

lug 30, 2026

Riunione del giorno 30 lug 2026

alle ore 14:15 CEST

Riepilogo

La sessione ha stabilito linee guida rigorose per l'uso dell'Intelligenza Artificiale, enfatizzando la responsabilità umana e sicurezza.

Responsabilità e sicurezza

L'Intelligenza Artificiale deve essere usata come supporto, mantenendo la responsabilità finale sull'operatore umano. È vietato inserire dati sensibili o riservati nei sistemi esterni.

Classificazione dei rischi

Le attività sono divise per rischio: uso libero per compiti amministrativi semplici e divieto per decisioni critiche. Ogni uso deve rispettare le procedure di autorizzazione aziendali.

Validazione e prompting

Gli output dell'Intelligenza Artificiale richiedono sempre validazione umana e verifica delle fonti. Richieste precise includenti contesto e vincoli migliorano significativamente la qualità dei risultati ottenuti.

Passaggi successivi

Creare standard richieste: Definire uno standard unificato per le richieste di autorizzazione all'utilizzo di strumenti di intelligenza artificiale in azienda.

Dichiarare uso AI: Elencare tutti gli strumenti di intelligenza artificiale attualmente in uso presso la propria area di competenza.

Segnalare rischi: Segnalare al referente qualsiasi funzione sospetta, biometrica o emozionale che possa presentare rischi elevati per l'azienda.

Analizzare attività: Individuare 2 attività lavorative ricorrenti per verificare se l'integrazione dell'intelligenza artificiale possa migliorarne l'efficienza.

Completare censimento: Completare le procedure di censimento relative agli strumenti di intelligenza artificiale in uso nel proprio dipartimento.

Proporre schemi: Proporre uno schema di richieste riutilizzabili per le proprie attività e sottoporlo a validazione con il referente.

Dettagli

- **Obiettivo del modulo:** Il modulo è dedicato all'utilizzo dell'Intelligenza Artificiale (AI) rispettando le regole stabilite e il perimetro consentito, con l'obiettivo di rendere i partecipanti consapevoli di come usare tali strumenti in azienda.
- **Domande fondamentali per l'uso dell'AI:** Prima di utilizzare uno strumento di AI, è necessario verificare se esso sia autorizzato dall'azienda e valutare attentamente il tipo di dati immessi, in particolare se contengono informazioni personali, riservate o di sicurezza.
- **Responsabilità del risultato:** La responsabilità finale di ogni atto, comunicazione o decisione basata su output dell'AI ricade interamente sull'operatore umano, che non può delegare tale responsabilità allo strumento tecnologico.
- **Dati protetti e riservatezza:** È vietato inserire dati sensibili, come informazioni su passeggeri, dipendenti, contratti o procedure di sicurezza, nei chatbot, poiché tali dati vengono trasferiti su server esterni non controllati.
- **Livelli di autorizzazione:** Esistono tre livelli di autorizzazione per l'uso dell'AI: l'uso individuale per dati non riservati (pre-autorizzato), l'autorizzazione ordinaria per processi aziendali tramite scheda di richiesta e il divieto per usi non conformi o rischiosi.
- **Standardizzazione delle richieste:** Per le autorizzazioni, è necessario fornire informazioni chiare su cosa fa il sistema, in quale processo interviene, quali dati riceve, chi è il destinatario dell'output e le conseguenze in caso di malfunzionamento.
- **Prevenzione del Lock-in:** È essenziale evitare la dipendenza totale dai sistemi di AI, assicurandosi di poter svolgere le medesime attività manualmente nel caso in cui lo strumento non fosse disponibile o funzionante.
- **Gestione delle bozze e verifica umana:** Gli output generati dall'AI devono essere considerati esclusivamente come bozze, che richiedono la rielaborazione e la verifica critica da parte di un esperto di dominio prima di diventare documenti ufficiali.

- **Sistema semaforico per l'uso dell'AI:** Le attività aziendali sono suddivise in categorie di rischio: uso libero per strumenti in elenco senza dati sensibili, uso con autorizzazione per processi aziendali e divieto assoluto per decisioni su persone o aree critiche.
- **Aree a basso rischio:** Attività come la stesura di bozze di corrispondenza, comunicazioni interne, traduzioni di materiale divulgativo o riordino di elenchi pubblici sono considerate a basso rischio e generalmente ammesse.
- **Gestione di contratti e gare:** È consentito l'uso dell'AI per spiegazioni di clausole standard o checklist di verifica offerte, ma è vietato analizzare contratti riservati o effettuare valutazioni comparative di offerte senza autorizzazione.
- **Risorse Umane e valutazione:** L'uso dell'AI nelle risorse umane è limitato ad attività di supporto (annunci, griglie colloqui), mentre è vietata l'analisi o il filtro automatico delle candidature e la valutazione automatizzata delle performance dei dipendenti.
- **Operatività e pianificazione:** L'utilizzo di software di pianificazione turni basato su AI è consentito solo se il sistema funge da supporto decisionale e non come decisore autonomo, mantenendo la responsabilità umana.
- **Sistemi di sicurezza:** È vietata l'automazione di decisioni operative e la delega all'AI per sistemi rilevanti per la sicurezza senza autorizzazione specifica e parere vincolante della funzione competente.
- **Manutenzione e impianti:** L'AI può essere usata per la ricerca di documentazione tecnica o rapporti di intervento (uso libero), mentre la previsione di guasti o la modifica di parametri d'impianto richiede autorizzazione.
- **Security e sorveglianza:** La maggior parte delle applicazioni in questo ambito richiede autorizzazione. È consentito il rilevamento di intrusioni basato su regole, mentre sono vietate analisi comportamentali avanzate o riconoscimento facciale non autorizzato.
- **Marketing e comunicazione:** La generazione di contenuti tramite AI richiede autorizzazione e l'obbligo di dichiarare chiaramente l'uso dello strumento, per evitare comunicazioni ingannevoli.
- **Supporto IT e programmazione:** L'AI può assistere nella scrittura o revisione di codice non riservato e nell'analisi di log anonimizzati, a condizione che l'operatore sia in grado di verificare e comprendere il lavoro svolto.
- **Formazione:** È vietata la valutazione automatizzata dell'apprendimento del personale tramite AI; tale attività deve rimanere un processo umano per garantire l'effettiva competenza.

- **Tecniche di prompting efficace:** Per ottenere risultati utili, la richiesta all'AI deve includere: ruolo, contesto, compito, formato di output desiderato e vincoli specifici.
- **Anonimizzazione dei dati:** Prima di inserire documenti nei chatbot, è obbligatorio anonimizzarli utilizzando strumenti locali per garantire che i dati sensibili non escano dall'infrastruttura aziendale.
- **Qualità dell'output:** È fondamentale includere vincoli negativi, come l'esplicito divieto di inventare informazioni, e chiedere di segnalare con parentesi quadre i segnaposti dove l'utente dovrà intervenire.
- **Verifica delle fonti:** Poiché l'AI può generare informazioni plausibili ma errate, è necessario chiedere al sistema di citare le fonti per ogni affermazione e verificare tali riferimenti personalmente.
- **Gestione dei compiti complessi:** È consigliabile spezzare i task complessi in sotto compiti più semplici, chiedendo al sistema di generare una scaletta di lavoro, per migliorare la qualità del risultato e ottimizzare le risorse.
- **Iterazione e contesto:** Invece di iniziare nuove conversazioni, è preferibile iterare sulla stessa chat per mantenere il contesto, facendo attenzione a non saturare la finestra di memoria del sistema.
- **Validazione umana finale:** Non accettare mai il primo risultato, chiedere al sistema di ragionare o criticare la propria risposta e verificare sempre il merito e la correttezza dei dati prima di utilizzare l'output.
- **Documentazione dell'uso:** Per decisioni, atti o comunicazioni verso l'esterno, è obbligatorio registrare l'uso dell'AI, chi ha effettuato la verifica del risultato e l'esito della stessa.
- **Inventario e censimento:** Il censimento dei sistemi AI utilizzati in azienda deve essere continuo; non devono essere introdotti nuovi sistemi senza preventiva autorizzazione e notifica.
- **Registrazione della formazione:** I dettagli relativi al percorso formativo, inclusi i partecipanti, i materiali utilizzati e le verifiche di apprendimento, sono conservati agli atti.
- **Uso appropriato degli strumenti di Intelligenza Artificiale:** L'Intelligenza Artificiale può essere utilizzata per attività di redazione, controllo della qualità linguistica o revisione dello stile comunicativo, a condizione che non vengano inseriti dati sensibili, nomi o informazioni identificative personali. La bozza prodotta dallo strumento richiede sempre una validazione umana per certificarne l'accuratezza e la correttezza prima dell'utilizzo.

- **Limitazioni nella delega:** È vietato delegare all'Intelligenza Artificiale giudizi di merito sulle persone, valutazioni, selezioni, provvedimenti o decisioni operative. La responsabilità finale degli atti e della firma di documenti aziendali resta esclusivamente in capo al personale, rendendo obbligatoria la verifica umana di ogni documento prima della sua uscita dall'azienda.
- **Gestione della responsabilità e monitoraggio:** Si richiede al personale di esplorare gli strumenti approvati e di utilizzarli esclusivamente per compiti semplici e autorizzati. È necessario riconoscere quando l'uso dell'intelligenza artificiale non è opportuno; i responsabili di area devono supervisionare l'uso degli strumenti da parte dei propri collaboratori, assumendosi la responsabilità finale delle attività svolte.
- **Procedure di autorizzazione e documentazione:** È in fase di emissione un disciplinare che regolerà l'uso dell'Intelligenza Artificiale. Le richieste di utilizzo ricorrenti dovranno essere validate e schematizzate per area; le autorizzazioni non saranno concesse direttamente dai responsabili dei sistemi informativi o dai referenti per l'Intelligenza Artificiale, ma richiederanno un processo decisionale specifico.
- **Struttura delle richieste (Prompt):** Per interagire correttamente con i sistemi di Intelligenza Artificiale, le richieste devono includere esplicitamente il ruolo, il contesto, il compito da eseguire, il formato di output desiderato e i relativi vincoli.
- **Fasi del processo di autorizzazione:** Il processo di autorizzazione si articola in sette fasi, che comprendono la richiesta, la classificazione del livello di rischio, il vaglio di sicurezza, la valutazione della rilevanza e l'istituzione di presidi interni. È necessario che le aree dispongano di controlli interni per monitorare l'uso dell'intelligenza artificiale, garantendo l'autotutela dei collaboratori e dell'azienda.
- **Monitoraggio e verifica dei dati:** Per la tutela di tutti gli attori coinvolti, è necessario attuare un sistema di monitoraggio e audit delle attività svolte con l'intelligenza artificiale. È fondamentale verificare sempre i riferimenti, i numeri e il merito delle informazioni prodotte dallo strumento.
- **Gestione delle competenze nell'uso dell'AI:** L'uso dell'Intelligenza Artificiale è considerato ideale solo se l'utente dispone del materiale di riferimento e possiede la competenza specifica per validare l'output. L'utilizzo basato esclusivamente sulla memoria dello strumento da parte di personale non competente è classificato come rischioso e deve essere evitato.
- **Azioni immediate richieste al personale:** Viene richiesto di dichiarare l'uso attuale degli strumenti di Intelligenza Artificiale, segnalare funzioni a rischio alto (come quelle biometriche o emozionali) e individuare due attività ricorrenti da ottimizzare.

È inoltre richiesta la partecipazione al censimento in corso, astenendosi dall'introdurre nuovi sistemi fino alla sua conclusione.

- **Gestione delle procedure operative interne:** Prima di utilizzare l'Intelligenza Artificiale per riassumere una procedura operativa interna, è obbligatorio verificare se il documento può essere divulgato all'esterno. Se autorizzato, occorre fornire il documento allo strumento chiedendo di operare esclusivamente su quel testo, senza confrontarlo con altre fonti.
- **Gestione di nuove funzioni software:** In caso di aggiornamenti di sistemi esistenti, come quelli del personale, che introducono intelligenza artificiale, non è consentita l'attivazione immediata. Poiché tali funzioni potrebbero rientrare in categorie ad alto rischio, è necessario segnalare il nuovo strumento al referente e attendere una valutazione prima di qualsiasi attivazione.
- **Approccio comunicativo per le nuove implementazioni:** Nel dubbio, è necessario consultare i referenti competenti prima di attivare nuove funzioni o prendere decisioni sull'uso dell'intelligenza artificiale. Chiedere supporto non riflette mancanza di competenza, ma dimostra proattività e volontà di crescita professionale.