SISTEMI DI GESTIONE DELL'INTELLIGENZA ARTIFICIALE

Guida generale
ISO 42001

LRQA

Contenuti

Navigare nel panorama dell'intelligenza artificiale

Comprendere le tendenze che stanno modellando la tecnologia, il rischio e la responsabilità

L 'intelligenza artificiale (AI) è sempre più applicata in tutti i settori che utilizzano le tecnologie dell'informazione e si prevede che sarà uno dei principali motori economici. Una conseguenza di questa tendenza è che alcune applicazioni possono dare origine a sfide sociali nei prossimi anni. Dalla finanza al settore manifatturiero, dalla sanità alla logistica, l'IA sta determinando progressi nell'automazione, nell'efficienza e nel processo decisionale. L'adozione diffusa dell'IA generativa e dell'apprendimento automatico ha aperto nuove possibilità, ma ha anche accelerato la necessità di una **governance più forte**, di una maggiore **trasparenza** e di una più chiara **responsabilità**.

Il panorama globale dell'intelligenza artificiale è caratterizzato da tre tendenze convergenti:

Implementazione accelerata

Le aziende si stanno muovendo rapidamente per incorporare l'IA nelle operazioni principali. Secondo IBM, il 42% delle imprese sta già esplorando o implementando attivamente l'IA generativa. Tuttavia, questo ritmo spesso supera lo sviluppo di strutture di governance formali, creando lacune nella supervisione, nella garanzia di qualità e nella gestione del rischio.

Evoluzione della normativa

I governi e le autorità di regolamentazione stanno rispondendo alle crescenti preoccupazioni della società con nuovi quadri di riferimento per garantire che i sistemi di IA siano sicuri, equi e spiegabili. La legge europea sull'IA, approvata nel 2024, costituisce un precedente per la regolamentazione basata sul rischio e iniziative simili sono in corso a livello globale. Il messaggio è chiaro: la fiducia nell'IA deve essere guadagnata, non data per scontata.

Crescente controllo e aspettative etiche

Dalla privacy dei dati alla proprietà intellettuale, dalla parzialità alla responsabilità, le organizzazioni sono sotto pressione per dimostrare che il loro uso dell'IA è etico, responsabile e sicuro. La fiducia del pubblico è fragile e i passi falsi possono portare rapidamente a danni di reputazione, conseguenze normative e opportunità perse.

Queste tendenze segnalano un punto di svolta. L'IA è passata da programmi pilota a infrastrutture strategiche. E con questo passaggio è necessaria una governance strutturata, a livello di sistema, in grado di scalare con le ambizioni e di resistere ai controlli.

Che cos'è la ISO 42001?

Il primo standard internazionale di sistema di gestione per l'IA

ISO 42001 è il primo standard di sistema di gestione specifico per l'intelligenza artificiale al mondo, che fornisce un quadro strutturato per aiutare le organizzazioni a gestire l'intelligenza artificiale in modo responsabile.

Pensato per le organizzazioni che sviluppano, implementano o si affidano all'intelligenza artificiale, lo standard definisce i requisiti per stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione dell'intelligenza artificiale (AIMS).

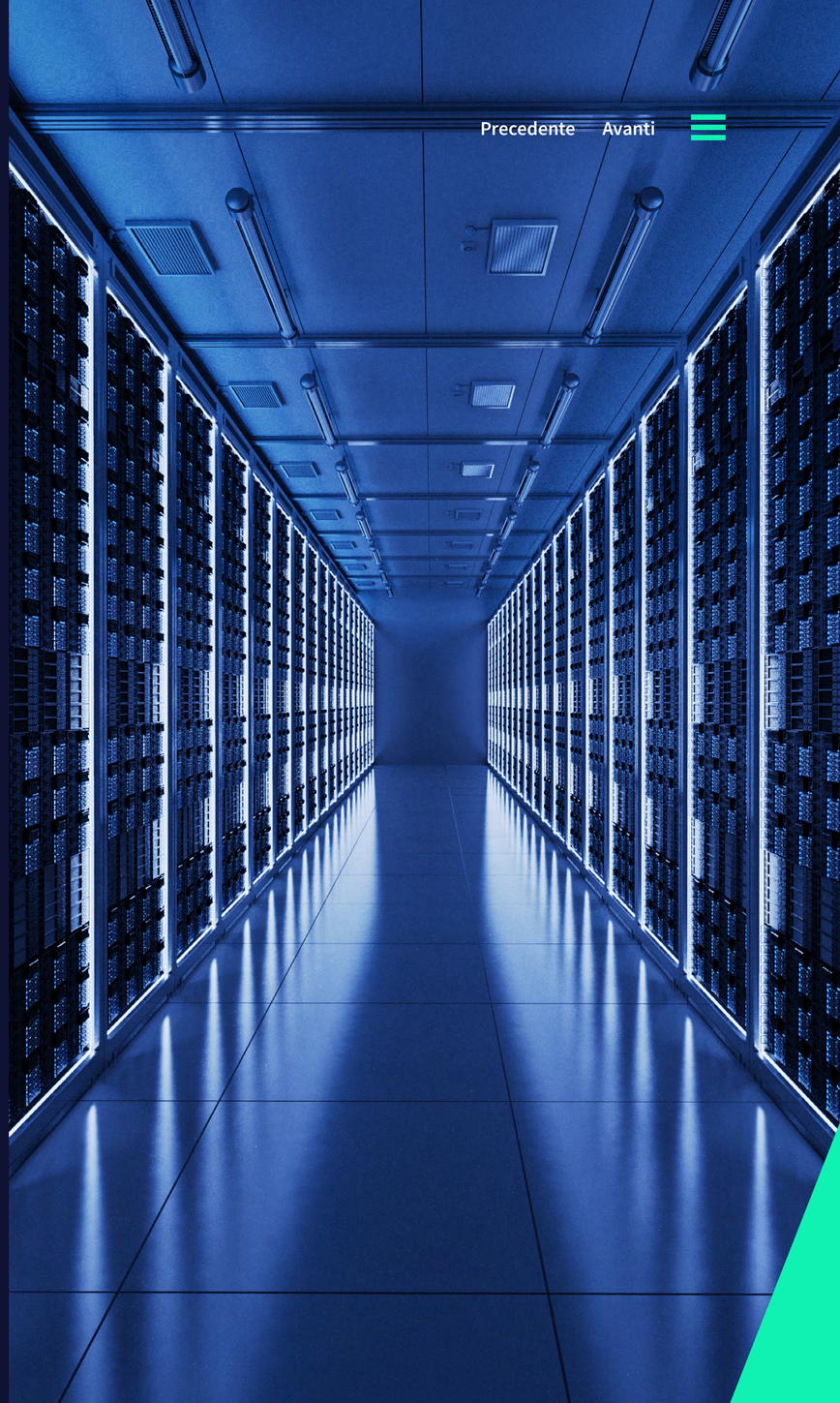
Sia che stiate integrando l'IA nelle operazioni aziendali o che stiate fornendo prodotti e servizi abilitati all'IA, la norma ISO 42001 vi aiuta a integrare i principi etici, a gestire i rischi e ad allinearvi alle aspettative globali sull'IA affidabile.

Gli elementi chiave dello standard includono:

- **Governance e responsabilità** – Definire ruoli, responsabilità e supervisione per le attività legate all'IA
- **Controlli basati sul rischio** – Identificare e affrontare i rischi durante l'intero ciclo di vita del sistema di IA
- **Trasparenza e spiegabilità** – Sostenere una comunicazione chiara di come i sistemi di IA funzionano e prendono decisioni
- **Miglioramento continuo** : utilizzare i dati di feedback, monitoraggio e performance per rafforzare gli obiettivi prefissati nel tempo

La ISO 42001 segue la struttura dell'Annex SL, rendendola facilmente integrabile con altri standard come la ISO 9001, la ISO 27001 o la ISO 45001, consentendo un approccio coerente e armonizzato alla gestione del rischio in tutta l'organizzazione.

Adottando la norma ISO 42001, le organizzazioni possono dimostrare un chiaro impegno per un'innovazione responsabile, creando fiducia con clienti, partner e autorità di regolamentazione in un mondo sempre più guidato dall'intelligenza artificiale.



Perché ottenere la certificazione?

La certificazione ISO 42001 è più di una formalità. È un marchio indipendente, riconosciuto a livello mondiale, che garantisce che la vostra organizzazione sta gestendo l'intelligenza artificiale in modo responsabile ed efficace.

Dimostra impegno verso le migliori pratiche
La certificazione segnala la serietà con cui si costruiscono sistemi di IA etici, trasparenti e ben governati, in linea con le aspettative internazionali.

Costruisce fiducia e credibilità con i clienti
Per molti settori, la certificazione sta diventando una licenza di commercio. Rassicura clienti, partner e stakeholder che le vostre pratiche di IA sono sicure, responsabili e ben gestite.

Supporta gli obiettivi di privacy, etica e sicurezza delle informazioni
Il processo di certificazione aiuta a integrare la governance dell'IA nei vostri sistemi di gestione del rischio più ampi, rafforzando la protezione dei dati, l'innovazione responsabile e la supervisione etica.

La conformità è a prova di futuro
Con l'accelerazione delle normative sull'IA a livello globale, la certificazione ISO 42001 aiuta a posizionare la vostra organizzazione in anticipo rispetto all'evoluzione dei requisiti legali e di settore, riducendo i rischi e sostenendo la resilienza a lungo termine.

Requisiti chiave della ISO 42001:

Allegato SL Struttura delle clausole

La struttura dell'Allegato SL dell'ISO è composta da dieci clausole. Tutti i contenuti di una norma di sistema di gestione, compresa la ISO 42001, devono soddisfare i criteri di tutte e dieci le clausole per seguire il quadro dell'Annex SL. Le clausole sono suddivise in categorie:

Clausola 1
Ambito di applicazione

Definisce i risultati previsti del sistema di gestione dell'IA e la sua applicabilità all'interno dell'organizzazione.

Clausola 2
Riferimenti normativi

Elenca gli standard di riferimento essenziali per l'applicazione della ISO 42001.

Clausola 3
Termini e definizioni

Fornisce le definizioni della terminologia di base utilizzata in tutto lo standard per garantire una comprensione condivisa.

Clausola 4
Contesto dell'organizzazione

Considera i fattori interni ed esterni, le aspettative degli stakeholder e l'ambito di utilizzo del sistema di IA.

Clausola 5
Leadership

Delinea la responsabilità del top management per le politiche, le risorse e la promozione di una cultura dell'IA responsabile.

Clausola 6
Pianificazione

Si occupa di come l'organizzazione identifica e risponde ai rischi e alle opportunità dell'IA e stabilisce gli obiettivi dell'IA.

Clausola 7
Supporto

Copre le risorse, la competenza, la consapevolezza, la comunicazione e la documentazione necessarie per una governance efficace.

Clausola 8
Operazione

Definisce come vengono implementati i controlli relativi all'IA, comprese le valutazioni dei rischi e dell'impatto del sistema.

Clausola 9
Valutazione delle prestazioni

Richiede monitoraggio, misurazione, audit interni e revisione della gestione per valutare le prestazioni del sistema.

Clausola 10
Miglioramento

Descrive l'approccio dell'organizzazione al miglioramento continuo, alla gestione delle non conformità e alle azioni correttive.

Nella maggior parte dei casi, queste clausole utilizzano un testo di base identico, indipendentemente dallo standard a cui sono applicate, e condividono termini e definizioni comuni per promuovere la coerenza e la compatibilità tra gli standard dei sistemi di gestione. Per la ISO 42001, ciò garantisce che la governance dell'IA sia inserita in una struttura di sistema di gestione familiare e collaudata.

Affrontare i requisiti della norma ISO 42001 nel contesto dell'IA

Come altri standard di sistema di gestione ISO, la ISO 42001 è costruita attorno alle clausole da 4 a 10, che coprono aree come il contesto, la leadership, la pianificazione, il supporto e il miglioramento continuo. Ciò che rende unica la ISO 42001 è il modo in cui questi concetti familiari vengono adattati alle sfide e ai rischi associati all'intelligenza artificiale.

Le sezioni seguenti riassumono le modalità di applicazione delle clausole nel contesto dell'IA, dalla governance etica alla trasparenza dei dati, dalla gestione del rischio alla supervisione del ciclo di vita.

Contesto dell'organizzazione

La norma ISO 42001 chiede alle organizzazioni di definire l'ambito del loro sistema di gestione dell'IA comprendendo il loro contesto interno ed esterno. Questo include gli obblighi di legge, i rischi dell'IA specifici del settore, le norme culturali ed etiche, le aspettative degli stakeholder e il ruolo dell'organizzazione nel ciclo di vita dell'IA – sia come sviluppatore, che come implementatore o utente. Queste conoscenze determinano il modo in cui l'IA viene governata e contribuiscono a determinare quali controlli sono rilevanti. Le organizzazioni sono inoltre incoraggiate a valutare se questioni sociali più ampie, come il cambiamento climatico o l'equità digitale, debbano informare il loro approccio.

Leadership e governance

Un requisito fondamentale della ISO 42001 è l'impegno visibile e duraturo della leadership per un uso responsabile dell'IA. L'alta direzione deve stabilire una chiara politica in materia di IA, fissare obiettivi allineati ai valori organizzativi e garantire la definizione di ruoli e responsabilità nell'intero ciclo di vita dell'IA. Ciò include il mantenimento della supervisione delle valutazioni del rischio, delle valutazioni d'impatto e dell'uso dell'IA, in particolare in contesti sensibili o ad alto rischio. L'impegno attivo dei vertici aziendali contribuisce a garantire che la governance sia integrata in tutta l'azienda, e non venga trattata come un ripensamento.

Etica e trasparenza

Le considerazioni etiche sono incorporate in tutto il percorso ISO 42001. Le organizzazioni devono dimostrare come valutano e affrontano i potenziali impatti dell'IA sugli individui e sulla società. Ciò include la considerazione dell'equità, della non discriminazione e dell'autonomia umana, nonché della privacy dei dati e della trasparenza dei risultati. Devono essere predisposti controlli per identificare e mitigare le conseguenze indesiderate e le prove di queste pratiche devono essere documentate, monitorate e aggiornate regolarmente.

Gestione dei rischi e delle opportunità

Le organizzazioni sono tenute a valutare e trattare i rischi specifici dell'IA, compresi quelli che riguardano la conformità, la reputazione e la sicurezza, identificando al contempo le opportunità di innovazione e miglioramento. La ISO 42001 riconosce che la propensione al rischio e le definizioni possono variare a seconda del settore, pertanto il quadro di riferimento è adattabile. L'importante è che le decisioni siano prese consapevolmente, guidate dalla politica e valutate nel tempo per verificarne l'efficacia.

Miglioramento continuo

La ISO 42001 segue il modello Plan-Do-Check-Act (PDCA). Ciò significa che il miglioramento continuo non è facoltativo, ma è intrinseco. Le organizzazioni devono monitorare le prestazioni del proprio sistema di IA, condurre audit interni e rivedere regolarmente i processi di governance. Che si tratti di un'azione correttiva o di un adeguamento alle modifiche normative, l'obiettivo è migliorare costantemente l'idoneità, l'adeguatezza e l'efficacia del sistema di gestione dell'IA.

ISO 42001 Allegato A Controlli

Tradurre l'IA responsabile in azione

Oltre alle 10 clausole principali, la norma ISO 42001 include una serie di obiettivi di controllo di supporto nell'Allegato A. Questi controlli sono concepiti per aiutare le organizzazioni a implementare misure pratiche e verificabili che supportino lo sviluppo e l'utilizzo affidabile dell'IA.

Strutturati in 10 categorie, i controlli dell'Allegato A riguardano:

- **Politiche relative all'IA** : garantire una direzione e un intento chiari da parte della leadership
- **Organizzazione interna** – definizione dei ruoli e delle responsabilità di governance
- **Risorse** – gestione di strumenti, dati e infrastrutture utilizzati nell'IA
- **Valutazioni d'impatto** – valutare i rischi per gli individui e la società
- **Supervisione del ciclo di vita** : allineare la progettazione del sistema agli obiettivi etici e normativi
- **Dati per i sistemi di IA** : garantire qualità, provenienza e rilevanza
- **Informazioni per le parti interessate** – promuovere la trasparenza e la responsabilità
- **Utilizzo del sistema di IA** – gestione dell'ambito, degli intenti e delle salvaguardie
- **Rapporti con le terze parti** : definire le aspettative per i fornitori e i partner
- **Documentazione e tracciabilità** – a supporto della spiegabilità e dell'audit

Queste aree di controllo costituiscono la base pratica per l'implementazione della ISO 42001. Possono essere adattate a diversi livelli di maturità e complessità dell'IA e costituiscono una parte fondamentale delle valutazioni di preparazione e della certificazione.

Attuazione della norma ISO 42001

Aree di interesse per l'operatività del sistema di gestione dell'IA

La norma ISO 42001 fornisce un quadro di riferimento per l'implementazione di pratiche di gestione dell'IA responsabili ed efficaci, utilizzando il modello Plan-Do-Check-Act (PDCA) – una base fondamentale condivisa da tutti gli standard ISO basati sull'Annex SL.

Lo standard supporta lo sviluppo di un Sistema di Gestione dell'Intelligenza Artificiale (AIMS) attraverso processi di gestione interconnessi, tra cui:

- **Consapevolezza**

  Le organizzazioni devono creare consapevolezza formando i team a comprendere i vantaggi, i rischi e le considerazioni etiche dell'IA, dagli sviluppatori ai responsabili delle decisioni.

- **Responsabilità**

  Devono essere assegnati ruoli e responsabilità chiaramente definiti, assicurando che la governance dell'IA sia compresa e incorporata in tutto il ciclo di vita del sistema

- **Risposta**

  Dovrebbe esserci un'azione tempestiva e coordinata per gestire i rischi, rispondere agli impatti del sistema di IA e applicare azioni correttive laddove necessario.

- **Valutazione del rischio**

  I rischi associati ai sistemi di IA – tra cui guasti tecnici, esiti indesiderati o uso improprio – devono essere valutati in modo strutturato e basato su prove.

- **Progettazione e sviluppo del sistema**

  I sistemi di IA devono essere sviluppati e distribuiti in linea con politiche e processi documentati, sostenendo l'uso etico, la trasparenza e la responsabilità del ciclo di vita.

- **Governance e controllo**

  Le organizzazioni dovrebbero adottare un approccio olistico alla gestione dell'IA, che comprenda la qualità dei dati, la spiegabilità, l'equità, l'affidabilità e la supervisione umana.

- **Rivalutazione e miglioramento continuo**

  Nell'ambito del modello PDCA, le prestazioni devono essere monitorate e riviste regolarmente. Gli audit interni e le revisioni della gestione aiutano a garantire che l'AIMS continui a raggiungere gli obiettivi e si adatti ai rischi e alle normative emergenti.

Costruire la vostra roadmap con la ISO 42001

Gettare le basi per una governance efficace dell'IA

L'implementazione della ISO 42001 inizia con una chiarezza di intenti e un forte sostegno da parte della leadership. Questi primi passi aiutano a garantire che il sistema di gestione dell'IA (AIMS) sia pratico e allineato agli obiettivi dell'organizzazione.

1. Ottenere l'impegno della leadership

L'alta dirigenza deve guidare gli AIMS, stabilendo obiettivi chiari che definiscano l'aspetto del successo per l'organizzazione. Che si tratti di migliorare la supervisione, di soddisfare le aspettative normative o di creare fiducia, la leadership deve assegnare le risorse e la direzione necessarie per incorporare l'uso responsabile dell'IA in tutta l'azienda.

2. Comprendere il contesto dell'IA

Valutare il modo in cui l'IA viene sviluppata, implementata o utilizzata nella vostra organizzazione. Considerate gli obblighi di legge, i rischi specifici del settore e le aspettative degli stakeholder. Questa comprensione dovrebbe informare le vostre risorse, compresi il tempo, le competenze e il budget necessari per gestire l'IA in modo responsabile ed efficace.

3. Valutare i requisiti di formazione

La governance dell'IA si estende ai settori tecnico, etico, legale e operativo. Coinvolgete i team interfunzionali e assicurate una formazione su misura, dalla sensibilizzazione per i team più ampi alla formazione sulla revisione per gli specialisti. La creazione di capacità trasversali ai ruoli è fondamentale per un'implementazione efficace e scalabile.

4. Definire l'ambito AIMS

Chiarite quali sono i team, i sistemi e le aree geografiche che copriranno il vostro AIMS, compresi l'IA sviluppata internamente, gli strumenti di terze parti e i casi d'uso ad alto rischio. Un ambito ben definito manterrà la vostra governance focalizzata e adatta allo scopo.

5. Pianificare e attuare gli obiettivi prefissati

Sviluppare un piano di implementazione realistico che comprenda tempistiche, responsabilità e risorse necessarie. Introdurre i controlli, la documentazione e i processi di governance necessari. Prevedere revisioni periodiche, cicli di feedback e monitoraggio delle prestazioni per garantire che l'AIMS si evolva con la vostra azienda e con il panorama dell'intelligenza artificiale.

6. Condurre un'analisi delle lacune

Esaminate i vostri attuali quadri di governance, rischio e conformità per identificare i punti in cui la vostra organizzazione è già conforme agli standard e le eventuali lacune o vulnerabilità. Questa analisi aiuterà a definire le priorità dei miglioramenti e a evitare duplicazioni.

7. Prenotate il vostro audit di certificazione

Una volta che il vostro AIMS è pronto, programmate l'audit di certificazione ISO 42001 con LRQA. Il nostro processo in due fasi valuterà la progettazione e l'implementazione del sistema, aiutandovi a dimostrare ai vostri interlocutori responsabilità, integrità e innovazione responsabile.

8. Incorporare il miglioramento continuo e la risposta

Un AIMS maturo non si limita all'implementazione iniziale, ma richiede meccanismi di apprendimento e miglioramento continuo. Stabilire cicli di feedback, verifiche regolari e metriche di performance per adattarsi all'evoluzione dei rischi e delle tecnologie dell'IA. Implementare un piano di risposta agli incidenti specifico per l'IA per garantire che gli errori, le distorsioni o i malfunzionamenti del sistema siano affrontati in modo rapido, trasparente ed efficace.

Integrazione della ISO 42001 con i sistemi di gestione esistenti

Costruire su ciò che sta già funzionando. Rafforzare la governance dell'IA e della sicurezza delle informazioni.

Per molte organizzazioni, la ISO 42001 non è un punto di partenza, ma un'estensione naturale. Se siete già in possesso della certificazione ISO 27001, siete in una posizione forte per integrare ISO 42001 in modo efficiente ed efficace.

La ISO 27001 fornisce un quadro comprovato per la gestione dei rischi legati alla sicurezza delle informazioni e i suoi controlli sulla riservatezza, l'integrità e la disponibilità dei dati supportano direttamente molti dei requisiti della ISO 42001. Combinando i due standard, è possibile creare un approccio di governance unificato che affronti i rischi legati alle informazioni e all'IA.

Perché l'integrazione ha senso

Struttura condivisa

La ISO 42001 segue il quadro dell'Annex SL, la stessa struttura di alto livello utilizzata in ISO 27001, ISO 9001, ISO 45001 e altre. Ciò consente di garantire la coerenza tra politica, leadership, pianificazione, funzionamento e valutazione.

Uso efficiente delle risorse

L'integrazione aiuta a ridurre la duplicazione di audit, documentazione e revisioni interne. I team possono allineare report, obiettivi e controlli, semplificando la conformità e migliorando la supervisione.

Gestione del rischio allineata

Entrambi gli standard richiedono un approccio basato sul rischio. Mentre la ISO 27001 si concentra sulle risorse informative, la ISO 42001 estende questo approccio ai sistemi di IA, compreso il modo in cui i dati vengono utilizzati per addestrarli, convalidarli e farli funzionare.

Maggiore resilienza del sistema

Un approccio integrato rende più facile individuare i problemi sistemici, risolverli in modo olistico e dimostrare a clienti, autorità di regolamentazione e partner un modello di governance unito.

I nostri servizi ISO 42001

Formazione

Sviluppate la vostra conoscenza della norma ISO 42001 con una serie di corsi progettati per diversi livelli di esperienza, erogati con diversi stili di apprendimento.

Visualizza i corsi disponibili

Analisi delle lacune

Un servizio opzionale in cui uno dei nostri auditor esperti vi aiuterà a identificare le aree critiche, ad alto rischio o deboli del vostro sistema prima della certificazione.

Certificazione

Valutiamo il vostro Sistema di Gestione dell'IA (AIMS) in linea con i requisiti della norma ISO 42001.

Valutazioni integrate

Se avete implementato più sistemi di gestione, potreste trarre vantaggio da un programma integrato di audit e sorveglianza: un modo più efficiente ed economico di gestire il rischio.

Perché lavorare con noi?

LRQA aiuta le organizzazioni a sviluppare programmi di gestione del rischio solidi e pronti per il futuro, che consentano l'adozione sicura, responsabile ed efficace dell'IA e della tecnologia.

Dalla garanzia di conformità alle normative sull'IA in continua evoluzione al rafforzamento della sicurezza dei dati e all'integrazione delle best practice nella governance, forniamo la garanzia necessaria per guidare l'innovazione con fiducia, aiutando le aziende a integrare l'IA e la tecnologia gestendo i rischi in modo proattivo.

Competenza sul campo

Le nostre soluzioni sono fornite da un team globale di esperti specializzati in cybersecurity, conformità e gestione del rischio della catena di approvvigionamento, che vi aiutano a gestire i rischi legati all'IA, a soddisfare i requisiti normativi in evoluzione e a integrare pratiche responsabili di IA nelle vostre operazioni.

Garanzia continua

I rischi legati all'intelligenza artificiale richiedono una supervisione continua. Il nostro approccio alla gestione del rischio in tempo reale consente di risolvere i problemi in modo proattivo, riducendo le interruzioni dell'attività e migliorando la resilienza. Il nostro portafoglio connesso di soluzioni di gestione del rischio aiuta le aziende ad andare oltre i requisiti normativi e a integrare la gestione del rischio dell'IA nelle operazioni quotidiane.

Partnership basate su soluzioni

Non ci limitiamo a certificare, ma lavoriamo al vostro fianco per integrare la governance dell'IA nella vostra più ampia strategia di rischio e conformità. Il nostro approccio personalizzato garantisce che l'IA e la tecnologia contribuiscano a guidare una crescita sostenibile, soddisfacendo al contempo le aspettative legali ed etiche in continua evoluzione.

Processo decisionale basato sui dati

Sfruttiamo piattaforme digitali e analitiche per fornire approfondimenti sui rischi legati all'IA in tutta l'azienda. La nostra intelligenza umana, potenziata da strumenti basati sui dati, aiuta le organizzazioni a identificare le vulnerabilità, a prevedere i rischi futuri e a prendere decisioni informate con fiducia.

Informazioni su LRQA

LRQA è il principale partner globale per l'assurance, che riunisce decenni di esperienza impareggiabile nei servizi di valutazione, supporto tecnico, ispezione e servizi di cybersecurity..

Le nostre partnership basate su soluzioni sono supportate da approfondimenti basati sui dati che aiutano i nostri clienti a risolvere le loro maggiori sfide aziendali. Presenti in oltre 150 Paesi con un team di oltre 5.000 persone, i pluripremiati specialisti di LRQA in materia di compliance, supply chain, cybersecurity ed ESG aiutano più di 61.000 clienti in quasi tutti i settori ad anticipare, mitigare e gestire il rischio ovunque essi operino.

In tutto ciò che facciamo, ci impegniamo a dare forma a un futuro migliore per il nostro personale, i nostri clienti, le nostre comunità e il nostro pianeta.

Contattate

Per ulteriori informazioni, visitare il sito **lrqa.com/it-it/** o inviare un'e-mail a **certificazione@lrqa.com**

LRQA Italy
Viale Monza 259/265
First Floor
Milan, Italy 20126
+39 02 30551200