GOVERNANCE DELL'INTELLIGENZA ARTIFICIALE IN AZIENDA

POLICY, ARCHITETTURE E MODELLI DI COSTO PER UN USO SICURO, CONFORME E SOSTENIBILE

ICT Consulting

White Paper

Luglio 2026

ict CONSULTING

SOMMARIO

L’adozione dell’Intelligenza Artificiale generativa e dei Large Language Models sta attraversando una fase di forte accelerazione all’interno delle imprese. Il fenomeno non riguarda più soltanto iniziative sperimentali promosse dalle funzioni IT o Innovation, ma si manifesta ormai in modo diffuso lungo tre direttrici principali.

La prima è rappresentata dagli strumenti individuali, gratuiti o premium, accessibili tramite web o app e utilizzati autonomamente dai dipendenti. La seconda riguarda gli strumenti di produttività integrati nella dotazione aziendale, come gli assistenti per la suite office, il supporto allo sviluppo software o le piattaforme collaborative. La terza è costituita dalle funzionalità AI embedded nelle applicazioni enterprise, tra cui ERP, CRM, ITSM e altre piattaforme verticali di processo.

Questa evoluzione genera opportunità rilevanti: incremento della produttività individuale, riduzione dei tempi di analisi e redazione, automazione di attività ripetitive, miglioramento dell’accesso alla conoscenza interna e accelerazione dell’innovazione. Tuttavia, se non governata, la diffusione dell’AI può introdurre rischi altrettanto significativi: esposizione di informazioni riservate, violazioni normative e contrattuali, utilizzi non tracciati, duplicazione di informazioni e strumenti, crescita incontrollata dei costi, lock-in e produzione di output non verificati o non coerenti con gli standard aziendali.

L’obiettivo di questo whitepaper è proporre un modello organico di governo dell’AI in azienda, capace di unire dimensione organizzativa, architetturale, economica e di sicurezza. In particolare, il documento delinea:

- un modello di governance dell’uso dell’AI;
- un sistema di policy differenziate per strumenti individuali, strumenti aziendali e soluzioni enterprise;
- una strategia architetturale basata su AI Gateway per un routing intelligente delle richieste verso modelli diversi e una gestione/fruizione centralizzata del contesto e delle informazioni aziendali;
- l’integrazione della governance AI con i controlli di cybersecurity già esistenti;
- un modello di monitoraggio, attribuzione e controllo dei costi legati a token, API, licenze e capacità computazionale;
- un modello di AI Capability Factory per trasformare, attraverso una catena governata di attività, la conoscenza dell’organizzazione in prompt, strumenti, memoria, agenti e workflow AI-driven.

La tesi di fondo è che l’AI non debba essere né lasciata alla sola iniziativa individuale, né bloccata con logiche difensive eccessivamente rigide. Al contrario, occorre costruire un quadro abilitante, in cui l’impresa renda disponibili strumenti sicuri e performanti, definisca regole comprensibili e applichi controlli proporzionati al rischio.

In questo disegno, l’AI Gateway governa l’accesso ai modelli, ai dati e al contesto aziendale, assicurando l’applicazione delle policy; l’AI Capability Factory governa invece il processo attraverso cui le capacità AI vengono progettate, sviluppate, testate, pubblicate e mantenute nel tempo.

INDICE

SOMMARIO 1
1. PERCHÉ SERVE UNA GOVERNANCE DELL'AI 3
1.1. LA DIFFUSIONE DELL'AI IN AZIENDA 3
2. I RISCHI DA GOVERNARE 3
3. IL MODELLO DI GOVERNANCE AZIENDALE 4
3.1. PRINCIPI GUIDA 4
3.2. STRUTTURA ORGANIZZATIVA E RESPONSABILITÀ 5
4. POLICY DI UTILIZZO DELL'AI 6
4.1. STRUMENTI INDIVIDUALI AI E USO CONSAPEVOLE 6
4.2. STRUMENTI DI PRODUTTIVITÀ AI AZIENDALI 6
4.3. FUNZIONALITÀ AI NEI SISTEMI ENTERPRISE 7
5. AI GATEWAY PER L'ACCESSO A MODELLI E CONTENUTI 7
5.1. AI GATEWAY E ROUTING INTELLIGENTE 8
5.2. QUANDO ADOTTARE MODELLI ON PREMISES E ARCHITETTURE IBRIDE 9
5.3. AI GATEWAY COME CONTEXT PROVIDER 9
5.4. AI CAPABILITY FACTORY: INDUSTRIALIZZARE IL TRASFERIMENTO DELLA CONOSCENZA 11
6. SICUREZZA, COMPLIANCE E CONTROLLI TECNICI 13
6.1. PRIVACY, PROPRIETÀ INTELLETTUALE E REQUISITI REGOLAMENTARI 13
6.2. INTEGRAZIONE CON I CONTROLLI DI CYBERSECURITY ESISTENTI 13
6.3. BILANCIARE CONTROLLO E USABILITÀ 16
7. MODELLO ECONOMICO E CONTROLLO DEI CONSUMI 16
7.1. MISURAZIONE PER STRUTTURA ORGANIZZATIVA, PROFILO UTENTE E GRUPPO DI LAVORO 16
7.2. USO CONTROLLATO E CONDIVISO DELLE RISORSE 16
8. ROADMAP DI IMPLEMENTAZIONE 17
8.1. AI GOVERNANCE 17
8.2. EVOLUZIONE VERSO AI CAPABILITY FACTORY 18
9. CONCLUSIONI 19
DIRITTO D'AUTORE E PROPRIETÀ INTELLETTUALE 20
GLI AUTORI 21
ICT CONSULTING 22

Copyright © 2026 ICT Consulting S.p.A.

1. PERCHÉ SERVE UNA GOVERNANCE DELL'AI

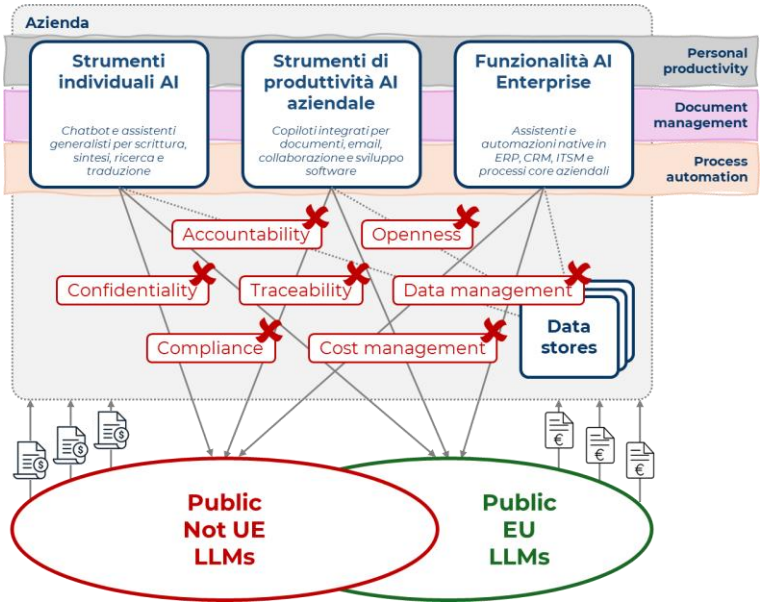
1.1. LA DIFFUSIONE DELL'AI IN AZIENDA

In molte organizzazioni, l'introduzione dell'AI è avvenuta in modo spontaneo e non pianificato. Dipendenti di funzioni diverse hanno iniziato a utilizzare chatbot pubblici, plugin del browser, app mobili e strumenti di generazione testi, immagini o codice per velocizzare attività quotidiane.

Questo approccio bottom up è comprensibile: gli strumenti sono accessibili, intuitivi e in grado di produrre benefici immediati. Tuttavia, in assenza di un quadro di governance, l'organizzazione perde visibilità su chi utilizzi quali strumenti, per quali finalità e con quali informazioni. Si genera così il fenomeno della *shadow AI*: un insieme di pratiche diffuse ma non censite, non validate e spesso non compatibili con le esigenze di sicurezza e compliance dell'impresa.

Parallelamente, molte aziende stanno introducendo soluzioni AI in forma più strutturata, attraverso strumenti di produttività aziendale e funzionalità generative integrate nelle piattaforme enterprise. Assistenti per documenti, email, meeting, sviluppo software e knowledge management promettono di incidere direttamente sui processi operativi e sulla produttività.

Anche in questo caso, però, l'adozione non può essere trattata come una semplice estensione funzionale degli strumenti già in uso. L'AI introduce infatti una nuova capacità di accesso, sintesi e rielaborazione dei dati, che può amplificare problemi preesistenti di gestione dei permessi, classificazione delle informazioni e qualità delle basi documentali.



La sfida è quindi duplice. Da un lato, occorre assicurare che le nuove funzionalità siano coerenti con le policy aziendali, i modelli di autorizzazione e i vincoli normativi. Dall'altro, è necessario prevenire duplicazioni, acquisti ridondanti e consumi non ottimizzati, soprattutto quando più piattaforme introducono componenti AI con logiche e costi differenti.

2. I RISCHI DA GOVERNARE

L'adozione dell'AI in azienda espone a un insieme di rischi che devono essere considerati in modo integrato.

Copyright © 2026 ICT Consulting S.p.A.

I **rischi informativi** riguardano la possibile perdita o diffusione di dati sensibili, inclusi dati di clienti, informazioni di pricing, segreti industriali, documentazione di ricerca e sviluppo e proprietà intellettuale dell'azienda. Anche quando non viene trasmesso un documento completo, la combinazione di prompt, allegati e interazioni successive può consentire la ricostruzione di informazioni strategiche che un'azienda vorrebbe proteggere dalla divulgazione.

I **rischi legali e normativi** comprendono violazioni della disciplina privacy, inosservanza di NDA o obblighi contrattuali, problemi di titolarità e riuso degli output, nonché possibili responsabilità derivanti da contenuti generati in modo inesatto, discriminatorio o fuorviante.

I **rischi economici** derivano dalla proliferazione di subscription, licenze e chiamate API, oltre che dal consumo non governato di token e risorse computazionali. Senza una gestione organizzata a livello aziendale l'uso degli strumenti AI non è ottimizzato dal punto di vista dei costi, che rischiano di assumere valori elevati e fuori controllo.

I **rischi tecnologici** derivano dall'adozione di ecosistemi chiusi, architetture proprietarie e integrazioni non standardizzate, che possono vincolare l'azienda a specifici provider, modelli o ambienti di esecuzione. Senza un disegno architetturale coerente, l'organizzazione può esporsi a fenomeni di lock-in tecnologico, riducendo la propria capacità di scegliere, sostituire o combinare modelli diversi in funzione di costo, prestazioni, sicurezza e requisiti di compliance.

I **rischi organizzativi** sono causati da un'adozione frammentata, priva di formazione e standard condivisi, che riduce il valore potenziale dell'AI e genera comportamenti non uniformi tra funzioni, paesi e business unit. In questo scenario, l'azienda non industrializza i benefici dell'AI, ma ne subisce soprattutto la complessità.

Infine, i **rischi legati alla qualità del dato** derivano dall'assenza di una rappresentazione condivisa e governata delle informazioni aziendali in input agli strumenti AI. In questo scenario, ogni strumento AI può costruire una propria visione dell'impresa, parziale o non verificabile, soprattutto quando accede direttamente a repository, database, fogli di lavoro o API senza mediazione centralizzata. Ne deriva una minore affidabilità degli output, con difficoltà a distinguere informazioni validate da contenuti semplicemente disponibili e con la proliferazione di integrazioni frammentate.

3. IL MODELLO DI GOVERNANCE AZIENDALE

3.1. PRINCIPI GUIDA

Un efficace modello di governance dell'AI deve fondarsi su alcuni principi cardine.

Sicurezza e protezione dei dati. Nessuna soluzione AI, indipendentemente dalla sua utilità, deve compromettere la riservatezza delle informazioni, la tutela dei dati dei clienti o la proprietà intellettuale dell'azienda.

Conformità normativa e contrattuale. L'utilizzo dell'AI deve avvenire nel rispetto delle leggi applicabili, dei regolamenti di settore e degli impegni assunti verso clienti, fornitori e partner.

Trasparenza e tracciabilità. L'organizzazione deve poter ricostruire quali modelli siano utilizzati, attraverso quali sistemi, con quali categorie di dati e da quali utenti o applicazioni, ovviamente con un'opportuna copertura giuslavoristica dei diritti dei lavoratori e di salvaguardia della privacy.

Proporzionalità ed efficienza dei costi. L'AI deve essere impiegata dove produce valore misurabile, evitando l'uso di modelli sovradimensionati, ridondanze architetturali e consumi fuori controllo.

Apertura architetturale e interoperabilità. L'azienda deve evitare dipendenze strutturali da un singolo provider, modello o ecosistema tecnologico, progettando soluzioni AI modulari, interoperabili

Copyright © 2026 ICT Consulting S.p.A.

e sostituibili. Questo consente di orchestrare modelli diversi in funzione di costo, prestazioni, sicurezza, localizzazione dei dati e compliance, riducendo il rischio di lock-in tecnologico e preservando la capacità evolutiva della strategia AI.

Accountability. Devono essere chiaramente definiti i ruoli di chi autorizza, chi progetta, chi usa, chi valida, chi controlla e chi monitora le soluzioni AI e deve essere messa in campo la gestione dei ruoli e dei privilegi.

Layer informativo condiviso, basato su fonti certificate e tracciabili. L'impresa deve rendere disponibili agli strumenti AI concetti di business, relazioni tra entità, documentazione, metadati, processi, ownership e regole di accesso attraverso una rappresentazione strutturata, interrogabile e governata. Tale contesto deve distinguere chiaramente dati master, dati derivati, documenti approvati, contenuti informali e informazioni obsolete.

Trasformazione industriale della conoscenza in capacità AI operative. La governance dell'AI non si deve limitare alla selezione dei modelli o alla sicurezza dei dati, ma deve includere una **AI Capability Factory** aziendale. Tale Factory deve governare la trasformazione progressiva della conoscenza dell'organizzazione in istruzioni, contesto, strumenti, memorie e agenti, attraverso processi di formalizzazione, test, versionamento, approvazione e monitoraggio. In questo modo l'uso dell'AI diviene ripetibile, misurabile e allineato alle responsabilità organizzative, evitando che i processi operativi siano governati in modo informale tramite testi inseriti manualmente e scollegati dai dati, dagli strumenti, dalla memoria e dai controlli aziendali.

Infine, è essenziale bilanciare **centralizzazione delle policy e decentramento dell'uso**. Le regole, gli standard e le architetture di sicurezza devono essere governati centralmente, mentre la valorizzazione dell'AI deve poter avvenire nelle diverse funzioni di business all'interno di confini chiari secondo il paradigma *centralized expertise and decentralized innovation*.

3.2. STRUTTURA ORGANIZZATIVA E RESPONSABILITÀ

Per rendere operativi questi principi, è opportuno istituire un **AI Governance Board** multidisciplinare. Il Board dovrebbe coinvolgere, in modo stabile, rappresentanti di IT, Digital, Data, Legal & Compliance, Information Security, HR e funzioni di business. In organizzazioni mature, può essere utile integrare anche una funzione dedicata di AI Office o Data Office.

Il Board non deve trasformarsi in un organismo burocratico, ma operare come cabina di regia. I suoi compiti principali includono la definizione e l'aggiornamento delle policy, l'approvazione del catalogo degli strumenti AI autorizzati, la classificazione dei casi d'uso per livello di rischio, la supervisione delle scelte architetturali e il monitoraggio dei principali indicatori di adozione, costo e compliance.

Per i casi d'uso a maggiore criticità, è opportuno prevedere un workflow di approvazione strutturato che coinvolga il process owner, le funzioni IT e Security, nonché Legal e Compliance. Il processo può essere articolato in quattro passaggi:

1. analisi del caso d'uso, dei dati trattati e dell'impatto potenziale;
2. valutazione del rischio privacy, sicurezza e compliance;
3. definizione delle misure tecniche e organizzative, inclusa la scelta dei modelli e dei controlli;
4. go-live con monitoraggio rafforzato nelle prime fasi operative.

Questo meccanismo permette di evitare sia approvazioni superficiali sia blocchi immotivati, introducendo una logica di rischio proporzionato.

Copyright © 2026 ICT Consulting S.p.A.

4. POLICY DI UTILIZZO DELL'AI

4.1. STRUMENTI INDIVIDUALI AI E USO CONSAPEVOLE

Ai fini della governance è utile distinguere due macro-categorie di strumenti AI individuali. La prima comprende gli **strumenti personali non autorizzati**, come account gratuiti su chatbot pubblici o applicazioni scaricate autonomamente. La seconda include gli **strumenti autorizzati ma non forniti direttamente dall'azienda**, eventualmente utilizzabili per attività limitate e con regole precise.

Questa classificazione permette di evitare un approccio indifferenziato. Non tutti gli strumenti presentano lo stesso livello di rischio, né possono essere ammessi o vietati con le stesse regole.

La policy aziendale dovrebbe innanzitutto sancire un principio semplice: **i dati aziendali non possono essere inseriti in strumenti AI non autorizzati**. L'uso di tali strumenti può restare consentito per attività generiche, studio, formazione o sperimentazione, a condizione che non vengano impiegati dati reali, informazioni riservate o contenuti riconducibili all'organizzazione.

È consigliabile formalizzare un catalogo articolato in tre insiemi: strumenti **Permessi**, **Condizionati** e **Vietati**. Gli strumenti permessi sono quelli approvati, configurati e, ove opportuno, contrattualizzati dall'azienda. Gli strumenti condizionati possono essere utilizzati solo per specifiche attività non sensibili. Gli strumenti vietati sono invece quelli privi di garanzie minime di sicurezza, riservatezza o conformità.

Particolare attenzione deve essere dedicata ai **contenuti personali e confidenziali**. In linea generale, è opportuno vietare l'inserimento nei prompt di dati personali identificativi, informazioni su clienti o dipendenti, dati finanziari, pricing, strategie commerciali, codice proprietario, documentazione R&D, segreti industriali e contenuti soggetti a NDA, salvo specifiche eccezioni formalmente approvate.

Tali eccezioni devono essere gestite esclusivamente tramite strumenti dotati di adeguate garanzie tecniche e contrattuali, ad esempio in materia di data residency, non utilizzo dei dati per training, logging e segregazione degli ambienti.

Un altro principio imprescindibile è l'**obbligo di verifica umana**. Gli output generati dall'AI non devono mai essere considerati automaticamente corretti o utilizzabili senza revisione. Essi rappresentano un supporto alla decisione e alla produzione, non una fonte autonoma di verità.

Infine, l'assegnazione di strumenti AI aziendali dovrebbe essere subordinata a un percorso minimo di **formazione e consapevolezza**, finalizzato a chiarire policy, rischi, limiti dei modelli e best practice di prompting sicuro.

4.2. STRUMENTI DI PRODUTTIVITÀ AI AZIENDALI

Gli strumenti di produttività AI integrati nelle piattaforme aziendali (es. copilot, cowork) presentano caratteristiche diverse rispetto ai chatbot generalisti. Essi possono essere connessi direttamente a documenti, email, calendari, repository di codice e basi informative interne. Proprio per questo motivo, il loro valore è elevato, ma altrettanto lo è la necessità di controllo.

Il primo requisito di controllo da implementare riguarda la **coerenza dei permessi**. L'AI deve poter accedere soltanto alle informazioni che l'utente è già autorizzato a visualizzare nei sistemi sottostanti. In altri termini, l'introduzione di un assistente AI non deve ampliare i privilegi effettivi, ma rispettare rigorosamente il principio del *least privilege*.

Il secondo elemento di controllo da considerare è la definizione di **use case approvati**. Attività come la bozza di documenti interni, il riassunto di riunioni, la redazione di email, il supporto alla documentazione tecnica o il recupero di informazioni da repository autorizzati possono essere

Copyright © 2026 ICT Consulting S.p.A.

abilitate in modo strutturato. Diversamente, casi d'uso ad alto impatto — ad esempio comunicazioni ufficiali, risposte legali, raccomandazioni cliniche o finanziarie — richiedono processi di validazione dedicati.

Le **linee guida operative** devono chiarire quando sia opportuno utilizzare tali strumenti, come formulare prompt sicuri, come verificare gli output e come gestire il tema delle fonti quando l'AI rielabora materiali preesistenti.

Sul piano del controllo, è necessario prevedere **logging e monitoraggio** delle interazioni, privilegiando la raccolta di metadati utili per audit e sicurezza senza introdurre una conservazione eccessiva di dati personali o particolari. Devono inoltre essere individuati pattern anomali, come picchi di utilizzo, orari inconsueti, tentativi ripetuti di elaborare dati non consentiti o utilizzi incompatibili con il ruolo dell'utente.

Le funzionalità in **anteprima o beta** non dovrebbero essere abilitate automaticamente. La loro attivazione deve essere preceduta da un'analisi di rischio e da una valutazione della loro coerenza con l'architettura di controllo complessiva.

4.3. FUNZIONALITÀ AI NEI SISTEMI ENTERPRISE

Le stesse logiche si applicano alle principali piattaforme enterprise, che stanno incorporando funzionalità AI generative direttamente nei propri moduli applicativi. ERP, CRM, piattaforme di customer service e soluzioni ITSM propongono assistenti, suggerimenti automatici, sintesi di ticket, generazione di insight e automazione di attività operative.

Per governare correttamente questa evoluzione, è necessario partire da una **valutazione centralizzata delle feature AI disponibili**. Ogni funzionalità dovrebbe essere censita, analizzata e classificata per livello di rischio in base ai dati trattati, ai processi supportati e all'impatto potenziale su clienti, dipendenti o decisioni aziendali.

L'attivazione deve avvenire in modo **selettivo per modulo, ruolo e processo**. L'abilitazione indiscriminata di tutte le opzioni offerte dal vendor espone l'impresa a rischi difficili da governare. Le funzionalità dovrebbero essere adottate quando esistono responsabilità chiare di validazione degli output, controlli a valle e una piena compatibilità con le policy aziendali.

Un ulteriore punto cruciale riguarda l'**allineamento contrattuale con i fornitori**. È opportuno ottenere garanzie esplicite sull'uso dei dati per training, sulla localizzazione delle informazioni, sul logging, sulle possibilità di audit e sulla gestione delle vulnerabilità.

Infine, ogni integrazione dovrebbe essere accompagnata da una **mappatura dei flussi di dati verso i modelli**. L'azienda deve sapere quali dati vengono inviati, da quale sistema, verso quale modello, in quale giurisdizione e con quali misure di protezione.

5. AI GATEWAY PER L'ACCESSO A MODELLI E CONTENUTI

Per evitare che ogni strumento o funzionalità AI attivi una propria relazione autonoma con provider LLM diversi e acceda direttamente alle fonti informative aziendali, è consigliabile definire un livello centralizzato di mediazione, un **AI Gateway aziendale**, attraverso cui orchestrare sia l'accesso ai modelli sia l'accesso ai dati.

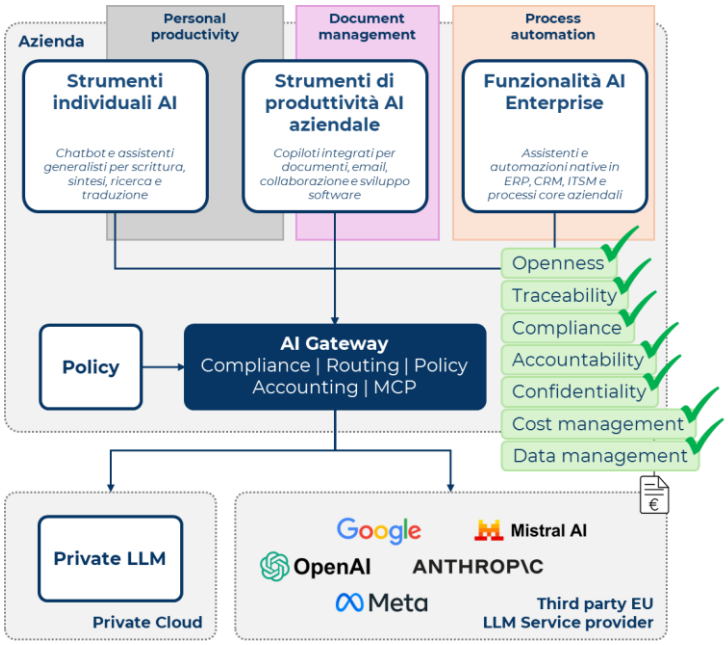
Questa scelta consente di standardizzare API, protocolli, policy di sicurezza, logiche di osservabilità e criteri di autorizzazione verso le fonti dati. Le applicazioni AI possono così invocare modelli e informazioni aziendali attraverso un punto di controllo comune, riducendo le integrazioni dirette non governate, prevenendo accessi disomogenei ai dati e semplificando l'applicazione delle policy.

Copyright © 2026 ICT Consulting S.p.A.

5.1. AI GATEWAY E ROUTING INTELLIGENTE

Il routing intelligente costituisce uno dei pilastri architetturali della governance AI. L'obiettivo non è soltanto instradare una richiesta verso un modello disponibile, ma scegliere in modo dinamico il modello più appropriato in funzione di costo, sensibilità dei dati, performance, disponibilità e requisiti di compliance.

Una richiesta semplice di classificazione o sintesi può essere indirizzata verso un modello più leggero ed economico. Un'elaborazione complessa, ma priva di dati riservati, può essere gestita da un modello cloud generalista più performante. Un'attività basata su dati strategici o altamente confidenziali dovrà invece essere trattata da modelli privati o on premises, nel rispetto delle policy aziendali.



L'AI Gateway, o Orchestrator, rappresenta il componente centrale di questa architettura. Esso espone un set di API interne standardizzate - ad esempio per chat, completamento, embedding, vision o analisi documentale - e applica le regole di instradamento verso una pluralità di modelli:

- modelli pubblici erogati da cloud provider;
- modelli gestiti dall'azienda in cloud privato;
- modelli on premises installati nel data center aziendale;
- modelli specializzati per domini specifici.

Il Gateway deve innanzitutto **classificare le richieste** sulla base di metadati, contesto applicativo, ruolo dell'utente, tipologia di processo e, ove possibile, contenuto analizzato in forma minimizzata o anonimizzata.

Su questa base vengono applicate **regole di routing**. Ad esempio, dati altamente confidenziali possono essere vincolati a modelli interni; richieste non confidenziali ad alta complessità possono essere indirizzate verso provider cloud; compiti seriali a basso valore unitario possono essere affidati a modelli ottimizzati per throughput e costo.

Copyright © 2026 ICT Consulting S.p.A.

Il Gateway deve inoltre incorporare **policy di geolocalizzazione e compliance**, assicurando che determinate tipologie di dati vengano elaborate esclusivamente in aree geografiche o ambienti conformi.

Un'architettura matura include poi funzionalità di **caching, throttling e rate limiting**, utili a contenere i costi, evitare picchi di carico e distribuire equamente le risorse tra business unit e applicazioni.

Infine, il Gateway AI deve garantire **logging e osservabilità**. Per ogni richiesta occorre tracciare il modello utilizzato, i tempi di risposta, i token consumati, gli eventuali blocchi per policy e i costi associati. Queste informazioni sono essenziali sia per il controllo economico sia per il monitoraggio di sicurezza.

5.2. QUANDO ADOTTARE MODELLI ON PREMISES E ARCHITETTURE IBRIDE

La gestione di modelli on premises o in private cloud dedicato può rappresentare una scelta strategica in diversi scenari. Essa è particolarmente indicata quando vengono trattati dati altamente confidenziali, come proprietà intellettuale, informazioni R&D, segreti industriali o basi documentali che non possono essere trasferite verso provider esterni.

L'on premises assume inoltre rilevanza quando il settore o la giurisdizione impongono vincoli stringenti sulla localizzazione dei dati, oppure quando l'impresa desidera un livello elevato di personalizzazione e controllo sui modelli, sui dataset di riferimento e sulle modalità di integrazione.

A volumi elevati e con casi d'uso stabili, tale approccio può anche offrire benefici in termini di prevedibilità dei costi e ottimizzazione della capacità computazionale, pur richiedendo competenze e investimenti infrastrutturali adeguati.

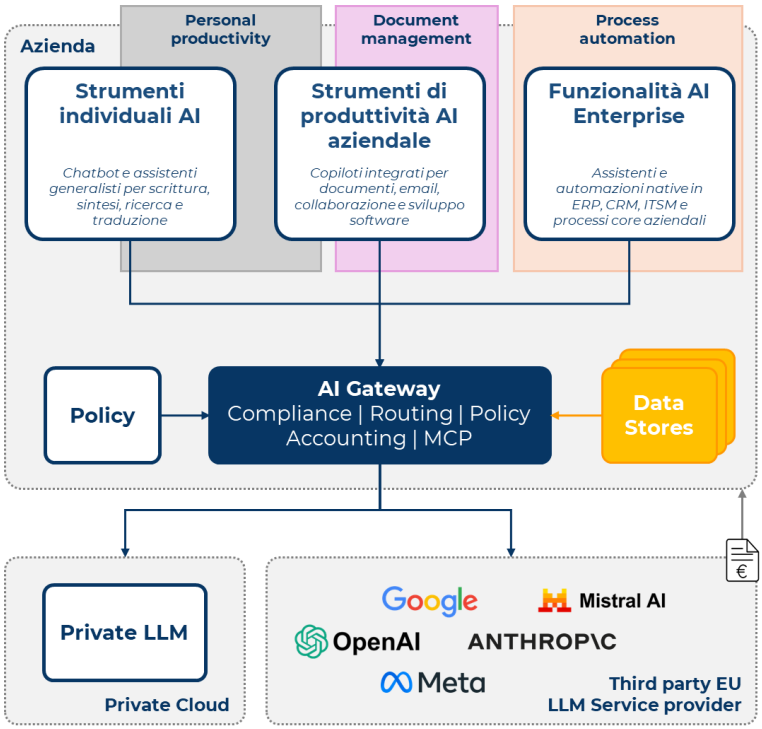
Nella maggior parte dei contesti aziendali, **il modello più equilibrato è di tipo ibrido**. I modelli privati o on premises possono essere riservati ai processi core, alle basi di conoscenza interne e ai dati ad alta confidenzialità. I modelli gestiti da provider esterni possono invece essere utilizzati per compiti generici, attività creative, supporto alla produttività e casi in cui i dati personali/confidenziali siano assenti, anonimizzati o compatibili con le policy definite.

Il valore dell'approccio ibrido risiede nella sua flessibilità. L'azienda non rinuncia alla potenza e all'innovazione dei modelli frontier, ma preserva un presidio forte sui casi d'uso più critici. L'AI Gateway diventa il meccanismo che rende operativo questo bilanciamento.

5.3. AI GATEWAY COME CONTEXT PROVIDER

La **capacità di esporre contenuti aziendali verso strumenti e funzionalità AI rappresenta un'evoluzione naturale dell'AI Gateway**. L'obiettivo non è soltanto governare l'accesso ai modelli, ma rendere disponibile agli strumenti AI un livello comune, controllato e strutturato di conoscenza aziendale. In questo modo, l'AI Gateway non agisce solo come punto di instradamento delle richieste, ma anche come Context Provider, capace di mettere in relazione modelli, dati, documenti, processi e conoscenza di dominio.

Copyright © 2026 ICT Consulting S.p.A.



In un'organizzazione che adotta applicazioni AI, infatti, il valore non deriva esclusivamente dalla disponibilità di modelli linguistici più potenti, ma dalla loro capacità di operare su informazioni affidabili, coerenti con le definizioni aziendali e accessibili nel rispetto delle policy di sicurezza e compliance. Senza un livello comune di contesto, ogni applicazione AI rischia di costruire una propria rappresentazione dell'impresa, con duplicazioni, incoerenze e integrazioni difficili da governare.

Il primo elemento di questa architettura è rappresentato dal **GraphRAG**. Rispetto a un approccio RAG tradizionale, basato prevalentemente sul recupero di porzioni di testo da basi documentali, il GraphRAG introduce un livello semantico fondato su entità, relazioni, attributi, gerarchie, processi, owner e metadati. Clienti, contratti, prodotti, asset, applicazioni, ticket, policy, unità organizzative, fornitori e KPI possono essere modellati come nodi e relazioni di un grafo, creando progressivamente un **digital twin dei dati aziendali** o, in una prima fase, delle aree informative più rilevanti.

Tale digital twin non deve essere interpretato come una replica indiscriminata di tutti i dati presenti nei sistemi aziendali. Al contrario, deve costituire un livello governato, alimentato da fonti certificate e arricchito con informazioni di lineage, classificazione del dato, ownership, qualità, freshness e regole di visibilità. Il grafo può contenere direttamente alcune informazioni, ma soprattutto deve descrivere il significato dei dati, le relazioni tra domini informativi e i percorsi autorizzati per raggiungere le fonti master quando sia necessario accedere al dato aggiornato.

In questo modello, l'AI Gateway svolge una funzione di mediazione tra strumenti AI e sistemi aziendali. Un assistente AI non dovrebbe interrogare direttamente ERP, CRM, data warehouse o piattaforme documentali con logiche proprietarie e non coordinate. Dovrebbe invece invocare servizi standard esposti dall'AI Gateway, che applicano le policy, verificano le autorizzazioni, selezionano le fonti corrette, tracciano l'accesso e restituiscono un contesto coerente con il ruolo dell'utente e con il caso d'uso.

Il **Model Context Protocol** (MCP) rappresenta il meccanismo attraverso cui esporre in modo standardizzato i tool utilizzabili dagli strumenti AI per accedere ai contenuti aziendali. Tramite MCP, l'azienda può pubblicare un catalogo controllato di capability, ad esempio ricerca nel grafo, recupero

Copyright © 2026 ICT Consulting S.p.A.

di documenti certificati, interrogazione di entità e relazioni, accesso a metriche, consultazione di knowledge base autorizzate, esecuzione di query text-to-SQL verso data platform o chiamate text-to-API verso sistemi applicativi. Ogni tool deve essere descritto, versionato, autorizzato e osservabile.

È utile distinguere due categorie principali di tool:

- tool di accesso al grafo e al contesto, che permettono agli strumenti AI di comprendere documenti, definizioni, relazioni, vincoli, ownership e fonti ufficiali;
- tool di accesso ai sistemi master, che consentono di recuperare dati aggiornati attraverso interfacce governate.

I primi riducono ambiguità e allucinazioni legate alla mancanza di contesto; i secondi evitano copie incontrollate dei dati e mantengono il principio secondo cui il dato operativo resta nel sistema che ne detiene la responsabilità.

Questo approccio consente di ridurre la frammentazione architetturale e, allo stesso tempo, di abilitare l'innovazione distribuita. L'IT mantiene la responsabilità di costruire e governare il contesto, i tool e le regole di sicurezza; le funzioni di business possono invece utilizzare strumenti AI per sviluppare automazioni, analizzare dati, supportare decisioni e creare nuove funzionalità senza dover implementare ogni volta le integrazioni di base.

5.4. AI CAPABILITY FACTORY: INDUSTRIALIZZARE IL TRASFERIMENTO DELLA CONOSCENZA

Parallelamente all'introduzione dell'AI Gateway, è opportuno definire un modello industriale per la trasformazione della conoscenza aziendale in capacità operative AI. Questo modello può essere descritto come **AI Capability Factory**, ossia una catena governata di attività attraverso cui la conoscenza dell'organizzazione viene resa utilizzabile in forma di prompt, strumenti, memoria, agenti e workflow AI-driven.

In questo disegno, l'AI Gateway governa l'accesso ai modelli e l'applicazione delle policy; l'AI Capability Factory governa la produzione, il test e la pubblicazione delle capacità AI che sfruttano tali modelli. L'AI Capability Factory si articola in quattro componenti principali, tra loro complementari:

Prompt factory

La prompt factory è il processo governato attraverso cui la conoscenza operativa, spesso distribuita tra procedure, documenti, prassi informali ed esperienza delle persone, viene trasformata in **pacchetti AI riutilizzabili**: istruzioni, esempi, fonti informative, criteri di valutazione, schemi di output, strumenti autorizzati e regole di validazione.

Il prodotto non è un singolo prompt informale, ma un **pacchetto operativo governato**, versionato, approvato, validato e monitorato nel tempo, che rende visibile e comprensibile il passaggio dalla conoscenza umana al comportamento del sistema AI.

Knowledge engineering

Il knowledge engineering comprende attività di classificazione, estrazione, normalizzazione, distillazione semantica e costruzione di tassonomie e grafi della conoscenza, finalizzate a trasformare le informazioni disponibili in **conoscenza esplicita** governata.

In questo contesto, documenti e basi informative non vengono trattati come semplici insiemi di frammenti testuali, ma come oggetti arricchiti con metadati, entità, relazioni, validità temporale, provenienza e livello di autorevolezza. Il principio architetturale di riferimento è: "*ciò che è noto deve essere rappresentato come conoscenza; ciò che non è noto può essere demandato all'inferenza*".

Copyright © 2026 ICT Consulting S.p.A.

Memory and inference layer

Il memory and inference layer è dedicato alla **memoria incrementale** di eventi, evidenze, inferenze e decisioni, con confronto tra lo stato precedente e i nuovi ingressi. La memoria viene modellata come insieme di oggetti distinti (episodica, semantica, procedurale, memoria degli esiti, memoria delle evidenze), ciascuno accompagnato da metadati quali provenienza, modello utilizzato, versione delle istruzioni, data di produzione, livello di confidenza, ambito di validità e condizioni di obsolescenza.

In questo modo il sistema può elaborare il **differenziale informativo**, riusando le inferenze pregresse senza trasformarle in fatti incontestabili, e conservando la distinzione tra:

- dato proveniente da una fonte autorevole;
- informazione estratta da un documento;
- inferenza prodotta dal sistema;
- decisione approvata da una persona;
- ipotesi ancora da verificare.

La memoria diviene così non soltanto uno strumento di efficienza, ma un elemento di tracciabilità e responsabilizzazione del sistema AI.

Cooperazione tra agenti

La cooperazione tra agenti riguarda la predisposizione di ambienti controllati per la collaborazione tra agenti specializzati, ad esempio incaricati di pianificazione dell'attività, ricerca e raccolta delle evidenze, analisi normativa, elaborazione quantitativa, esecuzione di operazioni sui sistemi, verifica della qualità, controllo delle autorizzazioni, approvazione o gestione delle eccezioni.

La cooperazione non viene lasciata a conversazioni libere e non governate tra modelli, ma avviene all'interno di un perimetro che definisce:

- identità e responsabilità di ciascun agente;
- capacità dichiarate;
- formati dei messaggi e degli artefatti scambiati;
- criteri di assegnazione e accettazione dei compiti;
- limiti di delega;
- autorizzazioni sui dati e sugli strumenti;
- timeout, gestione degli errori e compensazione delle operazioni;
- conservazione delle evidenze;
- responsabilità dell'approvazione finale;
- punti nei quali è obbligatorio l'intervento umano.

La **prompt factory** rappresenta il punto di ingresso più semplice e spesso più efficace, purché non venga presentata come "fabbrica di prompt" fine a sé stessa, bensì come **fabbrica di capacità AI**, nella quale il prompt è soltanto la prima forma, comprensibile e gestibile, di codificazione della conoscenza operativa, destinata a evolvere verso componenti più strutturate quali strumenti, agenti e workflow governati.

L'AI Gateway rappresenta il punto di applicazione operativa delle policy aziendali sull'AI, mentre la AI Capability Factory rappresenta il sistema industriale di produzione delle capacità

Copyright © 2026 ICT Consulting S.p.A.

AI che il Gateway governa. MCP e A2A operano come livelli di interoperabilità: MCP standardizza l'accesso a risorse, strumenti e prompt; A2A abilita la cooperazione tra agenti autonomi o organizzativamente distinti.

Insieme, questi componenti consentono di applicare due principi fondamentali:

- nessun consumo AI senza identità, finalità, policy, attribuzione economica e misurazione del risultato;
- nessuna capacità AI senza un processo governato di trasformazione della conoscenza aziendale.

6. SICUREZZA, COMPLIANCE E CONTROLLI TECNICI

6.1. PRIVACY, PROPRIETÀ INTELLETTUALE E REQUISITI REGOLAMENTARI

Le soluzioni AI devono essere progettate secondo i principi di **privacy by design** e **privacy by default**. Ciò implica minimizzazione dei dati, limitazione delle finalità, riduzione dei tempi di conservazione e ricorso a tecniche di pseudonimizzazione o anonimizzazione quando applicabili.

Per i casi d'uso che coinvolgono dati personali o producono impatti significativi sulle persone, è necessario valutare l'aggiornamento delle informative privacy, l'adeguamento dei registri dei trattamenti e, ove richiesto, l'esecuzione di una Data Protection Impact Assessment.

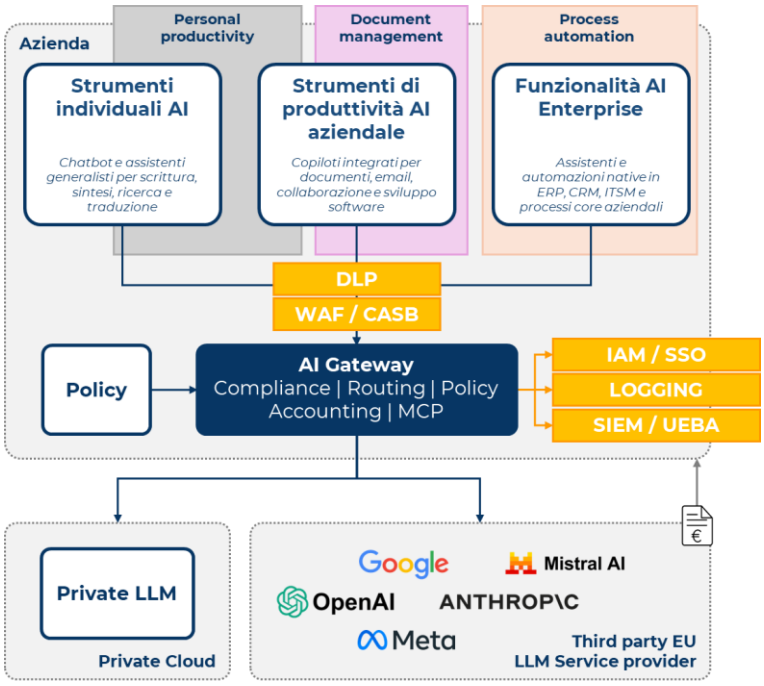
L'introduzione dell'AI pone inoltre domande specifiche in materia di proprietà degli output, uso di contenuti protetti da copyright e impiego di materiali generati in prodotti o servizi destinati ai clienti. La policy aziendale dovrebbe chiarire in quali circostanze gli output AI possano essere utilizzati, con quali verifiche e con quali responsabilità. Dovrebbero inoltre essere valutate le garanzie offerte dai provider rispetto ai dataset di training, alle clausole di indennizzo e ai rischi di riproduzione non autorizzata di contenuti protetti.

Nei settori finanziario, sanitario, energetico, nella pubblica amministrazione e in altri contesti ad alta regolazione, la governance AI deve integrarsi con requisiti specifici. Tra questi possono rientrare obblighi di explainability, audit trail, validazione dei modelli, tracciabilità delle decisioni, segregazione dei ruoli e certificazione dei processi.

6.2. INTEGRAZIONE CON I CONTROLLI DI CYBERSECURITY ESISTENTI

Per rendere effettive le policy di governance AI, è necessario tradurle in controlli tecnici concreti. Le organizzazioni dispongono già di strumenti consolidati in ambito cybersecurity e produttività: Identity & Access Management (IAM), Single Sign On (SSO), Role-Based Access Control (RBAC), Data Loss Prevention (DLP), proxy, Cloud Access Security Broker (CASB), Web Application Firewall (WAF), Security Information and Event Management (SIEM), User and Entity Behavior Analytics (UEBA), sistemi di logging e policy su email e file sharing.

Copyright © 2026 ICT Consulting S.p.A.



L'introduzione dell'AI non dovrebbe creare un ecosistema parallelo, ma estendere e valorizzare tali controlli. L'obiettivo è applicare misure restrittive coerenti con il rischio, garantire accountability e mantenere un'esperienza utente sostenibile.

Identità, ruoli e IAM: chi può usare cosa, dove e come

Un primo ambito di intervento riguarda l'estensione dei ruoli esistenti all'AI. È utile definire profili come *AI Basic User*, *AI Power User*, *AI Developer / Integrator* e *AI Admin / Governance*, collegandoli sia all'AI Gateway sia alle funzionalità AI attivate nei sistemi enterprise.

L'accesso ai servizi AI dovrebbe avvenire esclusivamente tramite identità aziendale, con Single Sign-On e autenticazione forte. L'uso di account personali o anonimi per attività aziendali deve essere escluso, perché impedisce tracciabilità e controllo.

Particolare attenzione va posta alla **segregazione dei privilegi**. L'AI non deve consentire ad un utente di accedere indirettamente a contenuti che non potrebbe consultare direttamente. Ciò è particolarmente rilevante per strumenti integrati con repository documentali, piattaforme collaborative e knowledge base interne.

DLP e protezione dei dati: cosa può essere inviato ai modelli

Le soluzioni di Data Loss Prevention possono essere estese al traffico verso servizi AI, con l'obiettivo di rilevare e bloccare l'invio di informazioni vietate. I controlli possono riguardare chatbot pubblici, endpoint API/MCP, strumenti AI integrati in SaaS e interfacce web dedicate.

L'estensione verso servizi AI deve però prevedere un aggiornamento tecnologico delle soluzioni di DLP tradizionali, principalmente basate sulla capacità di monitorare e controllare attività come il trasferimento di file, l'invio di allegati e-mail, il traffico di rete mediante l'identificazione di pattern di dati strutturati. I rischi legati alla perdita di confidenzialità in contesti AI, infatti, non si manifestano più soltanto nei canali classici, ma emergono in contesti dinamici come i prompt utente inseriti direttamente nei browser (es. copia-incolla massivo da documenti classificati) o le chiamate verso endpoint API/MCP. Inoltre, il riconoscimento dell'evento avverso deve evolvere da una comprensione sintattica del dato verso una comprensione semantica del contenuto scambiato

Copyright © 2026 ICT Consulting S.p.A.

dall'utente. I nuovi sistemi DLP AI-ready devono quindi poter operare in ambienti distribuiti (sistemi enterprise, MCP server ed end-point mediante plugin) e affiancare gli strumenti di rilevamento tradizionale con nuovi meccanismi di rilevamento dinamici basati sul contesto d'uso.

Le policy da implementare in questi nuovi sistemi DLP possono prevedere alert o blocchi in presenza di dati personali particolari, informazioni classificate come confidenziali, segreti aziendali o pattern riconducibili a dati regolamentati. Quando tecnicamente sostenibile, possono essere adottati meccanismi di mascheramento o sostituzione dei dati prima dell'invio.

Un'integrazione matura tra sistemi di classificazione documentale e AI Gateway consente inoltre di applicare policy dinamiche: un documento etichettato come *Restricted* può essere inviato solo a modelli interni o on premises, mentre un contenuto *Public* può essere elaborato anche da modelli esterni, se conforme alle regole aziendali.

Firewall applicativi, proxy e CASB: controllo degli endpoint AI

Proxy, web gateway e CASB possono essere utilizzati per mappare e categorizzare i servizi AI disponibili, distinguendo tra strumenti autorizzati, condizionati e vietati. Questa classificazione consente di bloccare l'accesso a chatbot non approvati, consentire l'uso solo tramite domini aziendali dedicati o applicare controlli differenziati per categoria di utente.

Davanti all'AI Gateway è opportuno posizionare un Web Application Firewall, utile a proteggere le API da abusi, attacchi applicativi, fuzzing e tentativi di manipolazione. Il WAF può inoltre supportare politiche di rate limiting e mitigazione di attacchi di tipo Denial of Service.

Nel contesto dei sistemi agentici e delle catene di orchestrazione, questo livello di difesa diventa ancora più importante, poiché occorre presidiare il rischio di prompt injection e richieste malevole finalizzate a deviare il comportamento degli agenti.

Estensione delle policy già applicate agli strumenti di produttività

Un approccio efficace consiste inoltre nel riutilizzare, per l'AI, concetti già consolidati nella sicurezza degli strumenti di produttività. Le regole applicate alle email possono essere tradotte nel principio secondo cui inviare dati a un sistema AI esterno equivale, in molti casi, a trasferire informazioni fuori dal perimetro aziendale.

Analogamente, le policy sulla condivisione file, sui link pubblici e sulla classificazione documentale possono essere estese alla possibilità di caricare documenti in un sistema AI, utilizzarli per indicizzazione o impiegarli in processi di fine-tuning.

Una regola operativa semplice può prevedere che documenti *Public* o *Internal* siano utilizzabili, entro certi limiti, in ambienti AI controllati, mentre documenti *Confidential* o *Restricted* siano trattabili soltanto tramite AI interna o modelli privati, con logging e protezioni rafforzate.

Per gli assistenti integrati nelle suite office, è importante allineare le label di sensibilità affinché l'AI non favorisca, anche involontariamente, la condivisione o la sintesi di contenuti altamente riservati verso canali non autorizzati.

Logging, audit e accountability

Ogni interazione con modelli AI, soprattutto quando mediata da un Gateway aziendale, dovrebbe generare log strutturati contenenti almeno: identità dell'utente, ruolo, applicazione sorgente, modello invocato, volume di token, classificazione del dato, tool di accesso ai dati utilizzati, esito della richiesta e decisione di routing.

Il contenuto dei prompt e degli output va invece gestito con prudenza. In via generale è preferibile registrare soltanto metadati. Nei casi ad alto rischio o in specifici contesti regolamentati, la

Copyright © 2026 ICT Consulting S.p.A.

conservazione dei contenuti può essere valutata in forma pseudonimizzata e su repository altamente protetti.

L'integrazione dei log nel SIEM permette di rilevare pattern anomali, quali utilizzi massivi, accessi fuori orario, ripetuti tentativi di trasmettere dati vietati o comportamenti incoerenti con il profilo dell'utente. Le soluzioni UEBA possono rafforzare ulteriormente questa capacità, evidenziando scostamenti rispetto ai comportamenti ordinari.

La disponibilità di audit trail affidabili è infine essenziale per indagini interne, verifiche ispettive, gestione degli incidenti e dimostrazione della due diligence nei confronti di clienti e autorità.

6.3. BILANCIARE CONTROLLO E USABILITÀ

La governance AI deve evitare due estremi ugualmente problematici. Un approccio basato unicamente su divieti e blocchi favorisce la nascita di pratiche non autorizzate. Un approccio permissivo e non presidiato, invece, espone l'azienda a rischi difficilmente sostenibili.

Le misure tecniche e organizzative devono quindi essere proporzionate: più rigorose per dati e processi critici, più leggere per attività generiche e a basso impatto. Devono inoltre essere trasparenti e comprensibili, accompagnate da formazione e dalla disponibilità di strumenti aziendali ufficiali sufficientemente efficaci da rappresentare una reale alternativa alle soluzioni pubbliche non governate.

7. MODELLO ECONOMICO E CONTROLLO DEI CONSUMI

7.1. MISURAZIONE PER STRUTTURA ORGANIZZATIVA, PROFILO UTENTE E GRUPPO DI LAVORO

La sostenibilità economica dell'AI richiede un sistema di misurazione puntuale dei consumi. Token, chiamate API, tempi di calcolo e licenze non devono essere considerati un costo indistinto, ma risorse da tracciare e governare.

Ogni richiesta gestita dall'AI Gateway dovrebbe includere un insieme minimo di metadati: applicazione sorgente, business unit, centro di costo, gruppo di lavoro, progetto e tipologia di utilizzo. Questa tassonomia consente di correlare i consumi ai contesti organizzativi e di analizzare non soltanto quanto viene speso, ma dove e perché.

Le **dashboard di consumo** devono fornire viste differenziate: volumi di richieste, token elaborati per modello, costo per funzione, trend temporali, tassi di errore, livelli di saturazione e principali casi d'uso.

Sulla base di tali informazioni, l'azienda può adottare modelli di **showback** o **chargeback**. Nel primo caso, le strutture vedono i consumi ma il costo resta centralizzato. Nel secondo, parte dei costi viene ribaltata sui centri di responsabilità, creando incentivi più diretti alla razionalizzazione.

È inoltre opportuno introdurre **quote, soglie e alert**, differenziati per ruolo, applicazione e struttura. Limiti giornalieri o mensili, notifiche di superamento soglia e politiche di priorità consentono di prevenire abusi e gestire le risorse nei momenti di maggiore domanda.

7.2. USO CONTROLLATO E CONDIVISO DELLE RISORSE

La governance economica non deve essere interpretata solo in chiave restrittiva. L'obiettivo non è scoraggiare l'uso dell'AI, ma orientarlo verso impieghi di maggiore valore.

Copyright © 2026 ICT Consulting S.p.A.

Per questo motivo, è consigliabile introdurre una governance dei progetti AI che valuti il rapporto tra beneficio atteso e consumo previsto di risorse. I processi critici e ad alto impatto possono ricevere priorità, mentre iniziative sperimentali o a basso valore possono essere soggette a limiti più stringenti.

La diffusione di best practice operative - prompt più efficaci, riuso dei risultati, gestione batch, scelta del modello proporzionata al compito, distillazione della conoscenza - contribuisce inoltre a ridurre sprechi e a migliorare la qualità complessiva dell'adozione.

8. ROADMAP DI IMPLEMENTAZIONE

8.1. AI GOVERNANCE

Fase 1 – Assessment, policy e baseline dei controlli

La prima fase consiste nel costruire una fotografia affidabile dello stato di partenza. Occorre censire gli strumenti AI già in uso, inclusi quelli adottati informalmente dai dipendenti, identificare i sistemi enterprise dotati di funzionalità AI e valutare i principali gap di governance.

In parallelo, vanno definite le prime policy aziendali, distinguendo tra strumenti individuali, soluzioni gestite e casi d'uso ammessi o vietati. È in questa fase che dovrebbe essere istituito l'AI Governance Board.

Lo stesso assessment deve riguardare i controlli già presenti in azienda: sistemi IAM e RBAC, soluzioni DLP, proxy, CASB, WAF, SIEM, regole di sicurezza su email e file sharing. L'obiettivo è individuare i gap rispetto all'uso dell'AI in termini di: domini non coperti, ruoli non definiti, assenza di tagging dei dati o impossibilità di tracciare i consumi in modo coerente.

L'assessment dovrebbe inoltre mappare le principali fonti informative aziendali: sistemi master, data platform, repository documentali, cataloghi dati, knowledge base, CMDB, workflow applicativi e ownership dei domini informativi. Questa mappatura è il prerequisito per definire quali porzioni del digital twin siano prioritarie e quali dati possano essere esposti agli strumenti AI attraverso l'AI Gateway.

Fase 2 – Architettura target, AI Gateway e sicurezza

La seconda fase riguarda la progettazione dell'AI Gateway con integrazione IAM, Single Sign-On, ruoli AI-specifici e enforcement delle regole di routing. Occorre definire le classi di dati, i criteri di instradamento, i modelli utilizzabili per ciascun livello di sensibilità e i requisiti di logging.

Contestualmente, devono essere aggiornate le regole DLP per includere il traffico verso LLM, configurati proxy e CASB per governare i domini AI e posizionato un WAF davanti al Gateway. È inoltre opportuno avviare le prime integrazioni con le piattaforme prioritarie e strutturare le dashboard di monitoraggio dei consumi e delle performance.

Nella stessa fase deve essere progettata la componente di Context Gateway: modello dati del knowledge graph, criteri di alimentazione GraphRAG, fonti certificate, regole di freshness, catalogo iniziale dei tool MCP e pattern di accesso ai sistemi master. È opportuno partire da domini informativi ad alto valore e perimetro controllabile, evitando un'iniziativa eccessivamente ampia che replichi indiscriminatamente l'intero patrimonio dati aziendale.

Fase 3 – Roll out, logging e accountability

Copyright © 2026 ICT Consulting S.p.A.

La terza fase prevede il roll out progressivo degli strumenti AI di produttività e dei primi casi d'uso in produzione. L'estensione degli accessi deve essere accompagnata da formazione obbligatoria, linee guida operative e supporto agli utenti.

In questa fase occorre abilitare il logging centralizzato delle chiamate AI e integrarlo con SIEM e strumenti UEBA. Devono essere realizzate dashboard distinte per finalità di sicurezza, governance e controllo economico. Le prime permetteranno di monitorare anomalie e tentativi di uso improprio; le seconde consentiranno di analizzare consumi per unità organizzativa, modello e caso d'uso.

Il roll out dovrebbe includere anche i primi casi d'uso basati su contesto condiviso, ad esempio assistenti per knowledge management, interrogazione controllata di dati commerciali o operativi, supporto al service desk e analisi documentale su fonti certificate. Questi casi d'uso consentono di validare il modello GraphRAG, il catalogo MCP e le regole di autorizzazione prima di estenderli a domini più critici.

Fase 4 – Ottimizzazione e miglioramento continuo

La quarta fase riguarda la maturazione del modello. Le policy devono essere aggiornate periodicamente in base all'evoluzione tecnologica e normativa. Le regole di routing vanno ottimizzate, i costi ridotti attraverso l'uso di modelli più efficienti e, dove necessario, può essere introdotta una componente on premises.

Contestualmente, l'impresa deve misurare il valore generato e adattare i meccanismi di priorità, chargeback e allocazione delle risorse. Policy di sicurezza, quote di consumo, controlli DLP, configurazioni firewall, modello dati GraphRAG e catalogo MCP dovranno essere riesaminati in modo continuativo, alla luce dell'evoluzione dei casi d'uso e delle minacce.

8.2. EVOLUZIONE VERSO AI CAPABILITY FACTORY

La roadmap di AI Governance può essere estesa introducendo un percorso di maturità specifico per l'AI Capability Factory, articolato in sei fasi. Questo percorso si integra con le fasi già previste (assessment, definizione dell'AI Gateway, roll-out, ottimizzazione), aggiungendo una **dimensione esplicita di industrializzazione della conoscenza e delle capacità AI**.

Fase 1 – Formalizzazione

Costruire un catalogo governato di casi d'uso, istruzioni, esempi, fonti e criteri di accettazione. In questa fase si rende esplicita la conoscenza degli esperti di dominio e si introduce una disciplina di valutazione della qualità e della stabilità degli output.

Fase 2 – Contestualizzazione

Collegare i pacchetti operativi alle fonti aziendali attraverso RAG, query strutturate e strumenti. L'utilizzo del Model Context Protocol (MCP) consente di ridurre la proliferazione di connettori proprietari verso document repository, knowledge graph, motori di ricerca e database, standardizzando l'accesso alle risorse e ai tool.

Fase 3 – Conoscenza strutturata

Arricchire documenti e fonti con metadati, entità, relazioni, validità temporale e provenance, distinguendo chiaramente dati master, documenti approvati, contenuti informali e informazioni obsolete. La RAG diventa così ibrida e knowledge-aware, combinando ricerca vettoriale, ricerca

Copyright © 2026 ICT Consulting S.p.A.

lessicale, filtri sui metadati, interrogazione di dati strutturati, grafi della conoscenza e regole di priorità delle fonti.

Fase 4 – Memoria incrementale

Introdurre meccanismi di riuso controllato delle inferenze pregresse, con elaborazione del solo differenziale informativo rispetto allo stato conoscitivo consolidato. Ogni inferenza viene memorizzata con metadati di provenienza, modello utilizzato, versione delle istruzioni, data di produzione, livello di confidenza, ambito di validità e condizioni di obsolescenza, preservando la distinzione tra dato, informazione estratta, inferenza, decisione e ipotesi.

Fase 5 – Agentificazione

Trasformare i pacchetti operativi più maturi in agenti specializzati, con strumenti autorizzati, obiettivi, limiti e responsabilità definiti. Gli agenti operano entro il perimetro di policy stabilito dall'AI Gateway, utilizzando tool esposti tramite MCP e accedendo alla memoria e alla conoscenza strutturata nel rispetto delle autorizzazioni e delle regole di sicurezza.

Fase 6 – Cooperazione

Consentire agli agenti di collaborare in ambienti controllati, eventualmente attraverso protocolli A2A per la delega e il coordinamento tra agenti appartenenti a piattaforme differenti. L'orchestrazione aziendale, l'audit end-to-end e i punti di controllo umano garantiscono che la distribuzione del lavoro tra agenti rimanga tracciabile, governata e coerente con le policy sull'AI.

9. CONCLUSIONI

L'adozione dell'Intelligenza Artificiale in azienda richiede un'integrazione stretta tra governance, architettura, controllo economico e cybersecurity. Non è sufficiente redigere policy formali: occorre renderle operative attraverso strumenti, processi e responsabilità chiare. La gestione della conoscenza che costituisce un patrimonio aziendale da valorizzare con i nuovi strumenti è un tassello chiave della trasformazione AI driven dei processi aziendali e deve essere guidata da una precisa strategia determinata e messa in opera dall'azienda.

Un modello efficace consente di controllare chi utilizza quali servizi AI, con quali dati e per quali scopi; prevenire fughe informative e violazioni normative; garantire accountability e tracciabilità; ottimizzare token, modelli, licenze e costi; e offrire agli utenti strumenti affidabili e ottimizzati per le loro funzioni aziendali, riducendo il ricorso a soluzioni non autorizzate.

La governance dell'AI non deve essere vista come un freno all'innovazione, ma come la condizione necessaria per portarla su scala in modo sicuro, conforme e sostenibile. Le aziende che sapranno costruire questo equilibrio saranno in grado di trasformare l'AI da fenomeno fuori controllo e frammentato a leva strutturale di competitività.

Copyright © 2026 ICT Consulting S.p.A.

DIRITTO D'AUTORE E PROPRIETÀ INTELLETTUALE

Copyright © 2026 ICT Consulting S.p.A. Tutti i diritti sono riservati.

Tutti i contenuti del presente documento, il relativo diritto d'autore e ogni altro diritto di proprietà intellettuale appartengono a ICT Consulting S.p.A. Nessuna parte del documento può essere riprodotta o trasmessa, in tutto o in parte, a persone fisiche o giuridiche senza il permesso scritto di ICT Consulting S.p.A. I contenuti del documento non possono essere altresì copiati, donati o venduti a terze parti senza il permesso scritto di ICT Consulting S.p.A.

ICT Consulting S.p.A. non si assume alcuna responsabilità per l'utilizzo del materiale contenuto nel presente documento.

GLI AUTORI

Vittorio Trecordi

Fondatore, Partner, COO e Presidente ICT Consulting

Laureato con Lode al Politecnico di Milano nel 1986, ha conseguito il Master in Information Technology presso CEFRIEL/Politecnico di Milano nel 1988.

Dopo un breve trascorso in Laben e Pirelli Cavi, diventa direttore tecnico del CEFRIEL/Politecnico di Milano, dove si occupa di ricerca applicata.

Nel 1998 fonda ICT Consulting insieme all'Ing. Salvatore Randi ed al Prof. Maurizio Decina.

Nel 2013-14 ha preso parte ai lavori del Commissario Straordinario nominato dal Presidente del Consiglio finalizzati alla redazione del Rapporto sulla Banda Larga. Successivamente, ha contribuito alla redazione della "Strategia Italiana per la Banda Ultra Larga".

È membro del Comitato Scientifico della Fondazione Ugo Bordoni, della Communications Society dell'IEEE e dal 1993 è Docente a Contratto presso il Politecnico di Milano, ove attualmente insegna "Communications Networks for Electricity Systems".

Negli anni ha sviluppato una profonda esperienza nel settore delle tecnologie digitali applicate ai diversi settori del mercato e della società, guidando numerosi progetti di grande impatto per primarie aziende nazionali ed estere.

Alessandro Soracco

Partner ICT Consulting, CEO AI4More

Laureato a pieni voti in Ingegneria delle Telecomunicazioni al Politecnico di Milano, lavora in ICT Consulting da più di 20 anni.

Esperto in bandi di gara e outsourcing di servizi ICT, ha contribuito a raggiungere importanti obiettivi di riduzione della spesa ICT per numerosi clienti. Profondo conoscitore dei processi di IT Service Management, dei processi di business degli operatori e delle architetture applicative a supporto, ha gestito con successo complessi progetti IT Transformation presso operatori nazionali e internazionali.

Socio di ICT Consulting dal 2008, è correlatore presso il Politecnico di Milano di numerose tesi. Dal 2025, Alessandro Soracco è CEO di AI4More, società specializzata nello sviluppo di soluzioni di Intelligenza Artificiale per le imprese, dove si occupa di rendere la conoscenza aziendale accessibile, sicura e utilizzabile attraverso workspace AI, sistemi di knowledge management e agenti intelligenti governati.

ICT CONSULTING

ICT CONSULTING è una società di consulenza tecnologica e strategica focalizzata sul mercato delle Telecomunicazioni.

Fondata nel 1998 da professionisti appartenenti a tre generazioni di Ingegneri delle Telecomunicazioni, la società ha continuato a crescere e svilupparsi.

Da oltre vent'anni affianca imprese e istituzioni nella definizione di strategie, architetture e modelli operativi per affrontare trasformazioni tecnologiche complesse, coniugando competenze tecniche, visione strategica e conoscenza dei contesti regolamentari.

Le attività di ICT Consulting comprendono l'analisi dei mercati e degli scenari tecnologici, la progettazione di infrastrutture e piattaforme digitali, la definizione di framework di sicurezza, il supporto alla trasformazione dei processi aziendali e il governo di programmi complessi.

Nell'ambito dell'Intelligenza Artificiale, ICT Consulting supporta le organizzazioni nella definizione di modelli di governance, policy di utilizzo, architetture di accesso ai modelli e ai dati, sistemi di controllo dei costi e percorsi di adozione sicuri, conformi e sostenibili.

L'approccio della società integra dimensioni organizzative, tecnologiche, economiche e di sicurezza, con l'obiettivo di trasformare l'innovazione in capacità operative concrete e governate.

Contatti

ICT Consulting

Piazzale L. Cadorna 4, 20123 Milano, Italy

Tel. +39-02-6764221

Fax +39-02-67642243

email: ictc@ictc.it