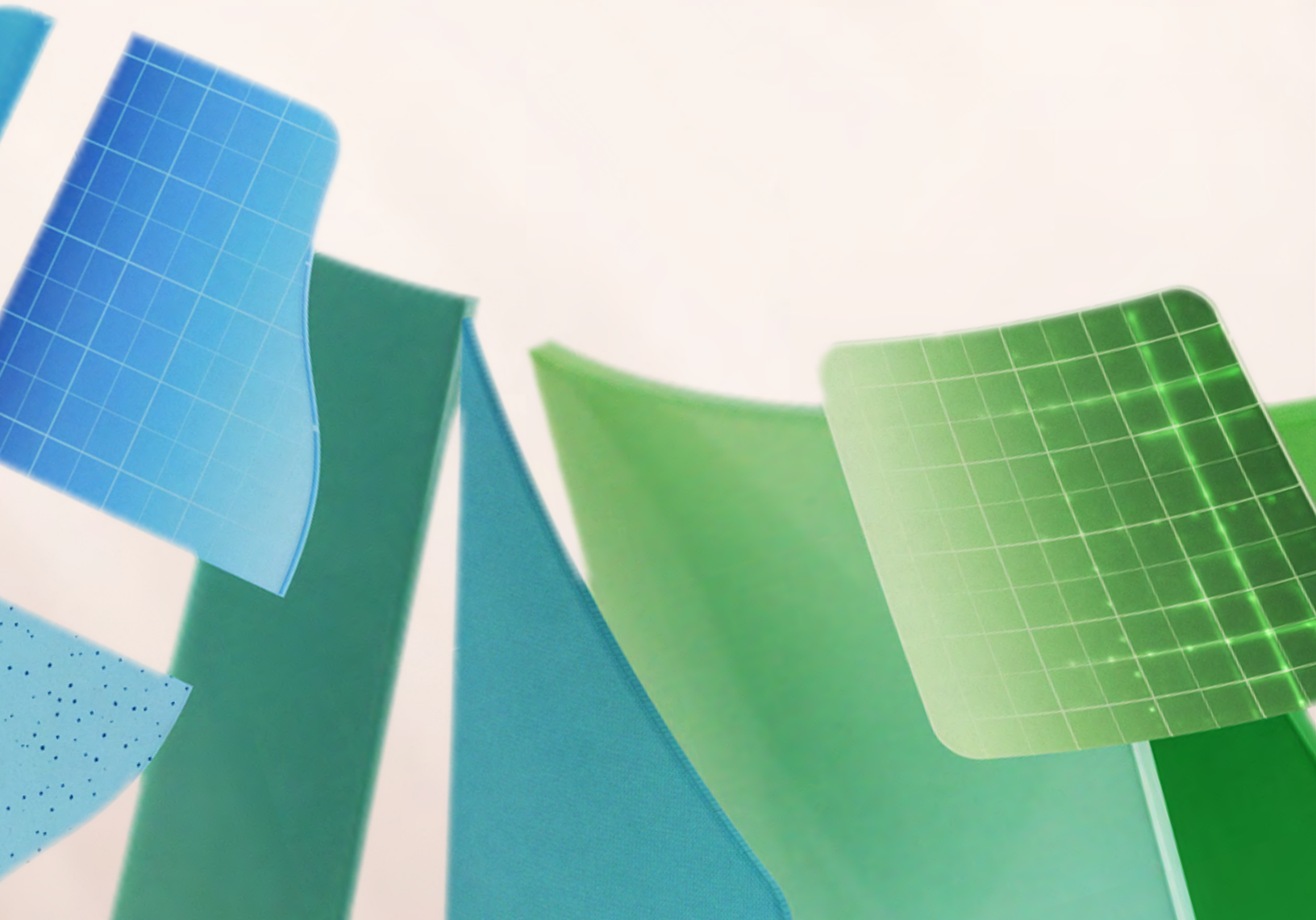
Microsoft 365

Dati sotto controllo

Gestione della governance dei dati per il successo dell'IA



Indice

Introduzione

La governance dei dati è fondamentale per un'adozione sicura dell'IA

L'intelligenza artificiale generativa promette la trasformazione del business, ma la realizzazione di questo potenziale dipende dalla qualità e dalla disponibilità dei dati aziendali.

Le organizzazioni che mettono al primo posto una solida governance dei dati creano le condizioni per ottenere un vantaggio competitivo con l'intelligenza artificiale. La governance dei dati aiuta a garantire che i dati sottoposti a query e generati dall'intelligenza artificiale siano corretti, sicuri, controllati e conformi.

Qualità e disponibilità dei dati: i sistemi di intelligenza artificiale si affidano a set di dati di grandi dimensioni e di alta qualità per restituire la migliore risposta possibile con il giusto contesto proveniente dai flussi di lavoro specifici dell'organizzazione. Una qualità migliore dei dati determina insights e previsioni IA più efficaci.

Compliance: una solida governance dei dati assicura l'aderenza ai requisiti normativi, riducendo il rischio di problemi legali e sanzioni.

Sicurezza: una corretta etichettatura e gestione dei dati protegge le informazioni sensibili da accessi non autorizzati, condivisioni inappropriate e violazioni.

Fiducia: una governance affidabile dei dati crea fiducia tra gli stakeholder negli output dell'intelligenza artificiale, promuovendo livelli più elevati di adozione e supporto per le iniziative correlate all'intelligenza artificiale.

Questo e-Book presenta pratiche fondamentali di governance dei dati che creano un'organizzazione pronta per l'intelligenza artificiale. Illustra come predisporre solidi standard di qualità dei dati, assicurare la compliance con i requisiti normativi e implementare misure di protezione e sicurezza dei dati. Che si tratti di impedire che i contenuti sensibili delle riunioni vengano condivisi all'esterno o di proteggersi dalle violazioni dei dati, scoprirai strategie per infondere fiducia nei sistemi di intelligenza artificiale e rendere i dati subito disponibili per ottenere insights utili. Adottando queste pratiche, la tua organizzazione potrà sfruttare il pieno potenziale dell'intelligenza artificiale per un'innovazione continua e un vantaggio competitivo.

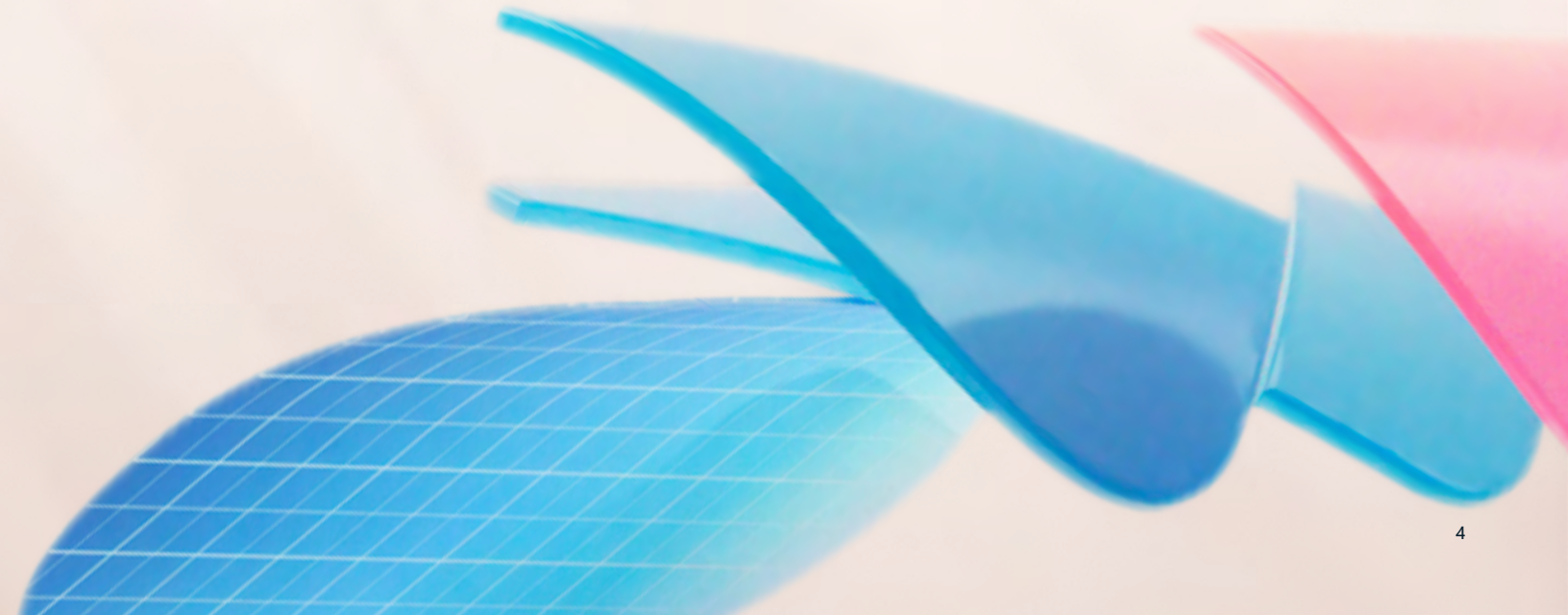
Casi d'uso dell'intelligenza artificiale generativa

Accelerare la comunicazione: genera bozze di contenuti personalizzati più velocemente, liberando tempo da dedicare alla costruzione di relazioni e alla collaborazione.

Migliorare l'efficienza: riduci il tempo dedicato alle attività di routine, migliora la produttività e taglia i costi.

Abilitare l'innovazione: aiuta a generare idee e proposte per nuovi prodotti e servizi.

Personalizzare le esperienze dei clienti: adatta contenuti e consigli per favorire la fidelizzazione e il coinvolgimento.



1

Rafforzare la governance dei dati per la trasformazione dell'IA

Ogni organizzazione ha criteri e processi che governano l'utilizzo dei dati. I framework di governance dei dati variano in termini di maturità e completezza, ma pochi sono stati pienamente ottimizzati per l'intelligenza artificiale. Mentre molte procedure consigliate per la governance dei dati restano le stesse, come ad esempio quelle che assicurano l'accuratezza e la coerenza dei dati, altri aspetti richiedono invece aggiornamenti per massimizzare gli investimenti in intelligenza artificiale.
Diamo un'occhiata ad alcune aree chiave.

Visibilità dei dati

La conoscenza dettagliata del flusso di dati all'interno dei sistemi di intelligenza artificiale consente di individuare e mitigare l'uso non autorizzato o inappropriato. Questa visibilità aiuta a supportare sicurezza e compliance, proteggendo i dati sensibili per massimizzare il valore dell'intelligenza artificiale.

La governance dei dati tradizionale si è concentrata sulla conoscenza delle posizioni in cui risiedono i dati e sul controllo dell'accesso. Tuttavia, con la maggiore integrazione dell'intelligenza artificiale nelle operazioni aziendali, la governance dei dati deve tenere il passo con esigenze di sicurezza in continua evoluzione. Ad esempio, con il lancio di un prodotto altamente sensibile, la governance deve ora estendersi alla gestione dei contenuti generati dall'intelligenza artificiale, garantendo la sicurezza dei documenti relativi al progetto, delle comunicazioni e degli insights prodotti dall'intelligenza artificiale. Questo comporta l'implementazione di misure di sicurezza finalizzate ad assicurarsi che solo i membri autorizzati del team possano accedere all'intelligenza artificiale e usarla per analizzare o riassumere le informazioni relative al progetto.

Inoltre, gestendo i volumi di elaborazione e storage dei dati, le organizzazioni possono controllare meglio i costi operativi associati all'intelligenza artificiale.

Qualità dei dati

L'intelligenza artificiale amplifica l'importanza della qualità dei dati, poiché una scarsa qualità influisce direttamente sui risultati. Quando si applicano strumenti di intelligenza artificiale per eseguire query sui dati aziendali, è importante assicurarsi che i dati siano aggiornati e affidabili. Altrettanto importante è comprendere la provenienza e la qualità dei dati che i team usano per creare le proprie app e i propri modelli di intelligenza artificiale. Controlli periodici, rigorosi processi di convalida e una gestione proattiva dei dati aiutano a garantirne l'integrità. Concentrandosi su queste aree, le organizzazioni possono ottenere dall'intelligenza artificiale risultati affidabili che migliorano i processi decisionali e stimolano l'innovazione.

Gestione degli utenti

Con l'intelligenza artificiale, gli utenti interagiscono con i dati in modi sofisticati. Comunicano con i sistemi di intelligenza artificiale, come Microsoft 365 Copilot, attraverso richieste in linguaggio naturale. Con autorizzazioni e protezioni attive, l'intelligenza artificiale può accedere al contesto pertinente dai dati – come file, chat ed e-mail – oltre a origini esterne tramite plug-in al fine di generare una risposta.

Per assicurarsi che l'intelligenza artificiale fornisca risposte corrette e fondate, è fondamentale monitorare i dati usati in questi processi. La trasparenza, fornita attraverso note a piè di pagina o collegamenti alle fonti originali, consente agli utenti di verificare le informazioni riducendo il rischio di uso improprio dei dati e garantendo la compliance alle normative.

Compliance e eDiscovery

La diffusione dell'intelligenza artificiale introduce nuove sfide in termini di compliance e eDiscovery (la gestione dei dati per i contenziosi), in particolare nella gestione dei dati generati dall'IA e nell'adattamento a requisiti legali in continua evoluzione. L'aggiornamento dei framework di governance dei dati per affrontare queste sfide comporta lo sviluppo di criteri relativi ai contenuti generati dall'intelligenza artificiale, ad esempio per garantire che le comunicazioni o i documenti prodotti dall'IA siano monitorati, classificati e archiviati in modo sicuro. Ad esempio, potrebbe essere necessario aggiornare i criteri per garantire che le e-mail o i report generati dall'intelligenza artificiale siano contrassegnati e archiviati correttamente per il successivo recupero.

Il miglioramento delle funzionalità di eDiscovery include ad esempio l'integrazione di strumenti di intelligenza artificiale capaci di cercare e identificare i contenuti generati dall'IA su varie piattaforme. Ad esempio, durante un'indagine legale, gli strumenti di eDiscovery devono essere in grado di trovare e recuperare specifici documenti generati dall'intelligenza artificiale, riassumere le comunicazioni rilevanti e fornire audit trail chiari per dimostrare la compliance. Aggiornando queste funzionalità, le organizzazioni possono gestire meglio i dati durante i controlli o le indagini legali, assicurandosi che tutte le informazioni rilevanti generate dall'intelligenza artificiale siano accessibili e sostenibili in tribunale.

Sicurezza dei dati

La protezione delle operazioni basate sull'intelligenza artificiale deve includere i principi Zero Trust a livello di identità per ridurre al minimo il rischio di accesso non autorizzato. Aggiornamenti periodici agli endpoint, inclusi dispositivi e applicazioni, riducono le vulnerabilità che potrebbero essere sfruttate. La consapevolezza degli strumenti di intelligenza artificiale generativa in uso all'interno dell'organizzazione consente di bloccare le applicazioni non autorizzate o non sicure, impedendo potenziali violazioni della sicurezza. Limitando l'accesso agli strumenti e ai dati di intelligenza artificiale al solo personale autorizzato, le organizzazioni possono raggiungere una maggiore integrità dei dati e proteggere le operazioni di IA da potenziali minacce.

Cos'è Zero Trust?

Zero Trust è un modello di sicurezza che si concentra sulla verifica di ogni richiesta come se questa provenisse da una rete non attendibile. Anziché presupporre che tutto ciò che si trova all'interno del firewall aziendale sia sicuro, questo approccio adotta il principio "non fidarsi mai, verificare sempre".

Principi Zero Trust

Verifica esplicita: esegui sempre l'autenticazione e l'autorizzazione in base a tutti i punti dati disponibili.

Uso dell'accesso con privilegi minimi: limita l'accesso degli utenti con approcci Just-In-Time e Just-Enough-Access (JIT/JEA), criteri adattivi basati sul rischio e protezione dei dati.

Presunzione di violazione: limita i danni, controlla l'accesso, garantisci la crittografia e usa i dati per individuare le minacce e rafforzare le difese.

2

Il ruolo dell'amministrazione dei dati nella trasformazione dell'IA: origini, qualità e affidabilità

Le organizzazioni che adottano l'intelligenza artificiale per supportare le decisioni aziendali devono assicurarsi che questi sistemi possano fornire risultati corretti e affidabili. I dati su cui si basano le risposte dell'IA devono essere disponibili, coerenti e ben documentati.

L'amministrazione dei dati sostiene un'intelligenza artificiale affidabile implementando criteri di governance che monitorano la provenienza dei dati, ne controllano la qualità e ne assicurano l'affidabilità e l'accuratezza. Queste procedure costituiscono la base per sistemi di intelligenza artificiale che restituiscono insights affidabili, consentendo processi decisionali informati e sicuri.

Derivazione dei dati: comprendere origini e modifiche alle informazioni

La derivazione dei dati tiene traccia del percorso dei dati all'interno di un'organizzazione. Ne documenta le origini, le trasformazioni e le destinazioni. Per le organizzazioni che usano l'intelligenza artificiale, la conoscenza della derivazione dei dati è fondamentale per diversi motivi:

- **Trasparenza:** conoscere la provenienza dei dati e come questi cambiano contribuisce a confermare l'accuratezza dei risultati generati dall'intelligenza artificiale e assicura la compliance alle normative, grazie a una chiara comprensione della storia dei dati.
- **Tracciabilità:** la derivazione dei dati consente alle organizzazioni di risalire alle origini di errori o incoerenze, semplificando la risoluzione dei problemi e la correzione dei dati.
- **Analisi dell'impatto:** comprendere come i dati sono usati dagli strumenti di intelligenza artificiale generativa aiuta a valutare il potenziale impatto delle modifiche nelle origini dati o nei metodi di elaborazione in termini di accuratezza dell'output e risultati aziendali.

Qualità dei dati: la qualità è alla base del valore delle risposte dell'IA

La qualità dei dati influisce direttamente sull'affidabilità degli output dell'intelligenza artificiale. Dati di alta qualità creano il contesto che consente ai modelli di intelligenza artificiale di restituire risposte corrette e di valore agli input dell'utente. Gli aspetti chiave della qualità dei dati includono:

- **Accuratezza:** i dati devono rappresentare correttamente le condizioni reali.
- **Completezza:** tutti i dati necessari devono essere presenti e presi in considerazione.
- **Coerenza:** i dati devono essere coerenti sui diversi sistemi e nel tempo.
- **Tempestività:** i dati devono essere aggiornati e disponibili quando servono.

Affidabilità dei dati: garantire dati affidabili

Dati affidabili sono quelli che soddisfano continuamente gli standard di qualità e sono disponibili quando servono. Per le organizzazioni che usano l'intelligenza artificiale, l'affidabilità dei dati è fondamentale per promuovere fiducia negli strumenti di IA e nelle decisioni prese in base a questi dati. L'affidabilità dei dati si ottiene con:

- **Ridondanza dei dati:** implementazione di sistemi di backup per prevenire le perdite e aumentare la disponibilità.
- **Backup regolari:** esecuzione di backup frequenti per la protezione da danni o perdite di dati.
- **Monitoraggio e avvisi:** predisposizione di sistemi di monitoraggio per rilevare e avvisare gli stakeholder di problemi ai dati in tempo reale.
- **Piani di disaster recovery:** sviluppo e test di piani per recuperare i dati e riprendere rapidamente le operazioni dopo le interruzioni.

3

La relazione tra governance, sicurezza e intelligenza artificiale responsabile

Insieme, la governance e la sicurezza dei dati sono fondamentali per un uso responsabile dell'intelligenza artificiale. Dati sicuri e di alta qualità garantiscono un funzionamento etico ed efficace dell'intelligenza artificiale. Le aree chiave da valutare includono: classificazione dei dati, controlli di accesso, crittografia, risposta agli incidenti e compliance normativa.

Classificazione dei dati

La classificazione dei dati è un aspetto fondamentale del controllo di come gli strumenti di intelligenza artificiale usano le informazioni sensibili. In genere, dati e riunioni sono classificati con etichette come Generale, Riservato o Strettamente riservato. Una classificazione corretta assicura che l'intelligenza artificiale acceda solo alle informazioni appropriate, riducendo il rischio di esporre dati sensibili a utenti non autorizzati.

Una classificazione errata, d'altro canto, può portare l'intelligenza artificiale a elaborare dati ad accesso limitato, con conseguenti violazioni della sicurezza o problemi di compliance. Una governance efficace dei dati, tramite strumenti automatizzati o criteri per gli utenti finali, assicura una corretta classificazione dei dati, salvaguardando le informazioni sensibili e supportando la capacità dell'intelligenza artificiale di restituire output affidabili e conformi.

Controlli di accesso

Questi controlli stabiliscono chi può accedere ai dati rilevanti per l'intelligenza artificiale e quali applicazioni o identità sono autorizzate a interagire con tali dati. Controlli di accesso deboli possono determinare l'esposizione non autorizzata di informazioni sensibili, aumentando il rischio di violazioni e uso improprio.

La governance dei dati gioca un ruolo fondamentale nell'applicazione di questi controlli limitando l'accesso ai dati al personale autorizzato e ad applicazioni specifiche, garantendo così una gestione corretta dei dati sensibili. Ciò protegge non solo l'integrità dei dati, ma assicura anche che i sistemi di intelligenza artificiale operino su set di dati sicuri e attendibili, per livelli di affidabilità e compliance migliori.

Crittografia

La protezione dei dati da intercettazioni e manomissioni attraverso la crittografia aiuta ad assicurarsi che gli strumenti di intelligenza artificiale generativa possano basare le loro risposte sul contesto corretto – come dati, file, chat ed e-mail di lavoro – senza rischiare perdite di dati.

I criteri di governance dei dati possono imporre severe pratiche di crittografia, proteggendo i dati durante l'intero ciclo di vita. Questo approccio assicura che gli strumenti di intelligenza artificiale possano restituire risposte affidabili, preservando la sicurezza dei dati e la fiducia.

Risposta agli incidenti

I dati sensibili dell'organizzazione possono essere esposti attraverso incidenti che coinvolgono strumenti di intelligenza artificiale generativa che concedono l'accesso non autorizzato a file, e-mail o altri dati aziendali usati dai sistemi per generare le risposte.

In questi scenari, un piano di risposta agli incidenti proattivo è fondamentale. In assenza di un simile piano, l'organizzazione rischia non solo di esporre dati sensibili, ma anche di ricevere dall'intelligenza artificiale output compromessi. La governance dei dati include la disponibilità di protocolli di risposta dettagliati per affrontare rapidamente le violazioni, ridurne al minimo l'impatto e preservare l'affidabilità dei sistemi di intelligenza artificiale.

Compliance normativa

Le applicazioni di intelligenza artificiale devono rispettare normative quali il GDPR o CCPA che disciplinano la protezione dei dati e la privacy. La mancata compliance può comportare sanzioni significative e minare la fiducia. È inoltre importante sapere dove gli strumenti di intelligenza artificiale elaborano i dati. Molti strumenti gratuiti possono infatti gestire i dati globalmente o all'esterno delle consuete posizioni di storage dell'organizzazione. La governance dei dati assicura che le applicazioni di intelligenza artificiale siano non solo eseguite all'interno di framework legali, ma anche che i dati siano mantenuti entro i giusti limiti del servizio, in linea con gli standard di compliance dell'organizzazione. Questo approccio supporta l'uso etico dell'intelligenza artificiale e contribuisce a infondere fiducia nella tecnologia IA.

4

Aggiornare il framework di governance dei dati per supportare l'adozione dell'IA

In un panorama IA in continua evoluzione, è importante identificare aree specifiche del framework di governance dei dati esistente che potrebbero richiedere un'attenzione particolare. Anziché rivedere l'intero framework, puoi concentrarti sulle aree con maggiori probabilità di evoluzione, puntando su iniziative finalizzate ad aumentare il valore dell'intelligenza artificiale e a garantire al contempo la protezione e la sicurezza dei dati. Ecco alcuni insights chiave da tenere in considerazione:

Adattamento di criteri e procedure

L'intelligenza artificiale comporta nuovi tipi di raccolta, elaborazione e utilizzo dei dati. L'aggiornamento dei criteri relativi ai dati può contribuire a soddisfare le esigenze relative alla privacy, alla compliance normativa e all'uso etico dei dati. Ad esempio, la richiesta di anonimizzazione dei dati in specifiche istanze può proteggere le informazioni personali, determinandone un uso più sicuro nell'intero ciclo di vita dell'intelligenza artificiale.

Ruoli e responsabilità

È essenziale integrare la preparazione per l'IA in tutti i ruoli coinvolti nella governance dei dati. I dipendenti che hanno familiarità con i requisiti dei dati di IA possono fungere da amministratori per supportare la qualità e la compliance dei dati. La collaborazione interfunzionale tra i team legali, IT e data science può aiutare ad affrontare le sfide specifiche dell'intelligenza artificiale in maniera più efficace.

Adattamento di standard e definizioni dei dati

La standardizzazione di formati, definizioni e metriche sulla qualità dei dati semplifica l'implementazione dei criteri che regolano l'utilizzo degli strumenti di intelligenza artificiale all'interno di un'organizzazione. Standard chiari relativi ai dati semplificano la scelta dei set di dati su cui gli strumenti di intelligenza artificiale possono ragionare per fornire il contesto aziendale e dei dati che gli utenti possono caricare per l'analisi. Questo assicura che le applicazioni di intelligenza artificiale usino i dati più rilevanti e attendibili, migliorandone l'efficacia e supportando la compliance con i criteri dell'organizzazione.

Miglioramento continuo

La governance dei dati è un processo continuo, soprattutto con l'intelligenza artificiale. Controlli e aggiornamenti periodici del framework di governance possono aiutare ad adattarlo ai nuovi sviluppi dell'intelligenza artificiale e ai cambiamenti normativi. L'intelligenza artificiale stessa può essere usata per controllare e migliorare le pratiche di governance, individuando potenziali lacune e suggerendo miglioramenti. Questo approccio proattivo migliora i livelli di compliance ed efficienza mentre le tecnologie di intelligenza artificiale evolvono.

Strumenti e tecniche per una governance dei dati efficace

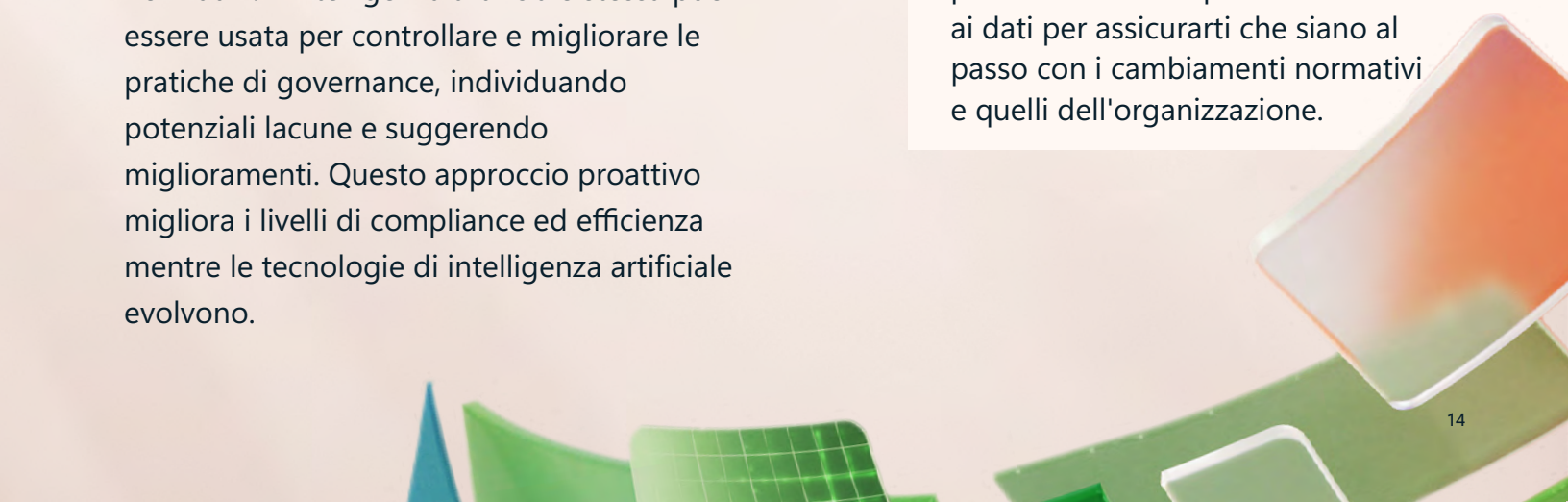
Allineamento agli obiettivi aziendali: assicurati che la tua strategia di governance dei dati supporti gli obiettivi di miglioramento del processo decisionale e dell'efficienza dell'organizzazione.

Automazione delle attività di routine: usa l'automazione per le attività ripetitive come la classificazione dei dati e la gestione degli accessi per ridurre gli errori manuali e migliorare la sicurezza.

Standard di accuratezza elevati: usa strumenti di convalida e pulizia per supportare l'integrità dei dati nel tempo.

Formazione degli utenti: offri formazione su strumenti e procedure di governance dei dati per prevenire la cattiva gestione e assicurare la compliance con i criteri.

Controlli periodici: rivedi periodicamente le procedure relative ai dati per assicurarti che siano al passo con i cambiamenti normativi e quelli dell'organizzazione.



Conclusioni

Governance efficace dei dati per l'abilitazione dell'IA con Microsoft 365

L'uso responsabile dell'intelligenza artificiale richiede una solida governance dei dati. Una governance dei dati efficace garantisce disponibilità, accuratezza e sicurezza dei dati, consentendo all'intelligenza artificiale di restituire insights affidabili e promuovere innovazione. Mettere al primo posto qualità, compliance e sicurezza dei dati migliora le capacità dell'intelligenza artificiale, promuovendo processi decisionali migliori e mantenendo un vantaggio competitivo.

Microsoft 365: inizia a prepararti per l'IA

Microsoft 365 offre app per la produttività all'avanguardia con strumenti integrati per la classificazione, il controllo e la protezione dei dati. Queste funzionalità supportano il framework di governance dei dati, agevolando l'adozione sicura dell'intelligenza artificiale quando l'organizzazione è pronta. Microsoft 365 ti aiuta a garantire:

- **Qualità dei dati:** supporta accuratezza e affidabilità degli output di IA.
- **Compliance:** rispetta i requisiti normativi, riducendo i rischi legali.
- **Sicurezza Zero Trust:** proteggi le informazioni sensibili da accessi non autorizzati, violazioni e minacce informatiche.

Scopri strumenti di produttività completi, potenziati con opzioni di intelligenza artificiale e solida protezione per aiutare la tua organizzazione a lavorare in modo efficiente e sicuro.

Esplora Microsoft 365