AGID | Agenzia per l'Italia Digitale

Linee guida per l'IA nella pubblica amministrazione

Schema di Capitolato Tecnico

Strumento B

Versione 1.0 del 11.03.2026 – Pubblicazione in consultazione pubblica

Indice

Premessa

Considerata la velocità dell'innovazione, le Linee guida per l'IA nella pubblica amministrazione intendono garantire un adattamento costante ai cambiamenti imposti dall'incessante rivoluzione digitale. Di qui la scelta di corredare le Linee guida di "Strumenti", ovvero documenti a supporto dell'attività operativa di applicazione delle Linee guida.

L'elenco aggiornato degli strumenti delle Linee guida IA è disponibile al link: <<da definire in fase di pubblicazione>>.

Gli Strumenti potranno essere periodicamente aggiornati per tener conto dell'evoluzione normativa e tecnologica e delle buone pratiche emergenti.

I – Schema di Capitolato Tecnico

Lo schema di capitolato ha l'obiettivo di fornire alle amministrazioni pubbliche una struttura sintetica e operativa per la predisposizione di capitolati tecnici o della documentazione di affidamento relativa a sistemi e servizi basati su Intelligenza Artificiale.

Lo schema è concepito come uno strumento di supporto alla redazione delle procedure di gara, utile per strutturare in modo chiaro e verificabile i requisiti funzionali, tecnici e organizzativi richiesti nei processi di acquisizione di soluzioni di IA.

Particolare attenzione è dedicata al principio di proporzionalità dei requisiti, sia funzionali sia di gestione, in relazione al caso d'uso, al livello di rischio del sistema e al contesto amministrativo di utilizzo. Tale approccio è coerente con l'impostazione basata sul rischio introdotta dal Regolamento (UE) 2024/1689 (AI Act). Lo schema tiene inoltre conto degli standard internazionali disponibili, nonché delle attività di standardizzazione tecnica attualmente in corso a livello europeo presso CEN e CENELEC, che contribuiranno a supportare l'attuazione dei requisiti previsti dal Regolamento.

Lo schema ripercorre la struttura tipica di un capitolato tecnico e individua, oltre agli articoli principali, una serie di allegati tecnici utili nelle diverse fasi della procedura: preparazione della gara, presentazione delle offerte, valutazione delle soluzioni e verifica delle prestazioni del sistema durante l'esecuzione del contratto. Gli allegati possono essere predisposti dall'Amministrazione, compilati dagli operatori economici nell'ambito dell'offerta tecnica, oppure utilizzati congiuntamente dalle parti nelle fasi di monitoraggio e collaudo.

Il presente schema ha carattere di riferimento adattabile e può essere utilizzato dalle amministrazioni per strutturare i propri capitolati in funzione delle specifiche esigenze organizzative e dei casi d'uso considerati.

Al fine di facilitarne l'applicazione pratica, ciascuno degli articoli e degli allegati potrà essere oggetto di ulteriori approfondimenti tematici, che saranno progressivamente pubblicati da AgID sul proprio sito istituzionale, con l'obiettivo di fornire esempi applicativi e indicazioni operative per specifici casi d'uso.

PARTE I – DISPOSIZIONI GENERALI

Articolo 1 - Oggetto dell'appalto

Obiettivo

L'articolo ha l'obiettivo di definire l'oggetto dell'appalto relativo alla fornitura e implementazione di sistemi di Intelligenza Artificiale e dei servizi connessi destinati a supportare le funzioni istituzionali dell'Amministrazione.

Razionale

L'adozione di soluzioni di IA nella PA richiede un approccio operativo che includa non solo la componente tecnologica, ma anche attività di integrazione, supporto, governance e sviluppo delle competenze, in modo da garantire un utilizzo efficace e conforme dei sistemi.

Aspetti chiave

Le amministrazioni devono in particolare:

- definire il caso d'uso o l'ambito applicativo del sistema di IA oggetto dell'affidamento;
- includere nel perimetro dell'appalto servizi di sviluppo, integrazione, supporto e formazione;
- prevedere soluzioni per la governance dell'IA e la gestione della conformità normativa;
- individuare codici del Vocabolario comune per gli appalti pubblici, ovvero CPV (Common Procurement Vocabulary) coerenti con la natura tecnologica e consulenziale dell'affidamento.

Implicazioni operative per la PA

L'Amministrazione deve strutturare la procedura di gara considerando l'intero ciclo di vita delle soluzioni di IA e identificando i codici CPV più appropriati per qualificare correttamente l'oggetto dell'appalto.

Articolo 2 - Ambito di valutazione dell'offerta

Obiettivo

L'articolo ha l'obiettivo di definire i principali criteri utilizzati dall'Amministrazione per la valutazione tecnica delle offerte relative a soluzioni e servizi di Intelligenza Artificiale.

Razionale

La selezione di soluzioni di IA richiede una valutazione che consideri non solo gli aspetti tecnologici, ma anche la maturità del fornitore, la qualità dei modelli di governance e la capacità di gestire rischi e conformità normativa lungo l'intero ciclo di vita del sistema.

Aspetti chiave

Le amministrazioni devono in particolare:

- valutare la capacità tecnica e organizzativa del fornitore;
- analizzare i modelli di governance e organizzativi proposti;
- verificare l'approccio alla gestione del rischio e alla conformità normativa;
- considerare la sostenibilità tecnica, economica e gestionale delle soluzioni.

Implicazioni operative

L'Amministrazione deve integrare tali elementi nei criteri di valutazione dell'offerta tecnica, assicurando una selezione dei fornitori basata sulla qualità complessiva delle soluzioni e sulla loro sostenibilità nel tempo.

Articolo 3 - Normativa di riferimento e obblighi di conformità

Obiettivo

Il presente articolo individua gli obblighi di conformità normativa che il Fornitore deve garantire nell'erogazione dei servizi e nell'implementazione delle soluzioni di Intelligenza Artificiale oggetto dell'appalto.

Razionale

I sistemi di IA utilizzati nella Pubblica Amministrazione devono essere sviluppati, integrati e gestiti nel rispetto del quadro normativo europeo e nazionale applicabile, al fine di garantire legalità, sicurezza, protezione dei dati e corretta gestione dei rischi tecnologici.

Aspetti chiave

Le amministrazioni devono in particolare:

- richiedere la conformità delle soluzioni all'AI Act (Reg. UE 2024/1689) e al GDPR (Reg. UE 2016/679);
- assicurare il rispetto del Codice dei contratti pubblici (D.Lgs. 36/2023) e della normativa nazionale sull'IA in particolare la Legge 132/2025;
- prevedere il rispetto delle norme in materia di digitalizzazione della PA, sicurezza informatica e protezione dei dati;
- richiamare l'applicazione di standard tecnici e norme tecniche pertinenti;
- prevedere l'obbligo di adeguamento del servizio in caso di evoluzione normativa;
- considerare, ove applicabile, gli strumenti di attuazione previsti dal Regolamento (UE) 2024/1689, inclusi il Codice di buone pratiche per i modelli di IA di uso generale (GPAI) previsti dall'articolo 56 dell'AI Act, fino all'adozione degli standard armonizzati.

Implicazioni operative

L'Amministrazione deve esplicitare nel capitolato i principali riferimenti normativi e prevedere clausole che obblighino il fornitore ad assicurare la conformità delle soluzioni e a adeguare le prestazioni in caso di aggiornamenti del quadro normativo.

Articolo 4 – Definizioni

Obiettivo

Il presente articolo stabilisce le definizioni applicabili ai fini dell'interpretazione e dell'attuazione del Capitolato, assicurando coerenza con il quadro normativo e tecnico di riferimento in materia di Intelligenza Artificiale.

Razionale

L'utilizzo di una terminologia uniforme è essenziale per garantire chiarezza interpretativa, coerenza giuridica e allineamento con la normativa europea, nazionale e con gli standard tecnici applicabili ai sistemi di IA.

Aspetti chiave

Le amministrazioni devono in particolare:

- richiamare prioritariamente le definizioni contenute nell'AI Act (art. 3, Reg. UE 2024/1689) e nel GDPR (art. 4, Reg. UE 2016/679);
- applicare le definizioni previste dalla normativa nazionale in materia di IA, in particolare la Legge 132/2025, ove applicabili;
- considerare le definizioni contenute nelle norme tecniche europee armonizzate e negli standard internazionali di settore;
- fare riferimento, per gli aspetti non disciplinati dalle fonti normative, allo Strumento "Termini e definizioni" delle Linee Guida AgID sull'Intelligenza Artificiale.

Implicazioni operative

L'Amministrazione deve indicare nel capitolato le fonti definitorie applicabili e stabilire un criterio di priorità interpretativa, prevedendo la prevalenza delle definizioni contenute nella normativa europea, quindi nella normativa nazionale e, in via residuale, nell'allegato termini e definizioni delle Linee Guida AgID.

PARTE II – REQUISITI TECNICI DEL SISTEMA

Articolo 5 – Classificazione del sistema e livello di rischio

Obiettivo

L'articolo definisce gli obblighi del Fornitore relativi alla classificazione del sistema di Intelligenza Artificiale ai sensi del Regolamento (UE) 2024/1689 (AI Act) e alla valutazione preliminare dei rischi connessi al suo utilizzo. L'articolo stabilisce inoltre le diverse classi di sistemi e servizi che possono rientrare nell'ambito dell'appalto.

Razionale

La corretta classificazione del sistema di IA rappresenta un passaggio fondamentale per determinare i requisiti normativi applicabili, il livello di controllo richiesto e le misure di gestione del rischio da adottare. L'articolo introduce quindi una struttura operativa che consente all'Amministrazione di distinguere tra diverse tipologie di sistemi e servizi di IA, applicando a ciascuna classe obblighi proporzionati in linea con l'AI Act.

Aspetti chiave

Le amministrazioni devono in particolare richiedere che il Fornitore:

- dichiari e motivi la classificazione del sistema ai sensi dell'AI Act (rischio minimo, limitato o alto rischio);
- presenti una valutazione preliminare dei rischi, comprensiva di rischi per diritti fondamentali, sicurezza, aspetti operativi e rischio residuo;
- dimostri la conformità ai requisiti degli articoli 8–15 dell'AI Act nel caso di sistemi classificati come ad alto rischio;
- documenti la corretta classificazione del sistema e garantisca la possibilità di riesame qualora cambino il contesto o le modalità di utilizzo;
- fornisca supporto all'Amministrazione negli obblighi di *deployer* previsti dalle normativa vigente, inclusa la predisposizione della documentazione necessaria per FRIA o DPIA ove applicabili.

Si suggerisce che l'articolo introduca **classi operative di fornitura** utili per strutturare l'affidamento, come ad esempio:

Classe 1 – Sistemi soggetti a obblighi di trasparenza (art. 50 AI Act), come chatbot o sistemi generativi.

Classe 2 – Sistemi non ad alto rischio, utilizzati per automazione o supporto interno a basso impatto regolatorio.

Classe 3 – Sistemi ad alto rischio, soggetti ai requisiti stringenti degli articoli 8–15 dell'AI Act.

Classe 4 – Servizi di consulenza, governance e supporto alla conformità, inclusi audit, monitoraggio e supporto a FRIA/DPIA.

Classe 5 – Servizi di formazione e sviluppo delle competenze, finalizzati anche agli obblighi di AI literacy previsti dall'articolo 4 dell'AI Act.

Classe 6 – Modelli di IA di uso generale (GPAI) e *foundation models*, con obblighi specifici di documentazione, trasparenza e gestione dei rischi sistemici.

In ogni caso, i sistemi oggetto dell'affidamento NON DEVONO rientrare tra le pratiche di Intelligenza Artificiale vietate ai sensi dell'articolo 5 del Regolamento (UE) 2024/1689 (AI Act).

Il Fornitore deve dichiarare che la soluzione proposta non ricade nell'ambito degli usi vietati previsti dal Regolamento. Qualora emergano elementi di non conformità, il Fornitore deve informare tempestivamente l'Amministrazione e adottare le necessarie misure correttive.

Implicazioni operative

In fase di redazione del capitolato, l'Amministrazione deve richiedere al fornitore la classificazione del sistema e la relativa motivazione, definire chiaramente il livello di rischio previsto e indicare le classi applicabili all'affidamento. Il capitolato deve inoltre prevedere obblighi di documentazione, gestione del rischio e supporto alla conformità normativa, proporzionati alla classe del sistema o del servizio oggetto della procedura.

Articolo 6 – Requisiti funzionali

Obiettivo

L'articolo definisce i requisiti funzionali che il sistema di Intelligenza Artificiale deve soddisfare e le modalità con cui tali requisiti devono essere descritti, misurati e verificati ai fini della valutazione dell'offerta e del collaudo.

Razionale

Nei sistemi di IA non è sufficiente descrivere in modo generico le funzionalità richieste: occorre tradurle in requisiti chiari, misurabili e verificabili, in modo da rendere confrontabili le offerte, difendibile la procedura di gara e oggettiva la verifica in fase di collaudo.

A tal fine, la descrizione delle funzionalità può essere strutturata secondo i principi dell'ingegneria dei requisiti definiti dalla norma ISO/IEC/IEEE 29148:2018, che stabilisce criteri di qualità dei requisiti quali chiarezza, verificabilità, tracciabilità e neutralità tecnologica. In generale, è auspicabile che la definizione dei requisiti funzionali nei capitolati per sistemi di IA si ispiri a standard tecnici internazionali riconosciuti, al fine di favorire requisiti chiari, comparabili e verificabili.

Aspetti chiave

Le amministrazioni devono in particolare:

- descrivere le funzionalità richieste nell'Allegato Tecnico A (vedi sezione allegati) secondo una struttura chiara, verificabile e orientata alla misurabilità;
- definire per ciascuna funzionalità almeno: finalità istituzionale, descrizione operativa, input, output, metriche di performance, livello di autonomia e impatto sul processo amministrativo;
- formulare requisiti neutri rispetto alla tecnologia, evitando specifiche ingiustificatamente restrittive e favorendo la comparabilità delle offerte;

- prevedere, per ciascuna funzionalità, criteri di accettazione, modalità di test e soglie minime di conformità;
- richiedere livelli minimi di accuratezza misurabili, tracciabilità delle decisioni automatizzate o degli output generati ed esportazione dei risultati in formato interoperabile e aperto, ove tecnicamente possibile;
- includere, ove pertinente, elementi specifici dei sistemi di IA quali rischi associati alla funzionalità, misure di mitigazione, *logging*, *audit trail*, versionamento, supervisione umana e requisiti di trasparenza;
- distinguere le funzionalità in core, abilitanti ed evolutive, così da graduare priorità, KPI, collaudo e penali in funzione della loro rilevanza;
- richiedere, nel caso di utilizzo di modelli di IA di uso generale (GPAI), informazioni aggiuntive su modalità di integrazione, limitazioni note del modello e gestione del degrado delle prestazioni nel tempo.

Implicazioni operative

In fase di redazione del capitolato, l'Amministrazione deve trasformare le esigenze funzionali in schede descrittive standardizzate (vedi Allegato A allo schema di capitolato), utilizzabili sia per la valutazione comparativa delle offerte sia per il collaudo del sistema. L'articolo 6 consente di collegare in modo diretto requisiti funzionali, test di verifica, indicatori di performance e penali contrattuali, rendendo le prestazioni del sistema di IA misurabili e verificabili.

Articolo 7 – Requisiti di qualità, processi e governance dei dati

Obiettivo

L'articolo definisce i requisiti operativi che il Fornitore deve rispettare per garantire una gestione responsabile, sicura e conforme dei dati utilizzati dal sistema di Intelligenza Artificiale lungo l'intero ciclo di vita.

Razionale

La qualità dei dati rappresenta uno dei fattori più critici per l'affidabilità dei sistemi di IA. Dataset incompleti, distorti o non adeguatamente governati possono generare errori sistematici, *bias* e rischi per i diritti delle persone. Per questo il capitolato richiede che la gestione dei dati sia strutturata come un processo continuo e documentato, integrato nella data governance complessiva dell'Amministrazione e coerente con gli obblighi previsti dal GDPR e dall'AI Act.

Aspetti chiave

Le amministrazioni devono in particolare richiedere che il Fornitore:

- gestisca i dati secondo un processo strutturato di data lifecycle (raccolta, preparazione, utilizzo, monitoraggio, aggiornamento e dismissione), garantendo sicurezza, qualità e tracciabilità;
- documenti fonti, natura e caratteristiche dei dataset, incluse le modalità di raccolta, selezione e trasformazione dei dati utilizzati per addestramento, test e aggiornamento dei modelli;

- dimostri qualità, completezza e rappresentatività dei dati, con controlli di qualità documentati e, per sistemi ad alto rischio, evidenze verificabili;
- identifichi e mitighi *bias* e distorsioni nei dati, prevedendo verifiche periodiche e meccanismi di monitoraggio delle prestazioni nel tempo;
- integri la gestione dei dati con la data governance complessiva dell'Amministrazione, evitando processi paralleli o non coordinati;
- consenta audit dei dataset e dei processi di gestione dei dati, anche tramite verifiche documentali e tecniche;
- garantisca che i dati dell'Amministrazione non siano riutilizzati per finalità diverse o per l'addestramento di modelli generali senza autorizzazione;
- adotti misure di sicurezza e protezione dei dati (controllo accessi, crittografia, segregazione, *logging*) lungo tutte le fasi del trattamento;
- indichi chiaramente localizzazione e giurisdizione dei dati (*data at rest*, *in transit*, *in use*) e le eventuali condizioni di trasferimento extra-UE;
- documenti eventuali dipendenze da infrastrutture cloud o *hyperscaler* e la disponibilità regionale delle funzionalità;
- forniscano informazioni necessarie per la DPIA e le valutazioni di impatto sui diritti fondamentali, ove richiesto;
- descriva le misure adottate per la sicurezza dei modelli di IA, inclusa la protezione da accessi non autorizzati, attacchi *adversarial* e vulnerabilità.

Implicazioni operative

In fase di redazione del capitolato, l'Amministrazione deve richiedere al fornitore una documentazione chiara sui processi di gestione dei dati, sulle fonti utilizzate e sulle misure di sicurezza adottate. Devono essere previste clausole che vietino il riutilizzo non autorizzato dei dati dell'Amministrazione, consentano audit tecnici e garantiscano la localizzazione dei dati conforme alle esigenze dell'ente. L'articolo permette inoltre di verificare in modo concreto la qualità dei dataset, la gestione dei *bias* e la sicurezza delle infrastrutture dati, riducendo rischi operativi e di non conformità normativa lungo tutto il ciclo di vita del sistema di IA.

Articolo 8 – Portabilità dei dati, prevenzione del lock-in e predisposizione all'uscita

Obiettivo

L'articolo definisce le condizioni pratiche che il Fornitore deve garantire per consentire all'Amministrazione di recuperare dati, modelli e artefatti della soluzione di IA e di migrare il servizio senza interruzioni o dipendenze eccessive dal fornitore.

Razionale

Nei contratti relativi a sistemi di IA, il rischio di dipendenza tecnologica dal fornitore (*vendor lock-in*) può derivare da formati proprietari, componenti non interoperabili, licenze restrittive o costi di uscita non trasparenti. L'articolo mira quindi a rendere la soluzione trasferibile, verificabile e sostenibile lungo tutto il ciclo di vita contrattuale, anche in caso di cambio fornitore o reinternalizzazione del servizio.

Aspetti chiave

Le amministrazioni devono in particolare:

- richiedere la portabilità completa e strutturata dei dati (*data portability*) e degli artefatti del sistema, inclusi dati, metadati, log, istruzioni operative (*prompt*), configurazioni, rappresentazioni vettoriali (*embeddings*), output e altri elementi rilevanti;
- privilegiare formati aperti, schemi interoperabili, interfacce di programmazione documentate (API) e standard tecnici comuni;
- chiedere al Fornitore di dichiarare in modo trasparente vincoli tecnici, contrattuali o di licenza che possano ostacolare la migrazione dei dati, il riutilizzo degli output o la continuità del servizio;
- garantire la separazione logica dei dati e degli artefatti dell'Amministrazione rispetto a quelli di altri clienti o ambienti;
- prevedere procedure di cancellazione sicura dei dati, con evidenze documentali dell'avvenuta cancellazione o sanitizzazione;
- richiedere un piano di uscita dal servizio (*exit plan*) con supporto alla transizione, documentazione tecnica, trasferimento delle conoscenze (*knowledge transfer*) e tempi stimati per la migrazione;
- chiarire il regime di proprietà intellettuale relativo a modelli, componenti software, dataset e output generati;
- esplicitare costi e condizioni di uscita, che non devono costituire un ostacolo irragionevole alla migrazione del servizio o alla sostituzione del fornitore.

Implicazioni operative

In fase di redazione del capitolato, l'Amministrazione deve richiedere al fornitore evidenze concrete sulla portabilità della soluzione e valutare le offerte anche attraverso una tabella comparativa dedicata alla portabilità dei dati (*data portability*), alla portabilità dei modelli (*model portability*), alla predisposizione all'uscita dal servizio (*exit readiness*) e al rischio di dipendenza tecnologica (*lock-in risk*).

Questo consente di verificare ex ante quanto la soluzione sia effettivamente trasferibile, quali dipendenze tecnologiche presenti e quanto sia onerosa o semplice la cessazione del servizio. L'articolo 8 halo scopo di trasformare il tema del lock-in da rischio teorico a elemento concreto di valutazione nelle procedure di gara e di gestione contrattuale.

Articolo 9 – Gestione del rischio

Obiettivo

L'articolo definisce le modalità operative con cui il Fornitore deve identificare, valutare e mitigare i rischi associati al sistema di Intelligenza Artificiale oggetto dell'appalto lungo l'intero ciclo di vita della soluzione.

Razionale

I sistemi di IA possono generare rischi tecnici, operativi e potenziali impatti sui diritti fondamentali, sulla sicurezza o sul corretto funzionamento dei servizi pubblici. L'articolo introduce pertanto un processo strutturato di gestione del rischio, coerente con il Regolamento (UE) 2024/1689 (AI Act) e con le buone pratiche internazionali (ISO 31000 e ISO/IEC 23894), nonché con gli standard tecnici in via di definizione da parte di CEN e CENELEC, quando disponibili, proporzionato alla classificazione del sistema. Il processo deve valutare i rischi in relazione alla finalità prevista del sistema (*intended purpose*) e assicurare che, a seguito dell'adozione delle misure di mitigazione, il livello di rischio residuo sia considerato accettabile rispetto al contesto operativo dell'Amministrazione.

Aspetti chiave

Le amministrazioni devono in particolare richiedere che il Fornitore:

- adotti un processo strutturato di gestione del rischio applicabile a tutte le fasi del ciclo di vita del sistema (progettazione, sviluppo, addestramento, integrazione, esercizio e dismissione);
- distingua tra sistemi non ad alto rischio e sistemi ad alto rischio, applicando livelli di controllo proporzionati alla classificazione del sistema ai sensi dell'AI Act;
- predisponga un Risk Management Plan che descriva metodologia, ruoli, responsabilità e modalità di monitoraggio dei rischi;
- identifichi e valuti i rischi in termini di probabilità e gravità del danno, considerando anche scenari di uso improprio ragionevolmente prevedibile;
- definisca misure tecniche e organizzative di mitigazione, privilegiando interventi progettuali, controlli tecnici, supervisione umana e formazione degli utenti;
- effettui test e verifiche del sistema prima della messa in esercizio per valutare l'efficacia delle misure di mitigazione;
- mantenga una documentazione aggiornata dei rischi, delle misure adottate e del rischio residuo accettabile;
- istituisca e aggiorni un Registro dei rischi del sistema di IA durante l'intera durata del contratto.

Implicazioni operative

In fase di gara e durante l'esecuzione del contratto, l'Amministrazione deve richiedere evidenze documentali della gestione del rischio, tra cui il Risk Management Plan, il registro dei rischi e i risultati dei test di verifica. I rischi identificati devono essere collegati a indicatori di performance, attività di monitoraggio e eventuali misure correttive.

Articolo 10 – Trasparenza, spiegabilità e auditabilità dei sistemi di IA

Obiettivo

Il presente articolo stabilisce i requisiti che il sistema di Intelligenza Artificiale deve rispettare per garantire trasparenza, spiegabilità e auditabilità, consentendo all'Amministrazione di comprendere il funzionamento del sistema, interpretarne gli output e verificare nel tempo il corretto comportamento del modello.

Razionale

A differenza dei sistemi software tradizionali, i sistemi di IA possono produrre risultati probabilistici o difficilmente interpretabili. Per questo il capitolato richiede che il sistema renda comprensibili i propri output, documenti le proprie prestazioni e consenta la ricostruzione delle decisioni automatizzate. Il livello di trasparenza deve essere proporzionato alla classificazione del sistema ai sensi dell'AI Act.

Aspetti chiave

Le amministrazioni possono, con particolare riferimento al caso d'uso e ai requisiti applicabili dell'AI Act, richiedere che il Fornitore:

- documenti chiaramente finalità del sistema (*intended purpose*), capacità, limiti operativi e metriche di accuratezza;
- consenta l'interpretazione degli output e indichi le condizioni in cui le prestazioni del sistema possono degradare;
- garantisca tracciabilità delle operazioni tramite log strutturati, versionamento dei modelli e registrazione degli input rilevanti;
- renda possibile la ricostruzione ex post del processo decisionale del sistema;
- fornisca documentazione tecnica e operativa sufficiente per verifiche e controlli;
- consenta forme effettive di supervisione umana significativa;
- nei sistemi di Intelligenza Artificiale generativa, renda identificabili i contenuti generati artificialmente e consenta di distinguerli da contenuti prodotti da persone;
- metta a disposizione informazioni tecniche e strumenti utili per attività di audit e verifiche indipendenti.

Per i sistemi classificati come ad alto rischio, il sistema deve inoltre garantire livelli più elevati di trasparenza, *logging* e documentazione tecnica, in conformità all'articolo 13 del Regolamento (UE) 2024/1689 (AI Act).

Implicazioni operative

In fase di gara e di esecuzione contrattuale, l'Amministrazione deve richiedere evidenze concrete del livello di spiegabilità del sistema (documentazione tecnica, report di validazione, log di sistema, strumenti di interpretazione degli output). Il capitolato può prevedere diversi livelli di spiegabilità – dalla semplice descrizione del sistema fino alla piena auditabilità tecnica – collegandoli alla classificazione del sistema e al livello di rischio.

Articolo 11 – Supervisione umana

Obiettivo

L'articolo definisce i requisiti operativi che il sistema di IA deve garantire per consentire una supervisione umana efficace durante l'utilizzo del sistema, assicurando che l'Amministrazione mantenga il controllo sulle decisioni e sugli output generati.

Razionale

I sistemi di IA possono generare risultati probabilistici o automatizzati che richiedono controllo umano per evitare errori, *bias* o utilizzi impropri. L'AI Act richiede che i sistemi di IA, in particolare quelli ad alto rischio, siano progettati in modo da permettere un intervento umano significativo. Le misure di supervisione devono essere proporzionate al caso d'uso, al livello di autonomia del sistema e alla classificazione del sistema ai sensi dell'AI Act.

Aspetti chiave

Le amministrazioni devono in particolare richiedere che il sistema:

- consenta intervento umano effettivo sugli output, inclusa la possibilità di modifica, annullamento o sovrascrittura (*override*) delle decisioni automatizzate;
- permetta monitoraggio continuo del funzionamento del sistema e individuazione di anomalie o comportamenti inattesi;
- garantisca meccanismi di arresto o sospensione sicura del sistema;
- renda possibile la comprensione delle capacità e dei limiti del sistema da parte degli operatori;
- fornisca strumenti per evitare fenomeni di eccessiva fiducia nell'automazione (*automation bias)*, ossia eccessiva fiducia negli output del sistema;
- registri tramite log strutturati gli interventi umani e le operazioni di supervisione;
- integri il funzionamento del sistema nei processi amministrativi, mantenendo la responsabilità decisionale in capo all'Amministrazione.

Differenziazione in base al livello di rischio (AI Act)

- Sistemi non ad alto rischio
    - supervisione umana proporzionata al caso d'uso;
    - monitoraggio periodico o a campione degli output;
    - possibilità di intervento e *override* degli operatori.
- Sistemi ad alto rischio
    - supervisione umana rafforzata e continuativa (art. 14 AI Act);
    - validazione umana delle decisioni critiche;
    - strumenti per individuare anomalie e mitigare l'*automation bias*;
    - tracciabilità completa delle decisioni del sistema e degli interventi umani.

Implicazioni operative

In fase di gara e di collaudo, l'Amministrazione deve verificare che il sistema integri meccanismi concreti di supervisione umana, quali strumenti di monitoraggio, possibilità di modifica o annullamento delle decisioni del sistema, registrazione delle attività tramite log e procedure di arresto sicuro del sistema.

I livelli di supervisione devono essere documentati dal fornitore, verificati in fase di collaudo e collegati ai processi amministrativi e alla formazione degli operatori, in modo da garantire un controllo umano effettivo sull'utilizzo del sistema di Intelligenza Artificiale.

Articolo 12 – Sicurezza e robustezza dei sistemi di IA

Obiettivo

Il presente articolo definisce i requisiti di sicurezza, robustezza e cybersicurezza che devono caratterizzare i sistemi di Intelligenza Artificiale acquisiti dall'Amministrazione, garantendo che tali sistemi operino in modo affidabile e sicuro lungo l'intero ciclo di vita.

Razionale

I sistemi di IA introducono rischi specifici legati ai dati, ai modelli, agli algoritmi e alle infrastrutture che li supportano. Il capitolato richiede quindi che la sicurezza sia integrata nella progettazione, nello sviluppo e nella gestione operativa del sistema. I requisiti devono essere proporzionati al caso d'uso, al livello di autonomia del sistema e alla classificazione prevista dall'AI Act, con misure rafforzate per i sistemi classificati come ad alto rischio.

Aspetti chiave

Le amministrazioni possono richiedere che il fornitore:

- progetti il sistema secondo i principi di sicurezza fin dalla progettazione e per impostazione predefinita, assicurando sicurezza lungo tutto il ciclo di vita del sistema (sviluppo, addestramento, integrazione, esercizio, aggiornamento e dismissione);
- identifichi e protegga gli asset critici del sistema di IA, tra cui dati, modelli, infrastrutture ICT, pipeline di sviluppo e attori della filiera tecnologica;
- implementi misure di protezione contro minacce tipiche dei sistemi di IA, come manipolazione dei dati di addestramento, attacchi *adversarial*, estrazione del modello o uso improprio dei sistemi generativi;
- definisca metriche di accuratezza, robustezza e sicurezza del sistema, con procedure di monitoraggio continuo delle prestazioni del modello;
- adotti misure di cybersicurezza adeguate, tra cui controllo degli accessi, crittografia dei dati, gestione delle chiavi e segregazione dei dati;
- predisponga un piano di gestione delle vulnerabilità, che includa identificazione delle vulnerabilità, aggiornamenti di sicurezza, gestione degli incidenti e procedure di ripristino;
- documenti in modo completo l'architettura di sicurezza del sistema, incluse le misure di protezione dei dati, dei modelli e delle infrastrutture;
- fornisca strumenti operativi per il monitoraggio della sicurezza, come log, dashboard, report e procedure di risposta agli incidenti;

- consenta verifiche e audit di sicurezza da parte dell'Amministrazione, fornendo le evidenze tecniche necessarie a dimostrare la conformità ai requisiti previsti dal capitolato.

Proporzionalità e differenziazione secondo l'AI Act

- Sistemi non classificati come ad alto rischio
  - applicazione di misure di sicurezza proporzionate al caso d'uso;
  - monitoraggio delle prestazioni e della sicurezza del sistema;
  - controlli di sicurezza standard su dati, modelli e infrastrutture.
- Sistemi classificati come ad alto rischio
  - applicazione dei requisiti di accuratezza, robustezza e cybersicurezza previsti dall'articolo 15 dell'AI Act;
  - monitoraggio rafforzato delle prestazioni del sistema;
  - documentazione tecnica più completa e verificabile;
  - controlli di sicurezza più stringenti su dati, modelli e pipeline di sviluppo.

Implicazioni operative

In fase di gara, collaudo ed esecuzione del contratto, l'Amministrazione deve verificare che il fornitore implementi controlli tecnici verificabili, come controlli di accesso, crittografia dei dati, gestione delle vulnerabilità, monitoraggio delle prestazioni del modello e protezione contro attacchi specifici ai sistemi di IA. L'utilizzo di matrici di controllo della sicurezza, indicatori di prestazione e test di verifica consente di collegare i requisiti di sicurezza alle responsabilità contrattuali del fornitore e di garantire un controllo continuo sulla sicurezza e sulla resilienza del sistema nel tempo.

Articolo 13 – Requisiti di sovranità digitale

Obiettivo

Il presente articolo definisce i requisiti necessari per garantire che l'Amministrazione mantenga il controllo giuridico, tecnico e operativo sui sistemi di Intelligenza Artificiale adottati, sui dati utilizzati e sulle infrastrutture tecnologiche impiegate.

Razionale

L'utilizzo di sistemi di IA, in particolare quando basati su infrastrutture cloud o modelli forniti da terzi, può generare dipendenze tecnologiche e rischi legati alla giurisdizione dei dati, alla catena di fornitura e al controllo operativo del sistema. Il capitolato introduce quindi requisiti di sovranità digitale che consentono all'Amministrazione di mantenere il controllo su dati, modelli, infrastrutture e fornitori lungo l'intero ciclo di vita del sistema. I requisiti devono essere proporzionati al caso d'uso, alla criticità dei dati trattati e alla classificazione del sistema ai sensi dell'AI Act, con requisiti più stringenti nei casi in cui il sistema presenti rischi elevati o tratti dati sensibili.

Aspetti chiave

Le amministrazioni possono richiedere che il fornitore:

- garantisca la sovranità dei dati, assicurando che i dati dell'Amministrazione siano soggetti alla giurisdizione dell'Unione europea o di altra giurisdizione autorizzata e che eventuali trasferimenti verso Paesi terzi siano esplicitamente dichiarati e giuridicamente giustificati;
- fornisca una mappatura completa dei flussi e delle localizzazioni dei dati, indicando dove i dati sono archiviati, elaborati e trasmessi;
- garantisca il controllo operativo dell'Amministrazione sul sistema, consentendo la gestione degli accessi, delle configurazioni di sicurezza, dei log e delle attività di monitoraggio;
- eviti dipendenze tecnologiche non giustificate, utilizzando ove possibile standard aperti, architetture interoperabili e interfacce documentate;
- dichiari eventuali dipendenze da infrastrutture *cloud*, *hyperscaler* o modelli di IA esterni, indicando le eventuali limitazioni tecniche o giurisdizionali;
- garantisca la conformità al GDPR e alla normativa europea applicabile, assicurando che eventuali subfornitori operino secondo clausole contrattuali coerenti con il diritto europeo;
- fornisca trasparenza sulla catena di fornitura tecnologica, includendo fornitori cloud, fornitori di modelli di IA, dataset utilizzati e componenti software rilevanti;
- preveda la possibilità di migrazione del sistema e dei dati verso altri fornitori o infrastrutture dell'Amministrazione, riducendo il rischio di dipendenza tecnologica.

Proporzionalità dei requisiti

I requisiti di sovranità digitale devono essere calibrati in funzione:

- della criticità del caso d'uso;
- della sensibilità dei dati trattati;
- del livello di rischio del sistema ai sensi dell'AI Act.

Nei casi più critici l'Amministrazione può richiedere misure rafforzate, quali:

- localizzazione dei dati esclusivamente nell'Unione europea;
- controllo completo sugli accessi e sulle configurazioni del sistema;
- piena portabilità dei dati e dei modelli;
- trasparenza completa sulla catena di fornitura tecnologica.

Implicazioni operative

In fase di gara l'Amministrazione può valutare il livello di sovranità digitale delle soluzioni proposte utilizzando matrici di valutazione strutturate, che analizzano dimensioni quali sovranità dei dati, controllo operativo, indipendenza tecnologica, garanzie giuridiche e trasparenza della supply chain.

Tali strumenti consentono di confrontare in modo oggettivo le offerte dei fornitori e di favorire soluzioni che garantiscano maggiore controllo sui dati pubblici, minore dipendenza tecnologica e maggiore resilienza dei sistemi di Intelligenza Artificiale nel lungo periodo.

PARTE III – GOVERNANCE, CONFORMITÀ E RESPONSABILITÀ

Articolo 14 – Sistema di gestione dell'Intelligenza Artificiale

Obiettivo

L'articolo definisce i requisiti organizzativi che il Fornitore deve dimostrare per garantire una gestione strutturata, controllata e verificabile dei sistemi di Intelligenza Artificiale lungo l'intero ciclo di vita della soluzione fornita all'Amministrazione.

Razionale

L'adozione di sistemi di IA richiede processi organizzativi e di governance che assicurino qualità, controllo dei rischi, responsabilità chiare e conformità normativa. A tal fine, il capitolato deve incoraggiare l'adozione di un Sistema di Gestione dell'Intelligenza Artificiale (*AI Management System*) secondo le norme tecniche internazionali disponibili.

Tale approccio è coerente con il quadro europeo introdotto dal Regolamento (UE) 2024/1689 (AI Act), che richiede ai fornitori di sistemi di IA ad alto rischio l'adozione di processi strutturati di gestione del rischio, controllo della qualità e supervisione lungo l'intero ciclo di vita del sistema. Nei casi che ricadono nell'ambito di applicazione dell'AI Act, tali sistemi di gestione dovranno essere allineati agli standard armonizzati adottati ai sensi del Regolamento, quando disponibili.

Il sistema di gestione adottato dal fornitore deve inoltre integrarsi con i sistemi di gestione della qualità, della sicurezza e della governance dei dati implementati dall'Amministrazione, in coerenza con quanto previsto dalle Linee Guida AgID per l'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione.

Aspetti chiave

I requisiti relativi al sistema di gestione dell'Intelligenza Artificiale devono essere proporzionati al caso d'uso, alla complessità del sistema e al livello di rischio associato, in coerenza con l'approccio basato sul rischio previsto dal Regolamento (UE) 2024/1689 (AI Act).

Le amministrazioni possono richiedere che il fornitore:

- dimostri di adottare un sistema di gestione dell'IA conforme agli standard internazionali disponibili, oppure un sistema equivalente di gestione dei processi e dei controlli relativi allo sviluppo e all'esercizio dei sistemi di IA;
- qualora non disponga di una certificazione, descriva in modo documentato la propria struttura di governance, indicando ruoli, responsabilità e processi decisionali relativi alla gestione dei sistemi di IA;
- definisca processi di controllo della qualità e di monitoraggio dei sistemi di IA, inclusi meccanismi di verifica delle prestazioni, gestione degli incidenti e aggiornamento dei modelli;
- dimostri l'esistenza di processi organizzativi per la gestione del rischio, della conformità normativa e della sicurezza dei sistemi di IA;

- descriva le modalità con cui tali processi sono applicati lungo il ciclo di vita del sistema, dalla progettazione allo sviluppo, fino alla gestione operativa e alla dismissione.

Il livello di formalizzazione e documentazione di tali processi deve essere adeguato alla natura del sistema di IA e rafforzato nei casi in cui il sistema rientri tra quelli classificati come ad alto rischio ai sensi dell'AI Act.

Specificità rispetto all'AI Act

L'applicazione di un sistema di gestione dell'IA consente al fornitore di strutturare in modo coerente i processi richiesti dal quadro normativo europeo, tra cui:

- gestione del rischio dei sistemi di IA;
- controllo della qualità dei dati e dei modelli;
- monitoraggio del funzionamento del sistema;
- gestione degli incidenti e dei malfunzionamenti.

Quando saranno pubblicati gli standard armonizzati previsti dall'AI Act, l'adozione di tali standard potrà costituire uno strumento per dimostrare la conformità ai requisiti tecnici del Regolamento.

Implicazioni operative

In fase di gara l'Amministrazione può richiedere al fornitore evidenze relative all'esistenza di un sistema strutturato di gestione dell'Intelligenza Artificiale e utilizzare tali informazioni per valutare il livello di maturità organizzativa e la capacità del fornitore di gestire in modo controllato lo sviluppo e l'esercizio dei sistemi di IA.

La presenza di un sistema di gestione conforme alle norme tecniche internazionali disponibili rappresenta un indicatore rilevante di affidabilità nella gestione dei sistemi di IA e può agevolare le attività di verifica della conformità ai requisiti durante l'esecuzione del contratto.

Nei casi in cui il sistema rientri nell'ambito di applicazione dell'AI Act, l'Amministrazione deve verificare puntualmente il rispetto dei requisiti previsti dal Regolamento, fino alla disponibilità degli standard armonizzati adottati ai sensi dello stesso Regolamento, che costituiranno il principale riferimento tecnico per la dimostrazione della conformità.

Articolo 15 – Documentazione tecnica

Obiettivo

L'articolo definisce i requisiti di documentazione tecnica che il Fornitore deve garantire per consentire all'Amministrazione di comprendere, utilizzare, monitorare e verificare il funzionamento del sistema di Intelligenza Artificiale lungo l'intero ciclo di vita.

Razionale

La disponibilità di una documentazione tecnica chiara e completa è essenziale per garantire la trasparenza, la controllabilità e la corretta gestione dei sistemi di IA nella Pubblica Amministrazione. Tali informazioni permettono all'Amministrazione di verificare le caratteristiche tecniche del sistema, di utilizzarlo in modo appropriato e di effettuare attività di monitoraggio, audit e manutenzione.

Nel caso di sistemi che rientrano nell'ambito di applicazione del Regolamento (UE) 2024/1689 (AI Act), la documentazione tecnica costituisce inoltre uno degli elementi fondamentali per dimostrare la conformità ai requisiti del Regolamento. In particolare, per i sistemi classificati come ad alto rischio, la documentazione tecnica deve essere conforme ai requisiti previsti dall'articolo 11 dell'AI Act, che richiede una documentazione idonea a consentire alle autorità e agli utilizzatori di valutare la conformità del sistema.

Aspetti chiave

Le amministrazioni possono richiedere che il fornitore fornisca una documentazione tecnica completa e aggiornata, proporzionata al caso d'uso e alla complessità del sistema di IA, che includa almeno:

- documentazione tecnica del sistema, contenente descrizione delle componenti, delle funzionalità e delle modalità di funzionamento del sistema di IA;
- manuale utente, con istruzioni operative per l'utilizzo del sistema, indicazione delle funzionalità disponibili, delle limitazioni e delle modalità di interpretazione degli output;
- manuale amministratore, con indicazioni tecniche per la configurazione, gestione e manutenzione del sistema;
- descrizione dell'architettura del sistema, incluse le principali componenti software, infrastrutturali e i servizi esterni eventualmente utilizzati;
- schemi dei flussi dei dati, che descrivano la raccolta, il trattamento, l'elaborazione e l'archiviazione dei dati utilizzati dal sistema di IA.

Specificità rispetto all'AI Act

Per i sistemi che rientrano nell'ambito di applicazione dell'AI Act, la documentazione deve consentire di:

- comprendere finalità prevista del sistema (*intended purpose*), capacità e limiti;
- verificare processi di sviluppo, addestramento e validazione del modello;
- analizzare flussi dei dati e modalità di gestione dei dataset;
- supportare attività di audit, monitoraggio e valutazione della conformità.

Nel caso di sistemi di IA ad alto rischio, la documentazione deve essere più dettagliata e strutturata, in modo da consentire la dimostrazione della conformità ai requisiti previsti dal Regolamento e dai futuri standard armonizzati dell'AI Act quando saranno disponibili.

Implicazioni operative

In fase di gara e di collaudo l'Amministrazione deve verificare che la documentazione tecnica sia completa, aggiornata e coerente con la soluzione proposta.

La documentazione costituisce uno strumento essenziale per consentire all'Amministrazione di gestire, monitorare e verificare il sistema di IA durante l'intero ciclo di vita, nonché per facilitare le attività di audit, manutenzione e eventuale migrazione del sistema verso altre soluzioni.

Articolo 16 – Monitoraggio successivo alla messa in esercizio (post-deployment)

Obiettivo

Il presente articolo definisce i requisiti operativi per il monitoraggio del sistema di Intelligenza Artificiale dopo la sua messa in esercizio, al fine di garantire il mantenimento nel tempo delle prestazioni, della sicurezza e della conformità normativa.

Razionale

I sistemi di IA possono modificare il proprio comportamento nel tempo a causa di cambiamenti nei dati, nel contesto operativo o nelle modalità di utilizzo. È quindi necessario prevedere attività di monitoraggio continuo che consentano di individuare tempestivamente degradazioni delle prestazioni, rischi emergenti o incidenti operativi.

Nel quadro del Regolamento (UE) 2024/1689 (AI Act), il monitoraggio successivo alla messa in esercizio (*post-deployment*) è particolarmente rilevante per i sistemi classificati come ad alto rischio, per i quali il Regolamento richiede attività strutturate di monitoraggio e gestione degli incidenti lungo l'intero ciclo di vita del sistema. I requisiti devono pertanto essere proporzionati al caso d'uso e rafforzati nei casi che rientrano nell'ambito di applicazione dell'AI Act.

Aspetti chiave

Le amministrazioni possono richiedere che il fornitore:

- garantisca monitoraggio continuo delle prestazioni del sistema, attraverso indicatori di performance e controlli periodici sulle prestazioni del modello;
- implementi strumenti per individuare degradazioni delle prestazioni, errori sistematici o anomalie operative, inclusi fenomeni di *model drift* o cambiamenti nel comportamento del sistema;
- notifichi tempestivamente all'Amministrazione eventuali incidenti rilevanti, malfunzionamenti o rischi identificati durante l'utilizzo del sistema;
- mantenga log e registrazioni delle attività del sistema, utili per attività di audit, verifica e analisi degli incidenti;
- aggiorni il sistema e la documentazione tecnica in caso di modifiche normative, aggiornamenti tecnologici o cambiamenti nel contesto operativo;
- metta a disposizione report periodici sul funzionamento del sistema, includendo indicatori di performance, incidenti rilevati e interventi correttivi effettuati.

Specificità rispetto all'AI Act

Per i sistemi che rientrano nell'ambito dell'AI Act, il monitoraggio successivo alla messa in esercizio (*post-deployment*) deve consentire di:

- individuare rischi emergenti e degradazioni delle prestazioni del sistema nel tempo;
- supportare la gestione e la segnalazione degli incidenti previsti dal Regolamento;

- mantenere aggiornata la documentazione tecnica e le misure di gestione del rischio.

Nel caso di sistemi classificati come ad alto rischio, il monitoraggio deve essere più strutturato e continuo, in modo da consentire all'Amministrazione di dimostrare la conformità ai requisiti del Regolamento e dei futuri standard armonizzati dell'AI Act, quando disponibili.

Implicazioni operative

In fase di gara e di esecuzione del contratto l'Amministrazione deve verificare che il fornitore preveda processi chiari di monitoraggio, gestione degli incidenti e aggiornamento del sistema.

Il monitoraggio successivo alla messa in esercizio (*post-deployment*) consente alla Pubblica Amministrazione di mantenere un controllo continuo sul funzionamento del sistema di IA, individuare tempestivamente eventuali criticità e garantire che il sistema rimanga conforme ai requisiti normativi e contrattuali durante tutto il suo ciclo di vita.

Articolo 17 – Licenze software e diritti di utilizzo

Obiettivo

L'articolo definisce le condizioni relative alle licenze software e ai diritti di utilizzo delle componenti tecnologiche impiegate nella soluzione di Intelligenza Artificiale, al fine di garantire all'Amministrazione la possibilità di utilizzare, gestire ed evolvere il sistema senza restrizioni non giustificate.

Razionale

Le soluzioni di IA possono includere componenti software proprietarie, modelli di IA, librerie *open source*, dataset e servizi di terze parti. È quindi necessario definire in modo chiaro i diritti di utilizzo concessi all'Amministrazione e assicurare trasparenza sulle componenti tecnologiche che compongono il sistema. Questa esigenza è coerente con il Regolamento (UE) 2024/1689 (AI Act), che richiede un adeguato livello di documentazione tecnica, trasparenza e tracciabilità delle componenti dei sistemi di IA, in particolare per i sistemi classificati come ad alto rischio.

A tal fine, il capitolato può richiedere la predisposizione di un *AI Bill of Materials*[1] (AIBOM), ossia un inventario strutturato delle componenti tecnologiche del sistema di IA. L'AIBOM consente all'Amministrazione di conoscere le componenti software, i modelli e i servizi utilizzati nella soluzione, facilitando attività di audit, gestione delle vulnerabilità, controllo della supply chain tecnologica e verifica della conformità ai requisiti dell'AI Act e ai futuri standard armonizzati del Regolamento.

Aspetti chiave

Le amministrazioni possono richiedere che il fornitore:

- indichi in modo trasparente tutte le licenze software utilizzate, inclusi componenti proprietari, software open source, modelli di IA e servizi di terze parti;

[1] National Telecommunications and Information Administration (NTIA). 2021. The Minimum Elements for a Software Bill of Materials (SBOM). U.S. Department of Commerce.

- specifichi i diritti di utilizzo concessi all'Amministrazione, inclusa la possibilità di utilizzare, configurare e gestire il sistema durante tutta la durata contrattuale;
- chiarisca eventuali limitazioni di licenza, incluse restrizioni relative all'uso del software, alla modifica delle componenti o alla distribuzione del sistema;
- indichi le condizioni di utilizzo dei modelli di IA e delle librerie software integrate nella soluzione;
- fornisca un *AI Bill of Materials* (AIBOM) contenente l'elenco delle principali componenti tecnologiche del sistema di IA, tra cui:
    - componenti software e librerie utilizzate
    - modelli di IA impiegati
    - dataset o fonti di dati rilevanti
    - servizi cloud o API esterne
    - componenti open source e relative licenze;
- garantisca che l'Amministrazione possa continuare a utilizzare il sistema e i dati generati anche dopo la cessazione del contratto, nei limiti previsti dalle licenze applicabili;
- descriva il regime di proprietà intellettuale relativo alle componenti sviluppate nell'ambito del contratto, inclusi eventuali diritti di riutilizzo da parte del fornitore.

Implicazioni operative

In fase di gara l'Amministrazione deve verificare che le condizioni di licenza siano chiare, compatibili con l'utilizzo pubblico del sistema e prive di restrizioni che possano compromettere la continuità operativa del servizio.

La disponibilità di un *AI Bill of Materials* (AIBOM) consente inoltre di aumentare la trasparenza della soluzione proposta, supportare le attività di audit tecnico e facilitare la verifica della conformità ai requisiti del Regolamento europeo sull'Intelligenza Artificiale (AI Act), in particolare per quanto riguarda documentazione tecnica, gestione della supply chain tecnologica e sicurezza del sistema.

Articolo 18 – Ciclo di vita del sistema e struttura dei costi

Obiettivo

L'articolo definisce i requisiti per la strutturazione dell'offerta economica secondo una logica di ciclo di vita del sistema, al fine di consentire all'Amministrazione di valutare in modo completo e trasparente i costi associati alla realizzazione, gestione, evoluzione e dismissione del sistema di Intelligenza Artificiale.

Razionale

I sistemi di IA generano costi distribuiti lungo l'intero ciclo di vita del sistema, che includono non solo lo sviluppo iniziale ma anche integrazione, esercizio, aggiornamento dei modelli, gestione dei dati e dismissione del sistema.

Per questo motivo le Linee Guida AgID per il procurement di sistemi di Intelligenza Artificiale raccomandano di valutare le soluzioni secondo una logica di costo complessivo lungo il ciclo di vita. Tale approccio è

coerente con il modello *Levelized Cost of Artificial Intelligence* (LCOAI), che consente di stimare il costo totale di una soluzione di IA lungo l'intero periodo di utilizzo, includendo costi operativi, infrastrutturali e di manutenzione.

L'adozione di una logica di costo lungo il ciclo di vita (*lifecycle cost*) consente all'Amministrazione di confrontare le offerte in modo più realistico e di prevenire soluzioni apparentemente economiche nella fase iniziale ma onerose nel lungo periodo.

Aspetti chiave

Le amministrazioni possono richiedere che l'offerta economica sia strutturata secondo le principali fasi del ciclo di vita del sistema di IA e includa almeno:

- costi di sviluppo o acquisizione della soluzione, inclusi progettazione, configurazione e personalizzazione;
- costi di integrazione, relativi all'interoperabilità con i sistemi informativi dell'Amministrazione e alle attività di implementazione;
- costi di esercizio, inclusi utilizzo delle infrastrutture, servizi cloud, utilizzo dei modelli e gestione operativa del sistema;
- costi di manutenzione, comprendenti supporto tecnico, gestione operativa e correzione di malfunzionamenti;
- costi di aggiornamento, inclusi aggiornamento dei modelli, evoluzione della soluzione e adeguamento a cambiamenti tecnologici o normativi;
- costi di dismissione, inclusi cessazione del servizio, trasferimento dei dati, migrazione del sistema o disattivazione delle infrastrutture.

Implicazioni operative

In fase di gara l'Amministrazione deve richiedere una scomposizione dei costi lungo il ciclo di vita del sistema, coerente con l'approccio indicato nelle Linee Guida AgID per il procurement dell'Intelligenza Artificiale e con i principi del modello LCOAI. Questo consente di confrontare le offerte non solo sulla base del prezzo iniziale, ma anche considerando i costi operativi e di gestione nel tempo, migliorando la sostenibilità economica delle soluzioni adottate e riducendo il rischio di costi nascosti durante l'esecuzione del contratto.

PARTE IV – VERIFICHE E COLLAUDO

Articolo 19 – Verifica di conformità

Obiettivo

L'articolo definisce le modalità con cui l'Amministrazione verifica che il sistema di Intelligenza Artificiale fornito sia conforme ai requisiti tecnici, organizzativi e normativi previsti dal capitolato prima della messa in esercizio e durante l'esecuzione del contratto.

Razionale

I sistemi di IA possono presentare rischi tecnici, operativi e normativi che devono essere verificati in modo sistematico prima della loro messa in esercizio. La verifica di conformità consente all'Amministrazione di accertare che la soluzione implementata rispetti i requisiti contrattuali, le specifiche tecniche e la normativa applicabile.

Nel caso di sistemi che rientrano nell'ambito del Regolamento (UE) 2024/1689 (AI Act), tali verifiche assumono particolare rilevanza per dimostrare che il sistema sia stato sviluppato e implementato in modo conforme ai requisiti previsti dal Regolamento, in particolare per i sistemi classificati come ad alto rischio.

Aspetti chiave

Le amministrazioni possono prevedere che le verifiche di conformità includano almeno:

- verifica della documentazione tecnica del sistema, inclusa architettura, flussi dei dati e istruzioni operative;
- verifica delle prestazioni del sistema, mediante test su dataset di validazione o scenari operativi rappresentativi;
- verifica dei requisiti di sicurezza, robustezza e affidabilità, inclusa la capacità del sistema di operare correttamente nel contesto operativo previsto;
- verifica dei requisiti di trasparenza, tracciabilità e *logging* del sistema;
- verifica dell'integrazione con i sistemi informativi dell'Amministrazione;
- verifica dei requisiti di supervisione umana, ove previsti;
- verifica delle misure di gestione del rischio e monitoraggio del sistema.

Le verifiche possono essere effettuate:

  - in fase di collaudo iniziale del sistema;
  - durante l'esecuzione del contratto;
  - in occasione di aggiornamenti rilevanti del sistema o dei modelli.

Specificità rispetto all'AI Act

Per i sistemi che rientrano nell'ambito dell'AI Act, le verifiche devono consentire di accertare il rispetto dei requisiti previsti dal Regolamento, tra cui:

- documentazione tecnica del sistema;
- gestione del rischio;

- qualità dei dati e dei modelli;
- supervisione umana;
- monitoraggio messa in esercizio *(post-deployment)*.

Nel caso di sistemi ad alto rischio, le verifiche devono essere più approfondite e documentate, in modo da supportare la dimostrazione della conformità ai requisiti del Regolamento e ai futuri standard armonizzati dell'AI Act quando saranno disponibili.

Implicazioni operative

In fase di gara e di esecuzione del contratto l'Amministrazione deve definire procedure di verifica e collaudo chiare e verificabili, incluse metriche di prestazione, test tecnici e modalità di audit.

Queste attività consentono di garantire che il sistema di IA implementato sia effettivamente conforme ai requisiti previsti dal capitolato e che il suo utilizzo nei processi amministrativi avvenga in modo controllato e sicuro.

Articolo 20 – Penali e responsabilità

Obiettivo

L'articolo disciplina le responsabilità del fornitore e le eventuali penali applicabili nel caso di mancato rispetto dei requisiti contrattuali relativi allo sviluppo, all'implementazione e al funzionamento del sistema di Intelligenza Artificiale.

Razionale

I sistemi di IA possono incidere sul funzionamento dei servizi pubblici e sul corretto svolgimento dei procedimenti amministrativi. È quindi necessario prevedere meccanismi contrattuali che consentano all'Amministrazione di intervenire in caso di mancato rispetto dei requisiti tecnici, di degrado delle prestazioni del sistema o di violazioni degli obblighi contrattuali.

L'introduzione di penali e responsabilità contrattuali consente di collegare in modo diretto i requisiti tecnici del sistema di IA alle prestazioni operative del fornitore, rafforzando la tutela dell'Amministrazione.

Aspetti chiave

Le amministrazioni possono prevedere che:

- il fornitore sia responsabile della conformità del sistema ai requisiti tecnici e normativi previsti dal capitolato;
- siano definite penali contrattuali in caso di mancato rispetto dei livelli di servizio o dei requisiti tecnici del sistema;
- siano previste penali in caso di:
  - mancato raggiungimento delle prestazioni minime del sistema;
  - mancata gestione o comunicazione di incidenti rilevanti;
  - mancata implementazione delle misure di sicurezza previste;
  - mancato rispetto delle tempistiche di aggiornamento o manutenzione;

- le penali siano proporzionate alla gravità dell'inadempimento e all'impatto sui servizi pubblici;
- siano previste misure correttive obbligatorie per il ripristino delle prestazioni del sistema.

Specificità rispetto all'AI Act

Nel caso di sistemi che rientrano nell'ambito dell'AI Act, il fornitore deve garantire il rispetto dei requisiti previsti dal Regolamento applicabili al sistema. Eventuali violazioni relative alla gestione del rischio, alla sicurezza del sistema, alla qualità dei dati o alla documentazione tecnica possono costituire inadempimenti contrattuali, con conseguente applicazione delle penali previste dal contratto.

Implicazioni operative

La definizione di penali e responsabilità consente all'Amministrazione di:

- collegare requisiti tecnici e prestazioni contrattuali;
- garantire il rispetto dei livelli di servizio;
- intervenire tempestivamente in caso di malfunzionamenti o violazioni contrattuali.

Questo approccio contribuisce a rendere il capitolato uno strumento effettivo di governo dei sistemi di Intelligenza Artificiale durante l'intero ciclo di vita contrattuale.

Sezione Allegati

Lo schema di capitolato è integrato da una serie di allegati tecnici, che costituiscono parte integrante della documentazione di gara.

Gli allegati hanno la funzione di:

- descrivere il contesto tecnico e organizzativo dell'intervento;
- strutturare la presentazione delle offerte tecniche da parte degli operatori economici;
- definire modelli standardizzati per la verifica delle prestazioni del sistema di Intelligenza Artificiale durante l'esecuzione del contratto.

Al fine di garantire chiarezza nella procedura di gara, gli allegati sono distinti nelle seguenti categorie:

1. allegati predisposti e compilati dall'Amministrazione, che descrivono il contesto, i fabbisogni funzionali e le condizioni operative del sistema;
2. allegati che individuano modelli di documenti e informazioni che devono essere compilati o forniti dall'Offerente, i quali costituiscono parte integrante dell'offerta tecnica e consentono di descrivere in modo strutturato la soluzione proposta;
3. allegati che individuano modelli di documenti e informazioni necessari nelle fasi di verifica, monitoraggio o collaudo, che possono essere utilizzati congiuntamente dall'Amministrazione e dal Fornitore durante l'esecuzione del contratto.

Allegato A – Descrizione funzionale del sistema e del caso d'uso

L'Allegato A ha lo scopo di descrivere in modo chiaro e strutturato il caso d'uso amministrativo e le principali funzionalità attese del sistema di Intelligenza Artificiale oggetto dell'affidamento. L'allegato è predisposto e compilato dall'Amministrazione e rappresenta il riferimento principale per comprendere il contesto organizzativo e operativo in cui il sistema dovrà essere utilizzato.

In particolare, l'allegato descrive:

- il processo amministrativo o il servizio pubblico oggetto di intervento;
- gli obiettivi istituzionali perseguiti mediante l'utilizzo del sistema di IA;
- le principali funzionalità attese del sistema;
- i flussi operativi coinvolti;
- il ruolo degli operatori umani nel processo decisionale.

La descrizione delle funzionalità deve essere formulata in modo neutro rispetto alla tecnologia, evitando riferimenti a specifiche soluzioni tecniche o architetture proprietarie. L'obiettivo è consentire agli operatori economici di proporre soluzioni tecnologiche diverse, purché in grado di soddisfare le esigenze funzionali indicate dall'Amministrazione.

L'Allegato A costituisce inoltre il riferimento per la valutazione della coerenza tra il caso d'uso e la soluzione proposta, nonché per la definizione dei criteri di verifica in fase di collaudo. Le informazioni contenute

nell'allegato permettono agli offerenti di comprendere il contesto applicativo del sistema e di sviluppare una proposta tecnica adeguata alle esigenze dell'Amministrazione.

Allegato B – Contesto dati e sistemi informativi coinvolti

L'Allegato B descrive il contesto informativo e tecnologico nel quale il sistema di Intelligenza Artificiale sarà implementato. L'allegato è predisposto e compilato dall'Amministrazione e fornisce agli operatori economici le informazioni necessarie per comprendere l'ecosistema digitale in cui la soluzione dovrà essere integrata.
In particolare, l'allegato può includere:

- la tipologia dei dati disponibili o previsti per l'utilizzo del sistema;
- le fonti dei dati (sistemi interni, banche dati pubbliche, dataset esterni);
- le principali caratteristiche dei dati, quali formato, volume, frequenza di aggiornamento e qualità;
- i sistemi informativi con cui la soluzione dovrà interoperare;
- eventuali vincoli normativi o organizzativi relativi alla gestione dei dati.

L'allegato ha la funzione di garantire trasparenza sul contesto informativo, permettendo agli operatori economici di valutare correttamente la fattibilità tecnica della soluzione e i requisiti di integrazione con l'infrastruttura esistente.
Le informazioni contenute nell'allegato possono inoltre essere utilizzate per supportare le attività di analisi del rischio, gestione della qualità dei dati e valutazione degli impatti, in coerenza con i requisiti previsti dal capitolato e con le disposizioni del Regolamento (UE) 2024/1689 in materia di gestione dei dati nei sistemi di Intelligenza Artificiale.

Allegato C – Schede funzionali della soluzione proposta

L'Allegato C contiene lo schema delle schede funzionali della soluzione proposta dall'Offerente e costituisce parte integrante dell'offerta tecnica.
Attraverso tali schede, l'Offerente descrive in modo strutturato le funzionalità del sistema di Intelligenza Artificiale che intende realizzare o fornire, indicando per ciascuna funzionalità:

- la descrizione operativa della capacità del sistema;
- i dati di input utilizzati;
- gli output generati;
- le metriche di performance applicabili;
- il livello di autonomia del sistema;
- le modalità di supervisione umana previste;
- eventuali rischi operativi e misure di mitigazione.

Le schede funzionali consentono all'Amministrazione di valutare in modo comparabile le diverse soluzioni proposte, verificando la coerenza tra le funzionalità richieste nell'Allegato A e quelle effettivamente offerte.

L'utilizzo di un modello strutturato favorisce inoltre la trasparenza tecnica della soluzione proposta, facilitando le attività di valutazione dell'offerta e le successive verifiche in fase di collaudo.

Allegato D – Matrice di gestione del rischio del sistema di IA

L'Allegato D contiene lo schema della matrice di gestione del rischio del sistema di Intelligenza Artificiale, che deve essere compilata dall'Offerente come parte integrante dell'offerta tecnica.
L'allegato ha lo scopo di documentare in modo strutturato i principali rischi associati al sistema proposto e le misure previste per la loro mitigazione.
La matrice consente di individuare:

- le principali categorie di rischio (tecnici, operativi, legali, organizzativi);
- la probabilità di accadimento dei rischi identificati;
- il potenziale impatto sui processi amministrativi o sugli utenti;
- le misure tecniche e organizzative previste per la mitigazione;
- il livello di rischio residuo.

La compilazione della matrice consente all'Amministrazione di valutare la maturità del fornitore nella gestione dei rischi connessi ai sistemi di IA e la coerenza della soluzione proposta con i requisiti di gestione del rischio previsti dal capitolato e dal Regolamento (UE) 2024/1689.

Allegato E – Inventario delle componenti del sistema di IA (AI Bill of Materials)

L'Allegato E contiene lo schema di inventario delle componenti tecnologiche del sistema di Intelligenza Artificiale, noto anche come *AI Bill of Materials* (AIBOM).
L'allegato deve essere compilato dall'Offerente e ha lo scopo di fornire una descrizione trasparente delle principali componenti che costituiscono la soluzione proposta.
In particolare, l'inventario può includere:

- modelli di Intelligenza Artificiale utilizzati;
- librerie software e componenti open source;
- dataset o fonti di dati rilevanti;
- servizi cloud o infrastrutture utilizzate;
- interfacce applicative (API) o servizi esterni.

La disponibilità di un inventario strutturato delle componenti del sistema consente all'Amministrazione di comprendere la catena tecnologica della soluzione proposta, facilitando le attività di audit, gestione della sicurezza e controllo della *supply chain* tecnologica.

Allegato F – Matrice di collaudo e verifica delle funzionalità

L'Allegato F contiene lo schema della matrice di collaudo e verifica delle funzionalità del sistema, che viene utilizzata nelle fasi di verifica e accettazione della soluzione.
La matrice è utilizzata congiuntamente dall'Amministrazione e dal Fornitore e consente di collegare in modo diretto:

- le funzionalità del sistema;
- i test di verifica previsti;
- gli indicatori di performance applicabili;
- le soglie minime di accettazione.

L'utilizzo della matrice di collaudo permette di rendere trasparente e oggettiva la verifica delle prestazioni del sistema, riducendo il rischio di interpretazioni divergenti tra le parti.

Allegato G – Matrice KPI e livelli di servizio (SLA)

L'Allegato G definisce gli indicatori di prestazione (KPI) e i livelli di servizio (SLA) applicabili al sistema di Intelligenza Artificiale durante l'esecuzione del contratto.
L'allegato è predisposto dall'Amministrazione e stabilisce gli indicatori utilizzati per monitorare le prestazioni del sistema nel tempo.
Gli indicatori possono riguardare, ad esempio:

- accuratezza del sistema;
- tempi di risposta;
- disponibilità del servizio;
- qualità degli output generati;
- frequenza di aggiornamento del sistema.

L'allegato definisce inoltre le modalità di misurazione degli indicatori e le eventuali soglie minime di conformità.

Allegato H – Piano di portabilità dei dati ed exit strategy

L'Allegato H contiene lo schema del piano di portabilità dei dati e di uscita dal servizio, che deve essere predisposto dall'Offerente.
L'allegato descrive le modalità con cui l'Amministrazione potrà:

- esportare i dati e gli output del sistema;
- migrare il servizio verso un altro fornitore o infrastruttura;
- garantire la continuità operativa del servizio.

Il piano di portabilità rappresenta uno strumento fondamentale per prevenire situazioni di dipendenza tecnologica dal fornitore e garantire che l'Amministrazione mantenga nel tempo il controllo sui dati e sui sistemi utilizzati.

<<Fine documento>>