



Introduzione dell'intelligenza artificiale nei processi aziendali

Costi, autorizzazioni, agenti autonomi, sicurezza e norme: i temi da discutere prima di portare l'intelligenza artificiale nei processi aziendali.

io Digitale Srl · Focus · 17 settembre 2026

Versione online: <https://iodigitale.it/focus/ai-nei-processi-aziendali>

In sintesi

L'intelligenza artificiale può portare benefici concreti, ma oggi il suo uso in azienda nasce spesso in modo spontaneo: costi non prevedibili, attività non autorizzate, personale senza competenze informatiche, sistemi di sicurezza non pensati per un software che agisce da solo.

Proponiamo di **stabilire regole e fare un censimento prima di proseguire**, e di adottare **applicazioni ibride**: software tradizionale che governa il processo e usa l'intelligenza artificiale solo dove serve davvero.

1. Governo, costi e autorizzazioni

- **Costi incerti.** L'uso non è stimabile in anticipo, e i listini dei fornitori non sono né negoziabili né stabili. Servono un budget, soglie di allarme e limiti di spesa.
- **Autorizzazione preventiva** di ogni attività che impegni risorse, valutandone il beneficio economico, gli aspetti etici, la sicurezza e la conformità alle norme.
- **Pianificazione e misurazione.** Risorse informatiche, licenze e tempo del personale vanno pianificati. I benefici vanno misurati con indicatori concreti, non con impressioni.
- **Dipendenza dai fornitori.** Continuità del servizio e costi non sono garantiti. Serve sempre una strategia di uscita, cioè un modo già previsto per cambiare fornitore o farne a meno.

2. I rischi degli agenti AI autonomi

Un **agente** è un programma basato su un modello di intelligenza artificiale a cui si concede di agire da solo: non si limita a rispondere a una domanda, ma legge e modifica file, interroga database, invia messaggi. È qui che i rischi cambiano natura.

- **Accesso diretto a dati e sistemi** da parte di personale senza preparazione informatica, attraverso gli agenti.
- **Le regole date all'agente non sono vincolanti.** Le istruzioni vengono interpretate, non eseguite come ordini: allo stato attuale non si possono imporre regole stringenti.

- **Comportamenti inventati, distruttivi o ingannevoli**, difficili da riconoscere per chi non è «del mestiere».

[ERRORE]

Casi reali

- Richiesta di preventivi con prezzi più bassi: l'intelligenza artificiale li ha prodotti e, per renderli coerenti, ha abbassato di propria iniziativa anche i preventivi emessi in precedenza.
- Una pulizia degli archivi solo ipotizzata, ed eseguita senza chiedere conferma.
- Dati statistici ricavati da materiali eterogenei per approssimazione, senza calcoli verificati matematicamente.

3. Fattore umano e immagine aziendale

- **La fase di «innamoramento»**. L'operatore non vede più difetti e limiti dello strumento, e rischia di perdere competenze delegando invece di capire.
- **Comunicazioni uniformate nello stile**. I testi scritti con l'intelligenza artificiale tendono ad assomigliarsi tutti e peggiorano l'immagine dell'azienda presso clienti e fornitori.
- **Uso non autorizzato** di account personali o gratuiti con dati aziendali: la cosiddetta *shadow AI*, l'intelligenza artificiale usata fuori dagli strumenti approvati dall'azienda. Va regolato con un regolamento d'uso e con la formazione.

4. Sviluppo di software: informatici affiancati dal personale interno

Gli strumenti di intelligenza artificiale fanno sembrare facile programmare, ma un progetto software resta un progetto informatico: logica, struttura dei dati, sicurezza, prove e manutenzione. Per questo lo sviluppo va **affidato a personale informatico**, affiancato da chi conosce l'azienda.

Tabella 1 — Chi fa cosa

RUOLO	COMPITI
Personale informatico	Analisi e progettazione, sviluppo con l'intelligenza artificiale e controllo del codice, sicurezza, prove, rilascio, documentazione e manutenzione
Personale aziendale	Descrive processi, casi reali ed eccezioni; fissa regole e priorità; valida e collauda
Proprietà	Autorizza il progetto, stabilisce il budget, approva il rilascio

- **Metodo.** Requisiti scritti prima di iniziare, rilasci a piccoli passi, prove su dati di test, codice con lo storico delle versioni.
- **Controllo e continuità.** Una seconda intelligenza artificiale o un secondo informatico verifica il codice. Il software è dell'azienda, è documentato e può essere mantenuto da altri, anche cambiando fornitore di intelligenza artificiale.

5. L'approccio consigliato: applicazioni ibride

È meglio non affidare all'intelligenza artificiale un intero processo, ma farlo gestire da un'**applicazione tradizionale**, con regole esplicite e controllabili, facendo intervenire l'intelligenza artificiale **solo nei passaggi** in cui porta un vantaggio reale.

Tabella 2 — Divisione dei compiti

ALL'APPLICAZIONE (PROCESSO ESATTO E RIPETIBILE)	ALL'INTELLIGENZA ARTIFICIALE (INTERPRETAZIONE VERIFICABILE)
Calcoli, prezzi e preventivi; scritture su gestionale e database; autorizzazioni; archiviazione e cancellazioni; invii a clienti e fornitori	Lettura di email e documenti non strutturati; estrazione di dati; classificazione delle richieste; riassunti e bozze di risposta; ricerca nella documentazione interna

- **L'intelligenza artificiale propone, l'applicazione verifica.** L'intelligenza artificiale può accedere ai dati **in sola lettura**, con autorizzazione esplicita. La **scrittura** è ammessa solo entro limiti e regole definiti in precedenza, e con autorizzazione a ogni occorrenza, dopo aver verificato in un report che cosa sta per essere scritto. Ogni intervento resta registrato.
- **Costi di esercizio contenuti e prevedibili.** L'intelligenza artificiale si chiama solo quando serve, anche con modelli più economici. Viene usata soprattutto per sviluppare più in fretta, molto meno durante il funzionamento quotidiano.
- **Controllo e continuità.** Le regole aziendali restano stabili e gli errori circoscritti. Il fornitore di intelligenza artificiale si può cambiare senza rifare l'applicazione e, se il servizio non è disponibile, il processo prosegue «manualmente».

Esempio: ordini e preventivi ricevuti via email, con l'intelligenza artificiale sempre più presente

Tabella 3 — Livelli di intervento dell'intelligenza artificiale

LIVELLO	COSA FA L'INTELLIGENZA ARTIFICIALE	AVALLO UMANO	COSTO DI ESERCIZIO
1. Di base	Legge email e allegati ed estrae cliente, articoli e quantità. L'applicazione verifica i dati, calcola i prezzi con le regole aziendali e segnala le anomalie.	L'operatore conferma i dati; l'applicazione registra l'ordine.	BASSO
2. Intermedio	Prepara anche una proposta di preventivo, senza scrivere nulla nel database aziendale.	L'operatore controlla, corregge e conferma; solo allora l'applicazione registra il preventivo.	MEDIO
3. Avanzato	Consulta lo storico del cliente e la documentazione, propone condizioni e testo di risposta, prepara gli aggiornamenti da scrivere nel gestionale.	Prima di ogni scrittura o invio, un report mostra che cosa sta per essere fatto; l'operatore autorizza caso per caso.	ALTO

[ATTENZIONE]

Più intelligenza artificiale, più costi e più controlli

Salendo di livello aumentano le chiamate al servizio, la quantità di dati elaborati e quindi i costi, oltre al lavoro di sviluppo di limiti, regole e report di verifica. In tutti i livelli la decisione finale resta a una persona.

6. Temi sistemistici e sicurezza

- **Censimento** delle attività dei singoli operatori, dei progetti in corso e conclusi, e delle applicazioni realizzate: chi le ha fatte, dove girano, a quali dati accedono.
- **Discussione preventiva obbligatoria** di ogni attività che interagisce con dati aziendali: file, database, gestionale, posta.
- **Regole imposte con i permessi tecnici, non solo con le istruzioni all'intelligenza artificiale**, soprattutto durante sviluppo e prove. Account dedicati con il minimo dei privilegi, sola lettura come impostazione predefinita, scrittura sui sistemi in produzione solo autorizzata caso per caso, credenziali gestite e revocabili. Così un agente non può scavalcare i recinti che esistono già.

- **Protezione dagli errori.** Ambienti di prova separati, backup verificato prima di qualsiasi operazione automatica, registro delle azioni. Attenzione anche alla *prompt injection*: istruzioni nascoste dentro documenti ed email, scritte per essere lette ed eseguite dall'intelligenza artificiale che li elabora.

7. Normativa e responsabilità

- **AI Act europeo e legge italiana sull'intelligenza artificiale.** Il Regolamento (UE) 2024/1689 e la legge 132 del 2025 introducono l'obbligo di formazione per chi usa sistemi di intelligenza artificiale, e obblighi che variano in base al rischio dell'uso.
- **GDPR e NIS2.** La seconda è la direttiva europea sulla sicurezza delle reti e dei sistemi informativi. Riguardano i dati personali inviati ai fornitori, gli accordi sul trattamento dei dati da firmare con loro (DPA), i trasferimenti fuori dall'Unione Europea e la valutazione d'impatto sulla protezione dei dati (DPIA). I fornitori di intelligenza artificiale vanno inclusi nella valutazione dei rischi della catena di fornitura.
- **Riservatezza e proprietà intellettuale.** Segreti aziendali scritti nelle richieste, titolarità del codice e dei contenuti generati, uso dei dati per addestrare i modelli.
- **Responsabilità.** Per ogni processo che usa l'intelligenza artificiale deve esserci un responsabile umano.

8. Proposta operativa

1. **Censimento** di attività, progetti e applicazioni esistenti.
2. **Regolamento aziendale sull'uso dell'intelligenza artificiale**, con strumenti ammessi, dati vietati e revisione umana obbligatoria, accompagnato dalla formazione del personale.
3. **Procedura di approvazione** dei nuovi progetti, con la valutazione di costi, benefici, sicurezza e conformità.
4. **Misure tecniche** di sicurezza e separazione degli ambienti.
5. **Sviluppo di applicazioni ibride**, guidato da personale informatico, partendo da un progetto pilota misurabile.