Risk Management per la privacy In Ambito medicale

e-privacy XXXV @ Brescia

Progetto Winston Smith & Ordine degli Ingegneri della Provincia di Brescia

Commissione ICT

Paolo Gibellini

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI BRESCIA

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI BRESCIA

Premessa

Il processo di Analisi dei Rischi per dispositivi e macchinari porta i suoi frutti ma può essere **lungo e costoso**.

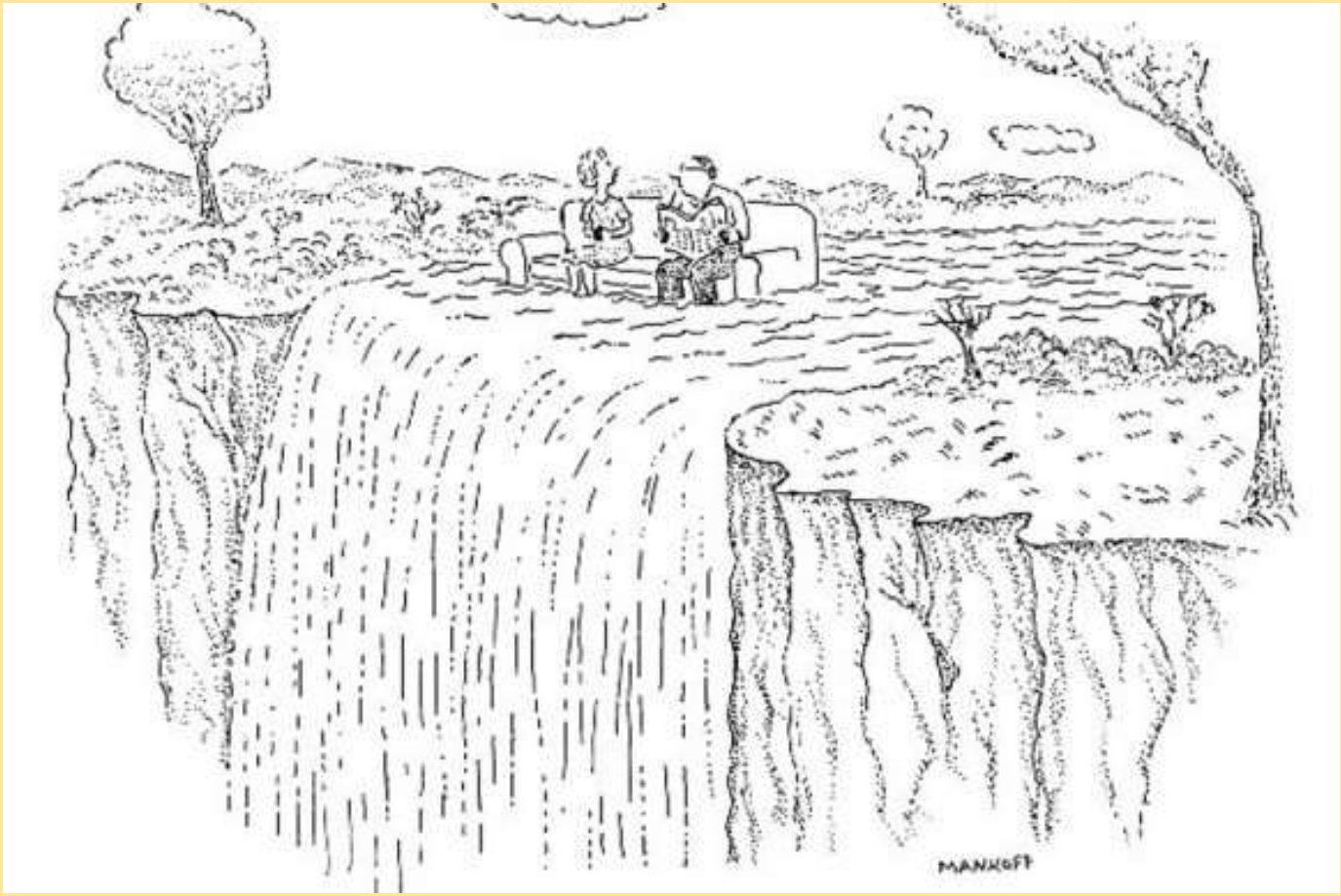
In alcuni casi La Legge ci chiede di **classificare il dispositivo** (in base alla sua complessità ed al potenziale rischio per l'utilizzatore) e di verificare che rispetti i **requisiti essenziali**, cioè le condizioni di sicurezza e di efficacia che devono possedere sia i dispositivi che il loro sistema produttivo. Questo vale sia per dispositivi **hardware** che **software**. Anche quando non è richiesta dalla legge, la Risk Analysis è una **buona pratica** a livello di progettazione.

In poche parole, è necessario progettare e produrre dispositivi in modo che siano **sicuri** per operatori, utilizzatori o comunque fruitori.

In questo intervento non affronteremo i rischi di tipo finanziario

Non parleremo neppure dei rischi legati alla sicurezza dei lavoratori

E tantomeno parleremo di norme o dei rischi legati ai segnali di avvertenza misteriosi



Ce ne staremo comodamente seduti sul nostro divano

Pensando ad una soluzione ragionevole per affrontare i rischi in cascata

Rischio (Safety)

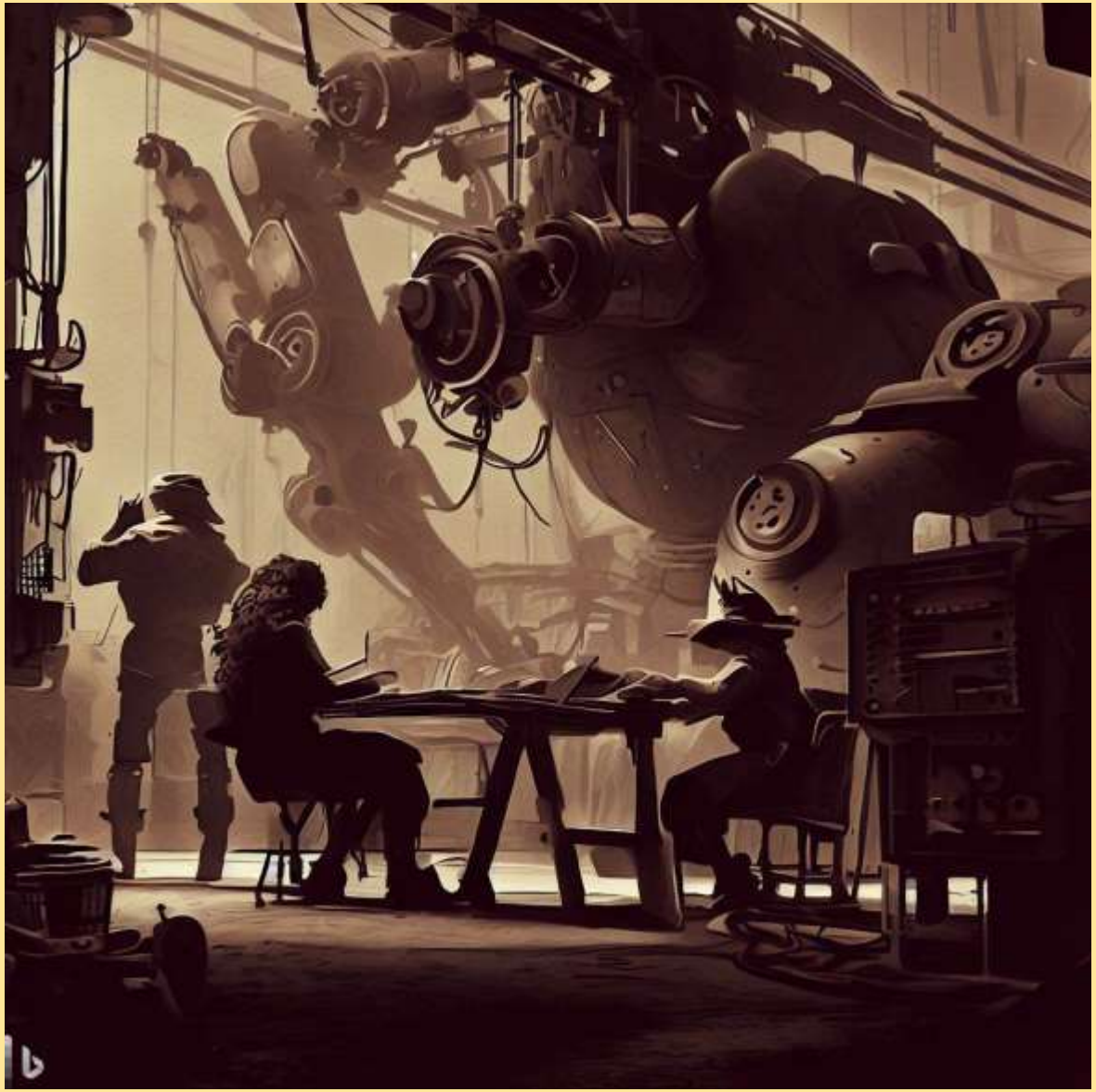
Il rischio è definito come la combinazione di due componenti:

- La **probabilità** che si verifichi un danno
- Le conseguenze del danno, ovvero la sua **gravità**

Gestione del Rischio

La Gestione del Rischio (**Risk Management**) è l'insieme di strumenti utilizzati per misurare o stimare il rischio e per sviluppare delle strategie per governarlo.
Viene condotta dal **Risk Team**, che è composto da persone esperte nel contesto.
Punto di partenza è il Piano di Gestione del Rischio (**Risk Plan**), che include:

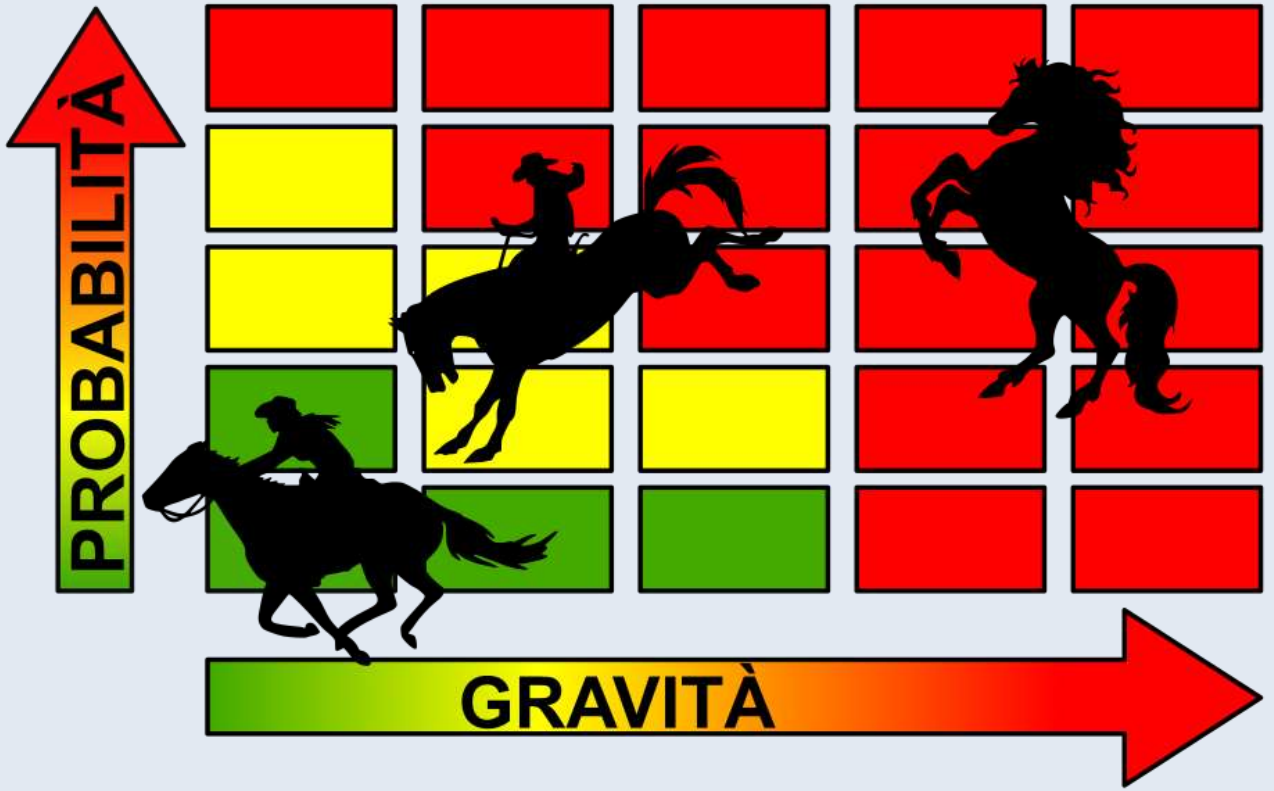
- Scopo e campo di applicazione del piano, con identificazione e descrizione del dispositivo.
- Piano di verifica.
- Responsabilità.
- Requisiti per esaminare le attività di gestione del rischio.
- Criteri per l'accettabilità del rischio.



Il Risk Team!

Matrice Semiquantitativa

Le **combinazioni accettabili** di Probabilità e Gravità vengono sintetizzate in una matrice semiquantitativa, che aiuta a dare priorità agli obiettivi di mitigazione



Analisi dei Rischi (Safety)

L'**Analisi dei Rischi** cerca di dare uno sguardo d'insieme ai possibili rischi, e si sviluppa in tre fasi:

1. Descrizione dell'**uso previsto** del dispositivo ed elenco delle **caratteristiche** relative alla sicurezza.
2. Identificazione dei **pericoli** noti o prevedibili del dispositivo, sia in condizioni normali che di guasto.
3. Stima dei **rischi** per ogni situazione di pericolo.

La **Valutazione del Rischio** consiste nel valutare se, in base ai criteri definiti nel Piano, il rischio stimato è così basso da non rendere necessaria una mitigazione.

Controllo del Rischio

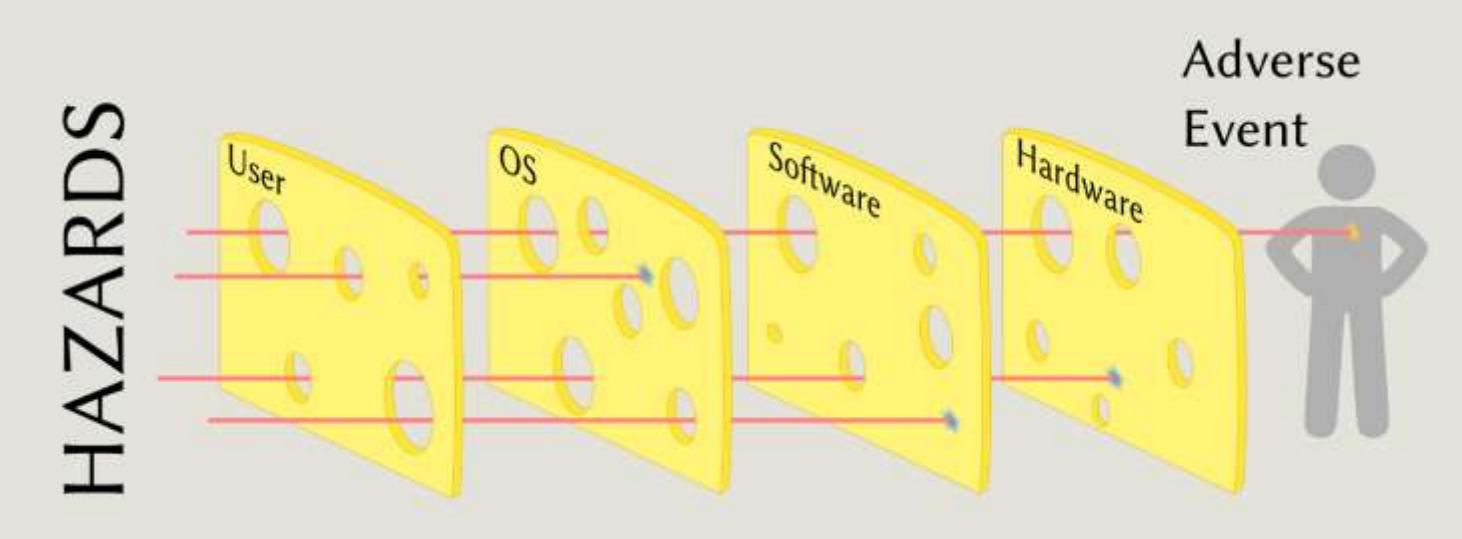
Il **Controllo del Rischio** serve a verificare che una volta applicate le dovute mitigazioni il rischio residuo sia accettabile, seguendo sei passaggi:

1. Analizzare le opzioni disponibili per **ridurre** il rischio: progettazione, misure protettive, informazioni.
2. Implementare le **misure di controllo** del rischio.
3. Valutare l'eventuale **rischio residuo** e dire se è accettabile o meno.
4. Se il rischio residuo non è accettabile, fare un'analisi **rischi/benefici** per capire se introdurre comunque il dispositivo sul mercato.
5. Valutare se le misure di controllo hanno introdotto **nuovi rischi**.
6. Garantire che siano stati valutati i rischi per tutti i pericoli identificati.

Concatenazioni

Nonostante l'efficacia delle mitigazioni, ci possono essere condizioni particolari per cui si verifica un evento avverso.

Una rappresentazione visiva di questi casi è data dal *Swiss Cheese model* di James Reason:



Altri aspetti da considerare sono le concatenazioni di rischi, che concorrono ad avere un effetto indesiderato maggiore del previsto.

Rischio Residuo Complessivo

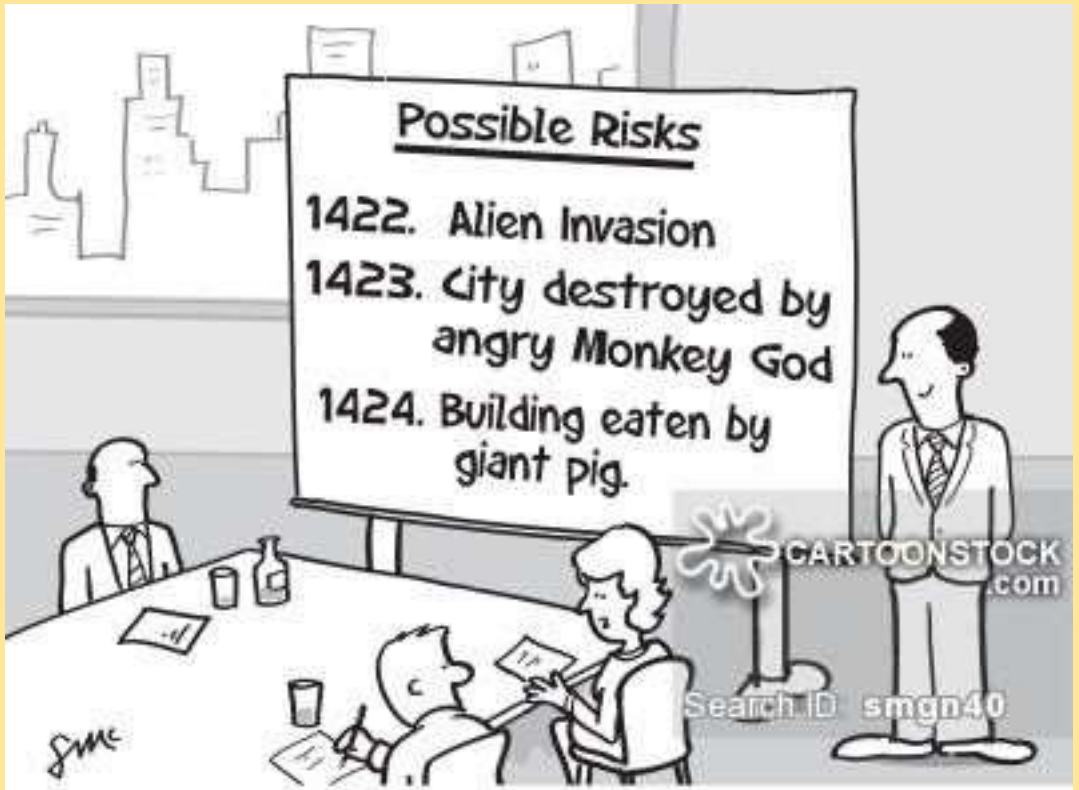
Il passaggio successivo è fare la Valutazione del **Rischio Residuo Complessivo**, ed il fabbricante dice se è accettabile o meno. I risultati del processo di gestione del rischio vengono registrati nel Rapporto di Gestione del Rischio.

- Quello che cos’è?

- Toh, è un Rischio Residuo

Riesame del processo di Rischio

A questo punto non va abbassata la guardia e bisogna organizzarsi per **esaminare** sistematicamente le **informazioni** che arrivano dalla **produzione** o dagli **utilizzatori** e capire se sono presenti pericoli che non erano stati identificati oppure se il rischio stimato derivante da un pericolo non è più accettabile oppure se le mitigazioni applicate non sono più valide. Se si verifica una di queste condizioni, va fatto un **riesame** del processo di gestione del rischio, ripercorrendo i punti visti sopra.



"Well he certainly does a very thorough risk analysis."

AI

Metafora dell'AI

Immaginiamo l'AI come un esploratore di possibilità…

...in un mondo tecnico e magico che si trova in una bottiglia...

...nella quale delle scimmie travasano cose usando un imbuto (tecnologico)...

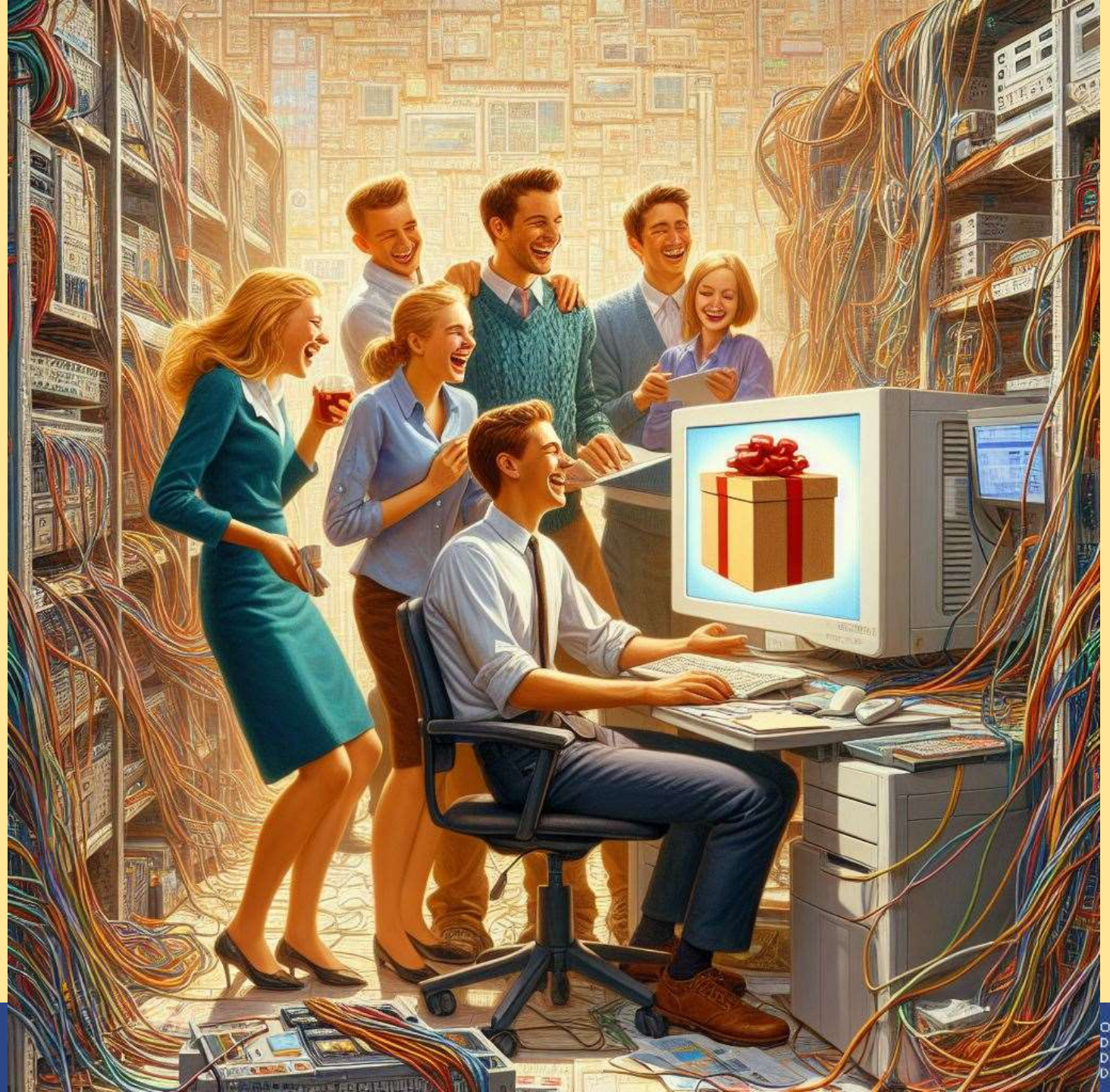
...e l'esploratore con uno schiacciasassi o una pressa appiattisce tutto...

...e quando riceve delle richieste, ritaglia dei pezzi del tritume...

...e li mette in una fotocopiatrice che fa delle copie tutte un po' diverse...

...quindi manda le risposte alla base...

...dove chi ha fatto le domande si sbellica dalle risate...



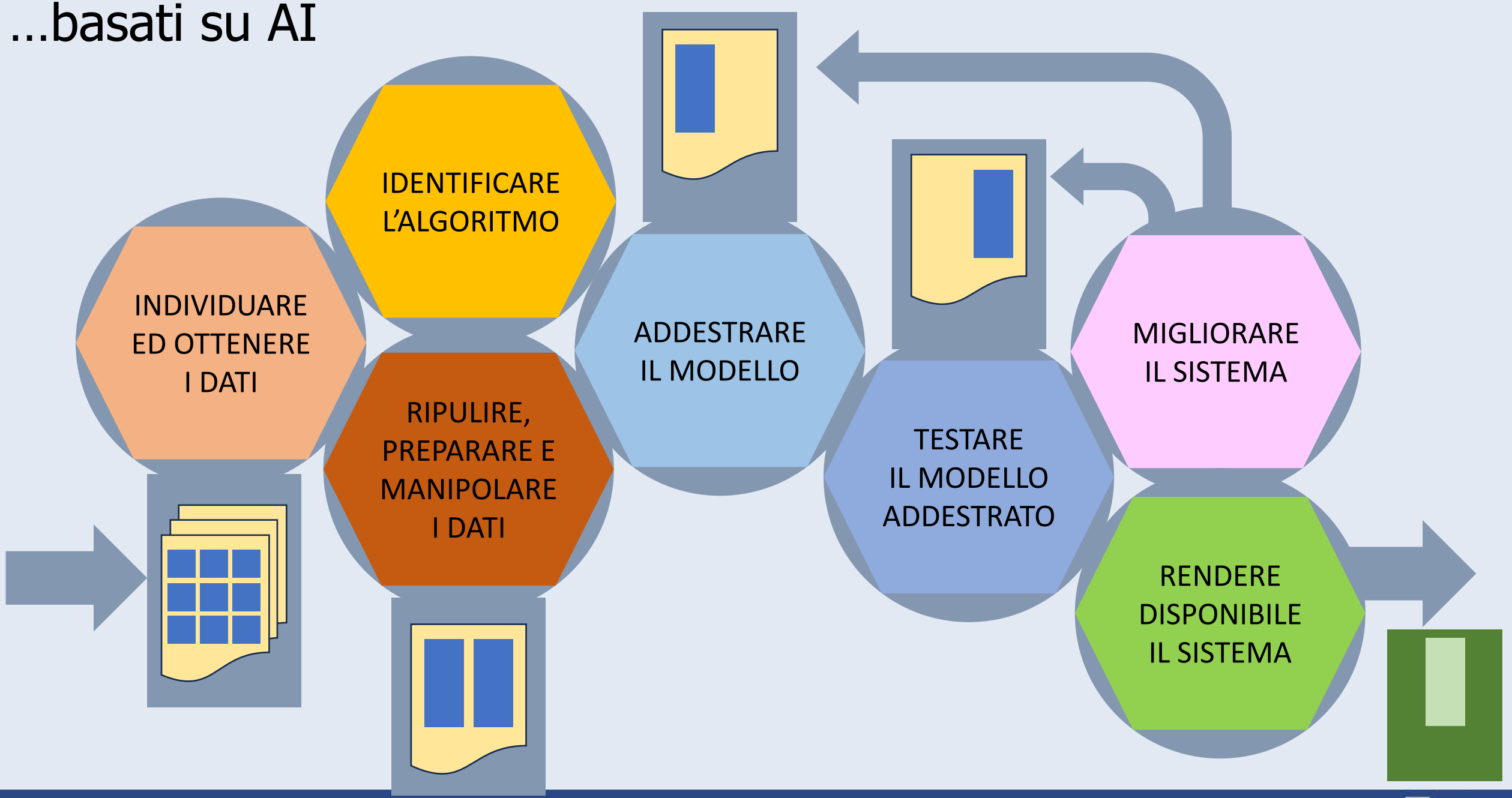
...oppure dove chi ha fatto le domande applica le risposte così come sono alla vita reale ed accadono cose terrificanti.

Cos’è l’AI?

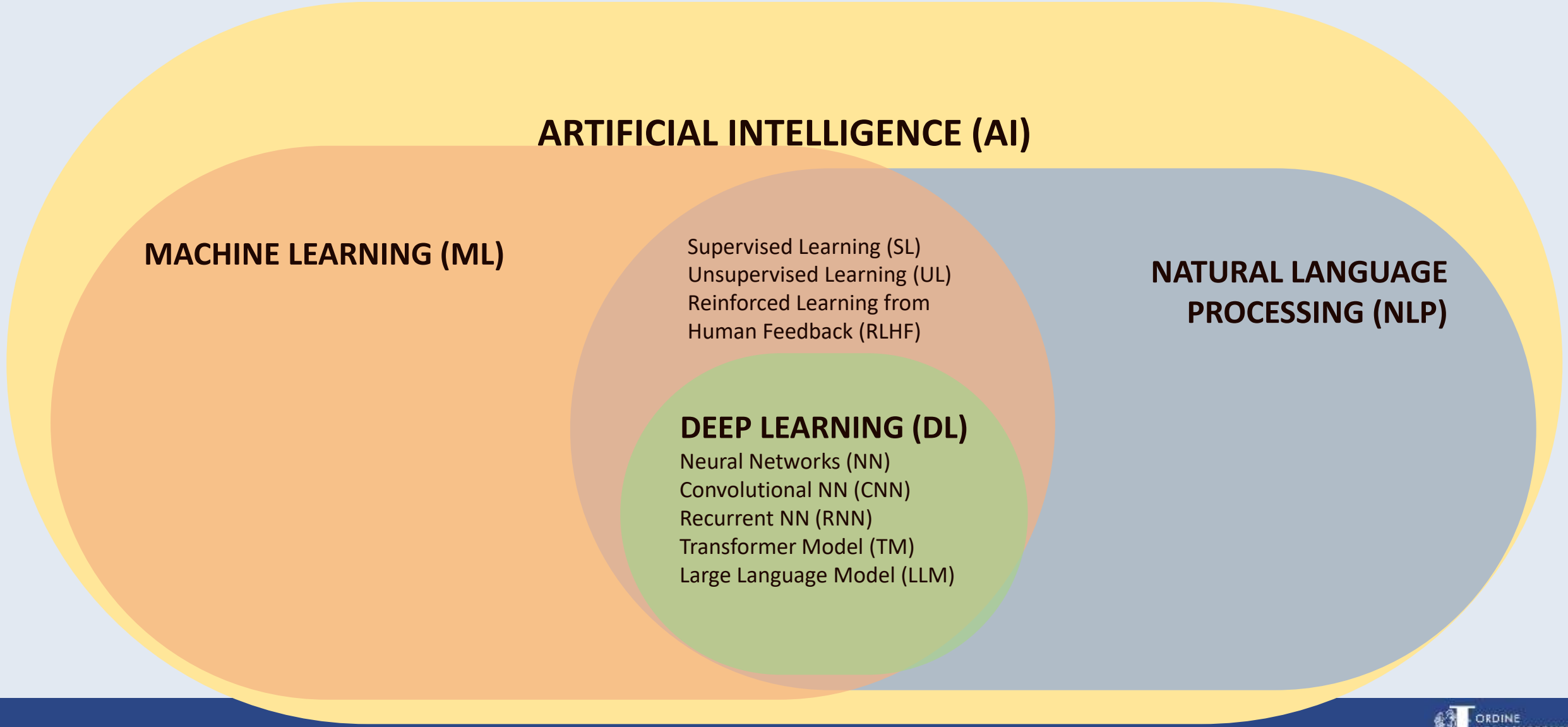
Niente di magico.

Ci sono persone che sviluppano programmi…

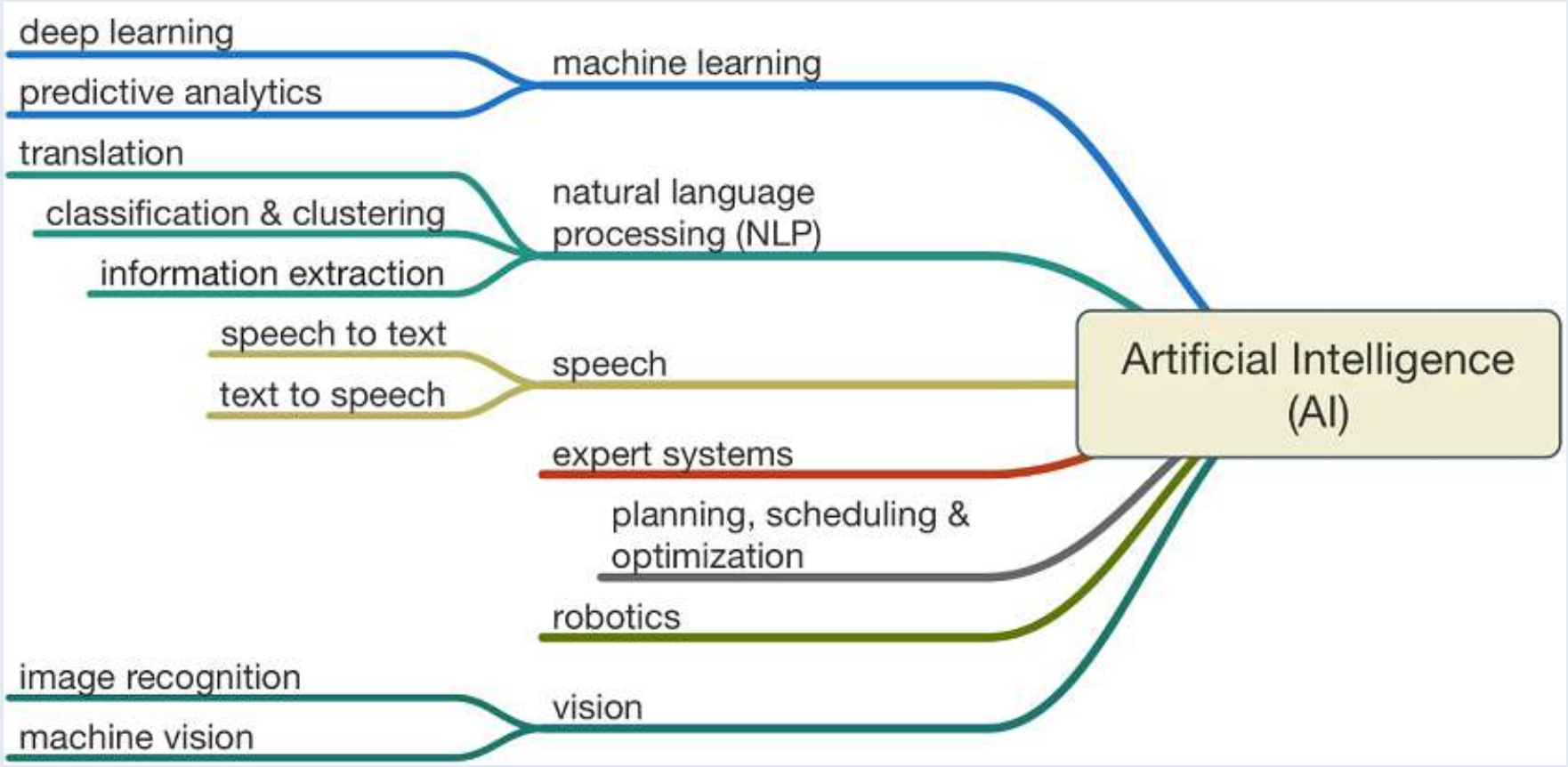
…basati su AI



Il mondo dell'AI…

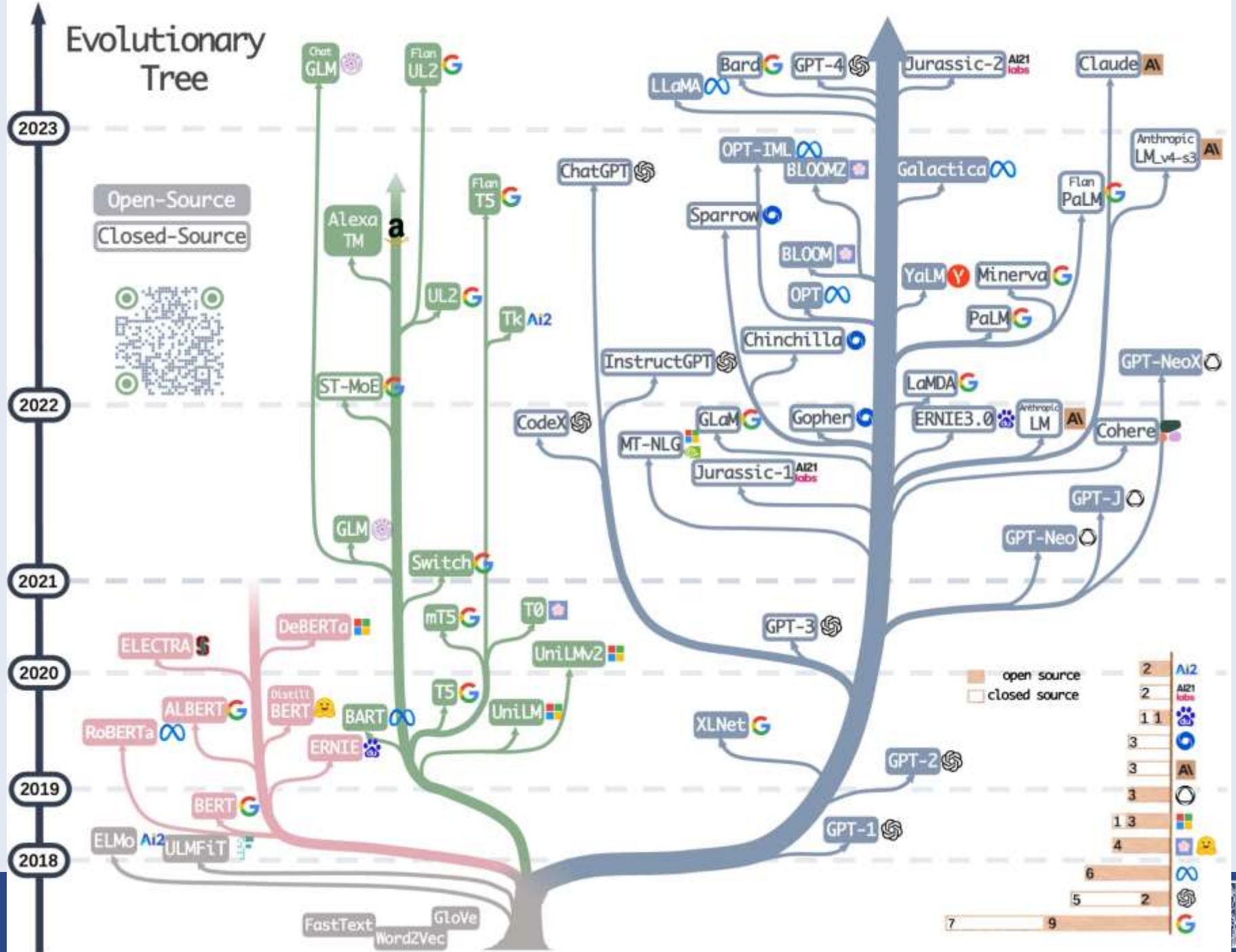


…è difficile da classificare…



Fonte: https://futurearchitectureplatform.org/news/28/ai-architecture-intelligence/

...molto difficile!

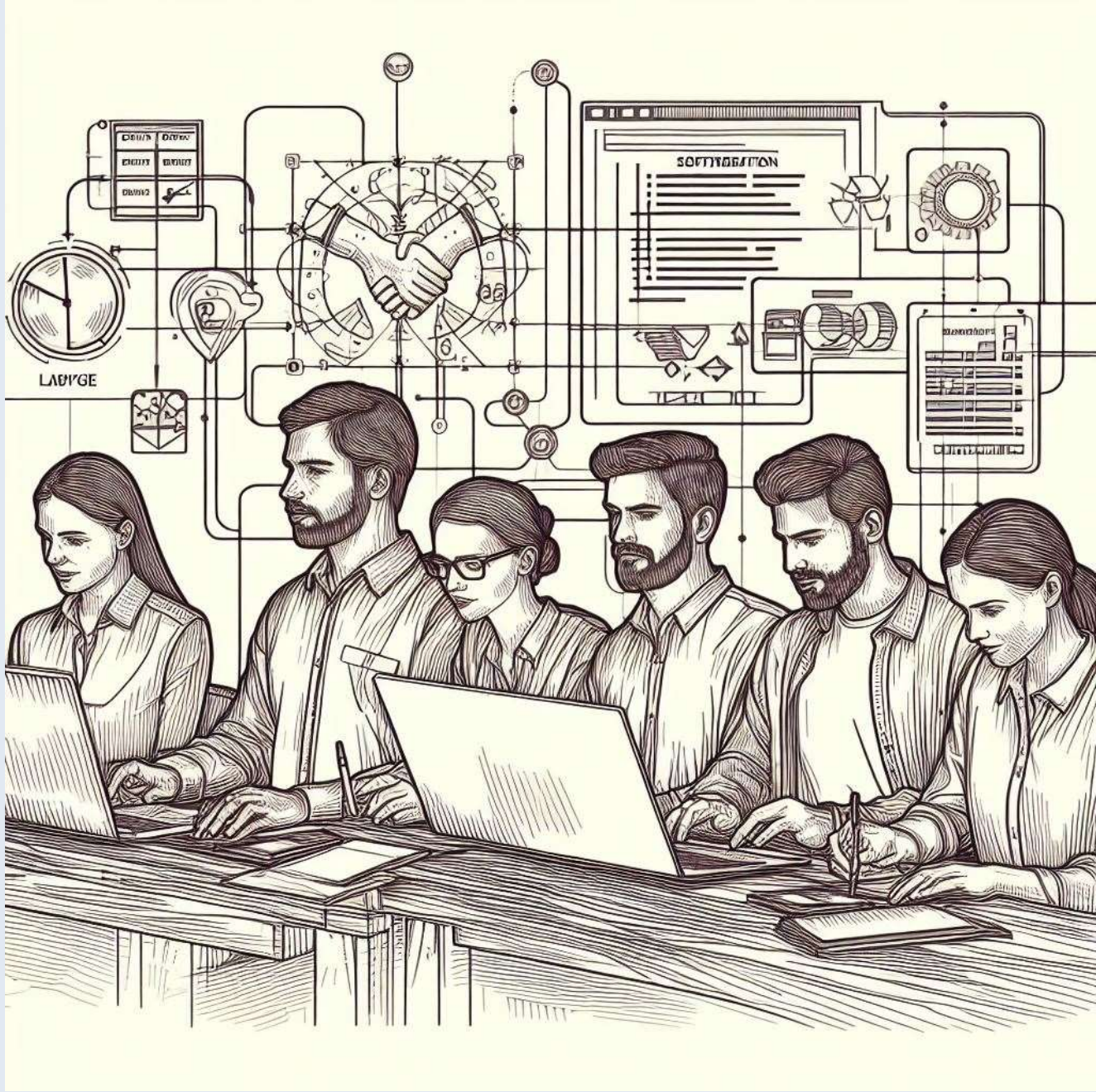


Fonte: https://github.com/Mooler0410/LLMsPracticalGuide

I sistemi basati su AI possono aiutarci a trovare informazioni…

…ma in fondo al pozzo non c’è niente di misterioso…

…ci sono programmi progettati, scritti, addestrati e testati da sviluppatori.



I sistemi *apprendono* da chi li istruisce

Chi si occupa di addestrare le AI?

- Nelle soluzioni commerciali il *training* viene fatto seguendo logiche di mercato.
- Ad addestrare i sistemi cooperativi o aperti al vasto pubblico sono quasi sempre volontari che inseriscono principalmente dati di loro interesse, e questo crea degli scostamenti (bias) dalla *via di mezzo* e conseguenti deviazioni nelle risposte *attese* (ma esiste una risposta *esatta*?).
- Ci sono *communities* che alla base pongono principi etici, ma c'è ancora tanta strada da fare.

E in ambito sanitario?

L’AI si sta diffondendo in ambito sanitario

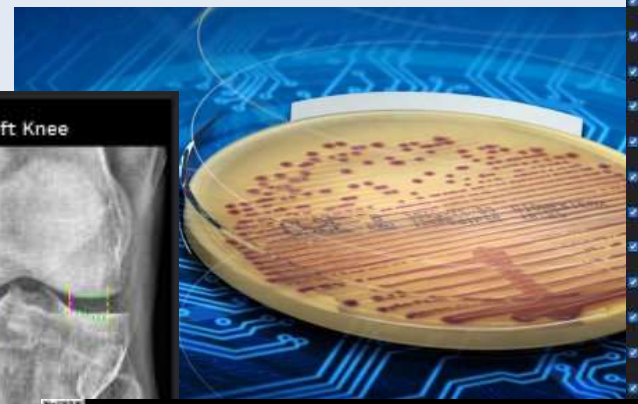
In ambito **diagnostico**, specialmente in Radiologia, si sono sempre utilizzate soluzioni all’avanguardia per velocizzare il processo di indagine attraverso software di analisi per le immagini o filtri di enhancement. Nell’ultimo periodo sono sorte soluzioni di vario tipo basate su AI, specifiche per tipi di patologia o per regione anatomica o per modalità.

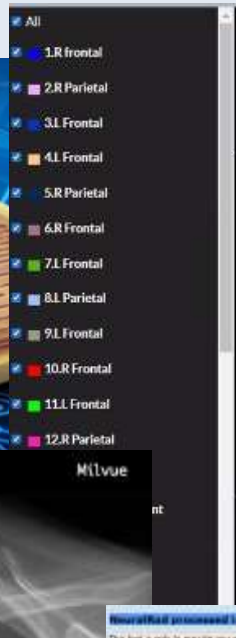
In ambito **preanalitico** sistemi basati su AI vengono utilizzati per l’identificazione di colonie batteriche e per lo studio degli antibiotici abbattendo i tempi di analisi ed anticipando i tempi di somministrazione della terapia.

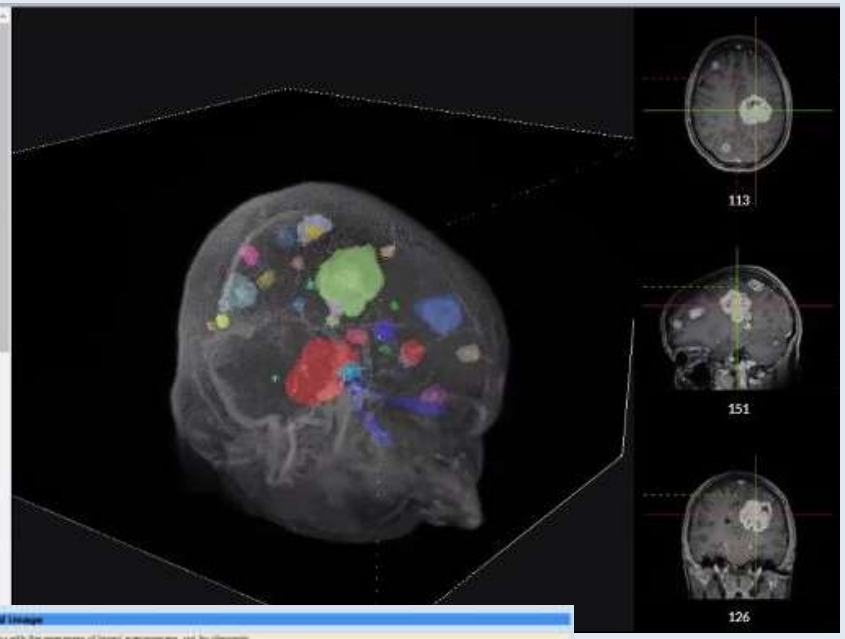
In ambito **farmaceutico** l’AI è un fattore considerato utile per ridurre tempi e costi di ricerca.

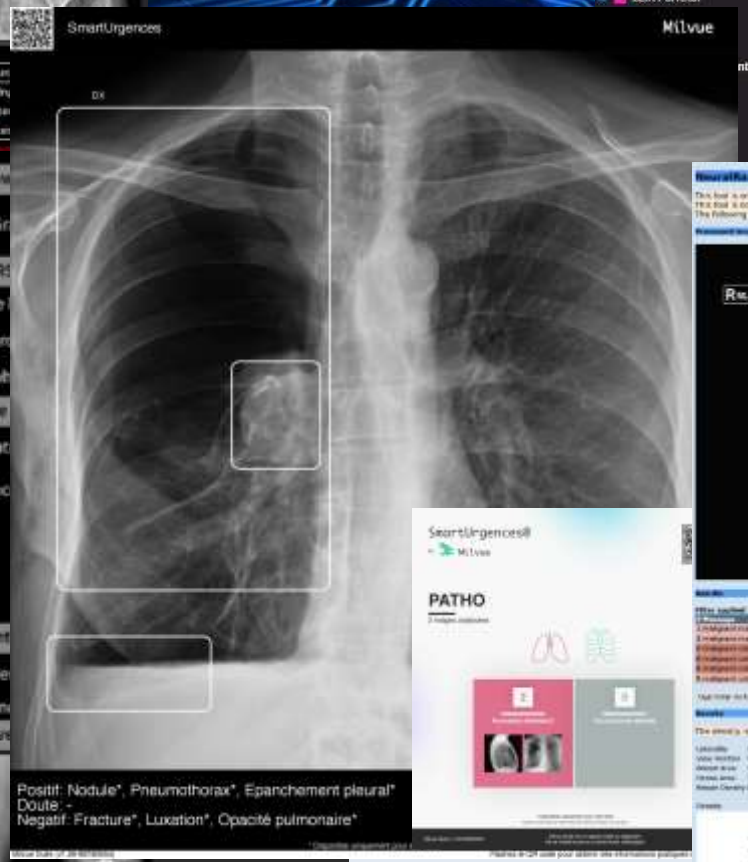
In ambito **terapeutico** si stanno facendo delle valutazioni sperimentali.

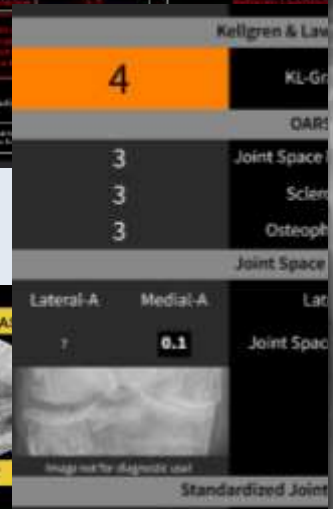
Molte soluzioni…

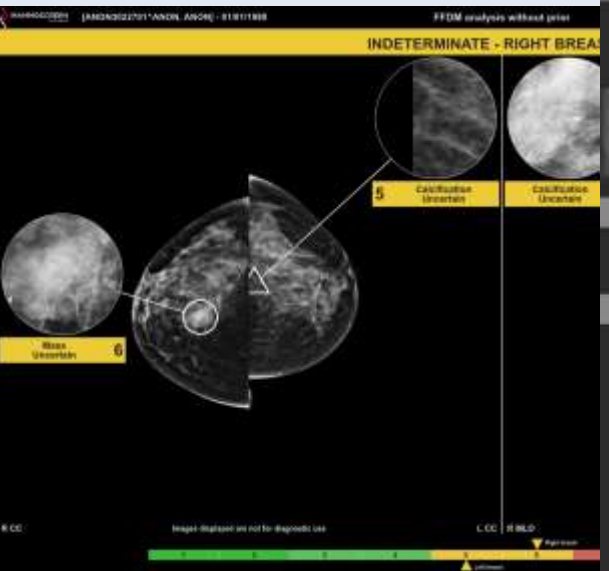


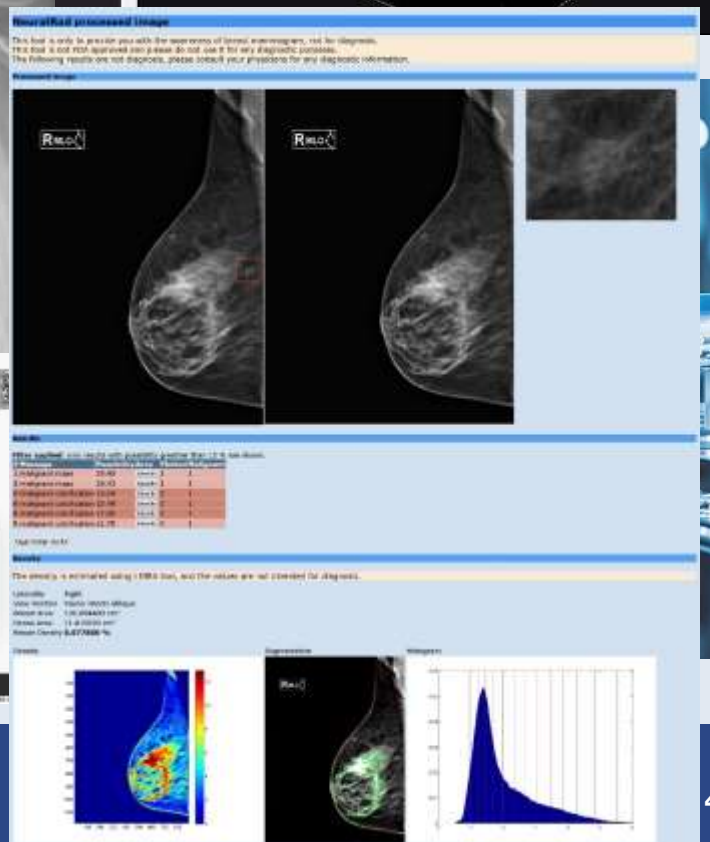












…ma i sistemi devono essere certificati

I sistemi contenenti software utilizzati in ambito sanitario devono essere certificati come **Dispositivi Medici** o come **Dispositivi Diagnostici in Vitro**, per cui devono passare attraverso un **pesante processo di validazione**.

Anche i sistemi composti da solo software.

Avevo promesso che non avrei parlato di norme, cito soltanto **MDR** ed **IVDR**.

E l'**AI Act**.

L’atteggiamento dello Specialista?

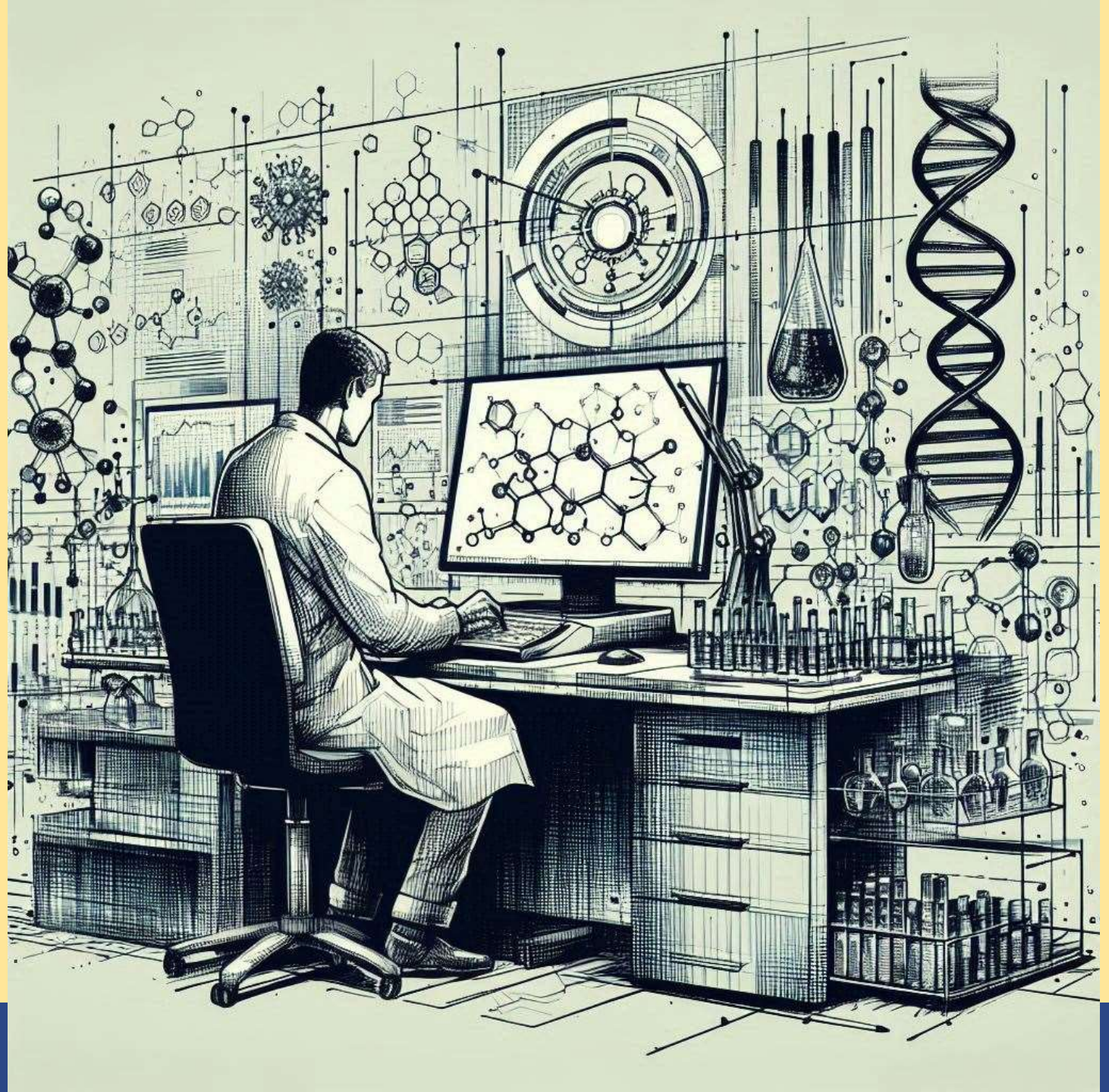
Nell’ultimo periodo l’utilizzo dell’AI è stato un **tema molto discusso** fra i Medici, ed al momento ci sono tre tendenze:

- Specialisti che **non vogliono** utilizzare sistemi basati su AI
- Specialisti che **utilizzano** sistemi basati su AI per eliminare i casi negativi o per *smaltire* la corrispondenza di basso livello
- Specialisti che utilizzano in **forma sperimentale** sistemi basati su AI

A Brescia

A Brescia ci sono vari tipi di esperienze sul tema AI in ambito medicale

- Ricerca, a livello di Università
- Sperimentazione a livello Ospedaliero
- Molti i Produttori di IVD e DM basati su AI
- Collaborazione fra Ordine dei Medici ed Ordine degli Ingegneri (ricordo convegno a tema del 14 dicembre)



Rischio (Cybersecurity)

Nel caso della **safety** i due elementi che definiscono il rischio sono la **gravità** e la **probabilità**, per cui se non si possono modificare i dispositivi per ridurre la gravità, vengono proposte contromisure per ridurre la probabilità che l'evento avverso si verifichi. In questo caso l'evento avverso porta ad una condizione di danno per un essere umano, perché la safety si occupa di tutelare un essere umano.

Per la **cybersecurity** ci sono **varie scuole di pensiero**. L'approccio che verrà presentato vede il rischio definito dalla combinazione delle **vulnerabilità** del sistema con l'**importanza delle risorse** da difendere. In questo caso l'evento avverso poterà ad un danno delle risorse da difendere.

E ci sono anche qui i Rischi Residui!

Gestione del Rischio

Anche nel caso della Cybersecurity la Gestione del Rischio (**Cybersecurity Risk Management**) viene condotta da un **Cybersecurity Risk Team** composto da persone esperte nel contesto.

Punto di partenza è sempre il Piano di Gestione del Rischio (**Cybersecurity Risk Plan**), che definisce i criteri, le attività e le responsabilità coinvolte nel processo di controllo dei Rischi.

Il Cybersecurity Risk Plan contiene le matrici semiquantitative utilizzate per la valutazione dell'impatto delle risorse sugli obiettivi di sicurezza.

Il Risk Team per la Cybersecurity!

Obiettivi fondamentali di sicurezza (Security Goals)

Vanno identificati all'inizio del processo di gestione del Rischio.
Seguendo le pratiche comuni più utilizzate, per l'esempio proposto viene proposta la cosiddetta **triade CIA**:

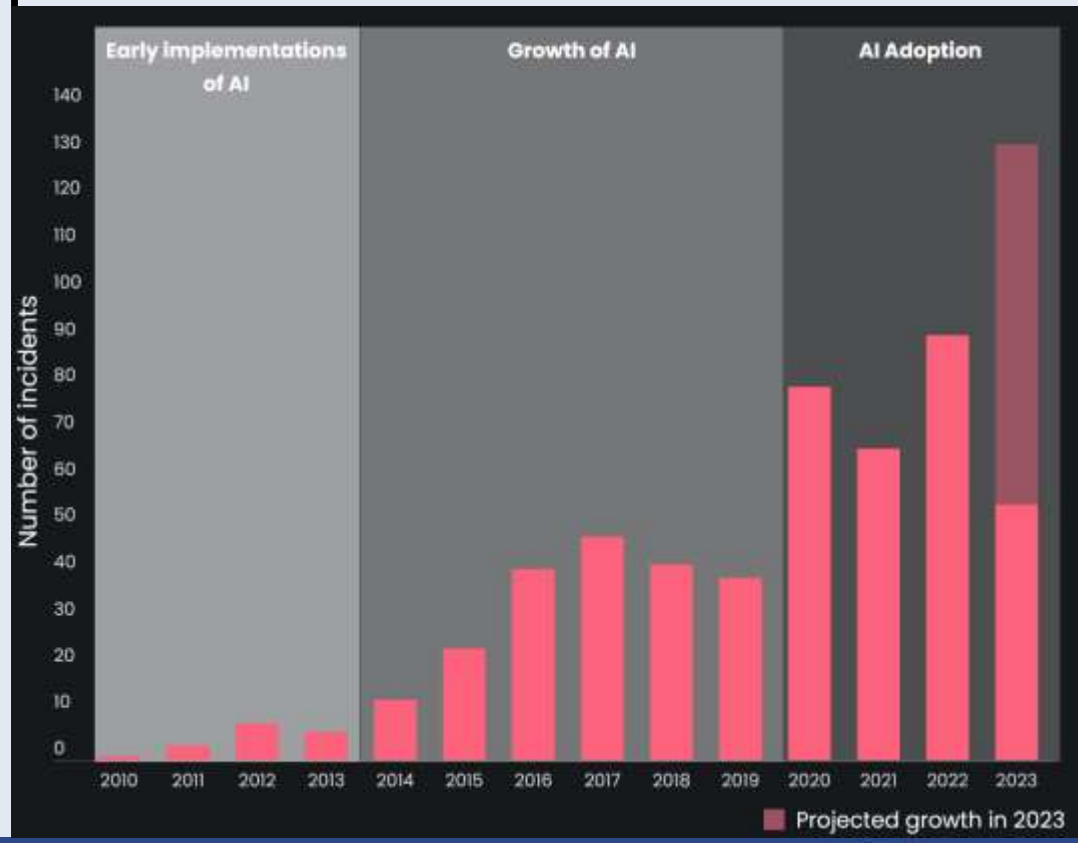
Confidentiality	Confidenzialità delle informazioni
Integrity	Integrità delle informazioni
Availability	Disponibilità delle informazioni

Un metodo diffuso per raggiungere questi obiettivi consiste nel dare loro un **peso** che dipende dal sistema oggetto della nostra attenzione. Avere valori numerici aiuta nella valutazione. Nell'esempio si useranno pesi da 1 a 10.

Incidenti ed infortuni

Data la vasta diffusione di sistemi basati su AI, c'è un'ampia casistica di incidenti ed infortuni in cui spunta lo zampino di questo tipo di tecnologia, ma una buona parte di questi problemi sono dovuti ad un utilizzo non consapevole dell'AI.

Ci sono siti che raccolgono casi rilevanti, ad esempio:
https://incidentdatabase.ai



L’esempio

A questo punto ci serve un **esempio**, che rende più semplice proseguire.

Supponiamo che ci abbiano chiesto di fare un’Analisi dei Rischi Cybersecurity di un dispositivo medico di cui sappiamo poco: un **gestore di cartelle cliniche** con un **modulo basato su AI** per **preparare lettere di dimissioni** ed **inviarle al Medico richiedente**.

Nel nostro **Cybersecurity Risk Team** c’è un infermiere che ci spiega come è stato acquisito il sistema e ci fa avere della **documentazione tecnica** dalla quale scopriamo che faceva parte di una fornitura esistente poi ampliata. Il sistema è marcato CE, ma la documentazione è molto vaga sui dettagli tecnici. Il venditore, interpellato, dice *«è un sistema sicuro e dato che è basato su cloud, non ci sono problemi hardware e non contiene software!»*, a questo punto noi iniziamo a rabbrividire...

Per l’esempio è stato scelto un dispositivo medico, ma il **principio** si può applicare a **qualsiasi sistema** contenente software.

I Security Goals dell'esempio

Dopo avere studiato il dispositivo, parlato con gli utilizzatori, letto a fondo i manuali tecnici e quanto offre la bibliografia, insomma dopo esserci documentati (es. sulle cartelle cliniche ed il fatto che secondo MDR possono essere classificate come Dispositivi Medici di classe IIb), diamo dei punteggi ai nostri Security Goals (è un esempio!):

Goal	**Confidentiality**	**Integrity**	**Availability**
Peso	8	10	6
Motivo	Sono memorizzati dati personali e dati sensibili. Una eventuale divulgazione potrebbe causare disagio al paziente, avere impatto su eventuali assicurazioni *e violerebbe il GDPR*.	Una variazione dei dati potrebbe portare ad una terapia errata, con possibile conseguente peggioramento dello stato di salute del paziente (impatto sulla safety).	Una mancata disponibilità dei dati porterebbe ad un ritardo della terapia (ma il Medico potrebbe somministrarne una generica).

Risorse (Assets) da proteggere

Il passo successivo consiste nell'**identificare le risorse da proteggere**, in particolare quelle che sono direttamente a contatto con un utente o con la rete, ed a valutare l'effetto di contromisure verso le alterazioni del sistema.

Anche alle risorse viene dato un peso, in base alla loro criticità valutata secondo i Security Goals.

Per avere dei numeri più semplici su cui ragionare, possiamo utilizzare questi persi per calcolare uno **score cumulativo** che ci esprima l'importanza della risorsa, ad esempio:

Score risorsa = Radice della Media dei prodotti dei pesi di risorsa e di Security Goals, arrotondata all'intero successivo (massimo 10)

Nel nostro esempio potremmo avere una serie di risorse:

Asset (Risorsa)	Confidentiality (x8)	Integrity (x10)	Availability (x6)	Asset Score
Modulo AI per preparare la Lettera di Dimissioni Ospedaliera	7 Un exploit andato a buon fine potrebbe portare alla generazione di una LDO con dati riservati in eccesso rispetto il contenuto atteso.	9 Un exploit andato a buon fine potrebbe portare alla generazione di una LDO contenente indicazioni terapeutiche errate.	1 Un exploit andato a buon fine potrebbe mandare in crash il modulo, causando rallentamenti.	√(7x8+9x10+1x6)/3 = 7,1 Per cui lo score sarà 7
Software e librerie di terze parti (SOUP)	10 Un exploit andato a buon fine porterebbe alla divulgazione dei dati clinici del paziente.	8 Un aggiornamento non retrocompatibile potrebbe portare a corruzione dei dati con conseguente rallentamento nella terapia.	8 Un aggiornamento non retrocompatibile di una libreria di terze parti potrebbe bloccare la comunicazione tramite rete	√(10x8+8x10+8x6)/3 = 8.3 Per cui lo score sarà 8

Asset (Risorsa)	Confidentiality (x10)	Integrity (x10)	Availability (x6)	Asset Score
Servizio di email	10 Un exploit andato a buon fine su di un servizio di email non sicuro porterebbe alla divulgazione dei dati clinici del paziente.	6 Un exploit andato a buon fine su di un servizio di email non sicuro potrebbe portare ad un rallentamento della terapia.	6 Un exploit andato a buon fine su di un servizio di email non sicuro potrebbe portare ad un rallentamento della terapia.	√(10x10+6x10+6x6)/3 = 8,1 Per cui lo score sarà 8
…				

A livello preliminare sembra che la risorse più critiche siano le librerie di terze parti ed il servizio di email non sicuro, ma per restare in tema vedremo in dettaglio dei possibili rischi legati al modulo AI.

Le risorse importanti vanno protette

Minacce (Threats)

Quando le minacce sono applicate ad una risorsa, è possibile dare loro uno score basato sulla **possibilità** che l'**attacco** vada a **buon fine**.

Per l'esempio viene utilizzato un modello di classificazione delle minacce che è vecchio ma ancora funzionale, il modello **STRIDE**. L'acronimo nasce dalle possibili famiglie di minacce:

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of Service (DoS)
- Elevation of privilege

Minaccia	Descrizione	Goal violato	Applicabile a
Spoofing	Un attacco di spoofing è una situazione in cui una persona o un programma si maschera con successo falsificando i dati per ottenere un vantaggio illegittimo. Può includere Man-in-the-middle attivo.	Integrity (Authentication)	User interfaces, Network interfaces
Tampering	Modifica intenzionale di prodotti o dati in modo tale da renderli dannosi per il consumatore. Ciò include anche virus, spyware, malware, trojan (software e hardware) e attacchi di inoltro (relay attacks).	Integrity	Operating System, Software, Data, Network
Repudiation	Una persona o un programma che si dichiara non responsabile di un'azione illecita, in un contesto per il quale il sistema non è in grado di tracciare operazioni vietate. È una minaccia legata alla mancanza di progettazione.	Integrity (Non-repudiation)	Software, Data, Network
Information disclosure	Una persona o un programma che rilascia informazioni sicure o private/confidenziali in un ambiente non attendibile. Ciò include Phishing, Sniffing, Man-in-the-middle, Compromised-key, Path Traversal, Predictable Resource Location, Ransomware, Wi-Fi Eavesdropping, Data breach, Data leak e Data spill.	Confidentiality	Data, Network

Minaccia	Descrizione	Goal violato	Applicabile a
Denial of Service (DoS)	Esaurimento delle risorse necessarie per fornire il servizio, in genere ottenuto inondando la macchina o la risorsa mirata con richieste superflue per sovraccaricare i sistemi e impedire che alcune o tutte le richieste legittime vengano soddisfatte. Include UDP bombing, TCP SYN flooding, Ping of death, Smurf attack, Teardrop attacks, Slow Read attack, Slowloris, R-u-Dead-Yet (RUDY), e Snooping.	Availability	Operating System, Software, Network
Elevation of privilege	Questa minaccia sfrutta un bug, un difetto di progettazione o una supervisione della configurazione in un sistema operativo o in un'applicazione software per ottenere un accesso elevato a risorse normalmente protette da un'applicazione o da un utilizzo. Comprende tutti gli esempi di attacco di cui sopra, oltre ad Adware, Worms, Luring attack.	Confidentiality (Authorization)	Operating System, User interfaces, Network

Vulnerabilità

Quando possibile, è bene controllare se sul sistema oggetto di analisi sono presenti **vulnerabilità** note, pubblicate con dovizia di particolari su registri pubblici come quello del **NIST** (https://nvd.nist.gov/vuln), cui ci riferiremo nel nostro esempio.

Se il sistema che stiamo studiando ha dei software o delle librerie che compaiono in questo database, possiamo utilizzare lo **score CVSS** come **fattore correttivo** per lo score che abbiamo assegnato alla minaccia.

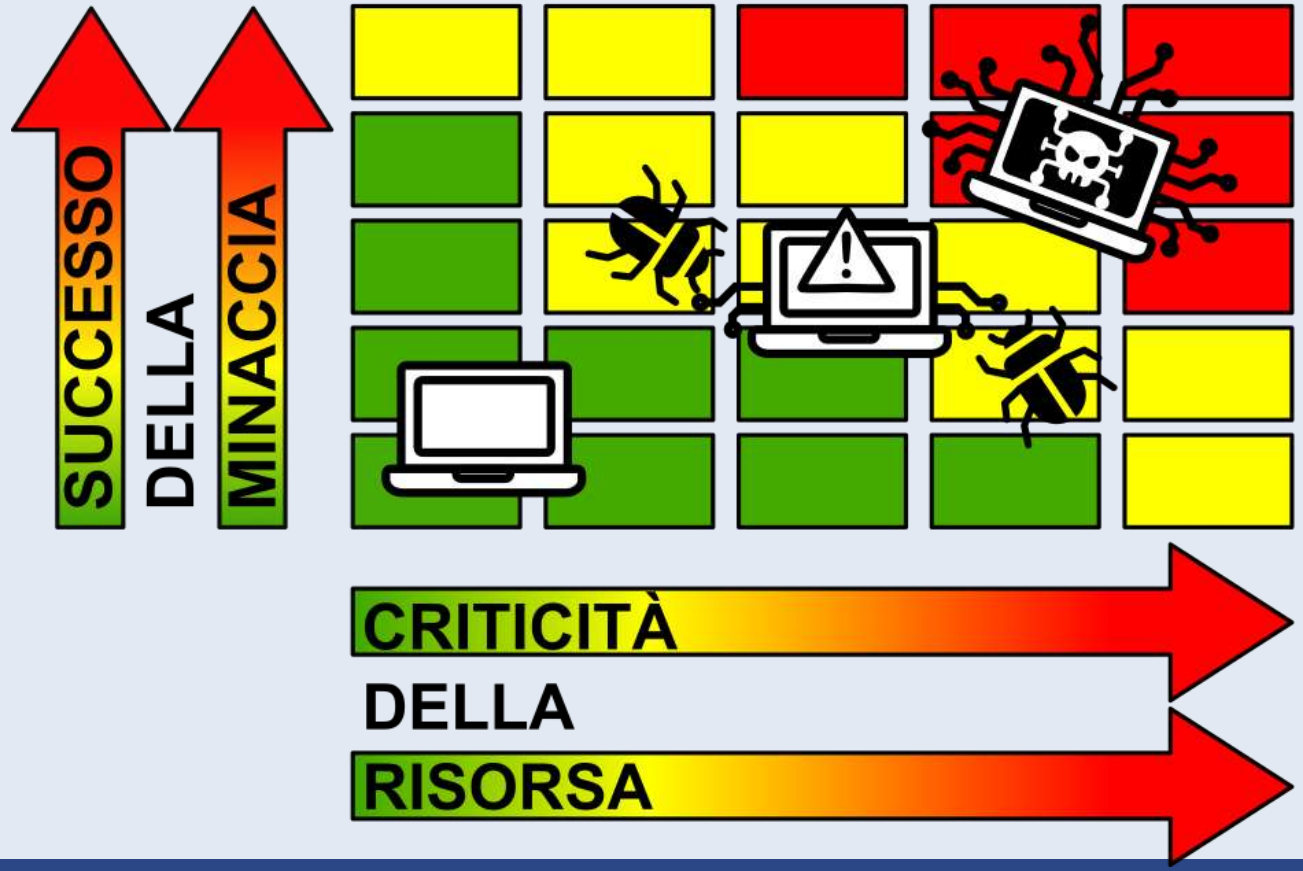
Ad esempio (è un esempio, non è una regola!) potremmo usare il valore massimo fra lo score della minaccia e lo score della vulnerabilità.

La minaccia può attraversare i punti vulnerabili e causare un evento avverso

Quindi bisogna preparare misure protettive adeguate

Matrice Semiquantitativa Cybersecurity

Le **combinazioni accettabili** dei possibili attacchi riusciti alle risorse vengono sintetizzate in una matrice semiquantitativa, che ci aiuta a classificare i rischi



Finalmente fanno capolino i Rischi…

Avendo definito tutto quello che può servire per il **Risk Plan**, possiamo concentrarci sui **possibili rischi**, e per il nostro esempio (non sappiamo molto sul cloud utilizzato e sul misterioso software) possiamo trovarne parecchi.

Come si individuano i rischi?

Studiando il dispositivo o il software, **parlando** con i progettisti, gli utilizzatori, le persone coinvolte, gli esperti del settore, adottando delle **tecniche note**, utilizzando delle **checklist** realizzate a partire da norme o linee guida o framework.

Si tratta di un **processo laborioso** che richiede di entrare nel dettaglio del dispositivo, focalizzandosi sul suo intended use, e richiede precisione.

Tecniche per l'identificazione dei rischi

Alcuni esempi di tecniche (non c'è tempo per entrare nel dettaglio):

- **Brainstorming**
- **Root Cause Analysis** (**RCA**), tipicamente utilizzata per il problem solving e quindi più efficiente quando ci sono problemi noti, comprende tecniche come:
  - **Five whys** (Cinque perché)
  - Failure mode and effects analysis (**FMEA**)
  - Fault tree analysis (**FTA**)
  - Diagrammi di **Ishikawa**
  - Analisi di **Pareto**
- **Strengths, Weaknesses, Opportunities, and Threats** (**SWOT**) **Analysis**

Framework o checklist per l'identificazione dei rischi

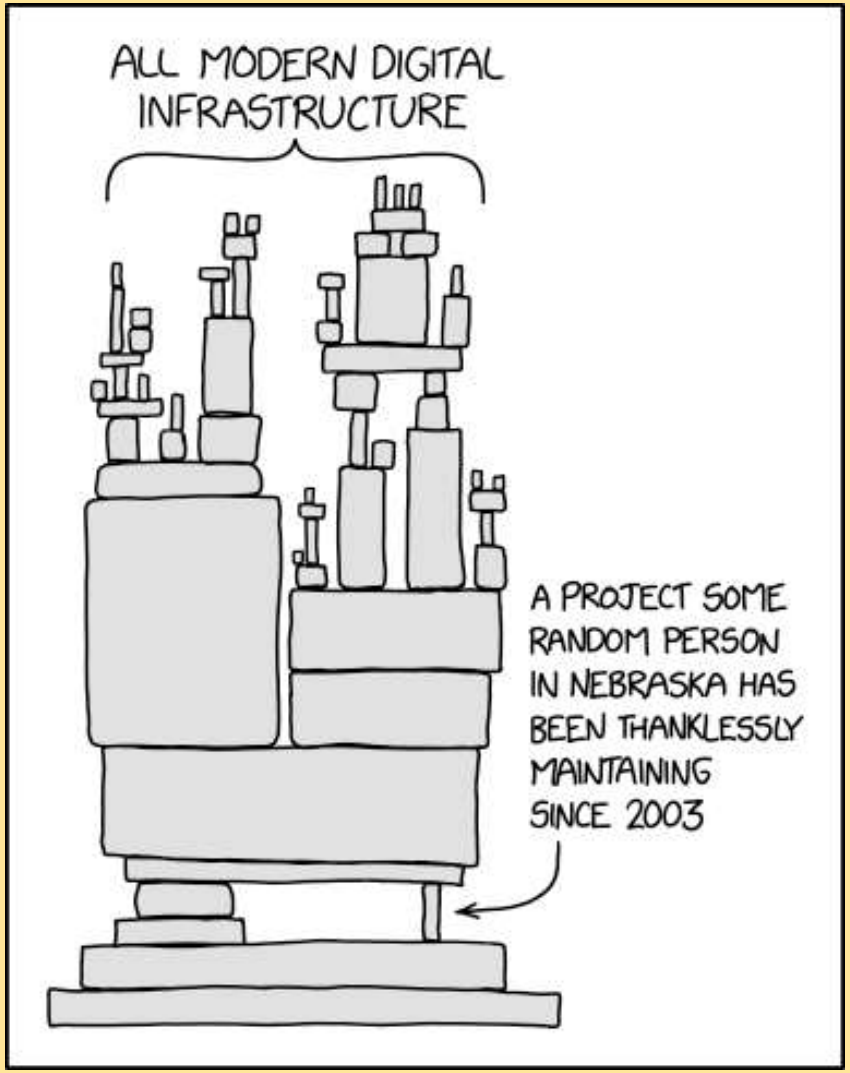
Alcuni esempi di **framework** (non c'è tempo per entrare nel dettaglio):

- Checklist basate sulle **norme ISO** (es. Direttiva Macchine, MDR, IVDR, Software Lifecycle, Usability, ICT Security, 27001/27002, ecc)
- Checklist basate sulle **guidances FDA**
- National Institute of Standards and Technology (**NIST**) Cybersecurity Framework (**CSF**): Identify, Protect, Detect, Respond, Recover
- Center for Internet Security (**CIS**) Controls
- Control Objectives for Information and Related Technologies (**COBIT**)
- Committee of Sponsoring Organizations (**COSO**) Enterprise Risk Management (ERM) Framework

Rischi identificati (esempio)

Una volta scelta ed applicata la tecnica che più si adatta al nostro problema, avremo identificato un certo numero di rischi. Per il nostro esempio:

#	Rischio
1	Se il modulo AI si trovasse su di un cloud non sicuro e fosse sensibile ad Injection attacks, degli utenti malevoli potrebbero portare a generare Lettere di Dimissioni Ospedaliere con dati incoerenti relativamente alla terapia, con possibili implicazioni anche sulla salute di un paziente.
2	Se il servizio che invia le email fosse ospitato presso un host gestito da utenti malevoli, questi potrebbero utilizzare tecniche di analisi per acquisire informazioni sui pazienti e profilarli al fine di venderne i dati, con conseguente danno di privacy.
…	Su software e librerie di terze parti (SOUP) ci sarebbe molto da dire…



I SOUP vanno tenuti sotto controllo, e possibilmente validati se utilizzati per un dispositivo o per un software

Step 1 Classifichiamo il Rischio - Asset

#	Rischio	Tipo di Asset	Score
1	Utente malevolo che altera il comportamento del sistema AI che genera le LDO.	Modulo AI per preparare la Lettera di Dimissioni Ospedaliera	7
2	Mail server malevolo che profila gli utenti.	Servizio di email	8

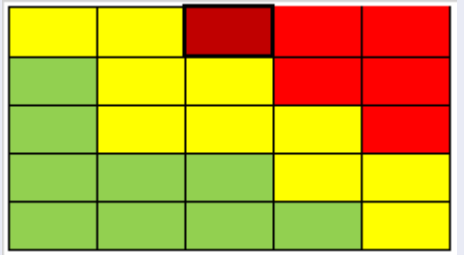
Step 2 Classifichiamo il Rischio - Vulnerability & Threat

#	Rischio	Offender	Vulnerabilità	STRIDE	Score
1	Utente malevolo che altera il comportamento del sistema AI che genera le LDO.	Network Attack	Weak access control	Potrebbe essere un caso di Spoofing, ma anche di Tampering	5
2	Mail server malevolo che profila gli utenti.	Malevolent host	Design flaw	Potrebbe essere un caso di Information Disclosure	8

Step 3 Classifichiamo il Rischio – Vulnerabilità note?

#	Rischio	CVSS	Score Finale
1	Utente malevolo che altera il comportamento del sistema AI che genera le LDO.	CVE-2016-10320 Score: 7.8	Max(5,7.8)=7.8
2	Mail server malevolo che profila gli utenti.	CVE-2018-8587 Score: 7.8	Max(8,7.8)=8

Step 4 Classifichiamo il Rischio – Così com'è

#	Rischio	Score Asset	Score Vulnerability & Threat	Matrice	Accettabile
1	Utente malevolo che altera il comportamento del sistema AI che genera le LDO.	7	7.8		Studiare in modo più approfondito
2	Mail server malevolo che profila gli utenti.	8	8		**No**

Step 5 Impatto sulla Safety?

Se si identificano Rischi che possono avere impatto sulla Safety, vanno segnalati al Team che si occupa della Gestione dei Rischi Safety

#	Rischio	Impatto sulla safety?
1	Utente malevolo che altera il comportamento del sistema AI che genera le LDO.	Una variazione della configurazione potrebbe portare ad una somministrazione errata della terapia, con possibile conseguente peggioramento dello stato di salute del paziente.
2	Mail server malevolo che profila gli utenti.	No (impatto sulla privacy ed eventuale impatto economico)

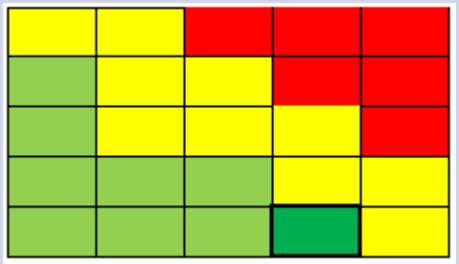
Step 6 Proporre delle mitigazioni

Un Rischio per sua natura non è mai eliminabile, ma adottando opportune **misure correttive** si può minimizzare l'impatto o la sua evenienza. Vanno mitigati anche i rischi in apparenza improbabili.

#	Rischio	Mitigazione proposta
1	Utente malevolo che altera il comportamento del sistema AI che genera le LDO.	Controllo accessi ed utenze. Vulnerability Assessment. Verifica durante l'uso che i dati di training siano quelli rilasciati con la release. Usare solo software di terze parti validato.
2	Mail server malevolo che profila gli utenti.	Invio messaggi cifrati o utilizzo di un portale validato per scaricare le LDO. Appoggiarsi a provider qualificati per le PA. Qualifica dei fornitori.

No, mandare i dati dei pazienti tramite WhatsApp non è una buona soluzione!

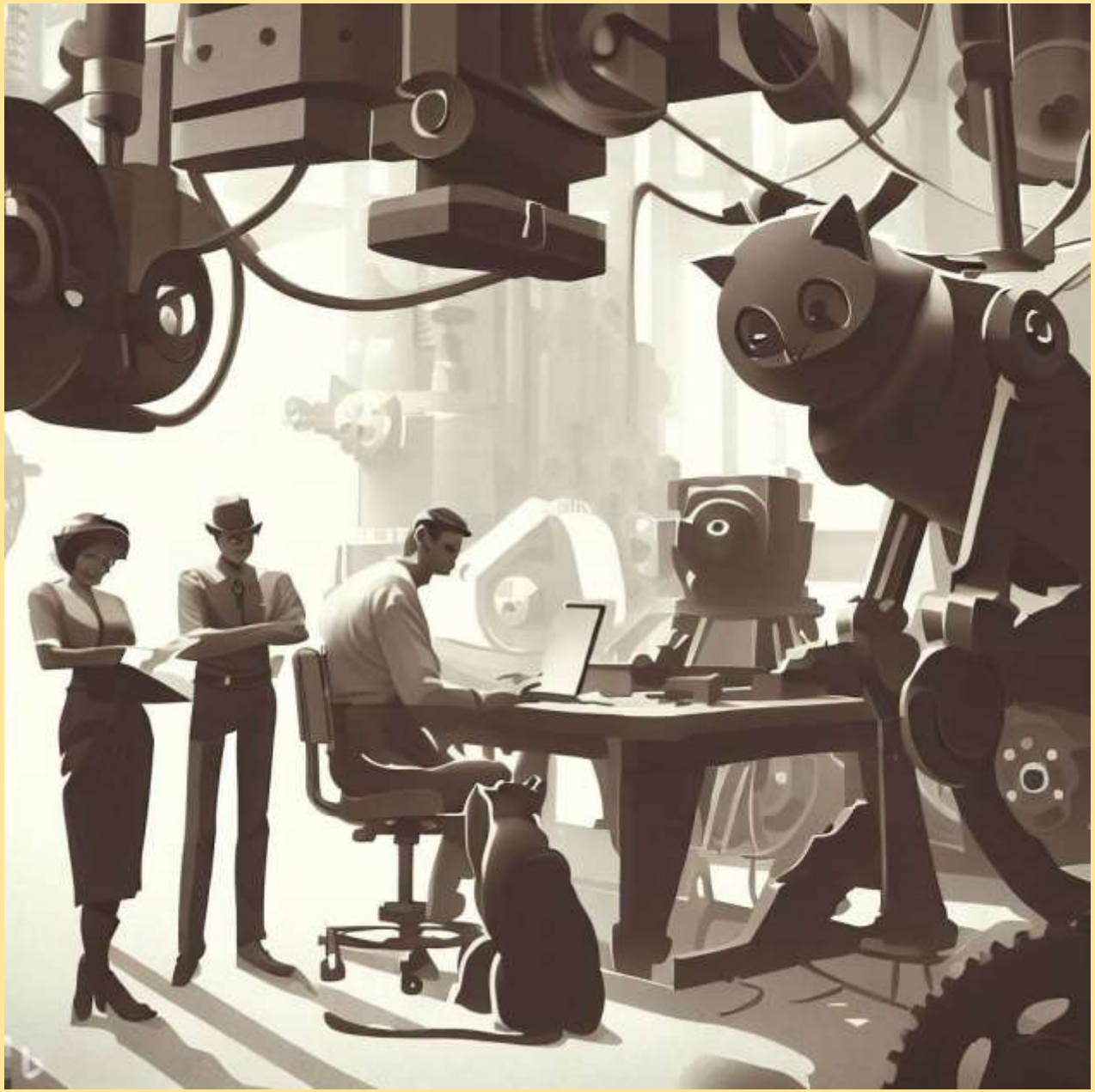
Step 7 Classifichiamo il Rischio – Cosa proponiamo

#	Rischio	Score Asset	Score Vulnerability & Threat	Matrice	Accettabile
1	Utente malevolo che altera il comportamento del sistema AI che genera le LDO.	7	2		Sì
2	Mail server malevolo che profila gli utenti.	8	5		Con Rischio Residuo

Step 8 Implementare le mitigazioni

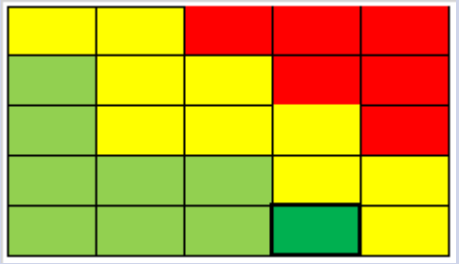
Le mitigazioni proposte possono dare origine ad esempio a:

- **Requisiti di Sicurezza**, da implementare a livello di progetto se il dispositivo o il software viene sviluppato all'interno.
- Richiesta di **nuove procedure** o di aggiornamento di procedure esistenti, da valutare insieme alla Qualità.
- **Formazione** utenti, operatori, manutentori, sviluppatori, …
- Adozione di **soluzioni software o hardware** per gestione, monitoraggio, controllo, …
- **Validazione** dei **fornitori** e del **software** di terze parti.



La Progettazione
oppure la Qualità
ricevono e sviluppano
i Requisiti di Security

Step 9 Classifichiamo il Rischio – Valutazione finale

#	Rischio	Score Asset	Score Vulnerability & Threat	Matrice	Accettabile
1	Utente malevolo che altera il comportamento del sistema AI che genera le LDO.	7	2		Sì
2	Mail server malevolo che profila gli utenti.	8	5		Con Rischio Residuo

Le mitigazioni portano
il loro beneficio

Step 10 Rischio Residuo

Un Rischio per sua natura non è mai eliminabile, per cui per ciascun Rischio va fatta una discussione sulla sua accettabilità

#	Rischio	Valutazione Rischio Residuo
1	Utente malevolo che altera il comportamento del sistema AI che genera le LDO.	Il beneficio dell'utilizzo del dispositivo medico oggetto del presente documento è superiore al relativo rischio residuo.
2	Mail server malevolo che profila gli utenti.	Dal punto di vista dell'utilizzo del sistema, sono state prese in considerazione tutte le misure per consentire robustezza agli attacchi digitali durante il funzionamento. Il rischio residuo è dovuto alla possibilità che il sistema si appoggi a servizi di fornitori non sicuri. Si ritiene che il rischio residuo sia accettabile, dal momento che la nuova procedura prevede un processo di qualifica dei fornitori, ed il mail server è stato spostato presso un provider qualificato per le PA.

Il Rischio Residuo è sempre in agguato

Step 11 – Cybersecurity Risk Management File

Cybersecurity **Risk Plan** e Cybersecurity **Risk Analysis** concorrono a formare il Cybersecurity **Risk Management File**

che verrà completato da un Cybersecurity **Risk Summary**
contenente un'analisi di alto livello e le
conclusioni sull'accettabilità

del dispositivo o del software dal punto di vista della Cybersecurity

Il Risk Summary conterrà anche un riepilogo dei Rischi Residui, che in molti casi vengono messi anche nei manuali d’uso

Conclusioni

- Un processo di **Gestione del Rischio** può essere uno **strumento** da tenere in considerazione quando si vuole trovare analiticamente un metodo per proteggere delle risorse, in particolare se critiche.
- La Gestione dei Rischi **coinvolge persone** che a tutti i livelli hanno a che fare con il dispositivo o il software oggetto di attenzione.
- Il processo **richiede un certo tempo** e porta alla **produzione di documenti** che compongono il **Risk Management File**.
- L'Analisi dei Rischi **può dare origine** a **requisiti di sicurezza** da sviluppare in fase di progetto. Anche per questo motivo è una buona pratica effettuare un'Analisi dei Rischi fin dalle prime fasi del progetto.

C’è il Rischio Residuo
di sforare con i tempi
a disposizione…

Risk Management per la privacy In Ambito medicale

e-privacy XXXV @ Brescia

Progetto Winston Smith & Ordine degli Ingegneri della Provincia di Brescia

Commissione ICT

Paolo Gibellini

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI BRESCIA

p.gibellini@gmail.com

gibellini@spe.net