ISACA Rome Chapter

Le prime norme e il primo standard per l'Intelligenza Artificiale

22/03/2024

Profice

Vietato ogni genere di riproduzione e divulgazione

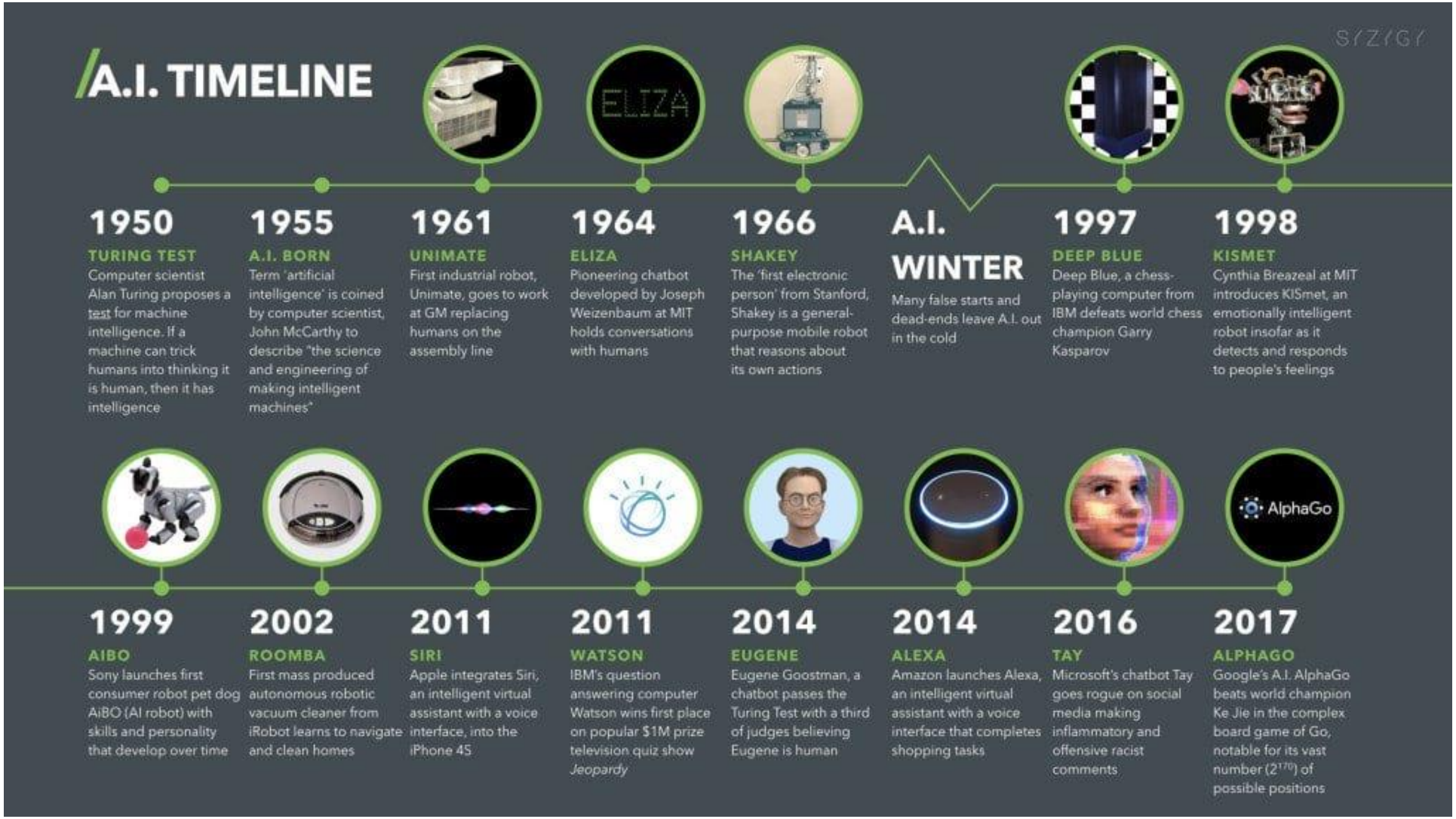
INTRODUZIONE

Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

Storia dell'AI:

Fonte *TECH4FUTURE*



Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

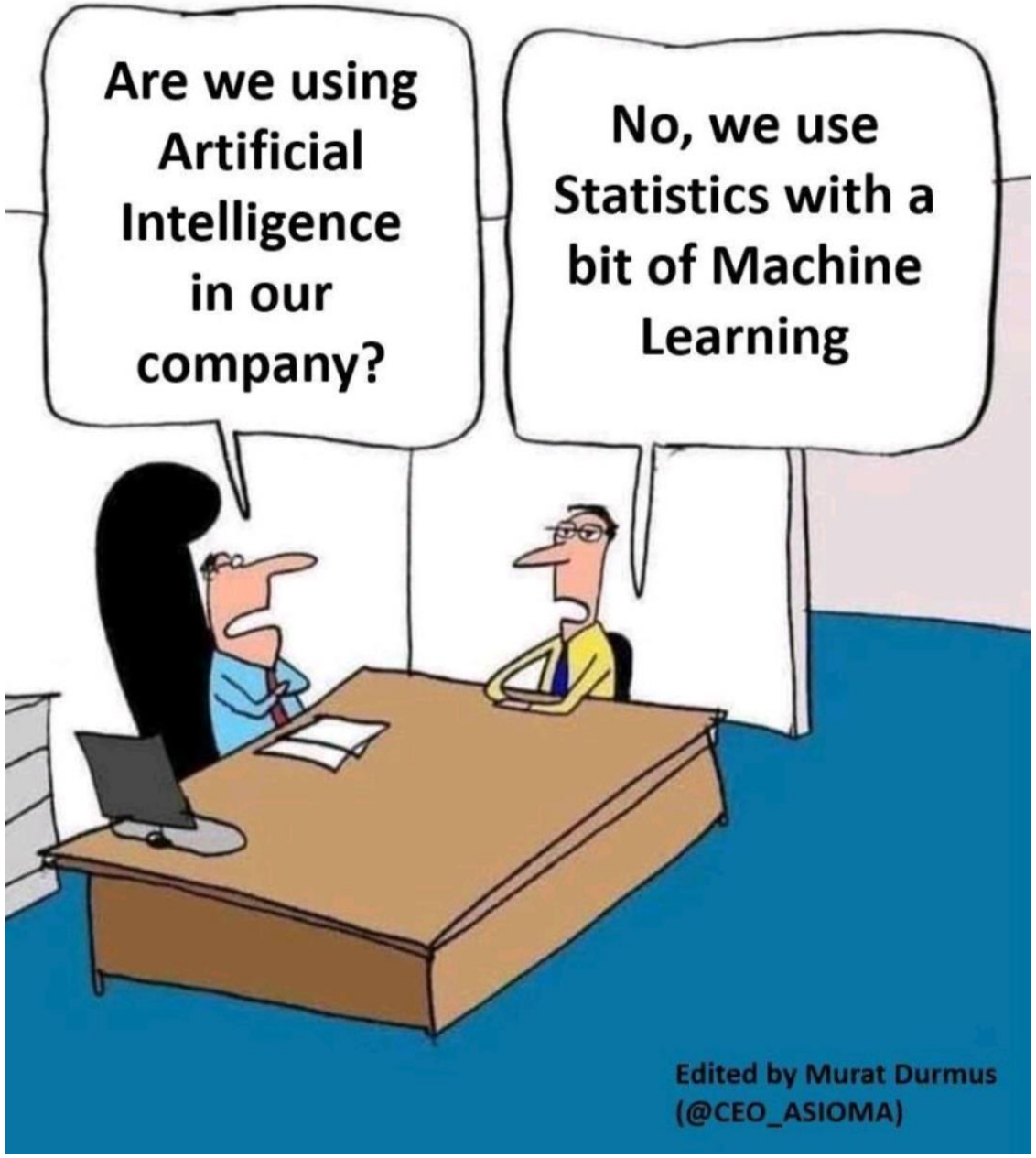
Storia dell'AI:

Fonte F. Conti Red Hot Cyber

Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

Definizioni di AI:



Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

Definizioni di AI:

Non esiste una definizione unica di AI

- Principali capacità e discipline scientifiche. Gruppo di esperti ad alto livello sull'intelligenza artificiale della Commissione Europea, aprile 2019;
- L'intelligenza artificiale è la scienza del far eseguire alle macchine le cose che richiederebbero intelligenza se fatte dall'uomo, Marvin Minsky;
- La capacità di un sistema di interpretare correttamente i dati esterni, di apprendere da tali dati e di utilizzare tali apprendimenti per raggiungere obiettivi e compiti specifici attraverso l'adattamento flessibile, Kaplan e Haenlein;
- Il campo che studia la sintesi e l'analisi di agenti computazionali che agiscono in modo intelligente, Poole e Mackworth;
- Lo studio di agenti, però intelligenti, che ricevono precetti dall'ambiente e agiscono. Ciascuno di questi agenti è implementato da una funzione che mappa le percezioni alle azioni, esistono diversi modi per rappresentare queste funzioni: come sistemi di produzione, agenti reattivi, pianificatori logici, reti neurali e sistemi di teoria delle decisioni, Russell e Norvig
- Ricerca e sviluppo di meccanismi e applicazioni dei sistemi di IA, ISO 22989
- Art.3 AI Act: «sistema di IA»: un sistema basato su macchine progettato per funzionare con diversi livelli di autonomia e che può mostrare capacità di adattamento dopo l'impiego e che, per obiettivi espliciti o impliciti, deduce, dall'input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare gli ambienti fisici o virtuali;

Vietato ogni genere di riproduzione e divulgazione

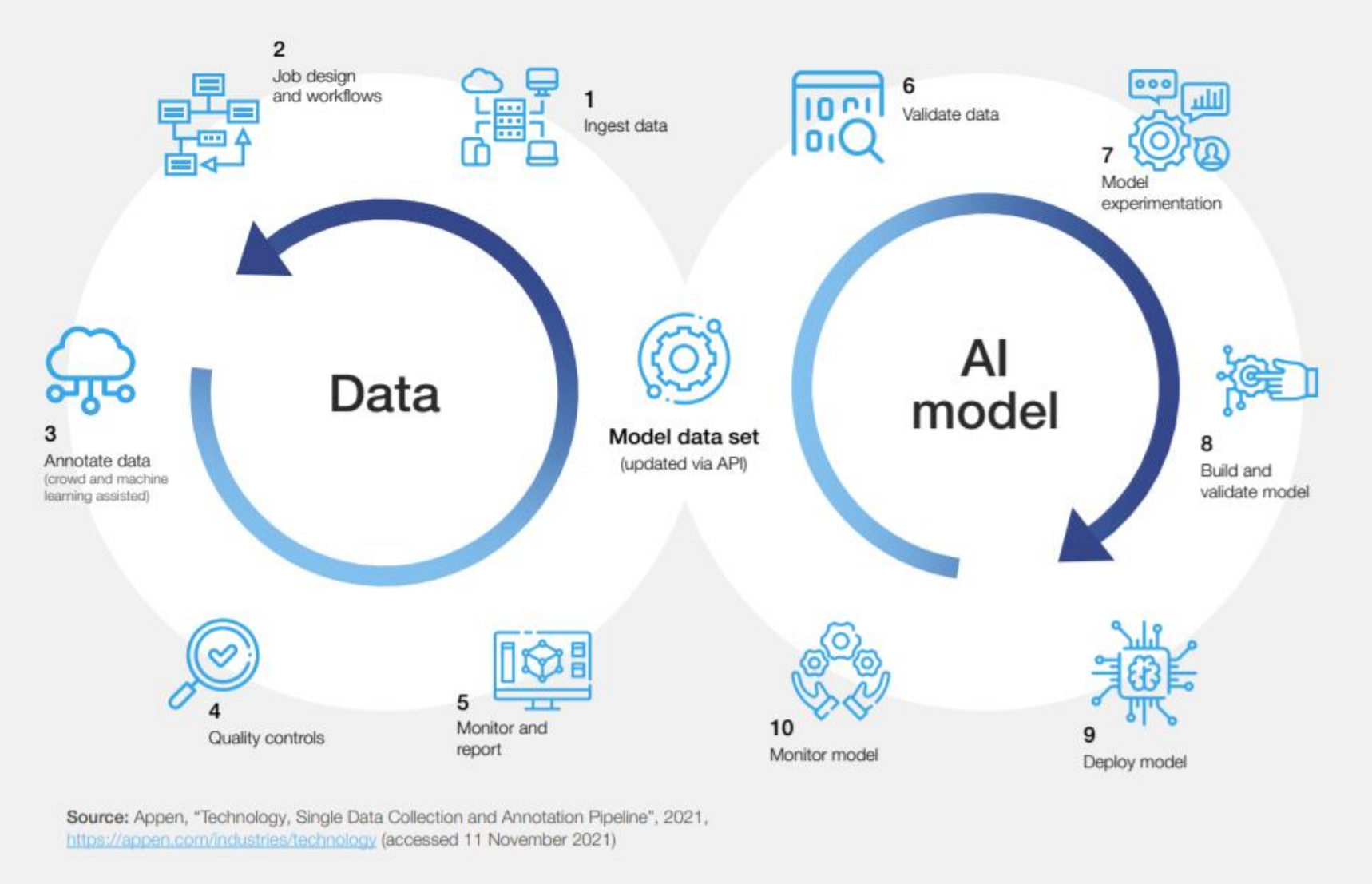
INTRODUZIONE

Esempi di AI:

Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

Ciclo di vita di AI:



Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

I principi dell'AI:

- Dignità e supervisione umana;
- Robustezza e sicurezza;
- Privacy e governance dei dati;
- Trasparenza;
- Diversità, non discriminazione ed equità;
- Benessere sociale e ambientale;
- Accountability.

Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

I principi dell'AI:

1. Supervisione umana e dunque che i sistemi di AI siano sorvegliati da personale umano, a garanzia del rispetto dei diritti fondamentali e del benessere dell'utente;

2. Robustezza e sicurezza, intese come sicurezza ed affidabilità degli algoritmi e come tenuta dei sistemi di controllo in caso di ipotetiche operazioni illecite;

3. Privacy, controllo e gestione dei dati;

4. Trasparenza a garanzia della tracciabilità dei sistemi e a dimostrazione delle operazioni compiute dell'algoritmo;

5. Diversità, correttezza, assenza di discriminazione: i sistemi di intelligenza artificiale dovrebbero tenere conto delle diverse e distinte abilità e capacità umane, al tempo stesso garantendo a tutti il libero accesso a tali strumenti;

6. Benessere sociale e ambientale, ossia avere sempre riguardo all'impatto sull'ambiente e sull'assetto sociale, promuovendo l'utilizzo dell'AI solo laddove il suo utilizzo possa garantire uno sviluppo sostenibile;

7. Responsabilità, ovvero verifica continua dei sistemi, sia internamente che esternamente.

Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

La governance dell’AI:

La governance dovrebbe garantire che le sue pratiche siano adatte allo scopo per gli usi specifici a cui l'IA viene applicata all'interno dell'organizzazione. Ciò può includere la revisione e, se necessario, il miglioramento di:

— Direzione: attraverso la politica, la strategia, l'allocazione delle risorse, i codici etici, le dichiarazioni di valori, lo scopo o altri strumenti relativi all'uso dell'IA nell'organizzazione;

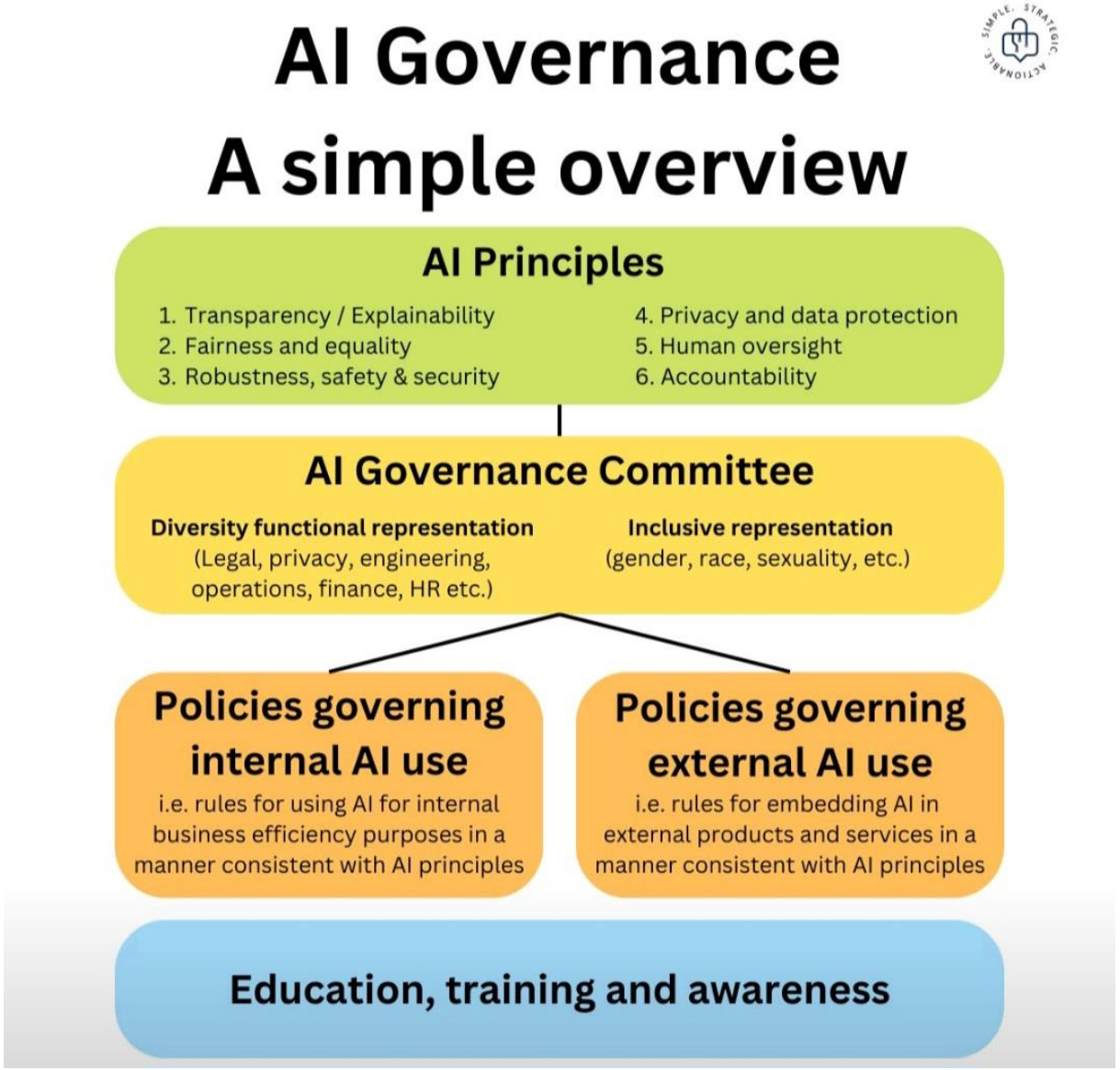
— Supervisione: attraverso una valutazione dell'IA, una valutazione del suo valore per l'organizzazione e la propensione al rischio dell'organizzazione e la garanzia di implementazione, monitoraggio, misurazione, assicurazione delle decisioni e altri meccanismi relativi all'uso dell'IA nell'organizzazione;

— Valutazione: considerare diversi elementi, ad esempio i fattori interni ed esterni relativi all'organizzazione, le minacce e le opportunità attuali e future, i risultati raggiunti, l'efficacia e l'efficienza dei meccanismi di governance in atto e i giudizi sulle decisioni e le opzioni adottate.

— Reporting: dimostrare alle parti interessate che l'uso dell'IA è effettivamente disciplinato da coloro che sono responsabili (confronta questo con i compiti di "valutare", "dirigere" e "monitorare" in ISO/IEC 38500:2015, 4.2).

Vietato ogni genere di riproduzione e divulgazione

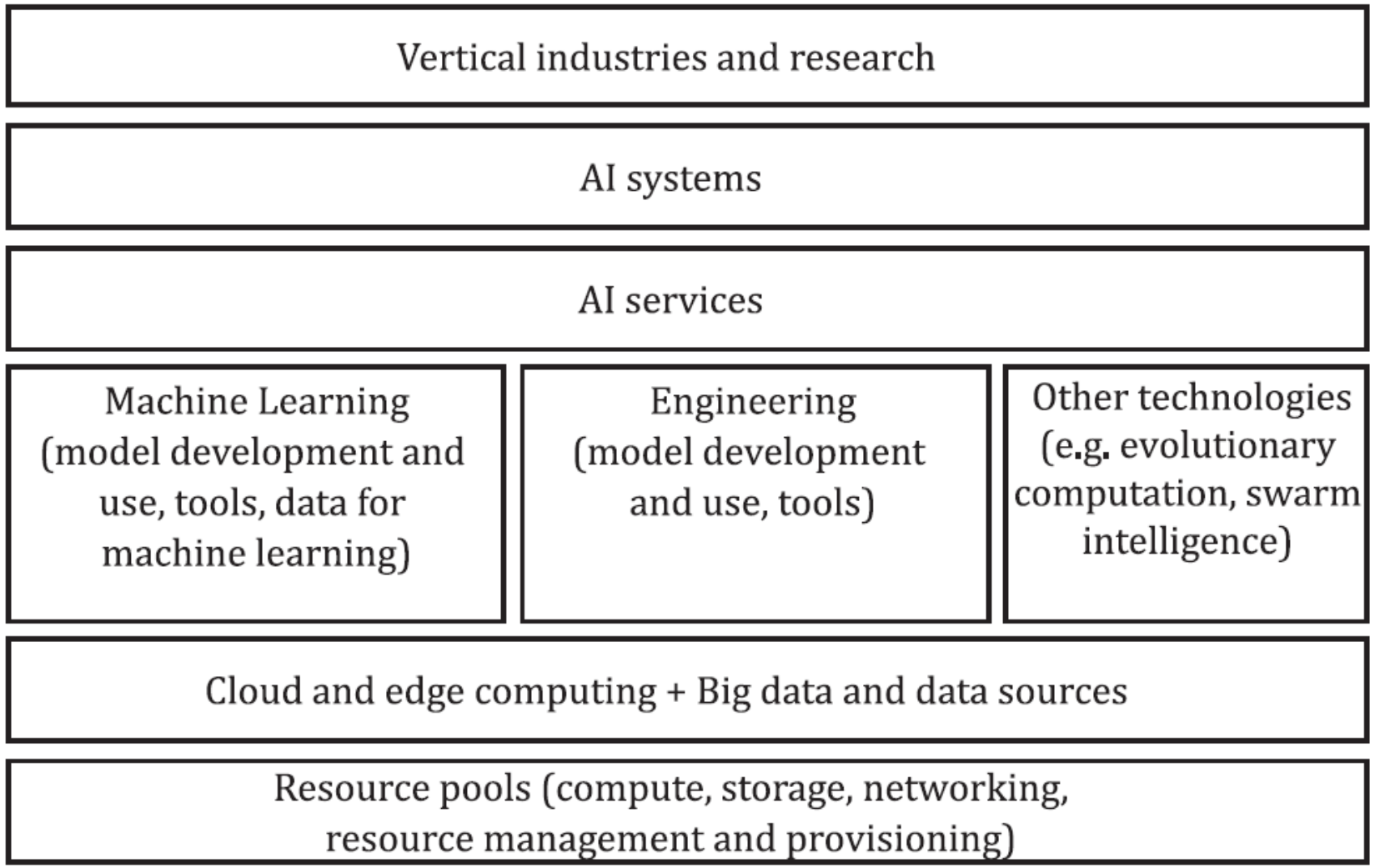
INTRODUZIONE



Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

Eco sistema dell'AI:



Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

I rischi dell'AI:

R1: Perdita di autonomia personale

R2: Responsabilità per i danni causati dai sistemi di AI

R3: Rischio di errori e manipolazione dell'AI

R4: Manipolazione, sorveglianza e comportamento illecito

R5: Perdita della privacy

R6: Mancanza di trasparenza dell'AI

R7: Perdita degli aspetti umani nelle relazioni sociali e mancanza di protezione della vita umana e della dignità umana

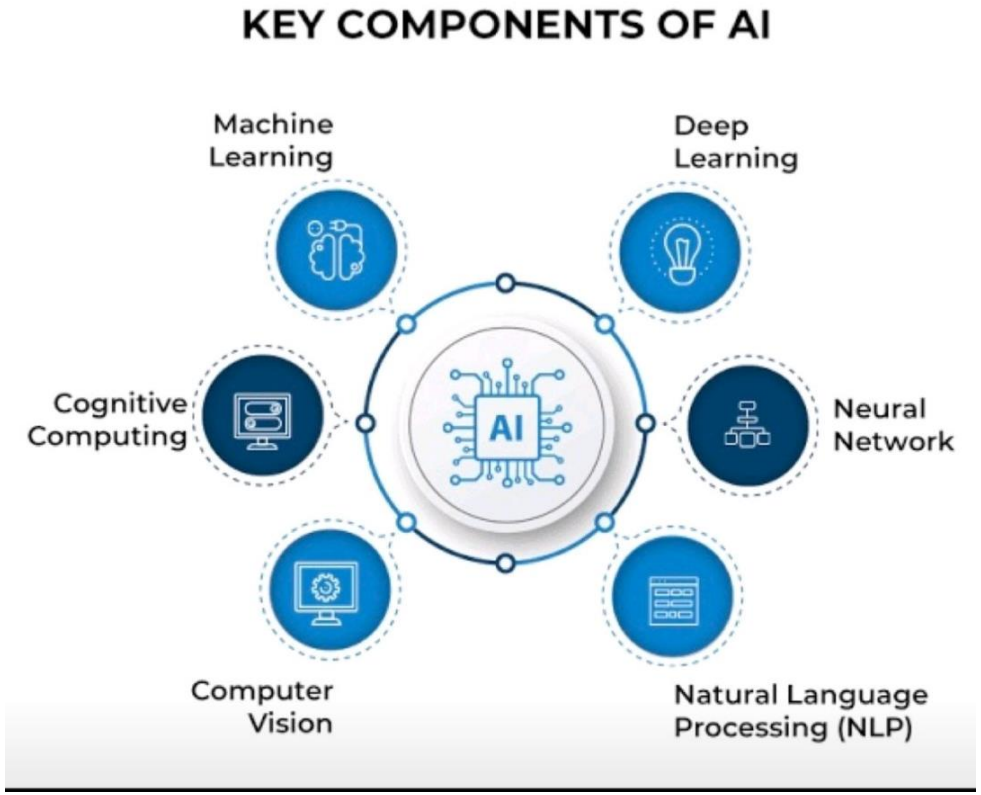
R8: Restrizione della pluralità delle opinioni e della concorrenza

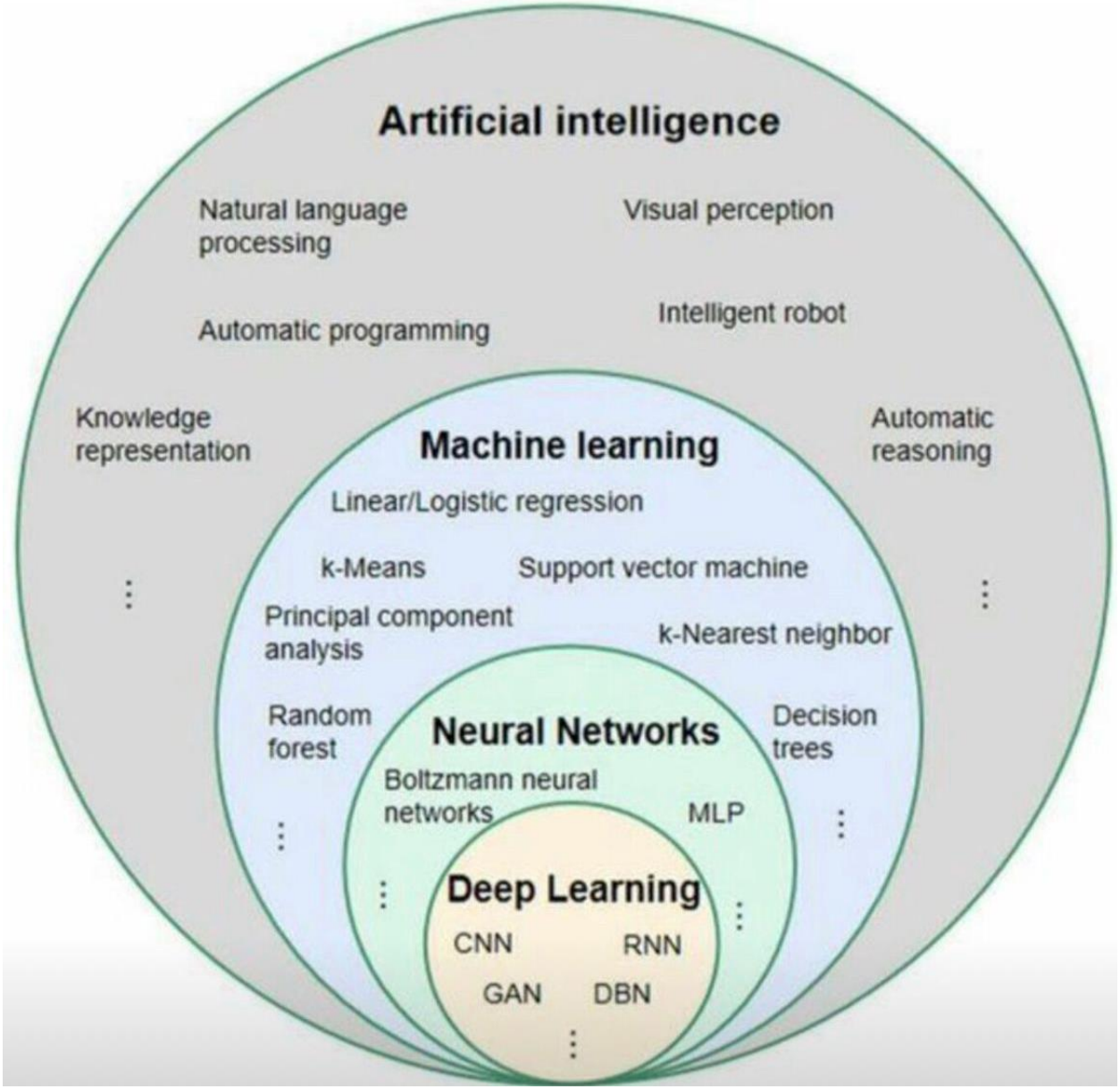
R9: Perdita dei posti di lavoro

Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

Il sistema AI





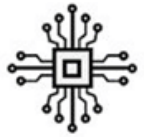
Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

Confronto fra le intelligenze

Fonte: Ninja Academy

Fonte: IntelligenzaArtificialeItalia

	Weight	Space	Processor Speed	Energy Efficiency
	3 pounds (1.4 kg)	1/6 basketball (80 cubic inches or 1,300 cm^3)	Up to 1,000,000 trillion operations per second	20 watts
	150 tons	Basketball court (cabinets over 4,350 square feet, or 400 m^2)	93,000 trillion operations per second	10 million watts

Nature	AI: Artificial	HI: Human
Flexibility	Less flexible	More flexible
Creativity	Less creative	More creative
Learning power	Rapid and precise	Complex and integrated

Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

Confronto fra le intelligenze

Fonte: IntelligenzaArtificialeItalia

Parametri	Intelligenza Umana	Intelligenza Artificiale
Evoluzione	Le abilità cognitive di pensare, ragionare, valutare e così via sono innati negli esseri umani.	Norbert Wiener, che ha ipotizzato meccanismi di critica, è accreditato di aver fatto un contributo significativo precoce allo sviluppo dell'intelligenza artificiale (IA).
Essenza	Lo scopo dell'intelligenza umana è quello di combinare una serie di attività cognitive al fine di adattarsi a nuove circostanze.	L'obiettivo dell'intelligenza artificiale (IA) è quello di creare computer in grado di comportarsi come esseri umani e di completare lavori che normalmente gli umani farebbero.
Funzionalità	Le persone fanno uso della memoria, delle capacità di elaborazione e dei talenti cognitivi che il loro cervello fornisce.	L'elaborazione dei dati e dei comandi è essenziale per il funzionamento dei dispositivi alimentati dall'IA.
Velocità di esecuzione	Per quanto riguarda la velocità, gli umani non sono all'altezza dell'intelligenza artificiale o dei robot.	I computer hanno la capacità di elaborare molte più informazioni a una velocità superiore rispetto alle persone.
Capacità di apprendimento	La base dell'intelletto umano è acquisita attraverso il processo di apprendimento attraverso una varietà di esperienze e situazioni.	Poiché i robot non possono pensare in modo astratto o trarre conclusioni basate sulle esperienze del passato, sono in grado di acquisire conoscenze solo attraverso l'esposizione al materiale e la pratica costante, anche se non creeranno mai un processo cognitivo unico per gli umani.
Decisioni	È possibile che fattori soggettivi che non si basano solo sui numeri influenzino le decisioni che prendono gli esseri umani.	Poiché valuta in base alla totalità dei fatti acquisiti, l'IA è eccezionalmente oggettiva quando si tratta di prendere decisioni.
Perfezione	Per quanto riguarda le intuizioni umane, c'è quasi sempre la possibilità di "errore umano", che si riferisce al fatto che alcuni dettagli potrebbero essere trascurati in un momento o nell'altro.	Il fatto che le capacità dell'IA si basino su una serie di linee guida che possono essere aggiornate le consente di fornire risultati accurati regolarmente.

Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

Tipi di AI: Machine Learning:

L'apprendimento automatico (ML) è un campo dell'informatica nato dalla ricerca sull'intelligenza artificiale. La forza dell'apprendimento automatico rispetto ad altre forme di analisi è nella sua capacità di scoprire intuizioni nascoste e prevedere i risultati di input futuri non visibili. Il ML non è certo completamente automatizzato ma necessità di attività umane per poter apprendere in che modo programmarsi e operare in modo automatico.

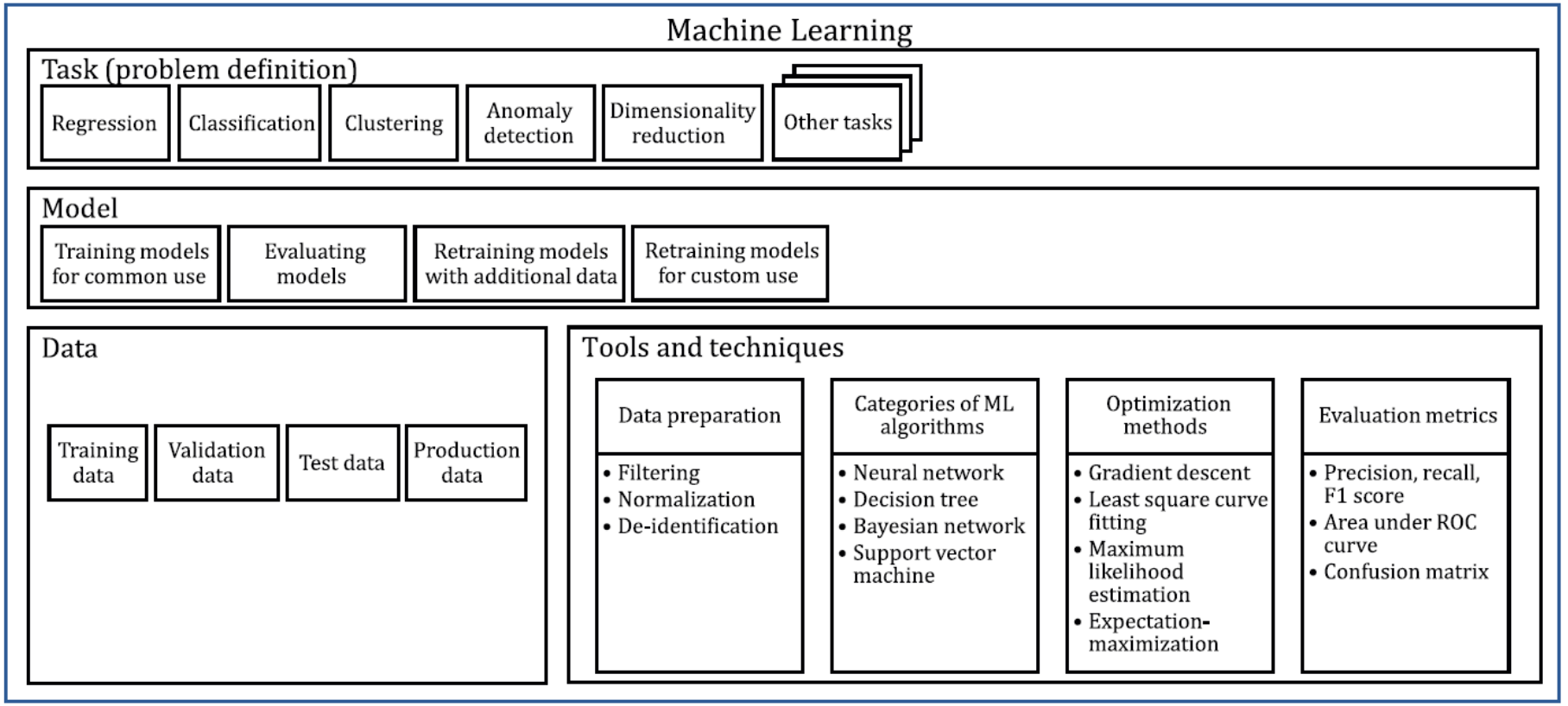
Le attività classiche e tipiche del ML sono sotto riportate:

- Clustering
- Classificazione
- Categorizzazione
- Filtro/Selezione
- Riconoscimento (pattern recognition)
- Simulazione di giochi
- Comportamento autonomo

Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

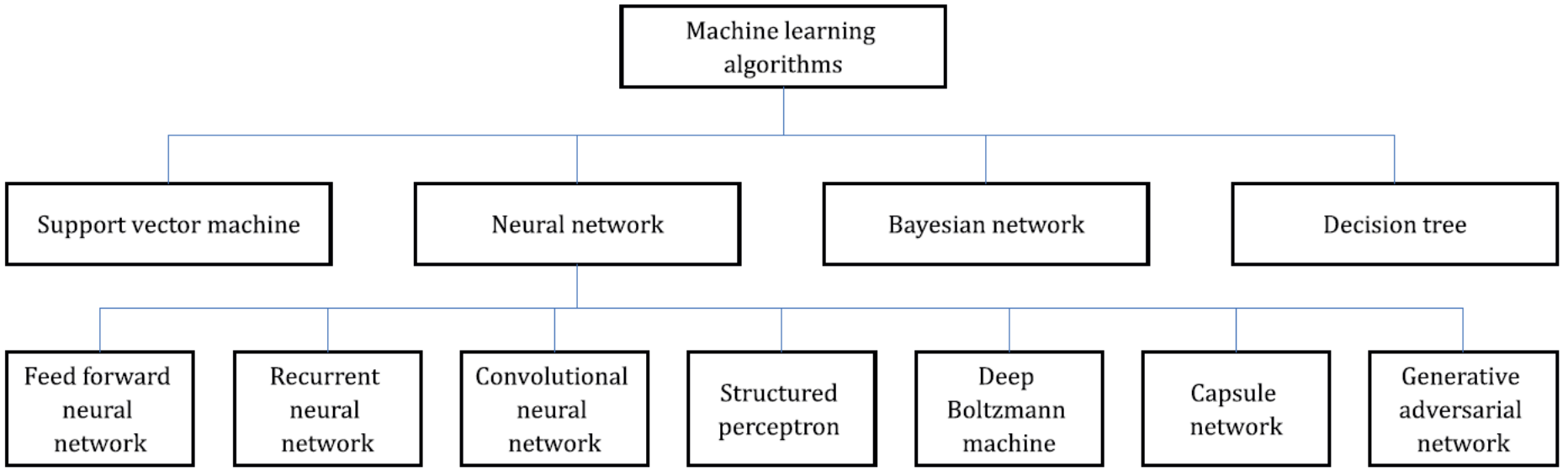
Elementi del sistema Machine Learning:



Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

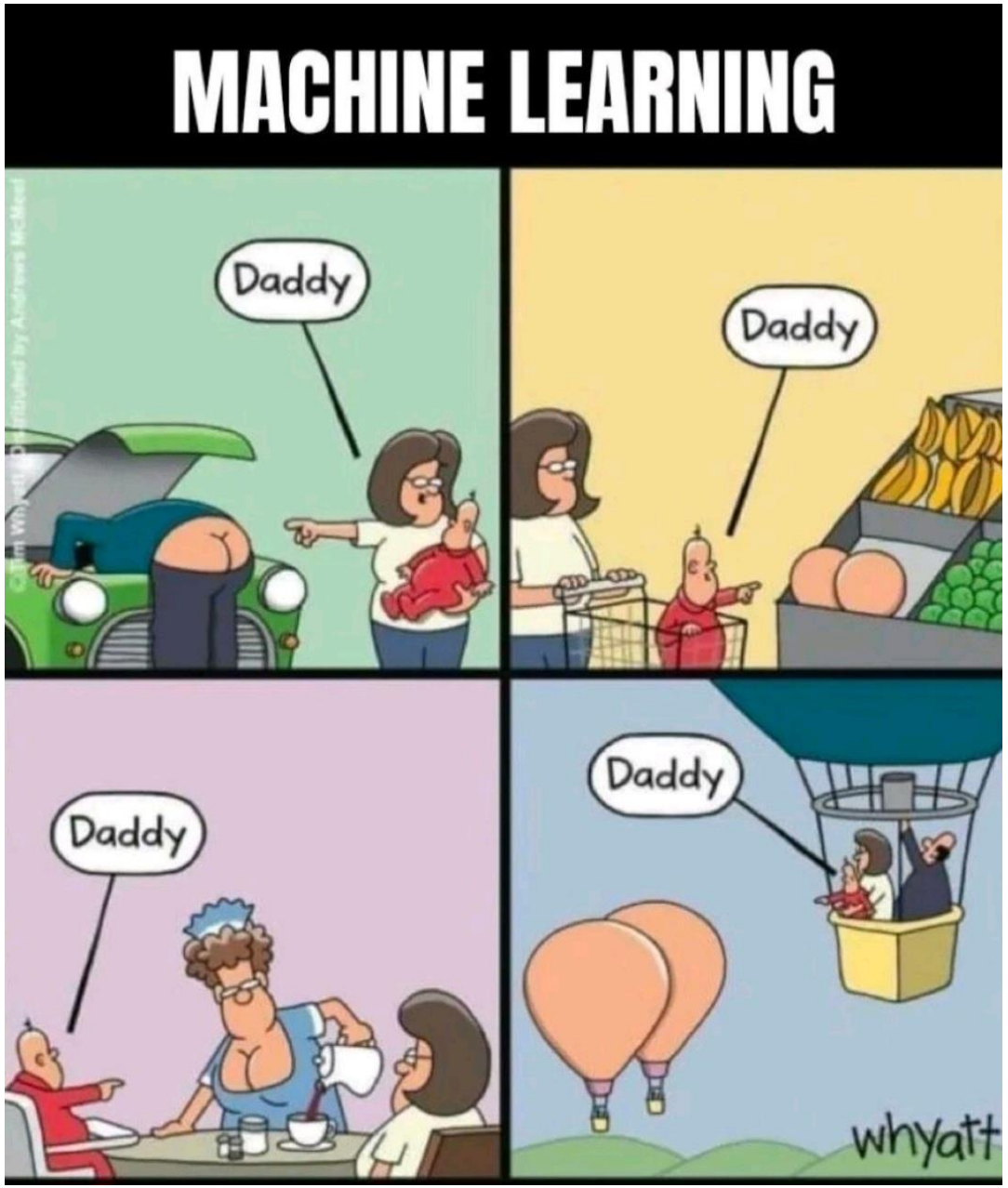
Esempi di algoritmi di Machine Learning:



Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

Come impara l’algoritmo?



Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

Tipi di AI (ML):

- **Apprendimento supervisionato**

L'apprendimento supervisionato è un tipo di algoritmo di apprendimento automatico che utilizza un set di dati noto (chiamato set di dati di addestramento) per effettuare previsioni. L'apprendimento supervisionato ha lo scopo di trovare modelli nei dati che possono essere applicati a un processo di analisi.

- **Apprendimento senza supervisione.**

L'apprendimento senza supervisione ci permette di affrontare i problemi con poca o nessuna idea di come dovrebbero essere i nostri risultati. Possiamo ricavare la struttura da dati in cui non conosciamo necessariamente l'effetto delle variabili. L'apprendimento non supervisionato è più adatto quando il problema richiede un'enorme quantità di dati senza etichetta.

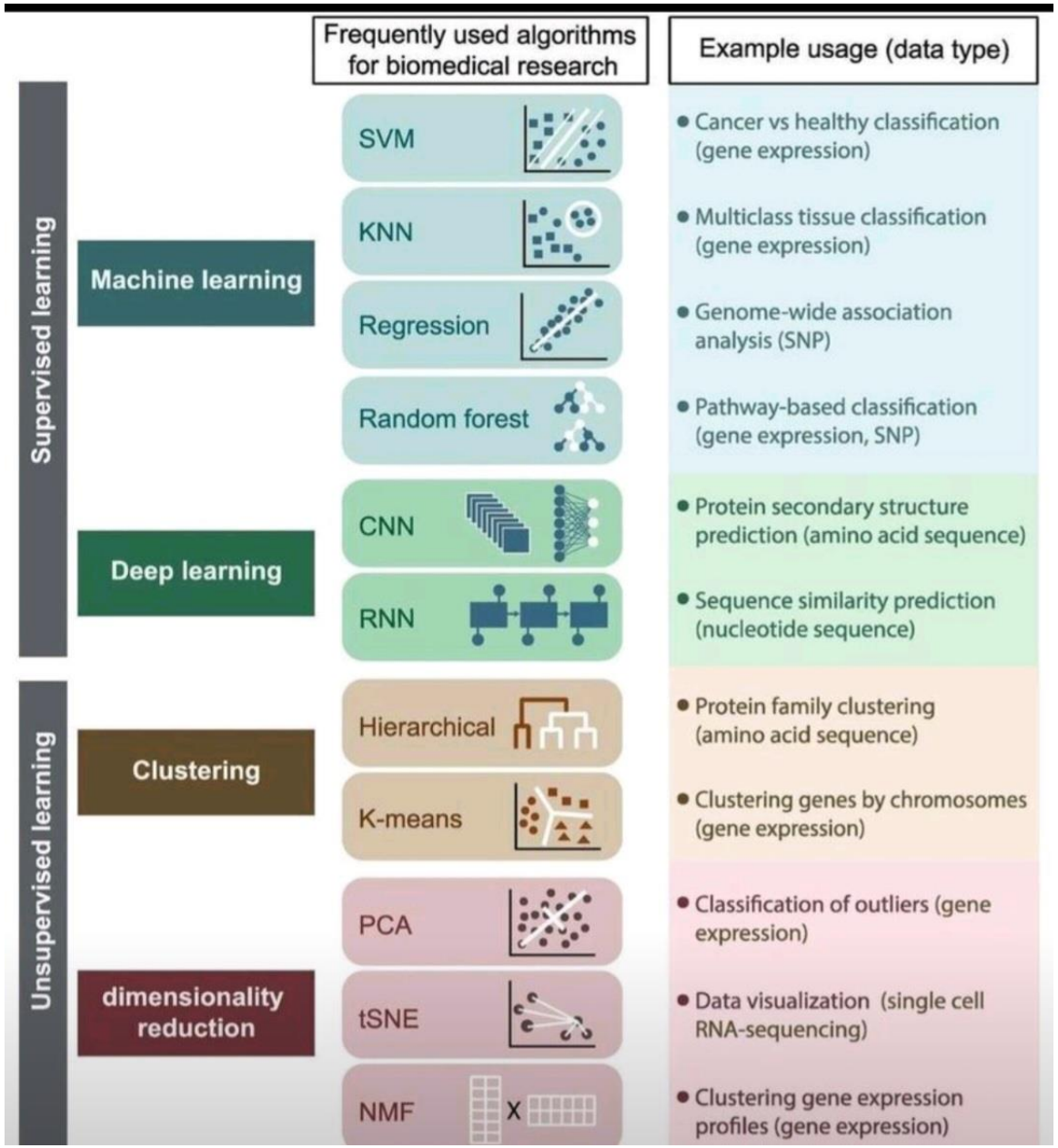
- **Apprendimento di rinforzo.**

L'apprendimento per rinforzo è un modello di apprendimento comportamentale. L'algoritmo riceve feedback dall'analisi dei dati in modo che l'utente sia guidato al miglior risultato. L'apprendimento per rinforzo si distingue da altri tipi di apprendimento supervisionato perché il sistema non è addestrato con il set di dati di esempio. Il sistema prova attraverso tentativi ed errori.

Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

ESEMPIO Tipi di AI (ML):



Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

Tipi di AI: **Deep Learning (apprendimento profondo)**

L'Apprendimento profondo è una parte dell'apprendimento automatico, in cui le reti neurali artificiali multistrato (stati successivi) sono utilizzate con lo scopo di apprendere in modo iterativo, regolandosi continuamente fino a raggiungere uno specifico punto di arresto. Il DL cerca di emulare/simulare il funzionamento del nostro cervello attraverso lo studio dei neuroni e delle sinapsi, riproducendo delle reti artificiali in modo che i computer possano essere addestrati ad affrontare astrazioni e problemi scarsamente definiti.

Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

Altri tipi di AI:

Natural Language Processing (NLP) – elaborazione del linguaggio naturale

Il NLP si riferisce al trattamento informatico (computer processing) del linguaggio naturale, per qualsiasi scopo, indipendente dal livello di approfondimento dell'analisi.

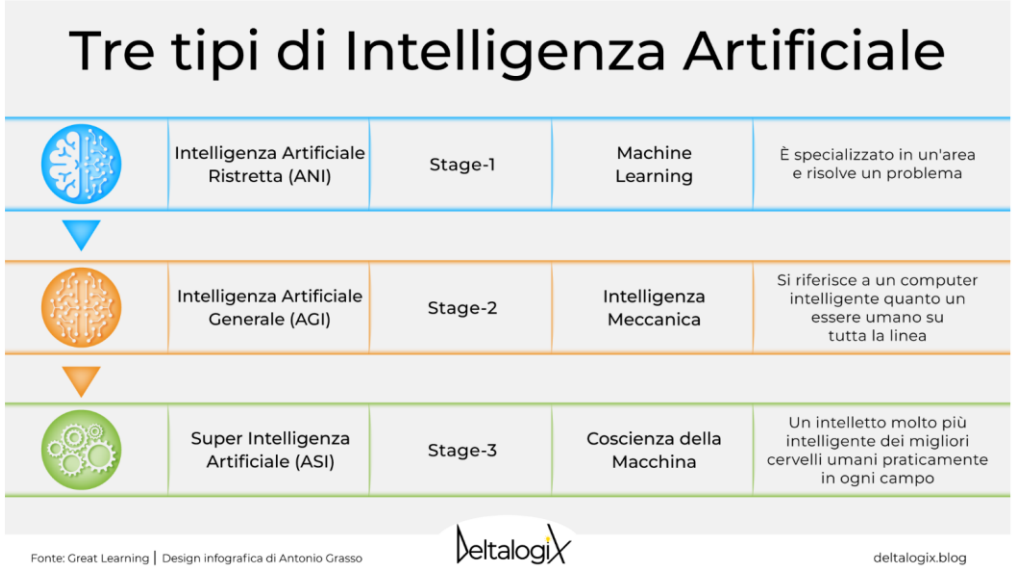
Computational Linguistics (CL) - questa è una materia interdisciplinare che comprende Informatica e Linguistica.

Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

In generale esistono tre tipi di AI:

- Intelligenza artificiale stretta (ANI), che ha una gamma ristretta di abilità, definita anche come debole o stretta;
- Intelligenza generale artificiale (AGI), che è alla pari con le capacità umane, definita anche come AI forte o profonda;
- Super intelligenza artificiale (ASI), che risulta più capace di un essere umano.



Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

In generale esistono tre tipi di AI:

ANI

L'intelligenza artificiale stretta (ANI), nota anche come AI debole o AI stretta, è l'unico tipo di intelligenza artificiale che abbiamo realizzato con successo fino ad oggi. L'intelligenza artificiale stretta è orientata agli obiettivi, progettata per eseguire compiti singoli, come ad esempio riconoscimento facciale, riconoscimento vocale, assistenti vocali, guidare un'auto o cercare in Internet, ed è molto intelligente nel completare l'attività specifica per cui è programmata.

AGI

L'intelligenza generale artificiale è il concetto di una macchina con intelligenza generale che imita l'intelligenza e/o i comportamenti umani, con la capacità di apprendere e applicare la sua intelligenza per risolvere qualsiasi problema. AGI può pensare, capire e agire in un modo che è indistinguibile da quello di un essere umano in una determinata situazione.

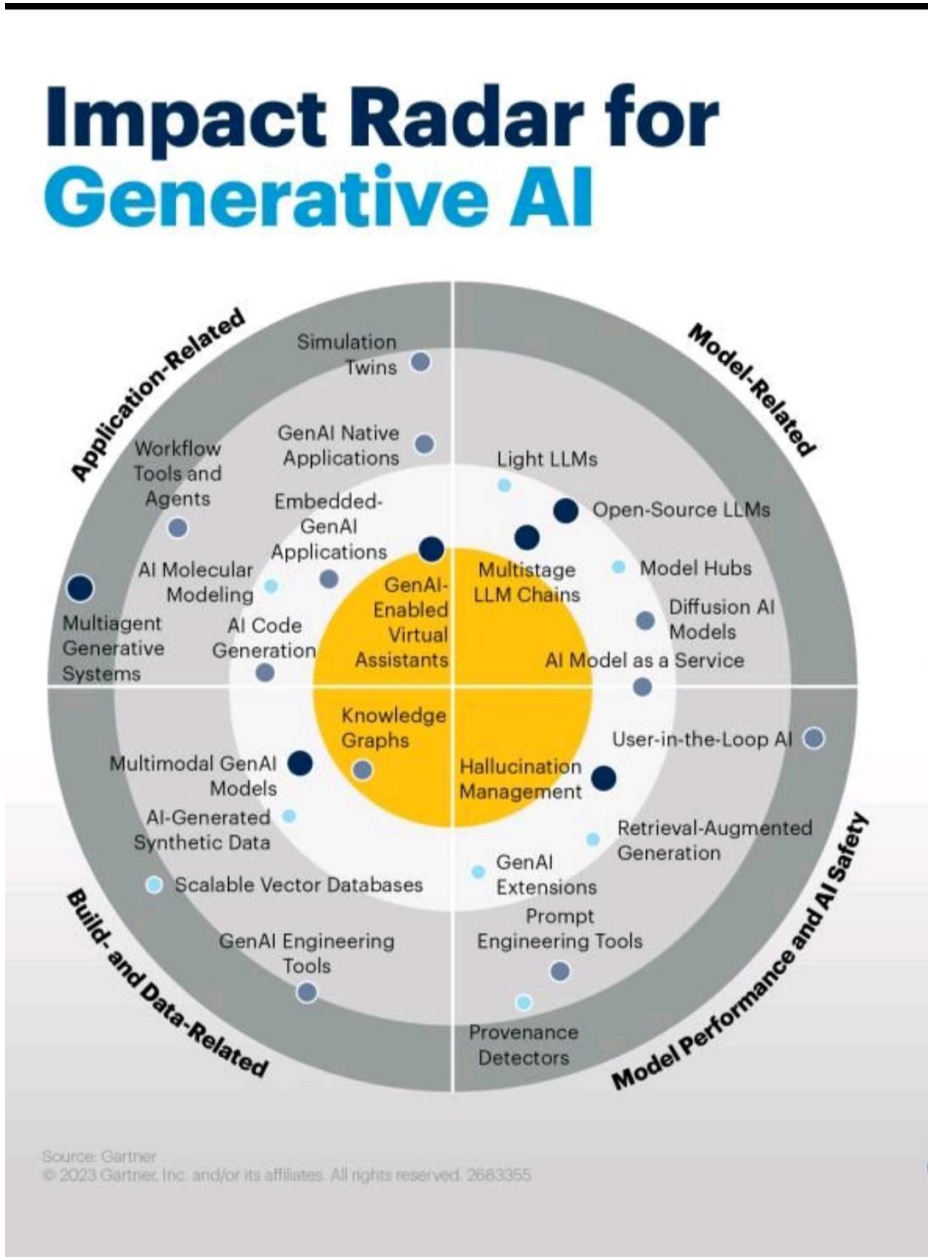
ASI

La super intelligenza artificiale è la fantascientifica AI che non si limita a imitare o comprendere l'intelligenza e il comportamento umano; l'ASI è il luogo in cui le macchine acquisiscono consapevolezza di sé e superano le capacità dell'intelligenza e delle capacità umane, evolvendosi per essere così simile alle emozioni e alle esperienze umane, che non solo le comprende, ma evoca emozioni, bisogni, convinzioni e desideri propri.

Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

Esempio Generative AI:

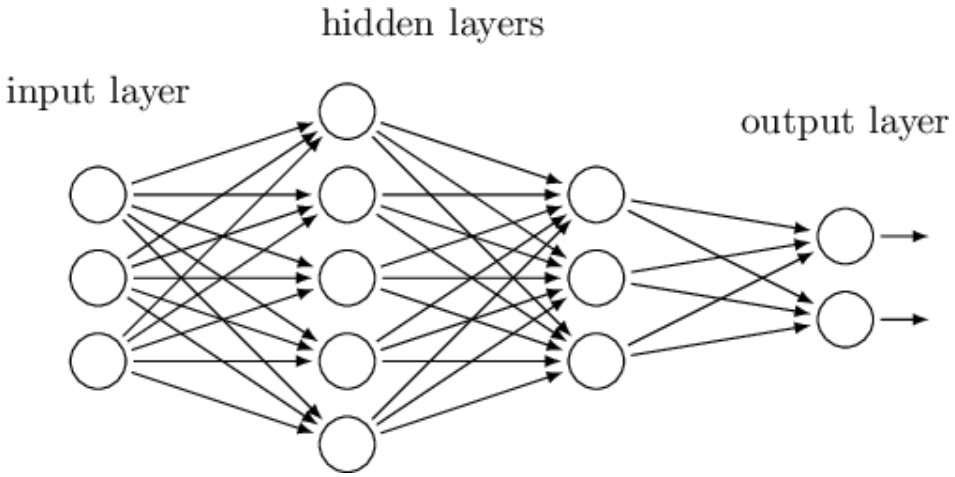


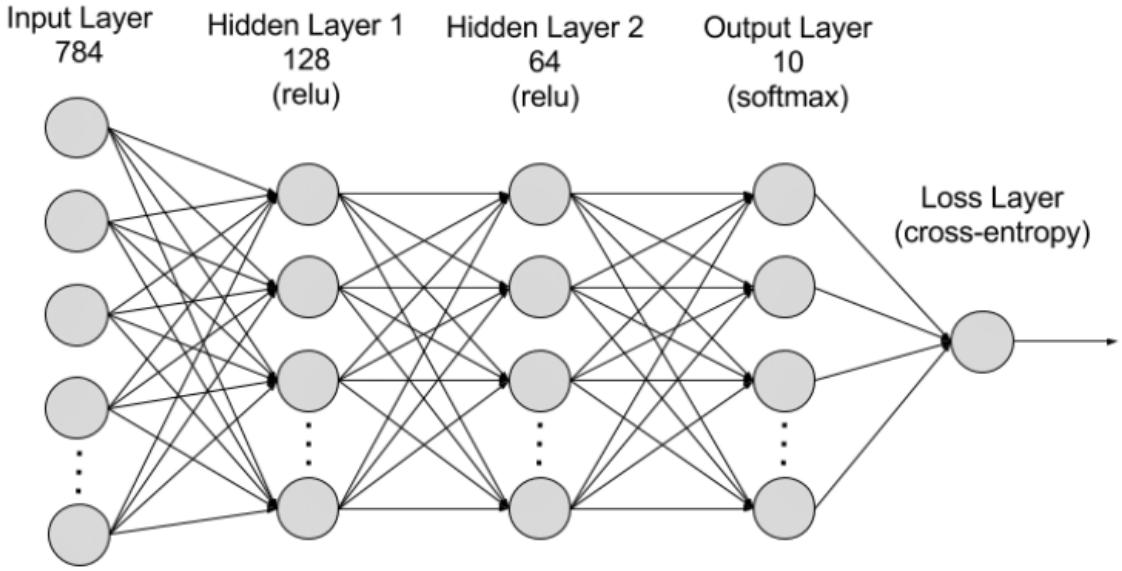
Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

Tipi di Reti Neurali:

Nel campo dell'apprendimento automatico, una rete neurale artificiale è un modello computazionale composto di "neuroni" artificiali, ispirato vagamente alla semplificazione di una rete neurale biologica.

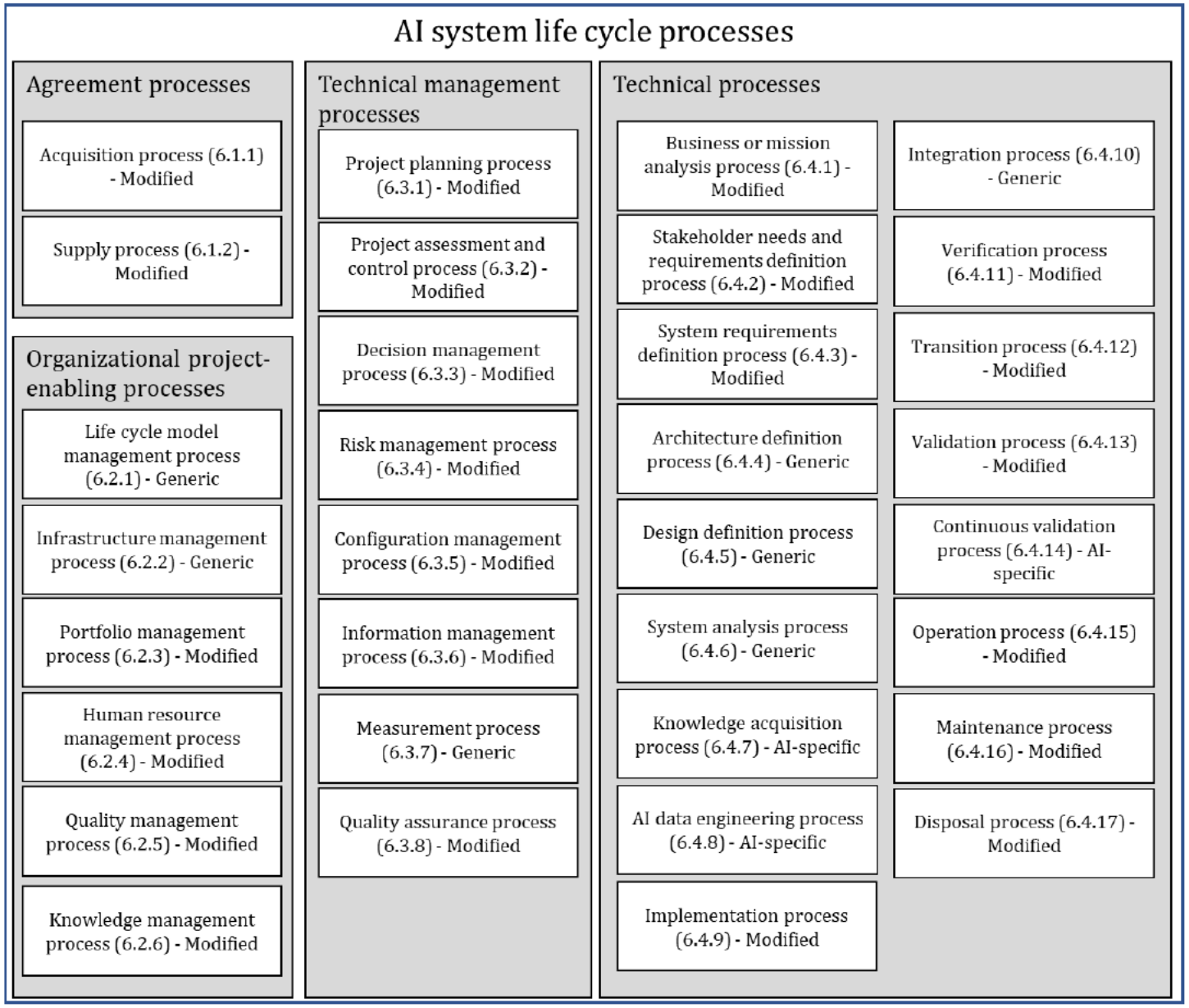




Vietato ogni genere di riproduzione e divulgazione

INTRODUZIONE

ISO 5338 Information technology — Artificial intelligence — AI system life cycle processes



Vietato ogni genere di riproduzione e divulgazione

LA NORME DI RIFERIMENTO

Norme di riferimento. Alcune delle norme elencate sono ancora in versione Draft o DIS

- ISO/IEC 24028 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence
- ISO/IEC 24027 Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making
- ISO/IEC 24368 Information technology — Artificial intelligence — Overview of ethical and societal concerns
- ISO/IEC 4213 Information technology — Artificial intelligence — Assessment of machine learning classification performance
- ISO/IEC 5259 1-5 Data quality for analytics and machine learning (ML) ISO/IEC 5339
- ISO/IEC 5469 Artificial intelligence — Functional safety and AI systems
- ISO/IEC 6254 Information technology — Artificial intelligence — Objectives and approaches for explainability of ML models and AI systems
- ISO/IEC 23053 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
- ISO/IEC 23894 Information technology — Artificial intelligence — Guidance on risk management
- ISO/IEC 38507 Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations
- ISO/IEC WD 5338 Information technology — Artificial intelligence — AI system life cycle processes

Vietato ogni genere di riproduzione e divulgazione

LA NORME DI RIFERIMENTO

- ISO/IEC WD 22989: Concetti e terminologia dell'intelligenza artificiale
- ISO/IEC NP TR 24027: Tecnologia dell'informazione — Intelligenza artificiale (AI) — Pregiudizio nei sistemi di IA e processo decisionale assistito dall'IA
- ISO/IEC 42005 - Tecnologia dell'informazione — Intelligenza artificiale (AI) Valutazione d'impatto dei sistemi IA
- ISO/IEC NP TR 24028: Tecnologia dell'informazione — Intelligenza artificiale (AI) — Panoramica del trustworthiness nell'intelligenza artificiale
- ISO/IEC NP TR 24029-1: Intelligenza Artificiale (AI) — Valutazione della robustezza delle reti neurali Parte 1: Panoramica
- ISO/IEC NP TR 24030: Tecnologia dell'informazione — Intelligenza artificiale (AI) — Casi d'uso
- ISO/IEC NP 23894: Tecnologia dell'informazione — Intelligenza artificiale — Gestione del rischio
- ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements
- NIST AI 100-1 Artificial Intelligence Risk Management Framework (AI RMF 1.0)
- REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

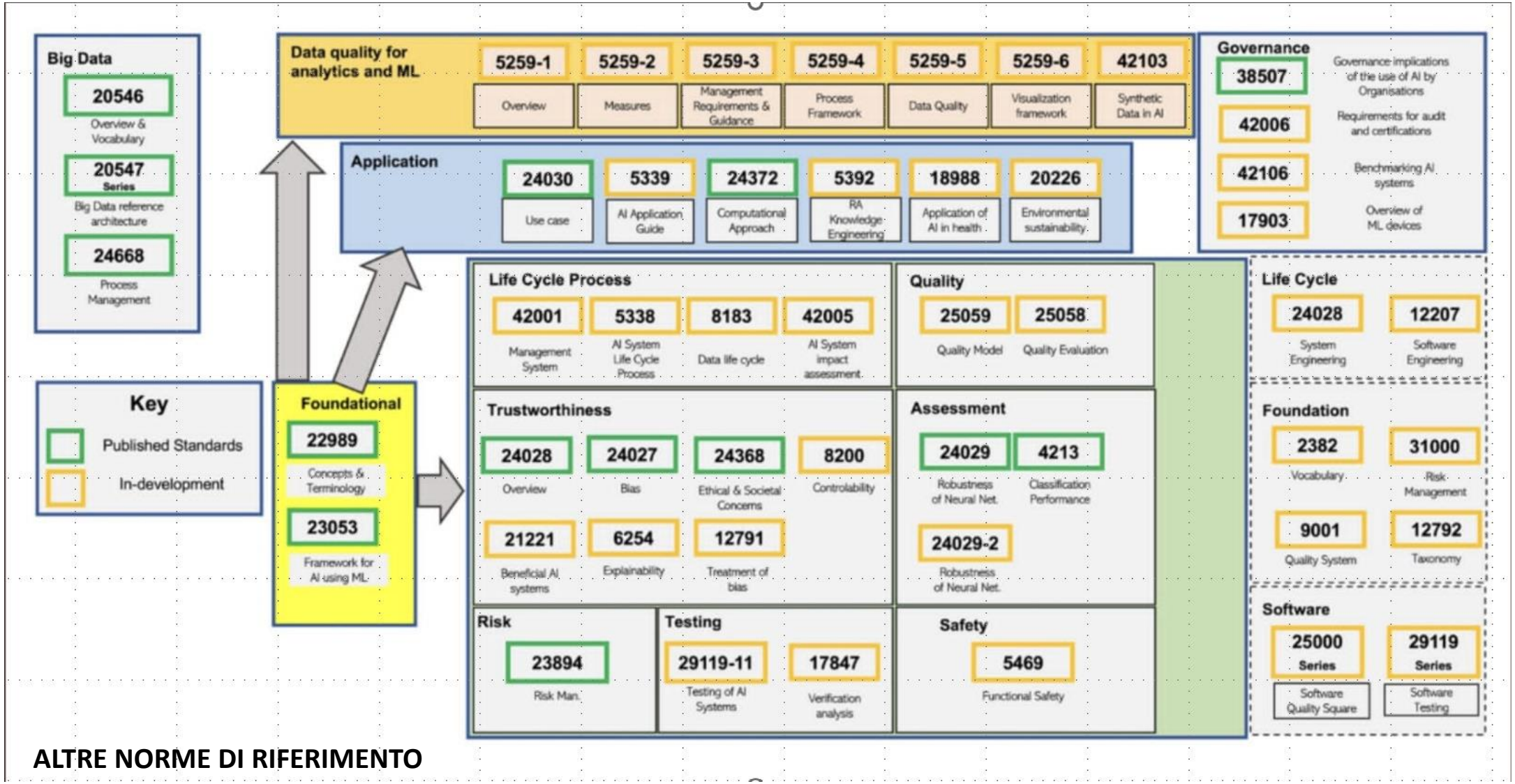
Vietato ogni genere di riproduzione e divulgazione

LA NORME DI RIFERIMENTO

- ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls
- ISO/IEC 27005 Information technology — Security techniques — Information security risk management
- ISO 22301 Security and resilience — Business continuity management systems — Requirements ISO 22320
- ISO 22313 Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
- ISO/TS 22317:2015 Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)
- ISO/IEC DIS 22989 - Information technology — Artificial intelligence — Artificial intelligence concepts and terminology
- ISO/IEC AWI TR 24372 Information technology — Artificial intelligence (AI) — Overview of computational approaches for AI systems
- ISO 31000 Risk management — Principles and guidelines
- ISO 9001 Quality management systems — Requirements
- ISO/IEC 20000-1 Information technology — Service management — Part 1: Service management system requirements
- NISTIR 82692 A Taxonomy and Terminology of Adversarial Machine Learning
- NISTIR 8312 Four Principles of Explainable Artificial Intelligence
- NISTIR 8367 Psychological Foundations of Explainability and Interpretability in Artificial Intelligence
- NIST Special Publication 1270 Towards a Standard for Identifying and Managing Bias in Artificial Intelligence

Vietato ogni genere di riproduzione e divulgazione

LA NORME DI RIFERIMENTO



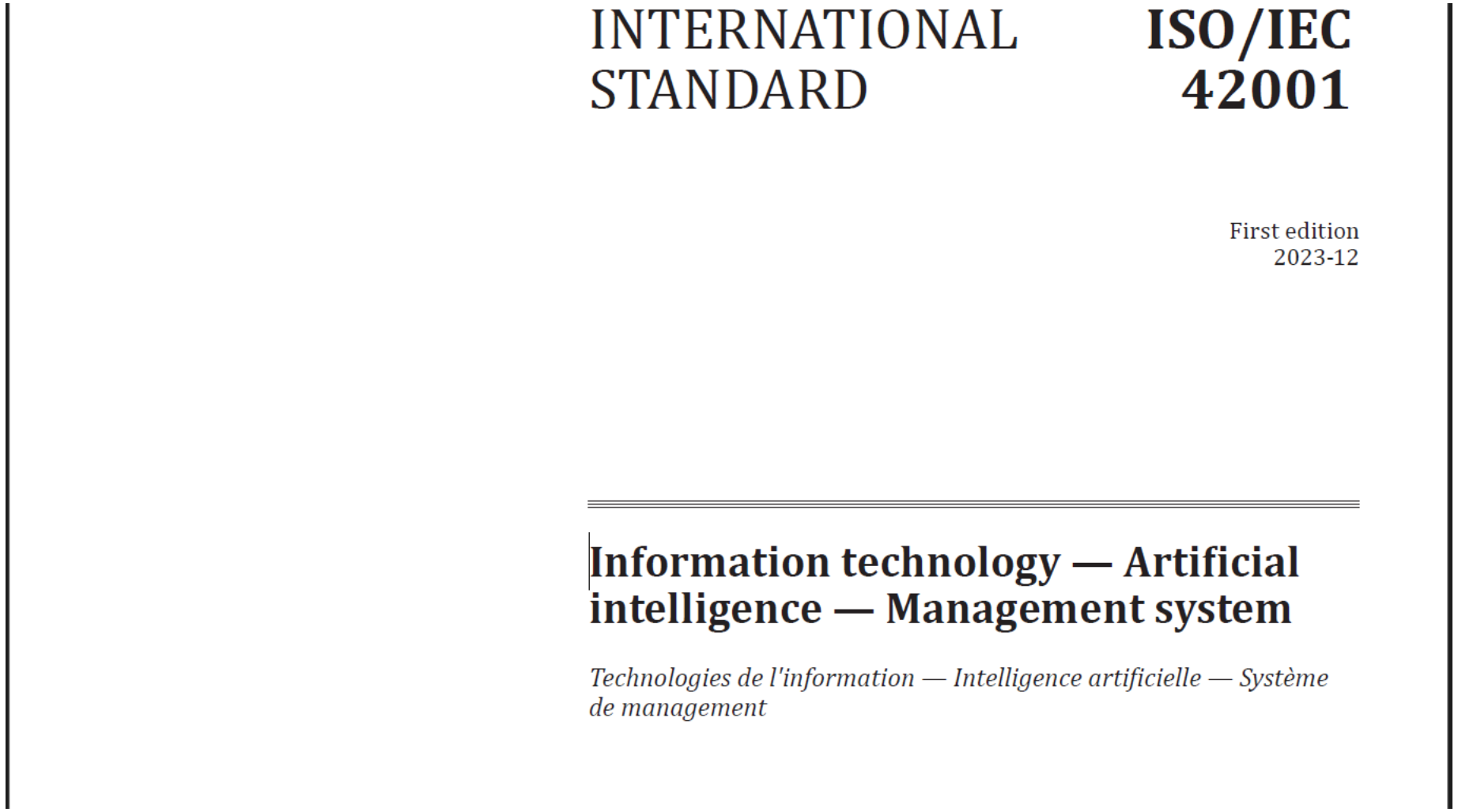
ALTRE NORME DI RIFERIMENTO

Vietato ogni genere di riproduzione e divulgazione

LA NORMA ISO 42001

Vietato ogni genere di riproduzione e divulgazione

LA NORMA ISO 42001



INTERNATIONAL STANDARD

ISO/IEC 42001

First edition
2023-12

Information technology — Artificial intelligence — Management system

Technologies de l'information — Intelligence artificielle — Système de management

Vietato ogni genere di riproduzione e divulgazione

LA NORMA ISO 42001

Vietato ogni genere di riproduzione e divulgazione

PIANIFICAZIONE

6.1 Azioni per affrontare rischi e opportunità

INTERNATIONAL STANDARD

ISO/IEC 23894

First edition
2023-02

Information technology — Artificial intelligence — Guidance on risk management

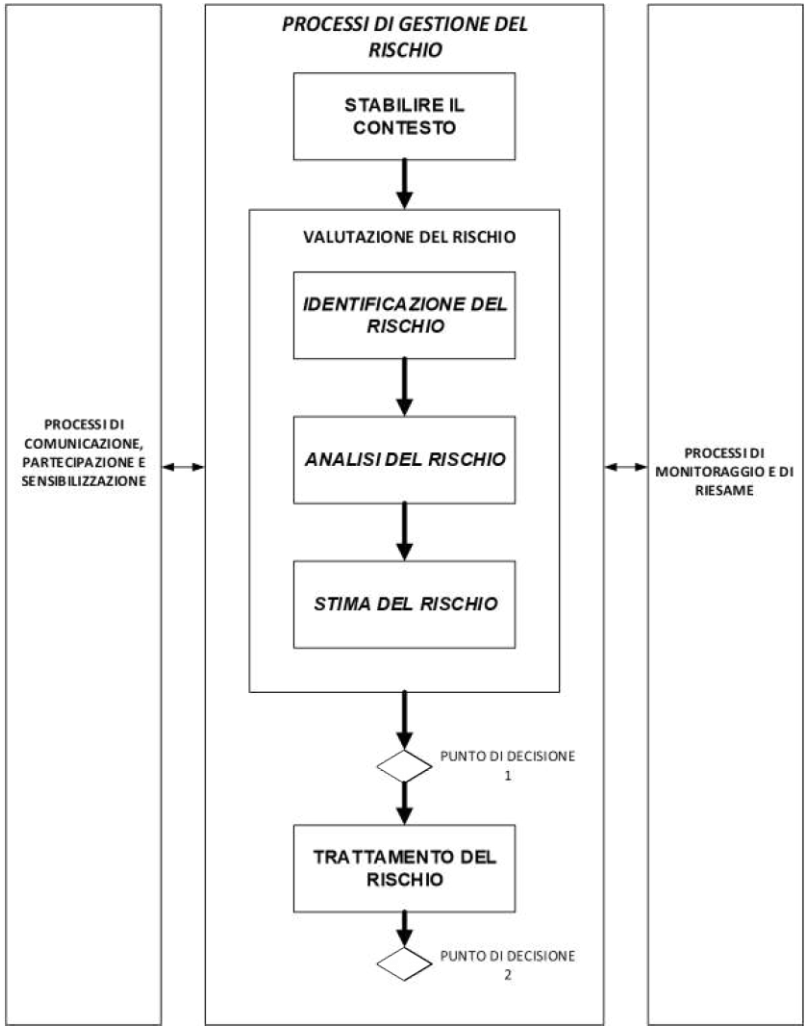
Technologies de l'information — Intelligence artificielle — Recommandations relatives au management du risque

Contents Page

Vietato ogni genere di riproduzione e divulgazione

PIANIFICAZIONE

6.1 Azioni per affrontare rischi e opportunità

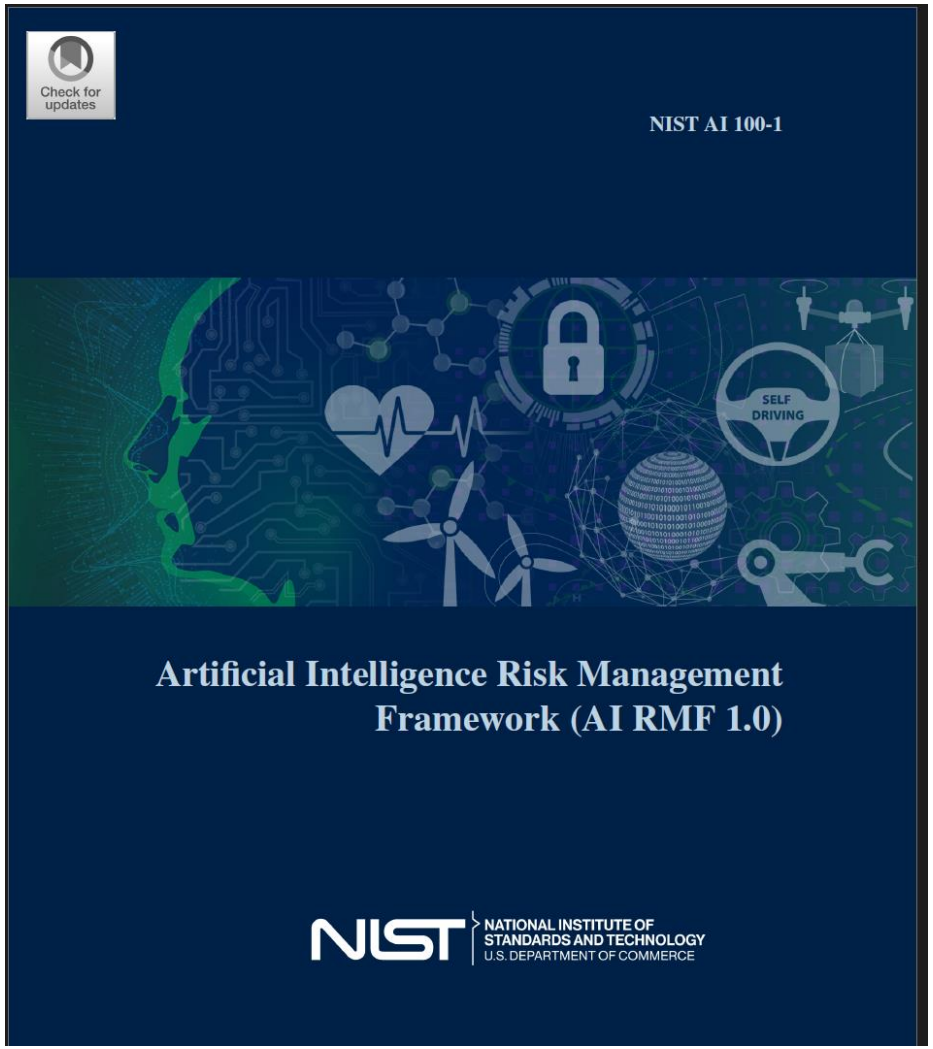


Vietato ogni genere di riproduzione e divulgazione

PIANIFICAZIONE

6.1.3 Trattamento dei rischi AI (Framework NIST)

Confronto tra NIST Risk AI



Vietato ogni genere di riproduzione e divulgazione

PIANIFICAZIONE

6.1.1 Azioni per affrontare rischi e opportunità

ISO TS 4213

Vietato ogni genere di riproduzione e divulgazione

PIANIFICAZIONE

6.1.1 Azioni per affrontare rischi e opportunità

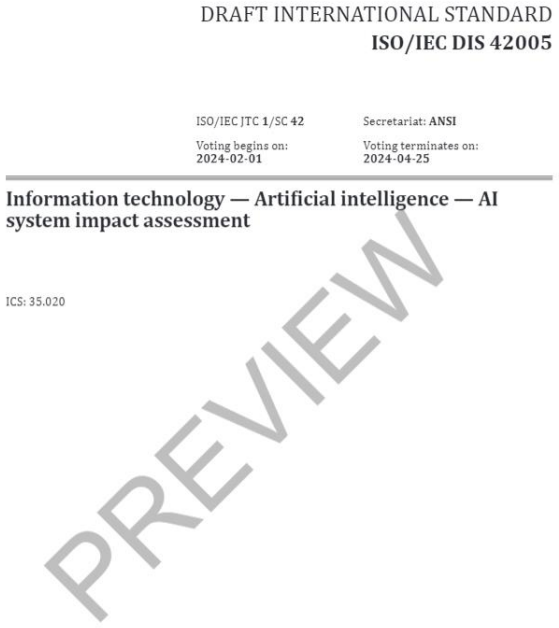
ISO TS 4213

Vietato ogni genere di riproduzione e divulgazione

PIANIFICAZIONE

6.1.4 Valutazione d'impatto dei rischi AI

ISO/IEC 42005 (Draft)


DRAFT INTERNATIONAL STANDARD
ISO/IEC DIS 42005

ISO/IEC JTC 1/SC 42 Secretariat: ANSI

Voting begins on: 2024-02-01 Voting terminates on: 2024-04-25

Information technology — Artificial intelligence — AI system impact assessment

ICS: 35.020

PREVIEW

Vietato ogni genere di riproduzione e divulgazione

PIANIFICAZIONE

6.1.4 Valutazione d'impatto dei rischi AI

Guida visiva di esempio per un impatto

Guida all'allineamento della valutazione

DRAFT

Row	Clause of this document	Subclause of this document	Potential inputs from a relevant HRIA	Potential inputs from a relevant PIA	Potential inputs from a relevant EIA	Potential inputs from a relevant FIA	Potential inputs from a relevant BIA	Potential inputs from a relevant SIA
1.	5.1	*N/A*	X	X				
2.	5.2	*5.2.1*	-	-				
3.		*5.2.2*	-	-				
4.		*5.2.3*	-	-				
5.		*5.2.4*						
6.		*5.2.5*	X	X				
7.	5.3	*5.3.1*	-	-				
8.		*5.3.2*	X	X				
9.	5.4	*5.4.1*	-	-				
10.		*5.4.2*	-	X				
11.		*5.4.3*	-	X				
12.		*5.4.4*	-	X				
13.		*5.4.5*	-	X				
14.	5.5	*5.5.1*	X	-				
15.		*5.5.2*	X	X				
16.	5.6	*5.6.1*	-	-				
17.		*5.6.2*	X	X				
18.	5.7	*5.7.1*	-	-				
19.		*5.7.2*	X	X				
20.		*5.7.3*	X	X				
21.	5.8	*N/A*	X	-				
Key X: Inputs likely to pertain to the AI **system** impact assessment								

Vietato ogni genere di riproduzione e divulgazione

PERFORMANCES

9.1 Monitoraggio, misurazione, analisi e valutazione

Esempi:

Single user licence only, copying and networking prohibited.

Technical Specification

ISO/IEC TS 25058

Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guidance for quality evaluation of artificial intelligence (AI) systems

Ingénierie des systèmes et des logiciels — Exigences et évaluation de la qualité des systèmes et des logiciels (SQuaRE) — Lignes directrices pour l'évaluation de la qualité des systèmes d'intelligence artificielle (IA)

First edition
2024-01

Contents Page

Vietato ogni genere di riproduzione e divulgazione

PERFORMANCES

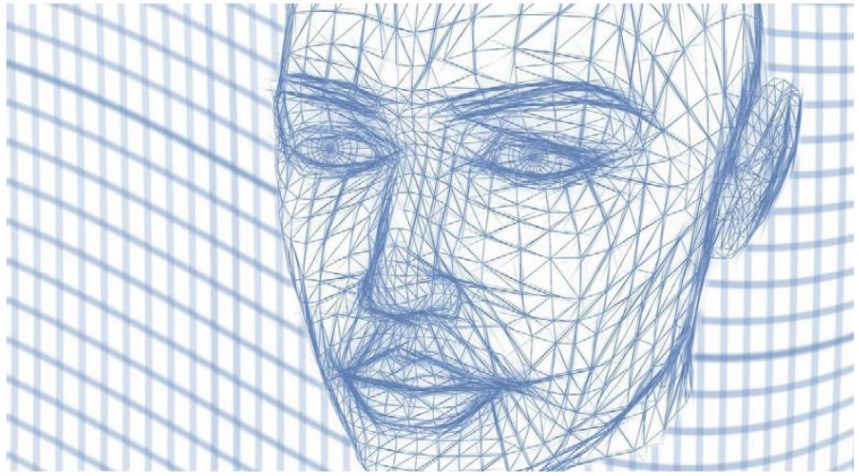
9.1 Monitoraggio, misurazione, analisi e valutazione

Esempi:

Vietato ogni genere di riproduzione e divulgazione

PERFORMANCES

9.2.2 Audit interno



DOCUMENTAZIONE APPLICABILE	
Regolamento di Schema RSGAI 01	DOWNLOAD NOW
TARIFFARIO	DOWNLOAD NOW
NORME DI DEONTOLOGIA	DOWNLOAD NOW
Referente di Schema S. Gorla	

© 2015 Aicq Sicev S.r.l. Tutti i diritti riservati.

aicq sicev	REQUISITI SPECIFICI PER LA CERTIFICAZIONE DELLE COMPETENZE DEI VALUTATORI E DEI RESPONSABILI DEL GRUPPO DI VALUTAZIONE DEI SISTEMI DI GESTIONE PER LA L'INTELLIGENZA ARTIFICIALE	*RSGAI 01* *Pag. 6/14* *Rev.00*

Esperienza di audit (Note 1 e 2)	4 audit completi (di cui almeno 1 di 2ª o di 3ª parte) per almeno 8 giornate; 2 devono essere condotti sotto la direzione di un RGVI certificato o qualificato; oppure 7 audit completi (di cui 2 di 2° o 3° parte) per almeno 14 giornate se gli audit non sono stati svolti con un RGVI certificato/qualificato (il che implica la discussione all'orale di un rapporto completo e corredato delle evidenze raccolte). Almeno 2 audit devono essere stati completati negli ultimi 2 anni.	In aggiunta a quanto previsto per VSAI: 3 audit completi per almeno 6 giornate (1°, 2° o 3° parte) come RGVI in addestramento/ facente funzione sotto la direzione e guida di un RGVI certificato o qualificato; oppure 5 audit come RGVI, di cui almeno 1 di 3° parte per almeno 10 giornate se gli audit non sono stati svolti con un RGVI certificato/qualificato (il che implica la discussione all'orale di un rapporto completo e corredato delle evidenze raccolte). Almeno 2 audit devono essere stati completati negli ultimi 2 anni.
Lingue Straniere (su richiesta)	Capacità di colloquio e di redazione di elaborati in lingua. Tale conoscenza può essere dimostrata da dichiarazioni rese da Istituti di formazione linguistica pubblici, privati o dalla Società di appartenenza del Candidato. AICQ SICEV si riserva di verificare durante la prova orale le reali conoscenze del candidato.	

Vietato ogni genere di riproduzione e divulgazione

ALLEGATO A

Obiettivi e controlli di controllo

A.2 Policies related to AI		
Objective: To provide management direction and support for AI systems according to business requirements.		
	Topic	Control
A.2.2	AI policy	The organization shall document a policy for the development or use of AI systems.
A.2.3	Alignment with other organizational policies	The organization shall determine where other policies can be affected by or apply to, the organization's objectives with respect to AI systems.
A.2.4	Review of the AI policy	The AI policy shall be reviewed at planned intervals or additionally as needed to ensure its continuing suitability, adequacy and effectiveness.
A.3 Internal organization		
Objective: To establish accountability within the organization to uphold its responsible approach for the implementation, operation and management of AI systems.		
	Topic	Control
A.3.2	AI roles and responsibilities	Roles and responsibilities for AI shall be defined and allocated according to the needs of the organization.
A.3.3	Reporting of concerns	The organization shall define and put in place a process for employees of the organization to report concerns about the organization's role with respect to an AI system throughout its life cycle.

Vietato ogni genere di riproduzione e divulgazione

ALLEGATO A

Obiettivi e controlli di controllo

A.4 Resources for AI systems		
Objective: To ensure that the organization accounts for the resources (including AI system components and assets) of the AI system in order to fully understand and address risks and impacts.		
	Topic	Control
A.4.2	Resource documentation	The organization shall identify and document relevant resources required for the activities at given AI system life cycle stages and other AI-related activities relevant for the organization.
A.4.3	Data resources	As part of resource identification, the organization shall document information about the data resources utilized for the AI system.
A.4.4	Tooling resources	As part of resource identification, the organization shall document information about the tooling resources utilized for the AI system.
A.4.5	System and computing resources	As part of resource identification, the organization shall document information about the system and computing resources utilized for the AI system.
A.4.6	Human resources	As part of resource identification, the organization shall document information about the human resources and their competences utilized for the development, deployment, operation, change management, maintenance, transfer and decommissioning, as well as verification and integration of the AI system.
A.5 Assessing impacts of AI systems		
Objective: To assess system impacts to interested parties of the AI system throughout its life cycle.		
	Topic	Control
A.5.2	AI system impact assessment process	The organization shall establish a process to assess the potential consequences for individuals and societies that can result from the AI system throughout its life cycle.
A.5.3	Documentation of AI system impact assessments	The organization shall document the results of AI system impact assessments and retain results for a defined period.
A.5.4	Assessing AI system impact on individuals and groups of individuals	The organization shall assess and document the potential impacts of AI systems to individuals or groups of individuals throughout the system's life cycle.
A.5.5	Assessing societal impacts of AI systems	The organization shall assess and document the potential societal impacts of their AI systems throughout their life cycle.

Vietato ogni genere di riproduzione e divulgazione

ALLEGATO A

Obiettivi e controlli di controllo

A.6 AI system life cycle		
A.6.1 Management guidance for AI system development		
Objective: To ensure that the organization identifies and documents objectives and implements processes for the responsible design and development of AI systems.		
	Topic	Control
A.6.1.2	Objectives for responsible development of AI system	The organization shall identify and document objectives to guide the development of trustworthy AI systems, and take those objectives into account and integrate measures to achieve them in the development life cycle.
A.6.1.3	Processes for trustworthy AI system design and development	The organization shall define and document the specific processes for the responsible design and development of the AI system.
A.6.2 AI system life cycle		
Objective: To define the criteria and requirements for each stage of the AI system life cycle.		
	Topic	Control
A.6.2.2	AI system requirements and specification	The organization shall specify and document requirements for new AI systems or material enhancements to existing systems.
A.6.2.3	Documentation of AI system design and development	The organization shall document the AI system design and development based on organizational objectives, documented requirements and specification criteria.
A.6.2.4	AI system verification and validation	The organization shall define and document verification and validation measures for the AI system and specify criteria for their use.
A.6.2.5	AI system deployment	The organization shall document a deployment plan and ensure that appropriate requirements are met prior to deployment.
A.6.2.6	AI system operation and monitoring	The organization shall define and document the necessary elements for the ongoing operation of the AI system. At the minimum, this should include system and performance monitoring, repairs, updates and support.
A.6.2.7	AI system technical documentation	The organization shall determine what AI system technical documentation is needed for each relevant category of interested parties, such as users, partners, supervisory authorities, and provide the technical documentation to them in the appropriate form.
A.6.2.8	AI system recording of event logs	The organization shall determine at which phases of the AI system life cycle, record keeping of event logs should be enabled, but at the minimum when the AI system is in use.

Vietato ogni genere di riproduzione e divulgazione

ALLEGATO A

Obiettivi e controlli di controllo

A.7 Data for AI systems		
Objective: To ensure that the organization understands the role and impacts of data in AI systems in the application and development, provision or use of AI systems throughout their life cycles.		
	Topic	Control
A.7.2	Data for development and enhancement of AI system	The organization shall define, document and implement data management processes related to the development of AI systems.
A.7.3	Acquisition of data	The organization shall determine and document details about the acquisition and selection of the data used in AI systems.
A.7.4	Quality of data for AI systems	The organization shall define and document requirements for data quality and ensure that data used to develop and operate the AI system meet those requirements.
A.7.5	Data provenance	The organization shall define and document a process for recording the provenance of data used in its AI systems over the life cycles of the data and the AI system.
A.7.6	Data preparation	The organization shall define and document their needs for and approaches to data preparation.
A.8 Information for interested parties of AI systems		
Objective: To ensure that relevant interested parties have the necessary information to understand and assess the risks and their impacts (both positive and negative).		
	Topic	Control
A.8.2	System documentation and information for users	The organization shall determine and provide the necessary information to users of the system.
A.8.3	External reporting	The organization shall provide capabilities for interested parties to report adverse impacts of the system.
A.8.4	Communication of incidents	The organization shall determine and document a plan for communicating incidents to users of the system.
A.8.5	Information for interested parties	The organization shall determine and document their obligations to reporting information about the AI system to interested parties.

Vietato ogni genere di riproduzione e divulgazione

ALLEGATO A

Obiettivi e controlli di controllo

A.9 Use of AI systems		
Objective: To ensure that the organization uses AI systems responsibly and per organizational policies.		
	Topic	Control
A.9.2	Processes for responsible use of AI systems	The organization shall define and document the processes for the responsible use of AI systems.
A.9.3	Objectives for responsible use of AI system	The organization shall identify and document objectives to guide the responsible use of AI systems.
A.9.4	Intended use of the AI system	The organization shall ensure that the AI system is used according to the intended uses of the AI system and its accompanying documentation.

Licensed to: Gorla, Stefano Mr

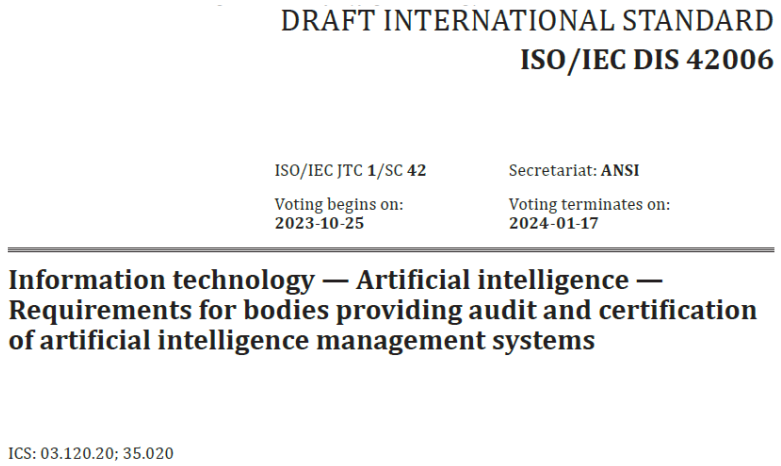
A.10 Third-party and customer relationships		
Objective: To ensure that the organization understands its responsibilities and remains accountable, and risks are appropriately apportioned when third parties are involved at any stage of the AI system life cycle.		
	Topic	Control
A.10.2	Allocating responsibilities	The organization shall ensure that responsibilities within their AI system life cycle are allocated between the organization, its partners, suppliers, customers and third parties.
A.10.3	Suppliers	The organization shall establish a process to ensure that its usage of services, products or materials provided by suppliers aligns with the organization's approach to the responsible development and use of AI systems.
A.10.4	Customers	The organization shall ensure that its responsible approach to the development and use of AI systems considers their customer expectations and needs.

Vietato ogni genere di riproduzione e divulgazione

LA ISO 42006

Vietato ogni genere di riproduzione e divulgazione

ISO 42006



DRAFT INTERNATIONAL STANDARD
ISO/IEC DIS 42006

ISO/IEC JTC 1/SC 42 | Secretariat: ANSI

Voting begins on: 2023-10-25 | Voting terminates on: 2024-01-17

Information technology — Artificial intelligence — Requirements for bodies providing audit and certification of artificial intelligence management systems

ICS: 03.120.20; 35.020

Questo documento specifica i requisiti aggiuntivi della norma ISO/IEC 17021-1.
I requisiti contenuti nel presente documento, una volta implementati, sostengono la dimostrazione di competenza, coerenza e affidabilità degli organismi che effettuano l'audit e la certificazione di un sistema di gestione dell'intelligence (AIMS) ISO/IEC 42001 per le organizzazioni che forniscono, sviluppano o utilizzano sistemi di intelligenza artificiale.
La certificazione AIMS è un'attività di valutazione della conformità di terza parte e gli organismi che questa attività sono organismi terzi di valutazione della conformità.

Vietato ogni genere di riproduzione e divulgazione

ISO 42006

7 Requisiti delle Risorse
7.1 Competenze delle persone

Knowledge	Certification function					
	Application reviewer (7.1.3.1)	Auditor (7.1.3.2)	Audit report reviewer (7.1.3.3)	Certification decision maker (7.1.3.4)	Appeal decision maker (7.1.3.5)	Evaluator of certification personnel (7.1.3.6)
Knowledge of business management practices						
a) management systems and management business practices, concepts and the interrelationship between policy, objectives and results.	x	x	x	x	x	x
Knowledge of audit principles, practices and techniques						

Knowledge	Certification function					
	Application reviewer (7.1.3.1)	Auditor (7.1.3.2)	Audit report reviewer (7.1.3.3)	Certification decision maker (7.1.3.4)	Appeal decision maker (7.1.3.5)	Evaluator of certification personnel (7.1.3.6)
a) principles of auditing.	-	x+	x+	-	-	x
Knowledge of specific management system standards/normative documents						
a) legal obligations that apply to artificial intelligence; b) ISO/IEC 42001:— and other normative documents used in the certification process; c) relevant certification schemes and necessary evaluation criteria for the conformity assessment.	x	x+	x+	x+	x+	x

Vietato ogni genere di riproduzione e divulgazione

ISO 42006

7 Requisiti delle Risorse
7.1 Competenze delle persone

Knowledge of certification body's processes						
a) requirements of ISO/IEC 17021-1 as well as the terminology and methods of ISO/IEC 17000; b) ISO/IEC 17029 for the validation and verification of claims; c) statistics for the calculation of representative samples from populations; d) requirements for conformity assessment bodies according to ISO/IEC 17011 and the requirements for reference to the status of accreditation.	**x**	**x+ (excl. d))**	**x+ (excl. d))**	**x+ (incl. d))**	**x+ (incl. d))**	**x**
Knowledge of client's business sector						
a) generic terminology, processes, technologies and risks related to the client business sector; b) tools, methods and techniques related to artificial intelligence	**x**	**x+**	**x+**	**x**	**x**	**-**

Vietato ogni genere di riproduzione e divulgazione

ISO 42006

7 Requisiti delle Risorse
7.1 Competenze delle persone

Knowledge	Certification function					
	Application reviewer (7.1.3.1)	Auditor (7.1.3.2)	Audit report reviewer (7.1.3.3)	Certification decision maker (7.1.3.4)	Appeal decision maker (7.1.3.5)	Evaluator of certification personnel (7.1.3.6)
management and their application; c) artificial intelligence management and governance structures including roles and responsibilities in the provision, development and use of an AI system; d) policies and business requirements for artificial intelligence management; e) codes of conduct as well as good practices and procedures on trustworthy AI (e.g. related to ISO/IEC TR 24028:2020 [6]) within the specific industry; f) relevant business sector practices; g) software developing processes.						
Knowledge of client products, processes and organization						
a) the effect of organization type, governance, structure, functions and relationships on development and implementation of the AIMS and certification activities, including outsourcing; b) technologies (including algorithms), methods, processes and tools that encompass data science and the discipline of AI as well as specific AI processes such as machine learning; c) processes applicable to AIMS;	x	x+	x+	-	x+	-

Vietato ogni genere di riproduzione e divulgazione

ISO 42006

7 Requisiti delle Risorse
7.1 Competenze delle persone

Knowledge	Certification function					
	Application reviewer (7.1.3.1)	Auditor (7.1.3.2)	Audit report reviewer (7.1.3.3)	Certification decision maker (7.1.3.4)	Appeal decision maker (7.1.3.5)	Evaluator of certification personnel (7.1.3.6)
d) AIMS-specific documentation structures, hierarchy and interrelationships; e) AIMS monitoring, measurement, analysis and evaluation; f) risk management processes, including assessment and mitigation procedures (in particular knowledge of ISO/IEC 23894 [7]; g) information and data security as well as impact assessment and risk assessment related to artificial intelligence management (in particular knowledge of ISO/IEC 22989, ISO/IEC 5259-3:— , ISO/IEC TR 24027:2021 [8], ISO/IEC CD 42005[4] [9] as well as ISO/IEC 27001 and, if applicable, ISO/IEC 27701); h) track and identify incidents with serious negative effects on affected persons within a client's AIMS.						
NOTE Further information on the principles of auditing can be found in ISO 19011 [5].						
Key x+ expert knowledge and major experience required for the function x knowledge and experience required for the function - competences not required for the function						

Vietato ogni genere di riproduzione e divulgazione

ISO 42006

7 Requisiti delle Risorse
7.1 Competenze delle persone.

Inoltre: Esempio (oltre alla norma, I documenti della norma, le tecniche di audit, il contest di business e leggi e regolamenti):

- Data Science
- Algebra
- Matrici e vettori
- Statistica descrittiva
- Teoria delle probabilità
- Principali distribuzioni
- Statistica Inferenziale
- Campionamento
- Il Machine Learning
- Gli Algoritmi
- Reti Neurali
- Deep Learning
- ……

Vietato ogni genere di riproduzione e divulgazione

ISO 42006

Tabella delle giornate di audit.

A.3.2 Fattori di adeguamento del tempo di audit
Il tempo assegnato tiene conto anche dei seguenti fattori che si riferiscono alla complessità degli AIMS e quindi allo sforzo necessario per controllare l'organizzazione che gestisce l'AIMS:
a) complessità degli AIMS (ad es. complessità dei dati, procedure di valutazione del rischio dell'AIMS, ecc.);
b) pertinenza dell'impatto sul sistema (ha un impatto elevato, medio o basso per il sistema in questione);
c) il tipo o i tipi di attività svolte nell'ambito dell'AIMS;
d) prestazioni precedentemente dimostrate dell'AIMS;

Number of persons under the organization 's control that are involved in the AI life cycle processes (based on ISO/IEC 5338:— [1] / ISO/IEC 22989:2022)	**AIMS roles**				**Further additive factors**	**Total audit time**
	Auditor days — AIMS for AI producer	**Auditor days — AIMS for AI developer or provider** (≈ 2/3 of AIMS audit time for AI producer)	**Auditor days — AIMS for AI user** (≈ 2/3 of AIMS audit time for AI producer)	**Auditor days — AIMS for clients with multiple roles** (≈ 1/3 additional audit time of AIMS for AI producer)		
1-10	5.0	3.5	3.5	6.5	See A.3.2	
11-15	6.0	4.0	4.0	8.0	See A.3.2	
16-25	7.0	4.5	4.5	9.5	See A.3.2	
26-45	8.5	6.0	6.0	11.5	See A.3.2	
46-65	10.0	7.0	7.0	13.0	See A.3.2	
66-85	11.0	7.5	7.5	15.0	See A.3.2	
86-125	12.0	8.0	8.0	16.0	See A.3.2	
126-175	13.0	9.0	9.0	17.5	See A.3.2	
176-275	14.0	9.5	9.5	19.0	See A.3.2	
276-425	15.0	10.0	10.0	20.0	See A.3.2	
> 425	Follow progression above	Follow progression above	Follow progression above	Follow progression above	See A.3.2	

Vietato ogni genere di riproduzione e divulgazione

ISO 42006

Tabella delle giornate di audit.

A.3.2 Fattori di adeguamento del tempo di audit
e) l'estensione e la diversità della tecnologia utilizzata nell'implementazione delle varie componenti di gli AIMS (ad esempio, numero di piattaforme informatiche diverse, IT-Cloud, numero di reti segregate);
f) l'entità dell'esternalizzazione e degli accordi con terzi utilizzati nell'ambito dell'AIMS;
g) numero di sedi aziendali e numero di siti di Disaster Recovery (DR);
h) numero di tutti i controlli necessari per soddisfare i requisiti ISO/IEC 42001 sulla base dei controlli delineati in ISO/IEC 42001 o altre fonti o entrambe;
i) l'estensione e la complessità dei controlli (compreso l'eventuale riesame prima della fase 2);
j) per l'audit di sorveglianza o di ricertificazione: l'entità e l'entità delle modifiche pertinenti per gli AIMS conforme alla norma ISO/IEC 17021-1, 8.5.3.

Complexity of the AIMS	Relevance of the AI system impact[a]			Total audit time
	Auditor days — high impact	**Auditor days —** medium impact (≈ 2/3 of auditor days of high impact)	**Auditor days —** low impact (≈ 1/3 of auditor days of high impact)	
Sensitive context of AI system(s)	8.0	5.5	3.0	
Non-sensitive context of AI system(s)	6.0	4.0	2.0	
Data complexity with reference to the managed AI system(s)	20.0	13.5	7.0	
Risk assessment with reference to the managed AI system(s)	25.0	17.0	8.5	
more than one legal framework to manage	6.0	4.0	2.0	
Number of outsourced services used in the scope of the AIMS	10.0	7.0	3.5	
AIMS running in more than one company location	4.0	3.0	1.5	
Number of Disaster Recovery Sites	1.5	1.0	0.5	
Diversity of technology	20.0	13.5	7.0	
Number of all documented controls needed to satisfy ISO/IEC 42001 requirements	20.0	13.5	7.0	

[a] Impact describes the real impact to be expected on the rights of the persons affected or on areas of public interest such as health and safety by the AI system(s) that is managed by the AIMS of an organization.

Vietato ogni genere di riproduzione e divulgazione

L’AIAct

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

Regolamento europeo.

Articolo 85 Entrata in vigore e applicazione

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea.

2. Il presente regolamento si applica a decorrere dal [24 mesi successivi alla sua entrata in vigore].

3. In deroga al paragrafo 2:

a) il titolo III, il capo 4 e il titolo VI si applicano a decorrere dal [tre mesi dopo l'entrata in vigore del presente regolamento];

b) L'articolo 71 si applica a decorrere dal [dodici mesi dopo l'entrata in vigore del presente regolamento].

EUROPEAN COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

Council of the European Union

Brussels, 26 January 2024
(OR. en)

5662/24

LIMITE

TELECOM 22
JAI 98
COPEN 18
CYBER 14
DATAPROTECT 32
EJUSTICE 3
COSI 6
IXIM 15
ENFOPOL 21
RELEX 77
MI 65
COMPET 68
CODEC 133

PUBLIC

Interinstitutional File:
2021/0106(COD)

NOTE

From:	Presidency
To:	Permanent Representatives Committee
No. Cion doc.:	8115/21
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Analysis of the final compromise text with a view to agreement

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

Il presente regolamento si applica:

a) i fornitori che immettono sul mercato o mettono in servizio sistemi di IA o immettono sul mercato modelli di IA per uso generale nell'Unione, indipendentemente dal fatto che tali fornitori siano stabiliti o che siano ubicati nell'Unione o in un paese terzo;

b) gli operatori di sistemi di IA che hanno il loro luogo di stabilimento o che sono ubicati all'interno dell'Unione;

c) i fornitori e gli operatori di sistemi di IA che hanno il loro luogo di stabilimento o che sono ubicati in un paese terzo, se l'output prodotto dal sistema è utilizzato nell'Unione;

c bis) importatori e distributori di sistemi di IA;

c ter) i fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il proprio nome o marchio;

c quater) i rappresentanti autorizzati dei fornitori che non sono stabiliti nell'Unione.

c quater) le persone interessate che si trovano nell'Unione.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

Sono vietate le seguenti pratiche di intelligenza artificiale:

a) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali al di là della coscienza di una persona o tecniche manipolative o ingannevoli intenzionalmente, con l'obiettivo o l'effetto di falsare materialmente il comportamento di una persona o di un gruppo di persone compromettendo sensibilmente la capacità della persona di prendere una decisione informata; inducendo in tal modo la persona a prendere una decisione che non avrebbe altrimenti preso in un modo che causi o possa causare a quella persona, a un'altra persona o a un gruppo di persone un danno significativo;

(b) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta una delle vulnerabilità di una persona o di un gruppo specifico di persone a causa della loro età, disabilità o di una specifica situazione sociale o economica, con l'obiettivo o l'effetto di falsare materialmente il comportamento di tale persona o di una persona appartenente a tale gruppo in un modo che provochi o possa ragionevolmente causare tale persona o un'altra persona un danno significativo;

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

b bis) l'immissione sul mercato o la messa in servizio per tale scopo specifico, o l'uso, di sistemi di categorizzazione biometrica che classificano le singole persone fisiche sulla base dei loro dati biometrici per dedurre o dedurre la loro razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche, la vita sessuale o l'orientamento sessuale. Tale divieto non riguarda l'etichettatura o il filtraggio di serie di dati biometrici acquisiti legalmente, come le immagini, sulla base di dati biometrici o la categorizzazione dei dati biometrici nel settore dell'applicazione della legge;

(c) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA per la valutazione o la classificazione di persone fisiche o di gruppi di persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o di personalità note, dedotte o previste, con il punteggio sociale che porta a uno o entrambi i seguenti elementi:

i) il trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche in contesti sociali che non hanno alcun rapporto con i contesti in cui i dati sono stati originariamente generati o raccolti;

ii) un trattamento pregiudizievole o sfavorevole nei confronti di determinate persone fisiche o di determinati gruppi di persone fisiche, ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità;

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

d) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di contrasto, a meno che e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti obiettivi:

i) la ricerca mirata di vittime specifiche di rapimento, tratta di esseri umani e sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse;

ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica di persone fisiche o di una minaccia reale, attuale o reale e prevedibile di un attacco terroristico;

iii) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato ai fini dello svolgimento di un'indagine penale, dell'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II bis e punibili nello Stato membro interessato con una pena o una misura di sicurezza privative della libertà per un periodo massimo di almeno quattro anni. Il presente paragrafo non pregiudica quanto previsto dall'articolo 9 del GDPR per il trattamento dei dati biometrici per finalità diverse dall'applicazione della legge.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

d bis) l'immissione sul mercato, la messa in servizio per tale scopo specifico o l'uso di un sistema di IA per effettuare valutazioni del rischio di persone fisiche al fine di valutare o prevedere il rischio di una persona fisica di commettere un reato, sulla base unicamente della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della sua personalità. Tale divieto non si applica ai sistemi di IA utilizzati per sostenere la valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili direttamente collegati a un'attività criminosa;

d ter) l'immissione sul mercato, la messa in servizio per tale scopo specifico o l'uso di sistemi di IA che creano o ampliano banche dati di riconoscimento facciale mediante lo scraping non mirato di immagini facciali da Internet o da filmati di telecamere a circuito chiuso;

d quater) l'immissione sul mercato, la messa in servizio per tale scopo specifico o l'uso di sistemi di IA per dedurre le emozioni di una persona fisica nei settori del luogo di lavoro e degli istituti di istruzione, tranne nei casi in cui l'uso del sistema di IA è destinato a essere messo in atto o immesso sul mercato per motivi medici o di sicurezza.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

Articolo 6

Regole di classificazione per i sistemi di IA ad alto rischio

1. Indipendentemente dal fatto che un sistema di IA sia immesso sul mercato o messo in servizio indipendentemente dai prodotti di cui alle lettere a) e b), tale sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le seguenti condizioni:

a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II;

b) il prodotto il cui componente di sicurezza a norma della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è tenuto a sottoporsi a una valutazione della conformità da parte di terzi, ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto a norma della normativa di armonizzazione dell'Unione elencata nell'allegato II.

2. Oltre ai sistemi di IA ad alto rischio di cui al paragrafo 1, anche i sistemi di IA di cui all'allegato III sono considerati ad alto rischio.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

Articolo 9

Sistema di gestione del rischio

È istituito, attuato, documentato e mantenuto un sistema di gestione del rischio in relazione ai sistemi di IA ad alto rischio.

Articolo 10

Dati e governance dei dati

I sistemi di IA ad alto rischio che si avvalgono di tecniche che comportano l'addestramento di modelli con dati sono sviluppati sulla base di set di dati di addestramento, convalida e prova che soddisfano i criteri di qualità di cui ai paragrafi da 2 a 5 ogniqualvolta tali serie di dati siano utilizzate

Articolo 11

Documentazione tecnica

1. La documentazione tecnica di un sistema di IA ad alto rischio è redatta prima dell'immissione sul mercato o della messa in servizio di tale sistema ed è mantenuta aggiornata.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

Articolo 12

Tenuta dei registri

I sistemi di IA ad alto rischio consentono tecnicamente la registrazione automatica degli eventi («registri») per tutta la durata del ciclo di vita del sistema.

Articolo 13

Trasparenza e fornitura di informazioni agli operatori

I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli operatori di interpretare i risultati del sistema e di utilizzarli in modo appropriato. Sono garantiti un tipo e un grado di trasparenza adeguati al fine di conseguire il rispetto dei pertinenti obblighi del fornitore e dell'operatore di cui al capo 3 del presente titolo.

Articolo 14

Supervisione umana

1. I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale, anche con adeguati strumenti di interfaccia uomo-macchina, da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui il sistema di IA è in uso.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

Articolo 15

Precisione, robustezza e sicurezza informatica

I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da raggiungere un livello adeguato di accuratezza, robustezza e cybersicurezza e da garantire prestazioni coerenti sotto tali aspetti durante tutto il loro ciclo di vita.

Capitolo 3 Fornitore, articolo 17

Sistema di gestione per la qualità

I fornitori di sistemi di IA ad alto rischio istituiscono un sistema di gestione della qualità che garantisca la conformità al presente regolamento. Tale sistema è documentato in modo sistematico e ordinato sotto forma di politiche, procedure e istruzioni scritte e comprende almeno i seguenti aspetti: .....

f) sistemi e procedure per la gestione dei dati, compresi l'acquisizione, la raccolta, l'analisi dei dati, l'etichettatura dei dati, l'archiviazione dei dati, il filtraggio dei dati, l'estrazione di dati, l'aggregazione dei dati, la conservazione dei dati e qualsiasi altra operazione relativa ai dati effettuata prima e ai fini dell'immissione sul mercato o della messa in servizio di sistemi di IA ad alto rischio;

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

Articolo 18

Conservazione della documentazione

Per un periodo che termina 10 anni dopo l'immissione sul mercato o la messa in servizio del sistema di IA, il fornitore tiene a disposizione delle autorità nazionali competenti: .....

Articolo 20

Registri generati automaticamente

1. I fornitori di sistemi di IA ad alto rischio conservano le registrazioni di cui all'articolo 12, paragrafo 1, generate automaticamente dai loro sistemi di IA ad alto rischio, nella misura in cui tali registrazioni sono sotto il loro controllo. Fatto salvo il diritto dell'Unione o nazionale applicabile, le registrazioni sono conservate per un periodo adeguato alla finalità prevista del sistema di IA ad alto rischio, pari ad almeno 6 mesi, salvo diversa disposizione del diritto dell'Unione o nazionale applicabile, in particolare del diritto dell'Unione in materia di protezione dei dati personali.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

Articolo 26

Obblighi degli importatori

Prima di immettere sul mercato un sistema di IA ad alto rischio, gli importatori di tale sistema garantiscono che tale sistema sia conforme al presente regolamento verificando che: .....

Articolo 27

Obblighi dei distributori

1. Prima di mettere a disposizione sul mercato un sistema di IA ad alto rischio, i distributori verificano che il sistema di IA ad alto rischio rechi la marcatura CE di conformità richiesta, che sia accompagnato da una copia della dichiarazione UE di conformità e delle istruzioni per l'uso e che il fornitore e l'importatore del sistema, a seconda dei casi, abbiano rispettato gli obblighi di cui all'articolo 16, lettere a bis) e b) e all'articolo 26, paragrafo 3.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

Articolo 28

Responsabilità lungo la catena del valore dell'IA

Qualsiasi distributore, importatore, distributore o altro terzo è considerato un fornitore di un sistema di IA ad alto rischio ai fini del presente regolamento ed è soggetto agli obblighi del fornitore di cui all'articolo 16 in una delle seguenti circostanze: .....

Articolo 29

Obblighi degli operatori di sistemi di IA ad alto rischio

Gli operatori di sistemi di IA ad alto rischio adottano misure tecniche e organizzative adeguate per garantire che utilizzino tali sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi, a norma dei paragrafi 2 e 5 del presente articolo.

Articolo 29 bis

Valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio

1. Prima di installare un sistema di IA ad alto rischio quale definito all'articolo 6, paragrafo 2, ad eccezione dei sistemi di IA destinati a essere utilizzati nel settore di cui all'allegato III, punto 2, gli operatori che sono organismi di diritto pubblico o operatori privati che forniscono servizi pubblici e gli operatori che utilizzano sistemi ad alto rischio di cui all'allegato III, di cui al punto 5, lettere b) e c bis), effettua una valutazione dell'impatto sui diritti fondamentali che l'uso del sistema può produrre. A tal fine, gli operatori effettuano una valutazione consistente in:.....

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

Articolo 28

Responsabilità lungo la catena del valore dell'IA

Qualsiasi distributore, importatore, distributore o altro terzo è considerato un fornitore di un sistema di IA ad alto rischio ai fini del presente regolamento ed è soggetto agli obblighi del fornitore di cui all'articolo 16 in una delle seguenti circostanze: .....

Articolo 29

Obblighi degli operatori di sistemi di IA ad alto rischio

Gli operatori di sistemi di IA ad alto rischio adottano misure tecniche e organizzative adeguate per garantire che utilizzino tali sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi, a norma dei paragrafi 2 e 5 del presente articolo.

Articolo 29 bis

Valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio

1. Prima di installare un sistema di IA ad alto rischio quale definito all'articolo 6, paragrafo 2, ad eccezione dei sistemi di IA destinati a essere utilizzati nel settore di cui all'allegato III, punto 2, gli operatori che sono organismi di diritto pubblico o operatori privati che forniscono servizi pubblici e gli operatori che utilizzano sistemi ad alto rischio di cui all'allegato III, di cui al punto 5, lettere b) e c bis), effettua una valutazione dell'impatto sui diritti fondamentali che l'uso del sistema può produrre. A tal fine, gli operatori effettuano una valutazione consistente in:.....

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

Articolo 48

Dichiarazione di conformità UE

1. Il fornitore redige una dichiarazione di conformità UE scritta a lettura ottica, fisica o firmata elettronicamente per ciascun sistema di IA ad alto rischio e la tiene a disposizione delle autorità nazionali competenti per 10 anni dopo l'immissione sul mercato o la messa in servizio del sistema di IA ad alto rischio. La dichiarazione UE di conformità identifica il sistema di IA ad alto rischio per il quale è stata redatta. Su richiesta, una copia della dichiarazione UE di conformità deve essere presentata alle autorità nazionali competenti.

Articolo 52

Obblighi di trasparenza per i fornitori e gli utenti di determinati sistemi di IA e modelli GPAI (general purpose AI)

1. I fornitori provvedono affinché i sistemi di IA destinati a interagire direttamente con le persone fisiche siano progettati e sviluppati in modo tale che le persone fisiche interessate siano informate del fatto che stanno interagendo con un sistema di IA, a meno che ciò non sia evidente dal punto di vista di una persona fisica ragionevolmente informata, attenta e avveduta, tenendo conto delle circostanze e del contesto d'uso.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

ALLEGATO III

Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

I sistemi di IA ad alto rischio ai sensi dell'articolo 6, paragrafo 2, sono i sistemi di IA elencati in uno dei seguenti settori:

1. Dati biometrici, nella misura in cui il loro uso è consentito dal pertinente diritto dell'Unione o nazionale:

a) Sistemi di identificazione biometrica remota. Sono esclusi i sistemi di IA destinati a essere utilizzati per la verifica biometrica il cui unico scopo è confermare che una determinata persona fisica è la persona che afferma di essere;

a bis) sistemi di IA destinati a essere utilizzati per la categorizzazione biometrica, in base ad attributi o caratteristiche sensibili o protetti sulla base dell'inferenza di tali attributi o caratteristiche;

a ter) Sistemi di intelligenza artificiale destinati ad essere utilizzati per il riconoscimento delle emozioni.

2. Infrastrutture critiche:

a) sistemi di IA destinati a essere utilizzati come componenti di sicurezza nella gestione e nel funzionamento delle infrastrutture digitali critiche, del traffico stradale e della fornitura di acqua, gas, riscaldamento ed energia elettrica.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

ALLEGATO III

Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

3. Istruzione e formazione professionale:

a) sistemi di IA destinati a essere utilizzati per determinare l'accesso o l'ammissione o per assegnare persone fisiche agli istituti di istruzione e formazione professionale a tutti i livelli;

b) sistemi di IA destinati a essere utilizzati per valutare i risultati dell'apprendimento, anche quando tali risultati sono utilizzati per orientare il processo di apprendimento delle persone fisiche negli istituti di istruzione e formazione professionale a tutti i livelli;

b bis) sistemi di IA destinati ad essere utilizzati allo scopo di valutare il livello appropriato di istruzione a cui l'individuo riceverà o potrà accedere, nel contesto di/all'interno dell'istituto di istruzione e formazione professionale;

b ter) Sistemi di IA destinati a essere utilizzati per monitorare e rilevare i comportamenti vietati degli studenti durante le prove nel contesto di/all'interno degli istituti di istruzione e formazione professionale.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

ALLEGATO III

Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

4. Occupazione, gestione dei lavoratori e accesso al lavoro autonomo:

a) sistemi di IA destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche, in particolare per pubblicare annunci di lavoro mirati, analizzare e filtrare le domande di lavoro e valutare i candidati;

b) l'IA destinata a essere utilizzata per prendere decisioni che incidono sulle condizioni dei rapporti di lavoro, sulla promozione e sulla cessazione dei rapporti contrattuali di lavoro, per assegnare compiti in base al comportamento individuale o a tratti o caratteristiche personali e per monitorare e valutare le prestazioni e il comportamento delle persone in tali rapporti.

5. Accesso e godimento dei servizi privati essenziali e dei servizi e delle prestazioni pubbliche essenziali:

a) sistemi di IA destinati a essere utilizzati dalle autorità pubbliche o per conto delle autorità pubbliche per valutare l'ammissibilità delle persone fisiche a prestazioni e servizi essenziali di assistenza pubblica, compresi i servizi sanitari, nonché per concedere, ridurre, revocare o richiedere tali prestazioni e servizi;

b) i sistemi di IA destinati a essere utilizzati per valutare il merito creditizio delle persone fisiche o stabilire il loro punteggio di credito, ad eccezione dei sistemi di IA utilizzati allo scopo di individuare le frodi finanziarie;

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

ALLEGATO III

Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

c) sistemi di IA destinati a valutare e classificare le chiamate di emergenza da parte di persone fisiche o da utilizzare per l'invio o per stabilire la priorità nell'invio di servizi di primo intervento di emergenza, compresi quelli di polizia, vigili del fuoco e assistenza medica, nonché di sistemi di triage dei pazienti per l'assistenza sanitaria di emergenza;

c bis) I sistemi di IA destinati a essere utilizzati per la valutazione del rischio e la fissazione dei prezzi in relazione alle persone fisiche nel caso dell'assicurazione sulla vita e dell'assicurazione malattia.

6. Le attività di contrasto, nella misura in cui il loro uso è consentito dal pertinente diritto dell'Unione o nazionale:

a) sistemi di IA destinati a essere utilizzati da o per conto delle autorità di contrasto, o da istituzioni, agenzie, uffici o organismi dell'Unione a sostegno delle autorità di contrasto o per loro conto, per valutare il rischio che una persona fisica diventi vittima di reati;

b) sistemi di IA destinati a essere utilizzati da o per conto delle autorità di contrasto o dalle istituzioni, dagli organi e dalle agenzie dell'Unione a sostegno delle autorità di contrasto come poligrafi e strumenti analoghi;

(d) sistemi di IA destinati a essere utilizzati da o per conto delle autorità di contrasto, o da istituzioni, agenzie, uffici o organismi dell'Unione a sostegno delle autorità di contrasto per valutare l'affidabilità delle prove nel corso delle indagini o del perseguimento di reati;

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

ALLEGATO III

Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

(e) sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto o da istituzioni, agenzie, uffici o organismi dell'Unione a sostegno delle autorità di contrasto per valutare il rischio di una persona fisica di commettere un reato o una recidiva non solo sulla base della profilazione di persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 o per valutare tratti e caratteristiche della personalità o comportamenti criminali passati di persone fisiche; Gruppi;

f) sistemi di IA destinati a essere utilizzati da o per conto delle autorità di contrasto o da agenzie, istituzioni, agenzie, uffici o organismi dell'Unione a sostegno delle autorità di contrasto per la profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 nel corso dell'accertamento, dell'indagine o del perseguimento di reati.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

ALLEGATO III

Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

7. Gestione della migrazione, dell'asilo e del controllo delle frontiere, nella misura in cui il loro uso sia consentito dal pertinente diritto dell'Unione o nazionale:

a) sistemi di IA destinati ad essere utilizzati dalle autorità pubbliche competenti come poligrafi e strumenti analoghi;

b) i sistemi di IA destinati a essere utilizzati da o per conto delle autorità pubbliche competenti o da agenzie, uffici o organismi dell'Unione per valutare un rischio, compresi un rischio per la sicurezza, un rischio di migrazione irregolare o un rischio per la salute, rappresentato da una persona fisica che intende entrare o è entrata nel territorio di uno Stato membro;

(d) sistemi di IA destinati ad essere utilizzati da o per conto delle autorità pubbliche competenti o da agenzie, uffici o organismi dell'Unione per assistere le autorità pubbliche competenti nell'esame delle domande di asilo, visti e permessi di soggiorno e dei relativi reclami per quanto riguarda l'ammissibilità delle persone fisiche che richiedono uno status, compresa la relativa valutazione dell'affidabilità delle prove;

d bis) Sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti o per loro conto, comprese le agenzie, gli uffici o gli organismi dell'Unione, nel contesto della gestione della migrazione, dell'asilo e del controllo delle frontiere, al fine di individuare, riconoscere o identificare le persone fisiche, ad eccezione della verifica dei documenti di viaggio.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

ALLEGATO III

Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

8. Amministrazione della giustizia e processi democratici:

a) sistemi di IA destinati a essere utilizzati da un'autorità giudiziaria o per suo conto per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione del diritto a un insieme concreto di fatti o utilizzati in modo analogo nella risoluzione alternativa delle controversie;

a bis) Sistemi di IA destinati a essere utilizzati per influenzare l'esito di un'elezione o di un referendum o il comportamento di voto delle persone fisiche nell'esercizio del loro voto nelle elezioni o nei referendum. Ciò non include i sistemi di IA i cui risultati non sono direttamente esposti alle persone fisiche, come gli strumenti utilizzati per organizzare, ottimizzare e strutturare le campagne politiche da un punto di vista amministrativo e logistico.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

ALLEGATO IV

Documentazione tecnica di cui all'articolo 11, paragrafo 1

ALLEGATO V

Dichiarazione di conformità UE

ALLEGATO VI

Procedura di valutazione della conformità basata sul controllo interno

1. La procedura di valutazione della conformità basata sul controllo interno è la procedura di valutazione della conformità di cui ai punti da 2 a 4.

2. Il fornitore verifica che il sistema di gestione della qualità istituito sia conforme ai requisiti di cui all'articolo 17.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

ALLEGATO VII

Conformità basata sulla valutazione del sistema di gestione della qualità e sulla valutazione della documentazione tecnica

1. Introduzione

La conformità basata sulla valutazione del sistema di gestione della qualità e sulla valutazione della documentazione tecnica è la procedura di valutazione della conformità di cui ai punti da 2 a 5.

2. Panoramica

Il sistema di gestione della qualità approvato per la progettazione, lo sviluppo e il collaudo dei sistemi di IA a norma dell'articolo 17 è esaminato conformemente al punto 3 ed è soggetto alla sorveglianza di cui al punto 5. La documentazione tecnica del sistema di IA è esaminata conformemente al punto 4.

3. Sistema di gestione della qualità .....

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

ALLEGATO VII

La domanda del fornitore comprende:

a) il nome e l'indirizzo del prestatore e, se la domanda è presentata dal rappresentante autorizzato, anche il nome e l'indirizzo;

b) l'elenco dei sistemi di IA contemplati dallo stesso sistema di gestione della qualità;

c) la documentazione tecnica per ciascun sistema di IA che rientra nello stesso sistema di gestione della qualità;

d) la documentazione relativa al sistema di gestione della qualità, che copre tutti gli aspetti di cui all'articolo 17;

e) una descrizione delle procedure in atto per garantire che il sistema di gestione della qualità rimanga adeguato ed efficace;

f) una dichiarazione scritta attestante che la stessa domanda non è stata presentata ad alcun altro organismo notificato.

Vietato ogni genere di riproduzione e divulgazione

IL REGOLAMENTO AIAct

ALLEGATO VII

3.2. Il sistema di gestione della qualità è valutato dall'organismo notificato, che ne determina la conformità ai requisiti di cui all'articolo 17.

La decisione è notificata al prestatore o al suo mandatario.

La notifica contiene le conclusioni della valutazione del sistema di gestione della qualità e la decisione di valutazione motivata.

3.3. Il sistema di gestione della qualità approvato deve continuare ad essere attuato e mantenuto dal fornitore in modo che rimanga adeguato ed efficiente.

3.4. Qualsiasi modifica prevista del sistema di gestione della qualità approvato o dell'elenco dei sistemi di IA contemplati da quest'ultimo deve essere portata a conoscenza dell'organismo notificato dal fornitore.

Le modifiche proposte sono esaminate dall'organismo notificato, che decide se il sistema di gestione della qualità modificato continua a soddisfare i requisiti di cui al punto 3.2 o se è necessaria una nuova valutazione.

L'organismo notificato notifica la sua decisione al fornitore. La notifica contiene le conclusioni dell'esame delle modifiche e la decisione di valutazione motivata.

4. Controllo della documentazione tecnica…….

5. Sorveglianza del sistema di gestione della qualità approvato .....

Vietato ogni genere di riproduzione e divulgazione

GRAZIE PER L’ ATTENZIONE

stefano.gorla@proficegroup.it

Vietato ogni genere di riproduzione e divulgazione