

LOGO AZIENDA	SOP-09: Procedura la valutazione dei rischi e dell'impatto dell'intelligenza artificiale	Verificato da: Approvato da:
--------------	---	---------------------------------

1. Scopo

Lo scopo della presente procedura è quello di stabilire un approccio strutturato per condurre **valutazioni dei rischi e dell'impatto dell'IA (AI-RIA)** all'interno di **NOME AZIENDA**. Ciò garantisce la conformità alla norma **ISO/IEC 42001:2023**, promuove una governance responsabile dell'IA e mitiga i potenziali rischi legati ai sistemi di IA.

2. Ambito

La presente procedura si applica a tutti i progetti, modelli e sistemi di IA all'interno di **NOME AZIENDA** durante il loro **intero ciclo di vita**, coprendo:

- Progettazione, sviluppo e implementazione di sistemi di IA
- **Rischi etici, di sicurezza e di conformità** relativi all'IA
- Monitoraggio dei sistemi di IA e strategie di mitigazione dei rischi

3. Responsabilità

- **Team di governance dell'IA:** supervisiona le valutazioni dei rischi dell'IA e garantisce la conformità.
- **Team Rischi e conformità dell'IA:** conduce analisi dei rischi e valutazioni dell'impatto.
- **Team di sviluppo e implementazione dell'IA:** implementa strategie di mitigazione dei rischi nei sistemi di IA.
- **Responsabile della protezione dei dati (DPO) e team per la sicurezza informatica:** garantiscono la conformità in materia di privacy e sicurezza dei dati.

4. Fasi della procedura

Fase 1: Identificare i rischi dell'IA e i potenziali impatti

- **Classificare i rischi** in base alla funzione del sistema di IA, al settore e ai requisiti normativi.
- Identificare i **potenziali rischi legati all'IA**, tra cui:
 - **Rischi etici:** problemi di parzialità, equità, trasparenza e responsabilità
 - **Rischi per la sicurezza:** minacce alla sicurezza informatica, attacchi ostili
 - **Rischi per la privacy:** violazioni della protezione dei dati (conformità al GDPR e al CCPA)

LOGO AZIENDA	SOP-09: Procedura la valutazione dei rischi e dell'impatto dell'intelligenza artificiale	Verificato da: Approvato da:
--------------	---	---------------------------------

- **Rischi operativi:** errori dei modelli, previsioni inaccurate o problemi di prestazioni
- **Rischi legali e di conformità:** non conformità alle normative specifiche del settore relative all'IA

Fase 2: Condurre un'analisi dei rischi e una valutazione dell'impatto

- **Valutare la probabilità e la gravità dei rischi** utilizzando una matrice di valutazione dei rischi.
- Valutare i potenziali **impatti sociali, economici e legali** dei guasti dell'IA.
- Utilizzare modelli di valutazione dei rischi quali:
 - **Modellizzazione delle minacce dell'IA:** identificazione delle vulnerabilità nei modelli di IA
 - **Analisi dei modi e degli effetti dei guasti (FMEA):** valutazione degli impatti dei guasti dell'IA
 - **Test di distorsione algoritmica:** valutazione dell'equità e della non discriminazione nei risultati dell'IA

Fase 3: Implementare strategie di mitigazione del rischio

- Definire **piani di trattamento dei rischi**, tra cui:
 - Meccanismi di rilevamento e mitigazione dei pregiudizi
 - Tecniche robuste di test, convalida e spiegabilità dell'IA
 - Strategie sicure di implementazione dei modelli di IA
 - Governance dei dati dell'IA e controlli di accesso

Fase 4: Documentare i risultati relativi ai rischi e le misure di conformità

- Mantenere un **registro dei rischi dell'IA** per tenere traccia dei rischi identificati e delle azioni di mitigazione.
- Assicurarsi che le valutazioni dei rischi dell'IA siano in linea con i requisiti di conformità normativa.
- Documentare i livelli di rischio dei sistemi di IA e la trasparenza del processo decisionale.

Fase 5: Monitorare i rischi dell'IA e condurre revisioni periodiche

- Stabilire un **monitoraggio continuo** dei rischi e delle anomalie del sistema di IA.
- Condurre **audit periodici sui rischi dell'IA** (ogni anno o dopo importanti aggiornamenti del sistema).
- Aggiornare le politiche di gestione dei rischi dell'IA in base **alle minacce emergenti e alle modifiche normative**.

LOGO AZIENDA	SOP-09: Procedura la valutazione dei rischi e dell'impatto dell'intelligenza artificiale	Verificato da: Approvato da:
--------------	---	---------------------------------

5. Conformità e miglioramento continuo

- Le valutazioni dei rischi dell'IA saranno **riviste annualmente** per garantire la conformità continua alla norma **ISO/IEC 42001:2023**.
- Le politiche di governance dell'IA saranno aggiornate sulla base delle **nuove scoperte in materia di rischi e delle migliori pratiche del settore**.

6. Documenti correlati

- /FORM -00010 (Analisi della valutazione dei rischi)