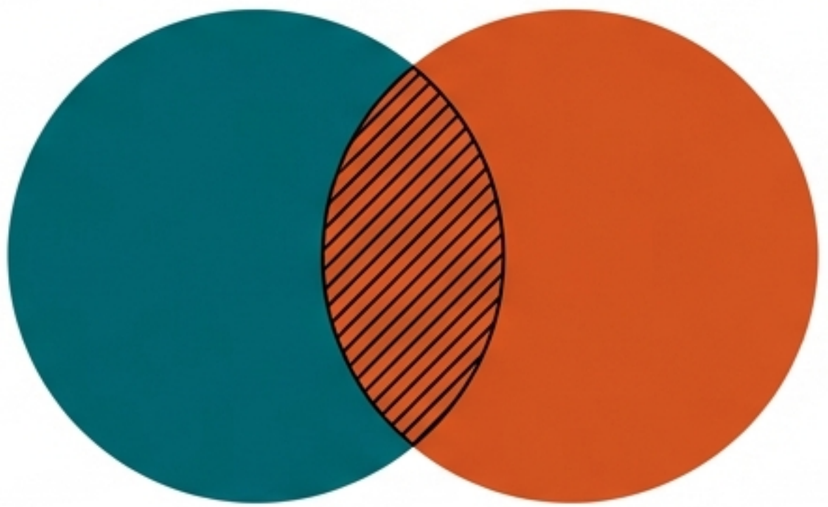
Metodologie di Valutazione del Rischio Cyber: Un'Analisi Comparativa

Dalla teoria alla pratica: un esame critico degli approcci Qualitativi, Quantitativi e Semi-quantitativi.



MODULO 6: ANALISI DEL RISCHIO

Il Mandato Normativo e il Vuoto Strumentale

Gli standard internazionali (ISO 31000, ISO 27000) e le linee guida governative (NIST) concordano unanimemente su un punto: la valutazione del rischio è uno step fondamentale per la gestione della sicurezza.

Tuttavia, esiste un paradosso fondamentale:

- Tutti indicano che il rischio vada valutato.
- Nessuno specifica come valutarlo o quale strumento implementare.

[*Nessuno ci dice: "il rischio va valutato usando questa tecnica".*]

La Proliferazione degli Strumenti e la Macro-Divisione

L’assenza di uno standard unico ha generato una ‘pletora di strumenti’. L’esistenza di centinaia di tool è la prova che nessuno di essi risolve il problema in modo assoluto.

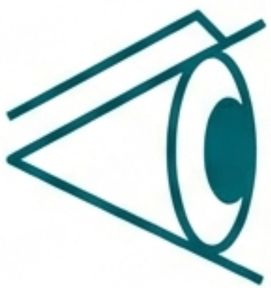
Una classificazione necessaria per ordinare il caos metodologico.

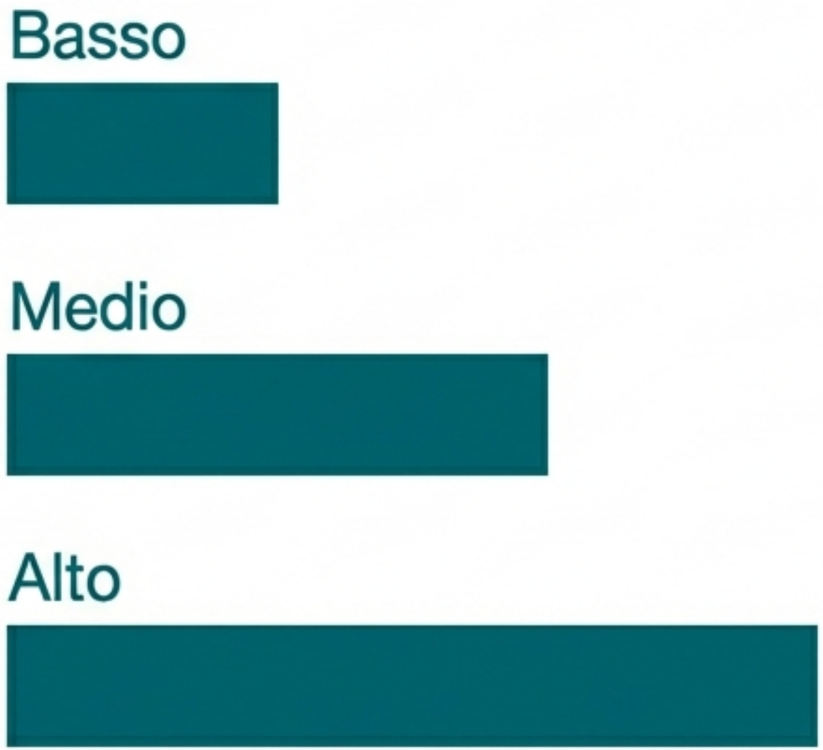
Metodi Qualitativi: Definizione e Meccanica

Approcci che utilizzano principi o regole basati su categorie descrittive o livelli livelli non numerici.

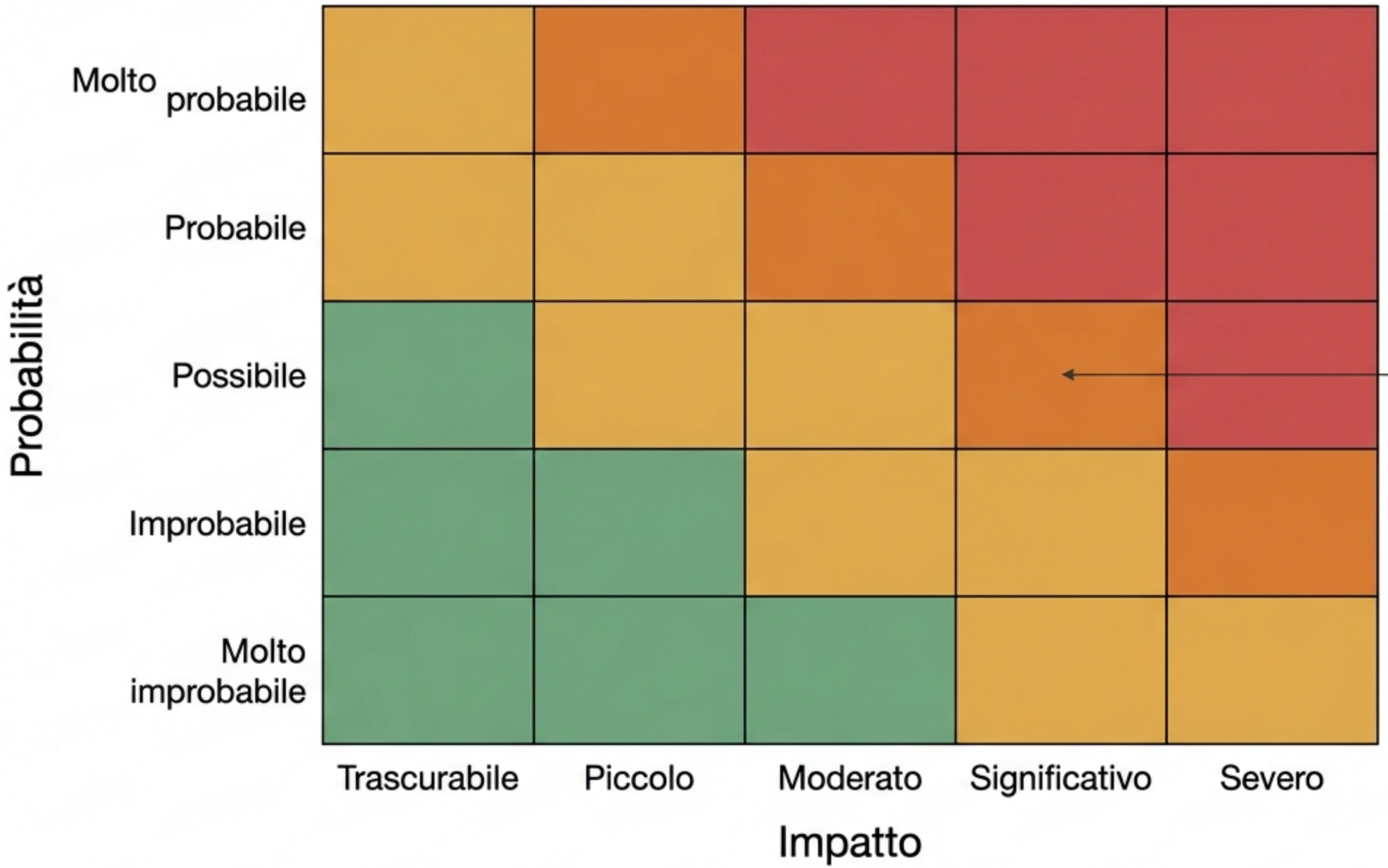
- **Input**: Non sono numeri fissi, ma valutazioni basate sull'osservazione.

- **Output**: Intervalli (range) o etichette categoriali (es. Basso, Medio, Alto).
- **Focus**: Identificazione rapida della situazione aziendale e delle aree di miglioramento.





L’Artefatto Qualitativo: La Matrice di Rischio



Impatto Visivo: 25 combinazioni che comunicano immediatamente la gravità della situazione.

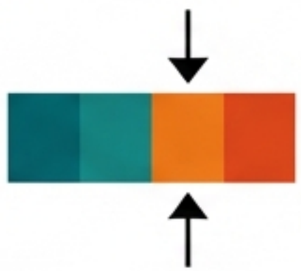
Esempio: Probabilità “Possibile” + Impatto “Significativo” = Rischio Medio-Alto (Arancio).

Analisi Critica: Efficienza contro Soggettività

I PRO: Efficienza

- **Tempi e Costi:** Molto efficienti. Non richiedono la stima di valori esatti.

- **Comunicazione:** L'output visivo (colori) è immediatamente comprensibile per il management.



I CONTRO: Soggettività

- **Irriproducibilità:** Esperti diversi possono produrre risultati diversi sullo stesso scenario.

- **Arbitrarietà:** Chi stabilisce che una certa combinazione sia "Arancio" invece che "Rosso"? La sensibilità dell'esperto altera il risultato.

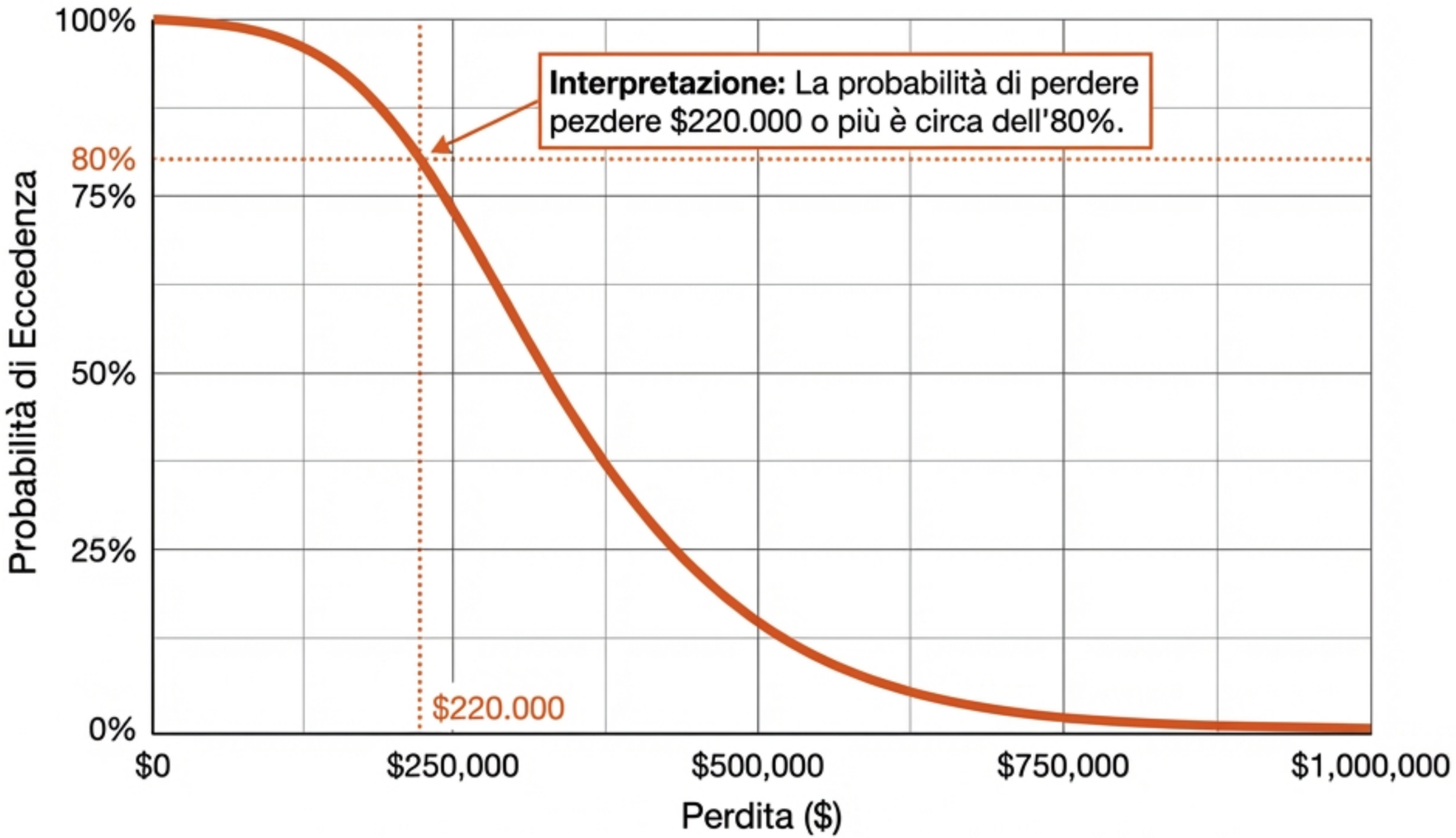
Conclusione: Il confronto tra risultati è complicato, se non impossibile.

Metodi Quantitativi: Definizione e Meccanica

Approcci che utilizzano modelli matematici per elaborare input numerici e produrre output numerici.

- **Input:** Dati statistici, valori monetari, frequenze.
- **Output:** Numeri puri (spesso valori monetari di perdita attesa).
- **Obiettivo:** Fornire stime rigorose, ripetibili e confrontabili oggettivamente.

L’Artefatto Quantitativo: La Curva di Perdita (LEC)



Loss Exceedance Curve (LEC): Cruda, numerica, ma confrontabile.

Analisi Critica: Rigore contro Complessità

I PRO: Rigore

- **Ripetibilità:** Dati gli stessi input, il modello restituisce lo stesso output.
- **Confrontabilità:** Permette confronti diretti e oggettivi tra diversi scenari di rischio.

I CONTRO: Costo e Complessità

- **Difficoltà di Stima:** È difficile assegnare un valore numerico unico a probabilità e impatti iniziali.
- **Interpretazione:** Richiede competenze avanzate per leggere i modelli matematici.
- **ROI:** I benefici dell'analisi potrebbero non bilanciare i costi elevati per implementare il modello.

La Zona Grigia: I Metodi Semi-Quantitativi

Un compromesso operativo tra le due metodologie maggiori.

1. Input Qualitativo

Scale e Intervalli

2. Trasformazione

Assegnazione numeri rappresentativi

3. Elaborazione

Algoritmi di Calcolo

La Trappola del Compromesso

I metodi semi-quantitativi rischiano di ereditare i Contro di entrambi gli approcci piuttosto che i Pro.

Input Soggettivi

Helvetica Neue Bold
Le scale di valutazione iniziali rimangono arbitrarie.

Falsa Oggettività

Trasformare un giudizio soggettivo in un numero non lo rende magico.

Output Confuso

Helvetica Neue Bold
Difficoltà nell'interpretare i risultati finali.

La Realtà Operativa: Il Mito del “Puro Quantitativo”

Esistono pochissimi metodi al 100% quantitativi. La valutazione del del rischio parte dalla postura dell’organizzazione, che è intrinsecamente qualitativa.

Facile da contare: PC con Antivirus

Impossibile da contare: Consapevolezza degli impiegati

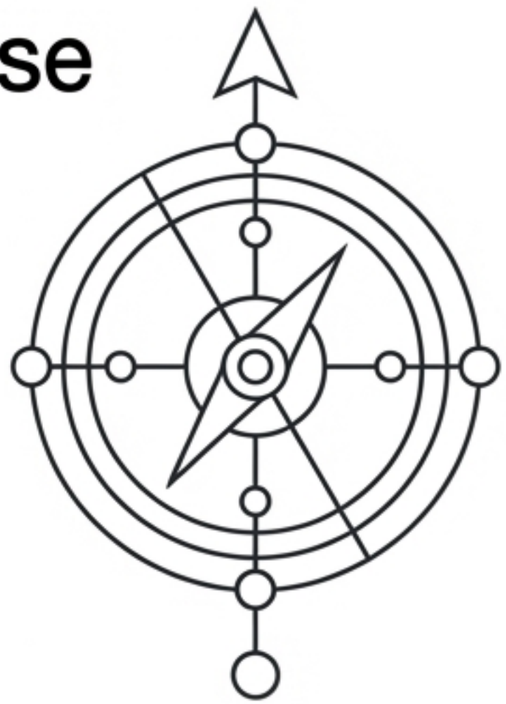
In tutti i metodi quantitativi c’è sempre un pizzico di qualitatività.

Sintesi Comparativa delle Metodologie

Caratteristica	Qualitativo	Semi-Quantitativo	Quantitativo
Input	Categorie / Intervalli	Qualitativo → Numerico	Dati Numerici / Statistici
Input	Categorie / Intervalli	Qualitativo → Numerico	Dati Numerici / Statistici
Output	Matrice di Rischio	Indici Numerici	Curva di Perdita (LEC)
Punto di Forza	Efficienza, Impatto Visivo	Compromesso	Rigore, Ripetibilità
Punto Debole	Soggettività	Ereditarietà dei difetti	Costo, Complessità

Conclusioni e Prospettive

1. Nessuno strumento risolve il problema in in assoluto. La scelta dipende dalle risorse e dagli obiettivi dell'organizzazione.
2. La soggettività è il nemico principale della riproducibilità.
3. Diffidare della falsa precisione matematica se i dati di input (come la consapevolezza umana) non sono solidi.



Riferimenti Bibliografici e Normativi

- ISO 31000 – Risk Management
- ISO/IEC 27000 Series – Information Security Management
- NIST – Guide for Conducting Risk Assessments