



**POLITICA
DELLA QUALITÀ, DELLA SICUREZZA
DELLE INFORMAZIONI E DELL'INTELLIGENZA ARTIFICIALE**

(cfr. cap. 5 – ISO 9001:2015, ISO 27001:2022 – ISO 27017:2015 - ISO 27018:2025 – ISO 42011:2023)

L'erogazione di servizi di qualità, la sicurezza e la salvaguardia del patrimonio informativo e la gestione responsabile e sicura di Sistemi di Intelligenza Artificiale costituiscono condizione imprescindibile per il raggiungimento degli obiettivi di business di K2K.

Il Sistema di Gestione Qualità, Intelligenza Artificiale e Sicurezza delle Informazioni (Sistema di Gestione Integrato - SGI) rappresenta lo strumento che consente il raggiungimento degli obiettivi dell'Organizzazione per la qualità, la sicurezza delle informazioni e per l'Intelligenza artificiale. Il SGI consente l'individuazione di corrette best practice e/o best in class per il miglioramento costante della qualità aziendale, la condivisione delle informazioni, lo svolgimento di operazioni corrette e la riduzione dei rischi connessi alle informazioni e ai sistemi di IA a livelli accettabili.

In considerazione di ciò, lo svolgimento delle attività aziendali deve sempre avvenire garantendo adeguati livelli di disponibilità, integrità e riservatezza delle informazioni, nonché la produzione responsabile, trasparente e affidabile dei Sistemi di Intelligenza Artificiale, attraverso l'adozione di un formale "Sistema di Gestione della Qualità, Sicurezza delle Informazioni e Intelligenza Artificiale" (Sistema di Gestione Integrato - SGI) in linea con i requisiti attesi dagli stakeholder di K2K.

In particolare, il Sistema di Gestione della Qualità, Sicurezza delle Informazioni e Intelligenza Artificiale è applicato a:

*«Produzione, Progettazione, Commercializzazione, Avvio Operativo e
Supporto di Architetture di Reti Neurali basate su Modelli Fondativi
di Intelligenza Artificiale, Vision Language Models, Agenti AI e delle
relative Piattaforme per privati e Pubblica Amministrazione erogati
in modalità Cloud Software as a Service, On Premises e Ibrida.»*

K2K è un'azienda di Intelligenza Artificiale che si occupa di ricerca e sviluppo di Architetture Neurali capaci di produrre reti generative e predittive. La nostra mission è l'agevolazione dell'introduzione di servizi digitali per i nostri clienti, con l'obiettivo di intraprendere un percorso digitale che possa accompagnare queste realtà nella trasformazione tecnologica.



**POLITICA
DELLA QUALITÀ, DELLA SICUREZZA
DELLE INFORMAZIONI E DELL'INTELLIGENZA ARTIFICIALE**

(cfr. cap. 5 – ISO 9001:2015, ISO 27001:2022 – ISO 27017:2015 - ISO 27018:2025 – ISO 42011:2023)

K2K persegue una gestione integrata della Qualità, della Sicurezza delle Informazioni e dell'Intelligenza Artificiale responsabile, adottando un approccio sistemico e orientato al miglioramento continuo.

Eccellenza nella qualità dei servizi e miglioramento continuo

K2K si impegna a dimostrare ai propri stakeholder la capacità di erogare servizi di qualità superiore, basati su processi chiaramente definiti, documentati e costantemente monitorati. L'organizzazione adotta metodologie strutturate per il miglioramento continuo, garantendo che ogni attività sia pianificata, eseguita e verificata secondo standard rigorosi che assicurino l'efficacia e l'efficienza delle prestazioni.

Affidabilità e sicurezza dei servizi erogati

K2K vuole dimostrare ai clienti la propria capacità di fornire con regolarità servizi sicuri, affidabili e performanti, attraverso la gestione proattiva delle criticità e il mantenimento di elevati standard di servizio.

Sicurezza dei servizi cloud

K2K integra le estensioni ISO 27017:2015 e 27018:2025 nel proprio Sistema di Gestione Integrato per garantire una gestione responsabile dei servizi cloud, agendo sia come erogatore diretto che come utilizzatore di infrastrutture terze. In particolare, l'organizzazione opera con la priorità di garantire la protezione dei dati personali, la configurazione sicura delle piattaforme, la massima continuità dei servizi erogati, servendosi di attente valutazioni per la selezione dei partner e supportando le proprie scelte da clausole contrattuali rigorose.

Protezione delle informazioni

K2K si impegna a minimizzare il rischio di perdita, compromissione e/o indisponibilità dei dati dei clienti attraverso la pianificazione e la gestione di attività specifiche volte a garantire la continuità di servizio e la protezione integrale del patrimonio informativo. L'organizzazione adotta un approccio strutturato basato sui tre pilastri fondamentali della sicurezza delle informazioni: disponibilità, integrità e riservatezza.

Gestione proattiva dei rischi

K2K conduce un'analisi continua e strutturata dei rischi connessi alla sicurezza delle informazioni, alla qualità dei servizi e alla gestione dell'intelligenza artificiale, esaminando sistematicamente le vulnerabilità tecniche e organizzative, le minacce interne ed esterne,



**POLITICA
DELLA QUALITÀ, DELLA SICUREZZA
DELLE INFORMAZIONI E DELL'INTELLIGENZA ARTIFICIALE**

(cfr. cap. 5 – ISO 9001:2015, ISO 27001:2022 – ISO 27017:2015 - ISO 27018:2025 – ISO 42011:2023)

nonché le opportunità di miglioramento associate alle attività a cui si applica il Sistema di Gestione Integrato. Tale analisi, basata su metodologie riconosciute a livello internazionale, viene aggiornata periodicamente e ogni volta che si verificano cambiamenti significativi nel contesto tecnologico, normativo, operativo o competitivo, consentendo all'organizzazione di identificare tempestivamente le minacce emergenti, valutarne la probabilità e l'impatto potenziale, così da adottare misure mitigative proporzionate e efficaci.

Sviluppo responsabile dell'Intelligenza Artificiale

K2K garantisce lo sviluppo responsabile dell'Intelligenza Artificiale attraverso l'adozione di procedure chiare, documentate e verificabili che disciplinano tutte le fasi del ciclo di vita dei sistemi di IA.

Utilizzo controllato dell'Intelligenza Artificiale

K2K assicura un utilizzo responsabile e limitato dell'Intelligenza Artificiale mediante l'implementazione di linee guida chiare, prevenendo usi impropri degli strumenti.

Competenza e formazione continua del personale

K2K assicura che gli specialisti coinvolti nello sviluppo, nella validazione e nella messa in produzione dei Sistemi di IA dispongano delle competenze necessarie attraverso programmi di formazione sul campo, aggiornamento professionale e sviluppo delle capacità tecniche.

Qualità e integrità dei dati

K2K si pone come obiettivo primario la qualità dei dati coinvolti nel ciclo di vita dell'Intelligenza Artificiale, assicurando accuratezza, completezza, pertinenza e monitorando costantemente l'assenza di bias discriminatori. Vengono implementati processi di validazione, pulizia e monitoraggio dei dataset per prevenire distorsioni che potrebbero compromettere l'equità e l'affidabilità dei risultati prodotti dai sistemi di IA.

Valutazione d'impatto dei Sistemi di IA

K2K opera una gestione responsabile dei Sistemi di Intelligenza Artificiale, adottando un approccio che bilancia innovazione tecnologica e responsabilità sociale, assicurando che i benefici dell'IA siano massimizzati e i potenziali rischi adeguatamente mitigati.



**POLITICA
DELLA QUALITÀ, DELLA SICUREZZA
DELLE INFORMAZIONI E DELL'INTELLIGENZA ARTIFICIALE**

(cfr. cap. 5 – ISO 9001:2015, ISO 27001:2022 – ISO 27017:2015 - ISO 27018:2025 – ISO 42011:2023)

Trasparenza

K2K sviluppa e gestisce i Sistemi di Intelligenza Artificiale nel segno della trasparenza, della reperibilità documentale e della tracciabilità completa, consentendo verifiche e audit quando richiesto.

Protezione dei dati personali

K2K garantisce la tutela della privacy e la protezione dei dati personali, assicurando che tutti i trattamenti derivanti dall'utilizzo dell'Intelligenza Artificiale rispettino il Regolamento Generale sulla Protezione dei Dati (GDPR) e i principi di minimizzazione, liceità, correttezza, trasparenza e limitazione delle finalità. Vengono implementate misure tecniche e organizzative appropriate per proteggere i diritti e le libertà degli interessati.

Sicurezza, robustezza e manutenibilità dei Sistemi

K2K garantisce la sicurezza, la robustezza e la manutenibilità dei propri Sistemi attraverso l'adozione di pratiche di sviluppo sicuro, test rigorosi e monitoraggio continuo, prevenendo vulnerabilità, minacce informatiche e attacchi che potrebbero compromettere l'integrità, la disponibilità o la riservatezza dei sistemi e dei dati trattati.

Conformità normativa e contrattuale

K2K si impegna a rispettare i requisiti contrattuali assunti con i clienti e le parti interessate, nonché le norme tecniche di riferimento, in particolare le ISO/IEC 9001:2015, ISO/IEC 27001:2022 con le relative estensioni 27017 e 27018, ISO/IEC 42001:2023, così come la conformità alle leggi vigenti, in particolare le norme di settore. La conformità viene verificata attraverso audit periodici.

Collaborazione con la catena di fornitura

K2K promuove attivamente la collaborazione, la comprensione e la consapevolezza del Sistema di Gestione Integrato da parte di fornitori strategici e partner commerciali, estendendo i propri principi di qualità, sicurezza e responsabilità lungo tutta la catena del valore. K2K seleziona e valuta i propri fornitori anche in base alla loro capacità di aderire agli standard e ai valori dell'organizzazione, favorendo relazioni di partnership basate su fiducia, trasparenza e obiettivi condivisi.



**POLITICA
DELLA QUALITÀ, DELLA SICUREZZA
DELLE INFORMAZIONI E DELL'INTELLIGENZA ARTIFICIALE**

(cfr. cap. 5 – ISO 9001:2015, ISO 27001:2022 – ISO 27017:2015 - ISO 27018:2025 – ISO 42011:2023)

Coinvolgimento e impegno dell'organizzazione

Tutta l'azienda, a ogni livello gerarchico e funzionale, unitamente ai suoi partner strategici e fornitori, è attivamente coinvolta e responsabilizzata nella segnalazione tempestiva di eventuali non conformità rispetto ai risultati attesi per la qualità dei servizi erogati e per la gestione responsabile ed etica dei sistemi di intelligenza artificiale, nella notifica immediata di incidenti di sicurezza delle informazioni (quali violazioni dei dati, accessi non autorizzati, perdite di disponibilità o compromissioni dell'integrità), nonché nell'identificazione proattiva di qualsiasi debolezza, vulnerabilità o opportunità di miglioramento rilevata nel Sistema di Gestione Integrato.

Tutto il personale si impegna concretamente nel supportare l'implementazione efficace delle politiche e delle procedure, la messa in opera dei controlli di sicurezza e qualità, il riesame periodico delle prestazioni del sistema attraverso audit interni e valutazioni, e il miglioramento continuo dei processi mediante la partecipazione attiva a iniziative di innovazione, formazione e condivisione delle conoscenze.

Il vertice aziendale assume la responsabilità diretta e dimostrabile di perseguire, con l'allocazione di mezzi adeguati, risorse competenti e il proprio coinvolgimento personale nelle decisioni strategiche, gli obiettivi definiti in questa politica, con il fine ultimo e prioritario del miglioramento continuo della qualità del proprio operato, dell'eccellenza nell'erogazione dei servizi, della sicurezza e riservatezza delle informazioni trattate, e dello sviluppo di sistemi di intelligenza artificiale affidabili, trasparenti e rispettosi dei diritti fondamentali, garantendo così la fiducia di clienti, stakeholder e della società nel suo complesso.

