestite da Consip sono strumenti che consentono alle Amministrazioni di acquisire servizi necessari ad implementare le strategie per la trasformazione digitale della Pubblica Amministrazione. In generale, quindi, sono disponibili servizi per operare sulla definizione di processi e sull'erogazione di servizi digitali, sulla analisi e realizzazione delle componenti applicative e infrastrutturali, con specifico riferimento al paradigma cloud.

Tali gare mirano a garantire contratti di elevata standardizzazione e qualità con il duplice obiettivo di:

- creare il "sistema operativo" del Paese, ovvero una serie di componenti fondamentali sui quali definire ed erogare servizi più semplici ed efficaci per i cittadini, le imprese e la stessa Pubblica Amministrazione
- incentivare l'utilizzo e supportare le amministrazioni nella definizione di contratti coerenti con gli obiettivi definiti dal Piano triennale.

Linee di azione per le PA



RA2.3.1

Da settembre 2025 - Le PA programmano i fabbisogni di adesione alle iniziative strategiche per il perseguimento degli obiettivi del Piano triennale per l'anno 2026 - Codice Linea di Azione: CAP2.PA.05

Attività Operative: L'Università, anche in ottemperanza all'obbligo di utilizzo di convenzioni e accordi quadro Consip, verifica prima di ogni acquisto la disponibilità di iniziative strategiche in grado di soddisfare le necessità.

Tempistiche di realizzazione e deadline: 31/12/26

Strutture responsabili: Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici



PARTE SECONDA – Componenti tecnologiche

Capitolo 3 - Servizi

Negli ultimi anni, la digitalizzazione ha assunto un ruolo cruciale nell'innovazione dei servizi pubblici, ponendo la PA al centro di un processo di trasformazione indefettibile. L'impiego di tecnologie digitali risulta fondamentale per ottimizzare le prestazioni, aumentare la trasparenza e assicurare la qualità dei servizi. A tale scopo, è necessario stabilire un quadro di riferimento che guidi e standardizzi le scelte tecnologiche, con particolare attenzione all'architettura a microservizi, la quale offre flessibilità e scalabilità, semplificando i processi digitali e agevolando la gestione del cambiamento nelle organizzazioni governative locali. In questo contesto, il modello di interoperabilità sta evolvendo in modo sensibile, passando dalla condivisione dei soli dati alla condivisione dei servizi a scala nazionale ed europea per arrivare poi ad avere strumenti come l'IT-Wallet e l'UE-Wallet.

L'adozione dell'architettura a microservizi consente di beneficiare delle soluzioni e dei servizi già esistenti, riducendo la duplicazione degli sforzi e dei costi ed innovando profondamente il concetto di riuso. Inoltre, la condivisione di e-service, attraverso la Piattaforma Digitale Nazionale Dati Interoperabilità (PDND), favorisce un utilizzo più efficiente delle risorse.

I vantaggi dell'utilizzo di un'architettura basata su microservizi sono:

- flessibilità e scalabilità;
- agilità nello sviluppo;
- integrazione semplificata;
- resilienza e affidabilità.

Permette la condivisione dei processi e lo sviluppo *once only*, riduce la duplicazione degli sforzi e dei costi. La condivisione di e-service vede nella PDND la base fondante per la condivisione di dati e processi.

E-Service in interoperabilità tramite PDND

Scenario

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

Il decreto-legge 31 maggio 2021, n. 77, recante “Governance del Piano nazionale di rilancio e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure”, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108, ha individuato nella Piattaforma Digitale Nazionale Dati lo strumento per attuare il principio dell’interoperabilità dei dati delle pubbliche amministrazioni, estendendone ulteriormente l’ambito di operatività. Il Decreto del 05/12/2023, emanato dal Dipartimento per la Trasformazione Digitale, ha messo in evidenza che l’adesione alla PDND fornisce alle pubbliche amministrazioni l’occasione per rendere disponibili i dati di rispettiva competenza ed in particolare, per fruire esse stesse dei dati in possesso di altri soggetti pubblici, al fine di migliorare le proprie procedure interne e di erogare servizi integrati e innovativi a cittadini ed imprese, attuando nel contempo un’opera di semplificazione dei propri sistemi informativi e di razionalizzazione delle proprie basi di dati.

Essa è lo strumento per gestire l’autenticazione, l’autorizzazione, la raccolta e la conservazione delle informazioni relative agli accessi e alle transazioni effettuate per suo tramite. La Piattaforma fornisce un insieme di regole condivise per semplificare gli accordi di interoperabilità, snellendo i processi di istruttoria, riducendo oneri e procedure amministrative. Un ente può aderire alla Infrastruttura interoperabilità PDND siglando un accordo di adesione, attraverso le funzionalità messe a disposizione dell’infrastruttura. Grazie al nuovo Modello di Interoperabilità, sul quale poggia il Piano triennale, le pubbliche amministrazioni possono collaborare tra di loro e con terze parti attraverso soluzioni tecnologiche che facilitano l’interazione e lo scambio di dati senza vincoli particolari sul modo in cui sono implementate. Questo consente di:

- sviluppare nuove applicazioni per gli utenti del settore pubblico;
- garantire, nel rispetto della privacy, l’accesso ai dati delle Pubbliche Amministrazioni anche a soggetti terzi.

L’Ateneo, quindi, dovrà adottare gli standard tecnologici per implementare i modelli e gli schemi proposti nel Modello nazionale di Interoperabilità, che permette di definire e rendere disponibili API che rispettino gli standard comuni, anche a livello europeo.

La realizzazione della PDND nell’ambito del PNRR è finalizzata a garantire la completa interoperabilità dei dataset e dei servizi chiave tra le varie amministrazioni, oltre che a valorizzare il patrimonio informativo pubblico.

La PDND permette alle amministrazioni di pubblicare *e-service* conformi alle Linee guida realizzati ed erogati attraverso l'implementazione di API (*Application Programming Interface*). Le API esposte vengono registrate e popolano il Catalogo pubblico degli *e-service*. La Piattaforma è una componente fondamentale del cosiddetto ecosistema di interoperabilità e rappresenta lo strumento primario per gestire l'identificazione, l'autorizzazione ed il monitoraggio dei soggetti autorizzati all'erogazione e fruizione degli *e-service*, garantendo così la protezione e l'integrità dei dati. Il suo obiettivo è stabilire norme comuni per favorire gli accordi di interoperabilità, semplificando i processi di verifica e riducendo l'onere burocratico.

La PDND offre un Catalogo di API, che elenca tutti i servizi digitali resi disponibili dagli enti pubblici e tramite il quale è possibile richiedere l'accesso ai dati, per integrarli poi nei propri servizi destinati ai cittadini.

La piattaforma offre diversi vantaggi:

- Gli enti che forniscono servizi digitali hanno la garanzia di uno scambio sicuro dei dati e una standardizzazione dei processi.
- Gli enti possono accedere al catalogo dei servizi digitali disponibili e integrare le API nei propri servizi rivolti ai cittadini e alle imprese.
- I professionisti che sviluppano e gestiscono i servizi digitali di un'istituzione possono effettuare integrazioni standardizzate grazie alla piattaforma.
- I responsabili della protezione dei dati delle istituzioni partecipanti possono accedere a documenti amministrativi standard e garantire un processo uniforme per tutte le istituzioni coinvolte.
- Le imprese e i cittadini possono beneficiare del principio "once only", evitando di dover fornire informazioni già comunicate in precedenza alle istituzioni pubbliche.

L'Ateneo ha ricevuto il finanziamento PNRR per la Misura 1.3.1 "Piattaforma Digitale Nazionale Dati -Università e AFAM pubblici - luglio 2023", si è attivato con il consorzio interuniversitario Cineca, grazie al quale ha implementato dodici servizi agli studenti attraverso il notification manager.

Obiettivo 3.1 - Migliorare la capacità di erogare *e-service*

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

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

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

Linee di azione per le PA

RA3.1.1

Da gennaio 2024 - Le PA cessano di utilizzare modalità di interoperabilità diverse da PDND per le nuove implementazioni - Codice Linea di Azione: CAP3.PA.01

Attività Operative: L'Ateneo, quando e se applicabile, per le nuove implementazioni e quando operativamente possibile, cessa di utilizzare modalità di interoperabilità diverse da PDND.

Tempistiche di realizzazione e deadline: 31/12/26

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Servizi digitali.

Da gennaio 2024 - Le Amministrazioni possono iniziare la migrazione dei servizi erogati in interoperabilità dalle attuali modalità alla PDND - Codice Linea di Azione: CAP3.PA.02

Attività Operative: L'Ateneo, quando e se applicabile, valuta la migrazione dei servizi erogati in interoperabilità dalle attuali modalità alla PDND.

Tempistiche di realizzazione e deadline: 31/12/26

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Servizi digitali.

Da gennaio 2024 - Le PA continuano a popolare il Catalogo delle API della Piattaforma Digitale Nazionale Dati con le API conformi alle "Linee guida sull'interoperabilità tecnica delle pubbliche amministrazioni" - Codice Linea di Azione: CAP3.PA.03

Attività Operative: L'Ateneo, quando e se applicabile, popola il Catalogo delle API della PDND con le API conformi alle "Linee guida sull'interoperabilità tecnica delle pubbliche amministrazioni".

Tempistiche di realizzazione e deadline: 31/12/26

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Servizi digitali.

Da gennaio 2024 - Le PA locali rispondono ai bandi pubblicati per l'erogazione di API su PDND - Codice Linea di Azione: CAP3.PA.04

Attività Operative: L'Ateneo, quando e se applicabile, risponde ai bandi pubblicati per l'erogazione di API su PDND.

Tempistiche di realizzazione e deadline: 31/12/26

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Servizi digitali.

RA3.1.2

Da gennaio 2024 - Le PA utilizzano le API presenti sul Catalogo - Codice Linea di Azione: CAP3.PA.06

Attività Operative: L'Ateneo, quando e se applicabile, utilizza le API presenti sul Catalogo.

Tempistiche di realizzazione e deadline: 31/12/26

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Servizi digitali.

Da luglio 2025 - Le PA effettuano richieste di fruizione di servizi erogati da privati - Codice Linea di Azione: CAP3.PA.07

Attività Operative: L'Ateneo, quando e se applicabile, effettua richieste di fruizione di servizi erogati da privati.

Tempistiche di realizzazione e deadline: 31/12/26

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Servizi digitali.

RA3.1.3

Da gennaio 2024 - 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 - Codice Linea di Azione: CAP3.PA.08

Attività Operative: L'Ateneo, quando e se applicabile, partecipa alla definizione di *pattern* e profili di interoperabilità per l'aggiornamento delle "Linee guida sull'interoperabilità tecnica

delle pubbliche amministrazioni”.

Tempistiche di realizzazione e deadline: 31/12/26

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici.

Progettazione dei servizi: accessibilità e *design*

Scenario

Il Responsabile per la Transizione Digitale (RTD), in sinergia con Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici e l'Area Gestione progetti strategici, terza missione e comunicazione, coordina la semplificazione dei processi e l'erogazione dei servizi nel pieno rispetto del CAD (accessibilità, privacy e gestione dati).

L'Ateneo considera l'abbattimento delle barriere digitali un dovere morale e una missione prioritaria per garantire equità d'accesso a tutti gli utenti.

Pertanto l'impegno nel miglioramento dell'accessibilità di ambienti digitali e dei servizi per gli utenti con limitazioni funzionali sarà rivolto alla:

- **Formazione dei redattori dei siti:** per garantire uniformità qualitativa e competenza tecnica su tutta la rete web di Ateneo. In particolare migliorare i testi alternativi alle immagini.
- **Accessibilità dei documenti amministrativi:** per assicurare che ogni atto prodotto sia nativamente fruibile da persone con disabilità.

Inoltre, in ottemperanza alla normativa vigente e nel rispetto di quanto stabilito dal Piano triennale, l'Ateneo:

- pubblica ogni anno, entro le scadenze previste, i propri obiettivi di accessibilità e le proprie dichiarazioni di accessibilità per sito web e APP mobile istituzionali;
- conferma l'adeguamento agli standard Web Content Accessibility Guidelines WCAG 2.1 per il portale istituzionale, i siti tematici e i corsi di studio;
- monitora i propri servizi attraverso [Web Analytics Italia](#), una piattaforma nazionale *open source* che offre rilevazioni statistiche su indicatori utili al miglioramento continuo dell'esperienza utente.

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

RA3.2.2 - Incremento dell'accessibilità dei servizi digitali

Linee di azione per le PA

RA3.2.2

Marzo 2026 - Le PA pubblicano gli obiettivi di accessibilità sul proprio sito *web* - Codice Linea di Azione: CAP3.PA.15

Attività Operative: L'Ateneo pubblicherà gli obiettivi entro la scadenza.

Tempistiche di realizzazione e deadline: 31/03/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, UF Comunicazione interna e Intranet.

Settembre 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 - Codice Linea di Azione: CAP3.PA.16

Attività Operative: L'Ateneo pubblicherà la dichiarazione dopo aver ricevuto il report di valutazione delle proprie app e siti web dal Consorzio Cineca, che li gestisce per suo conto.

Tempistiche di realizzazione e deadline: 23/09/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, UF Comunicazione interna e Intranet.

Formazione, gestione e conservazione dei documenti informatici

Scenario

Il tema della dematerializzazione degli archivi cartacei risulta cruciale affinché le amministrazioni possano conseguire i propri obiettivi di digitalizzazione.

Le nuove "Linee guida sulla formazione, gestione e conservazione dei documenti informatici" redatte da AgID nel maggio 2021 ed entrate in vigore il primo gennaio 2022 assumono particolare rilevanza in materia. Le pubbliche amministrazioni formano i loro documenti in conformità ad esse, che hanno carattere vincolante e sono efficaci erga omnes in quanto atto di regolamentazione di natura tecnica; contengono i necessari adeguamenti organizzativi e funzionali richiesti alle pubbliche amministrazioni e vanno ad affiancare la Legge 7 agosto 1990, n. 241, "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi", il Decreto del Presidente della Repubblica 28

dicembre 2000, n.445, “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (TUDA) ed il Decreto Legislativo 82/2005, “Codice dell’amministrazione digitale” (CAD).

Le Linee guida costituiscono la premessa fondamentale dell’agire amministrativo in ambiente digitale, in attuazione degli obiettivi di semplificazione, trasparenza, partecipazione e di economicità, efficacia ed efficienza, già prescritti dalla Legge n.241/1990, assicurando la corretta impostazione metodologica per la loro realizzazione nel complesso percorso di transizione digitale.

La pubblica amministrazione è tenuta ad assicurare la rispondenza alle suddette Linee guida, adeguando i propri sistemi di gestione informatica dei documenti, al fine di garantire effetti giuridici conformi alle stesse nei processi documentali, nonché ad ottemperare alle seguenti misure:

- corretta gestione dei documenti;
- corretta gestione dei flussi documentali,
- nomina dei responsabili preposti;
- adozione del Manuale di gestione documentale e del Manuale di conservazione;
- pubblicazione delle nomine dei Responsabili e dei Manuali in una sezione chiaramente identificabile dell’area “Amministrazione trasparente”, come previsto dall’art. 9 del 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”;
- rispetto delle “Misure minime di sicurezza ICT per le pubbliche amministrazioni”, emanate da AGID con la Circolare n. 2/2017;
- rispetto di quanto prescritto in materia di protezione dei dati personali del Regolamento 2016/679/UE, “Regolamento generale sulla protezione dei dati” (GDPR);
- versamento dei documenti al sistema di conservazione.

La responsabilità dell’Archivio e del trattamento degli atti viene attribuita dal Direttore Generale al Responsabile della Gestione documentale, il quale deve essere in possesso di idonee competenze giuridiche, informatiche ed archivistiche. Si occupa della gestione dei processi e dei flussi documentali, oltre ad assistere l’attività di protocollazione delle UOR, supportare le richieste provenienti dagli organi monocratici dell’Università, quali la Rettrice e

il Direttore Generale.

La struttura generale di funzionamento del Sistema Archivistico di Ateneo, come previsto nel Regolamento vigente, mira alla dematerializzazione nei procedimenti amministrativi, così da rendere virtuale la separazione logistica delle tre fasi temporali di vita del documento.

Attualmente il suddetto Sistema opera, però, in una modalità di gestione documentale ibrida, poiché all'interno della stessa pratica amministrativa possono convivere una componente analogica ed una digitale; ciò genera una serie di criticità nella produzione e nella conservazione delle pratiche, come:

- la necessità di archiviare e di conservare correttamente sia i documenti cartacei che quelli digitali;
- la gestione della logistica che la conservazione di documenti analogici comporta;
- la previsione di una nuova fase di adeguamento alla normativa nazionale per la gestione digitale della documentazione amministrativa.

Per sviluppare progetti di transizione digitale che siano efficaci per la gestione amministrativa documentale bisogna partire dagli archivi digitali, che sono indispensabili per garantire certezza e affidabilità della conservazione documentale nel tempo.

L'archivio digitale rappresenta un avamposto fondamentale per poter sviluppare progetti di trasformazione digitale: garantisce la corretta gestione documentale dell'intera mole di atti e documenti prodotti dall'Università nello svolgimento delle proprie attività, nonché la certezza e l'affidabilità della conservazione documentale a norma, come richiesto dalla normativa nazionale, nel tempo.

Dopo aver investito molto sulla corretta fascicolazione dei documenti, attività che è stata posta come obiettivo dirigenziale trasversale del 2025 e che ha visto come protagonisti i referenti di ogni struttura di Ateneo (che sono stati appositamente consultati per individuare i flussi ed i processi ed opportunamente formati per garantire l'uniformità dei principi che dovrebbero guidare le attività di archiviazione documentale d'ora in avanti), l'Ateneo continuerà con le attività a supporto della dematerializzazione documentale, valutando ulteriori misure che vengano ritenute necessarie, come l'attivazione di nuovi sistemi di flusso documentale o iter approvativi. Saranno, inoltre, definite ulteriori procedure per la dematerializzazione di processo e si continuerà con il processo di monitoraggio per il corretto utilizzo dei sistemi di identità e firma digitale.

Le funzioni legate alle attività relative ai processi e ai flussi documentali, che vanno ad alimentare l'archivio corrente di Ateneo, si svolgono prevalentemente attraverso il gestionale del protocollo informatico (Titulus) e riguardano:

- la correttezza delle operazioni di registrazione, segnatura, gestione dei documenti;
- le richieste di annullamento delle registrazioni di protocollo avanzate dalle unità organizzative responsabili (UOR).

L'Ateneo è organizzato come un'Area Organizzativa Omogenea unica (AOO) dotata di una gestione documentale unitaria e coordinata del protocollo, alla quale rispondono le diverse Unità Organizzative Responsabili (UOR) esistenti. L'Università ha scelto di adottare nel 2019 un modello di "protocollo diffuso", progettato nel 2018 anche con il concorso del personale del Sistema Informatico dell'Ateneo Fiorentino (SIAF), all'interno del quale la protocollazione (corrispondenza e pubblicazione nell'Albo Ufficiale) viene effettuata prevalentemente dalle diverse unità organizzative responsabili (UOR); ciò ha modificato profondamente il funzionamento del flusso documentale, decentrando la gestione della posta in entrata. Nei servizi connessi al gestionale del protocollo (Titulus), svolge un ruolo fondamentale l'Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici la quale, con due unità di personale dedicato, cura l'assistenza tecnica agli utenti interni e si interfaccia con CINECA (il gestore di Titulus), per tutte le criticità che riguardano il suo funzionamento. In particolare, l'Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici si occupa dell'aggiornamento del database e del gestionale di protocollo, dell'abilitazione degli utenti e dei loro livelli di accesso ad esso. L'attività sul gestionale del protocollo rappresenta la gestione dell'Archivio digitale delle pratiche prodotte dall'Ateneo.

La stesura del Manuale di gestione documentale è avvenuta con il contributo del gruppo di lavoro costituito presso l'Ufficio del RDT ed il vaglio di tutte le Aree dell'Ateneo, le quali hanno revisionato ed integrato il testo in base all'organizzazione delle proprie procedure documentali vigenti. Il Manuale è stato completato nel dicembre del 2021 e adottato in via definitiva il 10 febbraio 2022, rispettando uno degli adempimenti previsti dalle direttive dell'Agenzia per l'Italia Digitale per tutte le amministrazioni pubbliche e private. È uno strumento utile per descrivere in dettaglio la produzione documentale dell'ente, ma necessita di integrazioni e revisioni periodiche per poter rispondere al meglio ai cambiamenti in atto.

Obiettivo 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 per le PA

RA3.3.1

Dal primo gennaio 2022 sono entrate in vigore le Linee guida sulla formazione, gestione e conservazione dei documenti informatici. Oltre al rispetto della normativa previgente le amministrazioni sono tenute a rispettare quanto previsto dalle suddette Linee guida.

Giugno 2025 - 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 - Codice Linea di Azione: CAP3.PA.17

Attività Operative: Il "Manuale di gestione documentale dell'Università degli studi di Firenze", redatto nel corso del 2021 ed adottato ufficialmente il 10/02/2022, è attualmente pubblicato tra i contenuti della pagina dedicata al Sistema Archivistico di Ateneo, alla quale si accede attraverso un link dalla pagina Intranet "Gestione documentale e archivi" chiamata "Conservazione documentale". Il suddetto Manuale descrive il sistema di produzione e di gestione di documenti (analogici e digitali) dell'Università ed è una guida per l'operatore di protocollo per porre in essere le corrette operazioni di gestione documentale. Non è attualmente pubblicato sulla pagina "Amministrazione trasparente" del sito di Ateneo: a tal fine se ne ipotizza l'inserimento all'interno della sezione "Altri contenuti", così da essere in linea con la normativa vigente. Non risulta al momento presente la nomina del Responsabile della gestione documentale. Al fine della corretta individuazione della figura preposta, l'Università è stata considerata un'unica Area Organizzativa Omogenea unica (AOO) con una gestione documentale unitaria e coordinata del protocollo, alla quale rispondono le diverse Unità Organizzative Responsabili (UOR) esistenti.

Tempistiche di realizzazione e deadline: 30/06/2025

Strutture responsabili: Area per la Valorizzazione del Patrimonio Culturale/Sistema Archivistico di Ateneo



Giugno 2026 - Le PA devono verificare che in “Amministrazione trasparente” sia pubblicato il Manuale di conservazione e la nomina del Responsabile della conservazione - Codice Linea di Azione: CAP3.PA.18

Attività Operative: In attesa di descrivere i processi, l'organizzazione e le diverse tipologie di oggetti sottoposti a conservazione, per supplire alla mancanza di un Manuale di conservazione di Ateneo, si fa riferimento:

- al Manuale di Conservazione di Telecom Italia Trust Technologies per gli accordi di versamento in conservazione dei verbali relativi agli esami di profitto e delle tesi di laurea;
- al Manuale di Conservazione di CINECA per gli accordi di versamento in conservazione del registro informatico di protocollo giornaliero, dei vari repertori a tenuta illimitata, dei registri IVA, degli ordinativi e delle fatture attive (verso privati e PA) e passive.

Tempistiche di realizzazione e deadline: 30/06/2026

Strutture responsabili: Area per la Valorizzazione del Patrimonio Culturale/Sistema Archivistico di Ateneo, Responsabile per la Conservazione, Funzioni direzionali/Unità di Processo Prevenzione della Corruzione e Trasparenza

Capitolo 4 - Piattaforme

Il Piano triennale prende in esame l'evoluzione delle piattaforme della Pubblica Amministrazione, che offrono funzionalità fondamentali nella digitalizzazione dei processi e dei servizi della PA.

Le piattaforme nazionali che forniscono servizi a cittadini e imprese, includono pagoPA, Applo, SEND, SPID e CIE. L'obiettivo comune di tutte queste piattaforme è migliorare i servizi già esistenti.

Le Piattaforme rappresentano soluzioni chiave per la digitalizzazione dei processi amministrativi delle Pubbliche Amministrazioni, offrendo funzionalità fondamentali e trasversali che standardizzano la modalità di erogazione dei servizi. Queste soluzioni permettono alle amministrazioni di evitare lo sviluppo da zero di nuove funzionalità, riducendo così i tempi e i costi di implementazione, oltre a garantire una maggiore sicurezza informatica.

Attraverso l'adozione delle Piattaforme, si promuove un'interazione omogenea per i servizi offerti dall'Ateneo. L'Ateneo favorisce lo sviluppo delle piattaforme nell'ottica di:

- Completare l'implementazione delle Piattaforme abilitanti e incentivare la loro adozione.
- Migliorare o ampliare le funzionalità delle Piattaforme abilitanti esistenti, adeguando costantemente la tecnologia e il livello di sicurezza.
- Identificare e sviluppare eventuali nuove Piattaforme abilitanti che possano accelerare il processo di digitalizzazione dell'Ateneo

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

In questo contesto, l'Ateneo monitora attentamente l'eventuale necessità di sfruttare nuove piattaforme o di arricchire quelle esistenti, per offrire servizi digitali più sicuri e facili da usare e per semplificare i processi di pagamento. In particolare, valuta l'attivazione di nuovi servizi, relativamente alla piattaforma pagoPA, ogni volta che si renda necessario fornire ulteriori servizi a supporto degli utenti. Allo stesso tempo, l'Università prosegue il percorso di adesione a SPID e CIE per i servizi esistenti e per quelli nuovi, dismettendo le altre

modalità di autenticazione associate ai propri servizi online, tra le quali il rilascio di credenziali proprietarie a cittadini dotabili di SPID e/o CIE.

L'Ateneo adotta 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, lo fa implementando lo SPID di livello 2 insieme al «Login with eIDAS» per l'accesso transfrontaliero ai propri servizi.

Scenario

pagoPA

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

AppIO

L'app IO è l'esito di un progetto *open source* nato con l'obiettivo di mettere a disposizione di enti e cittadini un unico canale da cui fruire di tutti i servizi pubblici digitali, quale pilastro della strategia del Governo italiano per la cittadinanza digitale. La visione alla base di IO è mettere al centro il cittadino nell'interazione con la Pubblica Amministrazione, attraverso un'applicazione semplice e intuitiva disponibile direttamente sul proprio *smartphone*. In particolare, l'app IO rende concreto l'articolo 64 bis del Codice dell'Amministrazione Digitale, che istituisce un unico punto di accesso per tutti i servizi digitali, erogato dalla Presidenza del Consiglio dei ministri, attraverso un'esperienza utente coerente, *mobile-first* e inclusiva. Inoltre, in linea con il DPCM 10 agosto 2023 - è utilizzata come canale ufficiale per le notifiche di pagamento e comunicazioni della PA.

SEND

La piattaforma SEND - Servizio Notifiche Digitali (anche noto come Piattaforma Notifiche Digitali di cui all'art. 26 del decreto-legge 76/2020 s.m.i.) rende più veloce, economico e sicuro

l'invio e la ricezione delle notifiche a valore legale: permette infatti l'invio di atti e comunicazioni sia in modalità tradizionale che in modalità digitale, utilizzando canali *web*, app (AppIO) e PEC. Permette inoltre di scaricare i documenti notificati e pagare eventuali spese direttamente *online* su SEND o nell'app IO.

SEND solleva gli enti da tutti gli adempimenti legati alla gestione delle comunicazioni a valore legale e riduce l'incertezza della reperibilità del destinatario ed è un elemento chiave nell'attuazione dei principi "*digital first*", "*mobile first*" e "*once only*" e nel percorso verso una piena cittadinanza digitale.

SPID

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

SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia digitale, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese.

CIE

L'identità digitale CIE, 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. L'app CielD costituisce l'elemento abilitante per l'accesso più sicuro e semplificato ai servizi digitali erogati dalle pubbliche amministrazioni e dagli enti privati che svolgono funzioni pubbliche o di interesse pubblico ovvero permette di accedere ai servizi e ai portali della pubblica amministrazione italiana attraverso l'uso della CIE o delle credenziali rilasciate dal Ministero dell'Interno.

Catalogo delle procedure

La *milestone* PNRR M1C1-63 prevede che entro il 30 giugno 2026 venga realizzato un catalogo (ovvero l'elenco ordinato e sistematico delle procedure amministrative valide) contenente almeno 600 procedure semplificate a partire da marzo 2020, valide su tutto il territorio nazionale.

Una delle finalità del Catalogo delle procedure è la costituzione della Banca dati delle procedure semplificate, per rendicontare l'avvenuto conseguimento dell'obiettivo (semplificazione di almeno 600 procedure nel periodo di attuazione del PNRR).

La banca dati conterrà tutte le procedure sulle quali sono stati effettuati interventi di semplificazione, garantendone la consultazione a chiunque (e quindi una banca dati pubblica e accessibile via *Internet*) sulla base di diversi parametri.

Siope+

L'art. 1, comma 533, della Legge n. 232 del 2016 (Legge di bilancio 2017), al fine di favorire il monitoraggio del ciclo completo delle entrate e delle spese, ha previsto l'obbligo per tutte le Amministrazioni pubbliche di:

- ordinare gli incassi e i pagamenti al proprio tesoriere o cassiere esclusivamente attraverso ordinativi informatici emessi secondo lo standard OPI emanato dall'Agenzia per l'Italia digitale (AgID);
- trasmettere gli ordinativi al proprio tesoriere/cassiere per il tramite dell'infrastruttura SIOPE+ gestita dalla Banca d'Italia.

IT-Wallet

Il Sistema di Portafoglio digitale italiano (Sistema *IT-Wallet*) è l'ecosistema di soluzioni pubbliche e private che permettono a tutti i cittadini di disporre e gestire in maniera efficace della propria identità digitale e dei propri documenti ed attestazioni, anche attraverso applicazioni *mobile*. Ha l'obiettivo di rendere più semplice, accessibile, sicuro e trasparente il processo di presentazione dei propri dati e l'accesso ai servizi erogati da pubbliche amministrazioni e soggetti privati, sia nel mondo fisico che in quello digitale, mettendo al centro il cittadino secondo i principi di *user-centric design*, *mobile first*, *cross-border interoperability*, *self-sovereignty*, *once-only* e *data minimization*.

Il Sistema di portafoglio digitale pubblico italiano è stato istituito con il Decreto-legge n. 19 del 2 marzo 2024 (convertito con Legge n. 56 del 29 aprile 2024), Decreto per l'attuazione del PNRR.

Attraverso il proprio portafoglio digitale, le persone potranno presentare direttamente ad aziende e pubbliche amministrazioni le informazioni richieste per l'accesso ai servizi sotto forma di attestati elettronici. Proprio come un portafoglio fisico, l'*IT-Wallet* conterrà documenti in formato digitale da esibire all'occorrenza.

Con una solida collaborazione pubblico-privato, il progetto dell'IT *Wallet* mira a promuovere l'innovazione, contribuendo a rendere i servizi digitali più accessibili, sicuri e vantaggiosi per cittadini e aziende, sia a livello nazionale che internazionale.

L'IT-*Wallet*, inoltre, consentirà ai cittadini italiani di autenticarsi in modo sicuro presso i servizi pubblici e privati nazionali ed europei, presentare in modo selettivo attributi verificati e credenziali digitali, in conformità con il quadro europeo del *European Digital Identity Wallet* (EUDI *Wallet*).

Il Sistema IT-*Wallet*, infatti, si colloca nel più ampio contesto europeo dell'*European Digital Identity Framework*, un insieme di regole contenute all'interno del Regolamento (UE) n. 2024/1183 (c.d. "eIDAS 2") che modifica il già in essere Reg. (UE) n. 910/2014 (c.d. "eIDAS"). Le citate regole puntano, soprattutto, a superare la frammentazione di identità digitali presenti negli Stati Membri, e richiedono che ogni Stato Membro notifichi alla Commissione entro il 2026 almeno un *Wallet* nazionale da qualificare quale "EUDI *Wallet*". Quest'ultimo dovrà anzitutto disporre delle funzionalità, dei livelli di sicurezza e certificazione minimi prescritte dal Regolamento. L'obiettivo di eIDAS 2 è quello di fornire ai cittadini europei strumenti interoperabili che consentano di accedere a vari tipi di servizi, anche a livello transfrontaliero.

Obiettivo 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

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

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

RA4.1.5 - Promuovere l'adesione ai servizi della piattaforma NoiPA per supportare l'azione amministrativa nella gestione del personale

Linee di azione per le PA

RA4.1.1

Dicembre 2026 - 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) - Codice Linea di Azione: CAP4.PA.01

Attività Operative: Integrazione più fluida del servizio di pagamento all'interno dei vari servizi digitali, con l'obiettivo di migliorare l'usabilità e, conseguentemente, efficacia dalla soluzione e soddisfazione degli utenti; ottimizzazione dei flussi per lo scambio e il trattamento automatico dei dati fra i diversi sistemi interessati.

Tempistiche di realizzazione e deadline:31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Servizi digitali

RA4.1.2

Dicembre 2026 - Le PA aderenti ad AppIO 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) - Codice Linea di Azione: CAP4.PA.02

Attività Operative: Al momento non è emersa la necessità di implementare nuovi servizi su app IO. Tuttavia, fra i vari servizi già attivati su app IO, è previsto il consolidamento e diffusione della firma con app IO nell'ambito dei diversi processi di competenza dell'Ateneo che possono beneficiare della soluzione.

Tempistiche di realizzazione e deadline:31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Servizi digitali

RA4.1.4

Linee d'azione vigenti

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 - Codice Linea di Azione: CAP4.PA.04

Attività Operative: Integrazione del servizio di autenticazione con SPID/CIE all'interno dei nuovi servizi e sistemi gestionali in corso di attivazione. Monitoraggio delle evoluzioni riguardo a e-IDAS per valutarne la progressiva integrazione nei servizi digitali dell'Ateneo, condizionatamente al soddisfacimento dei necessari pre-requisiti sui relativi servizi di back-office. Monitoraggio per identificare eventuali nuove necessità o opportunità relativamente

all'autenticazione per l'accesso ai servizi pubblici.

Tempistiche di realizzazione e deadline:31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Servizi digitali

Le PA e i gestori di pubblici servizi interessati cessano il rilascio di credenziali proprietarie a cittadini dotabili di SPID e/o CIE - Codice Linea di Azione: CAP4.PA.05

Attività Operative: Integrazione del servizio di autenticazione con SPID/CIE all'interno dei nuovi servizi e sistemi gestionali in corso di attivazione. Monitoraggio delle evoluzioni riguardo a e-IDAS per valutarne la progressiva integrazione nei servizi digitali dell'Ateneo, condizionatamente al soddisfacimento dei necessari pre-requisiti sui relativi servizi di back-office. Monitoraggio per identificare eventuali nuove necessità o opportunità relativamente all'autenticazione per l'accesso ai servizi pubblici. Tutti servizi per i quali era richiesto sono stati resi accessibili solo tramite SPID/CIE.

L'Ateneo, tuttavia, non può rinunciare in toto al rilascio alla propria utenza (studenti, docenti, ricercatori) di credenziali interne, necessarie per permettere l'accesso alla rete Europea della ricerca EDUROAM/EDUGAIN. Vi sono, inoltre, alcuni studenti, provenienti da Paesi extra UE (e quindi non dotabili di SPID/CIE) che necessitano delle credenziali uniche di Ateneo per accedere ai servizi online.

Tempistiche di realizzazione e deadline:31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Servizi digitali

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 - Codice Linea di Azione: CAP4.PA.06

Attività Operative: Integrazione del servizio di autenticazione con SPID/CIE all'interno dei nuovi servizi e sistemi gestionali in corso di attivazione. Monitoraggio delle evoluzioni riguardo a e-IDAS per valutarne la progressiva integrazione nei servizi digitali dell'Ateneo, condizionatamente al soddisfacimento dei necessari pre-requisiti sui relativi servizi di back-

office. Monitoraggio per identificare eventuali nuove necessità o opportunità relativamente all'autenticazione per l'accesso ai servizi pubblici.

L'Ateneo, tuttavia, non può rinunciare in toto al rilascio alla propria utenza (studenti, docenti, ricercatori) di credenziali interne, necessarie per permettere l'accesso alla rete Europea della ricerca EDUROAM/EDUGAIN. Vi sono, inoltre, alcuni studenti, provenienti da Paesi extra UE (e quindi non dotabili di SPI/CIE) che necessitano delle credenziali uniche di Ateneo per accedere ai servizi online.

Tempistiche di realizzazione e deadline:31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici

Le PA devono adeguarsi alle evoluzioni previste dall'ecosistema SPID (tra cui OpenID Connect, uso professionale, *Attribute Authorities*, servizi per i minori e gestione degli attributi qualificati) - Codice Linea di Azione: CAP4.PA.07

Attività Operative: Integrazione del servizio di autenticazione con SPID/CIE all'interno dei nuovi servizi e sistemi gestionali in corso di attivazione. Monitoraggio delle evoluzioni riguardo a e-IDAS per valutarne la progressiva integrazione nei servizi digitali dell'Ateneo, condizionatamente al soddisfacimento dei necessari pre-requisiti sui relativi servizi di back-office. Monitoraggio per identificare eventuali nuove necessità o opportunità relativamente all'autenticazione per l'accesso ai servizi pubblici.

Tempistiche di realizzazione e deadline:31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Servizi digitali

RA4.1.5

Linee di azione vigenti

Le PA che intendono aderire a NoiPA esprimono manifestazione di interesse e inviano richiesta - Codice Linea di Azione: CAP4.PA.08

Attività Operative: la piattaforma NoiPA non è al momento disponibile per le università; ciò nonostante, questo Ateneo monitorerà l'eventuale apertura in tal senso ed invierà la propria eventuale richiesta di adesione.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Servizi digitali

Piattaforme che attestano attributi

Scenario

Negli ultimi anni, le azioni messe in atto dai diversi soggetti coinvolti nel Piano triennale hanno portato ad un notevole aumento nella diffusione delle principali piattaforme abilitanti, sia in termini di adozione da parte delle pubbliche amministrazioni che di utilizzo da parte degli utenti.

Queste piattaforme forniscono accesso ai dati di settore per i cittadini e le pubbliche amministrazioni, consentendo una maggiore razionalizzazione dei servizi e semplificando l'interazione tra cittadini e pubblica amministrazione attraverso l'uso delle tecnologie digitali, come la Piattaforma Digitale Nazionale Dati (PDND).

Le seguenti Piattaforme hanno la caratteristica di attestare attributi anagrafici e di settore.

ANPR: è l'Anagrafe Nazionale che raccoglie tutti i dati anagrafici dei cittadini residenti in Italia e dei cittadini italiani residenti all'estero, aggiornata con continuità dai comuni italiani. Consente di avere un set di dati anagrafici dei cittadini certo, accessibile, affidabile e sicuro su cui sviluppare servizi integrati ed evoluti per semplificare e velocizzare le procedure tra pubbliche amministrazioni e con i cittadini.

Al fine di agevolare lo sviluppo di sistemi integrati ed evoluti, che semplifichino e velocizzino le procedure tra le Pubbliche Amministrazioni, ANPR ha rilasciato oltre 30 *e-service* sulla Piattaforma Nazionale Digitale Dati (PDND - Interoperabilità), consentendo la consultazione dei dati ANPR da parte di altri Enti aventi diritto, nel rispetto dei principi del Regolamento *Privacy*.

Tra le piattaforme che attestano attributi, per rafforzare gli interventi nei settori di istruzione, università e ricerca, accelerare il processo di automazione amministrativa e migliorare i servizi per i cittadini e le pubbliche amministrazioni, sono istituite due Anagrafi:

- **ANIST:** Anagrafe nazionale dell'istruzione, a cura del Ministero dell'Istruzione e del Merito

- **ANIS:** Anagrafe nazionale dell'istruzione superiore, a cura del Ministero dell'Università e della Ricerca.

Le due Anagrafi mirano ad assicurare:

- la centralizzazione dei dati attualmente distribuiti su tutto il territorio italiano in oltre 10.000 scuole (ANIST) e 500 istituti di formazione superiore (ANIS);
- la disponibilità e l'accesso ai dati per:
 - scuole e istituti di formazione superiore (IFS), al fine di facilitare il reperimento delle informazioni relative al percorso scolastico e/o accademico dei propri studenti, efficientando le procedure di iscrizione;
 - cittadini, al fine rendere possibile, attraverso il Portale dedicato, la consultazione *online* dei dati relativi al proprio percorso scolastico e/o accademico, anche a fini certificativi;
 - PA per fini istituzionali;
 - Soggetti privati autorizzati, per gli scopi previsti dalla legge.
- l'interoperabilità con altre banche dati (es. con ANPR per la gestione dei dati anagrafici degli studenti, eliminando duplicazioni e rischi di disallineamento);
- il riconoscimento nell'UE ed extra-EU dei titoli di studio.
- L'iter normativo di ANIS è stato concluso il 18 gennaio 2023 e a settembre dello stesso anno è stato rilasciato il portale nazionale ANIS (<https://anis.mur.gov.it/>) con l'attivazione dei seguenti servizi online verso i cittadini:
 - consultazione dei propri titoli di studio;
 - possibilità di presentare una richiesta di rettifica degli stessi, ove necessario;
 - possibilità di ottenere attestazioni dei propri titoli di studio, firmate digitalmente dal MUR, da utilizzare nei rapporti con soggetti privati.

In particolare, il progetto ANIS, attraverso le sue componenti tecnologiche, ha diversi obiettivi chiave:

- Garantire la disponibilità dei dati e degli strumenti necessari alle istituzioni dell'istruzione superiore per svolgere le loro funzioni, in particolare per la certificazione. Questo include anche la possibilità per i cittadini di consultare i dati per le loro esigenze di certificazione.

- Consentire alle pubbliche amministrazioni di accedere ai dati contenuti nell'ANIS per scopi istituzionali, così come ai soggetti privati nei limiti delle leggi vigenti.
- Fornire i dati necessari per automatizzare le procedure di iscrizione online alle istituzioni dell'istruzione superiore.
- Assicurare l'interoperabilità con altre banche dati, anche di interesse nazionale, per le finalità istituzionali del Ministero.
- Garantire il riconoscimento dei titoli di studio nell'Unione europea e all'estero attraverso tecnologie per l'autenticità dei titoli.
- Automatizzare le procedure di iscrizione online ai corsi delle istituzioni dell'istruzione superiore, inclusa la consultazione delle banche dati di altre amministrazioni.
- Assicurare la disponibilità dei dati necessari per le funzioni di competenza delle istituzioni dell'istruzione superiore e delle pubbliche amministrazioni.
- Fornire accesso a specifiche categorie di soggetti per specifiche finalità istituzionali in relazione ai dati disponibili nell'ANIS.

Sono stati rilasciati, inoltre, i servizi sulla PDND, per consentire la verifica e il recupero dei dati relativi ai titoli di studio e alle iscrizioni da parte degli Enti aventi diritto.

Il Regolamento sulle modalità di attuazione e funzionamento dell'Anagrafe nazionale dell'istruzione (ANIST) è entrato in vigore il 23 marzo 2024 e a dicembre 2024 è stato attivato il portale con i primi servizi, consentendo ai cittadini di consultare online i dati relativi alle frequenze e ai titoli di studio, richiedere una eventuale rettifica degli stessi, nonché ottenere il rilascio di certificazioni spendibili nei rapporti con i privati.

Sono stati rilasciati, inoltre, i servizi sulla PDND, per consentire la verifica e il recupero dei dati relativi ai titoli di studio e alla frequenza da parte degli Enti aventi diritto.

Inoltre, l'ANIS è organizzata in modo da garantire l'uniformità dei dati all'interno del contesto delle altre banche dati del Ministero dell'Università e della Ricerca.

Queste comunicazioni avvengono tramite i servizi offerti dalla PDND. In conformità alle linee guida di Agid sull'interoperabilità, l'Ateneo mantiene il controllo dei dati di propria competenza, garantendone la correttezza, l'esattezza e l'aggiornamento attraverso l'ANS (Anagrafe Nazionale Studenti).

[Obiettivo 4.2 - Ottenere la piena interoperabilità tra le piattaforme](#)

RA4.2.2 - Disponibilità dei dati su iscrizioni e titoli di studio su ANIS

RA4.2.2

Da gennaio 2024 – Le PA possono consultare i dati dell'ANIS attraverso servizi resi fruibili dalla PDND secondo quanto descritto nell'area tecnica del sito

<https://www.anis.mur.gov.it/area-tecnica/documentazione> - Codice Linea di Azione:

CAP4.PA.19

Attività Operative: L'Ateneo, quando opportuno, valuta l'utilizzo di ANIS attraverso i servizi resi fruibili dalla PDND.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Servizi digitali

Da aprile 2025 * - Le Università possono trasmettere i propri dati per l'integrazione su ANIS attraverso l'uso di una *web application* - Codice Linea di Azione: CAP4.PA.20

Attività Operative: Esse3 risulta già integrato con PDND e l'Ateneo espone, per il tramite di CINECA, gli e-service con cui rende disponibili a livello nazionale informazioni sulla carriera degli studenti relative alle iscrizioni e ai titoli accademici. L'Ateneo risulta già integrato con ANIS e figura fra gli istituti presenti nel sistema.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Servizi digitali

Capitolo 5 - Dati e Intelligenza Artificiale

Dati e *data governance*

Scenario

La valorizzazione del patrimonio informativo pubblico è un obiettivo strategico per la Pubblica Amministrazione per affrontare efficacemente le nuove sfide dell'economia basata sui dati (*data economy*), supportare gli obiettivi definiti dalla Strategia europea in materia di dati, garantire la creazione di servizi digitali a valore aggiunto per cittadini, imprese e, in generale, per tutti i portatori di interesse e fornire ai vertici decisionali strumenti *data-driven* da utilizzare nei processi organizzativi e/o produttivi. L'ingente quantità di dati prodotti dalla Pubblica Amministrazione, se caratterizzati da un'alta qualità, potrà costituire, inoltre, la base per una grande varietà di applicazioni come, per esempio, quelle riferite all'intelligenza artificiale e fornire strumenti basati sui dati per il processo decisionale. La costruzione di un'economia dei dati è l'obiettivo che l'Unione Europea intende perseguire attraverso una serie di iniziative di regolazione avviate ormai dal 2020. La citata Strategia europea ha introdotto la creazione di spazi di dati comuni e interoperabili al fine di superare le barriere legali e tecniche alla loro condivisione e, di conseguenza, sfruttare l'enorme potenziale dell'innovazione guidata dai dati. Le tecnologie digitali hanno reso comune la produzione di dati, che possono essere riutilizzati per creare nuovi servizi, diventando così una risorsa fondamentale nell'economia digitale. I dati, per la loro natura flessibile e scambiabile, hanno assunto un ruolo centrale nell'innovazione e nella crescita economica: è, quindi, fondamentale garantire l'implementazione di processi efficaci per la produzione di dati di qualità.

Con l'adozione del regolamento sulla *governance* dei dati (Regolamento (UE) 2022/868, *Data Governance Act*) sono stati definiti e rafforzati i meccanismi per aumentare la disponibilità dei dati e superare gli ostacoli tecnici al riutilizzo di alcune particolari tipologie di dati altrimenti non disponibili.

In Italia, con il recepimento della Direttiva Europea (UE) 2019/1024 (cosiddetta Direttiva *Open Data*) sull'apertura dei dati e il riutilizzo dell'informazione del settore pubblico, attuato con il Decreto lgs. n. 200/2021, che ha modificato il Decreto lgs. n. 36/2006, l'obiettivo strategico sopra delineato può essere perseguito attraverso l'implementazione delle nuove

regole tecniche definite con le “Linee guida recanti regole tecniche per l’apertura dei dati e il riutilizzo dell’informazione del settore pubblico” (Linee guida *Open Data*, d’ora in avanti).

Tale documento, adottato con la Determinazione AgID n. 183/2023 ai sensi dell’art. 71 del CAD in applicazione dell’art. 12 del citato Decreto Lgs. N. 36/2006 e s.m.i., è finalizzato a supportare le pubbliche amministrazioni e gli altri soggetti interessati nel processo di apertura dei dati e, quindi, favorire l’aumento dell’offerta di dati pubblici preziosi a fini di riutilizzo.

Tra questi tipi di dati rientrano anche quelli di elevato valore, identificati con il Regolamento di esecuzione (UE) 2023/138 sulla base delle sei categorie tematiche (dati geospaziali, dati relativi all’osservazione della Terra e all’ambiente, dati meteorologici, dati statistici, dati relativi alle imprese e alla proprietà delle imprese, dati relativi alla mobilità) stabilite con la Direttiva *Open Data*. Per garantire la creazione di servizi digitali sempre più efficienti, i dati scambiati reciprocamente tra gli enti erogatori di servizi dovranno essere pienamente interoperabili, non solo da un punto di vista tecnico ma anche semantico. In altre parole, nello sviluppo di un servizio digitale, oltre a utilizzare applicazioni informatiche interoperabili, per la ricezione o l’invio dei dati, si dovrà garantire l’effettiva comprensione del significato e del formato delle informazioni scambiate, usufruendo di riferimenti nazionali come ad esempio le ontologie, i vocabolari controllati e gli schemi di dati presenti sul Catalogo Nazionale per l’Interoperabilità semantica dei dati (*National Data Catalog – NDC*).

L’adozione di una semantica comune nello scambio dei dati assicura la coerenza e favorisce lo sviluppo di informazioni coerenti e consistenti. È essenziale garantire la piena interoperabilità dei dati, sia dal punto di vista tecnico che semantico, implementando, per esempio, una semantica comune e utilizzando standard e protocolli che consentano lo scambio efficiente e la comprensione dei dati tra diverse entità (e.g., si potrebbe considerare l’adozione di ontologie, vocabolari controllati e schemi dati condivisi).

Il processo di apertura dei dati segue diverse fasi, che portano all’implementazione delle Linee Guida sui Dati Aperti, tra le quali: l’identificazione, l’analisi, l’arricchimento, la modellazione, la documentazione, la validazione e la pubblicazione.

Per attuare efficacemente questo processo, è fondamentale stabilire una chiara governance dei dati (sia interna che esterna), una pianificazione accurata ed un coinvolgimento attivo

delle diverse unità organizzative, nonché individuare ruoli e responsabilità chiari per garantire la gestione efficace dei dati lungo tutto il loro ciclo di vita.

Le attività di apertura e pubblicazione dei dati devono essere tracciate nel Piano triennale ICT, tenendo conto dell'impatto economico e sociale e delle necessità degli utilizzatori.

È possibile mettere in atto misure specifiche per garantire la qualità dei dati, includendo meccanismi di valutazione e monitoraggio, ispirati o basati sugli standard ISO pertinenti.

Questo processo potrebbe implicare la creazione di sistemi di misurazione della qualità dei dati e l'adozione di pratiche per migliorare continuamente la loro precisione e affidabilità.

Al fine di valutare l'impatto del processo di apertura dei dati e la conseguente ricaduta economica e sociale, dovranno essere attivate azioni mirate al monitoraggio del riutilizzo dei dati resi disponibili dalle pubbliche amministrazioni. Per poter abilitare attività di sviluppo di applicazioni innovative, inoltre, dovrà essere garantito un adeguato livello di qualità dei dati con la disponibilità di un sistema di misurazione e di *assessment* basato sui pertinenti standard ISO.

Tali standard ISO, relativi sia alle caratteristiche della qualità che alla loro misurazione, sono indicati come riferimento utile nelle Linee Guida *Open Data*, che forniscono raccomandazioni ed esempi su come garantire un livello minimo della stessa qualità. Le medesime Linee Guida richiamano, per i dati della ricerca in particolare ma con raccomandazione di applicarli per tutte le tipologie di dati, i requisiti di reperibilità, accessibilità, interoperabilità e riutilizzabilità che rappresentano i 4 principi del framework FAIR (*Findable - Accessible - Interoperable - Reusable*).

Indipendentemente dalla formattazione aperta di un dataset, ci sono aspetti fondamentali che influenzano la sua qualità complessiva: l'accuratezza, la coerenza, la completezza e l'aggiornamento regolare dei dati. È essenziale che:

- tutte le informazioni nel dataset siano prive di errori, sia di trascrizione che di inserimento.
- I dati e gli attributi siano rappresentati correttamente per garantire un'interpretazione accurata e le risorse siano ben descritte per una migliore comprensione.
- Vi sia coerenza, sia all'interno che all'esterno: i dati ed i relativi attributi non devono contraddirsi né internamente né rispetto ad altre fonti pubblicate.
- I dati siano completi: devono essere esaustivi e coprire tutti i valori attesi, rispettando le

fonti da cui provengono le informazioni.

- Vi sia la tempestività: i dati devono essere rilasciati e aggiornati regolarmente per mantenere la loro rilevanza nel tempo per essere sempre attuali e pertinenti al contesto in cui vengono utilizzati.

La *data governance* e la razionalizzazione delle banche dati esistenti interne alla PA, a garanzia dell'univocità e della qualità del dato, e la promozione della condivisione del patrimonio informativo detenuto dalle PA sono anche gli obiettivi richiamati nella Direttiva del Sottosegretario di Stato alla Presidenza del Consiglio dei ministri con delega di funzioni in materia di innovazione tecnologica e transizione digitale, concernente "Misure per l'attuazione dell'articolo 50-ter del decreto legislativo 7 marzo 2005, n. 82" e che la stessa Direttiva indica di inserire tra i compiti da affidare ad apposite strutture di coordinamento o gruppi di lavoro esistenti o da istituire, anche all'interno dell'ufficio del RTD.

L'attività di apertura e di pubblicazione dei dati, infine, può essere tracciata oltre che nel Piano triennale ICT anche come obiettivo del PIAO di ciascuna amministrazione.

La Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, "relativa all'apertura dei dati e al riutilizzo dell'informazione nel settore pubblico (rifusione)", in vigore dal 15 dicembre 2021, ha ampliato il proprio ambito di applicazione anche ai dati derivati dalla ricerca scientifica finanziata pubblicamente. L'accesso aperto dei dati migliora la qualità, riduce duplicazioni inutili nella ricerca, accelera il progresso scientifico, contrasta le frodi e può promuovere l'economia e l'innovazione.

L'Open Access e l'Open Data sono diventati sempre più importanti nei finanziamenti europei per la ricerca negli ultimi dieci anni: con Horizon 2020 e Horizon Europe, la pubblicazione dei contributi scientifici in accesso aperto è obbligatoria, così come la gestione dei dati secondo il modello FAIR.

L'Università è chiamata ad implementare il più possibile le previsioni della suddetta Direttiva, sia come centro di formazione e ricerca sia come ente pubblico. Sta facendo la propria parte sostenendo varie iniziative:

- Il Settore Ricerca Europea e Internazionale ed il Sistema Bibliotecario di Ateneo hanno redatto linee guida per orientare i ricercatori su Open Science e Open Data.
- Dal 2010, il Sistema Bibliotecario di Ateneo ha digitalizzato le proprie risorse, tra cui

oltre 237.000 immagini ad alta definizione. La maggior parte di esse è accessibile tramite la piattaforma nazionale "Internet Culturale" e il discovery di Ateneo "OneSearch".

- L'Ateneo promuove l'accesso aperto alla letteratura scientifica e la disseminazione delle pubblicazioni attraverso il repository istituzionale FLORE.
- La Firenze University Press sostiene l'Open Access attraverso monografie e riviste ad accesso aperto, è coinvolta nella definizione di strategie editoriali per promuovere l'accesso aperto, l'implementazione di standard internazionali e l'uso di licenze Creative Commons.

A partire dal 2022, l'Università di Firenze sta discutendo la possibilità di una Policy Open Data condivisa con altri Atenei italiani per valorizzare il patrimonio informativo pubblico attraverso la gestione dei dati. A tal fine, sarà fondamentale stabilire una chiara governance dei dati, sia interna che esterna, e coinvolgere tutte le figure pertinenti all'interno dell'amministrazione. Tali esigenze organizzative trovano utili elementi guida nella normativa, nel Codice dell'Amministrazione Digitale e, nei riferimenti operativi nazionali, nelle "Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico" (definite ed aggiornate da AgID), che individuano le figure coinvolte nel processo di gestione ed esposizione dei dati in formato aperto.

Un ruolo determinante su questo tema è svolto dal RTD che, sulla base della Circolare n. 3 del 1° ottobre 2018 del Ministro per la Pubblica Amministrazione, può costituire un apposito Gruppo di lavoro come possibile struttura per il governo del processo di apertura dei dati in cui, oltre ad un responsabile, siano coinvolti i referenti tematici che gestiscono e trattano dati nell'ambito delle singole unità organizzative e le altre figure coinvolte nel processo di digitalizzazione della Pubblica Amministrazione, quali il Responsabile per la conservazione documentale, il Responsabile per la prevenzione della corruzione e la trasparenza, il Responsabile della protezione dei dati, il Responsabile per la sicurezza.

Nelle linee guida nazionali viene definito il ruolo e le competenze del gruppo di lavoro open data, team multidisciplinare composto da risorse con competenze miste - legali, tecnologiche o manageriali - che ha il compito di promuovere l'uso e la diffusione dei dati aperti presso l'ente in cui opera. Il gruppo di lavoro open data ha il compito di riportare all'interno dell'amministrazione le novità che riguardano il mondo dell'open government in

generale e dei dati aperti in particolare, di valutare le esigenze di pubblicazione dei dati in base alla normativa di riferimento e di curarne la razionalizzazione rispetto ai processi di apertura del dato. Il gruppo di lavoro open data dovrebbe avere inoltre la responsabilità di pianificare e coordinare l'evoluzione continua dell'apertura dei dati presso l'amministrazione, nonché dell'infrastruttura ICT a supporto di questa attività.

All'interno del team open data dovrebbe essere nominato un Responsabile open data o Data manager, figura di coordinamento che ha il compito di pianificare la strategia di apertura dei dati, gestire le attività di pubblicazione e interfacciarsi con le figure di riferimento interne all'ente.

Prima di essere esposti sul web in formato aperto i dati dovrebbero essere raccolti e gestiti all'interno dell'Ateneo. Ognuna di queste banche dati ha un responsabile che viene appunto chiamato titolare della banca dati ed è colui che all'interno dell'amministrazione è responsabile del procedimento amministrativo che popola la specifica fonte del dato e ne cura la qualità e l'aggiornamento. Il titolare della banca dati è tipicamente un dirigente o un quadro che coordina un gruppo di persone, come i referenti tematici e i referenti delle banche dati che collaborano alla manutenzione e all'arricchimento delle informazioni presenti nella banca dati.

L'attività di apertura e di pubblicazione dei dati può dunque essere tracciata nei futuri Piani triennali per la Transizione Digitale dell'Università di Firenze sulla base di una eventuale scala di priorità basata, per esempio, su un approccio di tipo demand-driven che tenga conto dell'impatto economico e sociale nonché del livello di interesse e delle necessità degli utilizzatori.

In attesa di definire la strategia e la governance, l'Università continuerà a monitorare gli obblighi normativi, consolidatisi con l'approvazione da parte di AgID delle "Linee Guida recanti regole tecniche per l'apertura dei dati e il riutilizzo dell'informazione del settore pubblico" per l'attuazione della Direttiva (UE) 2019/1024.

Obiettivo 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

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

RA5.1.3 - Disponibilità delle categorie di dati protetti di cui all'art. 3 del Regolamento (UE) 2022/868 (DGA)

Linee di azione per le PA

RA5.1.1

Le PA adeguano i metadati relativi ai dati geografici all'ultima versione delle specifiche nazionali e documentano i propri *dataset* nel Catalogo nazionale geodati.gov.it - Codice Linea di Azione: CAP5.PA.01

Attività Operative: L'Ateneo, quando e se applicabile, valuta l'adeguamento dei metadati relativi ai dati geografici all'ultima versione delle specifiche nazionali e documenta i propri dataset nel Catalogo nazionale.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici

Le PA adeguano i metadati relativi ai dati non geografici alle specifiche nazionali e documentano i propri *dataset* nel Catalogo nazionale dati.gov.it - Codice Linea di Azione: CAP5.PA.02

Attività Operative: L'Ateneo, quando e se applicabile, adegua i metadati relativi ai dati non geografici alle specifiche nazionali e documenta i propri dataset nel Catalogo nazionale.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici

Le PA partecipano, in funzione delle proprie necessità, a interventi di formazione e sensibilizzazione sulle politiche *open data* - Codice Linea di Azione: CAP5.PA.03

Attività Operative: La partecipazione sarà valutata caso per caso.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale

RA5.1.2

Da giugno 2024 - 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 - Codice Linea di Azione: CAP5.PA.04

Attività Operative: L'Ateneo attua, quando possibile, le linee guida contenenti regole tecniche per l'implementazione del Decreto Legislativo n. 36/2006 di attuazione della direttiva (UE) 2019/1024, relativa all'apertura e al riutilizzo dei dati. A questo riguardo, in caso di presenza di dati di elevato valore, attua le indicazioni della guida operativa sui dati di elevato valore di AgID, per l'attuazione delle Linee Guida sui dati aperti e del Regolamento di esecuzione UE.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Tutte le strutture di Ateneo

RA5.1.3

Da gennaio 2026 - Le PA documentano i propri dati rientranti nelle categorie di cui all'art. 3 del Regolamento (UE) 2022/868 (DGA) nello sportello unico reso disponibile da AgID - Codice Linea di Azione: CAP5.PA.26

Attività Operative: L'Ateneo, quando e se applicabile, documenta i propri dati rientranti nelle categorie di cui all'art. 3 del Regolamento (UE) 2022/868 (DGA) nello sportello unico reso disponibile da AgID.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici

Obiettivo 5.2 - Aumentare la qualità dei dati e dei metadati

RA5.2.1 - Aumento del numero di dataset con metadati di qualità conformi agli standard di riferimento europei e nazionali

RA5.2.3 - Aumento del numero di amministrazioni non ancora presenti nel catalogo dati.gov.it che rendono disponibili dataset di tipo aperto

RA5.2.4 - Aumento del numero di dataset documentati sul portale dati.gov.it che rispettano la

caratteristica di qualità “attualità” (o tempestività di aggiornamento) di cui allo Standard ISO/IEC 25012

Linee di azione per le PA

RA5.2.1

Da giugno 2024 - Le PA pubblicano i metadati relativi ai dati di elevato valore, secondo le indicazioni presenti nel Regolamento di esecuzione (UE) e nelle Linee guida sui dati aperti e relativa guida operativa, nei cataloghi nazionali dati.gov.it e geodati.gov.it - Codice Linea di Azione: CAP5.PA.05

Attività Operative: L’Ateneo, quando e se applicabile, pubblica i metadati relativi ai dati di elevato valore nei cataloghi nazionali.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici

RA5.2.3

Dicembre 2026 - 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 nel catalogo dati.gov.it) pubblicano e documentano nel catalogo almeno 30 *dataset* - Codice Linea di Azione: CAP5.PA.18

Attività Operative: L’Ateneo, quando e se tecnicamente possibile, pubblica e documenta nel catalogo almeno 30 *dataset*.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici, Funzioni direzionali

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

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

Linee di azione per le PA

RA5.3.1

Da gennaio 2024 - 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 - Codice Linea di Azione: CAP5.PA.20

Attività Operative: L'Ateneo valuta la definizione di sistemi organizzativi e procedure, in modo tale da utilizzare le tecnologie e le strutture a disposizione per coordinare e integrare l'amministrazione dei dati in modo controllato e unificato. Per incrementare l'interoperabilità con le altre amministrazioni pubbliche e gli enti privati, si prende in considerazione la formalizzazione e l'implementazione di accordi per lo scambio di informazioni, con attenzione anche agli standard stabiliti a livello nazionale ed europeo. L'Ateneo si impegna a sfruttare le proprie risorse informative per ottimizzare e ristrutturare i procedimenti interni, basandosi su prove empiriche supportate dai dati disponibili, e adottando tecnologie innovative per condurre analisi, inclusa la previsione, il monitoraggio e l'automatizzazione dei processi.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Funzioni direzionali

Intelligenza artificiale per la Pubblica Amministrazione

Scenario

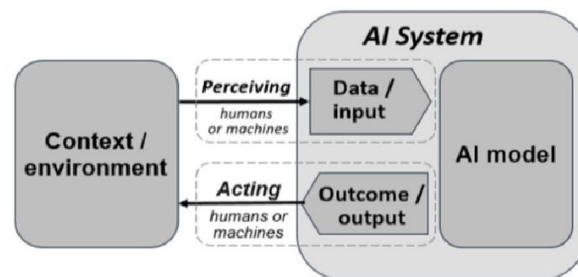


Figura 2 - Sistema di intelligenza artificiale (Fonte OECD: [OECD AI principles overview](#))

L'Ateneo promuove l'adozione di soluzioni basate su IA nei processi gestionali, didattici e di ricerca, favorendo automazione, analisi avanzata dei dati, personalizzazione dei servizi e miglioramento della comunicazione. Valuta inoltre l'uso di modelli linguistici e strumenti di IA generativa per supportare la produzione documentale, la ricerca di informazioni, la redazione multilingue e l'assistenza agli utenti.

L'IA è considerata strategica anche per la didattica. Nel marzo 2025 sono state pubblicate le "Linee di indirizzo sull'uso dell'IA nella didattica e per attività di studio", volte a formare docenti e studenti su opportunità, limiti ed implicazioni etiche, e a integrare l'IA nei processi

formativi in modo etico, trasparente e sostenibile, promuovendo competenze digitali avanzate e una cultura critica dell'uso dell'IA.

L'Ateneo sperimenta inoltre strumenti avanzati, come 1000 licenze EDU di ChatGPT e l'accesso a NotebookLM e Gemini, per supportare e velocizzare processi tecnici e amministrativi.

Coerentemente con le linee guida AgID e le politiche nazionali, l'Ateneo adotta un approccio fondato su trasparenza, equità, sicurezza e inclusività, orientando l'uso dell'IA al miglioramento dei servizi, alla riduzione dei costi, alla mitigazione dei rischi, all'accessibilità, alla protezione dei dati, alla formazione continua e alla sostenibilità ambientale.

L'Ateneo intende consolidare un modello di governance dell'IA allineato alle politiche europee e nazionali, integrando la gestione etica e tecnica dei sistemi nei processi istituzionali. Tale modello prevede l'inclusione dell'IA nei piani di digitalizzazione e risk management, la valorizzazione delle competenze interne e il sostegno alla ricerca interdisciplinare sulle applicazioni dell'IA nei diversi ambiti universitari.

Obiettivo finale è costruire un ecosistema di innovazione sostenibile e responsabile, in cui l'IA supporti la missione educativa, scientifica e istituzionale dell'Ateneo, contribuendo alla creazione di valore pubblico e al rafforzamento della competitività e reputazione dell'Ateneo a livello nazionale ed europeo.

Dati per l'intelligenza artificiale

La disponibilità di dati di alta qualità e il rispetto dei valori e dei diritti europei, quali la protezione dei dati personali, la tutela dei consumatori e la normativa in materia di concorrenza sono i prerequisiti fondamentali nonché un presupposto per lo sviluppo e la diffusione dei sistemi di IA. La disponibilità di dati rappresenta peraltro un requisito chiave per l'adozione di un approccio all'intelligenza artificiale attento alle specificità nazionali.

La Strategia Europea per i dati è implementata dal punto normativo dagli atti sopra citati che costituiscono il quadro regolatorio entro il quale deve muoversi una Pubblica Amministrazione che intende operare con sistemi di IA sui dati aperti.

L'Ateneo, nella consapevolezza che la qualità dei dati è fondamentale per l'addestramento di modelli di Intelligenza Artificiale, valuta con estrema attenzione la definizione di opportuni

processi per garantirne la correttezza. I dati sono una delle principali fonti di parzialità e divisione nei sistemi di IA, sia che si tratti di modelli ampiamente utilizzati o di applicazioni più specifiche sviluppate all'interno dell'Ateneo.

Si punta, pertanto, ad adottare approcci, procedure e strumenti per migliorare la qualità dei dati. L'implementazione di pratiche di gestione e controllo dei dati (governance dei dati) costituisce il fondamento di una strategia efficace per affrontare la parzialità che l'Ateneo intende perseguire, per la definizione di modelli robusti e per la minimizzazione del bias (l'errore di un algoritmo che devia dal risultato atteso).

Obiettivo 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 guida che definiscono i passi metodologici e organizzativi che le pubbliche amministrazioni devono seguire per definire attività progettuali di innovazione mediante l'utilizzo di IA. Le Linee guida forniranno strumenti di valutazione sull'utilizzo dell'intelligenza artificiale per rispondere alle esigenze delle amministrazioni, illustrando casi d'uso e promuovendo buone pratiche.

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

Linee guida che hanno l'obiettivo di orientare le pubbliche amministrazioni nella scelta delle procedure di approvvigionamento e nella definizione delle specifiche funzionali e non funzionali delle forniture al fine di garantire: la soddisfazione delle esigenze dell'amministrazione, adeguati livelli di servizio e la conformità con il quadro normativo vigente.

Le Linee guida forniranno indicazione sulla gestione dei servizi di IA da parte della PA.

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

Linee guida che hanno l'obiettivo di fornire alle pubbliche amministrazioni gli strumenti metodologici necessari per affrontare progetti di sviluppo di soluzioni IA, compresa la creazione di soluzioni basate su *foundation models*.

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

Sviluppo e implementazione di soluzioni basate su IA finalizzate al miglioramento della qualità dei servizi pubblici, con l'obiettivo di garantire uniformi livelli di servizio su tutto il

territorio nazionale.

Obiettivo 5.5 - Dati per l'intelligenza artificiale

RA5.5.1 - Basi di dati nazionali strategiche

Sviluppo di raccolte di *dataset* al fine di assicurare una base di conoscenza condivisa per le soluzioni di Intelligenza Artificiale nella Pubblica Amministrazione, preservando allo stesso tempo le peculiarità della Pubblica Amministrazione italiana e le specificità culturali nazionali.

Linee di azione per le PA

RA5.4.1

Da dicembre 2025 - Le PA dovranno rispettare le Linee per promuovere l'adozione dell'IA nella Pubblica Amministrazione - Codice Linea di Azione: CAP5.PA.21

Attività Operative: L'Ateneo rispetta e si impegna a promuovere l'adozione dell'IA nella Pubblica Amministrazione, attraverso iniziative di sensibilizzazione del personale ed eventi formativi.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Direzione Generale, Ufficio per la Transizione al Digitale

RA5.4.2

Da dicembre 2025 - Le PA dovranno rispettare le Linee guida per il *procurement* di IA nella Pubblica Amministrazione - Codice Linea di Azione: CAP5.PA.22

Attività Operative: L'Ateneo rispetta le Linee guida per il *procurement* di IA nella Pubblica Amministrazione.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Direzione Generale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici, Ufficio per la Transizione al Digitale

RA5.4.3

Da dicembre 2025 - Le PA dovranno rispettare le Linee guida per lo sviluppo di applicazioni di IA nella Pubblica Amministrazione - Codice Linea di Azione: CAP5.PA.23

Attività Operative: L'Ateneo rispetta le Linee guida per lo sviluppo di applicazioni di IA nella Pubblica Amministrazione.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Direzione Generale, Ufficio per la Transizione al Digitale

Da luglio 2026 - Le PA trasmettono periodicamente all'AgID i dati fondamentali delle iniziative nell'ambito delle tecnologie di IA - Codice Linea di Azione: CAP5.PA.27

Attività Operative: L'Ateneo, qualora svolga specifiche iniziative nell'ambito delle tecnologie di IA, si impegna a trasmettere all'AgID attraverso i canali che saranno messi a disposizione.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Direzione Generale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici, Ufficio per la Transizione al Digitale

RA5.4.4

Dicembre 2026 - Le PA adottano le applicazioni di IA a valenza nazionale - Codice Linea di Azione: CAP5.PA.24

Attività Operative: L'Ateneo, qualora verifichi la disponibilità di applicazioni di IA a valenza nazionale funzionali allo svolgimento delle proprie attività, si impegna ad adottarle.

Tempistiche di realizzazione e deadline:31/12/2026

Strutture responsabili: Direzione Generale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici, Ufficio per la Transizione al Digitale

RA5.5.1

Dicembre 2026 - Le PA adottano le basi dati nazionali strategiche - Codice Linea di Azione: CAP5.PA.25

Attività Operative: L'Ateneo, qualora verifichi la disponibilità di basi dati nazionali strategiche funzionali allo svolgimento delle proprie attività, si impegna ad adottarle.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Direzione Generale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici, Ufficio per la Transizione al Digitale

Capitolo 6 - Infrastrutture

Infrastrutture digitali e *Cloud*

Scenario

La Strategia "Cloud Italia" (adottata nel settembre 2021 dal Dipartimento per la Trasformazione Digitale e dall'Agenzia per la Cybersicurezza Nazionale), insieme agli investimenti del PNRR legati al cloud, offre un'opportunità significativa per riorganizzare le pubbliche amministrazioni. Questa iniziativa affronta sfide chiave, come garantire l'autonomia tecnologica, il controllo dei dati e l'aumento della resilienza dei servizi digitali. Con l'applicazione del principio "cloud first" si promuove l'adozione sicura delle suddette tecnologie nel settore pubblico: le amministrazioni devono preferire il cloud come prima opzione tecnologica, laddove disponibile, per i nuovi progetti, motivando eventuali valutazioni diverse che si rendano necessarie.

La suddetta strategia affronta tre sfide principali, che a loro volta mirano a garantire:

1. l'autonomia tecnologica;
2. il controllo sui dati;
3. la resilienza dei servizi digitali.

Inoltre fornisce un percorso definito per la migrazione verso il cloud per circa il 75% delle pubbliche amministrazioni italiane, questo in linea con il Piano Nazionale di Ripresa e Resilienza.

Con il principio *cloud first*, si vuole guidare e favorire l'adozione sicura, controllata e completa delle tecnologie *cloud* da parte del settore pubblico, in linea con i principi di tutela della *privacy* e con le raccomandazioni delle istituzioni europee e nazionali. In particolare, le pubbliche amministrazioni, in fase di definizione di un nuovo progetto, e/o di sviluppo di nuovi servizi, in via prioritaria devono valutare l'adozione del paradigma *cloud* prima di qualsiasi altra tecnologia.

Secondo tale principio, quindi, tutte le Amministrazioni sono obbligate ad effettuare una valutazione in merito all'adozione del *cloud*, che rappresenta una delle evoluzioni tecnologiche più dirompenti degli ultimi anni e che sta trasformando radicalmente tutti i sistemi informativi della società a livello mondiale. Nel caso di eventuale esito negativo della valutazione, la stessa dovrà essere motivata.

L'adozione del paradigma *cloud* rappresenta, infatti, la chiave della trasformazione digitale abilitando una vera e propria rivoluzione del modo di pensare i processi di erogazione dei servizi della PA verso cittadini, professionisti ed imprese. L'attuazione dell'art. 33-septies del Decreto-legge n. 179/2012, non rappresenta solo un adempimento legislativo, ma è soprattutto una occasione affinché ogni ente attivi gli opportuni processi di gestione interna necessari per modernizzare la propria infrastruttura, i propri applicativi e, al contempo, migliorare la fruizione dei procedimenti, delle procedure e dei servizi erogati.

L'evoluzione tecnologica espone, tuttavia, i sistemi informativi a nuovi e diversi rischi, anche con riguardo alla tutela dei dati personali. L'obiettivo di garantire una maggiore efficienza dei sistemi non può essere disgiunto dall'obiettivo di garantire contestualmente un elevato livello di sicurezza delle reti e dei sistemi informativi utilizzati dalla Pubblica Amministrazione.

Le amministrazioni pubbliche possono promuovere iniziative per lo sviluppo di applicazioni cloud native da erogare come servizi software (SaaS), anche attraverso il riuso di codice, disponibile su Developers Italia.

La migrazione al cloud offre opportunità di risparmio economico, ma richiede una corretta gestione dei costi e l'evoluzione verso architetture a "micro-servizi". A tal fine, è necessario porre attenzione anche agli aspetti tecnologici, come lo sviluppo di infrastrutture digitali affidabili, sicure ed economicamente sostenibili. La modernizzazione tecnologica deve, infatti, andare di pari passo con la sicurezza dei sistemi informativi per proteggere i dati sensibili dalla minaccia di attacchi cyber. È essenziale razionalizzare le infrastrutture per garantire la sicurezza dei servizi erogati attraverso la migrazione verso standard di qualità, sicurezza, performance e interoperabilità.

Nell'ambito della strategia Cloud Italia, uno degli obiettivi chiave è migliorare la qualità e la sicurezza dei servizi digitali offerti dalle amministrazioni pubbliche.

Seppur consapevoli dell'importanza della Strategia Cloud Italia e degli obiettivi di autonomia tecnologica, del controllo dei dati e della resilienza dei servizi digitali, bisogna prendere atto che gli Atenei non sono stati inclusi (o lo sono stati molto marginalmente) rispetto alla fruizione di fondi PNRR dedicati alla migrazione al Cloud e alla cybersicurezza.

Questo ha comportato un inevitabile rallentamento dei processi e dei servizi secondari erogati dall'Ateneo; ciò nonostante, per tutti i nuovi progetti l'Università si impegna a

valutare come prima opzione il paradigma cloud, valutando attentamente i problemi legati al lock-in, ai miglioramenti della postura di sicurezza ed alla riduzione dei costi di manutenzione dei data center. Quest'ultimo punto va inevitabilmente considerato poiché gli Atenei, non essendo una classica Pubblica Amministrazione Locale, hanno spesso bisogno di mantenere comunque infrastrutture on-premise per scopi di ricerca e trasferimento tecnologico.

La fruizione di servizi del PSN o di provider cloud qualificati viene sempre valutata, sia per nuovi progetti che per un eventuale spostamento dei servizi esistenti, soprattutto in logica SaaS, ma richiede probabilmente una migrazione completa dei servizi verso questa struttura per essere realmente efficace.

La ristrutturazione dei servizi esistenti in logica di microservizi pone delle sfide enormi, stanti le limitate risorse umane a disposizione per traghettare verso le tecnologie più attuali servizi sviluppati internamente. Ove possibile, anche in questo caso, la scelta prioritaria sarà quella di fruire di servizi Cloud certificati con la logica SaaS first che risultino già implementati secondo queste logiche.

Il Responsabile della transizione digitale ha inviato la classificazione dei dati e dei servizi digitali dell'Università degli studi di Firenze il 16/07/2022 (entro i termini previsti dal primo regolamento cloud 2022), la cui conformità è stata convalidata da ACN. Egli ha verificato, altresì, di aver già migrato quanto possibile e di non aver, al momento, altre esigenze di migrazione e di dover mantenere il proprio data center per **motivi di didattica e di ricerca**.

L'Ateneo, compatibilmente con la necessaria continuità operativa da assicurare ai vari servizi digitali, all'opportunità e alla possibilità di una loro reingegnerizzazione, valuterà con attenzione l'attuazione del paradigma Cloud, nell'ottica di una graduale migrazione dei servizi verso modelli SaaS certificati, in ottemperanza alla normativa vigente e alle raccomandazioni di AgID e ACN.

A giugno 2024 è entrato in vigore il nuovo Regolamento Cloud ACN (n. 21007/24), applicabile dal 1° agosto 2024, che aggiorna i livelli minimi e le caratteristiche al mutato scenario di rischio e i termini legati al procedimento di rilascio delle qualifiche. Il regolamento definisce, armonizzandole in un unico quadro normativo, le misure minime che le infrastrutture come i data center e i servizi cloud devono rispettare per supportare i servizi pubblici.

Il provvedimento descrive come classificare i dati e i servizi digitali, rappresentando, a seconda del livello di importanza e sensibilità delle informazioni, una guida sicura per le Pubbliche Amministrazioni nella individuazione delle eventuali soluzioni cloud da acquisire.

OB.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 per la PA

RA6.1.1

Linee di azione vigenti

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 previsti nei propri piani di migrazione -

Codice Linea di Azione: CAP6.PA.01

Attività Operative: il RTD richiede l'autorizzazione, come stabilito dalla Circolare AGID 1/2019, ogni qualvolta si presenti la necessità di acquisti in materia di Data Center

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale

Le PA continuano ad applicare il principio *cloud first* e ad acquisire servizi *cloud* solo se qualificati o adeguati ai sensi del Regolamento cloud ACN 21007/24 - Codice Linea di Azione: CAP6.PA.04

Attività Operative: L'Ateneo, quando e se applicabile, continua ad applicare il principio cloud first e in tal caso acquisisce servizi cloud solo se qualificati o adeguati ai sensi del Regolamento cloud ACN 21007/24.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale

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 -
Codice Linea di Azione: CAP6.PA.05

Attività Operative: L'Ateneo si impegna ad aggiornare 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.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale

Linee di azione 2024-2026

Da settembre 2024 * - 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 - Codice Linea di Azione: CAP6.PA.06

Attività Operative: l'Università degli Studi di Firenze ha già migrato in cloud tutto ciò che è stato possibile. Sono in valutazione altre iniziative di migrazione (è in corso la migrazione di ulteriori siti web) e saranno attuate a seconda delle priorità e disponibilità di risorse.

Tempistiche di realizzazione e deadline:31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale

Capitolo 7 - Sicurezza informatica

Scenario

L'evoluzione delle moderne tecnologie ed il loro utilizzo per ottimizzare l'attività amministrativa offrono grandi opportunità, ma espongono anche le Pubbliche Amministrazioni al crescente rischio di attacchi cyber: ecco perché la sicurezza e la resilienza delle reti e dei sistemi su cui tali tecnologie poggiano diventano fondamentali.

Il 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" (convertito con modificazioni in legge 4 agosto 2021, n. 109) mira a sviluppare e a rafforzare le capacità difensive in termini di sicurezza informatica di tutte le Pubbliche Amministrazioni. Per fare ciò, grazie ai fondi PNRR e a quelli della Strategia nazionale di cybersicurezza, sono state destinate significative risorse alla sicurezza informatica e alle misure tese a realizzare un percorso di miglioramento della postura di sicurezza del sistema Paese nel suo insieme e, in particolare, della Pubblica Amministrazione, anche se come evidenziato in precedenza gli Atenei non sono soggetti che potevano partecipare a questi bandi.

Con il decreto legislativo 4 settembre 2024 n. 138, l'Italia ha recepito nell'ordinamento nazionale la direttiva (UE) 2022/2555 (cd. Direttiva NIS2 - *Network and Information Security*), relativa a misure per un livello comune elevato di sicurezza informatica nell'Unione. Ai sensi della predetta disciplina, l'ACN è l'Autorità competente NIS e punto di contatto unico, mentre il Ministero dell'Università e della Ricerca (MUR) è l'autorità di settore per l'Ateneo. L'Università degli studi di Firenze sta proseguendo il proprio percorso di verifica della corrispondenza delle proprie strutture e dei propri processi in materia di sicurezza informatica alla normativa NIS2 e sta gradualmente definendo ruoli e procedure atti ad una gestione ottimale di tutti gli aspetti della cybersicurezza, dalla gestione del rischio alla segnalazione tempestiva degli incidenti informatici. Mantiene attivo il proprio impegno nelle attività di monitoraggio delle criticità e di erogazione di corsi di formazione mirati e diversificati a seconda del ruolo svolto all'interno della comunità universitaria (personale tecnico-amministrativo, docenti, dirigenti).

Obiettivo 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

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

Linee di azione per le PA

RA7.1.1

Da settembre 2024 - Le singole PA definiscono il modello unitario, assicurando un coordinamento centralizzato a livello dell'istituzione, di *governance* della cybersicurezza - Codice Linea di Azione: CAP7.PA.01

Attività Operative: L'Ateneo dà avvio alle attività di definizione della strategia di cybersecurity governance, dei ruoli, delle responsabilità e dei domini della cybersecurity, del modello operativo integrato di cybersecurity governance, e delle modalità di monitoraggio della strategia di cybersecurity governance, a seguito della pubblicazione di documenti informativi, che forniscono nozioni fondamentali, indicazioni metodologiche e operative sui temi di interesse da parte di ACN.

Tempistiche di realizzazione e deadline: A partire dal 2025 e comunque entro la scadenza prevista a Ottobre 2026 per l'adozione delle misure di base NIS2, il modello sarà declinato nell'organizzazione ed approvato dagli Organi di Ateneo.

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Sistemi, tecnologie cloud e di sicurezza informatica, Organi di amministrazione e direttivi, GdL dedicato

Da dicembre 2024 - Le PA adottano un modello di *governance* della cybersicurezza - Codice Linea di Azione: CAP7.PA.02

Attività Operative: L'Ateneo dà avvio alle attività di definizione della strategia di cybersecurity governance, dei ruoli, delle responsabilità e dei domini della cybersecurity, del modello operativo integrato di cybersecurity governance, e delle modalità di monitoraggio della strategia di cybersecurity governance, a seguito della pubblicazione di documenti informativi, che forniscono nozioni fondamentali, indicazioni metodologiche e operative sui temi di interesse da parte di ACN.

Tempistiche di realizzazione e deadline: A partire dal 2025 e comunque entro la scadenza prevista a Ottobre 2026 per l'adozione delle misure di base NIS2, il modello sarà declinato

nell'organizzazione ed approvato dagli Organi di Ateneo.

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Sistemi, tecnologie cloud e di sicurezza informatica, Organi di amministrazione e direttivi, GdL dedicato

Da dicembre 2024 - Le PA nominano i Responsabili della cybersicurezza e delle loro strutture organizzative di supporto - Codice Linea di Azione: CAP7.PA.03

Attività Operative: L'Ateneo ha dato avvio alle attività di definizione della struttura organizzativa della cybersecurity anche in base alle indicazioni recepite dalle Determinazioni ACN in ambito NSI2.

Tempistiche di realizzazione e deadline: Le tempistiche dovranno essere allineate alle scadenze di Ottobre 2026 entro le quali implementare le misure di base NIS2 in quanto l'organizzazione della cybersecurity è parte delle misure di base.

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Sistemi, tecnologie cloud e di sicurezza informatica, Organi di amministrazione e direttivi, GdL dedicato

RA7.1.2

Da dicembre 2024 - Le PA formalizzano i processi e le procedure inerenti alla gestione della cybersicurezza - Codice Linea di Azione: CAP7.PA.04

Attività Operative: L'Ateneo ha dato avvio anche grazie ad una consulenza a livello CODAU ad un processo di redazione dei piani previsti dalla normativa NIS2 a cui seguiranno la stesura di procedure a corredo dei piani stessi come richiesto dalla normativa nazionale.

Tempistiche di realizzazione e deadline: Ai fini degli adempimenti NIS2 la scadenza prevista è Ottobre 2026.

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Sistemi, tecnologie cloud e di sicurezza informatica, Organi di amministrazione e direttivi, GdL dedicato

Obiettivo 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

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

Linee di azione per le PA

RA7.2.1

Da giugno 2024 - Le PA definiscono e approvano i requisiti di sicurezza relativi al processo di approvvigionamento IT - Codice Linea di Azione: CAP7.PA.05

Attività Operative: Nell'ambito della compliance NIS2 il processo di revisione dei fornitori, le clausole per i contratti di appalti ed il monitoraggio della supply chain rientrano nelle misure di base richieste da ACN e di conseguenza nel 2026 è necessario rivedere criteri e modalità di approvvigionamento anche in questa logica

Tempistiche di realizzazione e deadline: Oltre al recepimento delle tempistiche che saranno pubblicate tramite le linee guida per la definizione dei requisiti di sicurezza nel processo di approvvigionamento IT da parte di ACN, come stabilito nel Codice Linea di Azione CAP7.03, entro Ottobre 2026 è previsto coprire i presidi delle misure di base NIS2 in relazione alla supply chain.

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Sistemi, tecnologie cloud e di sicurezza informatica, Organi di amministrazione e direttivi, GdL dedicato

Da dicembre 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 - Codice Linea di Azione: CAP7.PA.06

Attività Operative: Nell'ambito della compliance NIS2 il processo di revisione dei fornitori, le clausole per i contratti di appalti ed il monitoraggio della supply chain rientrano nelle misure di base richieste da ACN e, di conseguenza, nel 2026 è necessario rivedere criteri e modalità di approvvigionamento anche in questa logica

Tempistiche di realizzazione e deadline: Oltre al recepimento delle tempistiche che saranno recepite appena verranno pubblicate tramite le linee guida per la definizione dei requisiti di sicurezza nel processo di approvvigionamento IT da parte di ACN, come stabilito nel Codice Linea di Azione: CAP7.03, entro Ottobre 2026 è previsto coprire i presidi delle misure di base NIS2 in relazione alla supply chain.

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Sistemi, tecnologie cloud e di sicurezza informatica, Organi di amministrazione e direttivi, GdL dedicato

RA7.2.2

Da dicembre 2025 - Le PA realizzano le attività di controllo definite nel Piano di *audit* e verifica verso i fornitori e terze parti IT - Codice Linea di Azione: CAP7.PA.07

Attività Operative: Nel 2026 saranno rivisti i criteri interni per le attività di controllo definite nel piano di Audit e verifica dei fornitori, considerando anche i presidi previsti dalla NIS2 in ambito di controllo della supply chain

Tempistiche di realizzazione e deadline: da definire in funzione delle linee guida che saranno vigenti nel 2026 e comunque almeno i presidi NIS2 entro Ottobre 2026.

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Sistemi, tecnologie cloud e di sicurezza informatica, Organi di amministrazione e direttivi, GdL dedicato

Obiettivo 7.3 - Gestione e mitigazione del rischio cyber

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

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

Linee di azione per le PA

RA7.3.1

Da dicembre 2024 - Le PA definiscono e formalizzano il processo di *cyber risk management* e *security by design*, coerentemente con gli strumenti messi a disposizione da ACN - Codice Linea di Azione: CAP7.PA.08

Attività Operative: L'Ateneo dà avvio alle attività di definizione del processo di cyber risk management, a seguito della pubblicazione di documenti informativi, che forniscono nozioni fondamentali, indicazioni metodologiche e operative sul tema da parte di ACN. (L'Agenzia fornisce le Linee guida per la definizione dei processi di cyber risk management e security by design - (ACN) - Codice Linea di Azione: CAP7.05). Avendo già utilizzato in passato il tool di cyber risk assessment di AGID, l'Ateneo sta monitorando le funzionalità del tool ora passato all'Agenzia per valutare eventuali modifiche ed innovazioni. Oltre a questi elementi oltre a

definire un primo modello di valutazione del rischio e delle relative soglie di mitigazione effettuato nel 2025 è in sviluppo un modello più articolato e più vicino sia alla 270005 che al NIST nonché in linea con le linee guida ACN utilizzate anche per il perimetro di sicurezza nazionale.

Tempistiche di realizzazione e deadline: da definire in funzione delle linee guida, ma entro Giugno 2026 è prevista la revisione del calcolo del rischio almeno per i Servizi censiti per la NIS2.

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Sistemi, tecnologie cloud e di sicurezza informatica, Organi di amministrazione e direttivi, GdL dedicato

Dicembre 2025 - Le PA promuovono il censimento dei dati e servizi della PA, identificandone la rilevanza e quindi le modalità per garantirne la continuità operativa - Codice Linea di Azione: CAP7.PA.09

Attività Operative: In vista di questa scadenza, l'Ateneo sta realizzando una tabella dei servizi principali di Ateneo e di come essi possano essere impattati da diverse tipologie di disservizio o disastro corredata nei vari casi dalle misure esistenti o da quelle da prendere per minimizzare gli impatti e garantire la continuità operativa dei Servizi. La garanzia totale di copertura della continuità operativa può essere ragionevolmente raggiunta solo nel caso di migrazione verso servizi IaaS, PaaS, SaaS in datacenter che offrano una naturale ridondanza geografica.

Tempistiche di realizzazione e deadline: Avendo, a partire da dicembre 2024, avviato un censimento dei dati e dei servizi, con l'analisi di impatto per i servizi più rilevanti, ed avendo nel 2025 iniziato a censire a fini NIS2 i servizi erogati internamente e da parte di fornitori esterni, nel 2026 andrà affinato il modello di calcolo del rischio ed stabilito un remediation plan che tenga conto dei presidi nelle misura di base NIS2 in questo ambito..

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Sistemi, tecnologie cloud e di sicurezza informatica, Organi di amministrazione e direttivi, GdL dedicato

Dicembre 2026 - 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 - Codice Linea di Azione: CAP7.PA.11

Attività Operative: L'Ateneo nel corso del 2026 rivedrà il modello di valutazione del rischio proposto nel 2025 e provvederà a stabilire piani di mitigazione appositi anche in base alle misure di base previste per la NIS2 implementando e migliorando le attività di monitoraggio continuo del rischio cyber.

Tempistiche di realizzazione e deadline: 31/12/2026 con deadline intermedia a Ottobre 2026 per i presidi NIS2

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Sistemi, tecnologie cloud e di sicurezza informatica,

RA7.3.2

Da 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 - Codice Linea di Azione: CAP7.PA.12

Attività Operative: L'Ateneo nel corso del 2026 inizierà le attività di monitoraggio continuo del rischio cyber.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Sistemi, tecnologie cloud e di sicurezza informatica

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

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

Linee di azione per le PA

RA7.4.1

Da giugno 2024 - Le PA definiscono i presidi per la gestione degli eventi di sicurezza, formalizzandone i processi e le procedure - Codice Linea di Azione: CAP7.PA.13

Attività Operative: Nel corso del 2025 l'Ateneo ha avviato un percorso di rafforzamento delle proprie capacità di governo e coordinamento in ambito di sicurezza informatica, adottando soluzioni tecnologiche e organizzative a supporto del monitoraggio degli eventi e della gestione degli incidenti, nonché formalizzando una prima procedura interna coerente con il quadro normativo introdotto dalla direttiva NIS 2. Nel corso del 2026 è programmato un ulteriore consolidamento di tali capacità attraverso il ricorso a servizi specializzati, con l'obiettivo di migliorare l'efficacia operativa nella gestione degli incidenti, incrementare la tempestività di risposta e potenziare le attività di individuazione precoce di eventi rilevanti o potenzialmente incidentali.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Sistemi, tecnologie cloud e di sicurezza informatica

Da dicembre 2024 - Le PA formalizzano ruoli, responsabilità e processi, nonché le capacità tecnologiche a supporto della prevenzione e gestione degli incidenti informatici - Codice Linea di Azione: CAP7.PA.14

Attività Operative: L'Ateneo prosegue nel percorso di valutazione e adozione di soluzioni tecnologiche e servizi specialistici a supporto delle attività di prevenzione, monitoraggio e gestione degli incidenti informatici, con particolare attenzione al rafforzamento dei processi organizzativi e delle capacità di risposta. Nel corso del 2025 sono state consolidate alcune misure già in essere ed è stato avviato un primo intervento strutturato volto a migliorare il coordinamento nella gestione degli eventi di sicurezza, accompagnato dalla definizione di una procedura interna coerente con i requisiti introdotti dalla direttiva NIS 2. Nel corso del 2026 è prevista un'ulteriore evoluzione del modello operativo attraverso l'integrazione di servizi esterni qualificati, finalizzati ad aumentare la tempestività di intervento, la capacità di individuazione precoce di eventi rilevanti e il supporto continuativo alle attività di gestione degli incidenti.

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici/Settore Sistemi, tecnologie cloud e di

sicurezza informatica

RA7.4.2

Da dicembre 2024 - Le PA definiscono le modalità di verifica dei Piani di risposta a seguito di incidenti informatici - Codice Linea di Azione: CAP7.PA.15

Attività Operative: A seguito di ogni incidente informatico viene predisposto un audit atto a definire i contorni dell'incidente, la sua rilevanza e le contromisure da prendere per evitarne il ripetersi. Tale audit viene riportato in rapporti trimestrali sulla sicurezza in essere già da alcuni anni in Ateneo e le procedure di risposta sono adeguate sulla base delle evidenze dell'audit.

Tempistiche di realizzazione e deadline: audit al bisogno con processo di miglioramento continuo sia delle misure che delle procedure. Da considerarsi i presidi entro Ottobre 2026 previsti in questo ambito dalle misure di base NIS2.

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici

Da dicembre 2025 - Le PA definiscono le modalità di aggiornamento dei Piani di risposta e ripristino a seguito dell'accadimento di incidenti informatici - Codice Linea di Azione: CAP7.PA.16

Attività Operative: L'Ateneo è impegnato a definire le procedure per il ripristino di dati e servizi in seguito ad incidenti informatici definendo strumenti e procedure. Nel 2025 è stata completata la revisione dell'architettura del backup per aumentare la resilienza generale rispetto ad accadimenti che richiedano un ripristino di dati e servizi.

Tempistiche di realizzazione e deadline: L'ateneo, nel corso del 2026, grazie anche alle nuove licenze e strumenti previsti dal sistema di backup elaborerà un piano di adozione di verifica dei backup e simulazione di ripristino.

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici

Obiettivo 7.5 - Implementare attività strutturate di sensibilizzazione cyber del personale

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

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

Linee di azione per le PA

RA7.5.1

Da giugno 2024 - Le PA promuovono l'accesso e l'utilizzo di attività strutturate di sensibilizzazione e formazione in ambito cybersicurezza - [Codice Linea di Azione: CAP7.PA.17](#)

Attività Operative: Saranno proposte azioni formative dedicate e campagne di sensibilizzazione

Tempistiche di realizzazione e deadline: processo di miglioramento continuo sia delle misure che delle procedure, pianificazione delle relative attività formative in accordo con il piano di Ateneo

Strutture responsabili: Ufficio per la Transizione al Digitale, UP Formazione, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici, GdL dedicato

Da dicembre 2024 - Le PA definiscono piani di formazione inerenti alla cybersecurity, diversificati per ruoli, posizioni organizzative e attività delle risorse dell'organizzazione - Codice Linea di Azione: CAP7.PA.18

Attività Operative: Saranno proposte azioni formative dedicate

Tempistiche di realizzazione e deadline: pianificazione delle relative attività formative in accordo con il piano di Ateneo

Strutture responsabili: Ufficio per la Transizione al Digitale, UP Formazione, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici

RA7.5.2

Da dicembre 2025 - Le PA realizzano iniziative per verificare e migliorare la consapevolezza del proprio personale - Codice Linea di Azione: CAP7.PA.19

Attività Operative: l'Ateneo ha aderito nel 2025 al progetto Cyber Sapere del MUR che prevede varie attività di sensibilizzazione.

Tempistiche di realizzazione e deadline: Le attività seguiranno la pianificazione del progetto Cyber Sapere e le tempistiche previste dal MUR

Strutture responsabili: Ufficio per la Transizione al Digitale, UP Formazione, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici, GdL dedicato

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

RA7.6.1 - Distribuzione di Indicatori di Compromissione alle PA

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

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 per le PA

RA7.6.1

Da dicembre 2024 * - 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 Amministrazione da minacce *Malware* e *Phishing* - Codice Linea di Azione: CAP7.PA.20

Attività Operative: L'Ateneo ha già aderito continuerà ad alimentare il flusso di indicatori

Tempistiche di realizzazione e deadline: 31/12/2026

Strutture responsabili: Ufficio per la Transizione al Digitale, Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici

RA7.6.2

Da dicembre 2024 * - Le PA dovranno usufruire degli strumenti per la gestione dei rischi cyber messi a disposizione dal CERT-AgID - Codice Linea di Azione: CAP7.PA.21

Attività Operative: L'Ateneo ha già partecipato alla sperimentazione del tool di cyber risk assessment di AGID e, di conseguenza, non appena saranno fruibili ulteriori strumenti, ne valuterà l'adozione.

Tempistiche di realizzazione e deadline: dipendenti dalle tempistiche con cui gli strumenti saranno messi a disposizione dal CERT-AGID

Strutture responsabili: Ufficio per la Transizione al Digitale

RA7.6.3

Dicembre 2025 - Le PA, sulla base delle proprie esigenze, partecipano ai corsi di formazione



base ed avanzato erogati dal CERT-AgID - Codice Linea di Azione: CAP7.PA.22

Attività Operative: L'Ateneo parteciperà alle iniziative formative promosse dal CERT-AGID

Tempistiche di realizzazione e deadline: definite da CERT-AGID

Strutture responsabili: Ufficio per la Transizione al Digitale

APPENDICE 1 - Glossario e Acronimi

- **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.
- **AVA:** Autovalutazione, Valutazione, Accreditamento, è il modello italiano di assicurazione della qualità per le università, gestito dall'Agenzia Nazionale per la Valutazione dell'Università e della Ricerca (ANVUR), che mira a migliorare didattica e ricerca attraverso processi interni di autovalutazione e valutazione esterna da parte di commissioni di esperti, culminando in un giudizio di accreditamento per sedi e corsi di studio.
- **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).
- **EDUROAM:** Education Roaming, è un servizio di roaming wireless sicuro che permette a studenti, ricercatori e personale di università e istituti di ricerca di accedere a Internet

tramite Wi-Fi, usando le proprie credenziali istituzionali, sia nel proprio ente che in qualsiasi altra istituzione aderente a livello globale.

- **FVOE:** Il Fascicolo Virtuale dell'Operatore Economico è conservato presso la Banca dati nazionale dei contratti pubblici. Consente la verifica dell'assenza di cause di esclusione di partecipazione alle Gare e raccoglie i dati e i documenti relativi ai requisiti inseriti dall'Operatore Economico.
- **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.
- **MUR:** Ministero dell'Università e della Ricerca
- **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.
- **Openness:** 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.
- **PSN:** il Polo Strategico Nazionale è un'infrastruttura cloud sicura per la Pubblica Amministrazione che gestisce dati e servizi critici per il Paese.
- **RTD:** Responsabile per la Transizione al 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.
- **START:** Il Sistema Telematico Acquisti Regionale della Toscana è la piattaforma digitale della Regione Toscana per gestire tutte le procedure di appalto e acquisto pubblico in modo telematico.
- **STEM:** Science, Technology, Engineering, Mathematics.
- **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.

APPENDICE 2 - Riferimenti normativi

RIFERIMENTI NORMATIVI ITALIANI:

- Decreto legislativo 7 marzo 2005, n. 82 “Codice dell'amministrazione digitale” (in breve CAD);
- Circolare n. 3 del 1° ottobre 2018 del Ministro per la Pubblica Amministrazione sul Responsabile per la transizione al digitale;
- Direttiva del Ministro per la Pubblica Amministrazione del 23 marzo 2023 “Pianificazione della formazione e sviluppo delle competenze funzionali alla transizione digitale, ecologica e amministrativa promosse dal Piano Nazionale di Ripresa e Resilienza”;
- Direttiva del Ministro per la Pubblica Amministrazione del 14 gennaio 2025 “Valorizzazione delle persone e produzione di valore pubblico attraverso la formazione. Principi, obiettivi e strumenti”;
- Piano Nazionale di Ripresa e Resilienza: M1C1 - Investimento 1.7: "Competenze digitali di base":
 - MIC1 - Investimento 2.3: “Competenze e capacità amministrativa”;
 - M4C2.3 - “Potenziamento delle condizioni di supporto alla ricerca e all’innovazione”;
- Legge 24 dicembre 2007, n. 244 “Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato” (legge finanziaria 2008);
- 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”;
- Legge 27 dicembre 2017, n. 205 “Bilancio di previsione dello Stato per l'anno finanziario 2018 e bilancio pluriennale per il triennio 2018-2020”;
- 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 legislativo 31 marzo 2023, n. 36 “Codice dei contratti pubblici”;
- Decreto-legge 2 marzo 2024, n. 19 “Ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR);
- Decreto legislativo 31 dicembre 2024, n. 209 “Disposizioni integrative e correttive al codice dei contratti pubblici, di cui al decreto legislativo 31 marzo 2023, n. 36”;
- 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”;
- 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”;
- Determinazione AgID n. 137 del 1° giugno 2023 “Requisiti tecnici e modalità di

certificazione delle Piattaforme di approvvigionamento digitale”;

- Determinazione AgID n. 218 del 25 settembre 2023 “Schema operativo a supporto della Certificazione delle Piattaforme di approvvigionamento digitale”;
- Decisione di esecuzione del Consiglio del 13 luglio 2021, che approva il Piano Nazionale di ripresa e resilienza (Allegato);
- 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.
- Legge 28 dicembre 2015, n. 208 - “Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge di stabilità 2016);
- Decreto legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”;
- 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”;
- 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 - Presidenza del Consiglio dei Ministri - Dipartimento per la Trasformazione Digitale;
- 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 (2025);
- Linee Guida AgID Tecnologie e standard per la sicurezza dell’interoperabilità tramite API dei sistemi informatici;
- Direttiva concernente “Misure per l’attuazione dell’articolo 50-ter del decreto legislativo 7 marzo 2005, n. 82” del 28 febbraio 2024;

- Piano Nazionale di Ripresa e Resilienza:
 - Investimento M1C1 1.3: “Dati e interoperabilità”;
 - Investimento M1C1 2.2: “Task Force digitalizzazione, monitoraggio e performance”;
- Legge 9 gennaio 2004, n. 4 (Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici);
- Decreto Ministeriale 30 aprile 2008 (Regole tecniche disciplinanti l'accessibilità agli strumenti didattici e formativi a favore degli alunni disabili);
- Legge 3 marzo 2009, n. 18 - Ratifica ed esecuzione della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità;
- Decreto Legislativo 10 agosto 2018, n. 106 (Attuazione della direttiva (UE) 2016/2102 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici);
- Legge 241/1990, Nuove norme sul procedimento amministrativo;
- 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 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);
- Decreto Legislativo 27 maggio 2022, n. 82 - “Attuazione della direttiva (UE) 2019/882 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sui requisiti di accessibilità dei prodotti e dei servizi”;
- Linee Guida AgID su acquisizione e riuso del software per la Pubblica Amministrazione (2019);
- Linee Guida AgID sull'accessibilità degli strumenti informatici (2022);
- Linee Guida AgID di design per i siti internet e i servizi digitali della PA (2022);
- Determinazione AgID n.354/2022 del 22 dicembre 2022 - Linee Guida sull'accessibilità degli strumenti informatici adottate con Determinazione n. 437/2019 del 20 dicembre 2019 e rettificata con Determinazione n. 396/2020 del 10 settembre 2020 - Rettifica per adeguamento a norma tecnica europea armonizzata sopravvenuta;
- Piano Nazionale di Ripresa e Resilienza:

- M1C1 - Investimento 1.4: "Servizi digitali e cittadinanza digitale";
- Decreto-legge. 26 ottobre 2019, n. 124 convertito dalla legge 12 dicembre 2019, n. 157 "Disposizioni urgenti in materia fiscale e per esigenze indifferibili";
- Linee Guida AgID per l'Effettuazione dei Pagamenti Elettronici a favore delle Pubbliche Amministrazioni e dei Gestori di Pubblici Servizi (2018);
- Decreto del Presidente del Consiglio dei ministri del 10 agosto 2023 "Ripartizione delle risorse del Fondo straordinario per gli interventi di sostegno all'editoria per l'anno 2023";
- Linee Guida AgID per l'accesso telematico ai servizi della Pubblica Amministrazione (2021);
- Legge n. 160 del 2019 "Bilancio di previsione dello Stato per l'anno finanziario 2020 e bilancio pluriennale per il triennio 2020-2022";
- Decreto della Presidenza del Consiglio dei Ministri – Dipartimento per la trasformazione digitale del 8 febbraio 2022, n. 58 "Regolamento recante piattaforma per la notificazione degli atti della pubblica amministrazione";
- 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);
- 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-legge 9 giugno 2015, n. 78 "Disposizioni urgenti in materia di enti territoriali";
- Decreto Ministeriale del Ministro dell'Interno 23 dicembre 2015 - Modalità tecniche di emissione della Carta d'identità elettronica;
- Decreto Ministeriale del Ministro dell'Interno 8 settembre 2022 – Modalità di impiego

della carta di identità elettronica;

- Legge 31 dicembre 2009, n. 196 Legge di contabilità e finanza pubblica;
- Legge 27 dicembre 2013, n. 147 Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (Legge di stabilità 2014);
- Legge 11 dicembre 2016, n. 232 Bilancio di previsione dello Stato per l'anno finanziario 2017 e bilancio pluriennale per il triennio 2017-2019;
- Legge 30 dicembre 2020, n. 178 Bilancio di previsione dello Stato per l'anno finanziario 2021 e bilancio pluriennale per il triennio 2021-2023;
- Decreto del Ministro dell'Economia e delle Finanze del 14 giugno 2017;
- Decreto del Ministro dell'Economia e delle Finanze del 26 febbraio 2018 concernente l'anticipo dell'avvio a regime di SIOPE+ per singoli enti;
- Decreto del Ministro dell'Economia e delle Finanze 29 maggio 2018 concernente la codifica gestionale delle Autorità di sistema portuali;
- Decreto del Ministro dell'Economia e delle Finanze del 30 maggio 2018 concernente l'estensione di SIOPE + agli enti soggetti alla rilevazione SIOPE;
- Decreto del Ministro dell'Economia e delle Finanze del 23 luglio 2019, concernente la codifica gestionale delle Fondazioni lirico-sinfoniche, con decorrenza 1° gennaio 2020, di cui al decreto legislativo 29 giugno 1996, n. 367, e successive modificazioni, e di cui alla legge 11 novembre 2003, n. 310;
- Decreto del Ministro dell'Economia e delle Finanze del 8 agosto 2019, concernente la codifica gestionale delle Autorità amministrative indipendenti, con decorrenza 1° gennaio 2020, inserite nell'elenco delle amministrazioni pubbliche di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n.196 e successive modificazioni, escluse la Commissione di garanzia dell'attuazione della legge sullo sciopero nei servizi pubblici essenziali (CGSSE) e l'Agenzia nazionale di valutazione del sistema universitario e della ricerca (ANVUR);
- Delibera CIPE n. 114, del 23 Dicembre 2015 "Programma complementare di azione e coesione per la governance dei sistemi di gestione e controllo 2014-2020";
- Decreto-legge 6 novembre 2021, n. 152, convertito con modificazioni dalla Legge 29 dicembre 2021, n. 233 "Disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per la prevenzione delle infiltrazioni mafiose";
- Linee Guida AgID sull'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese (2023);
- Decreto del Presidente del Consiglio dei Ministri 10 novembre 2014, n. 194, Regolamento recante modalità di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (ANPR) e di definizione del piano per il graduale subentro dell'ANPR alle anagrafi della popolazione residente;
- Decreto del Presidente del Consiglio dei Ministri, 23 agosto 2013, n. 109, Regolamento recante disposizioni per la prima attuazione dell'articolo 62 del decreto legislativo 7

marzo 2005, n. 82;

- Decreto del Ministero dell'interno del 3 novembre 2021 Modalità di erogazione da parte dell'Anagrafe nazionale della popolazione residente dei servizi telematici per il rilascio di certificazioni anagrafiche on-line e per la presentazione on-line delle dichiarazioni anagrafiche;
- Decreto del Ministero dell'Interno del 17 ottobre 2022, Modalità di integrazione nell'ANPR delle liste elettorali e dei dati relativi all'iscrizione nelle liste di sezione di cui al decreto del Presidente della Repubblica 20 marzo 1967, n. 223;
- Decreto del Ministero dell'interno del 18 ottobre 2022, Aggiornamento della piattaforma di funzionamento dell'Anagrafe nazionale della popolazione residente per l'erogazione dei servizi resi disponibili ai comuni per l'utilizzo dell'Archivio nazionale informatizzato dei registri dello stato civile;
- Decreto del Ministero dell'interno del 3 marzo 2023 - Modalità di attribuzione, da parte dell'Anagrafe nazionale della popolazione residente, di un codice identificativo univoco per garantire la circolarità dei dati anagrafici e l'interoperabilità con le altre banche dati delle pubbliche amministrazioni e dei gestori di servizi pubblici;
- Decreto-legge 9 maggio 2003, n. 105 "Disposizioni urgenti per le università e gli enti di ricerca nonché in materia di abilitazione all'esercizio delle attività professionali";
- Decreto del Ministero dell'Università e Ricerca del 19 gennaio 2022 "Prima attuazione delle disposizioni istitutive dell'Anagrafe nazionale dell'istruzione superiore (ANIS)";
- Decreto del Ministero dell'Università e della Ricerca del 30 settembre 2022 "Seconda attuazione delle disposizioni istitutive dell'Anagrafe nazionale dell'istruzione superiore (ANIS)".
- Decreto del Ministero dell'Istruzione e del Merito del 7 dicembre 2023, n. 234, "Regolamento sulle modalità di attuazione e funzionamento dell'Anagrafe nazionale dell'istruzione";
- 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 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);
- Linee Guida AgID per i cataloghi dati (2017);
- Linee Guida AgID per l'implementazione della specifica GeoDCAT-AP (2017);

- Linee Guida AgID recanti regole tecniche per la definizione e l'aggiornamento del contenuto del Repertorio Nazionale dei Dati Territoriali (2022);
- Linee Guida AgID recanti regole tecniche per l'attuazione del decreto legislativo 24 gennaio 2006, n. 36 e s.m.i. relativo all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico adottate con Determinazione AgID n. 183/2023 del 3 agosto 2023;
- Manuale RNDT - Guide operative per la compilazione dei metadati RNDT;
- Guida operativa sulle serie di dati di elevato valore;
- 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";
- 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 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”;
- 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;
 - Decreto Legislativo 4 settembre 2024, n. 138, “Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148. (24G00155)”;
 - 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”;
 - 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 per le infrastrutture digitali e per i servizi cloud per la pubblica amministrazione, ai sensi dell’articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221 (2024) (Regolamento cloud per le PA di ACN ai sensi dell’art. 26 del Decreto Direttoriale ACN n.21007/2024);
 - Piano Nazionale di Ripresa e Resilienza:
 - M1C1 Investimento 1.1: “Infrastrutture digitali”;
 - M1C1 Investimento 1.2: “Abilitazione e facilitazione migrazione al cloud”;
 - Strategia italiana per l’intelligenza artificiale 2024-2026.

RIFERIMENTI NORMATIVI EUROPEI:

- Raccomandazione del Consiglio del 22 maggio 2018 relativa alle competenze chiave per l’apprendimento permanente (GU 2018/C 189/01);
- Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni COM (2020) 67 final del 19 febbraio 2020 - Plasmare il futuro digitale dell'Europa;
- Decisione (EU) 2022/2481 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 che istituisce il programma strategico per il Decennio Digitale 2030;
- Decisione del Parlamento Europeo e del Consiglio relativa a un Anno Europeo delle Competenze 2023 COM (2022) 526 final 2022/0326;
- 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 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;
- 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;
- 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);
- Regolamento (UE) 2024/903 del Parlamento europeo e del Consiglio, del 13 marzo 2024, che stabilisce misure per un livello elevato di interoperabilità del settore pubblico nell'Unione (regolamento su un'Europa interoperabile);
- Direttiva (UE) 2016/2102 del 26 ottobre 2016 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici;
- Decisione di esecuzione (UE) 2018/1524 della Commissione dell'11 ottobre 2018 che stabilisce una metodologia di monitoraggio e definisce le disposizioni riguardanti la presentazione delle relazioni degli Stati membri conformemente alla direttiva (UE) 2016/2102 del Parlamento europeo e del Consiglio relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici;
- Direttiva (UE) 2019/882 del parlamento europeo e del consiglio, del 17 aprile 2019, sui requisiti di accessibilità dei prodotti e dei servizi;
- Decisione di esecuzione (UE) 2021/1339 della Commissione dell'11 agosto 2021 che modifica la decisione di esecuzione (UE) 2018/2048 per quanto riguarda la norma armonizzata per i siti web e le applicazioni mobili;
- Web Content Accessibility Guidelines (WCAG) 2.2;
- Regolamento di esecuzione (UE) 2022/1463 del 5 agosto 2022 che definisce le specifiche tecniche e operative del sistema tecnico per lo scambio transfrontaliero automatizzato di

prove e l'applicazione del principio "una tantum" o "once only";

- Regolamento (UE) 2019/1157 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;
- 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;
- 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;
- 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;
- Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847;
- Comunicazione della Commissione 2014/C 240/01 del 24 luglio 2014 - Orientamenti sulle licenze standard raccomandate, i dataset e la tariffazione del riutilizzo dei documenti;
- Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni COM (2020) del 19 febbraio 2020 – Una strategia europea per i dati;
- Comunicazione della Commissione al Parlamento Europeo e al Consiglio, "Piano

Coordinato sull'Intelligenza Artificiale”, COM (2021) 205 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;
- Comunicazione della Commissione al Parlamento Europeo e al Consiglio “Sulla promozione delle start-up e dell'innovazione nell'IA affidabile”, COM (2024) 28 del 24 gennaio 2024;
- Regolamento (UE) 2024/1689 del 13 giugno 2024 del Parlamento europeo e del Consiglio “che stabilisce regole armonizzate sull'intelligenza artificiale”;
- Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, "Piano d'azione per il continente dell'IA”, COM(2025) 165 final del 9 aprile 2025;
- 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;
- Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022;
- Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza 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);
- Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il Regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (Regolamento sui dati);
- 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'Agencia 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»).

RIFERIMENTI NORMATIVI UNIFI:

- Statuto dell'Università degli Studi di Firenze (DR 1680/2018);
- Regolamento Generale di Ateneo (DR 991/2020);
- Regolamento dell'Albo Ufficiale di Ateneo (DR 1087/2013);
- Regolamento di Ateneo sulla disciplina del diritto di accesso (DR 508/2023);



- Regolamento di utilizzo dei servizi di comunicazione (DR 22/2025);
- Regolamento del Sistema Informatico dell'Ateneo Fiorentino (DR 15/2021);
- Regolamento del Sistema Archivistico di Ateneo (DR 707/2023);
- Regolamento per il trattamento dei dati sensibili e giudiziari in attuazione del Decreto legislativo 196/2003 (DR 906/2006);
- Regolamento di attuazione del Codice di protezione dei dati personali in possesso dell'Università degli Studi di Firenze (DR 1177/2005);
- Codice etico e di comportamento (DR 245/2025).