AGID | Agenzia per l'Italia Digitale

LINEE GUIDA PER INTELLIGENZA ARTIFICIALE NELLA PA

Come implementare sistemi di Intelligenza artificiale: dallo sviluppo al procurement

Giovanni Melardi – Alessandra Pieroni
Segreteria tecnica del Direttore Generale

CONTESTO

DEFINIZIONE

Per sistema di Intelligenza Artificiale (IA) si intende un sistema automatico che, per obiettivi espliciti o impliciti, **deduce dagli input ricevuti come generare output** come previsioni, contenuti, raccomandazioni o **decisioni che possono influenzare ambienti fisici o virtuali**. I sistemi di IA **variano nei loro livelli di autonomia e adattabilità dopo l'implementazione**
(Fonte: OCSE)

Potenzialità dell'IA nella Pubblica Amministrazione

- → **automatizzare attività** di ricerca e analisi delle informazioni **semplici e ripetitive**, liberando tempo di lavoro per attività a maggior valore
- → aumentare le capacità predittive, migliorando il **processo decisionale basato sui dati**
- → supportare la **personalizzazione dei servizi** incentrata sull'utente, aumentando l'efficacia dell'erogazione dei servizi pubblici anche attraverso **meccanismi di proattività**.

CONTESTO

Approccio Europeo – AI Act

Regolamento EU composto da **113 articoli -** stabilisce norme per lo sviluppo, l'immissione sul mercato e l'utilizzo dell'intelligenza artificiale in modo sicuro, responsabile ed etico

Obiettivo: Creare un quadro normativo armonizzato per l'intelligenza artificiale nell'Unione Europea.

Principi Fondamentali:

- Sviluppo e utilizzo sicuro ed etico dell'IA
- Rispetto dei diritti fondamentali e dei valori europei

Classificazione Basata sul Rischio: I sistemi di IA sono classificati in base al loro livello di rischio per la sicurezza e i diritti delle persone

CONTESTO

In vigore dal 10 ottobre 2025, la L. 132/2025 (cd. Legge italiana sull'intelligenza artificiale) è una legge di principi e delega che non introduce obblighi ulteriori rispetto all'AI Act, ma specifica la disciplina per la PA

Principi generali (Art. 2)

- **Autonomia decisionale** dell'uomo
- **Prevenzione** del danno
- **Trasparenza** e **spiegabilità**
- Sorveglianza e **intervento umano**

IA nella PA (Art. 14)

- IA ha carattere strumentale e di **supporto**
- Il **funzionario** resta unico **responsabile**
- Obbligo di **misure tecniche, organizzative e formative**
- Risorse a **legislazione vigente**

CONTESTO

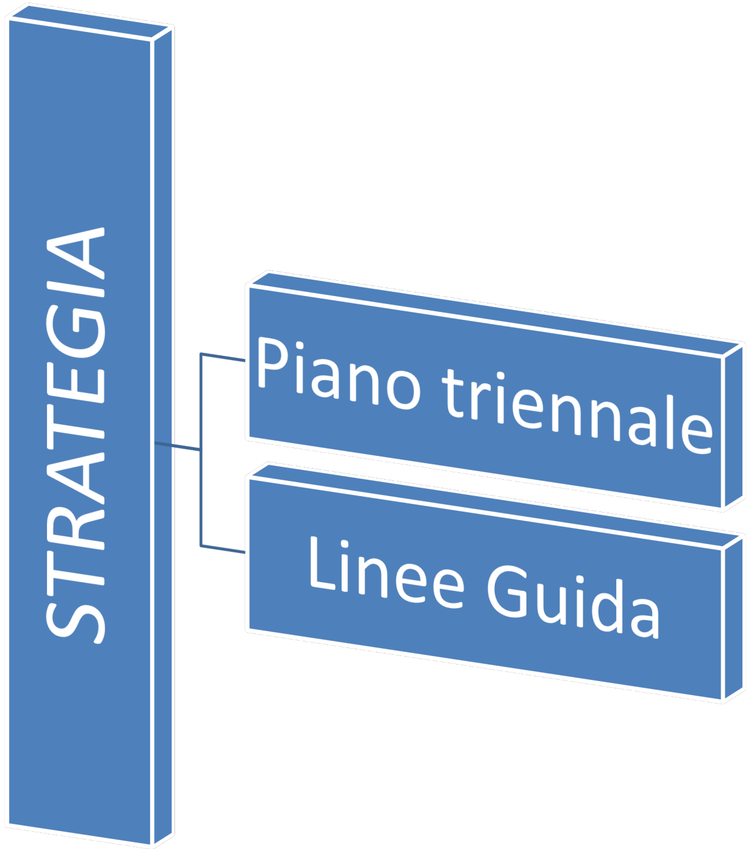
REGOLAMENTO AI ACT

Promuovere lo sviluppo affidabile dell'IA

Proteggere i diritti fondamentali delle persone

Garantire la sicurezza dei consumatori

Aumentare la fiducia pubblica nell'IA

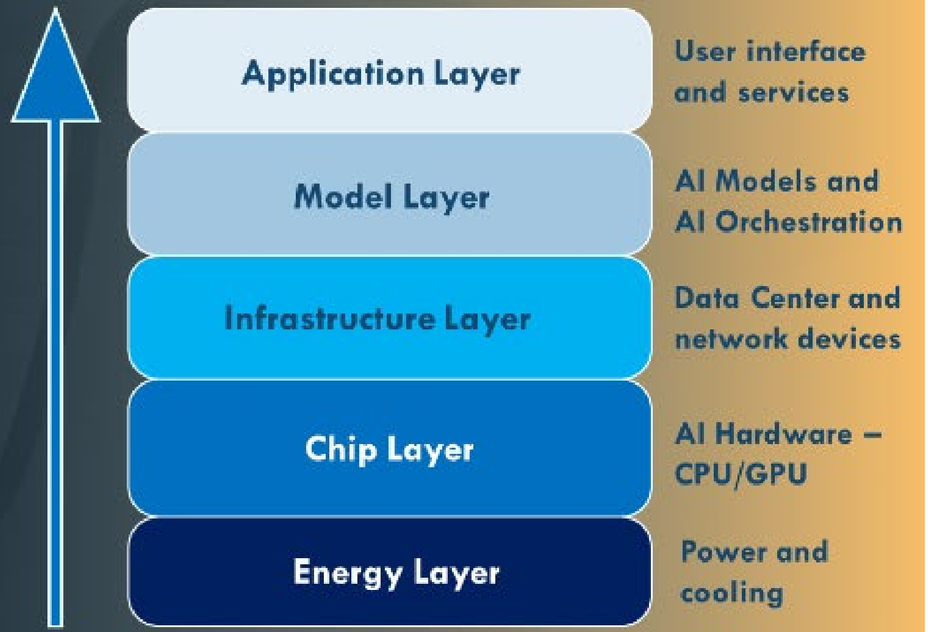


Full-Stack AI

--> End-to-end governance of the AI stack is essential to ensure scalable, secure, and trustworthy AI systems

--> Public Administrations are required to govern all layers of the AI stack— from infrastructure to models and monitoring— across the full lifecycle

The AI Stack represents an organized layering of the technical, hardware, and software components required to design, train, deploy, and operate artificial intelligence systems



Agentic AI - Levels of Autonomy

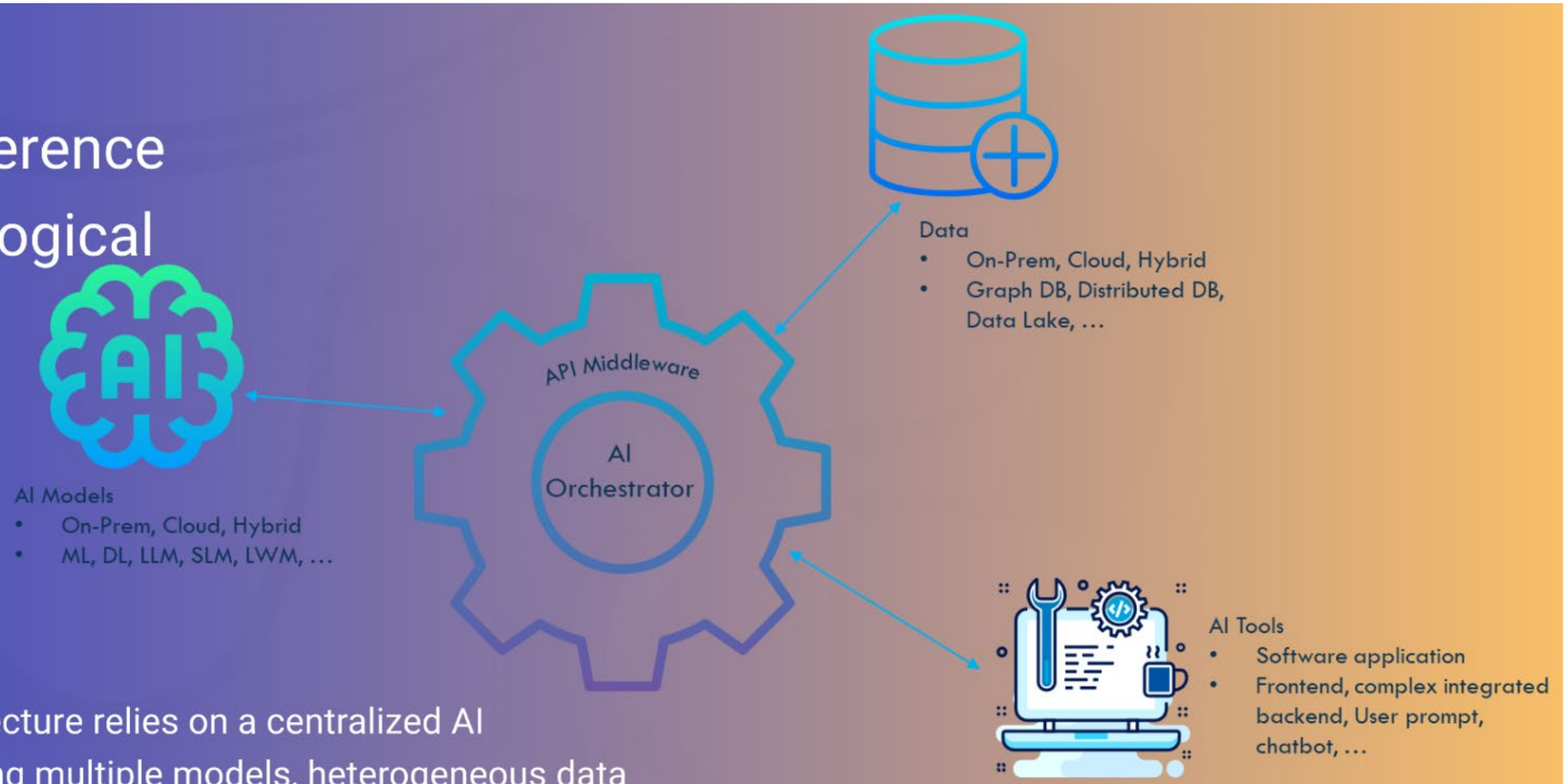
--> Agentic systems follow an observe–decide–act loop, analogous to the control cycle of SAE-based autonomous driving

--> Higher levels of autonomy require stronger governance mechanisms to ensure traceability, compliance, and continuous human oversight within established safety limits

Levels of AI Agent Autonomy

Level	Agent Capability	Car Analogy	Typical Use Cases
L0 – Manual	Fully human-driven	Manual driving	Manual workflows
L1 – Rule-based	Fixed-rule automation	Cruise control	RPA, rule engines
L2 – Intelligent	ML-based automation	ADAS	Document processing
L3 – Agentic	Reasoning & tool-using agents	Highway autopilot	Copilots, RAG agents
L4 – Semi-autonomous	Autonomous in bounded domains	Conditional self-driving	Robotics, driverless ops
L5 – Fully autonomous	Cross-domain autonomy	Full autonomy	Research only

Agentic AI Reference Architecture - logical view



--> The reference architecture relies on a centralized AI Orchestrator coordinating multiple models, heterogeneous data sources, and specialized tools

-->Intelligent orchestration, enabled through an API Middleware, ensures abstraction, interoperability, and uniform access across the AI ecosystem

LINEE GUIDA SVILUPPO

PERSONAS: PA Classification

Introduction of Public Operators - level of control and autonomy using or developing AI systems end-to-end

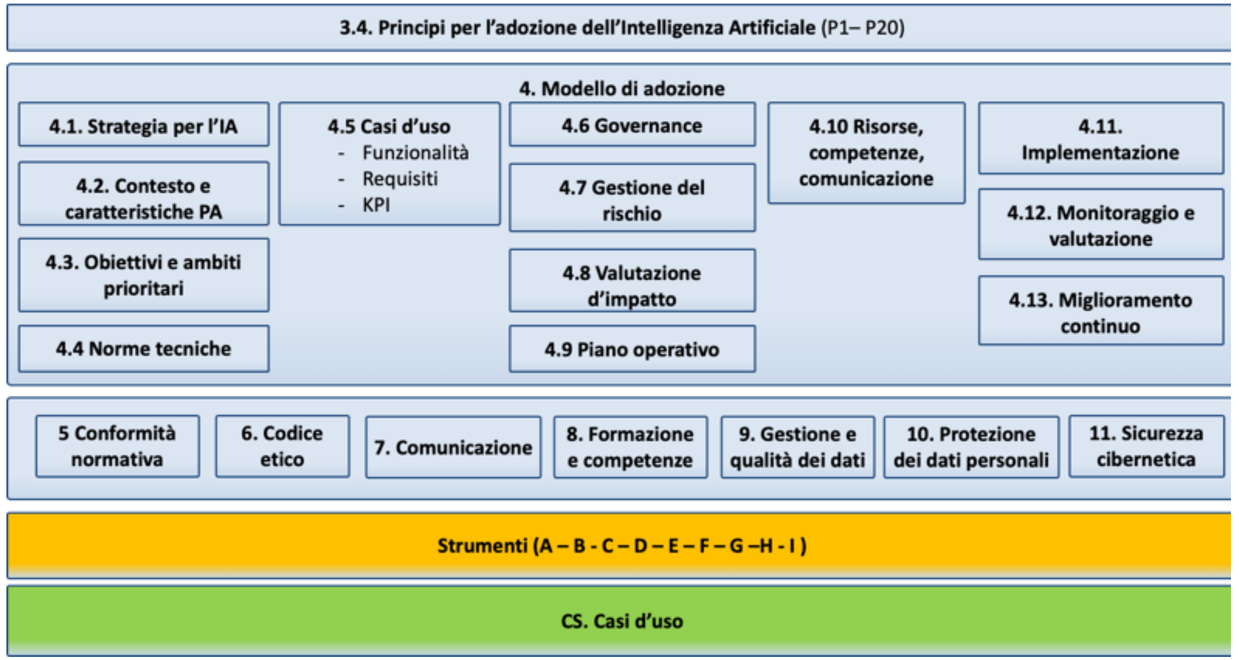
Basic Operator
No advanced specialist skills or specific human, financial, or technical resources are required.

Advanced Operator
Dedicated advanced specialist skills and human, financial, and technical resources are required

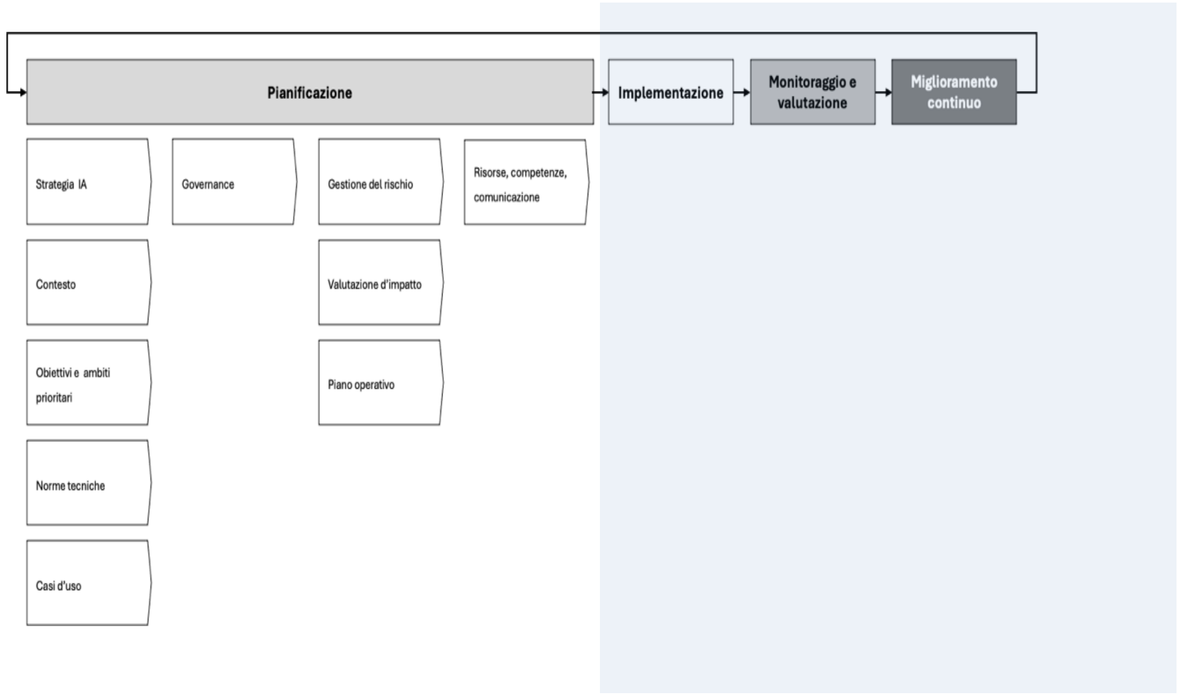
Expert Operator
Extensive advanced specialist expertise and substantial dedicated human, financial, and technical resources are required.

Controller Operator
Deep advanced specialist expertise and substantial dedicated human, financial, and technical resources are required.

LINEE GUIDA ADOZIONE



LINEE GUIDA ADOZIONE



Implementazione

- Le PA **DEVONO** attuare:
  - **piano operativo** (par. 4.9)
  - **valutazione e trattamento del rischio** (par. 4.7)
  - **valutazione d'impatto** (cfr. par. 4.8).

Monitoraggio e valutazione

- Le PA **DEVONO** monitorare regolarmente i **KPI** per:
  - **valutare le prestazioni tecniche** dei sistemi di IA.
  - **misurare l'efficacia** delle misure organizzative e tecniche adottate
  - **determinare il valore aggiunto** generato dal sistema di IA

Miglioramento continuo

- Le PA **DEVONO** garantire nel tempo: **idoneità, adeguatezza**, **efficacia** dei sistemi di IA delle misure tecniche e

organizzative adottate per la gestione dell'IA.

LG Procurement – Tre pilastri per l'approvvigionamento

LCOAI	Cooperazione	Capitolato
• Metriche economiche per stimare il costo lungo l'intero ciclo di vita (CAPEX + OPEX).	• Aggregazione della domanda per ridurre la frammentazione e generare economie di scala	• Progettazione della gara con definizione dei requisiti tecnici organizzativi e contrattuali coerenti con la natura dei sistemi di IA

LCOAI – LEVELIZED COST OF AI

Oltre il prezzo di acquisto

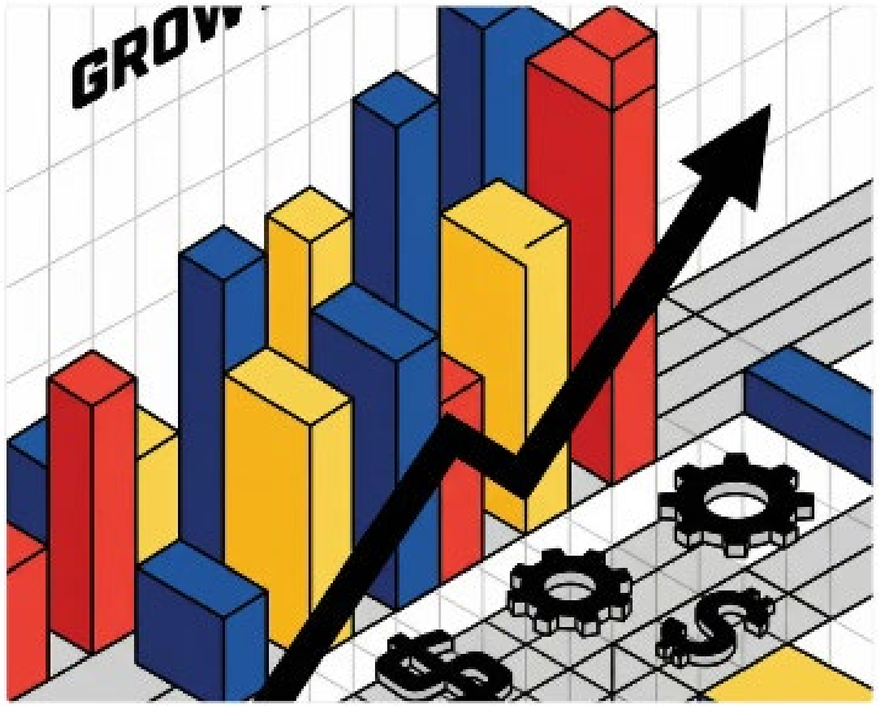
La metrica LCOAI consente di analizzare la sostenibilità finanziaria complessiva:

CAPEX: Investimenti iniziali per modelli e infrastrutture.

OPEX: Costi ricorrenti di calcolo, energia e gestione.

Valutazione accurata di soluzioni Cloud vs On-premises.

Pianificazione realistica delle basi d'asta.



ANALISI INTEGRATA DEI COSTI

Componente	Descrizione Operativa
CAPEX	Setup infrastrutturale, licenze, integrazione dati iniziale.
OPEX	Risorse cloud, manutenzione modelli, supporto specialistico.
IBRIDI	Storage dati a lungo termine, aggiornamento periodico dataset.

COOPERAZIONE E AGGREGAZIONE

Sinergie Istituzionali

- ✓ Rafforzare la capacità negoziale della PA tramite forme di aggregazione
- ✓ Riduzione della frammentazione degli investimenti.
  - ✓ Sviluppo di un ecosistema pubblico interoperabile.
  - ✓ Riutilizzo di soluzioni tecnologiche tra amministrazioni.
  - ✓ Percorsi di crescita professionale nelle Personas.

COOPERAZIONE E AGGREGAZIONE

La capacità di scambiare informazioni e servizi in modo standardizzato costituisce un presupposto fondamentale per realizzare amministrazioni più efficienti, coordinate e orientate all'utente

Evitare duplicazioni funzionali

Stesse soluzioni adottabili da più enti con adattamenti limitati

Condividere costi di sviluppo

Cooperazione riduce rischi e beneficia di competenze distribuite

Rafforzare il potere negoziale

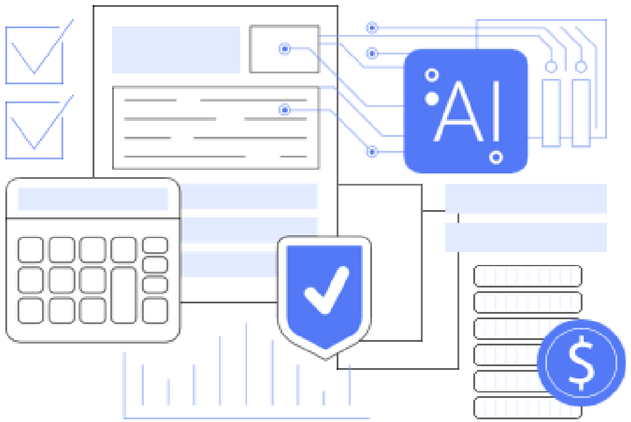
Domanda aggregata riequilibra il rapporto con i fornitori

Accelerare l'adozione

Standard comuni e governance condivisa favoriscono la circolazione dell'innovazione

IL CAPITOLATO DI GARA

Il capitolato deve accompagnare la soluzione lungo l'intero ciclo di vita contrattuale in quanto consente di adottare un approccio funzionale e orientato ai risultati

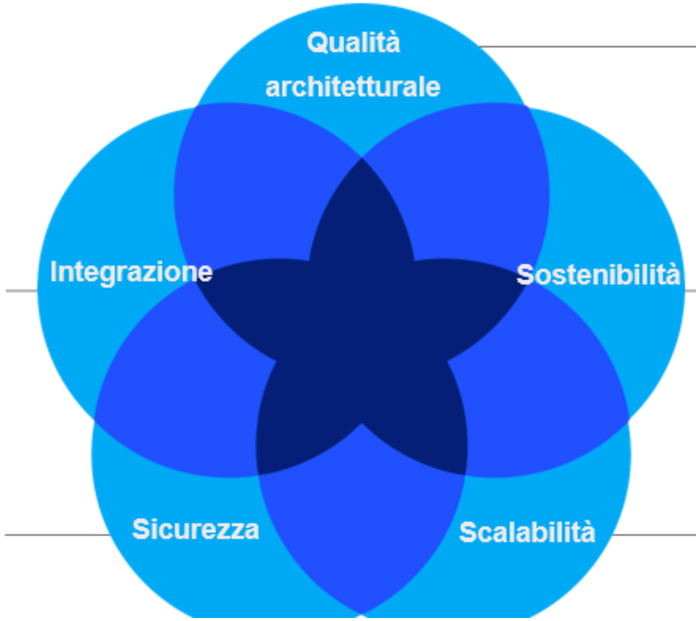


Sezione	Contenuto
Oggetto e obiettivi	Perimetro, benefici misurabili, KPI
Architettura	Coerenza con modello orchestratore-modelli-dati-tool
Requisiti funzionali e tecnici	Cosa deve fare; vincoli, neutralità hardware
Gestione dati	Accesso, utilizzo, conservazione, portabilità
SLA e sicurezza	Livelli di servizio, AI Act, GDPR, cybersicurezza

Il capitolato è strumento di governo, non mero elenco di specifiche

IL CRITERIO DI AGGIUDICAZIONE

L'OEPV è l'offerta economica più vantaggiosa – ovvero il prezzo iniziale non rappresenta l'elemento prevalente per prendere la decisione



Coerenza con il modello di riferimento AgID

Facilità di integrazione con l'ecosistema digitale dell'ente

Sostenibilità economica del ciclo di vita con l'uso del Levelised Cost of Ai come metrica normalizzata

Robustezza delle misure di sicurezza, grado di spiegabilità e trasparenza

Capacità evolutiva per cogliere l'adattamento a nuove esigenze senza riscrittura

STRUMENTI DI GARA FLESSIBILI

Le Linee Guida mettono a disposizione della PA tre strumenti di procurement innovativo che consentono di coinvolgere il mercato in modo più efficace, riducendo i rischi e accelerando l'introduzione di soluzioni innovative

1 Pre-commercial procurement

- Per soluzioni **non ancora sul mercato**
- Acquisto di **servizi R&D**: design, prototyping, testing

2 Public procurement of Innovation

- Per soluzioni innovative **già vicine al mercato**
- Acquisto di **prodotti/servizi innovativi**

3 Partneriato per l'innovazione

- Unica procedura che **combina R&D e acquisto** della soluzione finale
- Si struttura in **fasi iterative**

INDIPENDENZA TECNOLOGICA E LOCK-IN

Misure di Prevenzione:

- Promozione di standard tecnici documentati e aperti.
- Separazione tra componenti core (dati vs orchestratore).
- Clausole contrattuali per garantire la portabilità evolutiva.
- Piani di fallback e rollback per la continuità del servizio.

"Assicurare la capacità di evoluzione e sostituzione dei sistemi nel tempo."

Grazie per l’attenzione

direzione.generale@agid.gov.it

AGID | Agenzia per l’Italia Digitale