AGID | Agenzia per l'Italia Digitale

Linee guida per l'IA nella pubblica amministrazione

Termini e definizioni

Strumento A

Versione 1.0 del 11.03.2026 – Pubblicazione in consultazione pubblica.

Indice

Premessa

Considerata la velocità dell'innovazione, le Linee guida per l'IA nella pubblica amministrazione intendono garantire un adattamento costante ai cambiamenti imposti dall'incessante rivoluzione digitale. Di qui la scelta di corredare le Linee guida di "Strumenti", ovvero documenti a supporto dell'attività operativa di applicazione delle Linee guida.

L'elenco aggiornato degli strumenti delle Linee guida IA è disponibile al link: <<da definire in fase di pubblicazione>>.

Gli Strumenti potranno essere periodicamente aggiornati per tener conto dell'evoluzione normativa e tecnologica e delle buone pratiche emergenti.

A – Termini e definizioni

Il presente documento definisce i principali termini utilizzati nelle Linee Guida per lo sviluppo e il procurement di sistemi di Intelligenza Artificiale nella Pubblica Amministrazione.

Le definizioni sono formulate in coerenza con gli standard internazionali, in particolare:

- ISO/IEC 22989:2022 — Artificial Intelligence — Concepts and terminology
- ISO/IEC 23053:2022 — Framework for AI systems using machine learning
- ISO/IEC 23894:2023 — Artificial Intelligence — Risk management
- ISO/IEC 42001:2023 — Artificial Intelligence — Management system
- ISO/IEC 24029-1:2021 — Assessment of robustness of neural networks
- ISO 31000:2018 — Risk management — Guidelines
- ISO 9000:2015 — Quality management systems — Fundamentals and vocabulary
- ISO/IEC 25010:2011 — Systems and software quality models
- ISO/IEC 25012:2008 — Data quality model
- ISO/IEC 42010:2011 — Architecture description
- ISO/IEC 17788:2014 — Cloud computing — Overview and vocabulary
- ISO/IEC 19086-1:2016 — Cloud Service Level Agreement framework
- ISO/IEC 27001:2022 — Information security management systems
- ISO/IEC 27005:2022 — Information security risk management
- ISO/IEC 24760-1:2019 — Identity management
- ISO 20400:2017 — Sustainable procurement
- ISO 15686-5:2017 — Life-cycle costing
- ISO 22301:2019 — Business continuity management systems
- ISO/IEC 2382:2015 — Information technology — Vocabulary
- NIST AI Risk Management Framework 1.0 (2023)
- NIST SP 800-207 (2020) — Zero Trust Architecture

Ove pertinente, la terminologia è armonizzata con il Regolamento (UE) 2024/1689 sull'Intelligenza Artificiale (AI Act), il Regolamento (UE) 2016/679 GDPR e con la normativa nazionale in materia di intelligenza artificiale: Legge 132/2025.

In caso di divergenza interpretativa, prevalgono le definizioni contenute negli standard ISO/IEC applicabili e nella normativa europea vigente.

Il documento di Termini e definizioni ha finalità di uniformità terminologica e non sostituisce le definizioni giuridiche contenute nelle fonti normative primarie.

A. CONCETTI GENERALI DI IA

1. **Sistema di Intelligenza Artificiale (AI System)**

   Sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.

   Fonte: Regolamento (UE) 2024/1689 (AI Act), art. 3, punto 1.

2. **Modello di Intelligenza Artificiale (AI model)**

   Rappresentazione computazionale risultante da un processo di addestramento, che codifica relazioni apprese dai dati e che è utilizzata per generare output quali previsioni, raccomandazioni, classificazioni o contenuti a partire da dati di input.

   Fonte: ISO/IEC 22989:2022 — Artificial intelligence — Concepts and terminology.

3. **Modello di IA per finalità generali (General-purpose AI model)**

   Modello di intelligenza artificiale, anche qualora addestrato su larga scala mediante auto-supervisione e su grandi quantità di dati, che presenta un elevato grado di generalità ed è in grado di svolgere in modo competente un'ampia gamma di compiti distinti, indipendentemente dalle modalità di immissione sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati esclusivamente per attività di ricerca, sviluppo o prototipazione prima della loro immissione sul mercato.

   Fonte: Regolamento (UE) 2024/1689 (AI Act), art. 3, punto 63.

4. **Sistema di IA per finalità generali (General-purpose AI system)**

   Sistema di intelligenza artificiale basato su un modello di IA per finalità generali, avente la capacità di servire una pluralità di scopi, sia per uso diretto sia per l'integrazione in altri sistemi di intelligenza artificiale.

   Fonte: Regolamento (UE) 2024/1689 (AI Act), art. 3.

5. **Intelligenza artificiale (Artificial Intelligence, AI)**

   Disciplina che si occupa della realizzazione di sistemi in grado di svolgere compiti che richiederebbero intelligenza umana, quali apprendimento, ragionamento, percezione, comprensione del linguaggio o processo decisionale.

   Un sistema di IA è un sistema basato su macchina che, per obiettivi espliciti o impliciti, deduce dall'input ricevuto come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.

L'intelligenza artificiale comprende approcci simbolici, statistici e basati su apprendimento automatico.

Fonte: ISO/IEC 22989:2022 — Artificial Intelligence — Concepts and terminology; Regolamento (UE) 2024/1689 (AI Act), art. 3.

6. **IA statistica (Data-driven AI)**

   Approccio all'intelligenza artificiale fondato sull'analisi statistica dei dati e sull'apprendimento automatico, mediante il quale i modelli inferiscono regolarità, pattern o relazioni a partire da grandi quantità di dati.

   L'IA statistica si distingue dagli approcci simbolici basati su regole esplicite.

   Il Machine Learning e il Deep Learning costituiscono sottocategorie dell'IA statistica.

   Fonte: ISO/IEC 22989:2022; ISO/IEC 23053:2022.

7. **Machine Learning (Apprendimento automatico)**

   Approccio dell'intelligenza artificiale mediante il quale un sistema utilizza metodi computazionali per apprendere da dati, al fine di migliorare le proprie prestazioni rispetto a un compito definito, attraverso la determinazione o l'aggiornamento dei parametri di un modello secondo criteri specificati.

   Fonte: ISO/IEC 22989:2022 - Artificial intelligence - Concepts and terminology; ISO/IEC 23053:2022 - Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML).

8. **Rete neurale artificiale (Artificial Neural Network, ANN; Neural Network, NN)**

   Rete costituita da uno o più strati di neuroni artificiali interconnessi mediante collegamenti pesati con pesi regolabili, che riceve dati di input e produce un output.

   Sebbene la progettazione delle reti neurali sia stata inizialmente ispirata al funzionamento dei neuroni biologici, la maggior parte delle implementazioni attuali non riproduce direttamente tale modello biologico.

   Fonte: ISO/IEC 22989:2022 — Artificial intelligence — Concepts and terminology.

9. **Deep Learning (Apprendimento profondo)**

   Approccio all'intelligenza artificiale volto alla creazione di rappresentazioni gerarchiche complesse mediante l'addestramento di reti neurali con molteplici strati nascosti.

   Il Deep Learning costituisce una sottocategoria dell'apprendimento automatico (Machine Learning).

   Fonte: ISO/IEC 22989:2022 — Artificial intelligence — Concepts and terminology.

10. **IA generativa (Generative AI)**

    Categoria di sistemi di intelligenza artificiale in grado di generare nuovi contenuti quali testo, immagini, audio, codice o altri artefatti, sulla base di modelli addestrati su grandi quantità di dati.

    L'IA generativa utilizza tipicamente modelli di apprendimento automatico di grandi dimensioni, quali Large Language Model o modelli di diffusione.

    I sistemi di IA generativa possono essere impiegati per creazione di contenuti, supporto decisionale o automazione cognitiva.

    Nel contesto normativo europeo, taluni sistemi di IA generativa possono rientrare nella categoria dei modelli o sistemi di IA per finalità generali.

    Fonte: Coerente con ISO/IEC 22989:2022; Regolamento (UE) 2024/1689.

11. **Algoritmo (Algorithm)**

    Sequenza finita e ben definita di istruzioni formalizzate, eseguibili da un sistema computazionale, finalizzate alla trasformazione di input in output per la risoluzione di un problema o l'esecuzione di un compito.

    Fonte: ISO/IEC 22989:2022 — Artificial intelligence — Concepts and terminology.

12. **Addestramento (Training)**

    Processo mediante il quale un modello di intelligenza artificiale apprende dai dati, ottimizzando i propri parametri interni al fine di migliorare la capacità di generare output conformi agli obiettivi definiti.

    Fonte: ISO/IEC 22989:2022 — Artificial intelligence — Concepts and terminology.

13. **Inferenza (Inference)**

    Ragionamento mediante il quale si traggono conclusioni a partire da premesse note.

    Fonte: ISO/IEC 22989:2022 — Artificial intelligence — Concepts and terminology.

14. **Fine-tuning (messa a punto del modello)**

    Processo di addestramento ulteriore di un modello di intelligenza artificiale pre-addestrato, effettuato su un insieme di dati specifico di dominio o di applicazione, al fine di adattarne il comportamento o migliorarne le prestazioni rispetto a un caso d'uso determinato.

    Fonte: derivato da ISO/IEC 22989:2022 — concetti di training e model adaptation.

15. **Prompt**

    Input, espresso in forma testuale o in altra modalità strutturata, fornito a un modello di intelligenza artificiale generativo al fine di orientarne l'elaborazione e determinare la produzione di uno specifico output.

Il prompt può includere istruzioni, contesto, vincoli, esempi o parametri operativi.
Nel contesto dei modelli linguistici di grandi dimensioni, il prompt costituisce il principale meccanismo di interazione tra utente e modello.

Fonte: Derivato da ISO/IEC 22989:2022 (concetti di input e AI system); coerente con AI Act (sistemi generativi).

16. **Output generato (Generated output)**
Risultato prodotto da un sistema di intelligenza artificiale a seguito dell'elaborazione di dati di input, anche mediante inferenza, che può assumere la forma di previsione, classificazione, raccomandazione, decisione o contenuto.

Fonte: ISO/IEC 22989:2022 — concetto di output di AI system; coerente con Regolamento (UE) 2024/1689 (AI Act), art. 3.

17. **Large Language Model (LLM)**
Modello di apprendimento automatico che codifica il funzionamento del linguaggio naturale mediante un numero elevato di parametri e che consente l'esecuzione di una varietà di compiti di elaborazione del linguaggio naturale (Natural Language Processing, NLP).

I Large Language Model possono essere impiegati in diversi compiti di NLP, quali generazione di testo, riassunto automatico, traduzione automatica, classificazione e altri compiti analoghi.

I Large Language Model utilizzano grandi quantità di dati per l'addestramento e richiedono risorse computazionali significative.

Il funzionamento del linguaggio naturale può includere aspetti relativi a grammatica, semantica o altre caratteristiche proprie dell'uso del linguaggio.

Fonte: Definizione coerente con ISO/IEC 22989:2022 (machine learning model; natural language processing).

18. **Small Language Model (SLM)**
Modello linguistico che svolge attività di modellazione del linguaggio o di apprendimento di rappresentazioni con un numero inferiore di parametri rispetto ai Large Language Model (LLM), richiedendo minori risorse computazionali e risultando idoneo per ambienti con capacità di calcolo limitata.

Gli SLM possono essere sottoposti a fine-tuning su domini specifici per ottenere elevate prestazioni su compiti mirati, presentando tuttavia una minore generalità rispetto ai LLM.

Fonte: Coerente con ISO/IEC 22989:2022 (machine learning model; natural language processing).

19. **Apprendimento supervisionato (Supervised Learning)**
Metodo di apprendimento automatico nel quale il modello è addestrato utilizzando dati etichettati,

costituiti da coppie input–output, al fine di apprendere una funzione che consenta di prevedere correttamente l'output associato a nuovi input.

L'apprendimento supervisionato è comunemente utilizzato per compiti di classificazione e regressione.

Fonte: ISO/IEC 22989:2022; ISO/IEC 23053:2022.

20. **Apprendimento non supervisionato (Unsupervised Learning)**
Metodo di apprendimento automatico nel quale il modello è addestrato utilizzando dati non etichettati, al fine di identificare strutture, pattern o relazioni intrinseche nei dati.

L'apprendimento non supervisionato è comunemente impiegato per compiti quali clustering, riduzione della dimensionalità e apprendimento di rappresentazioni.

Fonte: ISO/IEC 22989:2022; ISO/IEC 23053:2022.

21. **Apprendimento per rinforzo (Reinforcement Learning)**
Metodo di apprendimento automatico nel quale un agente apprende a selezionare azioni all'interno di un ambiente, sulla base di un meccanismo di ricompensa o penalità, con l'obiettivo di massimizzare una misura cumulativa di ricompensa nel tempo.

L'apprendimento per rinforzo è caratterizzato dall'interazione iterativa tra agente e ambiente.

Fonte: ISO/IEC 22989:2022.

22. **Dataset**
Insieme strutturato di dati organizzati secondo un determinato schema o formato, utilizzato per finalità di addestramento, validazione, test o esercizio di un sistema di intelligenza artificiale.

Un dataset può includere dati etichettati o non etichettati, metadati e informazioni relative alla provenienza e alla qualità dei dati.

Fonte: ISO/IEC 22989:2022; coerente con ISO/IEC 23053:2022.

23. **Dati di addestramento (Training data)**
Sottoinsieme di un dataset utilizzato per determinare o aggiornare i parametri di un modello di apprendimento automatico durante la fase di addestramento.

I dati di addestramento possono essere etichettati o non etichettati, a seconda del metodo di apprendimento adottato.

Fonte: ISO/IEC 22989:2022; ISO/IEC 23053:2022.

24. **Dati di validazione (Validation data)**

Sottoinsieme di un dataset utilizzato per valutare le prestazioni di un modello durante la fase di addestramento e per supportare la selezione di iperparametri o configurazioni del modello.

I dati di validazione non sono impiegati per l'aggiornamento diretto dei parametri del modello.

Fonte: ISO/IEC 23053:2022 (framework ML lifecycle); coerente con ISO/IEC 22989:2022.

25. **Dati di test (Test data)**

Sottoinsieme di un dataset utilizzato per valutare in modo indipendente le prestazioni finali di un modello addestrato.

I dati di test devono essere distinti dai dati di addestramento e di validazione al fine di garantire una valutazione imparziale delle prestazioni del modello.

Fonte: ISO/IEC 23053:2022; coerente con ISO/IEC 22989:2022.

26. Data augmentation

Tecnica di preparazione dei dati che consiste nella generazione di nuovi dati a partire da dati esistenti mediante trasformazioni controllate, al fine di aumentare la variabilità del dataset e migliorare la capacità di generalizzazione del modello.

Le trasformazioni possono includere modifiche geometriche, sintattiche, semantiche o altre operazioni compatibili con il dominio applicativo.

Fonte: Coerente con ISO/IEC 23053:2022 (data preparation phase).

27. **Feature**

Caratteristica o attributo misurabile derivato dai dati di input, utilizzato come variabile nel processo di addestramento o inferenza di un modello di apprendimento automatico.

Le feature possono essere ottenute direttamente dai dati grezzi oppure attraverso processi di trasformazione o estrazione delle caratteristiche (feature engineering).

Fonte: ISO/IEC 22989:2022; coerente con ISO/IEC 23053:2022.

28. **Embedding**

Rappresentazione numerica, tipicamente in forma vettoriale a dimensione ridotta, che codifica proprietà semantiche o strutturali di dati quali testi, immagini o altri oggetti, al fine di facilitarne l'elaborazione da parte di un modello di apprendimento automatico.

Gli embedding consentono di rappresentare elementi simili in posizioni vicine nello spazio vettoriale.

Fonte: Coerente con ISO/IEC 22989:2022 (representation learning); ISO/IEC 23053:2022.

29. **Token**

Unità elementare di rappresentazione del testo o di altri dati sequenziali, utilizzata come elemento di input o output in modelli di elaborazione del linguaggio naturale.

Nei modelli linguistici, il token può corrispondere a una parola, parte di parola, carattere o altro segmento definito secondo uno specifico schema di tokenizzazione.

Fonte: Coerente con ISO/IEC 22989:2022 (natural language processing).

30. Iperparametro (Hyperparameter)

Parametro configurabile di un algoritmo di apprendimento automatico il cui valore è definito prima o durante il processo di addestramento e che influenza il comportamento del modello senza essere appreso direttamente dai dati.

Esempi di iperparametri includono tasso di apprendimento, numero di epoche, dimensione del batch e profondità della rete.
Gli iperparametri sono tipicamente selezionati mediante validazione su dataset di convalida o tecniche di ottimizzazione automatica.
Gli iperparametri si distinguono dai parametri del modello, che sono appresi durante l'addestramento.

Fonte: ISO/IEC 22989:2022 (machine learning model; training); ISO/IEC 23053:2022.

31. LoRA (Low-Rank Adaptation)

Tecnica di adattamento efficiente di modelli di grandi dimensioni che consiste nell'introdurre matrici di aggiornamento a rango ridotto nei pesi del modello pre-addestrato, mantenendo congelati i parametri originari.

LoRA consente il fine-tuning di modelli di grandi dimensioni riducendo significativamente il numero di parametri da aggiornare.
Tale tecnica diminuisce il consumo di memoria e le risorse computazionali necessarie all'adattamento del modello.
LoRA è frequentemente utilizzata nel fine-tuning di Large Language Model.

Fonte: Coerente con ISO/IEC 22989:2022 (model adaptation; training); ISO/IEC 23053:2022.

32. PEFT (Parameter-Efficient Fine-Tuning)

Insieme di tecniche di adattamento di modelli pre-addestrati che mirano a ridurre il numero di parametri aggiornati durante il fine-tuning, al fine di migliorare efficienza computazionale e sostenibilità operativa.

Le tecniche PEFT includono, tra le altre, LoRA, adapter layers e prompt tuning.
Il PEFT consente di mantenere la maggior parte dei parametri del modello invariati, riducendo costi di addestramento e requisiti hardware.
Nei contesti di procurement pubblico, il PEFT può contribuire alla riduzione del TCO e del LCOAI.

Fonte: Coerente con ISO/IEC 22989:2022 (training; model); ISO/IEC 23053:2022.

33. Prompt Tuning

Tecnica di adattamento di un modello pre-addestrato che consiste nell'ottimizzare un insieme limitato di parametri associati al prompt di input, mantenendo invariati i parametri principali del modello.

Il prompt tuning modifica rappresentazioni iniziali o vettori di embedding associati all'input.
Consente l'adattamento del modello a compiti specifici con un numero ridotto di parametri addestrabili.
È particolarmente utilizzato nei Large Language Model per ridurre costi computazionali e requisiti di memoria.

Fonte: Coerente con ISO/IEC 22989:2022 (training; representation learning); ISO/IEC 23053:2022.

34. Adapter Layers

Moduli aggiuntivi di piccole dimensioni inseriti tra gli strati di un modello pre-addestrato, i cui parametri sono addestrati per adattare il modello a un compito specifico, mantenendo congelati i parametri originari.

Gli adapter layers consentono riuso efficiente del modello base per più compiti.
Riducendo il numero di parametri aggiornati, migliorano efficienza e scalabilità del fine-tuning.
Possono essere considerati una tecnica di Parameter-Efficient Fine-Tuning (PEFT).

Fonte: Coerente con ISO/IEC 22989:2022 (model adaptation); ISO/IEC 23053:2022.

35. **Riduzione del modello (Model Reduction)**

Insieme di tecniche volte a diminuire la complessità strutturale, dimensionale o computazionale di un modello di apprendimento automatico al fine di migliorarne efficienza, portabilità e sostenibilità operativa lungo il ciclo di vita.

La riduzione del modello può comprendere tecniche quali pruning, quantizzazione e distillazione.
L'obiettivo della riduzione è minimizzare consumo di memoria, latenza e requisiti computazionali preservando prestazioni, robustezza e conformità ai requisiti applicativi.
Nei sistemi di IA, la riduzione del modello incide su TCO, LCOAI ed efficienza energetica.

Fonte: Coerente con ISO/IEC 22989:2022; ISO/IEC 23053:2022.

36. Pruning (Potatura del modello)

Tecnica di riduzione che consiste nella rimozione selettiva di pesi, connessioni, neuroni o interi strati di un modello ritenuti non essenziali, al fine di diminuirne dimensione e complessità computazionale.

Il pruning può essere strutturato o non strutturato.
Può essere applicato durante o dopo l'addestramento.
La potatura può richiedere una fase di ri-addestramento per recuperare eventuali perdite di accuratezza.

Fonte: Coerente con ISO/IEC 22989:2022 (model optimization); ISO/IEC 23053:2022.

37. Quantizzazione (Quantization)

Tecnica di ottimizzazione che consiste nella riduzione della precisione numerica dei parametri o delle attivazioni del modello, al fine di ridurre consumo di memoria e requisiti computazionali.

Può essere applicata in fase di addestramento o successivamente (post-training quantization).
La riduzione della precisione può comportare una variazione delle prestazioni del modello.
È particolarmente rilevante per deployment su dispositivi edge o ambienti con risorse limitate.

Fonte: Coerente con ISO/IEC 22989:2022; ISO/IEC 23053:2022.

38. Distillazione (Model Distillation)

Tecnica di compressione mediante la quale un modello di dimensioni ridotte è addestrato a riprodurre il comportamento di un modello più complesso, trasferendone conoscenza e capacità predittive.
La distillazione utilizza tipicamente le predizioni del modello originario come segnale di addestramento.
Consente la riduzione del numero di parametri mantenendo prestazioni comparabili.
È utilizzata per migliorare efficienza, scalabilità e sostenibilità economica del deployment.
Fonte: Coerente con ISO/IEC 22989:2022; ISO/IEC 23053:2022.

B. ARCHITETTURA E INGEGNERIA

39. Architettura agentica (Agentic Architecture)

Configurazione architetturale di un sistema di intelligenza artificiale nella quale uno o più agenti di IA operano in modo autonomo o semi-autonomo, pianificando ed eseguendo azioni in funzione di obiettivi definiti, eventualmente interagendo con strumenti, ambienti o altri sistemi.

L'architettura agentica può prevedere meccanismi di memoria, pianificazione, utilizzo di strumenti (*tool use*) e supervisione umana.

Fonte: Coerente con ISO/IEC 22989:2022 (AI system; autonomy) e ISO/IEC 42010:2011 (system architecture).

40. Agente di IA (AI Agent)

Sistema software basato su un modello di intelligenza artificiale che, sulla base di istruzioni, stato interno e memoria, pianifica ed esegue in modo autonomo o semi-autonomo sequenze di azioni multi-step mediante l'utilizzo di strumenti, operando entro uno spazio di azione definito e con un determinato livello di autonomia e supervisione umana.

L'agente di IA può interagire con ambienti digitali o fisici, ricevendo input e producendo output che influenzano tali ambienti.
Il livello di autonomia deve essere definito in coerenza con i meccanismi di controllo e supervisione previsti.

Fonte: Coerente con ISO/IEC 22989:2022 (AI system; autonomy; environment interaction).

41. Orchestratore (Orchestrator)

Componente software responsabile del coordinamento e della gestione dei flussi di esecuzione tra modelli di IA, agenti, strumenti e servizi applicativi, assicurando la corretta sequenza delle operazioni e la gestione degli stati.

L'orchestratore può implementare logiche di pianificazione, instradamento delle richieste, gestione delle dipendenze e controllo degli errori.

Fonte: Coerente con ISO/IEC 42010:2011 (architecture description) e ISO/IEC 23053:2022 (system workflow).

42. Stack di IA (AI Stack)

Insieme stratificato di componenti hardware e software che supportano lo sviluppo, l'addestramento, il deployment e l'esercizio di sistemi di intelligenza artificiale.

Lo stack di IA può comprendere infrastruttura computazionale, ambienti di sviluppo, framework di apprendimento automatico, modelli, servizi applicativi e interfacce utente.

Fonte: Coerente con ISO/IEC 42010:2011 (system architecture) e ISO/IEC 23053:2022.

43. Pipeline dei dati (Data pipeline)

Sequenza strutturata e automatizzata di processi mediante i quali i dati sono raccolti, trasformati, validati, archiviati e resi disponibili per l'addestramento, la valutazione o l'esercizio di un sistema di intelligenza artificiale.

La pipeline dei dati può includere fasi di estrazione, pulizia, normalizzazione, arricchimento, controllo qualità e tracciabilità.

Fonte: Coerente con ISO/IEC 23053:2022 (data preparation and processing).

44. Containerizzazione (Containerization)

Tecnica di virtualizzazione a livello di sistema operativo che consente di eseguire applicazioni e relativi componenti in ambienti isolati e portabili, condividendo il medesimo kernel del sistema host.

La containerizzazione favorisce portabilità, scalabilità e riproducibilità degli ambienti di esecuzione.

Fonte: Coerente con ISO/IEC 17788:2014 (cloud computing) e ISO/IEC 25010:2011 (portability).

45. Microservizi (Microservices)

Approccio architetturale che prevede la suddivisione di un'applicazione in servizi indipendenti, debolmente accoppiati e distribuiti, ciascuno responsabile di una specifica funzionalità.

L'architettura a microservizi consente scalabilità indipendente, resilienza e maggiore modularità del sistema.

Fonte: Coerente con ISO/IEC 42010:2011 (architecture description).

46. API (Application Programming Interface)

Interfaccia applicativa che definisce modalità e regole mediante le quali componenti software o sistemi distinti possono comunicare e scambiare dati o funzionalità.

Le API possono essere esposte mediante protocolli standardizzati e costituiscono elemento chiave per interoperabilità e integrazione.

Fonte: Coerente con ISO/IEC 42010:2011; ISO/IEC 25010:2011 (interoperability).

47. SDK (Software Development Kit)

Insieme strutturato di strumenti, librerie, documentazione e componenti software forniti per facilitare lo sviluppo, l'integrazione o l'estensione di applicazioni basate su una determinata piattaforma o servizio.

Un SDK può includere API, esempi di codice, ambienti di test e strumenti di configurazione.

Fonte: Coerente con ISO/IEC 42010:2011 (system components and interfaces).

48. Interoperabilità

Capacità di due o più sistemi, prodotti o componenti di scambiare informazioni e di utilizzare reciprocamente le informazioni scambiate.

L'interoperabilità può riguardare livelli tecnici, semantici e organizzativi.
Nei sistemi di IA, l'interoperabilità è rilevante ai fini dell'integrazione con basi dati, servizi applicativi e altri sistemi digitali.

Fonte: ISO/IEC 25010:2011.

49. Portabilità

Capacità di un sistema, prodotto o componente di essere trasferito da un ambiente hardware, software o operativo a un altro.

La portabilità comprende adattabilità, installabilità e sostituibilità.
Nei sistemi di IA, la portabilità è rilevante ai fini della prevenzione del lock-in tecnologico.

Fonte: ISO/IEC 25010:2011.

50. Scalabilità

Capacità di un sistema di gestire un aumento del carico di lavoro mediante l'incremento proporzionale delle risorse, mantenendo livelli di prestazione adeguati.

La scalabilità può essere verticale (incremento delle risorse su un singolo nodo) o orizzontale (incremento del numero di nodi).
Nei sistemi di IA, la scalabilità è rilevante sia in fase di addestramento sia in fase di inferenza.

Fonte: Coerente con ISO/IEC 25010:2011 (performance efficiency).

51. Elasticità

Capacità di un sistema di adattare dinamicamente le risorse computazionali in funzione della variazione del carico di lavoro, aumentando o riducendo tali risorse in modo automatico o semi-automatico.

L'elasticità è tipicamente associata a infrastrutture cloud.
L'elasticità consente l'ottimizzazione dei costi operativi nei sistemi di IA.

Fonte: ISO/IEC 17788:2014.

52. Resilienza

Capacità di un sistema di mantenere o ripristinare un livello accettabile di funzionamento in presenza di guasti, perturbazioni o condizioni avverse.

La resilienza può includere meccanismi di tolleranza ai guasti, ripristino e continuità operativa.
Nei sistemi di IA, la resilienza riguarda sia componenti infrastrutturali sia modelli e pipeline dei dati.

Fonte: ISO/IEC 25010:2011; ISO 22301:2019.

53. Alta disponibilità

Capacità di un sistema di garantire un elevato livello di operatività e accessibilità del servizio per un periodo di tempo definito.

L'alta disponibilità è generalmente espressa in termini percentuali di uptime su base temporale. Può essere ottenuta mediante ridondanza, bilanciamento del carico e meccanismi automatici di ripristino.

Fonte: ISO/IEC 25010:2011 (reliability — availability).

54. Failover

Meccanismo mediante il quale, in caso di guasto o indisponibilità di un componente, le funzioni del sistema sono automaticamente trasferite a un componente ridondante al fine di garantire la continuità del servizio.

Il failover può essere configurato in modalità attiva-attiva o attiva-passiva.
Nei sistemi di IA, il failover può riguardare sia componenti infrastrutturali sia servizi di inferenza.

Fonte: Coerente con ISO/IEC 25010:2011 (reliability) e ISO 22301:2019.

55. Logging

Processo di registrazione strutturata e persistente di eventi, operazioni e stati di un sistema informatico.

Il logging consente la tracciabilità delle attività e il supporto ad analisi forensi o di diagnostica.
Nei sistemi di IA, il logging può includere input, output, configurazioni del modello e parametri operativi.

Fonte: Coerente con ISO/IEC 42001:2023 (monitoring and auditability).

56. Audit trail

Insieme strutturato di registrazioni che consente di ricostruire cronologicamente le operazioni e le decisioni effettuate da un sistema o da un utente.

L'audit trail garantisce verificabilità e accountability delle operazioni.
Nei sistemi di IA, l'audit trail può includere informazioni relative a versioni del modello, dataset utilizzati e configurazioni operative.

Fonte: ISO/IEC 42001:2023; ISO 9000:2015.

57. Monitoraggio

Attività continuativa di osservazione e valutazione dello stato e delle prestazioni di un sistema rispetto a criteri o indicatori definiti.

Il monitoraggio può riguardare parametri tecnici, metriche di qualità, sicurezza e prestazioni del modello.

Nei sistemi di IA, il monitoraggio include la rilevazione di fenomeni quali data drift o degrado delle prestazioni.

Fonte: ISO 9000:2015; ISO/IEC 42001:2023.

58. Fallback

Meccanismo di continuità operativa mediante il quale, in caso di errore, degrado delle prestazioni o indisponibilità di un componente primario, il sistema attiva automaticamente una modalità alternativa di funzionamento al fine di garantire un livello minimo accettabile di servizio.

Il fallback può prevedere l'utilizzo di un modello alternativo, una versione semplificata del servizio o una procedura manuale con supervisione umana.
A differenza del failover, il fallback può comportare una riduzione delle funzionalità o delle prestazioni, configurandosi come meccanismo di degradazione controllata (*graceful degradation*).

Fonte: Coerente con ISO/IEC 25010:2011 (reliability); ISO/IEC 42001:2023 (operational control); ISO 22301:2019 (business continuity).

59. Fallback su CPU (CPU Fallback)

Meccanismo di continuità operativa mediante il quale, in caso di indisponibilità o malfunzionamento di acceleratori hardware dedicati (quali GPU, TPU o NPU), l'esecuzione del modello di intelligenza artificiale viene automaticamente trasferita su unità di elaborazione centrale (CPU), garantendo un livello minimo di servizio.

Il fallback su CPU può comportare un aumento della latenza e una riduzione delle prestazioni rispetto all'esecuzione su acceleratori dedicati.
Tale meccanismo contribuisce a resilienza e alta disponibilità del sistema.
Il fallback su CPU è particolarmente rilevante nei contesti di procurement pubblico per assicurare continuità operativa e neutralità hardware.

Fonte: Coerente con ISO/IEC 25010:2011 (reliability); ISO/IEC 42010:2011 (architecture); ISO/IEC 22989:2022 (computational resources).

60. Rollback

Meccanismo di ripristino mediante il quale un sistema ritorna a una versione precedente stabile di software, modello o configurazione, a seguito di malfunzionamenti, errori o degradazione delle prestazioni introdotti da un aggiornamento o modifica.

Il rollback è tipicamente utilizzato nei processi di deployment continuo e MLOps per garantire stabilità operativa.
Nei sistemi di IA, il rollback può riguardare versioni del modello, configurazioni della pipeline dei dati

o componenti infrastrutturali.
Il rollback non comporta necessariamente degradazione delle funzionalità, ma ripristino di uno stato precedentemente validato.

Fonte: Coerente con ISO/IEC 12207:2017 (software lifecycle processes); ISO/IEC 23053:2022 (ML lifecycle); ISO/IEC 25010:2011 (reliability).

61. Observability

Capacità di un sistema di consentire la comprensione del proprio stato interno attraverso l'analisi dei dati generati, quali log, metriche e tracce, al fine di diagnosticare anomalie e comprendere il comportamento operativo.

L'observability si basa tipicamente su log strutturati, metriche quantitative e tracciamento delle richieste.
Nei sistemi di IA, l'observability può includere il monitoraggio delle prestazioni del modello, della latenza e del consumo di risorse.

Fonte: Coerente con ISO/IEC 42001:2023 (monitoring and measurement); ISO/IEC 25010:2011.

62. Deployment

Processo di distribuzione e messa in esercizio di un sistema, modello o componente software in un ambiente operativo.

Il deployment può avvenire in ambienti on-premise, cloud o ibridi.
Nei sistemi di IA, il deployment riguarda tipicamente la fase successiva alla validazione del modello.

Fonte: ISO/IEC 23053:2022 (ML lifecycle — deployment phase).

63. Continuous Integration (CI)

Pratica di sviluppo software che prevede l'integrazione frequente e automatizzata delle modifiche al codice in un repository condiviso, accompagnata da test automatici.

La Continuous Integration riduce il rischio di errori derivanti dall'integrazione tardiva del codice.
Nei sistemi di IA, la CI può includere test su pipeline dei dati e configurazioni del modello.

Fonte: Coerente con ISO/IEC 12207:2017 (software lifecycle processes).

64. Continuous Deployment (CD)

Pratica che consente la distribuzione automatizzata in ambiente operativo delle modifiche validate, senza intervento manuale significativo.

La Continuous Deployment estende i principi della Continuous Integration fino alla messa in esercizio.
Nei sistemi di IA, la CD può includere il rilascio controllato di nuove versioni di modelli.

Fonte: Coerente con ISO/IEC 12207:2017 (software lifecycle processes).

65. MLOps

Insieme di pratiche, processi e strumenti volti a integrare sviluppo, addestramento, validazione, deployment e monitoraggio continuo di modelli di apprendimento automatico in ambienti operativi.

Il MLOps estende i principi DevOps al ciclo di vita dei sistemi di IA basati su Machine Learning.
Il MLOps comprende gestione delle versioni dei modelli, tracciabilità dei dataset, monitoraggio delle prestazioni e controllo del rischio operativo.

Fonte: Coerente con ISO/IEC 23053:2022 (ML lifecycle); ISO/IEC 42001:2023.

C. INFRASTRUTTURA E HARDWARE

66. CPU (Central Processing Unit)

Unità centrale di elaborazione di un sistema informatico, responsabile dell'esecuzione delle istruzioni generali e del controllo delle operazioni computazionali.

La CPU è progettata per l'elaborazione general-purpose di istruzioni sequenziali.
Nei sistemi di IA, la CPU è utilizzata principalmente per attività di orchestrazione, gestione dei dati e inferenza su modelli di dimensioni contenute.

Fonte: Coerente con ISO/IEC 2382:2015 (Information technology — Vocabulary).

67. GPU (Graphics Processing Unit)

Unità di elaborazione specializzata per il calcolo parallelo ad alte prestazioni, originariamente progettata per applicazioni grafiche e oggi ampiamente utilizzata per l'addestramento e l'inferenza di modelli di apprendimento automatico.

La GPU è particolarmente efficiente nell'esecuzione di operazioni matriciali e vettoriali.
Nei sistemi di IA, le GPU sono comunemente impiegate per il Deep Learning.

Fonte: Coerente con ISO/IEC 2382:2015; ISO/IEC 22989:2022 (computational resources).

68. TPU (Tensor Processing Unit)

Acceleratore hardware specializzato progettato per l'elaborazione efficiente di operazioni tensoriali tipiche dei modelli di apprendimento automatico.

Le TPU sono ottimizzate per l'esecuzione di reti neurali su larga scala.
L'impiego di TPU può ridurre i tempi di addestramento e migliorare l'efficienza energetica rispetto a soluzioni general-purpose.

Fonte: Coerente con ISO/IEC 22989:2022 (AI computational infrastructure).

69. NPU (Neural Processing Unit)

Unità di elaborazione dedicata all'accelerazione delle operazioni proprie delle reti neurali artificiali, integrata in dispositivi o sistemi embedded.

Le NPU sono progettate per ottimizzare inferenza ed elaborazione locale su dispositivi con risorse limitate.
Le NPU sono frequentemente utilizzate in contesti edge computing e dispositivi mobili.

Fonte: Coerente con ISO/IEC 22989:2022 (AI hardware acceleration).

70. FPGA (Field-Programmable Gate Array)

Dispositivo hardware riconfigurabile costituito da una matrice di blocchi logici programmabili e interconnessioni configurabili, che può essere adattato per implementare specifiche funzioni computazionali.

Gli FPGA consentono l'implementazione di acceleratori personalizzati per carichi di lavoro specifici.
Nei sistemi di IA, gli FPGA possono essere utilizzati per ottimizzare inferenza o elaborazioni a bassa latenza.

Fonte: ISO/IEC 2382:2015.

71. ASIC (Application-Specific Integrated Circuit)

Circuito integrato progettato e realizzato per svolgere una funzione specifica o un insieme limitato di funzioni applicative.

Gli ASIC sono ottimizzati per efficienza e prestazioni rispetto a soluzioni general-purpose.
Nei sistemi di IA, gli ASIC possono essere progettati per l'accelerazione dedicata di operazioni di apprendimento automatico.

Fonte: ISO/IEC 2382:2015.

72. Cloud Computing

Paradigma che consente l'accesso in rete, su richiesta e con modalità configurabile, a un insieme condiviso di risorse computazionali configurabili che possono essere rapidamente fornite e rilasciate con minimo sforzo di gestione o interazione con il fornitore del servizio.

Le risorse possono includere reti, server, storage, applicazioni e servizi.
Il cloud computing comprende modelli di servizio quali IaaS, PaaS e SaaS e modelli di distribuzione quali pubblico, privato e ibrido.

Fonte: ISO/IEC 17788:2014.

73. Edge Computing

Modello di elaborazione distribuita nel quale l'elaborazione dei dati avviene in prossimità della fonte di generazione degli stessi, anziché in un data center centralizzato.

L'edge computing riduce latenza e traffico di rete.
Nei sistemi di IA, l'edge computing consente inferenza locale su dispositivi con risorse limitate.

Fonte: ISO/IEC 17788:2014.

74. Cloud pubblico

Modello di distribuzione del cloud computing nel quale l'infrastruttura cloud è messa a disposizione del pubblico o di un ampio gruppo di utenti ed è di proprietà, gestione e controllo di un fornitore di servizi cloud.

Le risorse sono condivise tra più clienti secondo un modello multi-tenant.
L'accesso ai servizi avviene tipicamente tramite rete pubblica.

Fonte: ISO/IEC 17788:2014.

75. Cloud privato

Modello di distribuzione del cloud computing nel quale l'infrastruttura cloud è destinata all'uso esclusivo di una singola organizzazione.

Il cloud privato può essere gestito dall'organizzazione stessa o da un terzo.
L'infrastruttura può essere collocata presso i locali dell'organizzazione o in hosting esterno.

Fonte: ISO/IEC 17788:2014.

76. Cloud ibrido

Modello di distribuzione del cloud computing costituito dalla combinazione di due o più infrastrutture cloud distinte (pubbliche o private) che rimangono entità uniche ma sono collegate da tecnologie che consentono la portabilità di dati e applicazioni.

Il cloud ibrido consente di bilanciare requisiti di sicurezza, controllo e scalabilità.
Nei sistemi di IA, può essere utilizzato per separare addestramento e inferenza tra ambienti differenti.

Fonte: ISO/IEC 17788:2014.

77. On-premises

Modello di implementazione nel quale infrastrutture hardware e software sono installate e gestite direttamente dall'organizzazione presso i propri locali.

L'organizzazione mantiene il pieno controllo delle risorse e della sicurezza fisica e logica.
Nei sistemi di IA, l'on-premises è spesso adottato per esigenze di sovranità del dato o vincoli normativi.

Fonte: Coerente con ISO/IEC 17788:2014 (cloud deployment models).

78. HPC (High Performance Computing)

Insieme di tecnologie e infrastrutture computazionali ad alte prestazioni progettate per l'elaborazione di grandi volumi di dati o per l'esecuzione di calcoli complessi mediante l'utilizzo coordinato di risorse di calcolo parallelo.

L'HPC è comunemente impiegato per simulazioni scientifiche, analisi avanzate e addestramento di modelli di IA di grandi dimensioni.
Le infrastrutture HPC possono includere cluster di nodi computazionali interconnessi ad alta velocità.

Fonte: ISO/IEC 2382:2015 (Information technology — Vocabulary).

79. Virtualizzazione

Tecnica che consente la creazione di risorse computazionali virtuali, quali macchine virtuali, reti o storage, indipendenti dall'hardware fisico sottostante.

La virtualizzazione consente un uso più efficiente delle risorse hardware.
È componente fondamentale nei modelli di cloud computing.

Fonte: ISO/IEC 17788:2014.

80. Hypervisor

Componente software o firmware che consente la creazione e la gestione di macchine virtuali, controllando l'accesso alle risorse hardware sottostanti.

L'hypervisor può essere di tipo 1 (bare metal) o di tipo 2 (hosted).
È elemento chiave nei sistemi virtualizzati e negli ambienti cloud.

Fonte: ISO/IEC 17788:2014.

81. Storage distribuito

Architettura di memorizzazione dei dati nella quale le informazioni sono archiviate su più nodi fisicamente distinti e interconnessi, operanti come sistema logico unico.

Lo storage distribuito migliora scalabilità e resilienza.
Nei sistemi di IA, è utilizzato per gestire grandi dataset e modelli di dimensioni elevate.

Fonte: Coerente con ISO/IEC 17788:2014.

82. Data center

Struttura fisica destinata all'alloggiamento di sistemi informatici e componenti associati, quali server, sistemi di storage e infrastrutture di rete, nonché sistemi di alimentazione e raffreddamento.

Il data center può ospitare infrastrutture cloud o on-premises.
Nei sistemi di IA, il data center può includere risorse specializzate per l'elaborazione ad alte prestazioni.

Fonte: ISO/IEC 22237 (Data centre facilities and infrastructures).

83. Neutralità hardware

Principio architetturale secondo cui un sistema software è progettato per operare indipendentemente da specifiche piattaforme hardware o acceleratori proprietari, garantendo compatibilità e sostituibilità delle risorse computazionali.

La neutralità hardware favorisce portabilità e riduzione del rischio di lock-in tecnologico.
Nei sistemi di IA, implica la possibilità di eseguire modelli su diverse tipologie di CPU, GPU o altri acceleratori compatibili.

Fonte: Coerente con ISO/IEC 25010:2011 (portability) e ISO/IEC 42010:2011 (architecture description).

84. Infrastructure as-a-Service (IaaS)

Categoria di servizio di cloud computing che fornisce risorse computazionali fondamentali, quali elaborazione, storage e rete, sulle quali l'utente può distribuire e gestire software, inclusi sistemi operativi e applicazioni.

Il fornitore gestisce l'infrastruttura fisica sottostante, mentre l'utente mantiene il controllo sui sistemi operativi e sulle applicazioni.
L'IaaS è comunemente utilizzato per ambienti di addestramento e deployment di sistemi di IA.

Fonte: ISO/IEC 17788:2014.

85. Platform as-a-Service (PaaS)

Categoria di servizio di cloud computing che fornisce una piattaforma completa, comprendente ambiente di sviluppo, strumenti e servizi, sulla quale l'utente può sviluppare, eseguire e gestire applicazioni senza gestire direttamente l'infrastruttura sottostante.

Il fornitore gestisce infrastruttura, sistema operativo e middleware.
Nei sistemi di IA, il PaaS può includere framework di machine learning e strumenti di gestione dei modelli.

Fonte: ISO/IEC 17788:2014.

86. Software as-a-Service (SaaS)

Categoria di servizio di cloud computing che fornisce applicazioni software eseguite su infrastruttura cloud e accessibili agli utenti tramite rete.

L'utente non gestisce né controlla l'infrastruttura, il sistema operativo o le piattaforme sottostanti.
Nei sistemi di IA, il SaaS può comprendere servizi di inferenza o applicazioni basate su modelli di IA forniti come servizio.

Fonte: ISO/IEC 17788:2014.

D. DATI E GOVERNANCE

87. Data Governance

Insieme di ruoli, responsabilità, politiche, processi e controlli finalizzati ad assicurare qualità, integrità, sicurezza, disponibilità e conformità dei dati lungo il loro ciclo di vita.

La Data Governance definisce regole per gestione, accesso, condivisione e conservazione dei dati.
Nei sistemi di IA, la Data Governance è elemento essenziale per garantire affidabilità, tracciabilità e gestione del rischio.

Fonte: ISO/IEC 38505-1:2017; coerente con ISO/IEC 42001:2023.

88. Data Steward

Soggetto responsabile della gestione operativa dei dati, incaricato di garantirne qualità, coerenza e conformità alle politiche di Data Governance.

Il Data Steward cura definizioni, metadati e regole di utilizzo dei dati.
Può operare in coordinamento con il Data Owner e con le funzioni di controllo.

Fonte: ISO/IEC 38505-1:2017.

89. Data Owner

Soggetto che detiene la responsabilità ultima in merito alla classificazione, protezione e utilizzo di un insieme di dati, definendone requisiti e livelli di accesso.

Il Data Owner stabilisce le regole di accesso e le finalità di trattamento.
Nei contesti pubblici, il Data Owner può coincidere con il titolare del trattamento ai sensi della normativa sulla protezione dei dati.

Fonte: ISO/IEC 38505-1:2017; coerente con Regolamento (UE) 2016/679 (GDPR).

90. Data Drift

Variazione nel tempo della distribuzione statistica dei dati di input rispetto a quella osservata durante la fase di addestramento del modello, tale da poter incidere sulle prestazioni del sistema di intelligenza artificiale.

Il data drift può derivare da cambiamenti nel contesto operativo, nelle fonti dei dati o nei comportamenti degli utenti.
Il rilevamento del data drift costituisce parte integrante delle attività di monitoraggio continuo dei sistemi di IA.

Fonte: NIST AI Risk Management Framework 1.0; coerente con ISO/IEC 23053:2022 (monitoring phase).

91. Concept Drift

Variazione nel tempo della relazione tra dati di input e output attesi, tale da modificare il comportamento o le prestazioni del modello rispetto al compito originario.

Il Concept Drift può verificarsi anche in assenza di variazioni significative nella distribuzione dei dati di input.
La gestione del Concept Drift può richiedere ri-addestramento o aggiornamento del modello.

Fonte: NIST AI Risk Management Framework 1.0; coerente con ISO/IEC 23053:2022.

92. Data Lineage

Rappresentazione documentata del ciclo di vita dei dati, che descrive origine, trasformazioni, movimenti e utilizzi dei dati all'interno di un sistema.

La Data Lineage consente la tracciabilità delle operazioni effettuate sui dati.
Nei sistemi di IA, la Data Lineage è rilevante ai fini di auditabilità, qualità e gestione del rischio.

Fonte: Coerente con ISO/IEC 38505-1:2017; ISO/IEC 42001:2023.

93. Data Quality

Insieme di caratteristiche dei dati che ne determinano l'idoneità all'uso rispetto a specifici requisiti, quali accuratezza, completezza, coerenza, tempestività e affidabilità.

La qualità dei dati influisce direttamente sulle prestazioni e sull'affidabilità dei sistemi di IA.
La Data Quality deve essere valutata lungo l'intero ciclo di vita dei dati.

Fonte: ISO/IEC 25012:2008 (Data quality model); coerente con ISO/IEC 23053:2022.

94. Data Minimization

Principio secondo cui i dati trattati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

La Data Minimization riduce il rischio per i diritti e le libertà degli interessati.
Nei sistemi di IA, implica la limitazione dei dataset a informazioni strettamente necessarie agli obiettivi dichiarati.

Fonte: Regolamento (UE) 2016/679 (GDPR), art. 5.

95. Pseudonimizzazione

Trattamento dei dati personali tale che essi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, conservate separatamente e soggette a misure tecniche e organizzative.

La pseudonimizzazione non elimina la natura di dato personale.
È misura di mitigazione del rischio prevista dalla normativa sulla protezione dei dati.

Fonte: Regolamento (UE) 2016/679 (GDPR), art. 4.

96. Anonimizzazione

Processo mediante il quale i dati sono trasformati in modo irreversibile affinché l'interessato non sia più identificabile, direttamente o indirettamente.

I dati anonimizzati non rientrano nell'ambito di applicazione della normativa sui dati personali.
L'anonimizzazione deve impedire ogni forma ragionevole di re-identificazione.

Fonte: Regolamento (UE) 2016/679 (GDPR); considerando 26.

97. Data Lake

Repository centralizzato che consente di archiviare grandi quantità di dati grezzi in formato nativo o quasi nativo, indipendentemente dalla loro struttura o formato, per uso analitico o operativo.

I dati in un data lake possono essere strutturati, semi-strutturati o non strutturati.
Nei sistemi di IA, i data lake favoriscono l'aggregazione di dataset eterogenei per addestramento, validazione e inferenza.

Fonte: coerente con definizioni di mercato e ISO/IEC 38505-1:2017 (data governance).

98. Data Warehouse

Sistema di archiviazione dei dati progettato per supportare analisi e reporting, nel quale i dati sono integrati, puliti e organizzati secondo schemi predefiniti a supporto di querying ottimizzato.

I data warehouse sono tipicamente ottimizzati per interrogazioni complesse e analisi storica.
Nei sistemi di IA, i data warehouse possono fornire dati consolidati e normalizzati per l'analisi e la validazione.

Fonte: coerente con definizioni di mercato e ISO/IEC 38505-1:2017.

99. Metadato (Metadata)

Informazione descrittiva che caratterizza un insieme di dati o un oggetto digitale, al fine di facilitarne la gestione, la ricerca, la comprensione o l'utilizzo.

I metadati possono includere schema, origine, proprietario, data di creazione, qualità o relazione tra dati.
Nei sistemi di IA, i metadati sono fondamentali per tracciabilità dei dataset, metriche di qualità dati e auditabilità.

Fonte: ISO/IEC 11179 (Metadata registries); coerente con ISO/IEC 38505-1:2017.

100. Registro dei trattamenti (Record of Processing Activities)

Documento o sistema che contiene informazioni dettagliate sulle operazioni di trattamento dei dati personali effettuate da un'organizzazione, come prescritto dal GDPR, incluse finalità, categorie di dati, destinatari e misure di sicurezza adottate.

Il registro dei trattamenti facilita la conformità normativa e l'accountability.
Nei sistemi di IA che trattano dati personali, il registro dei trattamenti deve includere informazioni su dataset, finalità di utilizzo e basi giuridiche.

Fonte: Regolamento (UE) 2016/679 (GDPR), art. 30; coerente con ISO/IEC 38505-1:2017.

E. QUALITÀ, RISCHIO E CONFORMITÀ

101. Rischio

Combinazione della probabilità che si verifichi un danno e della gravità di tale danno.

Nel contesto dei sistemi di intelligenza artificiale, il danno può riguardare salute, sicurezza o diritti fondamentali delle persone.
La valutazione del rischio tiene conto sia della probabilità di accadimento sia dell'entità dell'impatto.

Fonte: Regolamento (UE) 2024/1689 (AI Act), art. 3.

102. Gestione del rischio

Attività coordinate volte a identificare, analizzare, valutare, trattare e monitorare i rischi associati a un sistema.

Nei sistemi di IA ad alto rischio, la gestione del rischio è parte integrante del sistema di gestione della qualità.
La gestione del rischio deve essere continua e coprire l'intero ciclo di vita del sistema.

Fonte: Regolamento (UE) 2024/1689 (AI Act), art. 9; coerente con ISO 31000:2018.

103. Risk assessment

Processo sistematico di identificazione, analisi e valutazione dei rischi al fine di determinarne livello e accettabilità.

Il risk assessment comprende l'identificazione dei pericoli e la stima della probabilità e della gravità del danno.
Nei sistemi di IA, il risk assessment deve essere aggiornato in presenza di modifiche significative.

Fonte: Regolamento (UE) 2024/1689 (AI Act), art. 9; coerente con ISO 31000:2018.

104. Risk mitigation

Insieme di misure tecniche e organizzative volte a ridurre la probabilità di accadimento o la gravità del danno associato a un rischio identificato.

Le misure di mitigazione possono includere controlli tecnici, procedure operative e supervisione umana.
Nei sistemi di IA, la mitigazione del rischio deve essere proporzionata alla natura e al livello del rischio.

Fonte: Regolamento (UE) 2024/1689 (AI Act), art. 9; coerente con ISO 31000:2018.

105. Bias

Inclinazione sistematica o distorsione nei dati, nel modello o nei processi che può determinare risultati non equi o discriminatori.

Il bias può derivare da dati di addestramento non rappresentativi, scelte di progettazione o contesto di utilizzo.
La gestione del bias è parte integrante delle attività di gestione del rischio nei sistemi di IA.

Fonte: NIST AI Risk Management Framework 1.0; coerente con ISO/IEC 22989:2022.

106. Robustezza

Capacità di un sistema di intelligenza artificiale di mantenere prestazioni adeguate anche in presenza di condizioni operative variabili, input perturbati o tentativi di manipolazione.

La robustezza include la resistenza a errori, rumore nei dati e attacchi avversari.
Nei sistemi di IA ad alto rischio, la robustezza è requisito essenziale di affidabilità tecnica.

Fonte: Regolamento (UE) 2024/1689 (AI Act), art. 15; coerente con ISO/IEC 24029-1:2021.

107. Accuratezza (Accuracy)

Grado di correttezza delle previsioni o decisioni prodotte da un modello rispetto ai valori effettivi o attesi.

L'accuratezza è generalmente espressa come proporzione di previsioni corrette sul totale delle osservazioni.
Nei sistemi di IA, l'accuratezza deve essere valutata in relazione al contesto di utilizzo e ai requisiti applicativi.

Fonte: ISO/IEC 22989:2022; coerente con Regolamento (UE) 2024/1689, art. 15.

108. Precision

Metrica di valutazione nei compiti di classificazione che misura la proporzione di predizioni positive corrette rispetto al totale delle predizioni positive effettuate dal modello.

La precision è particolarmente rilevante quando i falsi positivi comportano impatti significativi.
È definita come rapporto tra veri positivi e somma di veri positivi e falsi positivi.

Fonte: Coerente con ISO/IEC 22989:2022 (performance evaluation of ML models).

109. Recall

Metrica di valutazione nei compiti di classificazione che misura la proporzione di casi positivi correttamente identificati rispetto al totale dei casi positivi effettivi.

Il recall è particolarmente rilevante quando i falsi negativi comportano impatti significativi.
È definito come rapporto tra veri positivi e somma di veri positivi e falsi negativi.

Fonte: Coerente con ISO/IEC 22989:2022 (performance evaluation of ML models).

110. F1-score

Metrica di valutazione che rappresenta la media armonica tra precision e recall, fornendo una misura bilanciata delle prestazioni di un modello nei compiti di classificazione.

L'F1-score è particolarmente utile in presenza di dataset sbilanciati.
Assume valori compresi tra 0 e 1, dove valori più elevati indicano migliori prestazioni.

Fonte: Coerente con ISO/IEC 22989:2022 (performance evaluation of ML models).

111. Spiegabilità (Explainability)

Proprietà di un sistema di intelligenza artificiale che consente di fornire informazioni comprensibili sui fattori che hanno determinato uno specifico output o comportamento del modello.

La spiegabilità facilita la comprensione delle decisioni da parte degli utenti e delle autorità competenti.
Nei sistemi ad alto rischio, la spiegabilità contribuisce alla verifica del rispetto dei requisiti normativi.

Fonte: ISO/IEC 22989:2022; coerente con Regolamento (UE) 2024/1689.

112. Interpretabilità (Interpretability)

Grado con cui il funzionamento interno di un modello di intelligenza artificiale può essere compreso direttamente da un essere umano.

L'interpretabilità è generalmente associata a modelli strutturalmente semplici o trasparenti.
L'interpretabilità si distingue dalla spiegabilità, che può essere ottenuta anche mediante tecniche post-hoc.

Fonte: ISO/IEC 22989:2022.

113. Trasparenza (Transparency)

Caratteristica di un sistema di intelligenza artificiale che garantisce la disponibilità di informazioni appropriate sul suo funzionamento, sulle sue capacità e sui suoi limiti agli stakeholder pertinenti.

La trasparenza include obblighi di informazione verso utenti o soggetti interessati.
Nei sistemi di IA, la trasparenza è requisito previsto per specifiche categorie di sistemi ai sensi dell'AI Act.

Fonte: ISO/IEC 22989:2022; Regolamento (UE) 2024/1689.

114. Supervisione umana (Human Oversight)

Insieme di misure e meccanismi che assicurano la possibilità per persone fisiche di monitorare, intervenire o interrompere il funzionamento di un sistema di intelligenza artificiale.

La supervisione umana può includere interventi preventivi o correttivi.
Nei sistemi di IA ad alto rischio, la supervisione umana è requisito obbligatorio.

Fonte: Regolamento (UE) 2024/1689 (AI Act), art. 14.

115. Accountability

Principio secondo cui un'organizzazione o un soggetto è responsabile del rispetto delle norme applicabili e deve essere in grado di dimostrare tale conformità.

L'accountability implica documentazione, tracciabilità e capacità di audit.
Nei sistemi di IA, l'accountability riguarda l'intero ciclo di vita del sistema.

Fonte: Regolamento (UE) 2016/679 (GDPR), art. 5; coerente con ISO/IEC 42001:2023.

116. Auditabilità

Capacità di un sistema di consentire la verifica indipendente delle proprie operazioni, decisioni e controlli attraverso la disponibilità di evidenze documentate e tracciabili.

L'auditabilità richiede registrazioni affidabili, complete e accessibili.
Nei sistemi di IA, l'auditabilità riguarda modelli, dataset, configurazioni e processi decisionali.

Fonte: ISO 9000:2015; coerente con ISO/IEC 42001:2023.

117. Verifica

Conferma, mediante evidenze oggettive, che requisiti specificati sono stati soddisfatti.

La verifica riguarda la conformità rispetto a requisiti tecnici o specifiche definite.
La verifica può includere attività di test, ispezione o revisione documentale.

Fonte: ISO 9000:2015.

118. Validazione

Conferma, mediante evidenze oggettive, che i requisiti per uno specifico uso previsto sono stati soddisfatti.

La validazione è orientata alla valutazione dell'idoneità all'uso nel contesto applicativo reale.
La validazione può includere prove operative, simulazioni o valutazioni sul campo.

Fonte: ISO 9000:2015.

119. Conformità

Soddisfacimento di un requisito.

I requisiti possono derivare da norme, regolamenti, specifiche contrattuali o politiche interne.
Nei sistemi di IA, la conformità può riguardare requisiti tecnici, organizzativi e normativi.

Fonte: ISO 9000:2015.

120. Sistema di gestione dell'IA (AI Management System)

Parte del sistema di gestione di un'organizzazione che stabilisce politiche, obiettivi e processi per sviluppare, fornire o utilizzare sistemi di intelligenza artificiale in modo conforme ai requisiti applicabili.

Il sistema di gestione dell'IA può includere processi di gestione del rischio, controllo della qualità e monitoraggio continuo.
Nei sistemi di IA ad alto rischio, il sistema di gestione della qualità deve soddisfare i requisiti previsti dall'AI Act.

Fonte: ISO/IEC 42001:2023; Regolamento (UE) 2024/1689 (AI Act), art. 17.

F. SICUREZZA

121. Attacco adversarial (Adversarial Attack)

Tecnica volta a indurre un sistema di intelligenza artificiale a produrre output errati o inattesi mediante la manipolazione intenzionale dei dati di input o delle condizioni operative.

Gli attacchi adversarial possono essere condotti in fase di addestramento o di inferenza.
Tali attacchi possono compromettere affidabilità, sicurezza e integrità del sistema.

Fonte: NIST AI Risk Management Framework 1.0; coerente con ISO/IEC 23894:2023.

122. Evasion Attack

Tipologia di attacco adversarial condotto in fase di inferenza, consistente nella manipolazione degli input al fine di eludere il comportamento previsto del modello senza alterarne i parametri.

L'attacco di evasione sfrutta vulnerabilità del modello rispetto a perturbazioni impercettibili o mirate.
È particolarmente rilevante nei sistemi di classificazione e riconoscimento.

Fonte: NIST AI Risk Management Framework 1.0.

123. Poisoning Attack

Tipologia di attacco adversarial condotto in fase di addestramento, consistente nell'introduzione intenzionale di dati manipolati nel dataset al fine di alterare il comportamento del modello.

Il poisoning può compromettere integrità e affidabilità del modello nel lungo periodo.
La mitigazione richiede controlli sulla qualità e provenienza dei dati.

Fonte: NIST AI Risk Management Framework 1.0; coerente con ISO/IEC 23894:2023.

124. Model Inversion

Tecnica di attacco che mira a ricostruire o inferire informazioni sensibili relative ai dati di addestramento a partire dagli output o dall'accesso al modello.

Il model inversion può comportare rischi per la riservatezza dei dati personali.
È particolarmente rilevante nei modelli esposti tramite API pubbliche.

Fonte: NIST AI Risk Management Framework 1.0.

125. Privacy Attack

Categoria di attacchi volti a compromettere la riservatezza dei dati personali trattati o utilizzati da un sistema di intelligenza artificiale.

I privacy attack includono, tra gli altri, model inversion e membership inference.
La prevenzione richiede misure tecniche e organizzative adeguate, quali pseudonimizzazione e controlli di accesso.

Fonte: NIST AI Risk Management Framework 1.0; coerente con Regolamento (UE) 2016/679 (GDPR).

126. Security by design

Principio secondo cui la sicurezza è integrata fin dalle prime fasi di progettazione e sviluppo di un sistema, mediante l'adozione sistematica di misure tecniche e organizzative adeguate.

Il Security by design implica l'analisi preventiva delle minacce e l'implementazione di controlli proporzionati al rischio.
Nei sistemi di IA, include la protezione di modelli, dati e pipeline lungo l'intero ciclo di vita.

Fonte: ISO/IEC 27001:2022; coerente con ISO/IEC 23894:2023.

127. Encryption

Tecnica di protezione delle informazioni che consiste nella trasformazione dei dati in una forma illeggibile per soggetti non autorizzati, mediante l'utilizzo di algoritmi crittografici e chiavi.

L'encryption può essere applicata ai dati a riposo, in transito o in uso.
L'efficacia della cifratura dipende dalla gestione sicura delle chiavi crittografiche.

Fonte: ISO/IEC 27001:2022; ISO/IEC 2382:2015.

128. Identity Management

Insieme di processi e tecnologie finalizzati alla gestione delle identità digitali, comprese creazione, autenticazione, autorizzazione e disattivazione degli accessi.

L'identity management supporta la tracciabilità e l'accountability degli accessi ai sistemi.
Nei sistemi di IA, consente il controllo degli accessi a modelli, dataset e servizi di inferenza.

Fonte: ISO/IEC 24760-1:2019.

129. Access Control

Insieme di misure tecniche e organizzative che limitano l'accesso a sistemi, dati o risorse ai soli soggetti autorizzati.

Il controllo degli accessi può essere basato su ruoli, attributi o policy specifiche.
Nei sistemi di IA, l'access control è essenziale per la protezione di modelli e dati sensibili.

Fonte: ISO/IEC 27001:2022.

130. Zero Trust Architecture

Modello di sicurezza informatica basato sul principio "never trust, always verify", secondo cui nessun utente, dispositivo o sistema è considerato affidabile per impostazione predefinita e ogni accesso deve essere continuamente autenticato, autorizzato e monitorato.

La Zero Trust Architecture si fonda su verifica continua dell'identità, segmentazione delle risorse e principio del minimo privilegio.
Nei sistemi di IA, tale approccio contribuisce alla protezione di modelli, dataset e infrastrutture di elaborazione.

Fonte: NIST SP 800-207; coerente con ISO/IEC 27001:2022.

131. Vulnerability Assessment

Processo sistematico di identificazione, analisi e valutazione delle vulnerabilità presenti in un sistema, al fine di determinarne livello di esposizione al rischio.

Il vulnerability assessment può includere scansioni automatiche e revisioni manuali.
Nei sistemi di IA, può riguardare infrastruttura, codice applicativo, modelli e pipeline dei dati.

Fonte: ISO/IEC 27001:2022; ISO/IEC 27005:2022.

132. Penetration Test

Attività di verifica tecnica condotta mediante simulazione controllata di attacchi informatici al fine di valutare l'efficacia delle misure di sicurezza di un sistema.

Il penetration test è eseguito in modo autorizzato e documentato.
Nei sistemi di IA, può includere test su interfacce API, meccanismi di autenticazione e protezione dei modelli.

Fonte: ISO/IEC 27001:2022; ISO/IEC 27005:2022.

G. PROCUREMENT E CONTRATTUALISTICA

133. Neutralità tecnologica

Principio secondo cui requisiti, specifiche e criteri di selezione non devono favorire o escludere determinate tecnologie, fornitori o soluzioni, ma devono essere formulati in modo funzionale e prestazionale.

La neutralità tecnologica favorisce concorrenza, interoperabilità e prevenzione del lock-in.
Nel procurement di sistemi di IA, implica la definizione di requisiti basati su risultati attesi e livelli di servizio, anziché su tecnologie specifiche.

Fonte: Coerente con principi del diritto dell'Unione europea in materia di appalti pubblici; ISO/IEC 25010:2011 (portability, interoperability).

134. Total Cost of Ownership (TCO)

Costo totale associato all'acquisizione, implementazione, esercizio, manutenzione e dismissione di un sistema lungo il suo intero ciclo di vita.

Il TCO include costi diretti e indiretti, quali infrastruttura, licenze, energia, personale, formazione e gestione del rischio.
Nei sistemi di IA, il TCO deve considerare anche costi di addestramento, monitoraggio continuo, aggiornamento dei modelli e conformità normativa.

Fonte: ISO 15686-5:2017 (life-cycle costing); coerente con ISO 20400:2017 (sustainable procurement).

135. Levelized Cost of AI (LCOAI)

Indicatore economico che rappresenta il costo medio unitario di utilizzo o di output di un sistema di intelligenza artificiale lungo il suo ciclo di vita, ottenuto rapportando il costo totale attualizzato alle unità di servizio o di valore prodotte.

Il LCOAI può includere costi di infrastruttura computazionale, addestramento, inferenza, manutenzione, aggiornamento e dismissione.
L'indicatore consente il confronto tra diverse soluzioni tecnologiche o modelli di deployment su base omogenea.

Fonte: Derivato da metodologie di levelized cost (es. ISO 15686-5:2017); applicazione al dominio IA coerente con ISO 20400:2017.

136. CAPEX (Capital Expenditure)

Spesa in conto capitale sostenuta per l'acquisizione o la realizzazione di beni durevoli o infrastrutture, con effetti economici distribuiti nel tempo.

Il CAPEX include investimenti iniziali in hardware, infrastrutture, licenze perpetue o sviluppo personalizzato.
Nei sistemi di IA, il CAPEX può comprendere costi di acquisizione di acceleratori hardware, data center o piattaforme proprietarie.

Fonte: ISO 15686-5:2017 (life-cycle costing).

137. OPEX (Operating Expenditure)

Spesa operativa sostenuta per il funzionamento corrente di un sistema o servizio.

L'OPEX include costi ricorrenti quali canoni di servizio, energia, manutenzione, supporto e aggiornamenti.
Nei modelli cloud per sistemi di IA, l'OPEX è tipicamente associato al consumo di risorse computazionali e storage.

Fonte: ISO 15686-5:2017 (life-cycle costing).

138. Vendor lock-in

Situazione nella quale un'organizzazione risulta fortemente dipendente da un fornitore specifico, con elevati costi o difficoltà tecniche nel migrare verso soluzioni alternative.

Il vendor lock-in può derivare da formati proprietari, interfacce non standard o vincoli contrattuali.
Nei sistemi di IA, il lock-in può riguardare modelli, infrastrutture cloud o servizi API proprietari.

Fonte: Coerente con ISO/IEC 25010:2011 (portability); ISO/IEC 42010:2011.

139. Reversibilità contrattuale

Principio secondo cui un contratto deve prevedere condizioni e modalità che consentano il trasferimento ordinato di dati, modelli e servizi a un altro fornitore o all'organizzazione stessa alla cessazione del rapporto contrattuale.

La reversibilità contrattuale riduce il rischio di vendor lock-in.
Può includere obblighi di cooperazione, documentazione tecnica e supporto alla migrazione.

Fonte: Coerente con principi di procurement pubblico e ISO 20400:2017.

140. Clausola di exit

Clausola contrattuale che disciplina le condizioni, i tempi e le modalità di cessazione del rapporto con il fornitore, inclusa la restituzione o trasferimento di dati e asset tecnologici.

La clausola di exit può prevedere obblighi di continuità del servizio durante la fase di transizione.
Nei contratti relativi a sistemi di IA, deve disciplinare il trasferimento di dataset, modelli e configurazioni operative.

Fonte: Coerente con ISO 20400:2017 (sustainable procurement).

141. Service Level Agreement (SLA)

Accordo contrattuale che definisce i livelli di servizio attesi, le modalità di misurazione delle prestazioni e le responsabilità delle parti in relazione alla fornitura di un servizio.

Lo SLA può includere parametri quali disponibilità, tempi di risposta, tempi di ripristino e livelli di supporto.
Nei servizi di IA, lo SLA può prevedere metriche relative a prestazioni del modello, latenza e continuità operativa.

Fonte: ISO/IEC 19086-1:2016 (Cloud Service Level Agreement framework).

142. Service Level Indicator (SLI)

Metrica quantitativa utilizzata per misurare uno specifico aspetto delle prestazioni di un servizio.

Gli SLI costituiscono la base per la verifica del rispetto degli obiettivi di servizio.
Esempi di SLI includono percentuale di disponibilità, tempo medio di risposta o tasso di errore.

Fonte: ISO/IEC 19086-1:2016; coerente con ISO/IEC 25010:2011.

143. Service Level Objective (SLO)

Valore target o intervallo di valori stabilito per uno o più Service Level Indicator, che definisce il livello di prestazione atteso per un servizio.

Gli SLO sono utilizzati per monitorare e gestire la qualità del servizio.
Il mancato raggiungimento degli SLO può attivare meccanismi correttivi o penali contrattuali.

Fonte: ISO/IEC 19086-1:2016.

144. Key Performance Indicator (KPI)

Indicatore chiave di prestazione utilizzato per misurare il livello di raggiungimento di obiettivi strategici o operativi.

I KPI possono riguardare aspetti tecnici, economici o organizzativi.
Nei sistemi di IA, i KPI possono includere metriche di qualità del modello, efficienza operativa o conformità normativa.

Fonte: ISO 9000:2015; coerente con ISO/IEC 25010:2011

<<Fine documento>>