UNIVERSITÀ DI NAPOLI
L'ORIENTALE

Piano Triennale di Transizione Digitale 2026–2028

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

Sommario

PARTE I – CONTESTO STRATEGICO E GOVERNANCE

1. Premessa

Il presente Piano Triennale di Transizione Digitale 2026–2028 dell'Università di Napoli L'Orientale definisce la strategia di sviluppo e innovazione del sistema informativo, tecnologico e digitale dell'Ateneo, in coerenza con il quadro normativo nazionale ed europeo in materia di amministrazione digitale, sicurezza informatica e protezione dei dati personali.

Il documento si inserisce nel sistema integrato di pianificazione dell'Ateneo e costituisce, in attuazione delle disposizioni del Codice dell'Amministrazione Digitale (D.Lgs. 82/2005), lo strumento attraverso il quale l'Università pianifica, coordina e monitora gli interventi finalizzati alla trasformazione digitale dei processi e dei servizi, nel rispetto dei principi di efficacia, trasparenza, accessibilità e sostenibilità.

La redazione del Piano risponde ai compiti attribuiti al Responsabile per la Transizione Digitale (RTD) ai sensi dell'art. 17 del CAD, in raccordo con le *Linee Guida e con il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024–2026 – Aggiornamento 2026 dell'Agenzia per l'Italia Digitale (AgID).*

Il documento rappresenta pertanto il quadro di riferimento per l'attuazione della strategia digitale di Ateneo, assicurando l'allineamento con il Piano Strategico 2024–2026 e con il Piano Integrato di Attività e Organizzazione (PIAO) 2025–2027, con l'obiettivo di promuovere l'efficienza dei processi, la semplificazione amministrativa, l'interoperabilità dei sistemi e la valorizzazione del capitale informativo pubblico.

1.1 Finalità del Piano

Il Piano Triennale di Transizione Digitale (PTTD) definisce gli indirizzi strategici e operativi dell'Università di Napoli L'Orientale in materia di innovazione tecnologica, digitalizzazione dei processi e governance dei sistemi informativi.

Esso traduce le strategie nazionali e comunitarie in un quadro coerente con le specificità organizzative e funzionali dell'Ateneo, individuando le azioni necessarie a garantire la progressiva attuazione dell'amministrazione digitale, in conformità con i principi del Codice dell'Amministrazione Digitale (D.Lgs. 82/2005) e con le Linee Guida AgID.

In coerenza con le priorità delineate dal Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024–2026 – Aggiornamento 2026, il Piano persegue l'obiettivo di orientare l'azione dell'Ateneo verso un modello di governance digitale integrata, in grado di assicurare la qualità, la sicurezza e la sostenibilità dei servizi pubblici digitali, valorizzando al contempo il patrimonio informativo e tecnologico dell'istituzione.

L'azione pianificatoria si articola lungo alcune direttrici fondamentali.

In primo luogo, il Piano intende promuovere la piena attuazione dei diritti di cittadinanza digitale, attraverso la progettazione e l'erogazione di servizi accessibili, interoperabili e sicuri, che consentano a studenti, personale e stakeholder di interagire con l'Ateneo in modalità completamente digitale.

Parallelamente, esso mira a consolidare un modello di gestione dei dati e delle informazioni fondato su criteri di qualità, trasparenza e interoperabilità, in linea con le politiche europee di data governance e con la strategia nazionale per il patrimonio informativo pubblico.

Un ulteriore obiettivo consiste nel garantire la continuità operativa e la resilienza delle infrastrutture ICT, mediante l'adozione di architetture cloud ibride conformi alle Linee Guida AgID e alla Direttiva (UE) 2022/2555 (NIS2), applicando in modo sistematico i principi di security-by-design e privacy-by-design.

Contestualmente, si rafforza l'impegno dell'Ateneo verso la tutela dei dati personali e la protezione delle informazioni trattate, in osservanza del Regolamento (UE) 2016/679 (GDPR) e del D.Lgs. 196/2003, mediante un'integrazione organica tra misure tecniche, organizzative e procedurali di sicurezza.

Il processo di transizione digitale è concepito soprattutto come trasformazione culturale. Per questo, il Piano promuove la diffusione di una cultura dell'innovazione basata sulla crescita delle competenze digitali del personale docente, tecnico-amministrativo e di supporto, favorendo l'adozione consapevole delle tecnologie emergenti e la partecipazione attiva al cambiamento organizzativo.

Nel suo complesso, il presente documento rappresenta lo strumento attraverso cui l'Ateneo orienta, coordina e misura le iniziative digitali, assicurando la tracciabilità degli interventi del prossimo triennio e la valutazione dei risultati in termini di efficacia, efficienza e creazione di valore pubblico, secondo un approccio coerente con le metodologie di pianificazione previste dall'Agenzia per l'Italia Digitale

1.2 Quadro normativo di riferimento

La definizione e l'attuazione del Piano Triennale di Transizione Digitale si fondano su un corpus organico di norme europee, nazionali e interne che disciplinano l'amministrazione digitale, la sicurezza dei sistemi informativi, la protezione dei dati personali e la gestione del ciclo di vita dei contratti e dei servizi ICT. Tali riferimenti costituiscono il quadro regolatorio di riferimento cui il Piano si conforma e dal quale discendono gli obblighi, i principi e le linee di indirizzo cui l'Ateneo è tenuto a uniformare la propria azione di digitalizzazione.

Il principale riferimento normativo è rappresentato dal Codice dell'Amministrazione Digitale (D.Lgs. 82/2005 e s.m.i.), che stabilisce i diritti di cittadinanza digitale, i criteri per l'erogazione dei servizi pubblici digitali, la validità giuridica dei documenti informatici e i compiti del Responsabile per la Transizione Digitale, figura prevista dall'art. 17 del Codice. Il Piano recepisce tali disposizioni orientando la pianificazione tecnologica e organizzativa dell'Ateneo al rispetto dei principi di efficacia, efficienza, trasparenza, sicurezza e accessibilità.

Di particolare rilievo sono le disposizioni dell'Agenzia per l'Italia Digitale (AgID), in particolare il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024–2026 – Aggiornamento 2026, che definisce la strategia digitale nazionale e individua le misure operative relative a interoperabilità, infrastrutture cloud, piattaforme abilitanti, sicurezza informatica, dati e servizi digitali. Il presente Piano, in coerenza con le Linee Guida AgID, adotta la medesima articolazione per componenti strategiche e tecnologiche, recependo le indicazioni vincolanti e le raccomandazioni rivolte alle Pubbliche Amministrazioni, incluse le università.

Un ulteriore asse normativo è costituito dalla Direttiva (UE) 2022/2555 – NIS2, che innalza i requisiti di sicurezza delle reti e dei sistemi informativi stabilendo obblighi specifici per gli enti pubblici considerati "soggetti essenziali", categoria nella quale rientrano gli atenei. Essa richiede l'adozione di misure tecniche e organizzative proporzionate ai rischi, il

potenziamento della resilienza dei servizi digitali e la tempestiva gestione degli incidenti di sicurezza. Il Piano integra tali previsioni nel disegno complessivo della strategia di sicurezza e continuità operativa dell'Ateneo.

In materia di protezione dei dati personali, la normativa di riferimento è costituita dal Regolamento (UE) 2016/679 (GDPR) e dal D.Lgs. 196/2003, nella versione modificata dal D.Lgs. 101/2018. Tali fonti impongono l'adozione di misure idonee a garantire un trattamento dei dati conforme ai principi di liceità, correttezza, trasparenza, minimizzazione, integrità e riservatezza, oltre all'applicazione dei principi di privacy-by-design e privacy-by-default nei sistemi digitali dell'Ateneo.

Rilevanti per la pianificazione e il procurement ICT sono inoltre le disposizioni del D.Lgs. 36/2023 – Codice dei Contratti Pubblici, che introduce la digitalizzazione integrale del ciclo di vita dei contratti, l'uso delle piattaforme telematiche certificate, la tracciabilità dei flussi informativi e la qualificazione delle stazioni appaltanti. Tali previsioni incidono direttamente sulla gestione delle acquisizioni ICT, sulla scelta delle soluzioni tecnologiche e sulla programmazione degli investimenti digitali dell'Ateneo.

Il quadro normativo di riferimento si completa con il Regolamento (UE) 2022/2481 – "Programma per il Decennio Digitale 2030", che individua gli obiettivi europei per la trasformazione digitale in ambito pubblico, privato, educativo e infrastrutturale, e con le Linee Guida AgID in tema di accessibilità (Legge 4/2004), sicurezza informatica, interoperabilità tecnica e semantica, dati pubblici e intelligenza artificiale (Decalogo AgID IA nella PA, giugno 2024).

Infine, sotto il profilo interno, il Piano si coordina con il Piano Strategico 2024–2026, il PIAO 2025–2027, i Regolamenti ICT di Ateneo, il Decreto Dirigenziale ARIE n. 04/2025 che definisce l'assetto della governance ICT e le competenze del Settore Sviluppo Digitale, nonché con le disposizioni interne sulla sicurezza informatica e sulla gestione documentale.

1.3 Metodologia e fonti adottate

La metodologia adottata per la redazione del Piano Triennale di Transizione Digitale si fonda su un principio di piena coerenza con il quadro normativo nazionale ed europeo e con la programmazione strategica dell'Ateneo, oltre che sul rigoroso allineamento ai modelli metodologici definiti dall'Agenzia per l'Italia Digitale.

Il processo di costruzione del documento è stato sviluppato secondo un approccio sistematico, basato sull'analisi delle evidenze disponibili, sulla ricognizione puntuale delle esigenze dell'Università e sulla valorizzazione delle migliori pratiche emerse nel sistema universitario nazionale, con particolare riferimento agli indirizzi metodologici elaborati dal Laboratorio GoodPractice del Politecnico di Torino.

In conformità alla "Guida alla compilazione del Piano Triennale per l'informatica nella PA" pubblicata da AgID nel giugno 2024, la struttura del Piano è organizzata secondo il modello duale che distingue le componenti strategiche da quelle tecnologiche. Le prime riguardano gli aspetti organizzativi, procedurali, di governance e di sviluppo delle competenze; le seconde si concentrano sulle infrastrutture, sulle piattaforme abilitanti, sull'interoperabilità, sulla sicurezza informatica, sui dati e sui servizi digitali.

Pur mantenendo questa distinzione strutturale, il Piano integra le due componenti in una visione unitaria, attraverso un insieme coerente di linee di azione che richiamano i codici e le misure del Piano Triennale AgID, permettendo di associare a ciascun intervento obiettivi operativi, responsabilità interne, indicatori di monitoraggio e cronoprogrammi triennali.

La definizione dei contenuti è stata guidata dall'analisi del Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024–2026 – Aggiornamento 2026, dalla ricognizione delle progettualità ICT già in essere presso l'Ateneo e dalle esigenze espresse dalle strutture amministrative, dirigenziali e accademiche. Sono stati inoltre esaminati gli atti regolamentari e organizzativi interni, tra cui il Decreto Dirigenziale ARIE n. 04/2025, che individua il Settore Sviluppo Digitale quale struttura competente per la governance ICT, unitamente ai regolamenti relativi alla sicurezza informatica, all'amministrazione digitale e alla gestione dei dati e non per ultimo al e-procurement.

Il Piano adotta una prospettiva dinamica e orientata al miglioramento continuo, trovando riferimento nel modello PDCA (Plan–Do–Check–Act), previsto dal sistema AVA3 per la programmazione e il controllo dei processi. Tale modello consente di articolare la pianificazione in una sequenza logica che comprende l'individuazione degli obiettivi, l'attuazione delle iniziative, la verifica dei risultati ottenuti e la successiva revisione della programmazione, assicurando una costante capacità di adattamento alle evoluzioni normative, tecnologiche e organizzative. Le prescrizioni AVA3 hanno guidato la definizione delle modalità con cui valutare l'adeguatezza delle tecnologie, la qualità dei dati, la gestione delle informazioni e i flussi di conoscenza interni.

Attraverso tale impianto metodologico, il Piano assicura che le azioni proposte siano realistiche, misurabili e coerenti con il contesto normativo e strategico dell'Università di Napoli L'Orientale. La metodologia garantisce inoltre l'integrazione del Piano con gli strumenti di programmazione, monitoraggio e controllo dell'Ateneo, permettendo un presidio stabile e strutturato del percorso di trasformazione digitale e assicurando un costante allineamento con gli obiettivi istituzionali e con le linee evolutive del quadro regolatorio nazionale ed europeo.

2. Missione e principi della trasformazione digitale dell'Ateneo

La missione digitale dell'Ateneo è orientata alla creazione di un ecosistema tecnologico evoluto, accessibile e sicuro, capace di sostenere la qualità della didattica, della ricerca, della terza missione e dei servizi amministrativi. La trasformazione digitale è interpretata come un fattore strategico per migliorare l'efficacia dei processi, ampliare la fruibilità dei servizi e valorizzare il patrimonio informativo dell'Ateneo, in coerenza con le priorità delineate nel Piano Strategico.

Le linee operative del triennio 2026–2028 si articolano attorno alla progressiva realizzazione di servizi digitali pienamente integrati e orientati all'utente, alla costruzione di un ambiente ICT resiliente e affidabile, e allo sviluppo di una governance del dato basata su criteri di qualità, trasparenza e interoperabilità.

In questa prospettiva, la digitalizzazione non è intesa come semplice adozione di tecnologie, ma come leva di cambiamento che coinvolge l'intera organizzazione, promuovendo nuovi modelli di gestione, collaborazione e accesso alle informazioni.

L'Ateneo mira a consolidare un'infrastruttura tecnologica moderna e sostenibile, capace di garantire continuità operativa, sicurezza e adattabilità, e di supportare l'evoluzione dei servizi pubblici digitali in conformità con gli standard nazionali ed europei. Parallelamente, attribuisce un ruolo centrale allo sviluppo delle competenze digitali della comunità universitaria, consapevole che la trasformazione tecnologica è indissolubilmente legata alla crescita culturale e professionale del personale docente e tecnico-amministrativo.

Nel suo insieme, missione e visione delineano un percorso che integra innovazione, sicurezza, qualità dei dati e valorizzazione delle competenze, orientando l'Ateneo verso un modello digitale maturo, efficiente e pienamente coerente con le politiche nazionali per la transizione digitale della Pubblica Amministrazione.

2.1 Principi ispiratori

La strategia di trasformazione digitale dell'Università, che si basa sul rigoroso quadro normativo è guidata da un insieme coeso di principi tecnico-operativi che ne orientano in modo unitario la progettazione e l'erogazione delle soluzioni ICT nel triennio 2026–2028. Tali principi non sono mere appendici, ma la traduzione esecutiva delle disposizioni nazionali in criteri obbligatori per l'organizzazione e la funzionalità dei sistemi.

In particolare, l'elemento cardine è rappresentato dalla progettazione digitale integrata, che vincola l'Ateneo a concepire i processi e i servizi in modalità nativamente digitale. Questo approccio sistemico è essenziale per garantire l'omogeneità del flusso informativo, la completa dematerializzazione documentale e l'azzeramento delle attività ridondanti. Ne consegue una semplificazione procedurale diretta che alimenta l'automazione, elevando al contempo la user experience per l'intera comunità universitaria.

A garanzia di uno scambio informativo fluido ed efficiente, si pone come criterio cardine l'interoperabilità tecnica e semantica. Questo impone l'adozione rigorosa di standard condivisi, protocolli aperti e interfacce (API) per un dialogo strutturale e affidabile con l'ecosistema pubblico e le sue piattaforme centrali (es. PDND). L'interoperabilità non è vista come un'opzione, ma come un requisito di coordinamento per l'efficacia e la continuità dei servizi.

La protezione del patrimonio istituzionale e la resilienza operativa sono affidate alla filosofia della sicurezza by design. Le misure di cybersecurity sono intrinsecamente integrate nella fase di ideazione, sviluppo e gestione delle soluzioni, rendendo la tutela delle informazioni un elemento costitutivo dell'architettura infrastrutturale e applicativa, in piena aderenza ai dettami della Direttiva NIS2 e dei framework di rischio. A ciò si affianca il principio della protezione dati per impostazione predefinita (privacy by default), che concretizza i requisiti del GDPR vincolando lo sviluppo di servizi alla minimizzazione del trattamento, alla limitazione delle finalità e all'assoluta accountability in ogni fase del ciclo di vita del dato.

Per assicurare la longevità e l'efficacia degli investimenti, la strategia si basa sulla standardizzazione architetturale e sul riuso. L'Ateneo persegue l'uniformità dei modelli documentati e riutilizzabili, riducendo la frammentazione tecnologica, aumentando la resilienza complessiva dei sistemi e favorendo la scalabilità delle infrastrutture verso il paradigma cloud. Questo garantisce la piena sostenibilità economica e operativa.

La risorsa più strategica è il dato stesso, che necessita di essere governato secondo il principio della valorizzazione del patrimonio informativo. Ciò richiede l'istituzione di un rigoroso modello di data governance, definito per assicurare qualità, integrità e accessibilità. L'obiettivo è promuovere un uso informato e tracciabile delle informazioni, indispensabile per il supporto scientifico ai processi decisionali degli organi di governo e per l'adempimento degli obblighi di trasparenza.

Infine, la sostenibilità del Piano nel tempo è garantita dallo sviluppo continuo delle competenze digitali. Questo principio è cruciale affinché la trasformazione tecnologica si traduca effettivamente in un cambiamento organizzativo. La diffusione

di abilità adeguate permette al personale di utilizzare, governare e manutenere in sicurezza le nuove tecnologie, assicurando una gestione consapevole e lungimirante dell'innovazione introdotta.

Questi principi, operando sinergicamente, definiscono la matrice esecutiva che assicura la qualità progettuale, la coerenza metodologica e l'allineamento progressivo agli standard più elevati della pubblica amministrazione.

2.2 Coerenza con gli obiettivi del Piano Strategico 2024–2026

La strategia digitale delineata nel presente Piano (PTTD) si integra in modo organico e indissolubile con gli indirizzi definiti dal Piano Strategico 2024–2026 dell'Università di Napoli L'Orientale. La transizione digitale, lungi dall'essere considerata un ambito separato, costituisce la leva abilitante e trasversale che supporta e catalizza l'attuazione delle politiche strategiche, garantendo coerenza, sostenibilità operativa e continuità tra le diverse aree d'intervento dell'Ateneo.

In relazione all'obiettivo A – Innovare e valorizzare la ricerca, il Piano garantisce la disponibilità di infrastrutture digitali idonee a sostenere le attività scientifiche moderne, sempre più dipendenti da una gestione strutturata dei dati, dall'interoperabilità e dalla collaborazione in rete. La valorizzazione del patrimonio informativo della ricerca (data management) e l'adozione di piattaforme sicure e scalabili contribuiscono a potenziarne l'efficacia e a consolidarne la visibilità nel contesto scientifico internazionale.

Parallelamente, con riferimento all'obiettivo B – Innovare e valorizzare la didattica, la strategia digitale promuove servizi integrati e strumenti tecnologici avanzati che rafforzano la qualità dell'offerta formativa e ne amplificano le possibilità di fruizione. La progettazione di ambienti digitali accessibili e orientati all'utente sostiene il rinnovamento delle metodologie didattiche, favorisce l'inclusione e migliora in modo tangibile l'esperienza formativa complessiva degli studenti.

L'obiettivo C – Riqualificare e funzionalizzare gli spazi trova concreta applicazione nelle iniziative volte a dotare l'Ateneo di un'infrastruttura tecnologica moderna, sicura e sostenibile. L'adozione di architetture cloud, l'ottimizzazione delle reti e l'armonizzazione dei sistemi concorrono all'integrazione fluida tra spazi fisici e ambienti digitali, creando un ecosistema coerente con i principi dell'edilizia innovativa e degli ambienti di apprendimento evoluti.

Il Piano sostiene attivamente anche l'obiettivo E – Mettere la persona al centro, attraverso l'implementazione di un modello di servizi digitali che privilegia semplicità, usabilità e trasparenza. La crescita delle competenze digitali del personale, la promozione di ambienti di lavoro sicuri e la diffusione di strumenti che facilitano la gestione integrata delle attività amministrative contribuiscono direttamente a migliorare il benessere organizzativo e la qualità del lavoro della comunità accademica.

In relazione all'obiettivo D – Condividere la conoscenza e rafforzare il legame con la comunità, il Piano promuove la diffusione della cultura digitale e l'accesso ai servizi in modalità trasparente e inclusiva. La digitalizzazione dei processi, la valorizzazione dei dati e il potenziamento della comunicazione multicanale accrescono la qualità dei servizi agli stakeholder e consolidano il ruolo dell'Ateneo quale polo di produzione e disseminazione della conoscenza. In questa prospettiva, la comunicazione digitale istituzionale è considerata un asset strategico per assicurare chiarezza, accessibilità e coerenza informativa, valorizzando le attività scientifiche e culturali rivolte alla società.

Infine, l'obiettivo F – Senza frontiere: consolidare la dimensione internazionale trova applicazione diretta nella promozione di soluzioni digitali che facilitano la mobilità, lo scambio di informazioni, la partecipazione a reti collaborative e l'adozione

di standard conformi alle migliori pratiche europee. L'interoperabilità sistemica, la digitalizzazione dei servizi e la gestione strutturata dei dati supportano la proiezione internazionale dell'Ateneo e ne rafforzano la competitività globale.

Nel complesso, la strategia digitale proposta garantisce la piena convergenza con le priorità del Piano Strategico 2024–2026, realizzando gli obiettivi istituzionali attraverso interventi che integrano in modo sinergico tecnologia, organizzazione e governance per la trasformazione unitaria dell'Università di Napoli L'Orientale.

2.3 Contributo agli obiettivi dell'Agenda ONU 2030

La strategia digitale delineata nel presente Piano si inserisce nel più ampio quadro delle politiche globali per lo sviluppo sostenibile definite dall'Agenda ONU 2030, rispetto alla quale l'Università di Napoli L'Orientale ha già manifestato un esplicito impegno attraverso il proprio Piano Strategico 2024–2026.

La trasformazione digitale dell'Ateneo rappresenta infatti uno strumento concreto per contribuire al raggiungimento di diversi Obiettivi di Sviluppo Sostenibile (Sustainable Development Goals – SDGs), con particolare riferimento a quelli maggiormente connessi all'innovazione, alla qualità dei servizi pubblici e alla valorizzazione della conoscenza.

In primo luogo, il Piano sostiene l'SDG 4, dedicato all'istruzione di qualità, attraverso la promozione di servizi digitali accessibili, inclusivi e orientati al miglioramento dell'esperienza formativa. La progressiva integrazione tra ambienti fisici e digitali, la valorizzazione dei dati a supporto della didattica e l'innovazione dei processi amministrativi contribuiscono a rendere l'offerta formativa più moderna, flessibile e rispondente alle esigenze della comunità studentesca.

Un secondo asse di coerenza riguarda l'SDG 9, che valorizza infrastrutture resilienti, innovazione e capacità tecnologica. L'adozione di architetture cloud sicure e scalabili, il rafforzamento della continuità operativa, la standardizzazione dei sistemi e lo sviluppo di un ambiente ICT sostenibile rispondono direttamente a tale obiettivo, favorendo un impiego efficiente delle risorse tecnologiche e promuovendo modelli di innovazione responsabile.

Il Piano contribuisce inoltre all'SDG 16, relativo allo sviluppo di istituzioni trasparenti, efficaci e responsabili. La digitalizzazione dei processi, la tracciabilità delle informazioni, l'interoperabilità dei sistemi e la promozione di servizi accessibili e orientati all'utente rafforzano la capacità amministrativa dell'Ateneo, ne migliorano la trasparenza e favoriscono l'inclusione digitale della comunità accademica e degli stakeholder.

Infine, il Piano sostiene l'SDG 17, dedicato alle partnership e alla cooperazione. L'interoperabilità con le piattaforme nazionali, la valorizzazione dei dati condivisi, la capacità dell'Ateneo di integrarsi nei sistemi digitali del settore pubblico e la partecipazione a reti e progetti internazionali evidenziano un orientamento istituzionale aperto, collaborativo e in linea con le più avanzate pratiche europee.

Nel loro complesso, le azioni previste dal Piano Triennale di Transizione Digitale contribuiscono in modo significativo agli indirizzi dell'Agenda ONU 2030, rafforzando il ruolo dell'Università di Napoli L'Orientale quale istituzione impegnata nello sviluppo sostenibile, nell'innovazione responsabile e nella promozione di una società digitale più equa, inclusiva e consapevole.

3. Governance della transizione digitale

Il regime di gestione dell'innovazione tecnologica all'Università di Napoli L'Orientale si fonda su un modello organizzativo unitario che armonizza responsabilità di alta direzione, competenze specialistiche e mandati operativi. Tale struttura è stata delineata in coerenza con il Codice dell'Amministrazione Digitale (CAD) e con gli indirizzi programmatici del Piano Triennale per l'Informatica.

L'assetto, evoluto a seguito della riorganizzazione amministrativa e formalizzato con Decreto Dirigenziale ARIE n. 04/2025, stabilisce un presidio coeso sui processi di trasformazione, assicurando chiarezza nelle accountability e sostenendo la continuità e la coerenza nell'esecuzione delle politiche di sviluppo.

La trasformazione è direzionata dal Responsabile per la Transizione Digitale (RTD), figura istituita dall'art. 17 del CAD e ricoperta dal Direttore Generale (deliberazione del Consiglio di Amministrazione del 28 giugno 2022). Al RTD è conferito un mandato di alta direzione e vigilanza sulle strategie informatiche, pur tuttavia, garantendo l'allineamento imprescindibile delle iniziative ICT con gli obiettivi istituzionali, il Piano Strategico e la programmazione triennale. In particolare gli è affidato il coordinamento strategico dell'amministrazione digitale, la sicurezza cibernetica e la riprogettazione dei workflow.

L'attuazione operativa delle strategie è in capo all'Area Infrastrutture Edilizie e Digitali (ARIE). Quest'ultima, attraverso il Settore Sviluppo Digitale, coordina e gestisce le piattaforme applicative, le infrastrutture di rete e l'intero apparato informatico dell'Ateneo. Il Settore, con la sua articolazione in Uffici e Funzioni dedicate, assicura un modello integrato che consente all'istituzione di gestire la complessità tecnologica, mantenendo una vigilanza costante sull'interoperabilità, la qualità dei servizi erogati e l'integrità sistemica.

L'architettura direzionale si basa su una metodologia di lavoro sinergica e intersettoriale, che coinvolge attivamente i vertici dirigenziali, gli uffici amministrativi, gli organismi accademici e i referenti dipartimentali. Questa impostazione favorisce la circolazione delle conoscenze e l'allineamento delle decisioni, contribuendo a una visione omogenea sulle necessità di innovazione. La cooperazione tra settori garantisce, inoltre, la piena fusione tra lo sviluppo dei processi digitali, la pianificazione strategica e la gestione ottimizzata delle risorse finanziarie.

Il modello implementato valorizza, infine, i meccanismi di verifica e valutazione previsti dal Piano Integrato di Attività e Organizzazione (PIAO), dal sistema di Assicurazione della Qualità (AVA3) e dagli standard metodologici AgID. L'Università applica criteri di tracciabilità, misurabilità e miglioramento continuo, presidiando che l'efficacia, l'efficienza e l'impatto sul valore pubblico delle attività di trasformazione siano sistematicamente valutati in coerenza con gli orientamenti di programmazione nazionale ed europea.

Nel suo insieme, l'assetto di gestione garantisce una direzione integrata e responsabile sui processi informatici, promuovendo una solida sinergia tra funzioni direzionali, organizzative e tecniche. Questo assicura che l'evoluzione dell'Università di Napoli L'Orientale si sviluppi in un contesto strutturato, trasparente e pienamente orientato al conseguimento degli obiettivi istituzionali.

I compiti e le responsabilità della Governance Digitale dell'Ateneo sono descritti sinteticamente nella seguente tabella RACI:

Processo Strategico / Attività Chiave	RTD / Direttore Generale	Settore Sviluppo Digitale	Organi di Governo	Nucleo di Valutazione / PdQ	Uffici Amministrativi / Dirigenziali
1. Elaborazione e Proposta del PTTD	A	R	C	C	I
2. Approvazione Finale del PTTD e Budget	C	I	A	C	I
3. Definizione Architettura, Cloud Strategy e DR/BC	A	R	I	C	C
4. Implementazione Sicurezza Cibernetica (NIS2)	A	R	I	C	C
5. Sviluppo, Gestione Tecnica e Manutenzione Piattaforme ICT	C	A	I	I	R
6. Ridisegno dei Processi e Adozione dei Servizi Digitali	A	R	I	I	R
7. Valutazione dell'Efficacia e Monitoraggio KPI (AVA3/PIAO)	C	R	I	A	R
8. Strategia e Piano di Sviluppo Competenze Digitali	A	C	I	C	R

La cui legenda è indicata nella seguente tabella:

SIGLA	RUOLO	DESCRIZIONE
R	Responsible	Chi svolge materialmente il compito. Può essercene più di uno.
A	Accountable	Chi è il proprietario del risultato finale e approva il lavoro. Ne esiste uno e uno solo per attività.
C	Consulted	Chi deve essere interpellato e fornisce un contributo consultivo bidirezionale.
I	Informed	Chi deve essere tenuto aggiornato, tipicamente in forma unidirezionale.

3.1 Ruolo e funzioni del Responsabile per la Transizione Digitale (RTD)

Il Responsabile per la Transizione Digitale (RTD) rappresenta la figura centrale del modello di governance digitale dell'Università di Napoli L'Orientale. La sua funzione, prevista dall'art. 17 del Codice dell'Amministrazione Digitale, è volta a garantire la coerenza, l'unitarietà e la continuità dell'azione dell'Ateneo in materia di innovazione tecnologica, trasformazione dei processi e sviluppo dei servizi digitali.

L'Ateneo ha individuato tale funzione nella persona del Direttore Generale, nominato con Delibera del Consiglio di Amministrazione del 28 giugno 2022, assicurando un presidio strategico di livello apicale e una diretta integrazione della transizione digitale nelle attività di governo dell'istituzione.

Il RTD svolge un ruolo di indirizzo e coordinamento complessivo delle politiche digitali, assicurando che le iniziative ICT siano pienamente allineate agli obiettivi del Piano Strategico, ai programmi triennali di Ateneo e agli indirizzi nazionali definiti da AgID. La sua azione riguarda non solo la supervisione tecnica delle piattaforme e dei sistemi informativi, ma anche la promozione della trasformazione dei processi amministrativi, la definizione degli standard organizzativi e la garanzia della conformità alle normative in materia di amministrazione digitale, interoperabilità, sicurezza informatica e protezione dei dati personali.

Nell'esercizio delle sue funzioni, il RTD assicura l'integrazione tra innovazione tecnologica e riorganizzazione dei processi, promuovendo un uso efficace delle tecnologie digitali per migliorare la qualità dei servizi, semplificare i procedimenti interni e rafforzare la trasparenza nei confronti dell'utenza. La sua attività è varia svariando dalla valorizzazione del patrimonio informativo, all'adozione di modelli di interoperabilità fino alla definizione di un quadro di riferimento unitario per la gestione dei dati, in modo da assicurare un approccio sistemico e coerente alla digitalizzazione dell'Ateneo.

Un aspetto essenziale del ruolo del RTD riguarda il presidio della sicurezza informatica, attraverso la definizione delle linee di indirizzo per la gestione del rischio, il coordinamento delle misure di protezione dei sistemi e l'adozione dei paradigmi di sicurezza e privacy "by design" e "by default". Tale responsabilità include il raccordo tra gli aspetti tecnologici e quelli organizzativi della sicurezza, garantendo il rispetto della normativa vigente e la continuità dei servizi.

Il RTD opera, inoltre, come soggetto di raccordo tra le diverse articolazioni dell'Ateneo, assicurando un dialogo costante con i Dirigenti, i Responsabili delle strutture, i presìdi di qualità e gli organismi di governo. Tale funzione di coordinamento favorisce una visione integrata dei fabbisogni, delle priorità e delle progettualità digitali, consentendo di armonizzare le diverse iniziative e di adottare un approccio unitario alla trasformazione digitale.

Infine, il RTD svolge un ruolo essenziale nei processi di monitoraggio e di rendicontazione delle attività digitali, assicurando la coerenza del Piano Triennale di Transizione Digitale con il ciclo della performance, con il PIAO e con i sistemi di valutazione interni ed esterni. La sua funzione garantisce che l'azione dell'Ateneo in materia di digitalizzazione sia misurabile, trasparente e orientata alla creazione di valore pubblico.

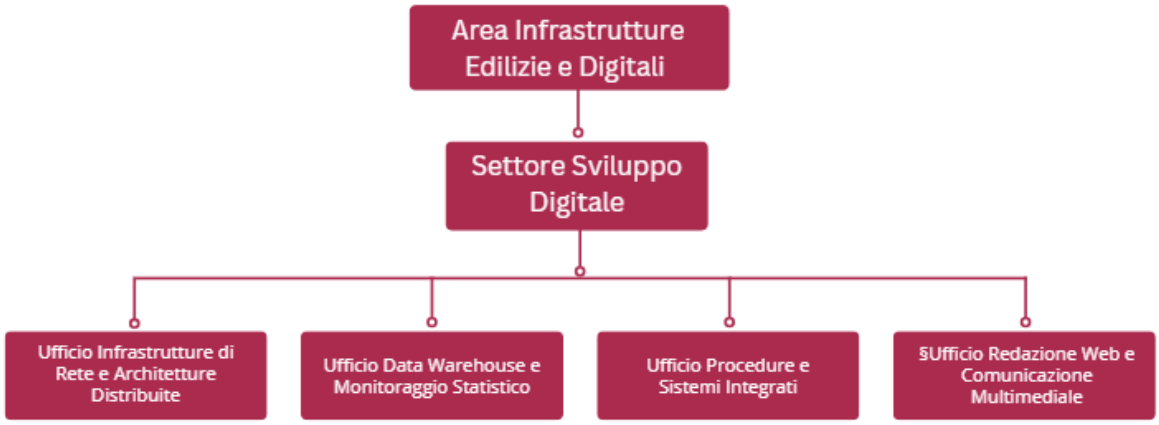
Nel complesso, il RTD rappresenta la guida strategica della trasformazione digitale dell'Università di Napoli L'Orientale, assicurando che l'innovazione tecnologica si sviluppi in modo responsabile, sicuro e coerente con la missione istituzionale e con gli indirizzi nazionali della Pubblica Amministrazione digitale.

3.2 Struttura organizzativa ICT

La governance della transizione digitale dell'Università di Napoli L'Orientale si realizza attraverso un'articolazione organizzativa definita dal Decreto Dirigenziale ARIE n. 04/2025, che identifica nell'Area Infrastrutture Edilizie e Digitali (ARIE) il presidio unico delle funzioni ICT e infrastrutturali dell'Ateneo.

La struttura ICT dell'Ateneo è caratterizzata, infatti, da un modello integrato che riunisce competenze tecniche, amministrative e specialistiche, permettendo un presidio completo delle diverse dimensioni della transizione digitale. Tale modello si articola in Uffici e Funzioni differenziate, ognuna con un ruolo specifico nel garantire sicurezza, continuità operativa, interoperabilità, gestione dei dati, sviluppo delle piattaforme e comunicazione digitale istituzionale.

All'interno dell'Area, il Settore Sviluppo Digitale costituisce la struttura centrale per la pianificazione, l'integrazione e la gestione dei servizi digitali, supportata da quattro Uffici a competenza tecnico-specialistica, che assicurano un presidio completo delle diverse dimensioni dell'ecosistema ICT.



- Il Settore Sviluppo Digitale

Il Settore Sviluppo Digitale coordina la transizione digitale dell'Ateneo e garantisce l'integrazione tra strategie tecnologiche, riorganizzazione dei processi e valorizzazione del patrimonio informativo. Svolge funzioni trasversali di governance, pianificazione, supporto al Responsabile per la Transizione Digitale (RTD), monitoraggio delle iniziative ICT, attuazione delle linee guida AgID, presidio dell'interoperabilità, dematerializzazione dei procedimenti, sicurezza applicativa, definizione degli standard digitali e supporto ai processi di garantire la conformità alle normative e alle politiche nazionali.

Il Settore coordina le attività dei quattro Uffici ICT, garantendo un'azione coerente, integrata e orientata alla qualità dei servizi digitali erogati all'intera comunità accademica:

- Ufficio Infrastrutture di Rete e Architetture Distribuite

Garantisce la progettazione, gestione e manutenzione dell'infrastruttura di rete dell'Ateneo, la sicurezza perimetrale e la continuità operativa dei sistemi. Presidia le reti cablate e wireless, le architetture server, i sistemi di virtualizzazione, i servizi di autenticazione e gli apparati di sicurezza informatica. Gestisce le politiche di disaster recovery business continuity, assicurando stabilità, resilienza e scalabilità delle infrastrutture, in conformità agli standard di sicurezza e alle prescrizioni nazionali in materia di protezione delle reti e sistemi.

- Ufficio Data Warehouse e Monitoraggio Statistico

L'Ufficio presidia la governance dei dati, il data warehouse di Ateneo, la produzione dei cruscotti informativi e il monitoraggio degli indicatori istituzionali (ANS, FFO, PNRR, AVA3). Sviluppa modelli di integrazione dei dati, garantisce qualità, coerenza e affidabilità delle informazioni, supporta NdV, PQA e gli Organi nelle attività di analisi e rendicontazione. In stretta sinergia con la **Funzione Specialistica – Referente Statistico** assicura la conformità agli standard SISTAN e alle normative sulla gestione del patrimonio informativo pubblico. Questa Funzione specialistica garantisce la validazione dei dati statistici, la conformità agli standard SISTAN e il rispetto dei criteri di qualità richiesti dai flussi informativi nazionali (MUR, ISTAT, ANVUR). Svolge un ruolo di presidio sulla correttezza e tempestività dei dati trasmessi e collabora con l'Ufficio Data Warehouse per assicurare un sistema informativo coerente, integrato e pienamente tracciabile.

- Ufficio Procedure e Sistemi Integrati

L'Ufficio governa i sistemi informativi d'Ateneo (UGOV, ESSE3, piattaforme gestionali), le identità digitali, la PEC e i servizi Microsoft 365, le piattaforme web applicative e il sistema di autenticazione. Coordina i processi di dematerializzazione, la gestione documentale, i percorsi di interoperabilità applicativa, l'integrazione delle basi dati e la sicurezza applicativa. Assicura inoltre il presidio delle piattaforme istituzionali, dei servizi online rivolti a studenti e personale, e dei sistemi di ticketing e di supporto ICT.

- Ufficio Redazione Web e Comunicazione Multimediale

Presidia il portale istituzionale, la comunicazione digitale, i social media, i contenuti multimediali e il rispetto delle Linee Guida AgID in materia di accessibilità (WCAG). Garantisce coerenza comunicativa, uniformità editoriale e qualità dei contenuti attraverso tutti i canali digitali dell'Ateneo. Supporta le strutture accademiche e amministrative nella produzione di contenuti e nel miglioramento dell'identità visiva digitale istituzionale.

ANNO	Totale Personale TAB	Personale ambito ICT	%
2022	185	7	3,8
2025	227	15	6,6

L'Ateneo ha avviato un robusto percorso di rafforzamento della propria capacità organizzativa complessiva, come testimoniato dal notevole incremento del personale Tecnico-Amministrativo (TAB) tra il 2022 e il 2025. Questo potenziamento generale ha consentito un proporzionale e mirato accrescimento delle unità operative dedicate all'ambito ICT.

Il dato evidenzia un raddoppio delle risorse in carico al Settore Sviluppo Digitale, che ha raggiunto il 6,6% del totale TAB. Il PTTD poggia la sua attuazione su questa capacità organizzativa in constante consolidamento. La maggiore dotazione di figure specialistiche, risultato del processo, costituisce la base operativa solida e necessaria per l'implementazione delle linee strategiche e per garantire la sostenibilità dei servizi digitali nel lungo periodo. Il PTTD, pertanto, è tarato per sfruttare al meglio l'infrastruttura umana attualmente disponibile per raggiungere gli obiettivi di trasformazione.

La struttura ICT intrattiene un rapporto costante e sistemico con tutte le componenti istituzionali dell'Università:

- Con le **strutture accademiche** (Dipartimenti, CdS, Ricerca, Dottorati) interagisce per garantire servizi digitali adeguati, interoperabilità delle piattaforme, supporto all'uso dei dati e sviluppo di soluzioni a supporto della didattica e della ricerca.
- Con le **unità amministrative** collabora nella digitalizzazione dei processi, nell'implementazione delle piattaforme applicative, nella dematerializzazione dei procedimenti e nel miglioramento dell'efficienza organizzativa.
- Con gli **Organi di governo**, supporta la pianificazione strategica, la rendicontazione digitale e la valutazione delle performance, in coerenza con PIAO, AVA3 e Piano Strategico.

- Con gli **uffici tecnici e logistici**, coordina l'implementazione delle infrastrutture tecnologiche negli edifici e negli spazi didattici, garantendo compatibilità impiantistica, sicurezza e standard tecnologici coerenti con le politiche di Ateneo.
- Con i presidi istituzionali di qualità (NdV, PQA) assicura la disponibilità di dati affidabili, tracciabili e coerenti con i modelli nazionali di valutazione.

Il modello collaborativo, integrato e trasversale assicura la coerenza del sistema ICT con le esigenze di tutte le funzioni istituzionali e rafforza la capacità dell'Ateneo di attuare una trasformazione digitale sostenibile, sicura e orientata al valore pubblico.

3.3 Coordinamento con PIAO, qualità e pianificazione strategica

La governance della transizione digitale dell'Università di Napoli L'Orientale è strettamente integrata con i sistemi di pianificazione, monitoraggio e valutazione dell'Ateneo, in coerenza con il quadro normativo nazionale e con gli strumenti di programmazione strategica vigenti.

L'allineamento tra il presente Piano, il Piano Strategico 2024–2026, il Piano Integrato di Attività e Organizzazione (PIAO) 2025–2027 e il sistema di Assicurazione della Qualità AVA3 rappresenta un elemento essenziale per garantire una trasformazione digitale stabile, sostenibile e orientata alla creazione di valore pubblico.

Il coordinamento con il PIAO consente di integrare gli obiettivi digitali nel ciclo della performance, assicurando che le iniziative ICT siano pianificate, monitorate e valutate secondo criteri di efficacia, efficienza e impatto. La digitalizzazione dei processi amministrativi, la semplificazione delle procedure, la valorizzazione dei dati e il miglioramento dei servizi online costituiscono componenti strutturali per la realizzazione delle finalità del PIAO, che mira a rafforzare la capacità amministrativa dell'Ateneo, a migliorare l'organizzazione del lavoro e a promuovere un utilizzo consapevole e responsabile delle tecnologie.

Sul versante della qualità, il Piano si integra con il sistema AVA3 attraverso un contributo diretto agli ambiti B.4 e B.5.

L'ambito B.4 – Attrezzature e tecnologie richiede un presidio continuo della disponibilità, adeguatezza e sicurezza delle tecnologie a supporto della didattica e della ricerca. Le iniziative ICT del presente Piano, orientate alla modernizzazione delle infrastrutture, all'adozione di architetture cloud ibride e al rafforzamento della sicurezza dei sistemi, contribuiscono al soddisfacimento dei requisiti di qualità definiti dall'ANVUR.

L'ambito B.5 – Gestione delle informazioni e della conoscenza trova riscontro nelle attività di governance dei dati, nella definizione dei criteri di qualità informativa, nell'interoperabilità dei sistemi e nella diffusione di strumenti che favoriscono la trasparenza, la tracciabilità e la corretta circolazione delle informazioni, elementi centrali nella valutazione dei flussi informativi istituzionali.

Il coordinamento con il Piano Strategico 2024–2026 garantisce una coerenza di lungo periodo tra gli obiettivi della transizione digitale e le ambizioni complessive dell'Ateneo. La digitalizzazione rappresenta, infatti, una dimensione trasversale a tutti gli obiettivi strategici, contribuendo alla valorizzazione della ricerca, all'innovazione della didattica, alla riqualificazione degli spazi, al rafforzamento della comunicazione istituzionale e alla proiezione internazionale dell'Università.

L'integrazione tra visione digitale e strategia istituzionale consente di assicurare che le scelte tecnologiche non siano orientate esclusivamente dall'esigenza di adottare nuove soluzioni, ma rispondano in modo diretto alle priorità accademiche e amministrative dell'Ateneo.

Il modello di governance adottato prevede un ciclo continuo di pianificazione, monitoraggio e valutazione, secondo la logica del miglioramento continuo e in coerenza con le metodologie AgID e AVA3. Le strutture ICT collaborano stabilmente con gli organi di governo, con le unità amministrative e con i presìdi di qualità, garantendo coerenza tra le iniziative digitali e gli strumenti istituzionali di programmazione e assicurando un presidio costante sulla qualità, sulla sicurezza e sull'interoperabilità dei sistemi informativi.

Nel suo complesso, il coordinamento tra Piano Triennale Digitale, PIAO, qualità AVA3 e programmazione strategica consente all'Ateneo di sviluppare un ecosistema digitale solido, misurabile e orientato al valore pubblico, assicurando che la transizione digitale si realizzi in modo strutturato e pienamente integrato nei processi istituzionali dell'Università di Napoli L'Orientale.

3.4 Modello di governance e cooperazione interna

La realizzazione della transizione digitale dell'Università di Napoli L'Orientale richiede un modello di cooperazione stabile, strutturato e trasversale, capace di coinvolgere in modo integrato le diverse componenti dell'Ateneo. Tale modello si sviluppa nel quadro di indirizzo strategico definito dal Responsabile per la Transizione Digitale (RTD), garante della coerenza delle politiche digitali e dell'allineamento dell'azione ICT con gli obiettivi istituzionali e con le linee guida nazionali.

La multidimensionalità dei processi digitali impone un'interazione continua tra l'Area Infrastrutture Edilizie e Digitali (ARIE), le strutture accademiche, le unità amministrative, i presìdi di qualità e gli organi di governo, al fine di assicurare efficacia, integrazione e coerenza delle strategie adottate.

In questo quadro, un ruolo specifico è svolto dal Responsabile della Protezione dei Dati (RPD), che, in piena autonomia e indipendenza, assicura il rispetto della normativa in materia di protezione dei dati personali e coopera, quando necessario, con le strutture ICT per gli aspetti inerenti alla sicurezza, alla valutazione dei rischi e all'applicazione dei principi di privacy-by-design e di privacy-by-default.

La cooperazione intersettoriale si fonda su un principio di corresponsabilità, in virtù del quale ciascuna struttura contribuisce, secondo le proprie competenze, alla pianificazione e all'attuazione delle iniziative digitali. L'ARIE, attraverso il Settore Sviluppo Digitale e i suoi Uffici, opera come nodo di coordinamento tecnico in raccordo con il RTD e nel rispetto dei vincoli imposti dalla normativa sulla protezione dei dati personali, assicurando un presidio unitario delle tecnologie, dei sistemi informativi e delle infrastrutture digitali.

Il rapporto con le strutture accademiche costituisce un elemento essenziale della governance digitale. Dipartimenti, Corsi di Studio e strutture di ricerca interagiscono regolarmente con il sistema ICT per garantire la continuità dei servizi didattici e scientifici, la gestione dei flussi informativi relativi agli studenti, la programmazione delle attività formative, la rendicontazione dei progetti, la gestione dei dati della ricerca e la fruizione dei servizi digitali trasversali. Tale interazione si traduce in un flusso costante di esigenze che orientano la pianificazione delle soluzioni tecnologiche, favorendo l'adozione di strumenti in grado di rispondere in modo efficace alla missione istituzionale dell'Ateneo.

Analogamente, la cooperazione con le unità amministrative consente di integrare la digitalizzazione nei processi gestionali e organizzativi. La dematerializzazione dei procedimenti, l'automazione dei flussi, l'integrazione tra piattaforme, la gestione documentale, l'identità digitale, la sicurezza informatica e l'interoperabilità dei sistemi richiedono un'interazione continua tra gli uffici ICT e le strutture responsabili dei processi amministrativi.

In particolare, le attività ICT supportano la programmazione economico-finanziaria, la gestione del personale, i servizi agli studenti, gli aspetti contabili e patrimoniali, la comunicazione istituzionale e tutte le funzioni che incidono sulla qualità dell'azione amministrativa.

Un ruolo fondamentale è svolto dai presìdi di qualità e dagli organismi istituzionali di monitoraggio. Il Nucleo di Valutazione, il Presidio della Qualità e le commissioni di Ateneo interagiscono con i sistemi digitali per garantire la disponibilità di dati affidabili, tempestivi e coerenti, indispensabili per la rendicontazione, per la programmazione accademica e per la valutazione delle performance. La cooperazione tra ICT e presìdi di qualità contribuisce in modo decisivo all'attuazione degli standard AVA3, soprattutto in relazione agli indicatori B.4 e B.5.

La collaborazione si estende anche all'Area Tecnica e alle strutture responsabili degli spazi universitari, in quanto la progettazione degli ambienti didattici, la realizzazione di laboratori, la predisposizione di reti, cablaggi e dotazioni multimediali presuppongono un coordinamento costante tra componenti digitali, logistiche e impiantistiche.

Infine, l'interazione con gli organi di governo dell'Ateneo assicura che le scelte tecnologiche siano pienamente allineate agli indirizzi istituzionali e ai processi decisionali. Il flusso strutturato di informazioni e analisi consente ai vertici dell'Università di monitorare l'avanzamento delle iniziative ICT, valutare l'impatto delle azioni intraprese e orientare le priorità nella pianificazione strategica e nella programmazione delle risorse.

Nel complesso, il modello di coordinamento istituzionale adottato dall'Università di Napoli L'Orientale garantisce un presidio integrato della trasformazione digitale, fondato sul raccordo con il RTD e sulla collaborazione tra funzioni tecniche, strutture accademiche e unità amministrative, e consente all'Ateneo di sviluppare soluzioni sostenibili, interoperabili e coerenti con il quadro strategico e normativo di riferimento.

3.5 Centrale di Committenza ICT

La Centrale di Committenza ICT costituisce un presidio strategico della governance digitale e assicura la coerenza, la trasparenza e l'unitarietà dei processi di acquisizione di beni e servizi informatici. Essa opera in attuazione del Regolamento di Ateneo per la programmazione e l'approvvigionamento dei beni e servizi ICT e dell'Allegato CPV, che definisce in modo puntuale le categorie merceologiche ICT, le responsabilità degli attori istituzionali e le modalità di classificazione tecnica delle forniture.

La funzione svolta dalla Centrale di Committenza ICT assume particolare rilevanza nel quadro della trasformazione digitale, poiché garantisce che tutte le iniziative di acquisizione siano allineate agli standard nazionali e istituzionali in materia di interoperabilità, sicurezza, continuità operativa, protezione dei dati personali, accessibilità digitale e qualità dei servizi. Il modello adottato consente di prevenire la frammentazione tecnologica, la proliferazione di soluzioni non integrate, l'insorgere di fenomeni di "shadow IT" e il rischio di incompatibilità architetturali, assicurando l'adozione di soluzioni coerenti con il disegno complessivo del sistema informativo di Ateneo.

In questo assetto, la Centrale di Committenza ICT svolge un ruolo di raccordo tra la programmazione strategica e l'attività amministrativa, assicurando che ogni procedura di approvvigionamento sia preceduta dalla valutazione tecnica del Settore Sviluppo Digitale e dal parere di conformità del Responsabile per la Transizione Digitale, previsti dall'art. 17 del Codice dell'Amministrazione Digitale e dal Regolamento ICT di Ateneo. Tale integrazione tra competenze tecniche e amministrative garantisce un processo decisionale unitario, fondato su criteri di efficacia, sostenibilità, sicurezza e piena conformità normativa.

La Centrale di Committenza ICT presidia inoltre la qualità dei capitolati tecnici, l'allineamento agli standard evolutivi delle piattaforme d'Ateneo, il monitoraggio delle scadenze contrattuali e la gestione dei rinnovi, assicurando continuità nei servizi critici e una visione integrata dell'intero ciclo di vita dei beni e degli applicativi acquisiti. La collaborazione strutturata con il Provveditorato, con gli uffici di gara e con la Direzione Generale consente di armonizzare le esigenze delle strutture richiedenti con gli obiettivi strategici del Piano ICT, promuovendo un utilizzo efficiente delle risorse e una razionalizzazione degli investimenti.

La presenza della Centrale di Committenza ICT rappresenta dunque una garanzia di presidio sistemico del dominio ICT, assicurando che ogni acquisizione concorra alla costruzione di un ecosistema digitale organico, interoperabile e sostenibile. Essa costituisce uno dei pilastri della governance dell'innovazione tecnologica dell'Ateneo, favorendo un modello di gestione orientato alla qualità, alla trasparenza, alla riduzione dei rischi operativi e all'armonizzazione delle scelte tecnologiche, nel pieno rispetto del quadro normativo vigente.

3.6 Ruolo e funzioni del Responsabile della Protezione dei Dati (RPD)

Il Responsabile della Protezione dei Dati (RPD) svolge una funzione di garanzia fondamentale nel modello di governance dell'Università di Napoli L'Orientale, assicurando che il trattamento dei dati personali avvenga in conformità al Regolamento (UE) 2016/679, al D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018, e alle Linee Guida del Comitato Europeo per la Protezione dei Dati (EDPB).

L'Ateneo ha provveduto alla sua nomina con atto formale degli Organi di governo, individuando tale figura come presidio indipendente a tutela dei diritti e delle libertà fondamentali delle persone fisiche nei trattamenti effettuati dall'istituzione universitaria.

Il RPD opera in condizioni di autonomia e indipendenza, come previsto dall'art. 38 del Regolamento, riferendo direttamente al vertice istituzionale e mantenendo un rapporto costante con i Dirigenti, i referenti delle strutture e con tutte le unità organizzative che effettuano trattamenti di dati personali. Il suo ruolo non comporta attività operative né poteri decisionali sui trattamenti, ma si configura come funzione di controllo, consulenza, vigilanza e supporto metodologico finalizzata a promuovere un trattamento conforme, trasparente e proporzionato dei dati.

Tra le sue attività rientrano il monitoraggio del rispetto della normativa e delle politiche interne in materia di protezione dei dati, l'analisi dei trattamenti esistenti e la verifica della loro conformità, la promozione di iniziative di sensibilizzazione e formazione del personale, nonché il supporto nella predisposizione e valutazione delle Data Protection Impact Assessment (DPIA) e delle misure di mitigazione del rischio.

Il RPD assicura inoltre la cooperazione con il Garante per la protezione dei dati personali e costituisce il punto di contatto per gli interessati che esercitano i propri diritti.

Nell'ambito della governance digitale, il RPD svolge un ruolo cruciale nel garantire che i principi di privacy-by-design e privacy-by-default siano incorporati nei processi di progettazione e realizzazione delle soluzioni tecnologiche. Tale attività avviene in stretto coordinamento con il Responsabile per la Transizione Digitale (RTD) per quanto riguarda la coerenza delle iniziative con la strategia digitale, e in collaborazione funzionale con l'Area Infrastrutture Edilizie e Digitali (ARIE) e con il Settore Sviluppo Digitale, in relazione agli aspetti tecnici che incidono sulla protezione dei dati personali.

Il RPD non esercita però funzioni gestionali o operative su sistemi e piattaforme, preservando la propria posizione di terzietà, come richiesto dalla normativa.

Il modello organizzativo dell'Ateneo prevede altresì un nucleo di supporto al RPD, composto da figure tecniche e amministrative incaricate, tra cui personale con competenze ICT, al fine di assicurare la piena operatività delle attività di monitoraggio, audit e gestione delle richieste degli interessati. Tale struttura di supporto consente di garantire tempestività negli adempimenti, adeguata capacità di analisi dei trattamenti e corretto raccordo con le unità operative coinvolte.

La cooperazione tra RPD, RTD e Settore Sviluppo Digitale rappresenta uno degli elementi qualificanti della governance digitale dell'Ateneo. Pur nella distinzione delle rispettive responsabilità, la sinergia tra indirizzo strategico, gestione tecnica e tutela della protezione dei dati consente di assicurare un approccio integrato alla sicurezza, alla compliance e alla qualità dei trattamenti. Tale integrazione è essenziale per consolidare un modello di amministrazione digitale conforme, responsabile e orientato alla tutela dei diritti degli utenti, in linea con gli standard europei e con le politiche nazionali in materia di protezione dei dati.

Nel complesso, il RPD rappresenta un presidio irrinunciabile nel sistema di governance della trasformazione digitale dell'Università di Napoli L'Orientale, contribuendo a garantire la conformità normativa dei processi, la proporzionalità dei trattamenti, la tutela degli interessati e l'adozione di soluzioni tecnologiche coerenti con i più elevati standard di protezione dei dati personali.

PARTE II – ANALISI DI CONTESTO

4. Analisi di contesto ICT

La definizione delle strategie di transizione digitale richiede una conoscenza approfondita, critica e sistematica dello stato attuale dell'ecosistema tecnologico dell'Ateneo. L'intento è quello di fornire una descrizione strutturata e dettagliata delle infrastrutture dei sistemi informativi messi a disposizione della comunità universitaria, con particolare attenzione alle aree di complessità e ai fattori di rischio che condizionano la capacità dell'Ateneo di evolvere in modo coerente con le linee di indirizzo nazionali.

L'analisi è condotta in conformità con il modello metodologico definito dalla Guida alla compilazione del Piano Triennale per l'informatica nella PA (AgID, giugno 2024) e con i contenuti del Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024–2026 – Aggiornamento 2026. In questa cornice, la ricognizione considera l'intero patrimonio ICT: infrastrutture on-premise e soluzioni cloud, apparati di networking e connettività, piattaforme applicative, sistemi gestionali, basi dati, strumenti di supporto alla didattica e alla ricerca, servizi all'utenza, processi documentali e componenti di sicurezza informatica.

L'impostazione riflette inoltre l'approccio elaborato dal GP_Lab, adottando un modello che procede dal livello infrastrutturale a quello applicativo, fino ad arrivare alla mappatura dei servizi e alla valutazione del livello di maturità digitale. Questa scelta permette di evidenziare non solo gli elementi di forza dell'ecosistema digitale, ma anche le discontinuità, le ridondanze, la frammentazione applicativa, la presenza di processi ancora non digitalizzati end-to-end e le criticità legate alla gestione del patrimonio informativo, all'interoperabilità e alla sicurezza.

In coerenza con le richieste del PIAO 2025–2027, l'analisi integra inoltre elementi relativi alla semplificazione amministrativa, all'accessibilità digitale, alla qualità dei servizi rivolti agli utenti interni ed esterni e ai fabbisogni organizzativi connessi all'evoluzione tecnologica. La fotografia restituita in questo capitolo costituisce quindi la baseline da cui derivano gli obiettivi operativi, le linee di intervento e le priorità strategiche del triennio 2026–2028.

Particolare attenzione è dedicata ai flussi informativi interni ed esterni, alle integrazioni applicative e all'adozione degli standard nazionali di interoperabilità (SPID, CIE, PagoPA, PDND, AppIO), con l'obiettivo di individuare i gap rispetto agli obblighi normativi, in particolare nell'ambito della sicurezza informatica e della compliance NIS2.

4.1 Stato di avanzamento della trasformazione digitale

L'Ateneo attraverso il presente documento fornisce il primo strumento organico e programmatico di pianificazione strategica per il dominio digitale istituzionale comando il gap storico di operatività in assenza di un PTTD formalmente conforme agli standard metodologici definiti da AgID. Il presente documento costituisce, pertanto,

Tale circostanza pregressa non ha implicato l'assenza di attività informatiche, essendosi comunque strutturato nel tempo dal punto di vista amministrativo ed avvalso di strutture tecniche competenti che hanno garantito la gestione dei sistemi, dell'infrastruttura di rete, dei servizi core (CINECA). Tuttavia, tali funzioni, pur assicurando la continuità operativa, erano distribuite in articolazioni organizzative frammentate e procedevano secondo logiche prettamente funzionali e reattive,

anziché aderire a una cornice unitaria di governance e standardizzazione. Questo deficit ha generato un significativo debito tecnico e di conformità che il presente Piano si prefigge di sanare.

Nel corso degli anni recenti, l'Ateneo ha comunque sviluppato un ecosistema applicativo esistente, composto da piattaforme consolidate, servizi Microsoft 365 e Azure, infrastrutture di rete, sistemi di gestione documentale e workflow amministrativi. Questa evoluzione si è sviluppata in modo incrementale e non architetturale, rispondendo a imperativi operativi o a normative specifiche. Ne è derivata la mancanza critica di un disegno architetturale di sistema complessivo e l'assenza di un modello formalizzato di ciclo di vita (lifecycle management) delle soluzioni, elementi che hanno innalzato il rischio operativo sistemico.

Proseguendo quanto già avvenuto nel recente passato, si è avuta nel 2022 la nomina del Direttore Generale quale Responsabile per la Transizione Digitale (RTD), fornendo un riferimento istituzionale chiaro. Parallelamente, la governance della protezione dei dati è stata rafforzata con la nomina del Responsabile per la Protezione dei Dati (RPD), in coordinamento con le funzioni ICT per l'adeguamento al quadro normativo GDPR e i primi requisiti della Direttiva NIS2.

Nonostante la frammentazione pregressa, il periodo post-COVID, anche grazie all'immissione di finanziamenti PNRR, ha visto un ampliamento significativo della digitalizzazione dei processi come l'adesione alla Piattaforma Digitale Nazionale Dati (PDND) con l'attivazione dell'API Manager (Misura 1.3.1 PNRR), l'adesione a Pago-PA (MISURA 1.4.3 PNRR), adozione SPID-CIE (MISURA 1.4.4 PNRR), e il consolidamento dell'utilizzo delle piattaforme gestionali. Questi risultati, pur essendo meritori, rendono indilazionabile l'esigenza di un modello strutturato di interoperabilità, di un Registro dei Dati Autorevoli e di un monitoraggio sistematico dei servizi erogati.

Il punto di svolta cruciale nella maturità digitale dell'Ateneo è stato segnato, a partire dal 2024, dall'istituzione del Settore Sviluppo Digitale convalidata dall'attribuzione delle competenze alle relative strutture con DD 4/2025. Questa azione di riorganizzazione ha per la prima volta integrato le competenze di infrastruttura, sicurezza, sistemi informativi, data governance e comunicazione digitale in una struttura unitaria, capace di fornire il necessario supporto operativo e di governance al RTD. L'istituzione della Centrale di Committenza ICT e del relativo Allegato CPV ha ulteriormente consolidato questo assetto, sancendo l'unificazione degli acquisti e la coerenza delle scelte tecnologiche.

La fotografia complessiva evidenzia un contesto attuale caratterizzato da competenze tecniche consolidate e da un patrimonio infrastrutturale significativo, ma gravato da una pregressa frammentazione organizzativa, dalla mancanza di un Disegno Architetturale Integrato e dall'assenza di un piano formale di Disaster Recovery/Business Continuity. Il presente Piano Triennale nasce specificamente per colmare questa distanza e mitigare i rischi ereditati: l'obiettivo primario è consolidare i progressi compiuti, ricostruire l'architettura sistemica e avviare un ciclo di pianificazione triennale coerente, misurabile e basato sul miglioramento continuo, stabilendo per la prima volta un modello unitario di governo del digitale nell'Ateneo.

4.2 Ecosistema infrastrutturale

L'ecosistema infrastrutturale dell'Università di Napoli L'Orientalesi fonda su un insieme articolato di componenti hardware, dotazioni di rete, sistemi di sicurezza e piattaforme di virtualizzazione che garantiscono la continuità dei servizi digitali e il supporto alle attività istituzionali, didattiche, amministrative e di ricerca. L'infrastruttura si è sviluppata nel tempo secondo

un modello ibrido, che combina risorse on-premise, collocate nei datacenter dell'Ateneo, con servizi cloud erogati tramite la convenzione CRUI–Microsoft e le piattaforme applicative fornite da CINECA. Tale modello ha assicurato una buona resilienza operativa, pur con elementi di eterogeneità e stratificazione che richiedono oggi una più chiara integrazione architetturale.

I datacenter principali sono collocati presso Palazzo Giusso e Palazzo del Mediterraneo e ospitano server fisici, sistemi di virtualizzazione, apparati di rete e componenti di sicurezza. Entrambi i siti sono dotati di sistemi UPS, climatizzazione controllata e politiche di accesso regolamentate. L'ambiente virtuale, basato su cluster VMware vSphere, consente la distribuzione dei carichi e la gestione delle macchine virtuali, ma presenta gradi diversi di obsolescenza e un livello di ridondanza non pienamente allineato agli standard nazionali di continuità operativa. I sistemi di backup e archiviazione, articolati su storage centralizzati, NAS e repository dedicati, garantiscono la salvaguardia dei dati, sebbene sia necessario il consolidamento di un piano di disaster recovery strutturato e verificato periodicamente.

La rete di Ateneo, distribuita su più sedi nel centro storico, si basa su dorsali in fibra ottica, apparati di switching di livello enterprise e firewall di nuova generazione, con un monitoraggio costante delle prestazioni e dello stato di integrità. La stratificazione degli apparati nel tempo e le diverse caratteristiche edilizie delle sedi determinano talvolta livelli non uniformi di copertura e complessità nelle attività di manutenzione, rendendo necessario un percorso progressivo di standardizzazione. Alla connettività interna si affianca quella tramite la rete GARR, che garantisce banda adeguata alla didattica e alla ricerca. La copertura wireless è assicurata tramite Eduroam®, integrata con le credenziali istituzionali e conforme agli standard internazionali di autenticazione federata.

L'infrastruttura di autenticazione è basata sul sistema di Identity Management di CINECA, integrato con Active Directory e con i meccanismi SPID/CIE per l'accesso ai servizi destinati agli utenti. Il provisioning delle utenze è in larga parte automatizzato, pur conservando componenti manuali e senza un modello compiuto di identity governance. Particolare rilevanza rivestono i sistemi critici della finanza digitale (InBiz), gestiti in collaborazione con la Direzione Generale, che richiedono misure di protezione ulteriori e un rafforzamento delle politiche di segregazione dei ruoli.

La fonia VoIP rappresenta un ambito infrastrutturale consolidato ma caratterizzato da elementi di obsolescenza. L'architettura basata su soluzioni VoIsmart garantisce il servizio telefonico istituzionale ma non dispone ancora di ridondanza, integrazione con piattaforme cloud né capacità avanzate di unified communication. L'evoluzione verso soluzioni PBX cloud integrate con Microsoft Teams costituisce uno degli ambiti prioritari del percorso di modernizzazione.

Completano il quadro infrastrutturale le dotazioni delle postazioni di lavoro, gli apparati multimediali delle aule e dei laboratori e le tecnologie dedicate alla didattica. Tali componenti, pur coperte da presidi antivirus e strumenti di gestione centralizzata, richiedono un allineamento progressivo agli standard di sicurezza previsti da NIS2 e un censimento sistematico attraverso una Configuration Management Database (CMDB) oggi non ancora pienamente formalizzata.

Nel loro complesso, le infrastrutture hardware e di rete dell'Ateneo costituiscono un sistema affidabile e solido, adeguato alle esigenze operative e integrato con i servizi cloud e SaaS in uso, ma al tempo stesso caratterizzato da elementi di eterogeneità, da un'evoluzione non completamente pianificata e dalla necessità di un consolidamento architetturale. Il presente Piano opera in questa direzione, ponendosi l'obiettivo di trasformare l'attuale infrastruttura in una piattaforma

coerente, scalabile, sicura e allineata agli standard nazionali di interoperabilità e resilienza, capace di sostenere in modo strutturato la crescita dei servizi digitali dell'Ateneo.

4.3 Ecosistema applicativo e servizi digitali istituzionali

L'ecosistema applicativo dell'Università di Napoli L'Orientale è costituito da un insieme articolato e in continua evoluzione di piattaforme digitali, sistemi gestionali, portali tematici e servizi online che supportano le attività istituzionali, didattiche, amministrative e di ricerca. Tale patrimonio applicativo, frutto di sviluppi progressivi e dell'adozione di soluzioni consolidate a livello nazionale, rappresenta oggi uno dei principali fattori abilitanti della trasformazione digitale dell'Ateneo, contribuendo alla qualità dei servizi erogati, all'efficienza dei processi e alla coerenza informativa.

La gestione delle carriere e dei servizi agli studenti si fonda sul sistema ESSE3 del Consorzio CINECA, piattaforma centrale per immatricolazioni, iscrizioni, verbalizzazione esami, pagamenti e gestione amministrativa del percorso formativo. Il sistema è integrato con il Course Catalogue per la consultazione dell'offerta formativa e con i portali dei Dottorati, sviluppati internamente in modo uniforme per garantire trasparenza, aggiornamento e standardizzazione della comunicazione verso gli studenti e i referenti accademici. La didattica digitale è supportata dalla piattaforma Moodle, gestita dal Centro Linguistico di Ateneo (CLAOR), che consente l'erogazione di contenuti multimediali, attività sincrone e asincrone e forme di apprendimento blended. A completamento dei servizi rivolti agli studenti, l'Ateneo mette a disposizione MyUniOr, applicazione che consente la fruizione integrata delle informazioni accademiche, e un sistema centralizzato di help desk dedicato al supporto su ESSE3, pagamenti, credenziali e servizi di carriera.

Per le attività dei docenti e dei ricercatori, l'Ateneo utilizza UniFIND come portale del docente per l'anagrafe della produzione scientifica, integrato con UNORA–IRIS, piattaforma per il deposito, la validazione e l'esportazione dei prodotti della ricerca verso i sistemi ministeriali. L'ecosistema applicativo comprende inoltre servizi specialistici quali Compilatio, adottato per il controllo antiplagio, Zoom per attività seminariali e di didattica a distanza, e software avanzati come Sketch Engine per analisi linguistiche complesse. Un ruolo rilevante è svolto dal Centro BIMA con la sezione Digital Humanities, che offre strumenti e servizi per la digitalizzazione e la valorizzazione del patrimonio culturale, basati su metodologie e standard internazionali.

La Biblioteca Digitale d'Ateneo è erogata tramite la piattaforma OrienTales, basata su D-Space, che raccoglie collezioni digitalizzate e nativamente digitali e utilizza standard evoluti di metadatazione e interoperabilità quali IIIF, OCR e analisi semantiche avanzate tramite la funzione Network Lab. Tale sistema rappresenta un asset strategico per la ricerca e per la conservazione del patrimonio documentale, con un livello di maturità digitale particolarmente elevato.

L'ecosistema applicativo a supporto del personale tecnico-amministrativo si basa sull'integrazione di diverse soluzioni gestionali. La piattaforma TITULUS governa il protocollo informatico e la gestione documentale; i principali processi amministrativi sono gestiti tramite i moduli U-Gov (contabilità, bilancio, personale, missioni, contratti e approvvigionamenti), integrati con il sistema U-Buy per il procurement digitale e con il Portale Amministrazione Trasparente per gli adempimenti normativi. Le procedure concorsuali e la gestione delle selezioni sono centralizzate su PICA, mentre i pagamenti e i servizi finanziari sono integrati con PagoPA e con le soluzioni CINECA ad esso collegate.

Accanto ai sistemi consolidati, negli ultimi anni l'Ateneo ha sviluppato e messo in esercizio una serie di piattaforme digitali interne, quali l'intranet istituzionale, il sistema di ticketing dell'Area Infrastrutture Edilizie e Digitali, la piattaforma Visiting Professor per la mobilità internazionale e il simulatore digitale delle tasse universitarie. Tali servizi, realizzati per rispondere a esigenze operative e per migliorare la qualità dell'erogazione, costituiscono un importante arricchimento dell'ecosistema applicativo, pur rappresentando un patrimonio tecnologico che richiede una progressiva standardizzazione delle architetture, dei modelli di sviluppo, delle integrazioni e della sicurezza applicativa.

Completano il panorama dei servizi digitali trasversali la posta elettronica istituzionale e la suite Microsoft 365, che forniscono strumenti avanzati di comunicazione e collaborazione, l'accesso autenticato alle risorse elettroniche tramite proxy e VPN e la piattaforma MySiteUniOr, regolamentata e gestita dal Settore Sviluppo Digitale, che consente la creazione controllata di micrositi istituzionali da parte dei Centri di ricerca e delle strutture accademiche.

Nel loro complesso, i servizi digitali istituzionali dell'Ateneo costituiscono un ecosistema applicativo esteso e articolato, con un livello crescente di integrazione con i sistemi centrali e con le infrastrutture cloud e SaaS adottate. Essi rappresentano uno dei pilastri della trasformazione digitale dell'Università: un patrimonio in continua evoluzione che necessita, nel triennio 2026–2028, di un consolidamento architetturale, del rafforzamento del modello di interoperabilità, della definizione di una data governance unitaria e di una maggiore uniformità dei modelli di sviluppo e gestione, al fine di garantire sicurezza, qualità e sostenibilità nel tempo.

4.4 Integrazioni applicative, interoperabilità e PDND

L'ecosistema informativo dell'Università "L'Orientale" è caratterizzato da un insieme ampio e diversificato di piattaforme applicative,\ molte delle quali fornite da CINECA o sviluppate internamente, che supportano i processi accademici, amministrativi e di ricerca. La capacità di queste piattaforme di dialogare tra loro e con i servizi esterni rappresenta un elemento centrale della trasformazione digitale, poiché consente di garantire coerenza informativa, riduzione delle duplicazioni e qualità dei dati, oltre a costituire un presupposto essenziale per l'erogazione dei servizi digitali alla comunità universitaria. L'integrazione applicativa dell'Ateneo si è sviluppata nel tempo attraverso un insieme di connettori, scambi automatici di dati e procedure operative consolidate, nate spesso per rispondere a esigenze specifiche e in assenza di un modello architetturale unitario; ciò determina oggi un ecosistema funzionante, ma eterogeneo e solo parzialmente allineato agli standard nazionali di interoperabilità.

Il sistema ESSE3 rappresenta la piattaforma maggiormente integrata con altri sistemi istituzionali: esso dialoga con PagoPA per la gestione dei pagamenti, con il sistema di autenticazione istituzionale mediante SPID/CIE, con l'identity management per il provisioning delle utenze e con i portali dedicati ai dottorati e all'offerta formativa. U-Gov, a sua volta, è interconnesso con Titulus per la gestione documentale, con U-Buy per gli approvvigionamenti digitali e con la piattaforma Trasparenza sviluppata da CINECA, generando un flusso di dati che accompagna l'intero ciclo amministrativo. PICA gestisce la pubblicazione e la ricezione delle candidature ai concorsi, collegandosi ai moduli ESSE3 per i ruoli accademici e a U-Gov per gli adempimenti amministrativi. Ulteriori integrazioni riguardano l'ambito della ricerca, con la connessione fra UniFIND, UNORA–IRIS e i sistemi di rendicontazione ministeriali, e l'ambito dei servizi digitali interni, come il simulatore tasse e il sistema di ticketing ARIE, che si interfacciano con l'identità istituzionale e con i flussi documentali.

Accanto alle integrazioni oggi operative, l'Ateneo ha compiuto un passo rilevante in materia di interoperabilità nazionale aderendo alla Piattaforma Digitale Nazionale Dati (PDND) nell'ambito della Misura PNRR 1.3.1. L'attivazione dell'API Manager CINECA e la pubblicazione degli e-service ESSE3 negli ambienti di test e produzione rappresentano un risultato strategico, che consente all'Ateneo di erogare gli otto servizi obbligatori relativi a iscrizioni, offerta formativa, titoli, ISEE e variazioni anagrafiche. Tale traguardo costituisce una premessa fondamentale per la transizione verso un modello di interoperabilità pienamente allineato al ModI nazionale; tuttavia, la gestione delle API e della loro qualità è oggi fortemente dipendente dal fornitore, mentre non è ancora presente un sistema interno di governo del ciclo di vita delle API, di catalogazione dei servizi, di definizione delle fonti dati autorevoli o di monitoraggio dei consumi e delle anomalie. Questo elemento strategico richiede un progressivo consolidamento nel triennio 2026–2028, attraverso l'introduzione di standard documentali, processi di gestione centralizzata e strumenti di controllo in grado di integrare la componente interna e quella esternalizzata.

L'integrazione applicativa si estende anche alle piattaforme sviluppate internamente, come MySiteUniOr, i portali dei dottorati, il portale Visiting Professor, l'intranet e il sistema di ticketing. Questi servizi, nati per rispondere a esigenze operative specifiche, si interfacciano con sistemi centrali attraverso l'identità istituzionale, i workflow documentali, i contenuti prelevati da ESSE3 o da U-Gov e i repository di Ateneo. Sebbene tali integrazioni assicurino un'esperienza utente più uniforme, esse presentano livelli non omogenei di standardizzazione tecnica e richiedono, nel presente Piano, una razionalizzazione delle modalità di scambio dati, delle API interne e dei modelli di sicurezza applicativa.

Nel complesso, l'interoperabilità dell'Ateneo è oggi caratterizzata da un insieme di integrazioni efficaci ma nate in un contesto di sviluppo progressivo e non pienamente coordinato, in cui convivono soluzioni standard del fornitore, connettori locali e scambi di dati basati su procedure operative consolidate nel tempo. Questo scenario evidenzia la necessità di adottare un modello organico di architettura applicativa, fondato su standard uniformi, sulla definizione di domini informativi, sulla introduzione di un registro dei dati autorevoli e sulla progressiva convergenza verso tecnologie e formati comuni. Il presente Piano si propone di consolidare le integrazioni esistenti, rafforzare l'interoperabilità interna ed esterna e costruire un assetto di governo che consenta all'Ateneo di operare in piena coerenza con il ModI, con le Linee Guida AgID e con gli obblighi derivanti dalla PDND, garantendo coerenza informativa, sicurezza e sostenibilità nel ciclo di vita delle applicazioni digitali.

4.5 Patrimonio informativo, data governance e qualità del dato

Il patrimonio informativo dell'Università di Napoli L'Orientalerappresenta uno degli asset strategici dell'Ateneo e costituisce la base sulla quale si fondano i processi amministrativi, didattici, finanziari e scientifici. Nel corso degli anni, l'Ateneo ha consolidato un insieme ampio di basi dati, generate e mantenute attraverso le piattaforme applicative centrali (ESSE3, U-Gov, Titulus, PICA, UniFIND, UNORA–IRIS, Datawarehouse CINECA, OrienTales), nonché tramite i numerosi servizi digitali sviluppati internamente. Questo insieme composito di risorse informative, pur ricco e di elevato valore istituzionale, è stato prodotto in un contesto di crescita progressiva e non coordinata, generando un ecosistema informativo eterogeneo che richiede oggi una visione unitaria di governo, qualità e sicurezza del dato.

I principali sistemi gestionali dell'Ateneo costituiscono le fonti autorevoli per i rispettivi domini informativi: ESSE3 per le carriere studentesche, U-Gov per la contabilità, il personale e gli approvvigionamenti, Titulus per il protocollo e i flussi

documentali, PICA per le selezioni e i concorsi, UNORA–IRIS e UniFIND per la produzione scientifica, OrienTales per il patrimonio digitale, il Datawarehouse CINECA per la reportistica e gli indicatori istituzionali. A questi sistemi si affiancano basi dati locali generate da servizi interni, quali l'intranet, il ticketing, i portali dei dottorati, le piattaforme Visiting e MySiteUniOr, e strumenti sviluppati per specifiche esigenze (come il simulatore tasse). La coesistenza di tali servizi ha favorito l'ampliamento dell'offerta digitale dell'Ateneo, ma ha anche incrementato il numero di punti di produzione del dato, determinando differenze nella qualità, nella periodicità di aggiornamento e nella definizione dei contenuti informativi.

A oggi, l'Ateneo non dispone ancora di una data governance formalmente definita, né di un registro organico delle fonti dati autorevoli. La definizione dei domini informativi, dei responsabili del dato, dei criteri di aggiornamento e delle regole di interoperabilità è avvenuta per prassi operative consolidate, senza un modello unitario né documentazione sistematica trasversale. Ciò comporta la presenza di duplicazioni, ridondanze, rappresentazioni non omogenee dello stesso dato in sistemi differenti e una dipendenza significativa dalle procedure applicative dei fornitori, in particolare CINECA, che gestisce i dati critici degli studenti, del personale, dei pagamenti e della didattica. Questo scenario evidenzia la necessità di introdurre un modello strutturato di governo del patrimonio informativo, capace di garantire coerenza, qualità e tracciabilità nel ciclo di vita dei dati.

Il ruolo del Responsabile della Protezione dei Dati (RPD), nominato con atto formale dell'Ateneo e supportato da uno staff tecnico e giuridico, rappresenta un presidio essenziale per la conformità al GDPR e per la valutazione dei trattamenti, ma non è ancora affiancato da un modello di governance dei dati che integri privacy, sicurezza ICT, interoperabilità e qualità informativa in una prospettiva unitaria. Allo stesso modo, il Settore Sviluppo Digitale, attraverso le unità ARIE04–07, gestisce componenti applicative e infrastrutturali critiche che producono, trasformano o espongono informazioni sensibili; tuttavia, manca un quadro formale che assegni responsabilità operative sulla correttezza, sull'integrità e sulla disponibilità dei dati in relazione ai sistemi gestiti.

L'arrivo della Piattaforma Digitale Nazionale Dati introduce un elemento ulteriore di rilevanza strategica. La pubblicazione degli e-service ESSE3 tramite l'API Manager CINECA consente all'Ateneo di condividere dati verso la PDND in conformità agli standard nazionali, ma rende necessario definire con chiarezza le fonti informative, le politiche di qualità del dato, le modalità di controllo, i sistemi di audit e la responsabilità interna sul dominio informativo, al fine di ridurre il rischio di non conformità nel quinquennio di obbligo previsto dal PNRR. La partecipazione alla PDND offre dunque un'opportunità di riorganizzazione del patrimonio informativo, ma richiede un'evoluzione dei processi e dei presidi interni.

In questo contesto, la qualità del dato rappresenta un obiettivo prioritario. Le verifiche condotte nel corso delle attività di accreditamento, dei processi AVA3, delle rendicontazioni ministeriali e delle analisi interne mostrano differenze nella coerenza dei dati tra sistemi, assenza di validazioni automatiche in alcuni processi, mancanza di criteri uniformi per la correzione delle anomalie e insufficienza di strumenti di monitoraggio continuo. Analogamente, la presenza di dati prodotti da piattaforme interne – talvolta privi di standard, formalismi documentali o metadatazione strutturata – rende necessario definire criteri comuni per l'esposizione, l'aggiornamento e la conservazione dei contenuti informativi.

Nel complesso, l'Ateneo possiede un patrimonio informativo ricco e di elevato valore istituzionale, ma privo di una governance organica che ne garantisca qualità, utilizzo strategico, sicurezza e interoperabilità. Il presente Piano si propone pertanto di avviare la definizione del modello di data governance d'Ateneo, basato sulla identificazione delle fonti dati

autorevoli, sulla formalizzazione dei domini informativi, sulla definizione dei responsabili del dato, sull'adozione di standard comuni di qualità e sulla progressiva integrazione con la PDND, in coerenza con le Linee Guida AgID, il GDPR e i requisiti emergenti di sicurezza e resilienza digitale. Tale modello costituisce un elemento essenziale per la maturità digitale dell'Ateneo e per la sostenibilità dell'intero ecosistema informativo nel triennio 2026–2028.

4.6 Fruizione dei servizi digitali e esperienza degli utenti

I servizi digitali istituzionali dell'Università di Napoli L'Orientalerappresentano l'interfaccia principale tra l'Ateneo e la propria comunità di utenti – studenti, docenti, ricercatori, personale tecnico-amministrativo, partner esterni e stakeholder – e costituiscono la dimensione più direttamente percepita della trasformazione digitale. Nel corso degli anni, l'Ateneo ha progressivamente ampliato il ventaglio di servizi online disponibili, combinando piattaforme consolidate, soluzioni CINECA, strumenti Microsoft 365, servizi dedicati alla didattica e applicazioni sviluppate internamente. Questo insieme eterogeneo di servizi consente un accesso integrato alle informazioni, ai processi accademici e ai procedimenti amministrativi, pur evidenziando la necessità di un maggiore coordinamento, di standard comuni e di un governo unitario dell'esperienza digitale.

Per gli studenti sono disponibili servizi digitali che coprono l'intero ciclo di vita universitario: ESSE3 costituisce il punto di accesso per le procedure amministrative (immatricolazioni, carriera, prenotazioni, esami, pagamenti), mentre MyUniOr offre un'interfaccia più immediata per la consultazione della propria carriera e delle informazioni essenziali. Il Course Catalogue e i portali dei Dottorati, uniformati nella struttura e nel linguaggio, garantiscono trasparenza e aggiornamento costante sull'offerta formativa, mentre Moodle sostiene la didattica digitale, la fruizione di contenuti multimediali e la gestione dei materiali didattici. Per esigenze specifiche sono stati introdotti servizi digitali ulteriori, quali il simulatore tasse e il sistema di help desk, che facilitano l'orientamento e il supporto operativo, rendendo i servizi fruibili anche da utenti con competenze digitali eterogenee.

I docenti e i ricercatori dispongono di servizi digitali dedicati alla gestione dell'attività accademica e scientifica: UniFIND e UNORA–IRIS consentono la consultazione, la validazione e il deposito dei prodotti della ricerca; strumenti specialistici come Compilatio, Zoom o Sketch Engine supportano la didattica e l'attività scientifica; MySiteUniOr permette la produzione e pubblicazione di contenuti istituzionali in modo controllato e standardizzato. L'integrazione progressiva di tali servizi con l'identità digitale istituzionale e con l'infrastruttura Microsoft 365 contribuisce a rendere più coerente l'esperienza dell'utenza, anche se permangono differenze nell'interfaccia, nei percorsi di accesso e nelle modalità di supporto.

Per il personale tecnico-amministrativo e i servizi di back-office, l'Ateneo mette a disposizione un insieme articolato di servizi digitali interni. L'intranet rappresenta il punto unico di accesso alla documentazione riservata, alla modulistica operativa e agli aggiornamenti istituzionali; Titulus consente la gestione del protocollo e dei flussi documentali; i moduli U-Gov, integrati con U-Buy e con il Portale di Amministrazione Trasparente, governano i processi amministrativi centrali. A tali servizi si affiancano soluzioni digitali specifiche, quali PICA per le procedure concorsuali, il sistema di ticketing dell'Area Infrastrutture Edilizie e Digitali per il supporto tecnico-specialistico e la piattaforma Visiting Professor dedicata alla mobilità accademica internazionale.

Una componente trasversale fondamentale è rappresentata dai servizi di comunicazione e collaborazione. La suite Microsoft 365, già ampiamente diffusa tra studenti e personale, consente l'utilizzo integrato di posta elettronica, strumenti

di produttività, videoconferenza, collaborazione in tempo reale e gestione dei contenuti digitali. L'accesso autenticato alle risorse elettroniche tramite VPN istituzionale, eduroam e proxy consente inoltre l'utilizzo sicuro dei servizi anche in mobilità. La comunicazione istituzionale e la diffusione dei contenuti digitali sono regolate da modelli editoriali uniformi, in coerenza con il Piano di Comunicazione di Ateneo, al fine di garantire chiarezza, accessibilità e aggiornamento delle informazioni.

Sebbene l'offerta complessiva dei servizi risulti ampia, articolata e in costante evoluzione, l'esperienza dell'utente evidenzia ancora margini significativi di miglioramento. La molteplicità dei punti di accesso, la disomogeneità delle interfacce, la mancanza di un portale unitario dei servizi digitali e l'assenza di standard uniformi di monitoraggio, accessibilità e usabilità limitano la percezione complessiva di coerenza del sistema. Al contempo, l'introduzione di nuovi servizi sviluppati internamente ha ampliato la disponibilità di funzionalità innovative, ma richiede un consolidamento delle modalità di pubblicazione, un modello di supporto più strutturato e una progressiva integrazione con i sistemi centrali.

Nel complesso, i servizi digitali istituzionali dell'Ateneo rappresentano una leva fondamentale per l'efficienza amministrativa, per la qualità della didattica e della ricerca e per l'accessibilità delle informazioni. Essi costituiscono un ecosistema ricco e dinamico, che necessita ora di un processo di razionalizzazione, semplificazione e unificazione dell'esperienza utente, in coerenza con il Modello di Interoperabilità nazionale, con gli standard AgID, con gli obblighi della PDND e con gli obiettivi strategici del presente Piano. La roadmap triennale prevista nel successivo capitolo individua gli interventi necessari per rendere i servizi più integrati, accessibili e orientati all'utente, contribuendo a rafforzare la maturità digitale complessiva dell'Ateneo.

4.7 Sicurezza informatica, rischio cyber

La sicurezza informatica costituisce uno degli assi portanti della trasformazione digitale dell'Università di Napoli L'Orientale, in un contesto normativo caratterizzato da requisiti sempre più stringenti e da un quadro di minacce in costante evoluzione. L'Ateneo gestisce dati personali, amministrativi, scientifici e didattici di elevato valore, distribuiti su piattaforme eterogenee e ospitati sia su infrastrutture on-premise sia su servizi cloud e SaaS; il livello di esposizione al rischio cyber è pertanto significativo e richiede un approccio sistemico alla protezione degli asset digitali, in coerenza con la direttiva NIS2, il GDPR, il CAD e le Linee Guida AgID.

L'infrastruttura ICT presenta alcuni elementi consolidati di sicurezza: l'Ateneo dispone di firewall di nuova generazione, sistemi di filtraggio e monitoraggio del traffico, VPN istituzionale per l'accesso remoto sicuro, segmentazioni di rete, sistemi antivirus e strumenti di aggiornamento centralizzato sugli endpoint. La gestione delle identità digitali poggia sul sistema IDM CINECA, integrato con Active Directory e con le identificazioni federate SPID/CIE e IDEM-GARR, assicurando un livello di controllo e tracciabilità adeguato agli accessi ai sistemi centrali. I datacenter sono protetti da misure fisiche, da sistemi UPS e da controlli sugli accessi, e il modello ibrido on-premise/cloud basato sulla convenzione CRUI–Microsoft consente di beneficiare di infrastrutture con standard di sicurezza elevati, in particolare per posta elettronica, collaborazione e archiviazione documentale.

Accanto a questi elementi di solidità, permangono tuttavia aspetti di criticità che richiedono un intervento strutturato. L'assenza di un piano formalizzato di sicurezza ICT e di gestione del rischio cyber costituisce ad oggi uno dei principali

gap rispetto ai requisiti NIS2, così come la mancata definizione di un inventario completo degli asset critici e delle dipendenze ICT dell'Ateneo. Analogamente, non sono ancora pienamente sviluppati i processi di classificazione dei dati, di valutazione delle vulnerabilità, di gestione dei log e di audit continuativo, strumenti indispensabili per individuare tempestivamente anomalie, accessi non autorizzati e potenziali compromissioni.

La fonia VoIP, l'infrastruttura di rete stratificata, la presenza di sedi con caratteristiche edilizie eterogenee, le dotazioni informatiche non uniformi e la mancanza di un disaster recovery completo rappresentano ulteriori elementi di rischio, poiché possono costituire punti di attacco privilegiati o limitare la capacità dell'Ateneo di garantire la continuità operativa in caso di incidente critico. Allo stesso modo, la progressiva diffusione di servizi digitali sviluppati internamente, pur rappresentando un valore aggiunto in termini di innovazione, introduce anche la necessità di definire criteri univoci di sviluppo sicuro, di gestione delle vulnerabilità, di aggiornamento delle dipendenze software e di integrazione con le piattaforme centrali.

Sul piano organizzativo, l'Ateneo ha adottato misure di rilievo, tra cui la nomina del Responsabile per la Protezione dei Dati (RPD) e del relativo staff multidisciplinare, che ha rafforzato il presidio privacy e la valutazione dei trattamenti secondo il GDPR. Tuttavia, non è ancora presente un modello pienamente operativo di coordinamento tra RPD, RTD e CSIRT interno, né un processo strutturato di reporting, comunicazione interna e gestione degli incidenti, elementi che la direttiva NIS2 richiede in modo esplicito. La presenza di competenze tecniche nel Settore Sviluppo Digitale costituisce un fattore abilitante, ma rende necessario un piano di formazione continua e di rafforzamento delle competenze cyber, in coerenza con le linee di sviluppo professionale previste per il personale ICT.

La partecipazione dell'Ateneo alla PDND aggiunge ulteriori responsabilità in termini di sicurezza e qualità dei dati. La pubblicazione degli e-service ESSE3 tramite l'API Manager CINECA impone la definizione di procedure interne di controllo, monitoraggio, audit e gestione delle anomalie, oltre alla necessità di garantire la sicurezza delle API, la verificabilità dei log e la tracciabilità delle operazioni effettuate dagli applicativi connessi. Un presidio non adeguato di tali aspetti espone l'Ateneo a rischi di non conformità e di compromissione dei servizi, con potenziali conseguenze di carattere operativo, reputazionale e finanziario.

Nel complesso, l'Università "L'Orientale" presenta un livello di sicurezza informatica adeguato alla gestione quotidiana dei servizi, ma non ancora pienamente conforme ai requisiti di resilienza, governance del rischio e coordinamento strategico richiesti dal nuovo quadro normativo. Il presente Piano assume questa consapevolezza come punto di partenza, definendo nel triennio 2026–2028 un percorso di rafforzamento che prevede: la formalizzazione del sistema di gestione della sicurezza, l'adozione di processi strutturati di risk management, la definizione dell'inventario degli asset ICT, l'implementazione di strumenti di monitoraggio avanzato, la revisione delle procedure di business continuity e disaster recovery, l'allineamento al framework NIS2, la formazione del personale e il consolidamento del modello di cooperazione tra RTD, RPD e Settore Sviluppo Digitale.

Questi interventi rappresentano una componente essenziale della maturità digitale dell'Ateneo e condizionano la capacità del sistema ICT di garantire continuità, integrità e sicurezza dei servizi pubblici digitali nel medio e lungo periodo.

4.8 Livello di maturità digitale dell'Ateneo

La valutazione del livello di maturità digitale dell'Università di Napoli L'Orientale rappresenta la sintesi dell'analisi condotta nei paragrafi precedenti e consente di collocare in modo oggettivo l'Ateneo lungo il percorso di sviluppo delineato dal Piano Triennale per l'Informatica nella PA e dalle metodologie del Laboratorio GoodPractice del Politecnico di Torino. La maturità digitale viene quindi interpretata come un insieme integrato di dimensioni infrastrutturali, applicative, organizzative, procedurali, informative, di sicurezza e di esperienza utente, tutte indispensabili per valutare la capacità dell'Ateneo di governare e sviluppare il proprio ecosistema ICT.

Nel complesso, l'Ateneo presenta un livello di maturità digitale intermedio, caratterizzato da solide basi tecniche e organizzative, da un patrimonio applicativo ricco e da una crescente disponibilità di servizi digitali, ma anche dalla presenza di alcune criticità che richiedono un piano strutturato di evoluzione nel triennio 2026–2028.

Dal punto di vista infrastrutturale, l'Ateneo dispone di datacenter fisici consolidati, cluster di virtualizzazione, una rete geografica estesa su tutte le sedi, connettività GARR, sistemi firewall di nuova generazione e un modello ibrido on-premise/cloud già in fase avanzata di adozione. Tali elementi configurano una base tecnologica affidabile, pur richiedendo investimenti per l'aggiornamento degli apparati, la standardizzazione della rete, la revisione della fonia VoIP e soprattutto l'adozione di un modello pienamente operativo di continuità e disaster recovery, oggi ancora non formalizzato.

Sul piano applicativo, l'Ateneo presenta un ecosistema maturo, strutturato su piattaforme centrali CINECA (ESSE3, U-Gov, PICA, Trasparenza, Datawarehouse), su sistemi a supporto della didattica e della ricerca (Moodle, UniFIND, UNORA–IRIS), su servizi istituzionali trasversali (Titulus, U-Buy, Microsoft 365) e su applicazioni sviluppate internamente dal Settore Sviluppo Digitale. Questo insieme, ampliato negli ultimi anni, consente un'elevata copertura funzionale e un buon livello di integrazione, pur evidenziando la necessità di una maggiore uniformità nelle architetture applicative, nei modelli di sviluppo e nelle politiche di manutenzione.

La maturità organizzativa dell'Ateneo in ambito ICT è in una fase avanzata di consolidamento: la nascita del Settore Sviluppo Digitale e delle unità ARIE04–07 ha permesso di superare la precedente frammentazione delle competenze, rafforzando il coordinamento tra RTD, RPD e funzioni tecniche. Questo assetto costituisce uno degli elementi più rilevanti della crescita dell'Ateneo, poiché offre per la prima volta un presidio stabile e trasversale dei sistemi informativi, dei processi digitali e del patrimonio informativo. Tuttavia, sono ancora necessari interventi per la piena definizione dei processi, per la standardizzazione delle pratiche operative e per la completa integrazione delle competenze professionali ICT.

Sul versante dell'interoperabilità, l'Ateneo ha raggiunto un livello significativo grazie all'adozione di SPID, CIE, PagoPA e IDEM-GARR e soprattutto alla piena adesione alla PDND tramite la pubblicazione degli e-service ESSE3. Nonostante questo avanzamento, la capacità dell'Ateneo di gestire in autonomia il ciclo di vita delle API, di documentare le integrazioni e di definire un modello interno di interoperabilità è ancora in fase di sviluppo, rendendo necessario un percorso di allineamento al Modello di Interoperabilità nazionale.

La dimensione relativa al patrimonio informativo risulta invece uno dei principali ambiti di miglioramento: l'assenza di una data governance formalizzata, di domini informativi definiti, di un registro delle fonti dati autorevoli e di processi strutturati

di qualità del dato limita la piena affidabilità dei flussi informativi e rallenta l'evoluzione dei processi digitali. Ciò incide in modo particolare sugli obblighi di rendicontazione, sulla reportistica strategica e sui requisiti richiesti da AVA3 e dai sistemi ministeriali.

La sicurezza informatica, come delineato nel paragrafo precedente, presenta elementi di solidità operativa ma richiede un allineamento strutturale ai requisiti della direttiva NIS2 e alle Linee Guida AgID. L'assenza di un modello formalizzato di gestione del rischio cyber, la mancanza di un inventario completo degli asset ICT, la necessità di potenziare il monitoraggio dei log e di definire strategie di business continuity rappresentano oggi aspetti centrali del percorso di maturità dell'Ateneo.

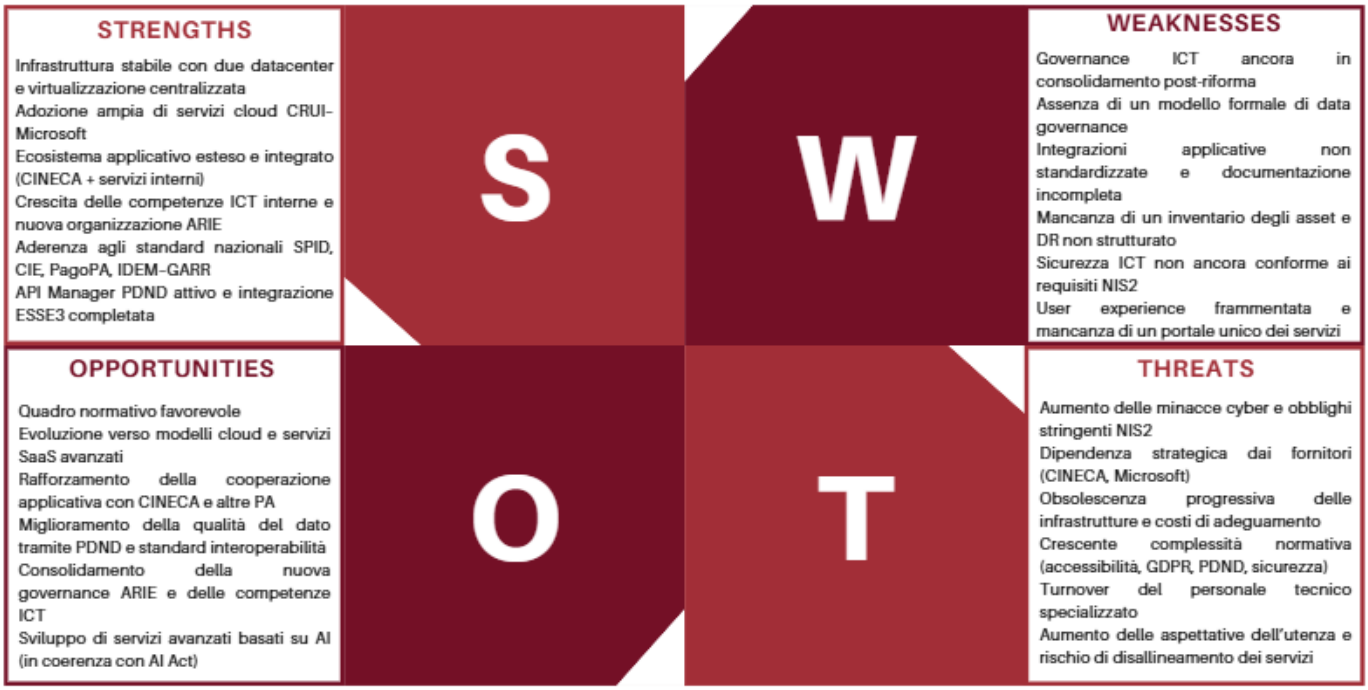
Infine, l'esperienza utente mostra un ecosistema ricco di servizi, ma non ancora pienamente coerente in termini di accessibilità, usabilità e punti di accesso. La disomogeneità delle interfacce e l'assenza di un portale unico dei servizi rendono necessario un lavoro di razionalizzazione e di semplificazione, che rappresenta una delle priorità del triennio.

Nel loro insieme, questi elementi configurano un Ateneo che ha posto basi solide per la trasformazione digitale, che ha superato le criticità storiche legate alla frammentazione organizzativa e che dispone oggi di un modello di governance ICT adeguato per sostenere una crescita strutturale. Tuttavia, il livello di maturità digitale può essere definito intermedio con forte potenziale evolutivo, caratterizzato da infrastrutture affidabili, da servizi digitali estesi, da un'organizzazione ICT in consolidamento e da aree critiche — data governance, interoperabilità interna, sicurezza avanzata, standardizzazione dei processi — che il presente Piano intende affrontare in modo prioritario e misurabile.

4.9 Analisi SWOT del dominio ICT

L'analisi SWOT del dominio ICT viene utilizzata come strumento di supporto alla decisione per tradurre l'analisi di contesto in un quadro sintetico delle leve strategiche e delle vulnerabilità del sistema digitale dell'Ateneo. Essa consente di connettere gli elementi emersi nei paragrafi precedenti con la definizione delle priorità di intervento del triennio 2026–2028, assicurando coerenza tra diagnosi, pianificazione e valutazione dei rischi.

La matrice illustra, in modo immediato, le condizioni interne (punti di forza e debolezza) e i fattori esterni (opportunità e minacce) che caratterizzano l'ecosistema ICT dell'Università, integrando aspetti infrastrutturali, applicativi, organizzativi, di data governance, di sicurezza informatica e di compliance normativa.



PARTE III – LINEE STRATEGICHE DI INTERVENTO

5. Linee strategiche di intervento

Le linee strategiche di intervento definiscono l'indirizzo attraverso cui l'Ateneo orienta e coordina il percorso di trasformazione digitale previsto per il triennio 2026–2028. Esse costituiscono l'esito naturale dell'analisi di contesto condotta nel Capitolo 4 e rappresentano il punto di raccordo tra la visione generale espressa nei Capitoli 1–3 e la successiva programmazione operativa del Piano.

Il quadro strategico si fonda sugli obiettivi delineati dal Piano Strategico 2024–2026 e dal Piano Integrato di Attività e Organizzazione (PIAO) 2025–2027, integrati con le disposizioni normative e metodologiche nazionali in materia di amministrazione digitale. Pertanto, le linee strategiche definiscono un percorso di sviluppo coerente, sostenibile e orientato alla creazione di valore pubblico attraverso l'innovazione dei processi, dei servizi e delle infrastrutture digitali.

Le linee di intervento sono articolate in sei assi strategici che riflettono le principali dimensioni della trasformazione digitale:

- il potenziamento e la sostenibilità delle infrastrutture tecnologiche;
- il rafforzamento dell'interoperabilità applicativa e della cooperazione digitale;
- la governance e la valorizzazione del patrimonio informativo;
- l'evoluzione dei servizi digitali rivolti alla comunità accademica;
- la sicurezza informatica, la protezione dei dati e la continuità operativa;
- lo sviluppo delle competenze digitali e la gestione del cambiamento.

Ciascun asse strategico non rappresenta un ambito autonomo, ma parte di un modello unitario e interdipendente, in cui l'evoluzione delle componenti infrastrutturali, applicative, organizzative e competenziali concorre alla piena realizzazione degli obiettivi istituzionali dell'Ateneo. Il complesso di queste linee orientano scelte, investimenti e priorità, pur tuttavia assicurando che la trasformazione digitale proceda secondo un approccio sistemico, progressivo e allineato alle esigenze di studenti, personale, docenti e ricercatori.

5.1 Infrastrutture digitali

Le infrastrutture digitali rappresentano il fondamento tecnico su cui poggia l'intero ecosistema ICT dell'Università di Napoli L'Orientale e costituiscono il cuore della pianificazione strategica triennale. L'analisi di baseline (Capitolo 4) ha delineato un quadro infrastrutturale complessivamente solido, basato su una solida presenza on-premise con due data center fisici ridondati (presso Palazzo Giusso e Palazzo del Mediterraneo), sistemi di virtualizzazione centralizzati e un'articolata rete di connettività intersede, inclusa la rete federata Eduroam®.

L'architettura attuale si configura come un sistema complesso e stratificato che integra soluzioni interne con piattaforme SaaS erogate da partner strategici come il Consorzio CINECA (per i gestionali U-Gov e ESSE3) e i servizi in cloud derivanti dalla convenzione CRUI (Microsoft 365, Zoom). Questo modello ibrido ha garantito finora la continuità operativa; tuttavia, presenta elementi di eterogeneità architetturale, apparati disomogenei, un sistema VoIP obsoleto e l'assenza di un Piano formalizzato e testato di Continuità Operativa e Disaster Recovery.

Il triennio 2026–2028 è dedicato alla trasformazione di questa dotazione in una piattaforma tecnologica moderna, scalabile e resiliente, attraverso l'attuazione di tre assi strategici interdipendenti.

L'Ateneo intende conseguire una razionalizzazione radicale delle componenti di rete e dei sistemi virtualizzati, mirando alla standardizzazione degli apparati e all'aggiornamento tecnologico delle dorsali. L'obiettivo è ridurre la complessità e l'eterogeneità storicamente stratificata che oggi incide negativamente sui tempi di gestione e sugli oneri manutentivi. Questo percorso è indissolubilmente legato al rafforzamento degli strumenti di monitoring, auditing e logging, azioni indispensabili per potenziare la capacità di intervento proattivo e per conformarsi pienamente ai requisiti di sicurezza cibernetica definiti dalla Direttiva NIS2.

In continuità con l'uso delle piattaforme collaborative esistenti (Microsoft 365), si persegue una decisa evoluzione verso un modello operativo Cloud-First. La migrazione selettiva e progressiva di servizi non critici, l'esternalizzazione delle componenti collaborative e una maggiore integrazione tra l'identità istituzionale (Active Directory / Azure AD) e gli strumenti in cloud consentiranno di potenziare i livelli di resilienza e scalabilità, riducendo la dipendenza esclusiva dal datacenter fisico. In questa prospettiva, il cloud si consolida come componente strutturale e complementare, rendendo l'infrastruttura ibrida più robusta e sostenibile a livello nazionale ed europeo.

Il secondo asse strategico mira a mitigare i principali fattori di vulnerabilità evidenziati, ovvero l'assenza di un piano formalizzato di ripristino. Sarà sviluppato un Sistema Integrato di Continuità Operativa, fondato sulla classificazione dei servizi critici (RTO/RPO) e sulla predisposizione di un sito di Disaster Recovery, preferibilmente basato su risorse cloud per maggiore flessibilità.

In parallelo, l'assenza di un CMDB (Configuration Management Database) istituzionale, che oggi rappresenta una criticità organizzativa elevata, sarà superata con l'introduzione di un modello strutturato di gestione del ciclo di vita degli asset. Tale strumento è essenziale per supportare le attività di manutenzione, potenziare la risposta agli incidenti e garantire la piena aderenza alle prescrizioni NIS2 in materia di dependency management.

Rientra tra le priorità del triennio anche la modernizzazione delle tecnologie di comunicazione e degli spazi didattici. La telefonia VoIP in esercizio necessita di una revisione strutturale verso modelli di comunicazione unificata (unified communication). Contemporaneamente, le dotazioni multimediali di aule e laboratori saranno oggetto di un piano di rinnovamento mirato a garantire ambienti didattici accessibili, integrati e allineati ai modelli di apprendimento contemporanei.

Nel loro complesso, queste direttive delineano un percorso di trasformazione che mira a ridurre la complessità dell'ecosistema tecnico, a rafforzare la sicurezza e la resilienza operativa, a valorizzare il modello ibrido e a porre basi solide per il futuro sviluppo applicativo. Il risultato atteso è un'architettura ICT più omogenea, governabile e sostenibile, capace di accompagnare l'evoluzione digitale dell'Ateneo.

5.2 Interoperabilità e cooperazione applicativa

L'interoperabilità costituisce uno degli assi strategici fondamentali per la trasformazione digitale dell'Università di Napoli L'Orientale, poiché consente la circolazione sicura, coerente e tempestiva delle informazioni tra sistemi interni, operatori istituzionali e piattaforme nazionali. L'analisi svolta nel capitolo 4 ha evidenziato un ecosistema applicativo ampio,

articolato e in parte già integrato, ma anche la presenza di connessioni sviluppate nel tempo in modo non omogeneo, l'assenza di standard tecnici condivisi e un modello di cooperazione applicativa ancora fortemente dipendente dai fornitori esterni. Il triennio 2026–2028 rappresenta quindi la fase nella quale l'Ateneo dovrà consolidare le integrazioni esistenti, rafforzare l'allineamento agli standard nazionali e costruire un'infrastruttura applicativa fondata su regole chiare, governance stabile e qualità dei flussi informativi.

La piena adesione alla Piattaforma Digitale Nazionale Dati, completata nel 2025 con la pubblicazione degli e-service ESSE3 attraverso l'API Manager CINECA, costituisce il principale punto di partenza di questo percorso. Tale risultato dimostra la capacità dell'Ateneo di operare all'interno di un ecosistema di interoperabilità regolato e standardizzato, ma evidenzia allo stesso tempo la necessità di sviluppare competenze e processi interni più maturi per governare il ciclo di vita delle API, monitorare la qualità dei dati esposti, garantire la sicurezza delle interfacce applicative e assicurare la conformità alle politiche di audit e controllo previste dalla PDND. Nei prossimi anni, l'Ateneo dovrà quindi evolvere da una interoperabilità basata principalmente sulle funzionalità offerte dai fornitori verso una capacità interna di presidio, governo e documentazione dei servizi digitali.

Il sistema informativo d'Ateneo, articolato nelle piattaforme gestionali CINECA, nei servizi documentali e amministrativi, nei sistemi per la didattica e la ricerca e nelle applicazioni sviluppate internamente, richiede un modello più organico di integrazione. Le connessioni oggi attive, spesso realizzate per risposte puntuali alle esigenze amministrative o accademiche, mostrano efficacia operativa ma non aderiscono tutte agli standard tecnici previsti dal Modello di Interoperabilità nazionale. Nei prossimi anni, l'Università dovrà promuovere la definizione di un'architettura applicativa più uniforme, basata su protocolli documentati, formati dati coerenti, integrazioni tracciabili e politiche condivise di versioning e manutenzione. La definizione dei domini informativi e l'identificazione delle fonti dati autorevoli, come delineato nel paragrafo 4.5, costituiranno la base di questo processo, consentendo di prevenire duplicazioni, ridondanze e disallineamenti tra sistemi.

Una delle priorità strategiche del triennio riguarda inoltre il rafforzamento della cooperazione applicativa interna. L'Ateneo dovrà sviluppare un modello che favorisca la convergenza delle applicazioni interne—quali l'intranet, il sistema di ticketing, i portali dei dottorati, il simulatore tasse, la piattaforma Visiting e i servizi web istituzionali—verso standard comuni di sviluppo, sicurezza e aggiornamento. La crescita di questi servizi interni rappresenta un valore significativo in termini di innovazione, ma richiede un'organizzazione capace di guidare la loro evoluzione, evitare frammentazioni e garantire interoperabilità con i sistemi centrali senza ricorrere a soluzioni isolate.

L'interoperabilità con gli attori esterni, inclusi ministeri, enti regionali, organismi di valutazione e altri provider pubblici, rappresenta una dimensione cruciale della strategia digitale. Le integrazioni con ADISURC, CISIA, ANVUR, INPS, PagoPA e con i sistemi ministeriali dovranno essere consolidate attraverso un presidio più sistematico, valutazioni periodiche della qualità dei servizi scambiati e un allineamento continuo agli standard richiesti dai diversi organismi istituzionali. L'Ateneo dovrà inoltre rafforzare il coordinamento tecnico con CINECA, al fine di garantire un utilizzo efficiente delle piattaforme nazionali, una maggiore tempestività nell'implementazione delle evoluzioni normative e una gestione coerente delle API condivise attraverso la PDND.

Infine, la transizione verso un modello più maturo di interoperabilità richiede la definizione di una governance interna che assegni ruoli chiari, responsabilità precise e processi formalizzati per la gestione delle integrazioni applicative. La cooperazione tra il Responsabile della Transizione Digitale, il Settore Sviluppo Digitale e le strutture amministrative fornirà la base per sviluppare un modello partecipato, capace di trasformare l'eterogeneità attuale in un sistema integrato, affidabile e orientato alla qualità. Nel complesso, le linee strategiche delineate in questo paragrafo mirano a costruire un ecosistema applicativo più coerente, trasparente e sicuro, pienamente allineato alle politiche nazionali e in grado di sostenere la trasformazione digitale dell'Ateneo nel prossimo triennio.

5.3 Patrimonio informativo e qualità del dato

Il patrimonio informativo dell'Università di Napoli L'Orientale rappresenta una delle risorse più rilevanti dell'Ateneo e costituisce il presupposto indispensabile per la programmazione istituzionale, la valutazione dei risultati, la qualità dei servizi e il monitoraggio dei processi amministrativi, didattici e di ricerca. La diagnosi sviluppata nel capitolo 4 ha evidenziato un sistema ricco e articolato, alimentato da piattaforme gestionali consolidate, da sistemi ministeriali e da applicazioni interne, ma caratterizzato dall'assenza di una data governance formalizzata e da livelli non omogenei di qualità, integrazione e tracciabilità delle informazioni. Nel triennio 2026–2028 il Piano intende pertanto costruire un quadro unitario, in grado di assicurare coerenza, sicurezza e affidabilità all'intero ciclo di vita del dato.

Uno degli obiettivi principali riguarda la definizione del modello di data governance d'Ateneo, basato sull'identificazione delle fonti dati autorevoli, sulla classificazione dei domini informativi, sulla definizione di ruoli e responsabilità e sulla standardizzazione dei processi di produzione, validazione, aggiornamento e conservazione delle informazioni. Tale modello, articolato in coordinamento con il Responsabile della Transizione Digitale, il Responsabile della Protezione dei Dati e le unità del Settore Sviluppo Digitale, consentirà di superare l'attuale frammentazione e di prevenire incoerenze, duplicazioni e ridondanze che oggi incidono sulla qualità del patrimonio informativo.

La strategia si fonda inoltre sulla progressiva qualificazione del Data Warehouse, che costituisce un elemento centrale nella costruzione degli indicatori istituzionali, dei cruscotti direzionali e dei flussi di monitoraggio necessari per la governance, il Nucleo di Valutazione, il Presidio della Qualità e le attività di pianificazione. Nel triennio, l'Ateneo intende rafforzare la capacità analitica del sistema mediante un ampliamento delle basi dati integrate, il miglioramento dei processi ETL, l'introduzione di controlli automatici di coerenza e l'adozione di tecniche avanzate di business intelligence, garantendo così una maggiore tempestività e affidabilità delle informazioni utilizzate nei processi decisionali.

La cooperazione applicativa con i sistemi gestionali CINECA e con le piattaforme ministeriali rappresenta un ulteriore asse strategico. La coerenza dei flussi di carriera, dei dati di bilancio, delle informazioni sul personale, dei prodotti della ricerca e dei dataset necessari alla rendicontazione costituisce una condizione essenziale per la qualità del patrimonio informativo complessivo. L'Ateneo intende potenziare i processi di validazione, consolidare le verifiche periodiche sui dataset, armonizzare gli schemi informativi e assicurare che i dati forniti agli organismi nazionali – tra cui MUR, ANVUR, ISTAT e SISTAN – siano completi, accurati e coerenti con i requisiti metodologici e normativi.

Un ruolo crescente è svolto dall'interoperabilità con la Piattaforma Digitale Nazionale Dati. La pubblicazione degli e-service ESSE3 rappresenta il primo passo verso un sistema integrato basato su API standardizzate e flussi certificati. Nel triennio, l'Ateneo dovrà rafforzare la qualità dei dati esposti, definire procedure interne di audit, consolidare le politiche di tracciabilità e sviluppare competenze interne nella gestione del ciclo di vita delle API, riducendo il rischio di disallineamenti e garantendo la conformità agli obblighi PNRR e alle Linee Guida AgID.

Particolare attenzione sarà riservata all'introduzione di politiche strutturate di data quality. Ne fanno parte la definizione di glossari semantici, la formalizzazione di metadati standard, la riduzione delle ridondanze, l'armonizzazione delle codifiche, la tracciabilità dei flussi e l'adozione di controlli automatici a monte dei processi. Il rafforzamento delle capacità interne di analisi e reporting – inclusa la progressiva introduzione di strumenti di data analytics e visualizzazione avanzata – permetterà di valorizzare il patrimonio informativo in una prospettiva sia operativa sia strategica.

Un ulteriore obiettivo riguarda la valorizzazione dei dati per finalità di trasparenza, accountability e comunicazione istituzionale. La maggior qualità dei dataset, unita alla disponibilità di strumenti di pubblicazione e consultazione unificati, consentirà di migliorare l'accessibilità delle informazioni verso la comunità accademica e verso la società, nel rispetto della normativa sul trattamento dei dati personali e degli standard sugli open data.

Nel complesso, la strategia dedicata al patrimonio informativo mira a superare le criticità attuali e a costruire un ecosistema dati affidabile, integrato e governato in modo sistematico. La qualità del dato, lungi dall'essere un elemento meramente tecnico, assume il ruolo di vero e proprio fattore abilitante della trasformazione digitale e condiziona la capacità dell'Ateneo di programmare, valutare, decidere e innovare. La trasformazione delineata nel presente Piano pone per la prima volta la qualità del dato al centro del governo del digitale, rendendola un elemento imprescindibile della maturità istituzionale dell'Università.

5.4 Servizi digitali ed esperienza utenti

L'evoluzione dei servizi digitali rappresenta una componente centrale della trasformazione dell'Università di Napoli L'Orientale, poiché definisce la qualità dell'interazione tra l'Ateneo e la propria comunità di utenti e incide in modo diretto sull'efficienza dei processi amministrativi, sulla fruibilità dei percorsi formativi, sulla gestione delle attività di ricerca e, più in generale, sull'accessibilità dei procedimenti istituzionali. L'analisi sviluppata nel capitolo 4 ha evidenziato un ecosistema applicativo ampio e articolato, arricchito negli ultimi anni da piattaforme consolidate, soluzioni cloud e servizi sviluppati internamente, ma caratterizzato anche da disomogeneità nelle interfacce, da percorsi di accesso non sempre uniformi, da modelli comunicativi differenti e da un'offerta di servizi percepita come frammentata. Nel triennio 2026–2028, il Piano intende intervenire su tali criticità, promuovendo un modello di servizio centrato sull'utente, unitario e pienamente coerente con gli standard nazionali di design e usabilità.

L'adozione di un approccio "digital-first" costituisce il principio ispiratore della strategia. Esso comporta la revisione delle modalità di erogazione, la semplificazione dei flussi informativi, la riduzione delle interazioni fisiche con gli uffici e l'eliminazione delle duplicazioni documentali, favorendo l'accesso digitale come canale primario per la fruizione dei servizi. In questa prospettiva, la piattaforma ESSE3, MyUniOr, PagoPA, i portali dei dottorati, il simulatore tasse, il sistema di Help Desk e i servizi del CLAOR costituiscono i pilastri su cui costruire un'esperienza più coerente, integrata e trasparente per gli studenti, che rappresentano la componente maggioritaria dell'utenza. Il triennio prevede azioni volte a semplificare i

percorsi, migliorare la tempestività dell'informazione, uniformare il linguaggio digitale e rafforzare la coerenza tra le diverse interfacce, contribuendo a un modello di servizio più intuitivo e orientato alle esigenze reali degli utenti.

Parallelamente, il Piano riconosce l'importanza crescente dei servizi digitali rivolti ai docenti e ai ricercatori, che svolgono un ruolo essenziale nei processi di produzione scientifica, nella gestione della didattica e nella partecipazione ai progetti internazionali. La piena integrazione tra UniFIND e IRIS/UNORA, i servizi per l'open access, le piattaforme per attività seminariali e telematiche, gli strumenti di ricerca lessicografica e i servizi dedicati ai visiting rappresentano ambiti nei quali l'Ateneo dovrà consolidare la coerenza dei flussi, ridurre la frammentazione delle interfacce e favorire un'esperienza d'uso più fluida e omogenea. La valorizzazione dei servizi digitali dedicati alla ricerca, incluse le applicazioni della sezione Digital Humanities del Centro BIMA, costituisce un ulteriore elemento strategico che il Piano intende integrare in una visione unitaria.

Per il personale tecnico-amministrativo, i servizi digitali rappresentano un fattore abilitante per l'efficienza interna e per la qualità dei processi. La combinazione tra l'intranet, i moduli U-Gov, Titulus, il Portale Amministrazione Trasparente, PICA, i workflow digitali interni e il sistema di ticketing dell'Area Infrastrutture Edilizie e Digitali consente di digitalizzare una parte significativa delle attività amministrative. Nel triennio sarà necessario consolidare tali strumenti, uniformare i modelli procedurali, ridurre le disomogeneità tra uffici e rafforzare i processi di tracciabilità, controllo delle versioni e gestione digitale dei procedimenti, contribuendo in modo significativo alla semplificazione amministrativa prevista dal PIAO.

Una componente trasversale della strategia riguarda il miglioramento dell'esperienza utente attraverso l'applicazione delle Linee Guida AgID in materia di design dei servizi digitali, accessibilità, usabilità e linguaggio chiaro. La revisione dei contenuti, la standardizzazione delle interfacce, la cura della comunicazione digitale, la verifica periodica dell'accessibilità dei portali e la misurazione della soddisfazione degli utenti costituiscono elementi essenziali per garantire servizi equi, inclusivi e pienamente conformi alla normativa vigente. L'Ateneo intende promuovere una cultura del servizio digitale che ponga l'utente al centro, superando la frammentazione storica e favorendo un approccio sistemico alla progettazione, gestione e valutazione dei servizi.

Nel complesso, la linea strategica dedicata ai servizi digitali e all'esperienza utente mira a costruire un ecosistema di servizi più semplice, integrato, accessibile e orientato alle esigenze delle persone. La qualità dell'esperienza utente diviene così un elemento strutturale del governo del digitale e uno dei principali indicatori della maturità dell'Ateneo, contribuendo al miglioramento complessivo dell'efficacia amministrativa, della qualità della didattica e del supporto alla ricerca. Il triennio 2026–2028 costituisce dunque una fase cruciale per rafforzare la coerenza, la chiarezza e la fruibilità dei servizi digitali, consolidando un modello di servizio moderno e pienamente in linea con gli standard nazionali.

5.5 Cybersecurity, privacy e continuità operativa

La sicurezza informatica, la tutela dei dati personali e la continuità operativa costituiscono l'asse strategico imprescindibile per l'Università di Napoli L'Orientale, configurandosi come la condizione sine qua non per garantire la stabilità dei servizi, la protezione del patrimonio informativo e la piena affidabilità dei processi. Muovendo dall'analisi di baseline che ha rilevato una maturità non omogenea e una storica frammentazione, il presente Piano definisce un impianto strategico orientato alla costruzione di un modello di resilienza integrato, capace di prevenire, gestire e mitigare i rischi in un quadro di costante evoluzione normativa. La cornice di riferimento è dettata dalla Direttiva NIS2, dalle prescrizioni dell'Agenzia per la

Cybersicurezza Nazionale (ACN), dal Regolamento GDPR e dagli indirizzi di AgID, la cui convergenza impone un approccio sistemico fondato sulla gestione del rischio e sulla protezione multilivello.

La governance è garantita dalla cooperazione strutturata tra il Responsabile della Transizione Digitale (RTD), il Responsabile della Protezione dei Dati (RPD) e il Settore Sviluppo Digitale, una sinergia indispensabile per assicurare la coerenza tra le misure tecniche, la tutela giuridica del dato e l'architettura dei sistemi. Il cardine di tale strategia è rappresentato dalla gestione del rischio, che richiede la classificazione dei servizi e dei dati secondo livelli di criticità, la valutazione delle minacce e l'individuazione di misure di mitigazione proporzionate, in piena conformità ai modelli proposti da ACN. Queste attività di risk assessment sono integrate da procedure di incident response, dedicate alla gestione tempestiva degli eventi avversi, all'analisi forense e alla notifica obbligatoria al RPD in caso di data breach, garantendo la massima accountability.

Dal punto di vista tecnologico, la strategia potenzia i presìdi in essere – firewalling, segmentazione della rete, protezione degli endpoint – evolvendo verso l'adozione di strumenti avanzati di monitoraggio continuo (logging e auditing) degli eventi critici, essenziali per la correlazione e la rilevazione precoce delle anomalie. La crescente complessità delle minacce cyber impone, infatti, un percorso di progressivo consolidamento del controllo centralizzato e della capacità di risposta, pienamente coerente con i requisiti di prontezza operativa di NIS2.

A integrazione della sicurezza attiva, la continuità operativa si configura come elemento prioritario. Nonostante la base resiliente dei due data center fisici, l'assenza di un piano strutturato e testato di disaster recovery rappresenta una criticità da sanare con urgenza. Il Piano definisce la necessità di formalizzare il modello di continuità, stabilendo i livelli di servizio attesi (RTO e RPO) per i servizi critici e predisponendo un sito di ripristino, preferibilmente in ambiente cloud, le cui procedure saranno validate attraverso esercitazioni periodiche per verificarne l'efficacia e l'allineamento.

La protezione dei dati personali si sviluppa come un asse trasversale e proattivo, promuovendo l'applicazione sistematica dei principi di privacy by design e by default nella progettazione di ogni nuovo applicativo o servizio digitale. Ciò si concretizza nella redazione delle valutazioni d'impatto (DPIA) per i trattamenti ad alto rischio, nell'aggiornamento costante dei registri e nel rafforzamento dei processi di controllo sui trattamenti. L'interazione costante tra RTD e RPD è vitale per garantire che le misure tecniche e organizzative siano sempre allineate alla normativa e alla tutela dei diritti degli interessati.

Infine, la difesa dell'ecosistema digitale non può prescindere dal fattore umano. La sicurezza non è affidata esclusivamente ai sistemi tecnologici, ma richiede un coinvolgimento consapevole dell'intera comunità. Il Piano prevede percorsi formativi strutturati e campagne periodiche di sensibilizzazione rivolte a tutto il personale, finalizzate a consolidare comportamenti sicuri e a promuovere una cultura digitale orientata alla responsabilità individuale e collettiva.

Nel suo complesso, la strategia qui delineata costruisce un sistema di protezione integrato, dinamico e pienamente conforme agli standard nazionali ed europei, elevando la sicurezza da mero requisito tecnico a elemento costitutivo della governance e garanzia fondamentale per la realizzazione della strategia di trasformazione digitale dell'Ateneo.

5.6 Competenze digitali e change management

La trasformazione digitale dell'Università di Napoli L'Orientale non può realizzarsi in modo efficace senza un parallelo investimento nelle competenze digitali e nella capacità dell'organizzazione di governare il cambiamento. Le innovazioni tecnologiche introdotte negli ultimi anni e quelle programmate nel triennio 2026–2028 richiedono, infatti, un'evoluzione culturale e professionale che coinvolga l'intera comunità accademica, ponendo al centro il capitale umano come elemento abilitante della strategia digitale. L'analisi condotta nel capitolo 4 ha evidenziato la presenza di competenze diffuse ma non omogenee, differenze rilevanti nei livelli di alfabetizzazione digitale, una conoscenza discontinua dei sistemi informativi e la necessità di rafforzare le capacità operative legate ai processi digitali, alla protezione dei dati personali e alla sicurezza informatica.

In questo contesto, il Piano adotta un approccio sistematico fondato sui modelli europei DigComp e DigCompOrg, sulle Linee Guida AgID e sulle previsioni del PIAO 2025–2027 relative alla formazione e allo sviluppo del personale. La strategia mira a sostenere la crescita graduale delle competenze digitali, differenziando gli interventi in relazione ai ruoli, alle responsabilità e ai processi gestiti da personale tecnico-amministrativo, docenti, ricercatori e figure di governo. Il rafforzamento delle competenze non è concepito come attività una tantum, ma come un processo continuativo, integrato nella programmazione del personale e nel ciclo di miglioramento dell'Ateneo.

Per il personale tecnico-amministrativo, il Piano prevede percorsi formativi orientati all'utilizzo avanzato dei sistemi gestionali, delle piattaforme collaborative, dei workflow documentali digitali e dei servizi offerti dal Settore Sviluppo Digitale. Particolare attenzione è dedicata alle competenze necessarie per garantire la qualità del dato, la protezione delle informazioni, la gestione dei trattamenti ai sensi del GDPR e la comprensione dei modelli di interoperabilità introdotti dalla PDND e dagli standard nazionali. L'obiettivo è aumentare la capacità degli uffici di operare in modo coerente con processi digitalizzati end-to-end, ridurre gli errori operativi e migliorare la qualità complessiva dei procedimenti amministrativi.

Per docenti e ricercatori, il Piano promuove lo sviluppo di competenze legate alla didattica digitale, alla produzione e gestione della ricerca attraverso le piattaforme IRIS/UNORA e UniFIND, all'utilizzo di strumenti di analisi e valorizzazione scientifica e all'adozione di pratiche digitali orientate alla trasparenza, all'impatto e alla condivisione dei risultati. La formazione dedicata a questo segmento dell'utenza assume un ruolo strategico per migliorare la fruibilità dei servizi accademici, per semplificare i flussi operativi e per sostenere la qualità dell'offerta didattica in un contesto sempre più digitale e internazionale.

La gestione del cambiamento costituisce un elemento essenziale della strategia. La trasformazione digitale richiede infatti l'allineamento tra processi, tecnologie e comportamenti organizzativi. Il Piano promuove un modello di change management basato sulla partecipazione attiva delle strutture, sulla comunicazione trasparente delle innovazioni introdotte, sul coinvolgimento progressivo degli utenti e sul supporto operativo costante nelle fasi di transizione. Tali attività sono integrate con la governance ICT e con i processi di programmazione del personale, in modo da garantire che l'evoluzione dei sistemi sia accompagnata da una chiara comprensione delle responsabilità e dei benefici attesi.

Un ruolo trasversale è svolto dalla sensibilizzazione alla sicurezza informatica e alla protezione dei dati personali. La crescita delle minacce cyber e l'applicazione delle normative europee richiedono un elevato livello di consapevolezza individuale. Il Piano prevede iniziative strutturate di formazione su phishing, social engineering, gestione delle credenziali,

corretto utilizzo dei dispositivi e adozione di comportamenti responsabili. Queste attività, coordinate tra RTD, RPD e Settore Sviluppo Digitale, contribuiscono a creare una cultura diffusa della sicurezza, essenziale per prevenire incidenti e garantire la tutela del patrimonio informativo.

Nel complesso, la linea strategica dedicata alle competenze digitali e al change management mira a trasformare il capitale umano in un elemento di forza dell'Ateneo, capace di sostenere l'innovazione, migliorare l'efficacia dei servizi e consolidare una cultura organizzativa orientata alla collaborazione, alla responsabilità e al miglioramento continuo. L'investimento nelle competenze costituisce così una delle leve principali per accompagnare la trasformazione delineata dal presente Piano e per garantirne la piena sostenibilità nel lungo periodo.

5.7 Innovazione tecnologica e intelligenza artificiale

L'innovazione tecnologica e l'adozione responsabile dell'intelligenza artificiale (IA) rappresentano un asse strategico della trasformazione digitale dell'Università di Napoli L'Orientale, in coerenza con il quadro normativo nazionale ed europeo e con le linee di indirizzo definite dal Decalogo AgID per l'IA nella Pubblica Amministrazione. L'Ateneo intende promuovere un uso dell'IA che sia etico, trasparente, affidabile e pienamente conforme alle prescrizioni dell'AI Act, del GDPR, delle Linee Guida AgID e delle misure di sicurezza previste dalla Direttiva NIS2.

In questa prospettiva, il presente documento riconosce l'innovazione come un processo culturale, organizzativo e metodologico, fondato sulla capacità dell'Ateneo di costruire modelli, servizi e processi che valorizzino il patrimonio informativo, migliorino l'efficienza amministrativa e supportino la qualità della didattica, della ricerca e delle attività istituzionali. L'adozione dell'IA sebbene in forte crescita esponenziale sia nell'uso quotidiano che in quello enterprise deve discendere da un percorso progressivo e controllato, basato su sperimentazioni misurabili, valutazioni di impatto e analisi concrete dei benefici e dei rischi.

In ambito amministrativo, il Piano promuove l'utilizzo di strumenti di automazione intelligente dei processi (IPA/RPA), sistemi di classificazione documentale assistita, categorizzazione semantica dei contenuti, supporto alle attività di front-office, rilevazione automatica delle anomalie nei flussi di dati e strumenti di analisi predittiva utili alla programmazione, al monitoraggio degli indicatori istituzionali e alla semplificazione dei procedimenti. Tali applicazioni sono sviluppate con un approccio human-in-the-loop, che garantisce il controllo umano nelle fasi critiche, assicurando trasparenza, verificabilità delle decisioni e rispetto delle responsabilità amministrative.

In ambito didattico e scientifico, il Piano sostiene l'utilizzo dell'IA per migliorare l'accessibilità dei contenuti, supportare la didattica digitale, offrire strumenti avanzati per l'analisi linguistica e documentale, potenziare le attività di ricerca nelle Digital Humanities e valorizzare i dati provenienti dalla produzione scientifica. L'integrazione tra IA e i sistemi istituzionali consente di ampliare le possibilità di studio, sperimentazione e disseminazione dei risultati, rafforzando la capacità dell'Ateneo di partecipare a progetti nazionali e internazionali sul tema.

Per garantire un utilizzo responsabile dell'IA, il Piano si allinea perfettamente con quello che è il mandato affidato al gruppo di lavoro individuato dalla governance di Ateneo ed incaricato di elaborare le Linee Guida per l'uso dell'IA generativa. Tale quadro include la definizione di criteri di valutazione dei rischi, linee guida per la selezione delle soluzioni, modalità di verifica degli algoritmi, requisiti di trasparenza verso gli utenti e procedure per gestire correttamente i trattamenti di dati

personali. In questa prospettiva, il coordinamento tra RTD, RPD, Settore Sviluppo Digitale, Presidio della Qualità e strutture accademiche costituisce un elemento essenziale per integrare la dimensione tecnologica con quella etica e giuridica.

La strategia prevede inoltre lo sviluppo di una cultura dell'innovazione diffusa, sostenuta da iniziative di formazione, sensibilizzazione e sperimentazione, che favoriscano l'adozione consapevole delle tecnologie emergenti e la capacità delle strutture di valutare criticamente le opportunità offerte dall'IA. Particolare attenzione è dedicata alla protezione dei dati personali, alla sicurezza degli algoritmi, alla gestione dei bias e alla verifica degli impatti sulle attività istituzionali, in modo da evitare rischi di non conformità o utilizzi inappropriati delle tecnologie.

Nel complesso, la linea strategica dedicata all'innovazione tecnologica e all'intelligenza artificiale mira a costruire un modello di sviluppo sostenibile, rigoroso e orientato al miglioramento dei servizi, valorizzando il patrimonio informativo e promuovendo soluzioni che rafforzino la qualità dei processi decisionali, didattici e scientifici. L'Ateneo intende adottare un approccio all'IA che sia al tempo stesso ambizioso e prudente, capace di coniugare innovazione, etica, sicurezza e piena conformità normativa, ponendo le basi per una crescita digitale matura e responsabile nel triennio 2026–2028.

PARTE IV – PIANO ATTUATIVO

6. Piano attuativo: Infrastrutture e cloud

L'efficacia dei servizi digitali dell'Università di Napoli L'Orientale si fonda su un'infrastruttura ICT capace di garantire disponibilità, continuità operativa, sicurezza e scalabilità. Negli ultimi anni l'Ateneo ha avviato un percorso di modernizzazione tecnologica orientato all'adozione di architetture ibride, nelle quali le componenti on-premise – datacenter, rete, sicurezza perimetrale, sistemi di virtualizzazione e storage – si integrano con soluzioni cloud e servizi SaaS erogati da partner istituzionali, in particolare il Consorzio CINECA.

Il modello adottato si ispira ai principi tecnico-normativi stabiliti dalle Linee Guida AgID, dal Piano Triennale per l'Informatica nella PA e dalle prescrizioni dell'Agenzia per la Cybersicurezza Nazionale, privilegiando un approccio cloud-first, sicurezza by-design, gestione centralizzata delle identità digitali e piena interoperabilità con le piattaforme nazionali. La progressiva evoluzione verso un'infrastruttura ibrida consente di distribuire i carichi di lavoro in modo efficiente, migliorare i livelli di servizio, ridurre la dipendenza dall'hardware locale e facilitare l'adozione di modelli organizzativi più flessibili.

Nel triennio 2026–2028 l'Ateneo concentrerà la propria azione su quattro direttrici principali:

- il rafforzamento dell'affidabilità delle server farm e della rete di Ateneo, anche attraverso interventi mirati di rilocalizzazione dei sistemi e di ridondanza della connettività;
- l'evoluzione del modello cloud ibrido, con la progressiva migrazione dei servizi compatibili verso soluzioni scalabili e ad elevati standard di sicurezza;
- il consolidamento delle misure di cybersicurezza, in linea con le prescrizioni della direttiva NIS2, del quadro nazionale ACN e con gli standard di continuità operativa previsti dalla normativa vigente.
- La verifica delle possibilità di acquisizione di strumentazioni atte all'adozione graduale di strumentazioni e piattaforme di intelligenza artificiale per il miglioramento dei tutte le attività interne ed esterne per sviluppi futuri;

L'intero impianto infrastrutturale costituisce il fondamento tecnologico necessario per sostenere lo sviluppo dei servizi digitali, la qualità dell'esperienza dell'utenza e la piena attuazione della strategia di trasformazione digitale dell'Università, assicurando che l'Ateneo possa operare in modo resiliente, sicuro e conforme agli standard nazionali ed europei.

6.1 Infrastrutture e cloud - Azioni 2026-2028

Nel triennio 2026–2028 l'Università di Napoli L'Orientale attuerà un programma organico di evoluzione delle infrastrutture ICT e del modello cloud, con l'obiettivo di consolidare la resilienza del sistema informativo, superare le eterogeneità accumulate nel tempo e allinearsi agli standard nazionali di sicurezza, interoperabilità e continuità operativa. Le azioni previste mirano a trasformare l'attuale architettura in una piattaforma più coerente, scalabile e sostenibile, in grado di supportare efficacemente l'espansione dei servizi digitali e le esigenze della comunità universitaria.

Le attività riguardano cinque ambiti prioritari: la modernizzazione dei datacenter, l'evoluzione delle infrastrutture di rete, lo sviluppo del modello cloud ibrido, il rafforzamento della sicurezza infrastrutturale e la standardizzazione delle postazioni e delle dotazioni periferiche.

Modernizzazione dei datacenter e consolidamento dell'infrastruttura on-premise

L'Ateneo avvierà un processo di aggiornamento progressivo delle componenti critiche dei datacenter di Palazzo Giusso e Palazzo del Mediterraneo, adeguando climatizzazione, sistemi UPS, apparati di rete e cluster di virtualizzazione. Tale intervento intende superare le attuali disomogeneità, incrementare il livello di ridondanza e assicurare un'infrastruttura pienamente rispondente agli standard di sicurezza ACN e ai requisiti di continuità previsti dalla normativa NIS2. Il Piano prevede inoltre la definizione di un modello strutturato di monitoraggio delle prestazioni, delle soglie di capacità e dei log di sicurezza, con una supervisione centralizzata del ciclo di vita delle macchine virtuali e dei servizi ospitati.

Evoluzione della rete di Ateneo e adeguamento delle dorsali

Le azioni programmate includono la progressiva sostituzione degli apparati di switching obsoleti, la segmentazione avanzata della rete per ambiti funzionali e l'introduzione di sistemi evoluti di gestione dei flussi, in modo da migliorare l'affidabilità, ridurre la superficie di vulnerabilità e assicurare prestazioni adeguate alle esigenze didattiche e scientifiche. È prevista inoltre la ridondanza delle dorsali GARR e l'introduzione di strumenti di diagnostica proattiva, necessari per garantire continuità di servizio e interventi preventivi in caso di criticità infrastrutturali.

Sviluppo del modello cloud ibrido e integrazione con i servizi SaaS

Il Piano promuove un'evoluzione verso un modello cloud ibrido, con una crescita controllata delle componenti esternalizzate e un forte presidio sulle architetture tecniche, sui livelli di sicurezza e sulle integrazioni applicative. L'Ateneo intende consolidare l'utilizzo dei servizi Microsoft 365 e Azure tramite la convenzione CRUI, ottimizzando la gestione delle identità, dei gruppi, delle policy di sicurezza e degli strumenti di collaborazione. Parallelamente, verranno introdotti criteri formali per valutare la migrazione a piattaforme cloud dei servizi non critici o ad alta variabilità, garantendo un equilibrio tra efficienza, sostenibilità economica e sovranità del dato.

Rafforzamento della sicurezza infrastrutturale

In coerenza con il Piano strategico e con i requisiti NIS2, saranno adottate misure per il potenziamento della sicurezza dei sistemi, con particolare attenzione all'aggiornamento dei firewall di nuova generazione, alla gestione centralizzata dei log, all'implementazione di sistemi IDS/IPS e all'introduzione di strumenti avanzati di endpoint protection. Il Piano prevede inoltre la definizione di un programma di test periodici di continuità operativa e disaster recovery, con una revisione strutturata dei piani CO/DR e la verifica del ripristino dei servizi critici.

Standardizzazione delle postazioni di lavoro e delle dotazioni periferiche

Nel triennio 2026–2028 saranno uniformate le postazioni di lavoro del personale tecnico-amministrativo e dei docenti, adottando modelli omogenei di configurazione, criteri di sicurezza comuni e strumenti di gestione centralizzata degli aggiornamenti, delle licenze e delle applicazioni. Particolare attenzione sarà dedicata alle dotazioni delle aule didattiche, dei laboratori e delle sale multimediali, con interventi di ammodernamento programmati e la definizione di standard tecnici minimi a cui uniformare le future acquisizioni.

6.2 Infrastrutture e cloud - Pre-requisiti

L'attuazione delle azioni previste nel dominio "Infrastrutture e cloud" richiede un insieme di condizioni abilitanti di natura organizzativa, tecnica, economica e procedurale, senza le quali il percorso di evoluzione definito nel presente Piano non potrebbe essere realizzato in modo efficace, sostenibile o conforme agli standard nazionali di sicurezza e interoperabilità. Tali pre-requisiti rappresentano quindi un elemento strutturale del Piano attuativo e costituiscono il quadro di riferimento entro cui collocare gli interventi programmati per il triennio 2026–2028.

Un primo requisito riguarda la piena operatività del modello di governance ICT, con particolare riferimento al ruolo del Responsabile per la Transizione Digitale (RTD), alla collaborazione con il Settore Sviluppo Digitale e alla funzionalità della Centrale di Committenza ICT. L'efficacia delle azioni infrastrutturali dipende dalla capacità di assicurare una valutazione tecnica uniforme, una programmazione coordinata degli investimenti e un presidio costante sulle scelte architetturali. L'assenza di un governo unitario rappresenterebbe una criticità rilevante, poiché rischierebbe di riprodurre logiche frammentate e soluzioni non interoperabili.

Un secondo pre-requisito fondamentale è rappresentato dalla disponibilità di un quadro economico dedicato e pluriennale. L'ammodernamento dei datacenter, la sostituzione degli apparati di rete, la ridondanza delle dorsali, l'evoluzione dei cluster di virtualizzazione e la migrazione progressiva verso architetture cloud ibride costituiscono investimenti significativi che richiedono continuità finanziaria e un piano di allocazione delle risorse coordinato con la programmazione triennale del budget ICT. La mancanza di una prospettiva finanziaria stabile comprometterebbe la sostenibilità delle azioni previste e ridurrebbe la capacità dell'Ateneo di mantenere livelli adeguati di servizio e sicurezza.

Un ulteriore pre-requisito è la definizione di un modello di gestione del rischio e di classificazione dei servizi, in coerenza con i requisiti della Direttiva NIS2 e con le indicazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN). La progettazione delle infrastrutture, la definizione delle priorità di intervento e le scelte di migrazione verso il cloud devono basarsi su criteri strutturati di criticità, valore degli asset e livelli di esposizione alle minacce cyber. L'assenza di questo modello determinerebbe scelte tecnologiche non allineate alla reale priorità dei servizi e aumenterebbe il livello di rischio operativo.

Ai fini dell'attuazione degli interventi, si rende necessaria anche la disponibilità di un inventario aggiornato delle componenti infrastrutturali, dei sistemi e delle configurazioni, attraverso una Configuration Management Database (CMDB) formalizzata e costantemente mantenuta. Senza un quadro completo e aggiornato degli asset, risulterebbe difficoltoso pianificare gli interventi, valutare gli impatti delle sostituzioni, stimare correttamente i costi e definire standard di sicurezza coerenti.

Sul versante procedurale, è indispensabile la piena integrazione tra le attività tecniche e i processi amministrativi gestiti dalla Centrale di Committenza ICT e dal Provveditorato. L'attuazione delle azioni infrastrutturali richiede capitolati tecnici uniformi, pareri tempestivi, procedure di gara coerenti con il Codice dei Contratti Pubblici e tempistiche compatibili con i cicli di sostituzione programmata. Un disallineamento tra competenze tecniche e attività amministrative potrebbe rallentare o compromettere l'attuazione degli interventi.

Infine, un pre-requisito trasversale riguarda la disponibilità di competenze interne adeguate e aggiornate nelle aree dell'infrastruttura, del cloud, della sicurezza e della gestione dei sistemi. L'evoluzione tecnologica delineata nel Piano richiede un livello di competenze specialistiche che non può essere dato per scontato e che deve essere sostenuto da percorsi strutturati di formazione e aggiornamento continuo, coordinati con il Piano Triennale dei Fabbisogni di Personale e con il PIAO.

Nel loro insieme, questi pre-requisiti costituiscono la condizione necessaria per garantire l'efficacia, la sicurezza e la sostenibilità degli interventi previsti nel dominio delle infrastrutture e del cloud, assicurando che la trasformazione tecnologica dell'Ateneo possa svilupparsi su basi solide, coerenti e pienamente conformi al quadro normativo vigente.

6.3 Infrastrutture e cloud – Risorse

L'attuazione delle azioni infrastrutturali previste nel triennio 2026–2028 richiede un insieme articolato di risorse tecniche, economiche, organizzative e professionali, la cui disponibilità rappresenta un fattore determinante per la piena realizzazione degli interventi programmati. La solidità di tale quadro di risorse costituisce un elemento essenziale per garantire continuità, sostenibilità e coerenza nell'evoluzione del sistema informativo di Ateneo.

Dal punto di vista economico, il Piano necessita di una programmazione pluriennale delle spese ICT, coordinata con il budget d'Ateneo e con la Centrale di Committenza ICT. Gli interventi di ammodernamento dei datacenter, l'evoluzione degli apparati di rete, la ridondanza delle dorsali, l'adozione di sistemi avanzati di sicurezza, l'aggiornamento dei cluster di virtualizzazione e l'ampliamento dei servizi cloud costituiscono investimenti non comprimibili, che richiedono una pianificazione strutturata dei costi e una distribuzione equilibrata nel triennio. A ciò si aggiungono gli oneri ricorrenti per licenze, rinnovi contrattuali, manutenzione evolutiva e servizi SaaS, che richiedono un monitoraggio costante e un approccio di sostenibilità economica fondato sulla razionalizzazione delle piattaforme esistenti.

Accanto alle risorse finanziarie, assume rilievo la disponibilità di risorse professionali adeguate alle responsabilità e alle competenze richieste. Il Settore Sviluppo Digitale necessita del consolidamento delle figure tecniche dedicate alle infrastrutture, alla sicurezza, alle reti, alla virtualizzazione, alla gestione cloud e al monitoraggio dei servizi, in coerenza con i fabbisogni rilevati nel PIAO e con il Piano dei Fabbisogni di Personale. La complessità degli interventi programmati richiede infatti un presidio interno stabile, capace di garantire competenze verticali e continuità operativa. L'assenza di risorse adeguate rischierebbe di compromettere la sostenibilità degli interventi e di aumentare la dipendenza da fornitori esterni.

Sul versante organizzativo, è necessario un coordinamento strutturato tra il Settore Sviluppo Digitale, la Centrale di Committenza ICT, il Provveditorato e le altre strutture tecniche coinvolte. L'efficacia delle azioni infrastrutturali dipende dalla capacità di garantire valutazioni tecniche tempestive, uniformità dei capitolati, gestione coordinata delle procedure di acquisto, monitoraggio dei livelli di servizio e controllo dei contratti in essere. Un disallineamento tra le aree tecniche e amministrative potrebbe determinare ritardi, duplicazioni o inefficienze, incidendo sulla calendarizzazione degli interventi e sulla coerenza architetturale complessiva.

Dal punto di vista tecnico, la realizzazione del Piano richiede la disponibilità di strumenti adeguati per il monitoraggio dei sistemi, la gestione dei log, la supervisione degli apparati e l'orchestrazione delle infrastrutture ibride. Sono necessari

inoltre strumenti di gestione degli endpoint, piattaforme di virtualizzazione aggiornate, sistemi di backup idonei alle politiche di retention previste e soluzioni avanzate di analisi dei flussi di rete. L'adozione di tali strumenti deve essere accompagnata da una razionalizzazione dei software già presenti e da una valutazione accurata delle possibili integrazioni.

Infine, la realizzazione degli interventi richiede un quadro di supporto contrattuale adeguato, comprensivo di accordi di assistenza tecnica, formule di manutenzione evolutiva, strumenti di supporto specialistico e SLA coerenti con la criticità dei servizi erogati. La definizione di contratti chiari, misurabili e controllabili costituisce un elemento imprescindibile per assicurare qualità e continuità operativa.

Nel complesso, le risorse necessarie per il dominio delle infrastrutture e del cloud devono essere considerate in una prospettiva integrata: economica, professionale, tecnica e organizzativa. Solo la combinazione equilibrata di tali fattori consente di garantire l'attuazione delle azioni previste, la sicurezza dei servizi, la continuità operativa e la sostenibilità delle scelte tecnologiche dell'Ateneo nel medio periodo.

6.4 Infrastrutture e cloud – KPI

Il monitoraggio dell'evoluzione infrastrutturale nel triennio 2026–2028 si fonda su un insieme di indicatori quantitativi e qualitativi che misurano l'affidabilità delle componenti on-premise, la maturità del modello cloud, il livello di sicurezza infrastrutturale, l'efficienza delle reti e la capacità dell'Ateneo di garantire continuità operativa. I KPI individuati rispondono alle linee guida AgID, agli standard ACN e alle prescrizioni della Direttiva NIS2, e sono stati selezionati in coerenza con la dimensione organizzativa dell'Ateneo e con la sostenibilità delle attività di monitoraggio.

KPI1 - Copertura dei servizi con sistemi di backup conformi alle policy CO/DR

Definizione: % dei servizi coperti da backup validati e ripristinabili.

Target 2028: ≥ 95%.

KPI2 - Standardizzazione delle postazioni di lavoro

Definizione: % del personale docenti dotato di strumentazioni uniformate.

Target 2028: ≥ 85%.

7. Piano attuativo: Interoperabilità e dati

L'interoperabilità e la gestione del patrimonio informativo rappresentano una componente fondamentale della strategia digitale dell'Università di Napoli L'Orientale e costituiscono un prerequisito essenziale per l'efficienza dei processi, la qualità dei servizi e la creazione di valore pubblico. L'evoluzione dell'ecosistema digitale dell'Ateneo, caratterizzato dall'integrazione tra infrastrutture on-premise, piattaforme cloud e soluzioni SaaS, rende necessario adottare un modello di cooperazione applicativa in grado di garantire coerenza, continuità, sicurezza e integrità dei flussi informativi.

In linea con il quadro normativo nazionale ed europeo, l'Ateneo orienta la propria azione ai principi del Codice dell'Amministrazione Digitale, del Piano Triennale per l'Informatica nella PA e delle politiche di interoperabilità definite dall'Agenzia per l'Italia Digitale, ponendo particolare attenzione ai modelli di interoperabilità semantica e tecnica, all'utilizzo di formati aperti e alla progressiva integrazione con le piattaforme nazionali abilitanti (SPID, CIE, PagoPA, PDND, AppIO).

Tale impostazione consente di assicurare la coerenza dei flussi documentali e amministrativi, la qualità dei dati e la piena integrazione delle informazioni provenienti dai sistemi gestionali, didattici e di ricerca.

La gestione del patrimonio informativo pubblico assume in questo contesto un ruolo strategico, non soltanto come insieme di dati detenuti dall'Ateneo, ma come risorsa condivisa e valorizzabile attraverso modelli di data governance orientati alla qualità, alla sicurezza e all'interoperabilità. Il processo di consolidamento dei sistemi informativi – tra cui le piattaforme CINECA, i sistemi di gestione documentale, i portali tematici e le soluzioni sviluppate internamente dal Settore Sviluppo Digitale – richiede un approccio unitario alla definizione delle politiche di accesso, alla classificazione dei dati, ai processi di integrazione applicativa e alla protezione delle informazioni.

Il presente capitolo definisce quindi il quadro di riferimento dell'interoperabilità applicativa dell'Ateneo e illustra le linee di sviluppo della data governance, ponendo al centro il principio secondo cui la qualità del dato e la capacità dei sistemi di dialogare in modo efficace costituiscono elementi determinanti per il miglioramento dei servizi, la semplificazione dei procedimenti e il pieno soddisfacimento degli standard AVA3 relativi alla gestione delle informazioni e della conoscenza.

7.1 Interoperabilità e dati - Azioni 2026-2028

Nel triennio 2026–2028 l'Università di Napoli L'Orientale attuerà un insieme coordinato di interventi finalizzati a rafforzare l'interoperabilità dei sistemi informativi, consolidare le integrazioni applicative, definire un modello maturo di data governance e garantire la qualità del patrimonio informativo istituzionale. Le azioni previste rispondono alle prescrizioni nazionali in materia di interoperabilità (Modello di Interoperabilità – ModI, PDND, SPID/CIE, PagoPA), ai requisiti di sicurezza e tracciabilità introdotti dalla Direttiva NIS2 e alle esigenze di semplificazione e integrazione dei processi amministrativi, didattici e scientifici.

L'Ateneo, che negli anni ha sviluppato un ecosistema applicativo ampio ma non pienamente integrato, si impegna a superare le attuali eterogeneità attraverso un percorso strutturato e progressivo, basato su standard comuni, definizioni condivise, responsabilità chiare e una visione unitaria del patrimonio informativo. Le azioni programmate si articolano lungo quattro direttrici principali: consolidamento dell'interoperabilità applicativa, definizione della data governance, potenziamento dei flussi informativi e integrazione con la PDND.

Consolidamento dell'interoperabilità applicativa e introduzione di standard comuni

Il Piano prevede la razionalizzazione delle integrazioni esistenti e la progressiva adozione di protocolli, modelli di dati e API conformi agli standard del ModI nazionale. Saranno mappati i flussi applicativi tra ESSE3, U-Gov, Titulus, IRIS/UNORA, UniFIND, OrienTales, PICA e i servizi digitali interni, con l'obiettivo di eliminare ridondanze, incoerenze semantiche e dipendenze non documentate. Verranno introdotti standard tecnici e linee guida per la realizzazione di nuove integrazioni, al fine di garantire uniformità, sicurezza e sostenibilità nell'evoluzione delle piattaforme.

Sviluppo del modello di data governance e definizione dei domini informativi

Un intervento prioritario riguarda la formalizzazione del modello di governo dei dati, attraverso l'identificazione delle fonti dati autorevoli, la definizione dei domini informativi (studenti, personale, ricerca, didattica, finanza, patrimonio, servizi digitali), la nomina dei responsabili del dato e la documentazione delle regole di qualità, aggiornamento e validazione.

Tale modello, sviluppato in coerenza con le Linee Guida AgID e con le esigenze di compliance GDPR, costituisce la base per garantire coerenza, tracciabilità e integrità nel ciclo di vita del patrimonio informativo.

Potenziamento dei flussi informativi istituzionali e ottimizzazione dei processi

Le azioni programmate prevedono la revisione dei flussi critici relativi alle carriere studentesche, alla produzione scientifica, alla gestione del personale, alla contabilità e alla rendicontazione. Verranno introdotti controlli automatici di validazione, strumenti di sincronizzazione più affidabili e processi di monitoraggio continuo delle anomalie, al fine di ridurre gli scostamenti tra sistemi, incrementare la qualità dei dati e garantire una rappresentazione univoca e coerente delle informazioni istituzionali. Gli interventi coinvolgeranno le strutture accademiche, le Direzioni di area e la Funzione Specialistica per il monitoraggio statistico.

Consolidamento dell'integrazione con la Piattaforma Digitale Nazionale Dati (PDND)

In continuità con quanto realizzato nell'ambito della Misura 1.3.1 del PNRR, il Piano prevede una piena messa a regime degli e-service ESSE3 esposti tramite API Manager CINECA, nonché l'estensione progressiva dell'interoperabilità verso altri domini informativi di Ateneo. Saranno adottate procedure interne per la gestione del ciclo di vita delle API, la documentazione tecnica dei servizi, la qualità dei dati condivisi e il monitoraggio del consumo. L'integrazione con la PDND costituirà il punto di riferimento per la progettazione di nuovi servizi e per l'evoluzione delle architetture applicative.

Armonizzazione dell'identità digitale e dei sistemi di autenticazione

Il triennio 2026–2028 prevede la standardizzazione dei meccanismi di autenticazione e gestione delle identità, promuovendo l'utilizzo di SPID, CIE, federazione IDEM-GARR e dei servizi di directory unificata (AD/Entra ID). L'obiettivo è garantire accesso uniforme e sicuro ai servizi digitali, semplificare le integrazioni applicative, ridurre le ridondanze e assicurare all'Ateneo un modello coerente di gestione degli accessi, in conformità con le prescrizioni del CAD e con gli standard internazionali.

Sono quindi azioni che puntano a costruire un sistema informativo pienamente integrato e affidabile, al fine di supportare in modo strutturato la programmazione istituzionale, le esigenze delle strutture accademiche e amministrative e lo sviluppo dei servizi digitali rivolti alla comunità universitaria. La strategia adottata si pone come modello di interoperabilità sostenibile, centrato sulla qualità del dato, sulla sicurezza, sulla standardizzazione e sulla piena conformità alle linee di indirizzo nazionali.

7.2 Interoperabilità e dati - Pre-requisiti

La piena realizzazione delle azioni previste nel dominio "Interoperabilità e dati" richiede la presenza di un insieme di condizioni abilitanti di natura organizzativa, tecnica, normativa e procedurale, che rappresentano elementi imprescindibili per assicurare la coerenza, la sostenibilità e l'efficacia degli interventi programmati nel triennio 2026–2028. L'assenza o l'incompletezza di uno solo di questi prerequisiti comprometterebbe in modo significativo la possibilità di raggiungere gli obiettivi delineati dal Piano.

Un primo prerequisito riguarda la formalizzazione del modello di data governance. Le attività previste necessitano di un quadro chiaro e condiviso che identifichi le fonti dati autorevoli, i domini informativi, i responsabili del dato (data owner), le

responsabilità operative (data steward), le regole di qualità, i criteri di aggiornamento e le modalità di validazione. Senza questo modello, l'Ateneo non può garantire coerenza semantica, tracciabilità dei flussi, accountability amministrativa né conformità al GDPR e alle linee guida AgID.

Un secondo prerequisito consiste nella disponibilità di una mappatura completa e aggiornata delle integrazioni applicative, comprensiva dei flussi dati, dei protocolli utilizzati, dei sistemi coinvolti, delle frequenze di sincronizzazione, dei punti di rischio e delle dipendenze rispetto ai fornitori esterni, in particolare CINECA. Tale documentazione è essenziale per pianificare interventi di razionalizzazione, per prevenire malfunzionamenti legati a integrazioni non documentate e per assicurare continuità operativa nei processi amministrativi e accademici.

Elemento altrettanto fondamentale è la presenza di un registro delle API e dei servizi interoperabili. La piena adesione alla Piattaforma Digitale Nazionale Dati e l'introduzione di standard comuni di scambio informativo richiedono che l'Ateneo disponga di un inventario dei servizi esposti e consumati, completo di descrizione, versionamento, documentazione, requisiti di sicurezza e livelli di qualità. L'assenza di tale registro rappresenterebbe un rischio significativo di non conformità rispetto agli obblighi derivanti dalla PDND nel quinquennio 2023–2028.

Sul piano infrastrutturale, le azioni previste richiedono la disponibilità di un sistema centralizzato di gestione delle identità e degli accessi (IAM) pienamente funzionante, con policy uniformi per tutto l'Ateneo, integrazione con SPID, CIE e IDEM-GARR, cicli di approvvigionamento delle utenze documentati e capacità di gestione coerente della dismissione. Senza un IAM consolidato, l'Ateneo non può garantire sicurezza, tracciabilità, né interoperabilità affidabile con i sistemi esterni.

Un prerequisito critico è rappresentato dalla presenza di un framework condiviso di qualità del dato, che includa criteri di completezza, accuratezza, unicità, tempestività e consistenza, nonché procedure strutturate per la gestione delle anomalie, la validazione dei dataset e il raccordo con le attività di monitoraggio dei flussi istituzionali (carriere, ricerca, personale, contabilità). Senza questo presidio, il rischio di incoerenze informative rimane elevato e incide direttamente sulla qualità della didattica, della rendicontazione e della valutazione AVA.

È inoltre indispensabile il coordinamento strutturato tra le strutture accademiche e amministrative coinvolte nella produzione o gestione dei dati. La piena interoperabilità richiede un dialogo costante tra RTD, Settore Sviluppo Digitale, Direzioni amministrative, Presidio della Qualità, Nucleo di Valutazione e responsabili dei sistemi applicativi. L'assenza di tale coordinamento genererebbe ritardi, duplicazioni informative e disallineamenti nei processi.

Dal punto di vista tecnico, un prerequisito rilevante è la disponibilità di strumenti adeguati al monitoraggio dei flussi informativi, la gestione dei log applicativi, la diagnostica sulle API e la supervisione degli scambi con i sistemi esterni. Senza tali strumenti l'Ateneo non può garantire affidabilità dei servizi, né rispondere ad audit o a richieste di verifica da parte di enti centrali o partner istituzionali.

Infine, il pieno sviluppo dell'interoperabilità richiede un contesto di competenze adeguate, in particolare nella modellazione dei dati, nella progettazione di API, nella gestione semantica delle informazioni, nell'analisi dei flussi e nella compliance ambito PDND. La carenza di queste competenze rappresenta uno dei principali fattori di rischio per gli atenei italiani e costituisce un elemento che il Piano intende affrontare anche attraverso le azioni previste nel dominio del change management e delle competenze digitali.

Nel complesso, i prerequisiti individuati rappresentano la base tecnica, organizzativa e normativa necessaria per garantire la qualità, la sicurezza e la sostenibilità del modello di interoperabilità e di gestione dei dati che l'Ateneo intende sviluppare nel triennio 2026–2028.

7.3 Interoperabilità e dati – Risorse

L'attuazione delle azioni previste nel dominio "Interoperabilità e dati" richiede la disponibilità coordinata di risorse economiche, professionali, tecniche e organizzative, senza le quali non sarebbe possibile garantire la piena realizzazione degli interventi programmati nel triennio 2026–2028. La solidità del modello di interoperabilità e la maturità della data governance dipendono infatti dalla presenza di strumenti adeguati, competenze specialistiche e un presidio strutturato dei processi informativi.

Dal punto di vista economico, il Piano necessita di un investimento pluriennale dedicato allo sviluppo e alla manutenzione delle integrazioni applicative, all'adozione di strumenti per la gestione delle API, all'aggiornamento dei sistemi informativi centrali e al rafforzamento delle piattaforme utilizzate per il monitoraggio dei flussi istituzionali. Le attività previste richiedono inoltre risorse per l'evoluzione dei sistemi di autenticazione e identity management, per l'adeguamento agli standard PDND e ModI, per l'implementazione di controlli automatici di qualità del dato e per l'assistenza specialistica necessaria nei casi in cui le integrazioni coinvolgano fornitori esterni, in particolare CINECA. La mancanza di risorse economiche adeguate rappresenterebbe un ostacolo significativo, compromettendo la continuità dei flussi critici e aumentando la dipendenza da soluzioni manuali o non standardizzate.

A livello professionale, l'Ateneo necessita di competenze specialistiche in ambito di modellazione dei dati, gestione semantica, progettazione e documentazione di API, analisi dei flussi informativi, qualità del dato, compliance PDND e gestione dei sistemi di identity federation. Tali competenze sono oggi distribuite in modo non uniforme e richiedono un rafforzamento mirato attraverso percorsi strutturati di formazione e l'eventuale inserimento di figure tecniche dedicate, in coerenza con il Piano dei Fabbisogni di Personale e con le priorità del Settore Sviluppo Digitale. L'assenza di un presidio adeguato determinerebbe ritardi nell'evoluzione del modello di interoperabilità e rischi di non conformità normativa.

Sul piano tecnico, l'attuazione delle azioni richiede strumenti idonei alla gestione del patrimonio informativo e dei flussi applicativi. Si rendono necessari: piattaforme di API management, sistemi per il monitoraggio dei log applicativi, strumenti per la validazione e la pulizia dei dati, ambienti per il versionamento delle integrazioni, repository documentali dedicati alla data governance e sistemi di diagnostica per l'analisi delle anomalie. È inoltre essenziale disporre di un registro ufficiale delle API e dei servizi interoperabili, nonché di un insieme di strumenti dedicati alla qualità del dato e al controllo dei flussi trasversali (studenti, personale, contabilità, ricerca, didattica).

Dal punto di vista organizzativo, l'Ateneo necessita di un coordinamento strutturato tra RTD, Settore Sviluppo Digitale, Direzioni amministrative, strutture accademiche, Presidio della Qualità, Nucleo di Valutazione e Funzione Specialistica dedicata alle statistiche istituzionali. Tale collaborazione è indispensabile per garantire un governo unitario del patrimonio informativo, evitare duplicazioni, ridurre le ridondanze e assicurare coerenza tra le diverse fonti. È altrettanto necessaria la formalizzazione di procedure interne che regolino la produzione, la validazione, la trasmissione e la conservazione dei dati, nonché l'adozione di modelli condivisi per la classificazione dei domini informativi e delle responsabilità associate.

Infine, l'implementazione del modello di interoperabilità richiede un adeguato supporto contrattuale, con accordi di assistenza specialistica e SLA coerenti con la criticità dei flussi gestiti. Le integrazioni che coinvolgono fornitori esterni devono poter contare su canali tecnici dedicati, tempi certi di intervento e una gestione documentale completa delle modifiche applicative. In assenza di tali garanzie contrattuali, l'Ateneo non sarebbe in grado di assicurare la continuità e l'affidabilità dei servizi connessi alle carriere, alla didattica, alla ricerca e alla gestione amministrativa.

Nel complesso, il dominio "Interoperabilità e dati" richiede un insieme organico e integrato di risorse che garantiscano non solo la realizzazione delle singole attività, ma anche la maturazione del sistema informativo nel suo complesso. La disponibilità di tali risorse costituisce un prerequisito essenziale per sviluppare un modello di interoperabilità stabile, sicuro e sostenibile, pienamente conforme agli standard nazionali e alle esigenze istituzionali dell'Ateneo.

7.4 Interoperabilità e dati – KPI

Il monitoraggio dell'interoperabilità e della qualità del patrimonio informativo nel triennio 2026–2028 si basa su un insieme di indicatori progettati per misurare il livello di integrazione tra le piattaforme applicative, la coerenza dei flussi informativi, la maturità del modello di data governance e l'adozione degli standard nazionali di interoperabilità. I KPI individuati riflettono le prescrizioni del Modello di Interoperabilità nazionale (ModI), gli obblighi della Piattaforma Digitale Nazionale Dati (PDND), le Linee Guida AgID e le esigenze emergenti di qualità, sicurezza e affidabilità del dato. La selezione degli indicatori tiene conto della struttura organizzativa dell'Ateneo, della sostenibilità delle attività di monitoraggio e della necessità di assicurare continuitità informativa e piena tracciabilità dei flussi nei sistemi gestionali e nei servizi digitali.

KPI3 - Percentuale di domini informativi con fonte autorevole definita

Definizione: % dei domini informativi istituzionali (studenti, personale, ricerca, didattica, contabilità, patrimonio documentale, servizi) per i quali è formalmente individuata la fonte dati autorevole, con responsabilità di gestione, criteri di aggiornamento e regole di interoperabilità documentate secondo il modello di data governance d'Ateneo.

Target 2028: 100%.

KPI4 - Percentuale di servizi con identità federata e policy uniformi

Definizione: % dei servizi digitali di Ateneo che utilizzano sistemi di autenticazione centralizzata (SSO, Active Directory/Entra ID, SPID/CIE) con policy di sicurezza uniformi e gestite dal Settore Sviluppo Digitale.

Target 2026: ≥ 90%.

8. Piano attuativo: servizi digitali e processi amministrativi

Il Piano attuativo dedicato ai servizi digitali e ai processi amministrativi definisce il percorso operativo attraverso il quale l'Università di Napoli L'Orientale intende rendere pienamente coerente, accessibile e orientata all'utente la propria offerta digitale nel triennio 2026–2028. Le azioni previste mirano a consolidare l'ecosistema applicativo esistente, eliminare frammentazioni, standardizzare i modelli di erogazione dei servizi, razionalizzare i flussi informativi, ridurre gli oneri amministrativi e migliorare in modo misurabile l'esperienza dell'utenza, in coerenza con il Modello di Interoperabilità, con le Linee Guida AgID e con gli obiettivi del Piano Strategico di Ateneo.

L'intervento si articola intorno a quattro assi prioritari: la piena digitalizzazione dei processi amministrativi, l'evoluzione dei servizi rivolti agli studenti, il rafforzamento dei servizi dedicati ai docenti e ai ricercatori, e il miglioramento dei servizi destinati al personale tecnico-amministrativo. Accanto a tali direttrici, il Piano riconosce come trasversali la centralità dell'accessibilità digitale, l'adozione di modelli editoriali uniformi e lo sviluppo di un sistema strutturato di supporto all'utenza.

Un primo ambito di intervento riguarda la digitalizzazione dei procedimenti amministrativi, che rappresenta la leva principale per la semplificazione dei flussi, la riduzione dei tempi di lavorazione, l'incremento della trasparenza e la piena tracciabilità delle attività svolte. Le azioni previste includono la revisione dei workflow documentali su Titulus, la standardizzazione dei modelli redazionali, il rafforzamento della cooperazione applicativa tra U-Gov, PICA, Intranet e le altre piattaforme interne, e il supporto alla progressiva eliminazione della documentazione cartacea. L'obiettivo è garantire processi end-to-end realmente digitali, riducendo le variabilità tra le strutture e assicurando un'esperienza uniforme e facilmente monitorabile.

In continuità con tale asse, un ruolo strategico è attribuito alla modernizzazione dei servizi rivolti agli studenti, che costituiscono il nucleo più ampio dell'utenza e la componente più sensibile all'efficienza del sistema digitale. Il Piano prevede interventi orientati a migliorare l'esperienza su ESSE3 e MyUniOr, a integrare in maniera più fluida i servizi di pagamento PagoPA, a semplificare la consultazione dell'offerta formativa, a rafforzare il supporto tramite Help Desk e a garantire un'interazione chiara, accessibile e omogenea durante tutte le fasi della carriera universitaria. L'obiettivo è costruire un ecosistema di servizi coerente, riducendo la frammentazione delle interfacce e migliorando la tempestività e la trasparenza informativa.

Per quanto riguarda i servizi digitali destinati ai docenti e ai ricercatori, il Piano definisce azioni orientate a consolidare l'integrazione tra UniFIND e IRIS/UNORA, a migliorare i servizi legati alla didattica digitale su Moodle, a semplificare la gestione delle attività scientifiche e dei moduli di rendicontazione, e a potenziare i servizi dedicati alla mobilità accademica internazionale tramite la piattaforma Visiting Professor. Particolare attenzione è riservata alla progressiva uniformazione degli accessi, alla riduzione delle duplicazioni e al miglioramento della coerenza tra le piattaforme istituzionali.

Un ulteriore asse riguarda i servizi digitali per il personale tecnico-amministrativo, per il quale il Piano promuove l'evoluzione dei workflow operativi, la piena integrazione tra Intranet, U-Gov, Titulus, PAT e i sistemi di ticketing ARIE, nonché il miglioramento delle funzionalità di supporto e monitoraggio. Tali azioni sono finalizzate a incrementare l'efficienza dei processi, ridurre gli errori operativi, rafforzare la tracciabilità e garantire maggiore uniformità nell'erogazione dei servizi interni.

Componente trasversale di tutto il Piano attuativo è il rafforzamento dell'esperienza utente e dell'accessibilità digitale, che si sostanzia nell'adozione dei principi delle Linee Guida AgID su design, usabilità, linguaggio chiaro e standard editoriali comuni per i contenuti digitali. Il Piano prevede l'introduzione di un modello di presenza istituzionale uniforme, l'allineamento dei micrositi MySiteUniOr agli standard di accessibilità, la verifica periodica dei contenuti e la promozione di processi di comunicazione strutturata e coordinata.

Il Piano attuativo mira, inoltre, a consolidare il sistema di supporto all'utenza, integrando i servizi dell'Help Desk studenti, del ticketing ARIE, dei servizi di assistenza docenti e delle attività di supporto alle piattaforme digitali. L'obiettivo è costruire

un modello di assistenza multicanale, con procedure uniformi, tracciabilità delle attività e capacità di monitorare in modo sistematico il livello di servizio percepito.

Le azioni previste sono volte alla realizzazione di un ecosistema di servizi digitali più semplice ed integrato ma al tempo stesso accessibile e coerente con capacità di supportare la missione dell'Ateneo e di rispondere alle esigenze di tutta la comunità universitaria in un contesto normativo e tecnologico, basti pensare agli sviluppi degli ultimi anni in ambito di intelligenza artificiale, in rapida evoluzione.

8.1 Servizi digitali e processi amministrativi - Azioni 2026-2028

Nel triennio 2026–2028 l'Università di Napoli L'Orientale attuerà un insieme coordinato di interventi finalizzati alla modernizzazione dei servizi digitali e alla piena digitalizzazione dei procedimenti amministrativi, con l'obiettivo di garantire maggiore semplicità operativa, qualità dell'esperienza utente, coerenza tra le piattaforme e riduzione degli oneri procedurali per studenti, docenti, ricercatori e personale tecnico-amministrativo.

Una prima linea di azione riguarda la reingegnerizzazione dei processi amministrativi, che prevede la revisione sistematica dei workflow documentali e procedurali, l'armonizzazione dei modelli redazionali, l'eliminazione delle duplicazioni e la convergenza verso processi completamente digitali. In questo ambito rientrano l'evoluzione dei flussi su Titulus, il consolidamento dei processi di firma digitale e la piena integrazione dei workflow con i sistemi U-Gov, PICA, PAT e con l'Intranet di Ateneo. L'obiettivo è ridurre i tempi di lavorazione, assicurare maggiore uniformità tra le strutture e garantire tracciabilità completa nei processi di protocollo, gestione atti, acquisti, missioni e gestione del personale.

Parallelamente, il Piano prevede la modernizzazione dell'esperienza digitale degli studenti, con interventi volti a potenziare la fruibilità dei servizi offerti da ESSE3, MyUniOr, PagoPA e dalla piattaforma di Help Desk. Le azioni comprendono l'ottimizzazione dei percorsi di immatricolazione e iscrizione, la semplificazione della consultazione dell'offerta formativa e dei portali dei dottorati, l'integrazione tra procedure amministrative e piattaforme per la didattica digitale e l'adozione di modelli comunicativi più chiari, coerenti e accessibili. Un'attenzione particolare è rivolta al miglioramento della tempestività delle informazioni e alla riduzione delle interazioni ridondanti con gli uffici.

Sul versante della didattica e della ricerca, il Piano promuove interventi volti a rafforzare l'integrazione tra UniFIND, IRIS/UNORA e i sistemi ministeriali, semplificare la gestione dei prodotti della ricerca e migliorare la coerenza dei servizi dedicati ai docenti e ai ricercatori. Rientrano in questa linea di azione la razionalizzazione degli strumenti di supporto alla didattica digitale, il potenziamento delle funzionalità di Moodle, l'evoluzione dei servizi dedicati alla mobilità accademica e l'introduzione di modelli più uniformi per la pubblicazione dei contenuti dei corsi e delle attività scientifiche.

Una linea di intervento rilevante riguarda inoltre i servizi digitali per il personale tecnico-amministrativo, per i quali il Piano prevede il consolidamento dell'integrazione tra Intranet, U-Gov, Titulus, PAT e il sistema di ticketing ARIE. Le azioni includono la revisione dei flussi operativi, la semplificazione delle attività di back-office, il rafforzamento della collaborazione interstruttura e l'introduzione graduale di strumenti di automazione dei processi amministrativi in settori critici quali rendicontazione, contrattualistica, missioni e gestione documentale.

Trasversale a tutte le direttrici è l'introduzione di un modello unitario di esperienza utente, fondato sui principi di accessibilità, chiarezza del linguaggio, coerenza grafica e usabilità. Il Piano prevede l'adozione degli standard di design

AgID, l'aggiornamento dei micrositi istituzionali tramite MySiteUniOr, la revisione dei contenuti digitali e la creazione di percorsi di accesso più intuitivi e uniformi per i servizi più utilizzati. Accanto a queste attività, il Piano promuove la realizzazione di un sistema organico di supporto all'utenza, che integra l'Help Desk studenti, il ticketing ARIE, i servizi di assistenza digitale e le attività di supporto dei presìdi tecnici.

8.2 Servizi digitali e processi amministrativi - Pre-requisiti

L'attuazione delle azioni previste nel triennio 2026–2028 richiede la presenza di un insieme di pre-requisiti tecnici, organizzativi e procedurali che garantiscano la sostenibilità degli interventi e la loro efficacia nel medio periodo. La modernizzazione dei servizi digitali e la reingegnerizzazione dei processi amministrativi possono produrre risultati significativi solo se sostenute da una governance chiara, da un'infrastruttura stabile, da un modello di cooperazione interna adeguato e da un livello minimo di standardizzazione già operativo nelle strutture amministrative e accademiche.

Un primo pre-requisito riguarda la disponibilità di un quadro infrastrutturale affidabile, in particolare per quanto concerne la continuità operativa dei sistemi gestionali, la stabilità delle piattaforme applicative CINECA, la piena operatività dei sistemi documentali e la capacità delle reti interne di sostenere un incremento dei volumi di mobilità digitale. Senza un'infrastruttura coerente e adeguata, l'introduzione di nuovi servizi digitali rischierebbe di generare discontinuità operative o carichi non sostenibili per le strutture coinvolte.

In parallelo, la trasformazione dei servizi richiede la definizione formalizzata dei processi amministrativi di riferimento, condizione indispensabile per evitare interpretazioni divergenti, duplicazioni procedurali o sviluppi applicativi non sostenibili. Il Piano necessita quindi di un sistema di process mapping condiviso tra le strutture, in particolare nei settori relativi alle carriere studentesche, alla gestione dei docenti, alla ricerca, al personale e alla contrattualistica. Tale lavoro di normalizzazione costituisce il fondamento della reingegnerizzazione digitale e permette di mantenere uniformità nel rapporto tra servizi digitali e attività in presenza.

Un ulteriore pre-requisito riguarda la standardizzazione delle basi dati e la disponibilità di fonti informative attendibili per alimentare i servizi digitali. La coerenza tra ESSE3, U-Gov, Titulus, IRIS/UNORA, UniFIND e i servizi interni rappresenta una condizione essenziale per garantire esperienze utente prive di incoerenze e per evitare errori nella generazione automatica di documenti, attestazioni, notifiche e contenuti informativi. In questo ambito assume rilievo la progressiva implementazione del modello di data governance delineato nelle linee strategiche.

La realizzazione delle azioni previste richiede inoltre un modello organizzativo stabile, fondato su ruoli chiari tra Settore Sviluppo Digitale, strutture TAB, referenti delle aree accademiche, presìdi amministrativi e responsabili dei servizi didattici e di ricerca. La disponibilità di referenti applicativi, di gruppi di lavoro trasversali e di processi di escalation definiti costituisce un elemento essenziale per la gestione dei servizi digitali e per il supporto operativo nella fase di transizione.

Trasversale a tali elementi è la necessità di una cultura digitale sufficientemente omogenea, che rappresenta un pre-requisito implicito ma determinante per la corretta adozione dei servizi. Le strutture amministrative devono essere in grado di utilizzare le funzionalità dei sistemi in modo uniforme; gli utenti devono poter comprendere le modalità di fruizione dei servizi digitali; i docenti e i ricercatori devono operare all'interno di un ecosistema coerente e privo di complessità inutili. Il

pre-requisito indicato dovrà essere sostenuto sia attraverso attività formative mirate sia mediante un sistema di comunicazione interna efficace.

Infine, le azioni del Piano richiedono un modello di supporto consolidato, che assicuri continuità nella gestione delle richieste dell'utenza, riduzione dei tempi di assistenza e presidio delle attività critiche. La piena integrazione dei sistemi di ticketing, la disponibilità di statistiche di servizio e il coordinamento tra ARIE e le strutture responsabili dei procedimenti sono elementi essenziali per evitare sovraccarichi e disallineamenti durante l'implementazione delle innovazioni.

Queste attività sopradescritte definiscono il contesto minimo necessario affinché la trasformazione dei servizi digitali e dei processi amministrativi possa essere condotta in modo sostenibile, coerente e orientato alle reali esigenze dell'utenza.

8.3 Servizi digitali e processi amministrativi – Risorse

L'attuazione delle azioni previste per il miglioramento dei servizi digitali e la digitalizzazione dei processi amministrativi richiede la disponibilità di risorse tecniche, professionali e finanziarie adeguate a sostenere interventi continuativi e ad accompagnare in modo stabile l'evoluzione dell'ecosistema applicativo. Il successo delle iniziative individuate dipende non solo dalla presenza di tecnologie idonee, ma soprattutto dalla capacità dell'Ateneo di garantire un presidio organizzativo strutturato, competenze dedicate, investimenti proporzionati e modelli di collaborazione interni sufficientemente maturi.

Un primo ambito di risorse riguarda il consolidamento delle competenze tecniche e funzionali. Il potenziamento dei servizi digitali richiede figure specialistiche in grado di presidiare lo sviluppo applicativo, la modellazione dei workflow, l'integrazione dei sistemi, la gestione dei contenuti digitali e il supporto operativo agli utenti. Le unità del Settore Sviluppo Digitale, in particolare ARIE04–ARIE07, costituiscono l'asse portante del presidio applicativo; tuttavia, la complessità crescente dei servizi e la necessità di mantenere elevati standard qualitativi richiedono il rafforzamento di questo presidio attraverso competenze aggiuntive in analisi dei processi, service design, user experience, data quality, assistenza applicativa di secondo livello e interoperabilità.

Accanto alle risorse interne, il Piano richiede un coinvolgimento strutturato delle competenze distribuite nelle aree amministrative e accademiche, che svolgono un ruolo cruciale nella gestione operativa dei processi digitali. Il consolidamento dei servizi non può prescindere da un contributo attivo dei referenti di processo, dei responsabili degli uffici, dei presìdi amministrativi e delle strutture didattiche e di ricerca. Tale contributo è indispensabile per mantenere coerenza tra processi digitali e prassi organizzative, per garantire la validazione delle informazioni pubblicate sui portali istituzionali e per sostenere la reingegnerizzazione dei procedimenti.

La realizzazione del Piano richiede inoltre risorse dedicate per il mantenimento e l'evoluzione delle piattaforme digitali, in particolare per lo sviluppo dei portali tematici, l'aggiornamento delle interfacce applicative, il miglioramento di MyUniOr, la gestione dei workflow su Titulus, l'ottimizzazione dei processi U-Gov e la manutenzione delle integrazioni applicative. Tali attività necessitano di investimenti progressivi, non occasionali, finalizzati a assicurare stabilità agli interventi, aggiornamenti costanti e capacità di risposta alle evoluzioni normative e dei fornitori.

Un ulteriore ambito di risorse riguarda il rafforzamento del sistema di supporto all'utenza, che rappresenta un elemento determinante per garantire la stabilità e la qualità dei servizi digitali. Il potenziamento dell'Help Desk studenti, l'unificazione dei modelli di assistenza, l'integrazione con il ticketing ARIE e la definizione di SLA misurabili richiedono risorse

organizzative e professionali in grado di sostenere un volume crescente di richieste e di assicurare un supporto tempestivo e uniforme.

A ciò si aggiunge la necessità di destinare risorse finanziarie specifiche al miglioramento dell'esperienza utente e dei contenuti digitali, comprendenti attività di redesign dei portali, revisione dei testi istituzionali secondo i principi di linguaggio chiaro, aggiornamento dei modelli editoriali, produzione di contenuti accessibili e adeguamento ai requisiti delle Linee Guida AgID su design e UX. Si tratta di interventi che richiedono sia competenze interne sia, in alcuni casi, supporto specialistico esterno.

Infine, la piena attuazione del Piano comporta l'impegno di risorse dedicate alla formazione del personale, volte a sostenere l'adozione dei nuovi servizi digitali, aggiornare le competenze nell'utilizzo degli strumenti applicativi, rafforzare la capacità delle strutture di integrare i servizi digitali nei processi quotidiani e supportare la transizione dei procedimenti a modalità pienamente digitali. La formazione non costituisce un elemento accessorio, ma una risorsa essenziale per la sostenibilità del modello operativo.

Nel complesso, le risorse necessarie per l'attuazione delle azioni sui servizi digitali e sui processi amministrativi riguardano un equilibrio tra investimenti tecnologici, rafforzamento delle competenze, potenziamento dei presìdi organizzativi e adeguata capacità di supporto. Solo attraverso tale equilibrio sarà possibile garantire la continuità, la qualità e l'efficacia dei servizi digitali dell'Ateneo nel triennio 2026–2028.

8.4 Servizi digitali e processi amministrativi – KPI

Il monitoraggio dell'evoluzione dei servizi digitali e della digitalizzazione dei processi amministrativi nel triennio 2026–2028 si fonda su un insieme di indicatori progettati per misurare il livello di maturità dei servizi erogati, la coerenza dell'esperienza utente, il grado di digitalizzazione dei procedimenti e l'efficacia del modello di supporto all'utenza. I KPI selezionati rispondono ai principi delle Linee Guida AgID su design e usabilità, agli standard di semplificazione amministrativa previsti dal PIAO e ai requisiti del Modello di Interoperabilità (ModI), e sono stati individuati considerando la sostenibilità operativa dell'Ateneo, la disponibilità di fonti dati attendibili e l'esigenza di disporre di misure oggettive e verificabili.

KPI5 - Livello di accessibilità digitale dei servizi

Definizione: servizi conformi ai requisiti di accessibilità (almeno livello AA).

Target 2028: ≥ 85% dei servizi con dichiarazione accessibilità aggiornata.

KPI6 - Soddisfazione media dell'utenza sui principali servizi digitali

Definizione: valutazione su scala 1–5 tramite survey periodiche integrate nell'Help Desk.

Target 2028: ≥ 3.5

9. Piano attuativo: Sicurezza e privacy

La sicurezza informatica e la protezione dei dati personali rappresentano dimensioni centrali della strategia digitale dell'Università di Napoli L'Orientale e costituiscono condizioni indispensabili per garantire affidabilità dei servizi, continuità

operativa e tutela del patrimonio informativo dell'Ateneo. L'evoluzione dei sistemi digitali, la crescente interconnessione delle piattaforme applicative, l'utilizzo di tecnologie cloud e la gestione di flussi di dati sempre più articolati rendono necessario adottare un modello di sicurezza che integri aspetti tecnologici, organizzativi, procedurali e normativi, in piena conformità al quadro europeo e nazionale.

L'Ateneo orienta la propria azione ai principi della Direttiva (UE) 2022/2555 (NIS2), agli standard e alle misure definite dall'Agenzia per la Cybersicurezza Nazionale (ACN), alle Linee Guida AgID sulla sicurezza, al Codice dell'Amministrazione Digitale e alle prescrizioni del Regolamento (UE) 2016/679 (GDPR) e del D.Lgs. 196/2003. Tale quadro richiede un approccio sistemico alla gestione della sicurezza, fondato sulla prevenzione delle minacce, sulla riduzione delle vulnerabilità, sulla protezione del dato nelle diverse fasi del suo ciclo di vita e sulla capacità dell'organizzazione di rispondere in modo tempestivo ed efficace a incidenti o anomalie.

La protezione dei dati personali, affidata al presidio istituzionale del Responsabile della Protezione dei Dati (RPD), costituisce un elemento strutturale della governance digitale e si integra con le misure di sicurezza informatica adottate dall'Ateneo. Il modello implementato è orientato al rispetto dei principi di trasparenza, liceità, minimizzazione, integrità e riservatezza, prevedendo misure tecniche e organizzative adeguate alla natura e al volume dei trattamenti, alla sensibilità delle informazioni trattate e ai rischi associati.

La sicurezza dell'infrastruttura ICT è garantita attraverso la gestione controllata degli accessi, la segmentazione della rete, l'autenticazione forte e federata, l'adozione di firewall e sistemi di protezione avanzata, la gestione degli aggiornamenti e il monitoraggio costante degli eventi. L'integrazione con piattaforme cloud e con i servizi SaaS del Consorzio CINECA avviene secondo criteri di sicurezza-by-design, assicurando che i livelli di protezione siano allineati agli standard della pubblica amministrazione e alle migliori pratiche del settore.

Particolare attenzione viene dedicata alla gestione degli incidenti di sicurezza, attraverso procedure formalizzate, canali di comunicazione istituzionali, sistemi di rilevazione precoce, attività di diagnosi tecnica e piani di ripristino orientati alla continuità dei servizi critici. Tale modello è oggetto di revisione e aggiornamento continuo, in funzione dell'evoluzione delle minacce e dell'adeguamento progressivo ai requisiti NIS2.

Sul versante della tutela dei dati personali, l'Ateneo integra gli adempimenti GDPR nei processi organizzativi e tecnologici, con attività di mappatura dei trattamenti, gestione delle basi giuridiche, valutazioni d'impatto sulla protezione dei dati (DPIA), regolamentazione degli accessi, gestione dei consensi e trattamenti, formazione del personale e cooperazione costante tra RPD, RTD, Settore Sviluppo Digitale e strutture responsabili dei procedimenti amministrativi.

9.1 Sicurezza e privacy - Azioni 2026-2028

Nel triennio 2026–2028 l'Università di Napoli L'Orientale attuerà un insieme coordinato di interventi volti a rafforzare il sistema di sicurezza informatica, garantire una piena conformità al quadro normativo europeo e nazionale e consolidare un modello di protezione dei dati personali che integri aspetti tecnologici, organizzativi e procedurali. Le azioni previste mirano a costruire un'architettura di sicurezza evoluta, sostenibile e coerente con gli standard definiti dalla Direttiva (UE) 2022/2555 (NIS2), dall'Agenzia per la Cybersicurezza Nazionale, dal GDPR e dalle Linee Guida AgID.

Un primo asse di intervento riguarda il rafforzamento dell'architettura di sicurezza infrastrutturale, attraverso l'evoluzione dei firewall di nuova generazione, l'adozione di strumenti di intrusion detection e intrusion prevention, la segmentazione avanzata delle reti e l'introduzione di sistemi centralizzati di monitoraggio degli eventi. L'obiettivo è ridurre la superficie di attacco, aumentare la capacità di rilevazione precoce e garantire coerenza nella gestione delle minacce all'interno dei datacenter, delle reti di sede e delle piattaforme cloud utilizzate dall'Ateneo.

Parallelamente, il Piano prevede la formalizzazione del modello di continuità operativa e disaster recovery, definendo in modo strutturato le criticità dei servizi, le priorità di ripristino, i livelli di servizio attesi, le responsabilità operative e le modalità di esecuzione dei test periodici. Questo intervento include la revisione dei piani CO/DR, il consolidamento della ridondanza dei datacenter, l'ammodernamento delle dorsali GARR e la definizione di procedure operative uniformi per la gestione delle emergenze. Si tratta di un'azione essenziale per assicurare resilienza ai servizi critici e per rispondere agli obblighi imposti da NIS2 e dalle linee guida ACN.

Una componente strategica del Piano riguarda il potenziamento delle politiche di identity security, mediante la piena integrazione dei sistemi di autenticazione federata (AD, SPID, CIE, IDEM-GARR), l'adozione di criteri uniformi per la gestione delle credenziali, la revisione periodica dei privilegi, l'introduzione graduale del principio del least privilege e la formalizzazione delle policy di account lifecycle. Questo intervento rappresenta una delle condizioni più rilevanti per il contrasto alle compromissioni di identità digitale e per l'allineamento ai requisiti del Modello Zero Trust.

Il Piano prevede inoltre la costruzione di un modello strutturato di gestione del rischio cyber, che integri le attività dell'RTD, del RPD, del Settore Sviluppo Digitale e delle strutture amministrative. Tale modello include la classificazione dei servizi in base alla criticità, la valutazione periodica delle minacce, la definizione dei rischi residui, la mappatura dei trattamenti di dati personali e l'aggiornamento delle misure tecniche e organizzative. Particolare attenzione è dedicata ai rischi derivanti da terze parti e dai servizi erogati da fornitori esterni, con l'introduzione di verifiche strutturate e clausole contrattuali coerenti con NIS2 e GDPR.

Un asse trasversale riguarda la formalizzazione del processo di gestione degli incidenti di sicurezza, che includerà procedure uniformi di rilevazione, classificazione, contenimento, notifica e reporting, integrate con il ruolo del RPD per gli aspetti di data breach. Il Piano prevede l'adozione di un registro degli incidenti, la definizione dei tempi massimi di risposta (SLR) e l'integrazione con i presìdi ACN per gli incidenti a impatto significativo.

Sul piano della protezione dei dati personali, il Piano promuove il consolidamento delle attività di privacy by design e privacy by default, la redazione periodica delle valutazioni d'impatto (DPIA) per trattamenti ad alto rischio, la revisione del registro dei trattamenti, l'aggiornamento dei protocolli per la gestione delle richieste degli interessati e il rafforzamento della cooperazione tra RPD, RTD e uffici responsabili dei servizi applicativi. Questo intervento mira a integrare in modo strutturale gli obblighi GDPR nei processi di progettazione, sviluppo e gestione dei servizi digitali.

Infine, il Piano attribuisce un ruolo determinante alla formazione e alla sensibilizzazione degli utenti, ponendo l'accento sulla necessità di consolidare una cultura della sicurezza diffusa in tutta la comunità accademica. Le azioni prevedono percorsi formativi mirati per personale TAB, docenti e studenti, campagne periodiche contro phishing e social engineering, simulazioni di attacco controllato e la diffusione di linee guida operative per l'utilizzo sicuro dei servizi digitali.

Nel loro complesso, le azioni previste nel triennio 2026–2028 intendono costruire un sistema di sicurezza e protezione dei dati che non sia solo reattivo, ma pienamente integrato nell'architettura digitale dell'Ateneo, capace di prevenire incidenti, garantire la resilienza dei servizi critici e assicurare la conformità normativa in un contesto caratterizzato da rischi in costante evoluzione.

9.2 Sicurezza e privacy - Pre-requisiti

L'attuazione delle azioni previste nel triennio 2026–2028 in materia di sicurezza informatica e protezione dei dati personali richiede la presenza di un insieme di pre-requisiti tecnici, organizzativi e procedurali che garantiscano la sostenibilità del modello di sicurezza e la sua coerenza con il quadro normativo nazionale ed europeo. In assenza di tali condizioni, gli interventi programmati rischierebbero di rimanere frammentati, rallentati o non pienamente efficaci, con potenziali impatti sulla resilienza complessiva dei servizi digitali e sulla conformità alle prescrizioni NIS2, ACN e GDPR.

Un primo pre-requisito riguarda la disponibilità di un'architettura infrastrutturale affidabile, capace di sostenere sistemi di monitoraggio avanzati, soluzioni di protezione centralizzate, logiche di segmentazione della rete e procedure di ripristino in caso di crisi. La presenza di apparati eterogenei, in parte stratificati nel tempo, rende necessario un livello minimo di standardizzazione tecnica, senza il quale sarebbe difficile applicare in modo uniforme le politiche di sicurezza e garantire una gestione coerente degli eventi critici.

Un secondo elemento cruciale è la formalizzazione delle responsabilità e dei ruoli. La sicurezza informatica e la protezione dei dati coinvolgono RTD, RPD, Settore Sviluppo Digitale, Direzione Generale, responsabili dei servizi digitali e referenti delle strutture amministrative e didattiche. L'efficacia delle misure previste richiede un modello di governance in cui siano chiaramente definiti compiti, responsabilità, procedure di escalation, flussi comunicativi e modalità di coordinamento tra funzioni tecniche e funzioni gestionali. L'assenza di una struttura organizzativa formalizzata rischierebbe di rendere difficoltosa la gestione del rischio cyber e degli incidenti di sicurezza.

Un ulteriore pre-requisito riguarda la disponibilità di un inventario aggiornato e completo degli asset ICT, condizione indispensabile per applicare controlli di sicurezza coerenti, verificare vulnerabilità, stabilire priorità di intervento, classificare i rischi e definire piani di continuità operativa basati su dati attendibili. La costruzione di un CMDB (Configuration Management Database) sufficientemente maturo rappresenta un elemento fondamentale per la piena implementazione del modello Zero Trust e per l'allineamento alle linee guida ACN.

La piena attuazione del Piano richiede inoltre la standardizzazione dei processi di gestione del rischio, attraverso l'adozione di metodologie uniformi di analisi, classificazione e valutazione delle minacce, integrate con le attività di DPIA, con i registri dei trattamenti e con i controlli tecnici e organizzativi previsti da GDPR e NIS2. Senza un quadro metodologico condiviso, la gestione del rischio rimarrebbe inevitabilmente frammentata, con differenze significative tra strutture e con difficoltà nel garantire un livello omogeneo di protezione.

Un pre-requisito trasversale riguarda la disponibilità di un sistema di logging e monitoraggio centralizzato, in grado di raccogliere, correlare e analizzare eventi provenienti da firewall, autenticazione, sistemi cloud, macchine virtuali, rete interna, applicativi e servizi terzi. Tale sistema costituisce una condizione essenziale per rilevare tempestivamente

comportamenti anomali, violazioni di sicurezza e tentativi di intrusione, e per disporre di evidenze documentate in caso di audit, ispezioni o incidenti con impatto significativo.

Infine, l'implementazione delle azioni previste richiede una cultura della sicurezza e della protezione dei dati diffusa all'interno dell'Ateneo, condizione che non può essere data per acquisita. La consapevolezza del personale, dei docenti, dei ricercatori e degli studenti rispetto alle minacce informatiche, all'utilizzo corretto delle credenziali, alla gestione dei dati sensibili e alle buone pratiche digitali rappresenta un pre-requisito indispensabile per ridurre il rischio derivante dal fattore umano, che costituisce una delle principali vulnerabilità evidenziate nei report nazionali di ACN e nei casi di compromissione più frequenti nel settore universitario.

9.3 Sicurezza e privacy – Risorse

La piena realizzazione delle azioni previste nel triennio 2026–2028 in materia di sicurezza informatica e protezione dei dati personali richiede la disponibilità di risorse tecniche, professionali, organizzative e finanziarie adeguate a sostenere un modello di sicurezza evoluto e pienamente conforme al quadro normativo vigente. La sicurezza non può essere garantita esclusivamente attraverso strumenti tecnologici: richiede infatti un presidio continuativo, una governance chiara, competenze specialistiche e capacità di risposta coerenti con la crescente complessità del contesto cyber nazionale ed europeo.

Un primo insieme di risorse riguarda il rafforzamento delle competenze tecniche del Settore Sviluppo Digitale, in particolare nelle aree di sicurezza delle reti, gestione delle identità digitali, protezione degli endpoint, monitoraggio degli eventi, gestione degli incidenti e sicurezza applicativa. La natura multidimensionale della sicurezza richiede profili professionali con competenze avanzate in ambito sistemistico, cloud security, vulnerability assessment, gestione del rischio e analisi forense. L'Ateneo dispone oggi di competenze consolidate, ma la piena implementazione degli standard NIS2 e ACN richiede un ulteriore ampliamento e specializzazione delle professionalità dedicate.

Accanto alle competenze tecniche, il Piano necessita di risorse professionali per il presidio della protezione dei dati personali, a supporto del Responsabile della Protezione dei Dati (RPD) e delle attività connesse alla redazione delle DPIA, alla gestione dei registri dei trattamenti, alla valutazione delle misure organizzative, al monitoraggio della conformità e alla gestione delle richieste degli interessati. La crescita dei servizi digitali e l'aumento dei flussi informativi richiedono un rafforzamento dello staff RPD, anche attraverso il coordinamento strutturato con gli uffici amministrativi coinvolti nei trattamenti.

Il Piano richiede inoltre risorse dedicate all'evoluzione delle infrastrutture di sicurezza, comprendenti firewall di nuova generazione, sistemi IDS/IPS, strumenti per il monitoraggio centralizzato (SIEM), soluzioni di endpoint protection avanzate, tecnologie di multifactor authentication, sistemi di segmentazione delle reti e apparati destinati alla continuità operativa. L'ammodernamento di questi componenti è essenziale per ridurre la superficie di attacco, garantire livelli adeguati di resilienza e sostenere un modello Zero Trust compatibile con gli standard ACN e con le prescrizioni NIS2.

Una parte significativa delle risorse è destinata alla gestione del rischio e alla continuità operativa, attività che richiedono competenze specializzate per l'analisi delle minacce, la classificazione dei servizi critici, l'identificazione dei rischi residui, la definizione delle priorità di ripristino e la revisione periodica dei piani CO/DR. Queste attività necessitano di personale

dedicato e di strumenti adeguati per il testing, il controllo degli SLA e la produzione di reportistica per Direzione Generale, RTD, RPD e organi di governo.

Elemento imprescindibile è la disponibilità di risorse per la formazione e la sensibilizzazione della comunità accademica, finalizzate a ridurre il rischio legato al fattore umano, che costituisce oggi una delle principali vulnerabilità del sistema informativo. Le attività formativa dovranno essere ricorrenti, differenziate per target (TAB, docenti, studenti, ricercatori), orientate alla prevenzione degli attacchi (phishing, social engineering, credential harvesting) e integrate con sistemi di simulazione e campagne periodiche.

Infine, la piena attuazione del Piano richiede un adeguato investimento in servizi di supporto specialistico, in particolare per attività complesse quali penetration test, vulnerability assessment, configurazioni avanzate di sicurezza, audit esterni, assessment NIS2 e test di resilienza. Questi servizi sono fondamentali per garantire un monitoraggio indipendente dello stato di sicurezza, verificare il rispetto dei requisiti normativi e assicurare alla governance dell'Ateneo un quadro oggettivo dei rischi e delle priorità di intervento.

Queste risorse necessarie delineano un assetto che integra competenze interne, supporto professionale, strumenti tecnologici avanzati e investimenti programmati. Solo attraverso questo equilibrio sarà possibile garantire un modello di sicurezza e protezione dei dati robusto, resiliente e pienamente conforme agli standard richiesti, assicurando all'Ateneo una protezione adeguata del proprio patrimonio informativo e la continuità dei servizi digitali in un contesto caratterizzato da rischi in costante evoluzione.

9.4 Sicurezza e privacy – KPI

Il monitoraggio dell'evoluzione della sicurezza informatica e della protezione dei dati nel triennio 2026–2028 si basa su un insieme di indicatori che consentono di valutare la maturità del sistema di difesa cyber, la capacità dell'Ateneo di prevenire e gestire gli incidenti, il livello di protezione dei dati personali e l'allineamento ai requisiti normativi della Direttiva NIS2, dell'Agenzia per la Cybersicurezza Nazionale (ACN), del GDPR e delle Linee Guida AgID. I KPI selezionati sono stati individuati considerando il contesto organizzativo dell'Ateneo, la disponibilità delle fonti informative, la sostenibilità delle attività di monitoraggio e la necessità di definire indicatori affidabili, verificabili e non meramente descrittivi.

KPI7 - Percentuale delle policy di sicurezza ICT previste dal Framework di cybersecurity d'Ateneo che risultano redatte e sottoposte all'iter di approvazione formale.

Target 2028: ≥ 100% delle policy previste da NIS2 redatte e pronte all'adozione.

KPI8 - DPIA sui trattamenti ad alto rischio

Definizione: Percentuale di trattamenti classificati ad alto rischio per i quali è stata redatta e validata una DPIA.

Target 2028: ≥ 50%.

10. Piano attuativo: competenze digitali

Lo sviluppo delle competenze digitali rappresenta uno dei fattori abilitanti fondamentali per la piena attuazione della trasformazione digitale dell'Università di Napoli L'Orientale. La maturità tecnologica, la qualità dei servizi digitali e la sicurezza dell'ecosistema ICT dipendono infatti dalla capacità della comunità accademica di utilizzare in modo consapevole, efficace e responsabile gli strumenti digitali messi a disposizione dall'Ateneo.

Nel triennio 2026–2028, il Piano prevede un insieme di interventi mirati a consolidare e rendere sistematico il processo di crescita delle competenze digitali di personale tecnico-amministrativo, docenti, ricercatori, figure di governo e studenti. L'obiettivo è creare un modello stabile e continuo di formazione, accompagnamento e aggiornamento, fondato sui principi del Quadro Europeo delle Competenze Digitali (DigComp), del modello organizzativo DigCompOrg e degli standard sulla didattica digitale (DigCompEdu).

La strategia poggia su tre direttrici principali. La prima riguarda il rafforzamento delle competenze del personale tecnico-amministrativo, con particolare riferimento all'utilizzo dei sistemi gestionali (U-Gov, ESSE3, Titulus), dei workflow digitali e degli strumenti collaborativi Microsoft 365. Le attività formative saranno integrate con interventi di accompagnamento operativo per supportare la transizione verso processi pienamente digitali, con particolare attenzione ai settori maggiormente coinvolti nella reingegnerizzazione dei procedimenti.

La seconda direttrice riguarda i docenti e i ricercatori, ai quali il Piano riconosce un ruolo strategico nella diffusione della cultura digitale e nell'adozione di strumenti didattici innovativi. L'Ateneo promuoverà azioni dedicate alla didattica digitale, all'utilizzo avanzato delle piattaforme e-learning, alla gestione dei contenuti multimediali, all'uso degli strumenti per la ricerca e per la produzione scientifica, nonché alla consapevolezza dei rischi legati alla sicurezza informatica e alla protezione dei dati personali.

Il terzo asse riguarda le competenze digitali del management e delle figure di governo, con l'obiettivo di assicurare una piena comprensione delle implicazioni organizzative, normative e tecnologiche dei processi di transizione digitale. Le attività previste includono percorsi formativi sui temi della governance ICT, della gestione del rischio cyber, della Piattaforma Digitale Nazionale Dati, della protezione dei dati personali e dei requisiti NIS2, così da garantire decisioni consapevoli e coerenti con il quadro regolatorio.

Accanto a queste direttrici, il Piano definisce un insieme di azioni trasversali finalizzate a diffondere una cultura digitale unitaria nell'Ateneo. Tra queste rientrano la creazione di percorsi formativi modulari disponibili in modalità sincrona e asincrona, l'attivazione di sessioni di aggiornamento su temi emergenti (intelligenza artificiale, cybersecurity, gestione dei dati, accessibilità digitale), la predisposizione di materiali di supporto e la costruzione di comunità di pratica interne. Saranno inoltre promosse campagne di sensibilizzazione rivolte all'intera comunità universitaria, con particolare attenzione ai rischi legati al phishing, alla gestione delle credenziali, ai comportamenti sicuri online e all'utilizzo corretto dei servizi istituzionali.

Il Piano riconosce infine la necessità di garantire alle strutture un sistema di supporto stabile, in grado di fornire assistenza tempestiva, centralizzata e coerente durante tutto il processo di adozione dei servizi digitali. Il rafforzamento del ruolo dei

referenti di processo, la definizione di procedure di escalation chiare e l'integrazione del supporto con le attività formative rappresentano elementi essenziali per la continuità e la coerenza degli interventi.

Nel complesso, il Piano attuativo dedicato alle competenze digitali mira a costruire un modello di crescita professionale continuo, strutturato e sostenibile, capace di accompagnare l'evoluzione dei servizi digitali, rafforzare la qualità dei processi e sostenere la trasformazione organizzativa dell'Ateneo. La capacità delle persone di utilizzare con competenza e consapevolezza gli strumenti digitali rappresenta infatti uno dei pilastri su cui si fonda l'intero percorso di innovazione delineato nel presente Piano.

10.1 Competenze digitali - Azioni 2026-2028

Nel triennio 2026–2028 l'Università di Napoli L'Orientale avvierà un programma organico di sviluppo delle competenze digitali finalizzato a sostenere la trasformazione organizzativa dell'Ateneo e a garantire un utilizzo consapevole, efficace e sicuro dei servizi digitali istituzionali. Le azioni previste si collocano all'interno di un modello di crescita continua, allineato ai quadri europei DigComp, DigCompOrg e DigCompEdu, e fortemente integrato con il sistema di governance ICT e con le esigenze operative delle strutture amministrative e accademiche.

Una prima linea di intervento è dedicata al rafforzamento delle competenze digitali del personale tecnico-amministrativo, con particolare attenzione ai processi maggiormente interessati dalla digitalizzazione. L'Ateneo introdurrà percorsi formativi modulari dedicati all'utilizzo avanzato dei sistemi gestionali, alla gestione documentale digitale, ai workflow amministrativi, al reporting tramite strumenti di business intelligence e all'uso efficace dei servizi di cooperazione applicativa. Tali iniziative saranno integrate con attività di assistenza operativa e sessioni di accompagnamento al cambiamento, in collaborazione con le strutture responsabili dei procedimenti, con l'obiettivo di uniformare prassi operative e promuovere modelli di lavoro coerenti con la trasformazione digitale.

Parallelamente verranno introdotte azioni dedicate ai docenti e ai ricercatori, finalizzate allo sviluppo delle competenze necessarie per l'utilizzo delle piattaforme didattiche e degli strumenti istituzionali di gestione della ricerca. I programmi includeranno percorsi sulla didattica digitale, sull'uso avanzato di Moodle e delle tecnologie multimediali, sulla gestione dei contenuti nei sistemi UNORA–IRIS e UniFIND, e su strumenti specialistici per l'analisi linguistica, bibliometrica e documentale. Particolare attenzione sarà dedicata alla corretta gestione dei dati personali degli studenti e all'utilizzo sicuro degli strumenti di collaborazione, in coerenza con le prescrizioni del GDPR e con le misure di sicurezza ICT.

Una terza linea di intervento riguarda lo sviluppo delle competenze digitali delle figure di governo e del management di Ateneo, riconosciute come componente essenziale per l'efficace implementazione della strategia ICT. In questo ambito verranno attivati percorsi specifici dedicati alla governance dei sistemi informativi, alla gestione del rischio cyber, alla compliance normativa (NIS2, GDPR, Linee Guida AgID), alla qualità del dato e alle implicazioni organizzative dell'interoperabilità e dei processi digitali. Tali percorsi saranno progettati per rafforzare la capacità decisionale e consentire un allineamento costante tra scelte strategiche e requisiti tecnologici.

Accanto ai percorsi formativi strutturati, il Piano prevede la realizzazione di un programma continuativo di sensibilizzazione rivolto all'intera comunità universitaria, con campagne tematiche dedicate al contrasto del phishing, alla gestione delle credenziali, ai comportamenti digitali sicuri, all'utilizzo appropriato dei servizi cloud e alla tutela dei dati personali. Saranno

inoltre introdotti materiali di supporto, guide operative, video-tutorial e documentazione consolidata dei servizi digitali, così da ridurre la frammentazione informativa e migliorare l'autonomia degli utenti.

Il Piano prevede inoltre la costituzione di una rete interna di referenti digitali, individuati nelle strutture amministrative e accademiche, con il compito di facilitare la diffusione delle competenze, supportare l'adozione dei nuovi sistemi e fungere da canale di comunicazione tra il Settore Sviluppo Digitale e le unità operative. Questo modello è volto a ridurre il rischio di diseconomia informativa, aumentare la tempestività del supporto e garantire una maggiore coerenza nelle modalità di utilizzo dei servizi.

Una parte delle azioni è specificamente orientata all'inclusione digitale e all'accessibilità, con percorsi dedicati alla creazione di contenuti digitali conformi agli standard WCAG 2.2, alla corretta gestione dei documenti accessibili e alle tecniche di comunicazione digitale istituzionale, in coerenza con il Piano di Comunicazione d'Ateneo.

Infine, il Piano prevede attività di aggiornamento periodico sulle tecnologie emergenti, con particolare attenzione agli strumenti di intelligenza artificiale, all'automazione dei processi, agli assistenti digitali, alle analisi predittive e agli strumenti di supporto decisionale. L'obiettivo è rafforzare la consapevolezza e la capacità di utilizzo responsabile delle tecnologie innovative, assicurando al contempo coerenza con i principi di etica, trasparenza e sostenibilità.

Nel complesso, le azioni del triennio 2026–2028 mirano a costruire un modello stabile, misurabile e coerente di sviluppo delle competenze digitali, capace di accompagnare la trasformazione organizzativa dell'Ateneo e di sostenere l'efficacia dei servizi digitali, la qualità dei processi e la sicurezza dell'intero ecosistema ICT.

10.2 Competenze digitali - Pre-requisiti

L'attuazione delle azioni previste per lo sviluppo delle competenze digitali richiede un insieme di condizioni preliminari, organizzative e operative, che consentano di garantire efficacia, sostenibilità e coerenza del percorso formativo nel triennio 2026–2028. La complessità dei processi digitali in corso, la necessità di standardizzare le pratiche operative e l'eterogeneità dei livelli di alfabetizzazione digitale all'interno dell'Ateneo impongono infatti la definizione di un quadro di prerequisiti chiaro e unitario.

Un primo prerequisito riguarda la disponibilità di un modello stabile di governance delle competenze digitali, che coordini attività formative, fabbisogni delle strutture, processi di change management e iniziative di sensibilizzazione. Tale modello richiede la collaborazione strutturata tra Settore Sviluppo Digitale, Direzione Generale, Ufficio Formazione, Presidio della Qualità, Responsabile della Transizione Digitale (RTD) e Responsabile della Protezione dei Dati (RPD), garantendo una visione integrata degli aspetti tecnologici, organizzativi e normativi. Senza un coordinamento unitario, il rischio è la frammentazione formativa, la duplicazione degli interventi e la dispersione delle competenze acquisite.

Un secondo prerequisito è rappresentato dalla definizione aggiornata dei processi amministrativi e dei modelli organizzativi sui quali le competenze dovranno innestarsi. La digitalizzazione dei procedimenti, se non accompagnata da una chiara identificazione di ruoli, responsabilità e flussi informativi, limita infatti l'efficacia della formazione e riduce la capacità degli utenti di applicare correttamente le competenze acquisite. È pertanto indispensabile disporre di workflow formalizzati, documentazione operativa consolidata e modelli di processo uniformi tra le strutture, così da garantire coerenza e ridurre la variabilità delle prassi interne.

Ulteriore prerequisito riguarda la disponibilità di strumenti tecnologici uniformi e adeguati, sia per la formazione sia per l'operatività quotidiana. La presenza di dotazioni eterogenee, livelli disomogenei di aggiornamento dei software, postazioni di lavoro obsolete o non standardizzate e modalità differenti di accesso ai servizi costituisce un limite significativo alla diffusione delle competenze digitali. La standardizzazione delle postazioni, l'uniformità delle configurazioni, la disponibilità di strumenti cloud aggiornati e l'adozione di policy comuni per la gestione degli endpoint rappresentano condizioni essenziali per assicurare percorsi formativi realmente efficaci.

La piena attuazione del programma richiede inoltre una ricognizione preliminare del livello di competenza digitale dell'utenza, realizzata attraverso strumenti di autovalutazione, analisi dei fabbisogni e confronto con i modelli DigComp, DigCompOrg e DigCompEdu. Questa attività è necessaria per differenziare i percorsi formativi, evitare approcci indistinti e costruire un catalogo di iniziative mirate, calibrate sui differenti profili professionali e accademici.

Un requisito fondamentale è rappresentato dalla disponibilità di un'infrastruttura organizzativa dedicata alla gestione del cambiamento. L'introduzione di nuovi sistemi, workflow digitali, servizi cloud e processi automatizzati richiede infatti presìdi locali che supportino le strutture nelle fasi di transizione. La presenza di referenti digitali interni ai dipartimenti e agli uffici, adeguatamente formati e in collegamento diretto con il Settore Sviluppo Digitale, costituisce una condizione indispensabile per garantire accompagnamento continuo, ridurre le resistenze organizzative e promuovere la diffusione delle competenze.

Infine, l'effettiva implementazione delle azioni previste dal Piano richiede la disponibilità di contenuti formativi aggiornati, materiali didattici accessibili, strumenti di e-learning istituzionali adeguati e un sistema di tracciamento delle attività che consenta di monitorare il livello di partecipazione, l'efficacia formativa e l'evoluzione delle competenze nel tempo. La definizione di criteri di valutazione, indicatori di efficacia e strumenti di certificazione interna delle competenze rappresenta un ulteriore prerequisito per garantire misurabilità e continuità al processo formativo.

Nel complesso, i prerequisiti individuati costituiscono la base operativa e organizzativa necessaria affinché le azioni previste nel triennio 2026–2028 possano produrre un impatto reale e misurabile sull'intera comunità accademica, favorendo una crescita omogenea delle competenze digitali e consolidando la capacità dell'Ateneo di governare il cambiamento tecnologico e organizzativo in modo strutturato, consapevole e sostenibile.

10.3 Competenze digitali – Risorse

La realizzazione delle azioni previste nel triennio 2026–2028 per lo sviluppo delle competenze digitali richiede un insieme articolato di risorse professionali, organizzative, tecnologiche ed economiche. L'Ateneo, pur disponendo oggi di un patrimonio crescente di professionalità interne, presenta ancora margini significativi di rafforzamento, soprattutto nei processi di formazione, accompagnamento al cambiamento e consolidamento delle pratiche operative digitali. La disponibilità, l'allocazione e la continuità delle risorse costituiscono pertanto un fattore abilitante imprescindibile per il successo delle iniziative pianificate.

La principale risorsa del programma è rappresentata dal capitale umano, in particolare dal personale del Settore Sviluppo Digitale, dalle strutture amministrative coinvolte nella digitalizzazione dei processi, dal Responsabile per la Transizione Digitale (RTD), dal Responsabile della Protezione dei Dati (RPD), dall'Ufficio Formazione e dai referenti accademici e

amministrativi delle singole strutture. L'incremento di competenze specialistiche ottenuto negli ultimi anni attraverso procedure concorsuali costituisce una base solida, ma non ancora sufficiente per sostenere in autonomia l'intero volume delle iniziative formative previste. Sarà pertanto necessario integrare il presidio interno attraverso attività di supporto, tutoraggio e affiancamento, privilegiando modelli collaborativi e favorendo la creazione di una rete stabile di referenti digitali.

Accanto alle risorse professionali, il Piano richiede una struttura organizzativa adeguata a sostenere i processi di formazione continua, di diffusione delle competenze e di monitoraggio degli effetti prodotti. Ciò implica la disponibilità di un coordinamento stabile, che operi in sinergia con il Settore Sviluppo Digitale e l'Ufficio Formazione, garantendo l'erogazione di percorsi omogenei, la calendarizzazione delle attività, la gestione degli spazi fisici o virtuali per la formazione e la raccolta sistematica dei feedback. Una parte delle risorse dovrà inoltre essere dedicata al supporto locale nei dipartimenti, nei centri di servizio e negli uffici amministrativi, al fine di affiancare l'utenza nelle fasi di transizione verso i nuovi modelli operativi.

Un'area cruciale riguarda gli strumenti tecnologici necessari per l'erogazione delle attività formative e per la misurazione dei risultati. L'Ateneo dovrà disporre di piattaforme di e-learning aggiornate, ambienti digitali per l'erogazione di webinar e moduli sincroni, sistemi di tracking per monitorare la partecipazione ai corsi e strumenti per la valutazione delle competenze acquisite. La suite Microsoft 365 rappresenta una base già disponibile, ma occorrerà potenziarne l'utilizzo per la didattica interna, integrandola con soluzioni dedicate, con repository centralizzati di contenuti formativi e con strumenti di certificazione interna anche in ottica DigComp.

Per una parte delle attività sarà opportuno ricorrere a risorse economiche dedicate, da destinare a servizi di formazione specialistica, interventi di aggiornamento avanzato, produzione di materiali didattici, supporto professionale e partecipazione del personale a percorsi di qualificazione esterni. Sebbene molte iniziative potranno essere gestite internamente senza oneri aggiuntivi, il raggiungimento degli obiettivi richiede una quota minima di investimenti, necessaria per garantire continuità, qualità e specializzazione delle attività.

Un ulteriore ambito di risorse riguarda la documentazione tecnica e la manualistica operativa, che dovrà essere predisposta e aggiornata per supportare le attività di formazione, facilitare la memorizzazione delle conoscenze e assicurare uniformità nelle prassi operative. La redazione di guide, workflow e modelli standard richiede tempo e competenze specifiche, e rappresenta un investimento indispensabile per consolidare in modo duraturo le competenze acquisite.

Nel complesso, l'attuazione del programma dedicato alle competenze digitali richiede un equilibrio tra risorse interne e supporto specialistico esterno, tra presidio operativo e visione strategica, tra strumenti tecnologici e interventi organizzativi. Solo attraverso la disponibilità coordinata e continuativa di tali risorse sarà possibile realizzare un percorso di potenziamento delle competenze digitali omogeneo, sostenibile e capace di produrre un impatto reale sulla capacità dell'Ateneo di governare la trasformazione digitale nel triennio 2026–2028.

10.4 Competenze digitali – KPI

Il monitoraggio dell'evoluzione delle competenze digitali nel triennio 2026–2028 richiede indicatori affidabili, misurabili e sostenibili, in grado di documentare in modo oggettivo il miglioramento delle capacità dell'utenza, l'efficacia delle azioni formative e l'impatto dei processi di change management. I KPI selezionati rispondono ai principi definiti da AgID, DigComp e PIAO 2025–2027, evitando misurazioni puramente descrittive e privilegiando indicatori verificabili attraverso strumenti e fonti interne all'Ateneo.

KPI 9 - Copertura del personale coinvolto nei percorsi formativi

Definizione: Percentuale del personale tecnico-amministrativo e dei docenti che ha partecipato ad almeno un'attività formativa strutturata sui temi della trasformazione digitale, della sicurezza ICT o della gestione dei processi digitali.

Target 2028: ≥ 60% del personale coinvolto.

KPI10 - Percorsi formativi completati e certificati

Definizione: Numero di percorsi formativi completati dagli utenti e tracciati tramite piattaforme istituzionali (Moodle, M365, sistemi e-learning istituzionali), con rilascio di attestazione interna.

Target 2028: ≥ 500 percorsi formativi fruiti complessivamente nel triennio.

11. Piano attuativo: procurement ICT e sostenibilità

Il procurement ICT rappresenta una componente centrale della governance digitale dell'Università di Napoli L'Orientale e costituisce il meccanismo attraverso il quale l'Ateneo assicura coerenza tecnologica, sostenibilità economica, continuità dei servizi e conformità al quadro normativo nazionale. L'evoluzione del sistema ICT, caratterizzato da un crescente utilizzo di soluzioni cloud, piattaforme esterne e servizi ad alta specializzazione, richiede infatti un modello di approvvigionamento capace di garantire standard comuni, qualità dei prodotti e allineamento alle linee di indirizzo strategiche dell'Ente.

L'Ateneo ha istituito la Centrale di Committenza ICT, disciplinata dal Regolamento per la programmazione e l'approvvigionamento dei beni e servizi informatici e dal relativo Allegato CPV ICT, che definisce i domini tecnologici, le categorie merceologiche e i processi autorizzativi applicabili a tutte le strutture accademiche e amministrative. Tale modello, coordinato dal Settore Sviluppo Digitale in collaborazione con la Direzione Generale, assicura un approccio unitario alle acquisizioni ICT, evitando duplicazioni, frammentazioni e soluzioni non standardizzate, e garantendo la piena osservanza del principio di economicità, trasparenza e coerenza strategica previsto dal D.Lgs. 36/2023.

Il procurement ICT opera in stretta integrazione con i sistemi CINECA (U-Buy, U-Gov Acquisti, U-Gov Contratti), che costituiscono l'infrastruttura digitale attraverso cui sono gestiti i processi di gara, gli ordini, i contratti e le verifiche amministrative. Tale integrazione consente un controllo unificato delle procedure, l'applicazione coerente degli schemi contrattuali, la standardizzazione dei flussi documentali e il tracciamento delle fasi di approvvigionamento, contribuendo a ridurre il rischio operativo e a migliorare la qualità dei processi.

Un ruolo strategico è svolto dal Responsabile della Transizione Digitale (RTD), che garantisce l'allineamento tra approvvigionamenti, architettura dei sistemi, sicurezza informatica e interoperabilità, e che assicura la conformità alle

Linee Guida AgID, al Modello di Interoperabilità, al Codice dell'Amministrazione Digitale e agli obblighi di sicurezza previsti dalla Direttiva NIS2. La sua funzione di supervisione consente di prevenire scelte non coerenti con l'ecosistema digitale dell'Ateneo e di assicurare che ogni acquisizione contribuisca alla sostenibilità tecnologica complessiva.

Il tema della sostenibilità è declinato in tre dimensioni: ambientale, tecnologica ed economico-organizzativa. La sostenibilità ambientale è garantita dall'applicazione dei Criteri Ambientali Minimi (CAM) nelle forniture ICT e dall'adozione di strumenti a basso consumo energetico, nonché da percorsi di razionalizzazione delle postazioni obsolescenti, riduzione dell'hardware locale e migrazione verso servizi cloud maggiormente efficienti. La sostenibilità tecnologica è perseguita attraverso la standardizzazione delle piattaforme, la riduzione della frammentazione applicativa, la gestione del ciclo di vita delle tecnologie e la definizione di criteri comuni per sicurezza, interoperabilità e qualità. La sostenibilità economico-organizzativa è assicurata attraverso la pianificazione triennale degli acquisti ICT, integrata con il budget, con la programmazione del PIAO e con gli obiettivi del Piano Strategico, riducendo il ricorso a spese impreviste, a soluzioni isolate o a forniture non coerenti con le priorità dell'Ente.

Nel complesso, il modello di procurement ICT adottato dall'Ateneo consente di garantire una visione unitaria delle acquisizioni, un controllo efficace dei processi, una maggiore sostenibilità nel ciclo di vita delle tecnologie e un utilizzo più efficiente delle risorse economiche. Esso rappresenta uno dei pilastri fondamentali per sostenere l'evoluzione dell'ecosistema digitale nel triennio 2026–2028, assicurando che ogni investimento tecnologico contribuisca in modo coerente alla trasformazione digitale dell'Ateneo.

11.1 Procurement ICT e sostenibilità - Azioni 2026-2028

Nel triennio 2026–2028, il procurement ICT dell'Università di Napoli "L'Orientale" sarà orientato al consolidamento della Centrale di Committenza ICT, alla piena integrazione con le piattaforme digitali di gestione degli acquisti e all'adozione di modelli di sostenibilità tecnologica coerenti con le linee guida nazionali. Le azioni previste mirano a rafforzare la capacità dell'Ateneo di programmare in modo unitario le acquisizioni, ridurre la frammentazione delle soluzioni digitali, garantire la coerenza con gli standard AgID e NIS2 e migliorare l'efficienza economica e organizzativa delle forniture ICT.

Una priorità strategica è rappresentata dal consolidamento della Centrale di Committenza ICT come unico presidio di governo degli approvvigionamenti tecnologici. Nel triennio si prevede il completamento e l'aggiornamento periodico dell'Allegato CPV ICT, la definizione delle categorie merceologiche emergenti (cloud, API management, cybersecurity, strumenti di IA), e l'adozione di un modello di valutazione preventiva che assicuri la coerenza delle richieste delle strutture con l'architettura ICT d'Ateneo. Questo processo rafforzerà l'unitarietà delle scelte tecnologiche e limiterà il rischio di acquisizioni incoerenti o ridondanti.

Parallelamente, il Piano prevede il rafforzamento dell'integrazione tra procurement ICT e programmazione strategica, assicurando l'allineamento con il PIAO, con gli obiettivi del RTD e con la pianificazione del Settore Sviluppo Digitale. Tale allineamento consentirà di anticipare i fabbisogni tecnologici, programmare gli investimenti pluriennali e garantire che le risorse economiche siano allocate in modo equilibrato tra manutenzione evolutiva, innovazione e sicurezza informatica. Una particolare attenzione sarà dedicata alla definizione di procedure per la valutazione dell'impatto delle nuove acquisizioni sui sistemi esistenti, sulla sicurezza e sulla qualità del patrimonio informativo.

Le azioni del triennio includono inoltre il potenziamento dei processi digitali di acquisizione, attraverso l'uso esteso delle piattaforme CINECA (U-Buy, U-Gov Acquisti, U-Gov Contratti) e la standardizzazione dei flussi documentali. L'obiettivo è garantire un sistema di procurement pienamente tracciabile, conforme alle prescrizioni del Codice dei Contratti Pubblici e integrato con i sistemi di gestione documentale, assicurando uniformità operativa e maggiore trasparenza.

Un asse di intervento fondamentale riguarda la sostenibilità tecnologica delle forniture ICT, elemento oggi indispensabile per contenere i costi di esercizio, prevenire l'obsolescenza e garantire coerenza architetturale. Nel triennio si prevede l'adozione di criteri di valutazione basati sul ciclo di vita delle tecnologie, sulla possibilità di riuso, sulla compatibilità con gli standard di interoperabilità e sulla scalabilità dei servizi. Saranno inoltre introdotte linee guida per la razionalizzazione delle postazioni di lavoro e per la riduzione delle soluzioni applicative isolate, favorendo modelli cloud e SaaS maggiormente sostenibili.

La sostenibilità ambientale rappresenta un ulteriore ambito di attenzione. L'Ateneo estenderà l'applicazione dei Criteri Ambientali Minimi (CAM) alle forniture ICT, promuovendo l'acquisto di dispositivi a basso consumo energetico, la riduzione dei materiali di scarto e il ricorso a soluzioni che ottimizzino l'utilizzo delle risorse hardware e la durata delle attrezzature. Il procurement ICT sarà inoltre orientato al contenimento dell'impatto ambientale, favorendo l'adozione di tecnologie virtualizzate e la riduzione dell'hardware obsoleto.

Infine, il Piano prevede l'introduzione di strumenti di monitoraggio continuo delle forniture ICT, finalizzati a valutare l'efficacia delle acquisizioni, verificare il rispetto dei requisiti tecnici, misurare la durata del ciclo di vita delle tecnologie e individuare tempestivamente eventuali criticità. Tale attività si integrerà con il sistema di governance ICT e con i processi di controllo strategico, contribuendo a migliorare la qualità delle decisioni e la sostenibilità complessiva degli investimenti.

11.2 Procurement ICT e sostenibilità - Pre-requisiti

La piena attuazione delle azioni previste nel triennio 2026–2028 in materia di procurement ICT e sostenibilità richiede un insieme di prerequisiti organizzativi, normativi, tecnologici e procedurali che consentano all'Ateneo di governare in modo unitario i processi di approvvigionamento, sostenere le scelte strategiche e garantire la coerenza con gli standard nazionali. Tali prerequisiti sono indispensabili per evitare frammentazioni, duplicazioni di spesa, rischi di non conformità e scelte tecnologiche non allineate all'evoluzione dell'ecosistema digitale dell'Università.

Un prerequisito essenziale è rappresentato dalla piena operatività della Centrale di Committenza ICT, che deve essere riconosciuta come unico presidio di controllo e coordinamento delle acquisizioni informatiche dell'Ateneo. La sua efficacia richiede la disponibilità di procedure formalizzate, istruzioni operative aggiornate, criteri valutativi condivisi e un'interazione strutturata con il Settore Sviluppo Digitale per la verifica della coerenza tecnico-architetturale delle richieste. L'assenza di tale quadro comporterebbe il rischio di approvvigionamenti eterogenei, di soluzioni non standard e di processi non conformi al D.Lgs. 36/2023.

La piena applicazione delle politiche di procurement ICT richiede inoltre un allineamento stabile con la programmazione triennale dell'Ateneo. L'integrazione tra Centrale di Committenza ICT, RTD, Settore Sviluppo Digitale, Direzione Generale e strutture accademiche rappresenta un prerequisito fondamentale per assicurare che il fabbisogno tecnologico sia valutato in un'ottica complessiva, non frammentata. Ciò include il raccordo con il PIAO, con il Piano delle Performance,

con la programmazione degli investimenti e con i cicli di bilancio, evitando interventi emergenziali o non pianificati che potrebbero compromettere la sostenibilità finanziaria e la coerenza delle scelte.

Ulteriore prerequisito riguarda la definizione di criteri comuni di valutazione tecnica e sostenibilità delle forniture ICT. È necessario predisporre un set condiviso di requisiti minimi riguardanti sicurezza, interoperabilità, accessibilità, qualità dei dati, ciclo di vita delle tecnologie e compatibilità con gli standard AgID e NIS2. L'adozione di tali criteri costituisce una condizione indispensabile per garantire processi di selezione trasparenti, comparabili e orientati alla riduzione della frammentazione tecnologica.

La piena attuazione delle politiche di sostenibilità richiede inoltre la disponibilità di dati strutturati sul ciclo di vita delle tecnologie, sulla durata delle forniture, sui contratti in essere, sulla spesa storica ICT e sulla gestione delle manutenzioni. Queste informazioni, integrate attraverso CINECA (U-Buy, U-Gov Acquisti, Contratti), rappresentano il prerequisito per una programmazione triennale fondata su evidenze, per la definizione di criteri di sostituzione delle dotazioni obsolete e per la valutazione della sostenibilità economica e ambientale delle soluzioni.

Un prerequisito strategico riguarda la standardizzazione delle architetture ICT e dei modelli applicativi. La capacità dell'Ateneo di valutare correttamente la coerenza tecnologica delle richieste dipende dalla presenza di un quadro architetturale condiviso, che definisca piattaforme preferenziali, criteri di integrazione, limiti alle soluzioni sviluppate in autonomia e requisiti minimi per sicurezza, interoperabilità e qualità dei dati. Senza tale standardizzazione, la Centrale di Committenza ICT non può svolgere pienamente il proprio ruolo di presidio tecnico e strategico.

La sostenibilità delle forniture ICT richiede inoltre la piena applicazione dei Criteri Ambientali Minimi (CAM), che rappresentano un obbligo normativo e un requisito essenziale per garantire il rispetto degli obiettivi di efficienza energetica e riduzione dell'impatto ambientale previsti dai piani nazionali. La loro adozione richiede la disponibilità di specifiche tecniche aggiornate, modelli di documentazione di gara e procedure di verifica dei requisiti in fase di aggiudicazione ed esecuzione.

Infine, la realizzazione delle azioni del triennio richiede un prerequisito organizzativo cruciale: la formazione del personale coinvolto nei processi di gara. La complessità crescente delle forniture ICT, la transizione verso modelli cloud e SaaS, l'introduzione di obblighi NIS2 e la necessità di valutare impatti su sicurezza, interoperabilità e qualità dei dati rendono indispensabile un rafforzamento delle competenze interne, sia nelle strutture amministrative sia nei presìdi tecnici.

I prerequisiti descritti rappresentano la condizione sine qua non per garantire che il procurement ICT si sviluppi in modo adeguato con la strategia digitale dell'Ateneo, con le esigenze di sostenibilità e con le prescrizioni normative nazionali, assicurando efficienza, trasparenza e sostenibilità nel ciclo di vita delle tecnologie adottate.

11.3 Procurement ICT e sostenibilità – Risorse

L'attuazione delle azioni previste per il procurement ICT e la sostenibilità nel triennio 2026–2028 richiede la disponibilità coordinata di risorse professionali, organizzative, tecnologiche ed economiche. La complessità crescente del panorama normativo, l'evoluzione delle architetture digitali dell'Ateneo e la progressiva centralizzazione dei processi di approvvigionamento rendono indispensabile un rafforzamento strutturato dei presìdi interni e un investimento continuo in competenze e strumenti.

La principale risorsa del sistema di procurement ICT è rappresentata dal capitale umano, in particolare dal personale del Settore Sviluppo Digitale, dalla Centrale di Committenza ICT, dai presìdi amministrativi coinvolti nei processi di gara e dai referenti tecnici delle strutture. Sebbene l'Ateneo abbia avviato un percorso di rafforzamento di tali presìdi, l'elevata specializzazione richiesta dalle forniture ICT – soprattutto in ambiti come cloud computing, interoperabilità, cybersecurity, intelligenza artificiale e garanzie contrattuali – impone un investimento mirato in aggiornamento professionale e affiancamento tecnico. Per garantire la piena coerenza delle valutazioni tecniche e la sostenibilità delle scelte, sarà necessario consolidare i raccordi operativi tra Settore Sviluppo Digitale, Direzione Generale, Ufficio Gare e appalti e strutture utilizzatrici.

Accanto alle risorse professionali, sono essenziali risorse organizzative dedicate al funzionamento della Centrale di Committenza ICT. Questa struttura necessita di procedure uniformi, documentazione operativa aggiornata, workflow integrati con CINECA e strumenti per la verifica di coerenza tecnica delle richieste provenienti dalle strutture. L'efficienza del procurement dipende inoltre dalla disponibilità di un sistema di coordinamento stabile con il RTD, che garantisca l'allineamento delle acquisizioni ai requisiti di sicurezza, interoperabilità e architettura ICT, evitando il rischio di soluzioni non conformi o non sostenibili nel medio periodo.

Una componente rilevante riguarda le risorse tecnologiche, necessarie per supportare l'intero ciclo di vita delle forniture ICT. L'Ateneo deve poter contare su sistemi di procurement digitali affidabili, pienamente integrati con U-Buy, U-Gov Acquisti e U-Gov Contratti, così da assicurare tracciabilità, trasparenza e standardizzazione delle procedure. Strumenti di analytics e reporting sono indispensabili per monitorare la spesa ICT, analizzare le ricorrenze, individuare inefficienze e programmare gli investimenti con una visione pluriennale. La disponibilità di un sistema centralizzato di documentazione tecnica e contrattuale rappresenta inoltre una risorsa fondamentale per garantire continuità nelle decisioni e ridurre il rischio di frammentazione informativa.

Il procurement ICT, inoltre, richiede risorse economiche dedicate, necessarie non solo per l'acquisizione di beni e servizi ma anche per la gestione del loro ciclo di vita, per gli aggiornamenti evolutivi e per le attività di supporto e manutenzione. La sostenibilità economica delle scelte richiede la pianificazione di un budget triennale coerente, che consideri non solo il costo di acquisizione ma anche il Total Cost of Ownership (TCO), ossia i costi complessivi della tecnologia nel suo intero ciclo di vita. Gli investimenti in ambiti strategici – tra cui sicurezza informatica, cloud, continuità operativa e infrastrutture di rete – richiedono un impegno economico programmato e non episodico, accompagnato da un monitoraggio continuativo delle ricadute organizzative e tecnologiche.

Infine, un fattore critico per la sostenibilità delle forniture ICT riguarda le risorse documentali e regolamentari. L'efficacia del procurement dipende dalla disponibilità di specifiche tecniche standard, capitolati-tipo, griglie di valutazione, modelli di requisiti minimi, tabelle CPV aggiornate e linee guida per la conformità a sicurezza, interoperabilità, accessibilità e CAM. La costruzione e l'aggiornamento di questo patrimonio documentale richiede competenze tecniche e giuridiche integrate, indispensabili per garantire uniformità, qualità e aderanza alle prescrizioni normative nazionali ed europee.

Nel complesso, il sistema di procurement ICT richiede un investimento continuativo in risorse professionali, organizzative, tecnologiche ed economiche per operare in modo stabile, coerente e strategico. Solo attraverso la disponibilità di tali

risorse sarà possibile assicurare sostenibilità tecnologica, riduzione dei rischi, razionalizzazione della spesa pubblica e pieno allineamento del processo di approvvigionamento con la strategia digitale dell'Ateneo.

11.4 Procurement ICT e sostenibilità: Adozione dei Criteri Ambientali Minimi (CAM ICT)

L'adozione dei Criteri Ambientali Minimi (CAM) rappresenta un elemento strutturale della sostenibilità nelle forniture ICT dell'Università di Napoli L'Orientale ed è obbligatoria ai sensi della normativa nazionale in materia di contratti pubblici. L'applicazione dei CAM ICT risponde infatti agli indirizzi del Ministero dell'Ambiente e della Sicurezza Energetica, alle previsioni del D.Lgs. 36/2023, ai principi di sostenibilità del PNRR e ai requisiti di responsabilità ambientale della Pubblica Amministrazione.

Nel triennio 2026–2028, l'Ateneo intende consolidare un modello di approvvigionamento ICT pienamente conforme ai CAM, garantendo la loro applicazione integrale in tutte le procedure di gara e nelle acquisizioni in convenzione aventi ad oggetto apparecchiature informatiche, servizi digitali e forniture connesse. Il rispetto dei CAM costituisce un requisito non solo normativo ma anche strategico, poiché consente di ridurre l'impatto ambientale delle tecnologie, migliorare l'efficienza energetica delle dotazioni, ottimizzare il ciclo di vita dei dispositivi e promuovere pratiche di acquisto sostenibile.

L'Ateneo prevede di integrare i CAM ICT in tutte le fasi del processo di procurement: dalla definizione delle specifiche tecniche alla predisposizione della documentazione di gara, dalla valutazione dell'offerta alla verifica di conformità in fase di esecuzione. A tal fine, la Centrale di Committenza ICT predisporrà capitolati-tipo e schede tecniche standardizzate contenenti i requisiti ambientali obbligatori per le diverse categorie di prodotti e servizi, assicurando uniformità e riducendo il rischio di inadempienze.

Parallelamente, saranno adottati criteri premiali volti a favorire soluzioni a minore impatto ambientale, apparecchiature a più elevata efficienza energetica, servizi cloud con certificazioni di sostenibilità, politiche di riduzione dei materiali di scarto e pratiche di riuso o rigenerazione delle apparecchiature. L'applicazione dei CAM ICT sarà inoltre accompagnata da attività di monitoraggio e verifica, integrate nei processi di controllo qualità del procurement e nei sistemi di tracciabilità delle forniture.

L'introduzione sistematica dei CAM ICT contribuisce a promuovere un modello di sostenibilità ambientale coerente con la strategia digitale dell'Ateneo, riducendo l'impatto ecologico delle tecnologie, migliorando la durata dei dispositivi e garantendo l'allineamento agli obblighi normativi. Essa costituisce un elemento qualificante del procurement ICT e un presupposto per la crescita responsabile e sostenibile dell'infrastruttura digitale dell'Università.

11.5 Procurement ICT e sostenibilità – KPI

Il monitoraggio del procurement ICT nel triennio 2026–2028 si fonda su un insieme di indicatori che consentono di valutare la coerenza delle acquisizioni con il modello di governance dell'Ateneo, la sostenibilità tecnologica delle forniture, l'allineamento ai criteri ambientali minimi e la capacità dell'Ente di programmare in modo unitario gli investimenti digitali. I KPI selezionati rispondono ai principi AgID, ai requisiti del Codice dei Contratti Pubblici e agli standard di sostenibilità tecnologica richiesti dalla trasformazione digitale, evitando indicatori meramente quantitativi e privilegiando misure verificabili e con un impatto strategico concreto.

KPI11 - Conformità ai Criteri Ambientali Minimi (CAM) nelle forniture ICT

Definizione: Percentuale delle forniture ICT per le quali risultano applicati e verificati i Criteri Ambientali Minimi previsti dalla normativa vigente.

Target 2026: ≥ 85%.

KPI12 - Percentuale di contratti ICT con clausole SLA/OLA

Definizione: Percentuale di contratti ICT (hardware, software, SaaS, cloud) contenenti clausole su livelli di servizio minimi (SLA) e obblighi del fornitore (OLA).

Target 2028: ≥ 90%.

12. Piano attuativo: intelligenza artificiale e innovazione

L'intelligenza artificiale rappresenta uno dei principali fattori abilitanti della trasformazione digitale dell'Università di Napoli L'Orientale e costituisce un ambito strategico di innovazione per la didattica, la ricerca, i servizi digitali e i processi amministrativi. Nel triennio 2026–2028, l'Ateneo intende sviluppare un modello di adozione dell'IA fondato su criteri di sicurezza, trasparenza, affidabilità, equità, sostenibilità e rispetto delle normative europee e nazionali, in particolare del Regolamento Europeo sull'IA (AI Act), delle Linee Guida AgID sulle tecnologie emergenti e del Decalogo AgID per l'intelligenza artificiale nella Pubblica Amministrazione.

L'Ateneo parte da un contesto in cui le tecnologie di IA non sono ancora integrate in modo sistematico nei processi istituzionali, ma sono già presenti in forma embrionale in attività di supporto alla didattica, strumenti di ricerca linguistica e sperimentazioni progettuali condotte da singole strutture accademiche. Tale scenario rende necessario un modello di governance che assicuri coerenza, controllo, conformità normativa e una visione unitaria delle applicazioni potenziali dell'IA.

Il Piano si propone di orientare l'adozione dell'intelligenza artificiale verso soluzioni che migliorino la qualità dei servizi, riducano gli oneri amministrativi, supportino la produzione e l'analisi del patrimonio informativo dell'Ateneo e favoriscano l'innovazione nei processi accademici e nella ricerca. In questa prospettiva, l'IA deve essere intesa non come un semplice strumento tecnologico, ma come un cambiamento organizzativo che incide sulla progettazione dei processi, sulla governance dei dati, sulla sicurezza informatica e sulle competenze digitali degli utenti.

Il percorso di adozione dell'IA richiede particolare attenzione agli aspetti etici, alla protezione dei dati personali, alle responsabilità decisionali e al rischio di bias algoritmici. Il ruolo del Responsabile della Protezione dei Dati (RPD), del Responsabile per la Transizione Digitale (RTD) e del Settore Sviluppo Digitale assume pertanto una rilevanza cruciale nel definire criteri di selezione, valutazione d'impatto, supervisione e monitoraggio dei sistemi basati su IA, in piena conformità con il quadro europeo e nazionale. Tali presidi sono indispensabili per prevenire l'utilizzo improprio delle tecnologie, garantire trasparenza nelle decisioni automatizzate e assicurare che l'IA sia impiegata in modo responsabile, spiegabile e verificabile.

La finalità del Piano non è diffondere indiscriminatamente soluzioni di intelligenza artificiale, ma individuare ambiti specifici in cui tali tecnologie possano produrre valore, migliorare l'efficienza, supportare l'analisi e la qualità dei dati, rafforzare la

ricerca e contribuire all'innovazione dei servizi digitali. La roadmap operativa prevede l'introduzione di strumenti di automazione, l'avvio di progetti pilota, la sperimentazione in ambito amministrativo, l'adozione di strumenti di IA generativa per il supporto alla didattica e ai processi informativi, la costruzione di modelli predittivi per la programmazione istituzionale e la valorizzazione del patrimonio digitale.

Nel complesso, il Piano attuativo in materia di IA e innovazione intende guidare l'Ateneo verso un utilizzo consapevole, sicuro e strategico delle tecnologie emergenti, in grado di sostenere l'evoluzione dell'ecosistema istituzionale e di garantire un approccio responsabile, trasparente e orientato al miglioramento continuo dei processi, in piena coerenza con il quadro normativo europeo e nazionale e con i principi del Decalogo AgID.

12.1 Intelligenza artificiale e innovazione - Azioni 2026-2028

L'attuazione delle politiche di intelligenza artificiale dell'Università di Napoli L'Orientalesi fonda sul mandato istituzionale attribuito al Gruppo di lavoro IA, costituito con Decreto Rettorale, che ha il compito di elaborare linee guida, definire policy d'Ateneo, proporre progetti autosostenibili e valutare rischi, impatti ed esigenze organizzative connesse all'adozione delle tecnologie IA. Tale gruppo opererà in raccordo con il Responsabile della Transizione Digitale, con il RPD e con le strutture accademiche e amministrative per garantire un approccio responsabile, conforme e pienamente allineato alle normative europee e nazionali.

Nel triennio 2026–2028, il Piano prevede l'avvio di una serie di azioni strategiche finalizzate a introdurre l'intelligenza artificiale in modo controllato, trasparente e orientato alla qualità dei processi e dei servizi. Una prima azione riguarda la definizione e l'approvazione della Policy di Ateneo sull'Intelligenza Artificiale, che rappresenta l'atto fondativo per disciplinare modalità d'uso, limitazioni, responsabilità, ambiti autorizzati e divieti relativi alle tecnologie IA da parte di studenti, docenti, ricercatori e personale tecnico-amministrativo. Tale documento, redatto dal Gruppo di lavoro IA, costituirà la cornice normativa interna per tutte le successive sperimentazioni e dovrà essere coerente con l'AI Act, con la Legge 132/2025 e con il Decalogo AgID.

Parallelamente, sarà elaborato un pacchetto di Linee Guida operative, distinte per categorie di utenti, che definiranno:

- le modalità di interazione con strumenti di IA generativa;
- le regole su citazione, trasparenza e integrità accademica;
- i criteri per l'adozione nella didattica;
- le procedure di valutazione dei rischi etici;
- gli standard di anonimizzazione dei dati;
- le responsabilità dei docenti nell'uso dell'IA nelle valutazioni.

Una seconda linea d'azione riguarda l'avvio di progetti pilota autosostenibili, verificati e selezionati dal Gruppo di lavoro IA, riguardanti:

- automazione dei processi amministrativi attraverso modelli linguistici;
- assistenti digitali per studenti e docenti;
- analisi predittive per la programmazione strategica (es. abbandoni, flussi di immatricolazione);
- strumenti linguistici avanzati e modelli NLP a supporto della ricerca;

- applicazioni per la valorizzazione del patrimonio digitale d'Ateneo (DH & BIMA).

Una terza azione riguarda la creazione di un processo di valutazione dell'impatto (AIA AI Impact Assessment) per ogni applicazione IA che l'Ateneo intenda adottare o sviluppare. Tale processo sarà condotto congiuntamente dal Gruppo di lavoro, dal RTD e dal RPD, e comprenderà:

- analisi di rischio algoritmico, etico e privacy;
- classificazione del sistema secondo le categorie dell'AI Act;
- verifica dei requisiti di sicurezza e governance dei dati;
- definizione delle misure di mitigazione.

Il Piano prevede inoltre la realizzazione di un catalogo dei casi d'uso IA dell'Ateneo, che raccoglierà sperimentazioni, servizi attivi e progetti in valutazione, favorendo trasparenza, conoscenza interna e allineamento con la governance ICT. Particolare attenzione sarà dedicata all'adozione di soluzioni IA per la comunicazione istituzionale, la gestione dei flussi informativi, la redazione assistita e il supporto ai processi di traduzione e revisione linguistica, nel pieno rispetto del Codice Etico.

Infine, saranno avviate iniziative di formazione e sensibilizzazione sull'IA responsabile, rivolte a tutte le categorie di utenti, con moduli specifici su:

- etica dell'IA;
- rischi e limiti delle tecnologie generative;
- uso corretto dei modelli nei processi didattici;
- tutela dei dati personali e anonimizzazione;
- prevenzione dei bias e delle decisioni automatizzate non trasparenti.

Queste azioni, integrate in una roadmap progressiva e sostenibile, guidano l'Ateneo verso un'adozione responsabile, controllata e innovativa dell'intelligenza artificiale, rafforzando il ruolo dell'Università come istituzione capace di governare consapevolmente le tecnologie emergenti nel rispetto dei principi etici, della qualità accademica e della normativa vigente.

12.2 Intelligenza artificiale e innovazione - Pre-requisiti

L'adozione dell'intelligenza artificiale nell'Università di Napoli L'Orientalerichiede la definizione preliminare di un insieme di pre-requisiti normativi, organizzativi, tecnici ed etici che costituiscono il quadro di riferimento indispensabile per un'implementazione responsabile, sicura e coerente con gli standard europei e nazionali. Tali precondizioni derivano dal quadro regolatorio vigente – in particolare l'AI Act (Regolamento UE 2024/1689), la Legge n. 132/2025, il GDPR, il Codice dell'Amministrazione Digitale e le Linee Guida AgID – e sono rafforzate dal mandato istituzionale attribuito al Gruppo di lavoro IA dell'Ateneo.

Un primo pre-requisito riguarda la definizione e l'approvazione della Policy di Ateneo sull'Intelligenza Artificiale, che stabilisce principi, limiti, responsabilità, requisiti di trasparenza, criteri di utilizzo consentito e processi di autorizzazione per studenti, docenti, ricercatori e personale tecnico-amministrativo. La policy costituisce il fondamento regolatorio per ogni iniziativa legata all'IA e definisce l'architettura di governance, in coerenza con i principi di eticità, non discriminazione, affidabilità e accountability imposti dall'AI Act.

Accanto alla policy, il Piano richiede la predisposizione di un insieme organico di Linee Guida operative che dettaglino modalità d'interazione con strumenti generativi, tecniche di citazione e disclosure dell'uso dell'IA, standard per la produzione e valutazione accademica, regole per l'utilizzo nelle attività di ricerca e requisiti per i materiali didattici prodotti o assistiti da IA. Tali Linee Guida, elaborate dal Gruppo di lavoro IA, rappresentano il presupposto necessario per garantire un uso corretto e culturalmente maturo delle tecnologie da parte della comunità universitaria.

Un ulteriore pre-requisito è la disponibilità di un modello strutturato di governance dei dati, poiché l'adozione dell'IA richiede basi dati affidabili, coerenti e trattate nel pieno rispetto della normativa privacy. Come previsto dal decreto istitutivo del Gruppo IA, "i dati richiesti e usati dovranno sempre essere preventivamente anonimizzati" : tale vincolo rende indispensabile la definizione di procedure uniformi di anonimizzazione, pseudonimizzazione, data minimization, valutazione del rischio e tracciabilità dei dataset impiegati nei progetti IA.

L'attivazione di soluzioni IA richiede inoltre l'istituzione di un processo di valutazione dell'impatto (AI Impact Assessment), da applicare a ogni progetto, sperimentazione o servizio che incorpori componenti algoritmiche. Tale processo – sviluppato congiuntamente da Gruppo IA, RTD e RPD – comprende la classificazione del sistema secondo le categorie del Regolamento europeo (basso rischio, rischio limitato, alto rischio), la valutazione di bias e rischi etici, la verifica delle fonti dati, la definizione delle misure di mitigazione e la stima dell'impatto sui diritti degli utenti.

Sul piano tecnico, l'Ateneo deve dotarsi di un ambiente di esecuzione controllato, che includa:

- infrastrutture sicure per l'elaborazione dei modelli;
- ambienti separati per sperimentazione e produzione;
- log di tracciabilità e auditing;
- sistemi per il controllo degli accessi;
- strumenti di monitoraggio delle prestazioni e delle anomalie.

Queste componenti sono indispensabili per garantire sicurezza, affidabilità e rispetto dei requisiti ACN e NIS2 anche per soluzioni basate su modelli linguistici o sistemi predittivi.

Un ulteriore pre-requisito è rappresentato dalla definizione di un catalogo dei casi d'uso ammessi, coerenti con il mandato del Gruppo IA e con le priorità dell'Ateneo. Il catalogo consente di evitare sperimentazioni isolate, ridurre il rischio di pratiche non autorizzate e assicurare che ogni iniziativa sia valutata in termini di sostenibilità, impatto e compliance normativa.

Infine, la piena attuazione delle iniziative IA richiede il consolidamento di competenze interne attraverso la formazione del personale tecnico-amministrativo, dei docenti e dei ricercatori, la sensibilizzazione etica della comunità universitaria e la costruzione di un modello di change management che sostenga l'evoluzione organizzativa. Senza adeguate competenze, nessuna innovazione tecnologica può essere adottata in modo consapevole, sicuro e conforme.

Nel loro complesso, questi pre-requisiti definiscono la cornice organizzativa, normativa e tecnica necessaria per garantire che l'intelligenza artificiale sia introdotta nell'Ateneo in modo responsabile e trasparente rispondente ai valori istituzionali e alla normativa vigente. Essi rappresentano la condizione preliminare e imprescindibile per ogni azione prevista dalla roadmap triennale di innovazione.

12.3 Intelligenza artificiale e innovazione – Risorse

L'attuazione delle iniziative dedicate all'intelligenza artificiale e all'innovazione richiede un insieme articolato di risorse organizzative, tecniche, professionali ed economiche che devono operare in modo coordinato per garantire un'adozione responsabile, sicura e coerente con il quadro normativo nazionale ed europeo. L'Ateneo possiede già una base significativa, ma la complessità dell'IA impone un rafforzamento mirato delle infrastrutture, delle competenze e dei presìdi di governance, affinché i progetti avviati nel triennio 2026–2028 possano essere sostenibili, tracciabili e pienamente integrati nei processi istituzionali.

Sotto il profilo organizzativo, un ruolo centrale è svolto dal Gruppo di lavoro sull'Intelligenza Artificiale, istituito con apposito decreto rettorale e dotato di una composizione multidisciplinare che include competenze informatiche, giuridiche, linguistiche, statistiche e organizzative. Tale organo, cui è affidato il compito di elaborare linee guida, supportare le strutture accademiche e amministrative e garantire la conformità alle prescrizioni normative ed etiche, rappresenta il fulcro della governance dell'IA d'Ateneo, e deve poter contare su un coordinamento costante con il Responsabile per la Transizione Digitale, con il Responsabile della Protezione dei Dati e con il Settore Sviluppo Digitale. La collaborazione strutturata di questi presìdi garantisce coerenza nella valutazione dei trattamenti, nell'analisi dei rischi, nella definizione delle policy e nella supervisione degli impatti organizzativi dei progetti di IA.

La realizzazione dei progetti richiede anche risorse tecniche adeguate. L'Ateneo necessita di ambienti di sviluppo e test dedicati, capaci di ospitare modelli linguistici, strumenti di automazione documentale e applicazioni predittive in condizioni di sicurezza e isolamento, conformemente alle indicazioni contenute nel decreto istitutivo del Gruppo IA, che prescrive l'uso di dataset anonimizzati e misure idonee a prevenire la re-identificazione. Diventa inoltre necessario disporre di un'infrastruttura computazionale scalabile, integrata con i servizi cloud offerti tramite convenzioni istituzionali, nonché di strumenti di auditing, monitoraggio e controllo che assicurino tracciabilità e verificabilità delle elaborazioni effettuate dai modelli. Alla stessa maniera, la gestione dei dati deve essere sostenuta da repository sicuri, da processi di anonimizzazione e da sistemi che garantiscano il versioning dei modelli e la loro validazione periodica, a tutela dell'affidabilità e della qualità dei risultati.

Accanto agli aspetti tecnici, rivestono particolare importanza le risorse professionali. L'adozione dell'intelligenza artificiale richiede competenze specialistiche che, pur presenti in Ateneo, devono essere consolidate e ampliate attraverso percorsi strutturati di formazione. Sono necessarie professionalità in grado di progettare, addestrare e valutare modelli, di gestire dataset complessi, di interpretare gli impatti organizzativi e giuridici delle tecnologie emergenti, di valutare i rischi legati ai bias algoritmici e di assicurare coerenza con il GDPR, con l'AI Act e con le future linee guida dell'Agenzia per la Cybersicurezza Nazionale. Allo stesso tempo, risulta fondamentale sostenere lo sviluppo delle competenze digitali diffuse tra docenti, ricercatori e personale tecnico-amministrativo, affinché l'utilizzo dell'IA non rimanga confinato a progetti sperimentali, ma diventi un fattore abilitante dei processi dell'Ateneo.

Le risorse economiche costituiscono l'ultimo elemento critico del modello attuativo. L'implementazione dei progetti di IA richiede investimenti specifici per l'acquisizione di tecnologie, il potenziamento dell'infrastruttura, l'adozione di strumenti cloud, l'aggiornamento professionale e il supporto specialistico necessario nelle fasi di progettazione, trial, validazione e diffusione. Tali risorse dovranno essere previste all'interno del budget ICT e integrate, ove possibile, da finanziamenti

derivanti da bandi competitivi, iniziative nazionali e collaborazioni istituzionali. L'Ateneo dovrà inoltre assicurare un adeguato sostegno economico al funzionamento del Gruppo IA e alle attività di governance, affinché il presidio etico, giuridico e tecnico dell'innovazione possa operare con continuità.

12.4 Intelligenza artificiale e innovazione – KPI

Il monitoraggio delle iniziative dedicate all'intelligenza artificiale e all'innovazione richiede indicatori specifici, capaci di misurare non soltanto l'adozione di strumenti tecnologici, ma soprattutto la capacità dell'Ateneo di sviluppare un modello di governance solido, responsabile e conforme al quadro normativo in rapida evoluzione. A differenza di altri ambiti più maturi, l'IA non può essere valutata esclusivamente sulla base di output immediatamente quantificabili: ciò che assume rilevanza strategica nel triennio 2026–2028 è la progressiva costruzione delle condizioni organizzative, metodologiche e tecniche che permetteranno all'Ateneo di utilizzare tali tecnologie in modo sicuro, controllato e sostenibile.

In questo senso, i KPI individuati riflettono un approccio orientato alla "capacity building": misurano la definizione di linee guida, la messa a regime dei processi autorizzativi, la capacità di documentare e valutare i trattamenti automatizzati, la realizzazione di prototipi controllati e la progressiva diffusione delle competenze interne. Si tratta di indicatori coerenti con il mandato del Gruppo di lavoro sull'Intelligenza Artificiale, con le prescrizioni dell'AI Act europeo, con le raccomandazioni del Decalogo AgID e con i principi di etica, trasparenza e accountability richiamati nel decreto istitutivo.

KPI14 - Adozione del quadro regolatorio interno per l'IA

Definizione: Numero degli atti regolamentari previsti (Linee guida IA, policy per l'uso degli strumenti generativi, regolamento per la sperimentazione, procedure di valutazione dei rischi) che risultano redatti, approvati e formalmente adottati.

Target 2026: nr. atti previsti adottati formalmente ≥ 1

PARTE V – ATTUAZIONE, MONITORAGGIO E MIGLIORAMENTO

13. Ciclo di vita del Piano (PDCA)

L'attuazione del Piano Triennale di Transizione Digitale dell'Università di Napoli L'Orientalesi fonda sul modello PDCA (Plan–Do–Check–Act), adottato dalle Linee Guida AgID e pienamente coerente con il sistema di Assicurazione della Qualità (AVA3), con la programmazione strategica e con il ciclo di gestione della performance dell'Ateneo. Il PDCA consente di garantire una gestione sistematica, misurabile e migliorativa del Piano, assicurando continuità operativa, verifica costante dei risultati e capacità di adeguamento alle evoluzioni normative, tecnologiche e organizzative.

Il modello introduce un approccio circolare alla pianificazione digitale, in cui ogni fase del processo alimenta la successiva, contribuendo a consolidare la resilienza, la trasparenza e l'allineamento strategico dell'intero ecosistema ICT.

13.1 Pianificazione

La fase di pianificazione rappresenta il momento centrale del ciclo di vita del Piano di Transizione Digitale, poiché consente all'Ateneo di definire in modo organico gli obiettivi, le priorità e gli interventi da realizzare nel triennio, assicurando coerenza con la strategia istituzionale e con il quadro normativo nazionale. La pianificazione si fonda sull'integrazione con gli strumenti programmatori già in essere — Piano Strategico 2024–2026, PIAO 2025–2027, programmazione finanziaria annuale e triennale — e garantisce l'allineamento tra il percorso di trasformazione digitale e le esigenze organizzative, amministrative, didattiche e scientifiche dell'Università.

L'attività di pianificazione comprende l'analisi preliminare del contesto ICT, la definizione delle linee strategiche di intervento, l'individuazione delle azioni da attuare nel ciclo triennale, la selezione degli indicatori di monitoraggio (KPI), la valutazione delle risorse necessarie e la calendarizzazione delle milestone operative. Tale processo avviene sotto il coordinamento del Responsabile per la Transizione Digitale, con il supporto del Settore Sviluppo Digitale e in raccordo strutturato con la Direzione Generale, il Presidio della Qualità, le Aree amministrative e le strutture accademiche.

La pianificazione si basa su un approccio evidence-based, fondato su analisi qualitative e quantitative relative a infrastrutture, servizi, interoperabilità, patrimonio informativo, sicurezza e competenze digitali. Gli esiti dell'analisi di contesto costituiscono la baseline da cui deriva la definizione degli obiettivi annuali e triennali, assicurando che il Piano risponda a esigenze reali, misurabili e sostenibili.

Elemento essenziale della pianificazione è la valutazione della fattibilità tecnica, normativa e organizzativa degli interventi previsti, nonché della sostenibilità finanziaria in rapporto al budget ICT. Ogni linea di intervento viene pianificata in modo da rispettare i requisiti delle Linee Guida AgID, del Modello di Interoperabilità nazionale, della Direttiva NIS2, del GDPR, del Piano Nazionale di Ripresa e Resilienza e delle disposizioni in materia di accessibilità digitale.

La fase di pianificazione si conclude con l'approvazione del Piano da parte degli Organi di governo dell'Ateneo e con la sua pubblicazione nelle sedi istituzionali, assicurando trasparenza, tracciabilità e allineamento con gli obblighi di

comunicazione previsti dalla normativa vigente. Essa rappresenta, pertanto, il punto di avvio formale del ciclo PDCA e la base per l'attuazione, il monitoraggio e la revisione continua del Piano nel triennio 2026–2028.

13.2 Attuazione

La fase di attuazione rappresenta il momento operativo del ciclo PDCA, nel quale gli obiettivi strategici e le linee d'intervento individuate in fase di pianificazione vengono tradotti in attività concrete, progetti, cantieri digitali e azioni coordinate rivolte alla comunità accademica. Essa costituisce la parte più estesa e delicata del ciclo di vita del Piano, poiché incide direttamente sulla trasformazione dei processi, sull'evoluzione delle infrastrutture, sull'erogazione dei servizi digitali e sulla valorizzazione del patrimonio informativo dell'Ateneo.

L'attuazione è guidata dal Responsabile per la Transizione Digitale e dal Settore Sviluppo Digitale, che assicurano il coordinamento tecnico-operativo delle attività, la gestione delle interdipendenze tra i diversi interventi e il raccordo continuo con la Direzione Generale, le Aree amministrative, le strutture accademiche e gli organismi preposti alla qualità e alla valutazione. Tale modello permette di mantenere una visione unitaria sullo sviluppo dei progetti e garantisce la coerenza delle soluzioni adottate con gli standard nazionali in materia di sicurezza, interoperabilità, accessibilità digitale e gestione del rischio.

Nel corso dell'attuazione, ogni linea di intervento procede secondo i cronoprogrammi definiti, attraverso attività quali l'implementazione delle infrastrutture tecnologiche, l'attivazione dei sistemi applicativi, l'integrazione dei flussi informativi, la digitalizzazione dei processi amministrativi, l'introduzione di nuovi servizi per studenti, docenti e personale TAB, la realizzazione delle attività di formazione e la predisposizione delle misure organizzative e tecniche previste in materia di sicurezza, privacy e intelligenza artificiale. Particolare attenzione è rivolta alle interazioni tra i sistemi, alla qualità dei dati, alla comunicazione verso gli utenti e al supporto operativo durante il passaggio ai nuovi modelli digitali.

La fase attuativa comprende inoltre attività di accompagnamento al cambiamento, necessarie per garantire la piena adozione delle innovazioni introdotte. Ciò include iniziative di informazione, documentazione, supporto tecnico-specialistico e formazione continuativa, che consentono alle strutture e al personale di integrare in modo efficace i nuovi strumenti nei processi quotidiani. L'ascolto degli utenti e la raccolta sistematica dei feedback rappresentano un ulteriore elemento chiave, poiché consentono di individuare tempestivamente eventuali criticità ed effettuare adeguamenti durante la messa in esercizio dei servizi.

L'attuazione del Piano è, infine, strettamente collegata alla gestione operativa del rischio, alla supervisione della sicurezza informatica e alla verifica della conformità normativa. In tale contesto, la collaborazione tra RTD, RPD, Settore Sviluppo Digitale e Responsabili dei processi assicura che ogni intervento sia sviluppato in condizioni di sicurezza, minimizzando le esposizioni e garantendo la piena tutela del patrimonio informativo e dei diritti degli utenti.

Nel suo complesso, la fase di attuazione costituisce il cuore pulsante della trasformazione digitale dell'Ateneo: è il momento in cui la visione strategica delineata nel Piano si traduce in progetti concreti, in servizi reali e in un miglioramento tangibile dell'efficienza, dell'esperienza utente e della maturità digitale dell'Università.

13.3 Monitoraggio

La fase di monitoraggio rappresenta il momento in cui l'Ateneo verifica in maniera sistematica lo stato di avanzamento del Piano di Transizione Digitale, valutando l'efficacia delle azioni attuate, il livello di raggiungimento dei KPI e la coerenza complessiva degli interventi rispetto agli obiettivi strategici definiti nella fase di pianificazione. Si tratta di un passaggio essenziale del ciclo PDCA, poiché consente di mantenere il controllo dell'esecuzione del Piano, individuare tempestivamente eventuali scostamenti e orientare le attività correttive necessarie a preservarne l'efficacia.

Il monitoraggio è coordinato dal Responsabile per la Transizione Digitale, con il supporto del Settore Sviluppo Digitale, e si svolge in raccordo con la Direzione Generale, il Presidio della Qualità, il Nucleo di Valutazione e le strutture amministrative e accademiche coinvolte nei singoli interventi. Tale modello garantisce una visione unitaria dell'andamento del Piano e permette di integrare il processo di verifica con i meccanismi istituzionali di programmazione, performance e autovalutazione previsti dagli standard AVA3.

La verifica periodica dell'attuazione si basa sulla raccolta strutturata di dati, indicatori, evidenze documentali e report tecnici relativi all'avanzamento dei progetti, all'adozione dei servizi digitali, all'evoluzione delle infrastrutture, alla qualità del patrimonio informativo, ai livelli di sicurezza, alle attività di formazione e alla maturità complessiva dei processi. Il monitoraggio tiene inoltre conto delle eventuali criticità riscontrate nell'utilizzo dei sistemi, dei feedback provenienti dagli utenti, della sostenibilità delle risorse impiegate e del rispetto delle tempistiche definite nel cronoprogramma triennale.

L'attività di monitoraggio comprende anche la verifica della conformità del Piano ai requisiti normativi emergenti (Modello di Interoperabilità, NIS2, Linee Guida AgID, GDPR, standard di accessibilità), assicurando che l'Ateneo mantenga un livello adeguato di allineamento alle prescrizioni nazionali ed europee. Particolare attenzione è riservata ai controlli sui sistemi critici, ai processi di trattamento dei dati personali, ai flussi verso la PDND e ai presìdi di sicurezza, in modo da garantire continuità operativa, integrità informativa e tutela dell'utenza.

I risultati del monitoraggio sono formalizzati attraverso report periodici e confluiscono in un bilancio annuale di attuazione del Piano, che costituisce la base per la revisione del ciclo successivo e per l'aggiornamento delle priorità di intervento. Tale documentazione è messa a disposizione degli Organi di governo, consentendo loro di valutare lo stato di implementazione delle strategie digitali e di orientare con maggiore consapevolezza le scelte future.

Nel complesso, il monitoraggio assicura che la trasformazione digitale dell'Ateneo proceda in modo controllato, trasparente e orientato al miglioramento continuo, rappresentando il cardine attraverso il quale il Piano si traduce in un processo evolutivo stabile, verificabile e sostenibile.

13.4 Revisione e miglioramento

La fase di revisione e miglioramento costituisce l'ultimo passaggio del ciclo PDCA e rappresenta il momento in cui l'Ateneo rielabora i risultati del monitoraggio, valuta criticamente l'efficacia delle azioni intraprese e definisce gli interventi correttivi necessari a garantire un percorso di trasformazione digitale coerente, sostenibile e progressivamente più maturo. Tale fase assume una rilevanza strategica, poiché consente di trasformare l'esperienza maturata durante l'attuazione in un patrimonio di conoscenze utile a orientare in modo informato la programmazione successiva.

La revisione del Piano si fonda sull'analisi sistematica dei KPI, sulla verifica del raggiungimento delle milestone, sull'esame delle eventuali criticità registrate e sul confronto con le esigenze emergenti delle strutture accademiche e amministrative. Tale processo permette di individuare scostamenti rispetto agli obiettivi, di comprenderne le cause e di definire misure correttive adeguate, che possono riguardare la riprogrammazione delle attività, l'aggiornamento delle priorità, la ridefinizione delle risorse, la revisione delle responsabilità operative o la necessità di interventi integrativi su infrastrutture, servizi, sicurezza o processi.

La revisione tiene conto anche dell'evoluzione del quadro normativo e tecnologico. Le innovazioni introdotte da AgID, ACN, dal Modello di Interoperabilità, dalla Direttiva NIS2, dal GDPR, dalle linee guida sull'accessibilità digitale e dalle politiche europee sull'intelligenza artificiale impongono un costante adeguamento delle strategie e dei presìdi. Il Piano deve pertanto essere considerato un documento dinamico, soggetto a revisione periodica e capace di adattarsi a scenari in continua evoluzione. La sua capacità di rimanere aggiornato rappresenta un indicatore essenziale della maturità digitale dell'Ateneo.

La revisione si realizza attraverso un processo partecipato che coinvolge il Responsabile per la Transizione Digitale, il Settore Sviluppo Digitale, la Direzione Generale, le Aree amministrative, i Dipartimenti, il Presidio della Qualità, il Nucleo di Valutazione e gli Organi di governo. Tale modello collegiale garantisce una comprensione condivisa dei risultati, un allineamento sugli interventi da attuare e una visione complessiva dell'evoluzione del sistema ICT.

Gli esiti della revisione sono formalizzati in un documento annuale di aggiornamento del Piano, che definisce gli adeguamenti necessari per l'anno successivo e incorpora le lezioni apprese, i miglioramenti da implementare e le priorità emergenti. Tale documento costituisce la base per l'avvio del nuovo ciclo PDCA, assicurando continuità e coerenza tra i diversi esercizi di pianificazione.

Nel complesso, la fase di revisione e miglioramento consente all'Ateneo di consolidare un modello di governo del digitale basato sull'apprendimento organizzativo, sulla valutazione trasparente dei risultati e sulla capacità di adattamento alle nuove sfide tecnologiche e normative. Essa rappresenta il presupposto indispensabile per garantire che il Piano di Transizione Digitale rimanga uno strumento vivo, efficace e orientato alla crescita continua della qualità dei servizi e della maturità digitale dell'Università.

14. Indicatori di performance e rendicontazione

Il sistema degli indicatori di performance e delle attività di rendicontazione costituisce un elemento essenziale per garantire trasparenza, misurabilità e controllo dell'attuazione del Piano Triennale di Transizione Digitale. La definizione di un quadro strutturato di KPI consente di collegare in modo diretto gli interventi programmati ai risultati ottenuti, assicurando la piena integrazione con il ciclo di performance, con il PIAO, con il Piano Strategico e con i requisiti di autovalutazione previsti dal modello AVA3.

Gli indicatori rappresentano uno strumento operativo fondamentale per il Responsabile per la Transizione Digitale, per il Settore Sviluppo Digitale, per la Direzione Generale e per gli Organi di governo, poiché consentono di verificare l'efficacia delle azioni implementate, la coerenza degli investimenti, il livello di digitalizzazione dei processi e il grado di maturità

complessiva del sistema ICT. Il sistema di indicatori è costruito secondo criteri di affidabilità, verificabilità e sostenibilità, evitando metriche puramente descrittive e privilegiando misure legate a fenomeni osservabili, ripetibili e documentabili.

Il processo di rendicontazione si articola su due livelli: un monitoraggio interno periodico, finalizzato alla verifica dell'avanzamento del Piano, e una rendicontazione annuale, indirizzata agli Organi di governo e agli organismi preposti al controllo strategico e alla valutazione. Tale processo consente di illustrare in modo chiaro e trasparente il livello di raggiungimento degli obiettivi, l'efficienza degli interventi, l'impiego delle risorse e gli eventuali scostamenti riscontrati, offrendo un quadro informativo completo e funzionale alle decisioni istituzionali.

La logica di misurazione si inserisce inoltre nel più ampio sistema di programmazione dell'Ateneo: gli indicatori del Piano di Transizione Digitale concorrono alla definizione degli obiettivi e degli indicatori di performance organizzativa, alimentano i cruscotti direzionali e forniscono evidenze utili ai processi di valutazione interna ed esterna. Attraverso la rendicontazione periodica, l'Ateneo rafforza la propria capacità di apprendimento organizzativo, consolida il sistema di governance del digitale e garantisce una supervisione continua sull'allineamento agli standard nazionali in materia di interoperabilità, sicurezza, accessibilità digitale, qualità del dato e innovazione tecnologica.

Nel suo complesso, il sistema degli indicatori e della rendicontazione rappresenta una componente imprescindibile del Piano, poiché permette di trasformare la strategia digitale in un processo valutabile, tracciabile e orientato al miglioramento continuo, consolidando la cultura della misurazione e assicurando la piena accountability delle attività realizzate nel triennio 2026–2028.

14.1 Indicatori di output e outcome

La misurazione degli indicatori di output e outcome rappresenta un elemento fondamentale per valutare in modo oggettivo l'attuazione del Piano di Transizione Digitale e l'impatto delle iniziative realizzate nel triennio 2026–2028. Gli indicatori di output consentono di verificare il completamento delle attività programmate, mentre gli indicatori di outcome misurano il miglioramento prodotto sui processi, sui servizi e sulla qualità complessiva dell'esperienza degli utenti. Tale distinzione è pienamente coerente con il modello di monitoraggio previsto dalle Linee Guida AgID e con il sistema di gestione della performance organizzativa previsto dal PIAO.

Gli output permettono di valutare il grado di realizzazione degli interventi pianificati in termini di infrastrutture attivate, servizi digitali implementati, processi dematerializzati, integrazioni applicative completate, politiche di sicurezza formalizzate, linee guida adottate e attività formative erogate. Misurano la "produzione" del Piano, ovvero la capacità dell'Ateneo di portare a compimento le azioni individuate e di rispettare i cronoprogrammi definiti.

Gli outcome, invece, rilevano l'effettivo cambiamento generato dagli interventi sul funzionamento dell'Ateneo: miglioramento dell'efficienza amministrativa, incremento dell'accessibilità dei servizi, elevata qualità del patrimonio informativo, maggiore resilienza dei sistemi, riduzione dei rischi operativi e cyber, crescita delle competenze digitali, miglioramento della soddisfazione dell'utenza e rafforzamento della compliance normativa. Essi rappresentano la dimensione di "impatto" del Piano e consentono di comprendere quanto le azioni intraprese contribuiscano alla maturità digitale complessiva dell'Università.

La misurazione congiunta di output e outcome permette di disporre di un quadro completo della performance digitale, garantendo una valutazione equilibrata che tenga conto sia del raggiungimento dei risultati formali sia dei benefici derivanti dall'innovazione tecnologica e organizzativa. Tali indicatori alimentano i cruscotti direzionali, concorrono alla definizione dei report annuali di attuazione del Piano e rappresentano una base informativa essenziale per la revisione del ciclo PDCA, per la programmazione delle risorse e per le attività di autovalutazione interna ed esterna.

Nel suo complesso, questo sistema consente all'Ateneo di monitorare in modo trasparente, verificabile e continuo il valore prodotto dalla trasformazione digitale, garantendo una governance orientata ai risultati e un processo decisionale fondato su evidenze misurabili.

14.2 KPI quantitativi e qualitativi per linea d'azione

La struttura dei KPI individuati nel Piano di Transizione Digitale segue una logica di coerenza interna fra le linee di intervento strategiche (Parte III) e i Piani attuativi dedicati (Parte IV), consentendo all'Ateneo di disporre di un sistema unico di misurazione che renda verificabile il contributo di ogni ambito alla maturità digitale complessiva.

I KPI, già definiti nelle rispettive sezioni tematiche (infrastrutture, interoperabilità, servizi digitali, sicurezza, competenze, procurement, innovazione e IA), sono organizzati secondo due principi fondamentali:

KPI quantitativi, che misurano grandezze osservabili e verificabili (percentuali, numeri assoluti, livelli di conformità, coperture dei servizi);

KPI qualitativi, che misurano la qualità dei processi, la maturità del sistema, il livello di compliance e l'efficacia degli interventi.

Tali indicatori permettono di valutare in modo sistematico lo stato di avanzamento delle attività operative e, allo stesso tempo, la capacità dell'Ateneo di consolidare un modello di governance digitale stabile, sicuro e pienamente conforme ai requisiti nazionali.

La struttura dei KPI è organizzata per linea d'azione secondo la seguente articolazione:

Linea d'azione 1 – Infrastrutture digitali

KPI volti a misurare il livello di evoluzione delle componenti tecnologiche di base, la capacità di garantire continuità operativa e l'allineamento agli standard di sicurezza e resilienza (backup, standardizzazione postazioni, maturità cloud).

Linea d'azione 2 – Interoperabilità e cooperazione applicativa

Indicatori che misurano la qualità delle integrazioni applicative, la definizione delle fonti dati autorevoli, la diffusione delle policy di identità federata e l'adesione agli standard del Modello di Interoperabilità e della PDND.

Linea d'azione 3 – Patrimonio informativo e qualità del dato

KPI orientati alla misurazione della maturità della data governance, della coerenza dei domini informativi, della tracciabilità dei flussi e dell'affidabilità dei dati istituzionali nei sistemi CINECA e nelle piattaforme interne.

Linea d'azione 4 – Servizi digitali e user experience

Indicatori che misurano la qualità dell'esperienza utente, il livello di accessibilità, la soddisfazione della comunità accademica e il grado di digitalizzazione dei processi amministrativi.

Linea d'azione 5 – Cybersecurity, privacy e continuità operativa

KPI dedicati alla misurazione della maturità della postura di sicurezza, della conformità al GDPR e alla Direttiva NIS2, della copertura delle policy ICT, dell'esecuzione delle DPIA e della gestione dei rischi.

Linea d'azione 6 – Competenze digitali e change management

Indicatori legati alla formazione, alla diffusione delle competenze digitali, alla partecipazione ai percorsi formativi e all'impatto delle attività di accompagnamento al cambiamento.

Linea d'azione 7 – Procurement ICT e sostenibilità

KPI relativi alla qualità degli acquisti ICT, all'applicazione dei Criteri Ambientali Minimi (CAM), alla presenza di SLA/OLA nei contratti e alla capacità dell'Ateneo di assicurare sostenibilità economica, tecnica e ambientale.

Linea d'azione 8 – Innovazione tecnologica e intelligenza artificiale

Indicatori finalizzati a misurare la maturità dei processi di IA, l'adozione del quadro regolatorio interno, la gestione dei rischi algoritmici e l'integrazione dei progetti pilota all'interno dell'ecosistema digitale dell'Ateneo.

Questo approccio garantisce una visione unitaria e coerente dei risultati, riduce la frammentazione informativa e consente all'Università di operare con un modello di governance digitale misurabile, trasparente e orientato al miglioramento continuo.

I KPI indicati, come detto, sono conformi a quanto previsto da AGID, essi derivano dai Risultati Attesi (RA), ovvero la macro–unità strategica del Piano Triennale AGID, delimitano gli obiettivi che AGID assegna all'intero sistema pubblico nel triennio, e dal Codice della Linea di Azione del Piano (CAP) ossia le linee di azione riferite ad AGID/Dipartimento, di seguito la matrice riepilogativa di associazione KPI – RA – CAP:

KPI	DESCRIZIONE	TARGET	ANNO	RA	CAP
1	Copertura dei servizi con backup conformi CO/DR	≥ 95%	2027	RA7.3.1	CAP7.PA.09
2	Standardizzazione postazioni di lavoro	≥ 85%	2028	RA3.2.2	CAP3.PA.13 CAP3.PA.14 CAP3.PA.15 CAP3.PA.16
3	Percentuale domini informativi con fonte autorevole definita	100%	2028	RA5.3.1	CAP5.PA.20
4	Percentuale servizi con identità federata (SSO, SPID/CIE)	≥ 90%	2026	RA4.1.4	CAP4.PA.04
5	Livello di accessibilità digitale dei servizi	≥ 85% servizi con dichiarazione aggiornata	2028	RA3.2.2	CAP3.PA.14 CAP3.PA.15 CAP3.PA.16

6	Soddisfazione media dell'utenza sui servizi digitali	≥ 3.5	2028	RA3.4.1 RA3.4.2	CAP3.PA.19 CAP3.PA.20 CAP3.PA.21
7	Percentuale policy sicurezza ICT adottate (NIS2)	≥ 100%	2028	RA7.x	CAP7.PA.01 CAP7.PA.02 CAP7.PA.03 CAP7.PA.04 CAP7.PA.05 CAP7.PA.06 CAP7.PA.07
8	DPIA sui trattamenti ad alto rischio	≥ 50%	2026	RA7.3.1	-
9	Copertura personale nei percorsi formativi digitali	≥ 60%	2028	RA1.2.x	CAP1.PA
10	Percorsi formativi completati	≥ 500 percorsi	2028	RA1.x	CAP1.PA
11	Conformità ai CAM nelle forniture ICT	85%	2026	RA2.1.1	CAP2.PA.01 CAP2.PA.02 CAP2.PA.03 CAP2.PA.04 CAP2.PA.05
12	Contratti ICT con SLA/OLA	≥ 90%	2028	RA2.1.1	CAP2.PA CAP7.PA.05 CAP7.PA.06 CAP7.PA.07
13	Adozione quadro regolatorio interno per l'IA	≥ 1	2026	RA5.4	CAP5.PA.21 CAP5.PA.22 CAP5.PA.23

14.3 Reporting

Il reporting costituisce lo strumento fondamentale attraverso il quale l'Ateneo assicura trasparenza, controllo e monitoraggio continuo sull'attuazione del Piano di Transizione Digitale nel triennio 2026–2028. Attraverso un sistema strutturato di rendicontazione, il Piano viene tradotto in evidenze documentate e verificabili, che consentono agli Organi di governo, alla Direzione Generale, al Responsabile per la Transizione Digitale e alle strutture coinvolte di valutare in modo oggettivo lo stato di avanzamento degli interventi, la coerenza delle attività realizzate e l'efficacia complessiva delle azioni intraprese.

Il reporting si articola in due livelli complementari. Il primo riguarda la produzione di report periodici, predisposti con cadenza almeno semestrale, contenenti l'analisi dei KPI associati alle diverse linee d'azione, il monitoraggio delle milestone operative, la verifica della sostenibilità delle risorse impiegate e la descrizione delle eventuali criticità riscontrate. Tali report permettono di mantenere una visione aggiornata dell'esecuzione del Piano e offrono uno strumento decisionale utile per correggere tempestivamente eventuali scostamenti o ritardi.

Il secondo livello è rappresentato dalla rendicontazione annuale, che fornisce un quadro organico dell'attuazione del Piano nel periodo di riferimento. Tale documento integra i risultati ottenuti nei diversi ambiti – infrastrutture, interoperabilità, servizi digitali, sicurezza, competenze, procurement, innovazione – e evidenzia i progressi rispetto agli obiettivi programmati. La rendicontazione annuale costituisce un elemento di sintesi strategica, utile non solo agli Organi di governo, ma anche ai processi di valutazione interna ed esterna, inclusi quelli previsti dal modello AVA3, dal PIAO e dalle Linee Guida AgID.

Il reporting è inoltre strettamente collegato alla fase di revisione del ciclo PDCA: i risultati delle analisi periodiche alimentano infatti la ridefinizione delle priorità, la calibrazione dei KPI per gli anni successivi e l'aggiornamento delle linee di intervento. In tal modo, il sistema di reporting non si limita a svolgere una funzione informativa, ma diventa un meccanismo dinamico di apprendimento organizzativo e di miglioramento continuo.

Nel suo complesso, il reporting assicura che la trasformazione digitale dell'Ateneo sia accompagnata da un processo di monitoraggio trasparente, metodologicamente solido e orientato ai risultati, garantendo agli attori istituzionali gli elementi necessari per una governance consapevole e basata su evidenze.

15. Cronoprogramma triennale e risorse

La realizzazione del Piano Triennale di Transizione Digitale 2026–2028 richiede una programmazione temporale strutturata, che assicuri coerenza tra gli obiettivi strategici, le linee d'azione, le risorse rese disponibili dall'Ateneo e la capacità operativa delle strutture coinvolte. Il cronoprogramma triennale non costituisce un mero elenco di scadenze, ma rappresenta lo strumento principale attraverso cui coordinare le attività, monitorare l'avanzamento, ottimizzare l'impiego delle risorse e garantire un allineamento continuo con gli obiettivi istituzionali e con gli adempimenti normativi nazionali.

Il Piano adotta un'impostazione progressiva, articolata in tre fasi:

1. Fase di avvio (2026)

dedicata all'attivazione delle azioni preliminari – definizione dei modelli di governance, progettazione tecnica delle attività infrastrutturali, predisposizione dei regolamenti e dei processi documentali, avvio delle iniziative di interoperabilità e delle attività propedeutiche ai servizi digitali e all'IA.

2. Fase di implementazione (2027)

in cui si concentrano gli interventi a maggior impatto, compresa l'evoluzione infrastrutturale, la standardizzazione dei servizi, la messa in esercizio delle integrazioni applicative, la pubblicazione delle policy di sicurezza, l'adozione delle nuove piattaforme e il rafforzamento della data governance.

3. Fase di consolidamento (2028)

focalizzata sulla stabilizzazione dei servizi, sulla verifica dei risultati, sulla valutazione dei KPI, sul perfezionamento delle procedure, sull'aggiornamento dei regolamenti e sull'integrazione degli strumenti di monitoraggio e rendicontazione.

In ciascun anno sono previste milestone intermedie che consentono un controllo puntuale degli avanzamenti e l'eventuale riallineamento delle attività, in coerenza con il ciclo PDCA descritto nel Capitolo 13.

15.1 Timeline e milestone (2026–2028)

La pianificazione triennale si articola lungo le principali linee strategiche del Piano.

Di seguito la struttura sintetica del cronoprogramma, in cui ogni linea d'azione è associata alle milestone principali:

2026 – Avvio e predisposizione

Definizione del modello di data governance e dei domini informativi.

Progettazione degli interventi infrastrutturali e delle soluzioni cloud ibride.

Revisione dei flussi documentali e progettazione dei nuovi servizi digitali.

Avvio del percorso di definizione delle policy ICT (NIS2, ACN, AgID).

Costituzione del quadro regolatorio interno sull'intelligenza artificiale.

Avvio percorsi formativi e iniziative di change management.

Allineamento dei processi di procurement al nuovo modello centrale ICT.

2027 – Implementazione

Attuazione degli interventi infrastrutturali e aggiornamento di cluster, reti, postazioni.

Messa a regime delle integrazioni PDND e adozione degli standard ModI.

Rilascio dei primi servizi digitali uniformati e potenziamento dei processi amministrativi digitali.

Pubblicazione delle policy di sicurezza ICT e completamento delle DPIA prioritarie.

Avvio dei progetti pilota di IA e dei modelli semplificati di valutazione del rischio.

Potenziamento dei percorsi formativi e del sistema di supporto all'utenza.

2028 – Consolidamento e verifica

Verifica del livello di maturità digitale raggiunto.

Conclusione del piano di standardizzazione delle postazioni e dei criteri di sicurezza.

Validazione dei flussi PDND e consolidamento dei servizi interoperabili.

Verifica dei KPI associati a servizi digitali, sicurezza, accessibilità e IA.

Aggiornamento del quadro regolatorio e revisione del Piano per il triennio successivo.

Rendicontazione dei risultati agli Organi di governo e predisposizione del nuovo ciclo PDCA.

15.2 Risorse umane e finanziarie

L'attuazione del Piano di Transizione Digitale richiede un impiego coordinato e sostenibile di risorse umane, tecniche e finanziarie, collocate all'interno del quadro programmatorio dell'Ateneo e coerenti con il bilancio triennale di previsione. Le

risorse sono articolate in modo da garantire continuità operativa, evoluzione tecnologica e capacità di risposta alle esigenze emergenti legate all'interoperabilità, alla sicurezza informatica, ai servizi digitali e alla gestione dei dati.

Sotto il profilo delle risorse umane, il Piano si fonda sul contributo del Settore Sviluppo Digitale (ARIE04–ARIE07), responsabile della governance tecnica dell'ecosistema ICT, della gestione delle infrastrutture e dei sistemi applicativi, della sicurezza informatica e delle attività di integrazione. La Direzione Generale assicura il coordinamento istituzionale e la supervisione strategica, mentre il Responsabile della Protezione dei Dati presidia la conformità al GDPR e supporta i processi di valutazione del rischio e di protezione dei dati personali. Gli uffici amministrativi e accademici contribuiscono all'evoluzione dei processi digitali e alla gestione dei servizi rivolti all'utenza. Questo, unito all'opera di rafforzamento e di reclutamento che l'Ateneo sta sostenendo garantisce la sostenibilità nel medio periodo delle linee d'azione del Piano.

Descrizione voci costo COAN	Conto COAN	Annualità di Competenza		
		2026	2027	2028
Acquisto banche dati on line e su Cd Rom - istituzionale	CA.04.40.03.02	10.000,00€	10.000,00€	10.000,00€
Manutenzione ordinaria e riparazioni di apparecchiature	CA.04.41.01.02	134.594,77€	134.594,77€	134.594,77€
Manutenzione software	CA.04.41.01.05	10.000,00€	10.000,00€	10.000,00€
Pubblicità	CA.04.41.02.02	23.000,00€	23.000,00€	23.000,00€
Altre spese per servizi tecnici	CA.04.41.04.03	44.398,00€	44.398,00€	44.398,00€
Trasporti. facchinaggi e competenze spedizionieri	CA.04.41.07.07	75.000,00€	26.965,84€	
Altre prestazioni e servizi da terzi	CA.04.41.09.03	767.046,00€	737.046,00€	738.846,00€
Cancelleria e altri materiali di consumo - istituzionale	CA.04.40.01.01	15.000,00€	15.000,00€	15.000,00€
Altri materiali - istituzionale	CA.04.40.06.01	35.000,00€	35.000,00€	35.000,00€
Acquisto software per PC (spesati nell'anno)	CA.04.40.04.02	279.276,58€	194.276,58€	194.276,58€
Noleggi e spese accessorie	CA.04.42.01.03	6.000,00€	6.000,00€	6.000,00€
Contributi e quote associative	CA.04.46.03.01	9.740,00€	9.740,00€	9.740,00€
Attrezzature informatiche	CA.01.11.02.05	225.000,00€	225.000,00€	225.000,00€
Attrezzature elettromeccaniche ed elettroniche	CA.01.11.02.08	220.000,00€	220.000,00€	220.000,00€
Software applicativo acquistato a titolo di licenza d'uso a tempo determinato	CA.01.10.04.02	40.000,00€	25.000,00€	25.000,00€

Relativamente alle risorse finanziarie, il Piano si basa sulle dotazioni previste nel budget ICT triennale, imputate sulle voci COAN del Bilancio di Ateneo. Tale articolazione consente di sostenere gli investimenti infrastrutturali, i servizi cloud e SaaS, le manutenzioni tecniche, i progetti di interoperabilità, gli interventi di sicurezza e le iniziative di formazione e change management. A titolo esemplificativo, la voce CA.04.41.09.03 – "Altre prestazioni e servizi da terzi" rappresenta la componente principale della spesa corrente ICT: essa assorbe, in modo strutturale, i canoni dei sistemi gestionali integrati (U-Gov, ESSE3, IRIS/UNORA) erogati dal Consorzio CINECA, pari complessivamente a € 701.846 annui fino al 2027, nonché i servizi cloud, i contratti SaaS e parte dei servizi tecnico-specialistici necessari al funzionamento dell'ecosistema digitale.

Si precisa inoltre che, in coerenza con la strategia delineata nel presente Piano, la stessa voce CA.04.41.09.03 include anche una quota di € 30.000 destinata agli adeguamenti in materia di cybersecurity e NIS2, mentre ulteriori risorse per

l'evoluzione della sicurezza (rispettivamente € 130.000 nel 2026 e € 45.000 nel 2027 e 2028) sono allocate nella voce CA.04.40.04.02 – Acquisto software per PC (spesati nell'anno), in quanto riferite all'acquisizione di componenti software specialistici e strumenti di protezione.

Il budget triennale comprende inoltre le voci relative alle manutenzioni hardware, alle dotazioni multimediali, alle licenze applicative, alle attrezzature informatiche e agli strumenti di supporto tecnico-operativo necessari alla realizzazione delle linee di intervento previste. Le risorse derivanti da eventuali finanziamenti esterni – quali fondi dedicati alla sicurezza, all'IA o all'interoperabilità – saranno integrate annualmente nella programmazione finanziaria, senza gravare sul Fondo di Finanziamento Ordinario.

Nel complesso, la struttura delle risorse umane e finanziarie garantisce la sostenibilità del Piano, la coerenza con gli indirizzi strategici dell'Ateneo e la capacità di attuare gli interventi previsti nel triennio, assicurando continuità dei servizi, evoluzione tecnologica e progressivo adeguamento agli standard nazionali.

15.3 Collegamento con budget ICT

Il Piano di Transizione Digitale è pienamente integrato con il budget ICT triennale, secondo la tabella precedentemente descritta, che costituisce lo strumento finanziario attraverso il quale l'Ateneo assicura la sostenibilità delle iniziative programmate e il raggiungimento degli obiettivi strategici. Tale collegamento consente di armonizzare la pianificazione digitale con il processo di bilancio, garantendo coerenza, trasparenza e capacità di monitoraggio.

A livello strategico, il budget ICT è allineato agli indirizzi definiti nel Piano Strategico d'Ateneo, negli strumenti di programmazione integrata (PIAO) e negli orientamenti della Direzione Generale, assicurando che le risorse destinate alla transizione digitale rispondano alle priorità istituzionali e ai requisiti normativi nazionali. Sul piano tecnico-operativo, il budget consente di finanziare le linee di intervento relative a infrastrutture, interoperabilità, sicurezza, servizi digitali, competenze e innovazione, distribuendo le risorse tra investimenti, manutenzioni e servizi specialistici secondo una programmazione triennale sostenibile e verificabile.

Il collegamento si completa attraverso il livello di monitoraggio e controllo, che prevede la verifica annuale delle milestone, dell'avanzamento dei progetti e della coerenza tra spesa effettiva e linee di intervento. Tale meccanismo consente di riallineare le risorse alle esigenze emergenti, assicurando piena tracciabilità e capacità di adeguamento del Piano.

In questo quadro, il budget ICT triennale non rappresenta solo una fonte finanziaria, ma un elemento strutturale della governance della transizione digitale, che garantisce l'effettiva implementazione delle azioni programmate e la sostenibilità dell'evoluzione tecnologica dell'Ateneo nel periodo 2026–2028.

16. Comunicazione, trasparenza e accessibilità

La piena efficacia del Piano Triennale di Transizione Digitale 2026–2028 richiede un sistema di comunicazione istituzionale chiaro, continuo e coerente, capace di assicurare la piena conoscibilità delle iniziative, la trasparenza dei processi e l'accessibilità delle informazioni rivolte alla comunità accademica e agli stakeholder esterni. In questo senso, la comunicazione non è un'attività accessoria, ma una componente strutturale della governance digitale, indispensabile

per sostenere la partecipazione degli utenti, facilitare la comprensione delle innovazioni introdotte e rafforzare la fiducia nel percorso di trasformazione dell'Ateneo.

Il modello comunicativo adottato si ispira ai principi di trasparenza amministrativa, responsabilità pubblica e accessibilità digitale, assicurando che le informazioni relative al Piano, alle sue fasi attuative e ai risultati conseguiti siano diffuse in modo tempestivo, verificabile e coerente con gli obblighi normativi. L'Ateneo garantisce che la pubblicazione del Piano e dei relativi aggiornamenti avvenga nelle sezioni istituzionali previste dalla normativa vigente, in particolare nell'area "Amministrazione Trasparente" e negli spazi dedicati alla programmazione strategica. Tale pubblicazione si accompagna alla disponibilità dei documenti in formati accessibili, conformi alle Linee Guida AgID e ai requisiti WCAG, al fine di assicurare una piena fruibilità anche da parte degli utenti con disabilità.

Parallelamente, la comunicazione interna assume un ruolo determinante per sostenere l'adozione dei nuovi processi digitali e facilitare il coinvolgimento del personale tecnico-amministrativo, dei docenti e dei ricercatori. Il Piano prevede la diffusione di aggiornamenti periodici, linee operative, istruzioni d'uso, contenuti formativi e materiali divulgativi che consentono agli utenti di comprendere le innovazioni introdotte, partecipare attivamente ai processi di digitalizzazione e contribuire alla corretta implementazione delle misure previste. Tale attività si integra con il sistema di supporto all'utenza, che rappresenta un presidio imprescindibile per accompagnare la transizione e per rilevare eventuali criticità emergenti.

La comunicazione rivolta al pubblico esterno, inclusi enti partner, istituzioni pubbliche, organismi di valutazione e soggetti interessati, è impostata in modo da evidenziare la trasparenza delle azioni intraprese, l'allineamento del Piano alle strategie nazionali e il contributo dell'Ateneo alla trasformazione digitale del sistema universitario. Questa visione favorisce la valorizzazione delle iniziative realizzate e rafforza il ruolo dell'Università come soggetto pubblico impegnato in un percorso di innovazione responsabile e sostenibile.

La piena accessibilità dei documenti e dei contenuti digitali rappresenta un ulteriore asse strategico. Il Piano promuove la produzione di documenti conformi ai requisiti tecnici di accessibilità e l'adozione di pratiche redazionali coerenti con gli standard nazionali, garantendo una fruizione inclusiva delle informazioni. Ciò include l'impiego di linguaggi chiari, la correttezza dei metadati, la struttura logica dei testi, l'attenzione agli elementi grafici e la regolare verifica della conformità mediante strumenti di validazione automatica e controlli umani.

In questo quadro integrato, comunicazione, trasparenza e accessibilità assumono un valore determinante non solo per assicurare la conoscibilità delle attività e la conformità normativa, ma anche per rafforzare la dimensione partecipativa della trasformazione digitale, sostenere la cultura del miglioramento continuo e consolidare il ruolo dell'Ateneo quale istituzione aperta, responsabile e orientata al servizio della comunità.

16.1 Piano di comunicazione interna

La comunicazione interna rappresenta uno strumento essenziale per garantire la piena comprensione, condivisione e partecipazione alle azioni previste dal Piano Triennale di Transizione Digitale 2026–2028. In un contesto organizzativo complesso come quello universitario, la diffusione tempestiva e chiara delle informazioni costituisce un prerequisito imprescindibile per assicurare coerenza operativa, ridurre asimmetrie informative, supportare il processo di cambiamento e facilitare l'adozione dei nuovi modelli digitali da parte di tutte le componenti dell'Ateneo.

Il Piano di comunicazione interna definisce un modello strutturato, continuo e multilivello di interazione con il personale tecnico-amministrativo, i docenti, i ricercatori e le strutture di governo, con l'obiettivo di garantire trasparenza nelle decisioni, coordinamento organizzativo e accompagnamento alle innovazioni introdotte. Tale modello si fonda su una comunicazione istituzionale unitaria, coordinata dal Direttore Generale e dal Responsabile per la Transizione Digitale, che assicura coerenza dei messaggi, uniformità dei contenuti e allineamento rispetto alle priorità strategiche del Piano.

La comunicazione avviene attraverso canali consolidati e strumenti digitali istituzionali: l'intranet di Ateneo come punto unico di accesso alle informazioni riservate, la posta elettronica istituzionale per comunicazioni operative e informative, le piattaforme M365 e i canali digitali dedicati alla diffusione di linee guida, istruzioni d'uso, aggiornamenti, materiali formativi e notifiche sui cambiamenti introdotti. L'utilizzo delle piattaforme collaborative consente inoltre di favorire un dialogo più diretto e bidirezionale tra le funzioni responsabili della transizione digitale e le strutture che ne recepiscono gli effetti operativi, promuovendo un approccio partecipativo fondato sul confronto e sul contributo attivo dei destinatari.

Particolare attenzione è dedicata alla comunicazione destinata ai referenti amministrativi, ai coordinatori di processo e alle figure che operano nel presidio quotidiano dei servizi digitali. L'informazione verso questi attori è orientata alla precisione operativa, alla chiarezza procedurale e alla tempestività, con l'obiettivo di assicurare la corretta applicazione delle misure previste e di prevenire disallineamenti nell'attuazione. Allo stesso modo, la comunicazione rivolta alle strutture accademiche valorizza la dimensione funzionale della digitalizzazione nella didattica e nella ricerca, facilitando l'utilizzo dei servizi digitali e promuovendo un modello organizzativo omogeneo nell'interazione con gli strumenti istituzionali.

Il Piano prevede inoltre momenti periodici di condivisione strutturata, quali sessioni informative, webinar istituzionali, presentazioni dei nuovi servizi e incontri di aggiornamento sullo stato di avanzamento delle attività. Queste iniziative contribuiscono a consolidare la consapevolezza dell'intero Ateneo sul percorso di transizione digitale e a rafforzare la cultura del miglioramento continuo, in coerenza con il modello PDCA adottato per la gestione del Piano.

Complessivamente, il Piano di comunicazione interna costituisce un elemento cardine della governance digitale, volto a garantire coesione, partecipazione e consapevolezza diffusa. La qualità della comunicazione interna diventa così un fattore di successo della trasformazione digitale, poiché consente all'Ateneo di attuare un cambiamento realmente condiviso, sostenibile e orientato ai bisogni della comunità universitaria.

16.2 Diffusione e pubblicazione del Piano

La diffusione e la pubblicazione del Piano Triennale di Transizione Digitale costituiscono una fase centrale del ciclo di vita del documento, poiché assicurano trasparenza, accessibilità e piena conoscibilità delle strategie digitali adottate dall'Università di Napoli L'Orientale. In coerenza con le disposizioni del Codice dell'Amministrazione Digitale, delle Linee Guida AgID e degli obblighi previsti dal quadro normativo in materia di trasparenza amministrativa, l'Ateneo garantisce un sistema strutturato di divulgazione interna ed esterna del Piano, volto a promuovere un'informazione chiara e tempestiva verso la comunità universitaria e verso i soggetti istituzionali interessati.

La pubblicazione ufficiale del Piano avviene attraverso la sezione "Amministrazione Trasparente" del portale istituzionale, nella sottosezione dedicata alla "Programmazione" e agli "Obiettivi strategici", assicurando consultabilità pubblica e aggiornamento periodico. Contestualmente, il documento è reso disponibile anche sul sito istituzionale nella sezione

dedicata alla digitalizzazione e ai servizi ICT, affinché le strutture accademiche, gli uffici amministrativi e gli stakeholder possano accedere a una versione sempre aggiornata, completa dei relativi allegati tecnici e degli eventuali atti integrativi emanati nel corso del triennio.

La diffusione interna è coordinata dal Direttore Generale, anche in qualità di Responsabile per la Transizione Digitale, con il supporto del Settore Sviluppo Digitale. Tale processo prevede la trasmissione del Piano alle strutture di governo (Senato Accademico, Consiglio di Amministrazione, Nucleo di Valutazione, Presidio della Qualità), alle direzioni centrali, ai dipartimenti, ai coordinatori dei corsi di studio e ai responsabili di processo, affinché possano integrare le indicazioni strategiche del Piano nelle rispettive attività di programmazione. Il documento viene inoltre reso disponibile sulla intranet istituzionale, accompagnato da una sintesi operativa che evidenzia obiettivi, priorità e responsabilità.

La diffusione presso la comunità studentesca avviene attraverso i canali informativi istituzionali dell'Ateneo, con particolare attenzione alla comunicazione trasparente degli interventi che incidono sui servizi digitali, sull'accessibilità delle procedure e sull'esperienza d'uso delle piattaforme. Tale comunicazione consente agli studenti di comprendere le innovazioni in corso e di orientarsi all'interno dei processi digitali previsti dal Piano.

In un'ottica di accountability e di cooperazione istituzionale, il Piano è inoltre condiviso con i principali enti partner – quali CINECA, ADISURC, GARR, ACN e le reti universitarie di coordinamento – al fine di garantire coerenza, allineamento tecnico e osservanza degli standard nazionali di interoperabilità e sicurezza.

Complessivamente, il sistema di diffusione e pubblicazione garantisce che il Piano Triennale di Transizione Digitale sia non soltanto un documento formale, ma uno strumento realmente operativo, condiviso e fruibile da tutte le componenti dell'Ateneo e dagli stakeholder esterni. La trasparenza nella pubblicazione e la corretta circolazione delle informazioni costituiscono, pertanto, elementi essenziali per il pieno successo del processo di trasformazione digitale delineato dall'Università.

16.3 Accessibilità e fruibilità dei documenti

L'accessibilità e la piena fruibilità della documentazione istituzionale costituiscono un requisito essenziale della trasparenza amministrativa e rappresentano un obbligo per le pubbliche amministrazioni, ai sensi della Legge 4/2004, delle Linee Guida AgID e degli standard internazionali WCAG 2.1. Il presente Piano adotta un approccio orientato alla massima leggibilità, inclusione e conformità, al fine di garantire che tutti gli utenti – compresi coloro che utilizzano tecnologie assistive – possano accedere ai contenuti in modo corretto e senza discriminazioni.

L'Ateneo si impegna pertanto a garantire che la documentazione sia redatta e pubblicata in formati pienamente accessibili, privilegiando strutture del testo chiare, gerarchie di titoli coerenti, contrasti cromatici adeguati, descrizioni alternative degli elementi visivi e metadati completi. Particolare attenzione è riservata alla produzione di versioni digitali fruibili mediante screen reader e alla verifica preventiva dell'accessibilità prima della pubblicazione ufficiale.

Inoltre, il documento sarà reso disponibile attraverso canali istituzionali che ne facilitano la consultazione – sito web, intranet e sezione dedicata dell'Amministrazione Trasparente – garantendo uniformità nella presentazione, aggiornamenti tempestivi e una fruizione ottimizzata anche da dispositivi mobili. La progressiva adozione delle Linee Guida AgID in

materia di design dei servizi digitali orienta l'intero processo, assicurando continuità tra la qualità del contenuto, del formato e dell'esperienza complessiva dell'utente.

Nel suo complesso, la strategia adottata mira a promuovere un modello di comunicazione istituzionale inclusivo, responsabile e pienamente conforme agli standard vigenti, rafforzando la trasparenza dell'Ateneo e la capacità degli utenti di accedere agevolmente alle informazioni relative alla trasformazione digitale.