0103396 del 27/10/2026 - Rep. Delibere del Consiglio di Amministrazione n. 286/2026 - [UOR: SARISS - Class

2026-2030

# Piano di Ateneo per la transizione digitale e la cybersecurity 2026–2030

UNIVERSITÀ DEGLI STUDI DELL'INSUBRIA

# Piano di Ateneo per la transizione digitale e la cybersecurity 2026–2030

Università degli Studi dell'Insubria
Documento di visione – livello strategico

Sommario


1 PREMESSA E INQUADRAMENTO ..... 2
2 LO STATO ATTUALE (AS-IS) DELL'ASSETTO DIGITALE DELL'ATENEO ..... 2
2.1 Analisi SWOT ..... 3
2.2 Processi e servizi ..... 5
2.3 Portafoglio applicativo e integrazione ..... 5
2.4 Dati, qualità informativa e interoperabilità ..... 6
2.5 Didattica digitale e ambienti di apprendimento ..... 6
2.6 Infrastrutture digitali e postazioni di lavoro ..... 6
2.7 Sostenibilità del presidio ICT e capacità di governo ..... 7
2.8 Cybersecurity e continuità operativa ..... 7
2.9 Competenze e capacità organizzative ..... 7
2.10 Contesto esterno e driver di cambiamento ..... 7
3 GOVERNANCE DELLA TRANSIZIONE DIGITALE ..... 8
4 AREE STRATEGICHE DI INTERVENTO NEI DOCUMENTI DI PIANIFICAZIONE STRATEGICA/ OBIETTIVI ..... 8
4.1 Area della didattica digitale e dei servizi agli studenti ..... 8
4.2 Area della Ricerca e innovazione ..... 9
4.3 Amministrazione digitale ..... 9
4.4 Infrastrutture e cybersecurity ..... 9
4.5 Dati, analytics e interoperabilità ..... 9
4.6 Competenze digitali ..... 9
5 STRATEGIA E OBIETTIVI 2026–2030 (STRUTTURA PER PROGRAMMI) ..... 10
Programma 1 – Insubria Secure++ ..... 12
Programma 2 – Insubria AI Governance ..... 13
Programma 3 – Insubria Digital Process ..... 14
Programma 4 – Insubria Data & Analytics ..... 15
Programma 5 – Insubria Digital Campus EVO ..... 16
Programma 6 – Insubria Ecosistema Web ..... 17
Programma 7 – Insubria ICT Academy ..... 18
Programma 8 – ..... 19
6 RACCORDO CON IL PIANO TRIENNALE OPERATIVO AD AGGIORNAMENTO ANNUALE DI TRANSIZIONE DIGITALE ..... 19
7 GOVERNANCE, MONITORAGGIO E AGGIORNAMENTO DEL PIANO ..... 20
7.1 Ciclo di monitoraggio ..... 20
7.2 8 Roadmap strategica 2026–2030 ..... 20
8 APPENDICE A – GLOSSARIO MINIMO (ACRONIMI E DEFINIZIONI) ..... 23

# 1 Premessa e inquadramento

Nel quadro della transizione digitale dell'Università degli Studi dell'Insubria, l'evoluzione del contesto normativo — con particolare riferimento alla **Direttiva NIS2** e al relativo recepimento nazionale — rafforza l'esigenza di governare innovazione digitale, **cybersecurity**, gestione del rischio, continuità operativa e accountability istituzionale. L'Ateneo non parte da zero: molte linee di intervento e numerosi obiettivi in ambito ICT sono già presenti nei documenti di pianificazione, negli obiettivi di performance, nelle iniziative avviate e negli adeguamenti richiesti da driver esterni, in particolare normativi, tecnologici e organizzativi. Il Piano si colloca quindi in coerenza con il **Piano Strategico di Ateneo 2024–2030** e con il **PIAO** di tempo in tempo vigente, contribuendo al presidio dei servizi digitali critici e al miglioramento di servizi, processi, dati, didattica e ricerca.

Il presente **Piano di Ateneo per la transizione digitale e la cybersecurity 2026–2030** — di seguito, il **Piano** — definisce una cornice strategica e organizzativa per l'evoluzione digitale dell'Ateneo. Non introduce un ulteriore livello di programmazione separato, ma organizza, rende leggibili e mette in evidenza, in chiave ICT, piani, indirizzi strategici, obiettivi di performance e strumenti di programmazione già presenti. In questo modo il Piano raccorda iniziative esistenti e nuove priorità in un quadro unitario, evidenziando il contributo di tecnologie digitali, dati, infrastrutture e cybersecurity al perseguimento delle priorità istituzionali. In particolare, il Piano mira a:

- organizzare e valorizzare, in chiave ICT, obiettivi e linee di intervento già presenti nella programmazione di Ateneo;
- integrare piani, indirizzi e obiettivi istituzionali con i principali driver esterni, normativi, tecnologici e organizzativi;
- collocare la transizione digitale nel quadro degli indirizzi strategici di Ateneo, esplicitando principi guida, ambiti prioritari e modello di governance;
- raccordare la visione 2026–2030 con programmazione operativa, monitoraggio e riesame.

Il raccordo con la programmazione operativa è assicurato dal **Piano Triennale operativo ad aggiornamento annuale di Transizione Digitale**, che traduce gli indirizzi strategici in iniziative, responsabilità, indicatori e fabbisogni economici, in coerenza con **PIAO**, controllo di gestione e piattaforma **SPRiNT**.

In coerenza con il **Piano Strategico di Ateneo 2024–2030**, il Piano orienta la transizione digitale verso un ecosistema sicuro, accessibile, integrato e sostenibile, capace di migliorare servizi, didattica, ricerca e amministrazione, valorizzare i dati, presidiare l'eventuale adozione dell'Intelligenza Artificiale e rafforzare il governo dei rischi IT e cyber.

I criteri guida trasversali — centralità dell'utente, interoperabilità, sicurezza e protezione dei dati by design, sostenibilità, presidio interno, innovazione responsabile, misurabilità dei risultati e miglioramento continuo — orientano la lettura delle aree strategiche, la definizione dei programmi e la successiva attuazione operativa.

# 2 Lo Stato attuale (AS-IS) dell'assetto digitale dell'Ateneo

L'ecosistema digitale dell'Università degli Studi dell'Insubria si è sviluppato nel tempo su una **base ampia, concreta e già operativa**, a supporto di didattica, ricerca, terza missione e amministrazione.

L'Ateneo dispone oggi di **piattaforme istituzionali consolidate, servizi digitali diffusi, infrastrutture cloud e SaaS, ambienti per la didattica digitale, strumenti di collaborazione, sistemi di reporting** e prime esperienze di governo dei dati.

La fase 2026–2030 non muove quindi da una condizione iniziale o da una carenza di strumenti, ma dalla necessità di valorizzare in modo più sistematico quanto già disponibile, ridurre frammentazioni residue, rafforzare integrazione, sicurezza e capacità di misurazione e orientare i nuovi investimenti verso ambiti strategici, inclusi servizi avanzati e piattaforme di calcolo a supporto della ricerca.

## 2.1 Analisi SWOT

L'analisi SWOT assume come punto di partenza un assetto digitale già significativo: i punti di forza descrivono un patrimonio da consolidare e rendere più omogeneo, mentre debolezze, opportunità e minacce aiutano a individuare le priorità di evoluzione per il periodo 2026–2030.

| **Punti di forza** | **Punti di debolezza** |
|---|---|
| • Ecosistema digitale già operativo su processi core e servizi istituzionali, con adozione significativa di piattaforme condivise/qualificate (es. ecosistema CINECA in modalità SaaS) come base di standardizzazione e continuità evolutiva.<br>• Per i servizi didattici e amministrativi, workload computazionale ormai sostanzialmente migrato sul cloud Microsoft in coerenza con il percorso di razionalizzazione dei data center pubblici e con gli indirizzi del Cloud della PA successivi alla classificazione dei data center d'Ateneo nel Gruppo B.<br>• Ecosistema per la didattica digitale già evoluto, con LMS in modalità SaaS e automazioni a supporto dell'offerta formativa, servizi video, Aule EVO diffuse e dotazioni professionali per la produzione di contenuti, che costituiscono una base solida per innovazione metodologica e qualità dell'esperienza studente.<br>• Crescente attenzione a data governance, reporting direzionale e uso dei dati per | • Nella didattica digitale, disponibilità di strumenti e dotazioni non sempre accompagnata da analoga consapevolezza metodologica, progettazione interattiva e adeguati meccanismi di accompagnamento o incentivazione dei docenti all'uso pieno delle potenzialità disponibili.<br>• Comprensione non sempre pienamente governata di configurazioni, dipendenze e integrazioni tra sistemi, con rischio di ricorso a lavorazioni parallele, aumento della complessità gestionale e maggiore difficoltà nel gestire il cambiamento in modo uniforme.<br>• In un ecosistema applicativo integrato, qualità del dato in input e responsabilità degli operatori non ancora presidiate in modo pienamente uniforme, con il rischio che errori o incoerenze inseriti a monte producano effetti negativi a cascata su processi, servizi, reportistica e decisioni basate su evidenze.<br>• Presenza di asset e servizi ICT a supporto della ricerca sviluppati in modo |

| | |
|---|---|
| decisioni basate su evidenze, con prime basi concettuali su "fonti autorevoli", qualità informativa e interoperabilità. | distribuito e non sempre governato unitariamente, con rischio di duplicazione di risorse, costi non ottimizzati, gestione eterogenea della sicurezza e ridotta visibilità centrale su infrastrutture e piattaforme scientifiche.<br>• Assetto fortemente dipendente da pochi fornitori chiave per componenti essenziali dell'ecosistema digitale (cloud Microsoft per il workload applicativo e CINECA per un'ampia quota dei sistemi informativi in modalità SaaS) e crescente ricorso a servizi esternalizzati, con necessità di rafforzare non solo governo contrattuale, interoperabilità, reversibilità e presidio architetturale, ma anche la capacità interna di governo delle commesse e di valutazione autonoma della qualità dei servizi. |
| **Opportunità** | **Minacce** |
| • Razionalizzazione del portafoglio applicativo e rafforzamento dell'architettura di integrazione/interoperabilità, riducendo soluzioni ad hoc e abilitando processi più coerenti e sostenibili.<br>• Potenziamento dei servizi self-service e della digitalizzazione end-to-end dei processi prioritari, con misurazione di tempi/qualità e miglioramento dell'esperienza utente per studenti e personale.<br>• Valorizzazione del patrimonio informativo tramite data governance, interoperabilità, analytics e cruscotti direzionali, abilitando decisioni basate su evidenze e un successivo governo prudente di eventuali casi d'uso AI. | • Crescita del rischio IT/cyber (incl. ransomware e compromissione identità) e aumento dei requisiti di presidio, risposta agli incidenti e resilienza dei servizi.<br>• Indebolimento progressivo del presidio ICT interno per riduzione delle risorse umane disponibili e peggioramento della capacità di investimento, con rischio di crescente dipendenza da fornitori esterni, perdita di controllo sulla qualità dei servizi e riduzione delle leve di governo tecnico-organizzativo.<br>• Concentrazione del rischio su un numero molto limitato di fornitori core — in particolare **Microsoft Azure** per il cloud e **CINECA** per una quota rilevante dei sistemi SaaS — con possibili effetti di lock-in tecnologico, contrattuale e operativo, nonché impatti rilevanti su |

| | |
|---|---|
| | continuità ed evoluzione dei servizi in caso di cambiamenti non governati.<br>• Esternalizzazione di servizi operativi rilevanti (assistenza tecnica di primo livello, assistenza didattica in aula, assistenza alla comunicazione, portierato) con rischio, nel medio-lungo periodo, di perdita progressiva di know-how interno, riduzione della capacità di governo delle commesse e crescente dipendenza da soggetti esterni.<br>• Pressione regolatoria e requisiti di conformità in materia di cybersicurezza, che impongono maggiore formalizzazione di controlli, gestione del rischio, governo della supply chain ICT, continuità operativa, capacità di notifica degli incidenti e responsabilizzazione dei vertici, con aumento del rischio di non conformità se tali presìdi non vengono consolidati. |

Alla luce dello stato attuale, la transizione digitale richiede un assetto di governo chiaro, capace di assicurare coerenza strategica, priorità condivise e monitoraggio continuativo.

I paragrafi che seguono specificano e articolano, per ambiti tematici, gli elementi sintetizzati nella tabella SWOT, evidenziando le principali evidenze dell'assetto AS-IS e le priorità di evoluzione che ne derivano. Il quadro di governance è definito di seguito nei suoi elementi essenziali e sviluppato, per quanto riguarda monitoraggio e aggiornamento del Piano, nella sezione **"Governance, monitoraggio e aggiornamento del Piano"**.

## 2.2 Processi e servizi

L'Ateneo dispone già di una copertura ampia dei processi core attraverso piattaforme istituzionali, con un utilizzo esteso dell'ecosistema CINECA e di altri servizi digitali consolidati. Il quadro AS-IS evidenzia quindi un livello di digitalizzazione non iniziale, nel quale la priorità non è introdurre strumenti di base, ma aumentare maturità d'uso, uniformità organizzativa, conoscenza dei workflow e qualità delle integrazioni tra sistemi, accompagnando nel tempo l'adozione da parte delle strutture.

## 2.3 Portafoglio applicativo e integrazione

Il portafoglio applicativo dell'Ateneo si fonda su una base ampia e strutturata, con forte presenza di soluzioni core condivise e un livello elevato di copertura applicativa. Una quota molto significativa dei sistemi informativi istituzionali, in particolare nell'area amministrativa e gestionale, è oggi fornita in

modalità **SaaS** attraverso l'ecosistema **CINECA**, con benefici in termini di standardizzazione, continuità evolutiva e allineamento al sistema universitario nazionale. Il tema strategico non è quindi colmare un vuoto applicativo, ma governare meglio ciclo di vita, configurazioni, integrazioni, punti di accesso e conoscenza d'uso dei sistemi adottati, così da valorizzare pienamente le funzionalità disponibili e ridurre lavorazioni manuali o parallele nate da uso incompleto o non omogeneo.

## 2.4 Dati, qualità informativa e interoperabilità

Il patrimonio informativo dell'Ateneo è già alimentato da numerosi sistemi gestionali e servizi digitali integrati, che producono dati rilevanti per processi, servizi, reportistica e decisioni. Proprio questa ricchezza informativa richiede regole più strutturate su fonti autorevoli, qualità del dato, catalogazione, reporting e interoperabilità, in un contesto in cui il medesimo dato viene inserito una volta e riutilizzato molte volte. Diventa quindi essenziale che tutti gli operatori coinvolti nella filiera siano consapevoli della qualità richiesta in input, poiché errori o incoerenze nei dati possono produrre effetti negativi a cascata su processi, servizi, reportistica e decisioni basate su evidenze. **[Piano Strategico di Ateneo 2024–2030 – Pag. 7; Pag. 9]**

## 2.5 Didattica digitale e ambienti di apprendimento

L'Ateneo dispone di un **ecosistema per la didattica digitale già evoluto**, basato su piattaforme LMS in modalità SaaS, servizi video, automazioni a supporto dell'offerta formativa, **aule ibride diffuse** e dotazioni professionali per la **produzione di contenuti**. Questo patrimonio costituisce una base solida per l'innovazione metodologica, la qualità dell'esperienza studente, l'accessibilità dei percorsi formativi e la continuità dei servizi didattici anche in contesti ibridi o tecnologicamente mediati.

La priorità evolutiva riguarda quindi la **piena valorizzazione delle funzionalità disponibili**. Diventano centrali la **progettazione didattica più moderna e interattiva**, la maggiore consapevolezza d'uso da parte dei docenti, l'accompagnamento metodologico-tecnologico, la valorizzazione dei servizi video e degli ambienti di produzione contenuti, nonché meccanismi strutturati di raccolta del feedback e monitoraggio della qualità percepita da studenti e docenti.

## 2.6 Infrastrutture digitali e postazioni di lavoro

Le infrastrutture digitali e di rete costituiscono la base abilitante dei servizi dell'Ateneo. Per i servizi didattici e amministrativi, il relativo **workload computazionale** risulta ormai sostanzialmente migrato sul cloud Microsoft, in coerenza con il percorso nazionale di razionalizzazione dei data center pubblici avviato da **AgID** e con gli indirizzi del **Cloud della PA**, anche a seguito della classificazione dei data center dell'Ateneo nel **Gruppo B**, categoria riferita a infrastrutture da migrare verso il cloud della PA in quanto non qualificate come poli strategici o data center adeguati all'evoluzione interna. Questo assetto ha consentito maggiore standardizzazione, scalabilità e continuità dei servizi, ma rende al tempo stesso ancora più rilevanti il governo architetturale, la reversibilità, il presidio delle configurazioni, il monitoraggio e la gestione del rischio di concentrazione tecnologica su un numero limitato di fornitori.

## 2.7 Sostenibilità del presidio ICT e capacità di governo

Si rileva una crescente pressione sulla sostenibilità del presidio ICT interno, dovuta sia alla dinamica delle risorse umane sia al peggioramento della capacità di investimento, in particolare sugli investimenti in conto capitale relativi a dotazioni e ambienti tecnologici. In tale contesto, il ricorso a supporti esterni rappresenta in molti casi una scelta necessaria, anche alla luce di un mercato del lavoro poco favorevole al reclutamento e alla permanenza di profili ICT ad alta qualificazione, soprattutto in un territorio fortemente esposto alla concorrenza salariale della vicina Svizzera. Questa necessità, tuttavia, fa emergere i rischi strutturali di una esternalizzazione sempre più spinta. Una quota rilevante di servizi operativi a diretto impatto sull'esperienza d'uso — quali **assistenza tecnica di primo livello**, **assistenza didattica in aula**, **assistenza alla comunicazione** e **portierato** — è oggi esternalizzata. Tale configurazione può risultare efficiente nel breve periodo, ma nel medio-lungo termine può comportare **perdita di know-how interno**, riduzione della capacità di accumulare competenze organizzative e progressivo indebolimento della capacità di **governare le commesse** e valutare con piena autonomia qualità, priorità e livelli di servizio. A ciò si aggiunge il fatto che i fornitori operano fisiologicamente secondo logiche commerciali proprie, non sempre perfettamente coincidenti con l'interesse istituzionale dell'Ateneo e con l'esigenza di preservare nel tempo autonomia, controllo e capacità di indirizzo. Per queste ragioni, il ricorso all'esternalizzazione deve rimanere compatibile con il mantenimento di un solido presidio interno sulle funzioni di governo, controllo, architettura, qualità e valutazione del servizio.

## 2.8 Cybersecurity e continuità operativa

La cybersecurity costituisce un importante presidio strutturale della **transizione digitale** e richiede un rafforzamento continuo di governance, gestione del rischio, protezione di identità ed endpoint, monitoraggio degli eventi, compliance e continuità operativa, in coerenza con l'evoluzione dei servizi e del quadro regolatorio. Questo rende particolarmente rilevanti, per l'Ateneo, la formalizzazione dei controlli, la documentabilità delle misure, il governo dei fornitori critici e la capacità di dimostrare in modo continuo l'adeguatezza del proprio assetto di sicurezza. **[Piano Strategico di Ateneo 2024–2030 – Pag. 7; Pag. 9]**

## 2.9 Competenze e capacità organizzative

Le competenze digitali presenti costituiscono una base importante, ma richiedono un consolidamento più strutturato e continuo, e un ampliamento dell'organico per sostenere l'evoluzione dei sistemi, il turn-over del personale e la piena valorizzazione delle piattaforme attive. Diventano quindi centrali formazione continua, knowledge transfer, *onboarding* sui processi e sulle soluzioni, chiarificazione di ruoli e responsabilità e un modello operativo che renda scalabile l'innovazione attraverso raccolta della domanda, prioritizzazione e gestione del portafoglio iniziative.

## 2.10Contesto esterno e driver di cambiamento

L'evoluzione del contesto esterno influenza in modo crescente le priorità digitali degli Atenei. In particolare:

- **Aspettative degli utenti**: studenti e personale richiedono servizi digitali affidabili, accessibili, coerenti e fruibili su più dispositivi, con esperienze di accesso unificate.

- **Pressione regolatoria e requisiti di conformità**: cybersecurity, protezione dei dati, accessibilità e obblighi di rendicontazione richiedono approcci strutturati e documentabili.
- **Interoperabilità e integrazione con sistemi nazionali**: l'integrazione con piattaforme e standard di riferimento aumenta la necessità di architetture coerenti e gestione delle API.
- **Evoluzione tecnologica, dati e AI**: la crescente disponibilità di strumenti avanzati rende strategico, da un lato, il governo del dato, delle fonti autorevoli e dell'interoperabilità e, dall'altro, la definizione di regole comuni per valutare eventuali usi dell'AI. Gli impatti potenziali riguardano servizi, processi, didattica, ricerca e profili amministrativi e di compliance, con particolare rilievo per valutazioni privacy, coinvolgimento del **DPO** e, ove necessario, stesura di **DPIA**. **[Piano Strategico di Ateneo 2024–2030 – Pag. 7]**

# 3 Governance della transizione digitale

L'assetto di governo della transizione digitale è definito per assicurare coerenza strategica, priorità condivise, capacità di indirizzo e monitoraggio continuativo. Esso si fonda su una chiara attribuzione di responsabilità tra indirizzo strategico, coordinamento, attuazione tecnica e supporto alla prioritizzazione.

I soggetti potenzialmente coinvolti potrebbero essere:

- **Rettrice/Prorettore vicario**: indirizzo politico-strategico.
- **Delegata della Rettrice per i sistemi informativi, la cybersecurity e la transizione digitale e Delegato della Rettrice all'intelligenza artificiale:** indirizzo politico – strategico tematico
- **Direzione Generale**: coordinamento delle politiche digitali.
- **Responsabile della Transizione Digitale (RTD)**: garante dell'allineamento alle linee guida e del governo complessivo della trasformazione digitale.
- **Area Risorse Infrastrutturali, Strumentali e Sistemi Informativi (ARISS)** : attuazione tecnica e gestione delle infrastrutture.
- **Eventuali gruppi di lavoro tematici**: didattica digitale, ricerca, cybersecurity, processi amministrativi, dati e analytics, AI governance.

# 4 Aree strategiche di intervento nei documenti di pianificazione strategica/ obiettivi

Le **aree strategiche** forniscono una cornice sintetica degli ambiti in cui la transizione digitale genera valore per l'Ateneo. In questa sezione sono richiamate in forma essenziale le principali direttrici, mentre la sezione **"Strategia e obiettivi 2026–2030 (struttura per programmi)"** sviluppa l'attuazione attraverso i programmi.

## 4.1 Area della didattica digitale e dei servizi agli studenti

L'area riguarda un ecosistema per la didattica digitale e i servizi agli studenti già evoluto e non basico, che comprende piattaforme SaaS consolidate per e-learning e gestione della didattica (incluse automazioni sull'offerta formativa), servizi video, aule ibride diffuse e dotazioni professionali per la produzione di contenuti. La priorità strategica non è quindi l'introduzione di strumenti elementari, ma la loro piena

valorizzazione attraverso progettazione didattica più moderna e interattiva, maggiore consapevolezza d'uso e accompagnamento dei docenti all'adozione. **[Politiche Offerta Formativa 2026/27 – Pag. 5; Pag. 7; Pag. 8]**

## 4.2 Area della Ricerca e innovazione

L'area comprende il rafforzamento delle infrastrutture e dei servizi digitali per la ricerca, la valorizzazione dei dati di ricerca, l'interoperabilità dei repository e il supporto a progettualità avanzate su HPC, analytics, AI, cybersecurity, Digital Humanities e Digital Health, secondo un approccio interdisciplinare e conforme. **[DBSV 2025–2027 – Pag. 20–21; DiSTA 2025–2027 – Pag. 19–20; DMC 2025–2027 – Pag. 21–22]**

Il supporto ICT alla ricerca presenta inoltre un'evoluzione storicamente più distribuita e dipartimentale rispetto ai servizi ICT centrali di Ateneo. Questa configurazione, pur avendo favorito flessibilità e aderenza ai fabbisogni scientifici locali, può determinare frammentazione delle infrastrutture, duplicazione di risorse di calcolo, ricorso non governato a servizi cloud, gestione eterogenea di sale macchine e piattaforme scientifiche e livelli non uniformi di sicurezza, compliance e sostenibilità economica.

## 4.3 Amministrazione digitale

L'area riguarda la digitalizzazione end-to-end dei processi amministrativi e gestionali, con obiettivi di standardizzazione, dematerializzazione, servizi self-service, monitoraggio continuo delle pratiche e riduzione delle criticità operative. Eventuali sperimentazioni AI a supporto dei flussi amministrativi sono ricondotte al quadro di governance previsto dal Programma 2. **[DiECO 2025–2027 – Pag. 39; DiSAT 2025–2027 – Pag. 29–30]**

## 4.4 Infrastrutture e cybersecurity

L'area riguarda il rafforzamento delle infrastrutture digitali e dei presìdi di sicurezza come base abilitante dei servizi di Ateneo: reti e accesso, resilienza, continuità operativa, gestione delle identità, protezione degli endpoint e adozione progressiva di modelli di sicurezza più maturi. **[Piano Strategico di Ateneo 2024–2030 – Pag. 7; Pag. 9]**

## 4.5 Dati, analytics e interoperabilità

L'area riguarda la valorizzazione del patrimonio informativo di Ateneo attraverso data governance, analytics, interoperabilità con ecosistemi nazionali e strumenti di tracciabilità e misurazione, con particolare attenzione ai domini utili al governo, alla performance e alla terza missione. **[DiDEC 2025–2027 – Pag. 12; DiSUIT 2025–2027 – Pag. 14]**

## 4.6 Competenze digitali

L'area riguarda lo sviluppo continuo delle competenze digitali della comunità di Ateneo, includendo alfabetizzazione, formazione specialistica, faculty development, awareness su sicurezza, data literacy e uso

consapevole dell'AI, in raccordo con i programmi Insubria ICT Academy e Insubria AI Governance. **[Piano Strategico di Ateneo 2024–2030 – Pag. 21; Politiche Offerta Formativa 2026/27 – Pag. 7]**

# 5 Strategia e obiettivi 2026–2030 (struttura per programmi)

Il Piano organizza gli interventi in **programmi** che raccolgono iniziative e progetti coordinati. Ogni programma dovrà essere tradotto, a livello operativo, in un portafoglio di iniziative con milestone, responsabilità e indicatori nel **Piano Triennale operativo ad aggiornamento annuale di Transizione Digitale**. La progettazione e l'attuazione dei programmi seguono criteri trasversali comuni: chiara attribuzione di responsabilità, misurazione dei risultati e miglioramento continuo, sicurezza, privacy e accessibilità by design, interoperabilità e uso di standard, presidio interno delle funzioni critiche, sviluppo delle competenze e accompagnamento al cambiamento.

La tabella seguente fornisce una vista sintetica e comparabile dei programmi, utile a evidenziare priorità, stato iniziale, principali fasi temporali, impatto economico e interdipendenze. Le indicazioni hanno valore orientativo e saranno dettagliate nel **Piano Triennale operativo ad aggiornamento annuale di Transizione Digitale**, anche in termini di owner, milestone, KPI e coperture economiche.

| Programma | Priorità | Stato iniziale | Macro-fasi / deadline indicative | Impatto economico | Natura costi | Dipendenze principali |
|---|---|---|---|---|---|---|
| **1 – Insubria Secure++ Cybersecurity, resilienza e asset critici** | Alta | Da rafforzare su base già attiva | 2026 assessment e adeguamento NIS2; 2027–2028 messa a regime dei presìdi; 2029–2030 riesame e rafforzamento. | Alto | OPEX + CAPEX | Tutti i programmi; in particolare Data, Campus, Web e AI Governance. |
| **2 – Insubria AI Governance Uso responsabile e presidiato dell'AI** | Alta / abilitante | Da strutturare | 2026 regole, processo e registro; 2027 sperimentazioni controllate; 2028–2030 monitoraggio, riesame e scaling selettivo. | Medio | OPEX prevalente | Data & Analytics, Web, Digital Campus, Digital Process, ICT Academy. |
| **3 – Insubria Digital Process Processi amministrativi end-to-end** | Alta | Da consolidare | 2026 process inventory e priorità; 2027–2028 reingegnerizzazione dei processi critici; 2029–2030 estensione e miglioramento continuo. | Medio / alto | OPEX + CAPEX selettivo | Data & Analytics, ICT Academy, Secure++, Ecosistema Web. |
| **4 – Insubria Data & Analytics Data governance e reportistica certificata** | Alta / abilitante | Avviato, da strutturare | 2026 modello di data governance e fonti autorevoli; 2027 cruscotti prioritari; 2028–2030 estensione, qualità e interoperabilità. | Medio / alto | OPEX + CAPEX | Digital Process, AI Governance, Governance, PIAO, controllo di gestione. |
| **5 – Insubria Digital Campus EVO Didattica, servizi studenti e ambienti digitali** | Alta | Base avanzata da valorizzare | 2026 standard, backlog e priorità; 2027–2028 evoluzione aule, piattaforme e servizi; 2029–2030 riesame, refresh e scalabilità. | Alto | CAPEX + OPEX | Secure++, ICT Academy, AI Governance, Ecosistema Web. |

| | | | | | | |
|---|---|---|---|---|---|---|
| **6 – Insubria Ecosistema Web Portali, accessibilità, UX e contenuti** | Media / abilitante | Avviato | 2026 governance, backlog e standard editoriali; 2027 accessibilità, UX e qualità contenuti; 2028–2030 estensione e misurazione. | Medio | OPEX prevalente | Data & Analytics, AI Governance, ICT Academy, Digital Process. |
| **7 – Insubria ICT Academy Competenze digitali e change management** | Abilitante | Da strutturare | 2026 modello, catalogo e target; 2027–2028 erogazione e rete key user; 2029–2030 stabilizzazione e misurazione dell'impatto. | Medio / basso | OPEX | Tutti i programmi, con particolare rilievo per Processi, Campus, Data e AI. |
| **8 – Insubria AI e Big Data Platform Piattaforma scientifica per AI e Big Data** | Strategica / selettiva | Da validare | 2026 studio di fattibilità e governance; 2027 decisione di investimento; 2028–2030 realizzazione, servizi e scaling selettivo. | Alto | CAPEX + OPEX | Ricerca, Secure++, Data & Analytics, AI Governance, infrastrutture. |

**Legenda sintetica**: rosso chiaro = priorità o impatto economico alto; arancione chiaro = impatto medio o medio/alto; verde chiaro = impatto medio/basso; blu chiaro = programma abilitante o trasversale. L'impatto economico è espresso a livello qualitativo e non sostituisce la stima analitica demandata al Piano Triennale operativo.

## 1 Programma 1 – Insubria Secure++

*Cybersecurity, resilienza e governo degli asset critici*

**Obiettivo**: aumentare resilienza e continuità dei servizi digitali, rafforzando infrastrutture, monitoraggio e cybersecurity (security by design), con capacità strutturata di prevenzione, rilevazione e risposta agli incidenti, includendo la protezione di **identità digitali** ed **endpoint** come superfici di attacco prioritarie e preservando il presidio interno delle funzioni critiche di governo, architettura, qualità e controllo.

**Linee di azione:**

- **Governance cyber e adeguamento NIS2**: rafforzamento di ruoli, responsabilità, misure di gestione del rischio, presidio documentale, incident reporting e governo della supply chain ICT, in coerenza con il quadro europeo e nazionale.
- **Identity, access ed endpoint security**: messa a regime del ciclo di vita delle identità digitali, provisioning/deprovisioning, conditional access, baseline di sicurezza, patching, cifratura, EDR e reportistica di compliance.
- **Monitoraggio, SOC e risposta agli incidenti**: valutazione di un presidio SOC unitario, preferibilmente a servizio gestito, con funzioni di indirizzo, escalation, controllo e valutazione della qualità mantenute in capo all'Ateneo.
- **Raccordo con CSIRT Italia e ACN**: formalizzazione di canali, ruoli e procedure per monitoraggio degli alert, gestione delle segnalazioni, notifica degli incidenti e integrazione con i flussi nazionali.
- **Asset critici e infrastrutture per la ricerca**: censimento e governo unitario di calcolo, storage, sale macchine, piattaforme scientifiche e ambienti cloud, con criteri condivisi su sicurezza, lifecycle e sostenibilità.
- **Continuità operativa e disaster recovery**: definizione e verifica di presìdi, priorità, scenari, responsabilità e piani di ripristino per i servizi digitali critici.

## 2 Programma 2 – Insubria AI Governance

*Uso responsabile, conforme e presidiato dell'intelligenza artificiale*

**Obiettivo**: definire un quadro di Ateneo per la valutazione, l'eventuale sperimentazione e l'adozione responsabile di soluzioni di Intelligenza Artificiale, assicurando coerenza con le finalità istituzionali, protezione dei dati, sicurezza, qualità delle fonti, trasparenza, accessibilità, supervisione umana e sostenibilità organizzativa. Il programma non assume l'AI come soluzione generalizzata, ma come ambito da presidiare con regole comuni, competenze adeguate e processi di valutazione preventiva.

**Linee di azione:**

- **Linee guida di Ateneo sull'AI**: definizione di principi, perimetri d'uso, responsabilità, limiti e casi da sottoporre a valutazione rafforzata nei diversi contesti istituzionali.
- **Processo di valutazione dei casi d'uso**: scheda istruttoria per finalità, dati trattati, benefici attesi, rischi, sicurezza, privacy, accessibilità, impatti organizzativi e necessità di DPIA.
- **Registro delle sperimentazioni AI**: censimento dei casi proposti, avviati o in esercizio, con owner, strumenti, dati trattati, stato, decisioni assunte, misure di mitigazione e monitoraggio.
- **Usi assistivi e a basso rischio**: eventuali sperimentazioni per ricerca informativa, sintesi documentale, knowledge base, supporto agli operatori, triage e automazioni di back-office, con supervisione umana e controllo delle fonti.
- **Didattica, ricerca e ambiti sensibili**: supporto a linee guida e consapevolezza, con esclusione di automatismi decisionali, valutazioni individuali non presidiate e sostituzione del giudizio umano o degli organi competenti.
- **Privacy, sicurezza e compliance**: coinvolgimento di sicurezza ICT, RTD, DPO e strutture responsabili nei casi con dati personali, impatti organizzativi rilevanti o rischi per diritti, libertà e continuità dei servizi.
- **Competenze, monitoraggio e riesame**: percorsi di AI literacy in raccordo con **Insubria ICT Academy** e verifica periodica di efficacia, rischi, qualità degli output, conformità e necessità di revisione o dismissione.

## 3 Programma 3 – Insubria Digital Process

*Processi, servizi amministrativi e digitalizzazione end-to-end*

**Obiettivo**: realizzare una digitalizzazione end to end dell'amministrazione che valorizzi in modo più maturo, uniforme e integrato i sistemi già disponibili, rafforzando standardizzazione dei processi, governabilità dei workflow e qualità dei servizi, e riducendo lavorazioni parallele, tempi di attraversamento e duplicazioni informative non necessarie.

**Linee di azione:**

- mappatura e prioritizzazione dei processi end-to-end (process inventory) con definizione di owner, criticità e benefici attesi;
- reingegnerizzazione e **digitalizzazione** dei processi prioritari, con standardizzazione di moduli, workflow e firme;
- integrazione con i sistemi core (es. suite gestionali) e riduzione di duplicazioni informative tramite regole di interoperabilità e API;
- sviluppo di **servizi self-service** e sportelli digitali, con tracciabilità dello stato pratica e notifiche;
- misurazione sistematica di tempi, volumi e qualità (lead time, rework) e ciclo di miglioramento continuo, con supporto a change management e formazione degli utenti (raccordo con **Insubria ICT Academy**).

## 4 Programma 4 – Insubria Data & Analytics

*Data governance, qualità del dato, interoperabilità e reportistica certificata*

**Obiettivo**: valorizzare il patrimonio informativo di Ateneo attraverso data governance, qualità del dato, interoperabilità, analytics e reportistica certificata, rafforzando la capacità dell'Ateneo di assumere decisioni basate su evidenze, rendere più tracciabili e riutilizzabili i dati prodotti nei processi istituzionali e migliorare la coerenza dei cruscotti direzionali e degli indicatori.

Il programma valorizza attività già avviate su sistemi gestionali, strumenti di controllo, servizi digitali, cruscotti CINECA e Power BI, con l'obiettivo di rendere più affidabile, governato e riutilizzabile il patrimonio informativo di Ateneo.

**Linee di azione:**

- **Data governance e fonti autorevoli**: definizione di ruoli, responsabilità, domini informativi, data owner e data steward, con regole condivise su qualità, aggiornamento, riuso, accesso e responsabilità del dato.
- **Qualità del dato**: rafforzamento dei controlli sul dato in input e consapevolezza degli effetti a cascata di errori o incoerenze su processi, servizi, reportistica e decisioni basate su evidenze.
- **Base dati per analisi e report**: costruzione progressiva di una base dati comune per gli ambiti prioritari, senza sostituire i sistemi gestionali di origine, distinguendo analisi di lavoro e report ufficiali.
- **Cruscotti direzionali e reportistica certificata**: sviluppo dei cruscotti già realizzati con **CINECA** e **Power BI**, estendendone copertura, qualità e integrazione per governo, programmazione, performance, AVA3, PIAO e controllo di gestione.
- **Interoperabilità e API**: governo delle integrazioni tra sistemi interni ed ecosistemi nazionali, inclusi ove applicabile PDND, SPID/CIE, pagoPA, sistemi MUR e altre basi dati pubbliche.
- **Dati dei servizi digitali e data literacy**: uso strutturato di ticket, log, analytics web, feedback e indicatori di qualità, con sviluppo di competenze diffuse in raccordo con **Insubria ICT Academy**.

## 5 Programma 5 – Insubria Digital Campus EVO

*Didattica, esperienza studente e innovazione metodologica*

**Obiettivo**: valorizzare e integrare un ecosistema già avanzato di servizi e piattaforme per la didattica e l'esperienza studente, aumentando la qualità dell'adozione da parte dei docenti, la progettazione didattica in modalità moderna e interattiva e la piena utilizzazione delle funzionalità disponibili.

Il programma parte da piattaforme LMS/video in modalità SaaS, automazioni a supporto dell'offerta formativa, aule evolute e dotazioni professionali già disponibili. La sfida strategica è renderne più sistematico l'uso avanzato, integrato e metodologicamente consapevole.

**Linee di azione:**

- **Piattaforme didattiche e video**: consolidamento di LMS, servizi video e integrazioni con l'offerta formativa, valorizzando funzionalità avanzate, standard di servizio, accessibilità e tracciamento delle attività.
- **Esami digitali e automazioni**: introduzione o consolidamento di una piattaforma per prove di valutazione integrata con **Esse3**, con workflow tracciabili, onboarding docenti e supporto operativo in raccordo con **Insubria ICT Academy**.
- **Aule EVO e spazi didattici**: standardizzazione e scalabilità delle aule ibride, ammodernamento delle aule non ibride, dotazioni AV minime, manutenzione programmata e attenzione a comfort, qualità audio e affidabilità.
- **Didattica immersiva e simulazione**: sviluppo selettivo di VR/AR e mondi virtuali, con requisiti di integrazione LMS, gestione della flotta dispositivi e raccordo con i presìdi di sicurezza del **Programma 1 – Insubria Secure++**.
- **Accessibilità e qualità dei servizi studenti**: audit periodici, backlog di correzioni e miglioramento di usabilità e accessibilità dei principali portali, procedure e servizi informativi.
- **Supporto ai docenti e faculty development**: knowledge base, FAQ, guide, onboarding metodologico-tecnologico, casi d'uso, community of practice e valorizzazione di servizi video e studio di registrazione.
- **Ticketing, feedback e qualità percepita**: sistema unificato per richieste su aule e servizi digitali, triage, SLA, escalation, raccolta strutturata di feedback e rendicontazione periodica.
- **Sperimentazioni controllate**: eventuali strumenti di supporto alla didattica, incluse componenti AI presenti nelle piattaforme, nel quadro del **Programma 2 – Insubria AI Governance**.

## 6 Programma 6 – Insubria Ecosistema Web

*Web istituzionale, accessibilità e qualità dell'esperienza utente*

**Obiettivo**: rafforzare l'ecosistema web come infrastruttura istituzionale integrata di Ateneo, a supporto di comunicazione, servizio all'utenza, qualità dell'informazione e accesso ai servizi digitali, valorizzando il ruolo del **Polo di coordinamento e indirizzo dell'Ecosistema Web di Ateneo** quale presidio stabile di governance editoriale, coerenza informativa, accessibilità, usabilità e integrazione tra portali, applicazioni e contenuti.

Il programma accompagna il percorso già avviato per superare la frammentazione informativa e costruire una filiera web integrata tra portale istituzionale, sito inglese, intranet, siti di struttura, Course Catalogue, UniFind, Amministrazione Trasparente, web application verticali e servizi digitali.

**Linee di azione:**

- **Governance del Polo**: consolidamento del Polo di coordinamento e indirizzo dell'Ecosistema Web di Ateneo come raccordo stabile tra comunicazione, strutture, redazione distribuita e presidio tecnico.
- **Filiera integrata dei sistemi web**: coordinamento di portali, siti di struttura, Course Catalogue, UniFind, intranet, Amministrazione Trasparente e web application, con continuità dei percorsi utente.
- **Qualità dei contenuti**: linee guida editoriali, modelli di pagina, workflow di pubblicazione, responsabilità sui contenuti, verifiche di aggiornamento e formazione della rete dei redattori.
- **Accessibilità, inclusività e conformità**: accessibilità by design, audit periodici, monitoraggio delle non conformità, backlog di correzioni e allineamento alle evoluzioni normative.
- **Esperienza utente, SEO e misurazione**: miglioramento di navigazione, ricerca interna, architettura informativa, performance, indicizzazione e analytics a supporto delle priorità.
- **Servizi digitali e contenuti multimediali**: integrazione di FAQ, simulatori, pagine di servizio, strumenti di orientamento e contenuti video istituzionali, inclusa la valorizzazione di **InsubriaPlay**.
- **Sperimentazioni controllate**: valutazione di assistenti digitali e funzioni AI per ricerca, navigazione e gestione contenuti, nel quadro del **Programma 2 – Insubria AI Governance**.

## 7 Programma 7 – Insubria ICT Academy

*Competenze digitali, uso dei sistemi e change management*

**Obiettivo**: **Insubria ICT Academy** sviluppa competenze digitali e operative di PTA e docenti, in raccordo con il percorso di mappatura e sviluppo delle competenze coerente con il progetto **RIVA** della Funzione Pubblica, l'applicativo **Minerva** e l'integrazione delle indicazioni in **HR Suite di CINECA**. Il programma ha una funzione complementare e pratica: consolidare uno skill digitale di base, secondo un modello assimilabile a **ICDL** — evoluzione dell'ex **ECDL** — e accompagnare l'uso concreto di sistemi gestionali, piattaforme digitali e servizi ICT di Ateneo.

**Linee di azione:**

- **Raccordo competenze e HR Suite**: collegamento con il percorso di Ateneo su mappatura e sviluppo delle competenze, progetto **RIVA**, applicativo **Minerva** e integrazione in **HR Suite di CINECA**.
- **Skill digitale di base**: definizione di un livello minimo di competenza digitale, secondo un modello assimilabile a **ICDL** — evoluzione dell'ex **ECDL** — quale prerequisito trasversale per l'uso consapevole degli strumenti ICT.
- **Formazione operativa PTA**: piano annuale su strumenti digitali, sicurezza, data literacy, processi e servizi, con onboarding e knowledge transfer sull'uso corretto di sistemi e funzionalità.
- **Key user e casi d'uso reali**: laboratori brevi, dimostrazioni operative e materiali pratici su applicativi, workflow e sistemi gestionali in uso, integrando ma non duplicando la formazione specialistica dei fornitori.
- **Docenti e faculty development**: percorsi su didattica digitale, metodologie, uso critico degli strumenti digitali e consapevolezza sull'AI in raccordo con il **Programma 2 – Insubria AI Governance**.
- **Change management e supporto di prossimità**: comunicazione, kit di adozione, onboarding ai servizi, rete di key user/ambassador e continuità nei passaggi di ruolo.
- **Portfolio formativo e impatto**: governo di calendario, priorità e target, misurazione dell'efficacia e raccordo con awareness cybersecurity, data literacy, accessibilità e strumenti di mappatura delle competenze.

## 8 Programma 8 – Insubria AI e Big Data Platform

*Piattaforma scientifica dedicata alla AI e Big Data*

**Obiettivo:** valutare e, se sostenibile, sviluppare una piattaforma istituzionale di Ateneo per applicare tecniche di analytics avanzati e, ove appropriato, di Intelligenza Artificiale all'analisi di dati trasversali dell'Ateneo, al fine di produrre modelli previsionali, indicatori evoluti e strumenti di supporto alle decisioni. Il programma riguarda domini informativi generali quali carriere studenti, didattica, servizi digitali, processi amministrativi, indicatori di performance, qualità percepita e utilizzo delle piattaforme istituzionali. Sono esclusi dal perimetro i dati di ricerca, le infrastrutture scientifiche dipartimentali, le scelte metodologiche e le progettualità autonome dei singoli Dipartimenti.

Il programma ha carattere selettivo e non introduce automatismi decisionali: eventuali analisi, modelli o strumenti AI sono utilizzati solo a supporto degli organi e delle strutture competenti, con supervisione umana, qualità del dato, trasparenza, sicurezza, protezione dei dati personali e raccordo con il Programma 2 – Insubria AI Governance e il Programma 4 – Insubria Data & Analytics. Si raccorda inoltre con il Programma 1 – Insubria Secure++ per i presìdi di sicurezza, con il Programma 3 – Insubria Digital Process per i dati e gli indicatori dei processi amministrativi, con il Programma 5 – Insubria Digital Campus EVO per i dati relativi a didattica e servizi agli studenti, con il Programma 6 – Insubria Ecosistema Web per analytics e qualità dell'esperienza utente, e con il Programma 7 – Insubria ICT Academy per competenze, data literacy e accompagnamento all'uso consapevole degli strumenti**.**

**Linee di azione:**

• **Perimetro e fattibilità:** definizione del perimetro istituzionale, verifica delle fonti dati disponibili, dei requisiti privacy e sicurezza, dei costi e del modello di gestione.

• **Casi d'uso prioritari:** selezione di pochi casi ad alto valore per l'Ateneo, come analisi del rischio di abbandono, monitoraggio delle carriere studenti, qualità dei servizi digitali, andamento dei processi amministrativi e supporto a programmazione, performance e assicurazione della qualità.

• **Analytics avanzati e decision support:** sperimentazione controllata di tecniche statistiche, machine learning e AI su dati istituzionali governati, con risultati spiegabili e usati come supporto istruttorio, non come decisione automatica.

• **Ambiente analitico evoluto:** eventuale realizzazione progressiva di un ambiente di analisi avanzata, alimentato da fonti autorevoli, tracciabile nelle trasformazioni e distinto dai sistemi gestionali di origine.

• **Validazione e scaling selettivo:** avvio per sperimentazioni circoscritte, misurazione di benefici, rischi e sostenibilità, con estensione solo dopo validazione tecnica, organizzativa, giuridica ed economica.

# 6 Raccordo con il Piano Triennale operativo ad aggiornamento annuale di Transizione Digitale

Il presente **Piano**, in quanto documento strategico riferito al periodo **2026–2030**, non include un piano finanziario di dettaglio. La sostenibilità economica della strategia è assicurata attraverso il **Piano Triennale operativo ad aggiornamento annuale di Transizione Digitale**, che traduce i programmi strategici in iniziative prioritarie, tempi di attuazione, responsabilità esecutive e coperture economiche coerenti con il ciclo di bilancio di Ateneo. In tale strumento attuativo, il Piano viene declinato in termini

operativi mediante **KPI**, **milestone**, owner, dipendenze, priorità e stima puntuale dei fabbisogni economici, con esplicita distinzione tra componenti di **spesa corrente (OPEX)** e di **investimento (CAPEX)**.

In tale sede sono definiti, e aggiornati annualmente, il perimetro economico delle iniziative, la distinzione tra spese correnti e investimenti, la priorità degli interventi, la tracciabilità rispetto a milestone e risultati attesi e l'allineamento con gli altri strumenti di programmazione e performance. Il **Piano Triennale operativo ad aggiornamento annuale di Transizione Digitale** è inoltre costruito per integrarsi nativamente con i processi di monitoraggio e riesame già sviluppati in Ateneo, così da garantire un raccordo continuo con gli **obiettivi annuali del PIAO** e con gli strumenti del **controllo di gestione**, con particolare riferimento alla piattaforma **SPRiNT**, che costituisce uno dei supporti fondamentali per la pianificazione, il monitoraggio e la rendicontazione dello stato di avanzamento.

Il Piano mantiene quindi la funzione di cornice strategica e di indirizzo, mentre il **Piano Triennale operativo ad aggiornamento annuale di Transizione Digitale** costituisce lo strumento deputato alla pianificazione attuativa ed economico-finanziaria.

# 7 Governance, monitoraggio e aggiornamento del Piano

La governance, già definita nel capitolo dedicato alla **Governance della transizione digitale**, assicura coerenza strategica, priorità condivise e misurazione continuativa. In questa sezione sono richiamati il ciclo di monitoraggio, le modalità di aggiornamento del Piano e il riesame periodico, da svolgere secondo una logica **PDCA** — pianificare, attuare, verificare e correggere — così da consentire eventuali riallineamenti delle priorità, delle iniziative e delle modalità attuative.

## 7.1 Ciclo di monitoraggio

Il Piano adotta un ciclo di **monitoraggio annuale** finalizzato a verificare lo stato di avanzamento dei programmi, rilevare eventuali scostamenti e individuare azioni correttive o di riallineamento secondo la logica **PDCA**. Il monitoraggio si raccorda con gli strumenti di programmazione, performance e controllo già richiamati nei capitoli precedenti e si basa su:

- indicatori e milestone definiti nella programmazione operativa annuale;
- riesame annuale verso la governance, con evidenza di avanzamento, scostamenti, rischi emersi e azioni correttive proposte;
- allineamento con il ciclo annuale di programmazione e performance dell'Ateneo;
- utilizzo dei processi e degli strumenti di controllo di gestione disponibili per documentare avanzamento, risultati e criticità;
- aggiornamento annuale delle priorità e della roadmap sulla base degli esiti del monitoraggio e del riesame.

# 8 Roadmap strategica 2026–2030

La roadmap strategica articola l'orizzonte 2026–2030 in due fasi, mantenendo una logica di aggiornamento continuo. In coerenza con il modello AVA3 e con l'impostazione ANVUR

dell'Assicurazione della Qualità, il Piano adotta un ciclo ricorrente di pianificazione, attuazione, monitoraggio, riesame e miglioramento, orientato sia alla responsabilizzazione verso gli stakeholder sia al miglioramento continuo dei servizi e dei risultati. Il riesame intermedio 2029–2030 rappresenta quindi un passaggio strutturato di autovalutazione: non una semplice verifica amministrativa, ma un momento di analisi degli esiti, degli scostamenti, dei rischi emergenti e dell'adeguatezza dell'impianto di governance digitale rispetto agli obiettivi del Piano.

**2026–2028: Avvio, attuazione e consolidamento dell'impianto operativo**

- Allineamento del Piano al Piano Strategico di Ateneo 2024–2030, al ciclo PIAO, al sistema di performance e agli strumenti di controllo di gestione, mantenendo un orizzonte strategico 2026–2030.
- Consolidamento della governance della transizione digitale, con ruoli, responsabilità, flussi decisionali e modalità di prioritizzazione della domanda chiaramente definiti.
- Messa a regime del Piano Triennale operativo ad aggiornamento annuale di Transizione Digitale 2026–2028, con iniziative, owner, milestone, KPI, coperture economiche e dipendenze.
- Avvio del ciclo annuale di monitoraggio e riesame, con raccolta sistematica di evidenze, dati di avanzamento, feedback degli utenti, criticità e azioni correttive, in coerenza con la logica AVA3 di miglioramento continuo.

**2029–2030: Riesame intermedio, maturità del sistema e riallineamento strategico**

- Svolgimento di un riesame intermedio strutturato del Piano, fondato su evidenze documentali, indicatori, stato di avanzamento delle iniziative, risultati conseguiti, scostamenti rispetto alle milestone e analisi dei rischi emergenti.
- Valutazione dell'efficacia della governance digitale, del modello di portfolio management, del presidio interno delle funzioni critiche e della capacità dell'Ateneo di governare fornitori, integrazioni, sicurezza, qualità del dato e servizi digitali.
- Raccordo del riesame con il Sistema di Assicurazione della Qualità di Ateneo, in coerenza con AVA3, con particolare attenzione alla disponibilità di indicatori, alla documentabilità delle decisioni, al monitoraggio dei risultati e alla capacità di attivare azioni di miglioramento.
- Aggiornamento del portafoglio iniziative e della roadmap fino al 2030 sulla base degli esiti del riesame, distinguendo tra interventi completati, iniziative da consolidare, priorità da ripianificare e nuove esigenze derivanti dall'evoluzione normativa, tecnologica e organizzativa.
- Rendicontazione sintetica alla governance degli esiti del riesame intermedio, delle principali aree di miglioramento e delle decisioni assunte, così da assicurare trasparenza, tracciabilità e continuità con il ciclo PIAO, performance e controllo di gestione.

La tabella seguente traduce la roadmap strategica in un **Gantt di altissimo livello**, utile a visualizzare la distribuzione temporale dei programmi, le principali fasi di avvio, consolidamento, estensione e riesame, nonché le interdipendenze più rilevanti. La rappresentazione ha valore orientativo e sarà dettagliata nel **Piano Triennale operativo ad aggiornamento annuale di Transizione Digitale**, anche in termini di iniziative, owner, milestone, KPI, CAPEX e OPEX.

| Programma | 2026 | 2027 | 2028 | 2029 | 2030 | Nota di lettura |
|---|---|---|---|---|---|---|
| **1 – Insubria Secure++** | Assessment NIS2, asset critici, | Messa a regime presìdi cyber, | Consolidamento continuità operativa e | Riesame controlli, incident | Rafforzamento selettivo e nuovo ciclo di priorità | Programma trasversale e |

| | | | | | | |
|---|---|---|---|---|---|---|
| | baseline sicurezza | identity, endpoint, SOC | supply chain ICT | readiness, adeguamenti | | abilitante per tutti gli altri. |
| **2 – Insubria AI Governance** | Linee guida, processo di valutazione, registro AI | Sperimentazioni controllate e AI literacy | Monitoraggio, riesame e scaling selettivo | Stabilizzazione modello e revisione rischi | Aggiornamento quadro e dismissioni/estensioni | Abilita sperimentazioni AI nei programmi Data, Web, Campus e Processi. |
| **3 – Insubria Digital Process** | Process inventory, priorità, owner, benefici attesi | Reingegnerizzazione processi critici e workflow | Estensione self-service, integrazioni e misurazione | Scaling e miglioramento continuo | Riesame portafoglio processi e nuove priorità | Dipende da Data & Analytics, ICT Academy e presidio cyber. |
| **4 – Insubria Data & Analytics** | Data governance, fonti autorevoli, domini prioritari | Cruscotti prioritari e qualità del dato | Estensione analytics, interoperabilità e report certificati | Consolidamento, data literacy e riesame | Estensione a nuovi domini e riallineamento strategico | È base informativa per performance, PIAO, AI e processi. |
| **5 – Insubria Digital Campus EVO** | Standard, backlog, priorità aule e piattaforme | Evoluzione aule, servizi studenti, piattaforme didattiche | Refresh selettivo, accessibilità e qualità percepita | Riesame modello, feedback e scalabilità | Nuovo ciclo evolutivo e priorità infrastrutturali | Programma ad alto impatto economico e forte visibilità utente. |
| **6 – Insubria Ecosistema Web** | Governance, backlog, standard editoriali | Accessibilità, UX, qualità contenuti e misurazione | Estensione integrazioni, servizi digitali e contenuti | Monitoraggio, ottimizzazione e riesame | Consolidamento e riallineamento ai bisogni utente | Interagisce con Data, AI Governance, ICT Academy e Processi. |
| **7 – Insubria ICT Academy** | Modello, catalogo, target e raccordo competenze | Erogazione percorsi, key user, materiali pratici | Estensione community, change management e impatto | Stabilizzazione e misurazione efficacia | Aggiornamento catalogo e nuovo ciclo formativo | Programma abilitante per l'adozione effettiva degli altri programmi. |
| **8 – Insubria AI e Big Data Platform** | Studio di fattibilità, fabbisogni ricerca, governance | Decisione di investimento e modello di sostenibilità | Realizzazione o procurement, servizi e sicurezza | Scaling selettivo e valutazione impatti | Riesame strategico e continuità del servizio | Programma selettivo, con impatto economico alto e dipendenze da ricerca, Data, AI Governance e Secure++. |

**Legenda Gantt**: blu chiaro = impostazione, governance, analisi o progettazione; rosso chiaro = fase realizzativa o investimento ad alta intensità; arancione chiaro = consolidamento, estensione o messa a regime; verde chiaro = monitoraggio, stabilizzazione, riesame e miglioramento continuo.

# Appendice A – Glossario minimo (acronimi e definizioni)

Per assicurare chiarezza terminologica e coerenza tra documenti strategici e operativi, il Piano include un glossario minimo.

**Acronimi (esteso)**

- **AS-IS**: stato attuale (fotografia del contesto "così com'è")
- **AVA3**: Autovalutazione, Valutazione, Accreditamento (modello ANVUR – versione 3)
- **BIA**: Business Impact Analysis
- **CAPEX**: Capital Expenditure (spesa in conto capitale / investimenti)
- **CEV**: Commissione di Esperti della Valutazione (ANVUR)
- **CSAT**: Customer Satisfaction
- **DR**: Disaster Recovery
- **EDR**: Endpoint Detection & Response
- **IAM**: Identity and Access Management
- **IDM**: Identity Management (gestione del ciclo di vita delle identità digitali: creazione, modifica, disattivazione; ruoli e attributi; provisioning/deprovisioning)
- **LMS**: Learning Management System
- **MFA**: Multi-Factor Authentication
- **MTTA**: Mean Time To Acknowledge (tempo medio di presa in carico/triage iniziale)
- **MTTR**: Mean Time To Resolve/Recover (tempo medio di risoluzione/ripristino)
- **NIS2**: Direttiva (UE) 2022/2555 su misure per un elevato livello comune di cibersicurezza; nel Piano è richiamata come driver regolatorio trasversale per governance, risk management, incident reporting, continuità operativa e supply chain ICT.
- **OPEX**: Operational Expenditure (spesa corrente/di esercizio)
- **PAM**: Privileged Access Management
- **PDND**: Piattaforma Digitale Nazionale Dati
- **PIAO**: Piano Integrato di Attività e Organizzazione
- **RPO**: Recovery Point Objective
- **RTD**: Responsabile per la Transizione Digitale
- **RTO**: Recovery Time Objective
- **SLA**: Service Level Agreement
- **SOC**: Security Operations Center
- **TO-BE**: stato target (contesto desiderato "come sarà")
- **UX**: User Experience

**Prodotti e nomi propri**

- **App IO**: app dei servizi pubblici italiani; citata come possibile canale/integrazione per servizi e notifiche.
- **Anatomage Table**: tavolo per anatomia interattiva/digital dissection, usato per didattica medico-sanitaria.
- **Body Interact**: piattaforma di simulazione di scenari clinici per didattica/assessment.
- **CINECA**: consorzio/fornitore di piattaforme e servizi per università (ecosistema gestionale e progetti, es. Esse3, Sprint, IDM).
- **Cyberguru**: piattaforma per campagne di cyber awareness e formazione (es. phishing simulato).

- **Digital Pathology**: tecnologie e piattaforme per digitalizzazione e analisi di preparati istologici/diagnostica digitale.
- **EDR (soluzioni)**: strumenti di Endpoint Detection & Response per rilevazione e risposta su endpoint.
- **Esse3**: sistema informativo per la gestione delle carriere studenti (suite CINECA) e servizi correlati.
- **GARR**: rete nazionale dell'istruzione e ricerca; connettività e servizi per gli enti aderenti.
- **Intune**: servizio Microsoft per gestione e compliance di endpoint (MDM/MAM), citato per endpoint management.
- **Microsoft 365 (M365)**: suite cloud Microsoft per produttività e collaborazione.
- **Microsoft Teams**: piattaforma di collaborazione e videoconferenza (M365), citata come strumento didattico e organizzativo.
- **Moodle**: piattaforma LMS (Learning Management System) utilizzata per e-learning e monitoraggio apprendimento.
- **NAS**: Network Attached Storage; citato come storage locale in alternativa/integrazione a SharePoint.
- **PagoPA**: sistema nazionale per pagamenti verso la PA; citato tra gli standard/integrazioni.
- **PSN**: Polo Strategico Nazionale; citato per avvio nucleo servizi e percorso cloud/hosting qualificato.
- **SharePoint**: piattaforma Microsoft per condivisione documentale e collaboration (M365), citata in relazione a sostituzione/razionalizzazione di storage locali.
- **SIOPE+**: piattaforma nazionale per gestione telematica di incassi/pagamenti delle PA; citata nel Piano operativo.
- **SPC2/SPC3**: contratti/ambiti di connettività della PA; citati per continuità e transizione.
- **SPID**: Sistema Pubblico di Identità Digitale; citato per integrazioni autenticazione/servizi.
- **CIE**: Carta d'Identità Elettronica; citata per integrazioni di autenticazione.
- **SPRiNT**: applicativo (CINECA) per pianificazione e monitoraggio (es. ciclo performance/obiettivi).
- **Consip**: centrale acquisti della PA; citata per convenzioni/accordi (es. cybersecurity).
- **Oculus/VR**: visori e tecnologie di realtà virtuale per didattica immersiva (ambiti selezionati).

**Termini e concetti (esteso)**

- **API**: interfaccia applicativa che consente a sistemi diversi di scambiare dati e funzionalità in modo standardizzato.
- **Auditability**: possibilità di ricostruire e verificare decisioni/azioni di un sistema tramite log, evidenze e tracciabilità.
- **Change management**: insieme di attività (comunicazione, formazione, supporto, engagement) per accompagnare le persone nell'adozione del cambiamento.
- **Conditional Access**: insieme di regole che consentono o bloccano l'accesso a un servizio in base a condizioni (es. identità/ruolo, rischio, posizione, stato di *device compliance*), a supporto delle politiche di sicurezza.
- **Continuità operativa**: capacità di mantenere o ripristinare in tempi definiti i servizi critici in caso di incidenti o indisponibilità.
- **Data governance**: insieme di ruoli, regole e processi per garantire qualità, responsabilità, sicurezza e uso corretto dei dati.

- **Data lineage**: tracciabilità del percorso del dato (origine, trasformazioni, utilizzi) lungo i sistemi e i processi.
- **Data owner**: responsabile del dato (dominio informativo) dal punto di vista di finalità, correttezza e regole d'uso.
- **Data steward**: ruolo operativo che presidia qualità, definizioni, metadati e corretto utilizzo del dato nel tempo.
- **Device compliance**: stato di conformità di un dispositivo rispetto a requisiti/policy di sicurezza definiti (es. cifratura attiva, sistema aggiornato, antivirus/EDR attivo, configurazioni minime). È spesso usata come condizione nelle regole di **Conditional Access**.
- **Digital first**: principio per cui servizi e processi sono progettati prioritariamente in digitale, con semplificazione e orientamento all'utente.
- **Drift (AI)**: variazione nel tempo delle prestazioni o del comportamento di un modello/soluzione AI rispetto alle condizioni iniziali, che richiede monitoraggio e tuning.
- **Fonti autorevoli**: fonti dati considerate ufficiali e "di riferimento" per uno specifico dominio informativo, con regole di qualità e ownership.
- **Interoperabilità**: capacità dei sistemi di scambiare dati e cooperare tramite standard e interfacce coerenti.
- **Key user**: utente di riferimento in una struttura che supporta raccolta requisiti, test, validazioni e adozione (anche tramite knowledge base e feedback).
- **Playbook**: procedura operativa standard (spesso automatizzabile) per gestire un evento/incidente o un'attività ricorrente (es. risposta a incidenti cyber).
- **Remediation**: insieme di azioni correttive per riportare un sistema/dispositivo in conformità o mitigare un rischio.
- **Security by design**: integrazione dei requisiti di sicurezza fin dalla progettazione e lungo tutto il ciclo di vita.
- **Self-service**: fruizione autonoma di un servizio digitale da parte dell'utente, con riduzione di passaggi manuali e richieste "di sportello".
- **Service owner**: responsabile del servizio in esercizio (SLA, continuità, roadmap evolutiva), inclusa gestione rilasci e dipendenze.
- **Triage**: fase di classificazione e prioritizzazione iniziale di richieste/ticket o alert di sicurezza.
- **Workflow**: sequenza strutturata di attività e regole che descrive un processo (dalla richiesta all'esito), spesso automatizzabile tramite strumenti digitali.
- **Zero Trust**: modello di sicurezza basato sul principio "never trust, always verify", con controlli continui su identità, dispositivi, reti e contesto.