Risk Assessment: Metodologie e Framework per lo Spazio Cyber

Modulo 5: Analisi dei processi NIST 800-30r1 e metriche di valutazione

Il Contesto nel Ciclo di Gestione del Rischio

Riferimento ISO 31000 (2018):
Il Risk Assessment non è un'attività isolata, ma costituisce il secondo step fondamentale della procedura di gestione del rischio.

Obiettivo:
Trasformare l'incertezza in dati analizzabili per supportare il processo decisionale.

I Limiti della Misurazione nello Spazio Cyber

Imprecisione Strumentale

A differenza delle scienze fisiche, il Risk Assessment cyber Atsssessment cyber non dispone di strumenti di misurazione assoluta. Non esiste un “righello” per il rischio digitale.

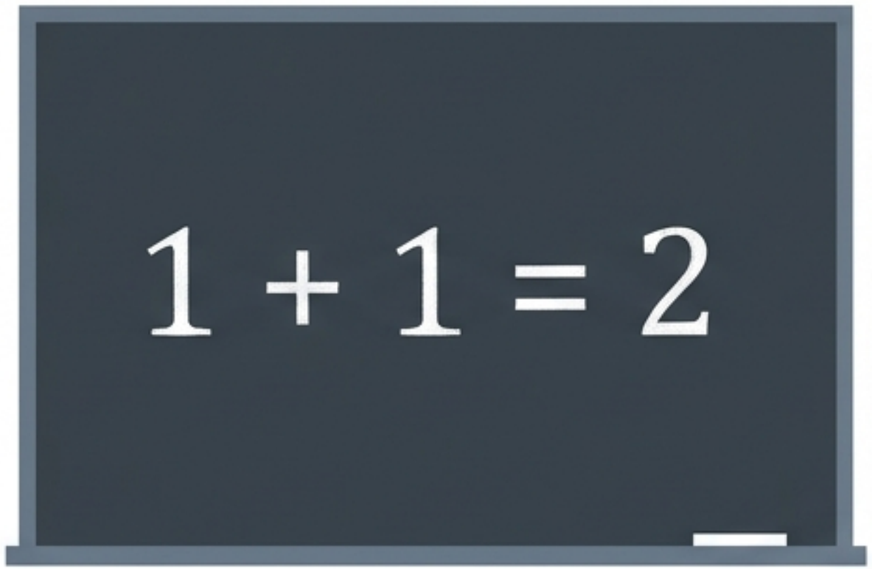
Soggettività dell’Esperto

Esperti diversi con background differenti possono produrre output divergenti per la stessa organizzazione.
L’interpretazione è legata alla sensibilità del valutatore.

Qualità del Dato

- Dati scarsi (specifici dell’organizzazione)
- Dati non strutturati (troppo rumore informativo da organizzazioni affini).

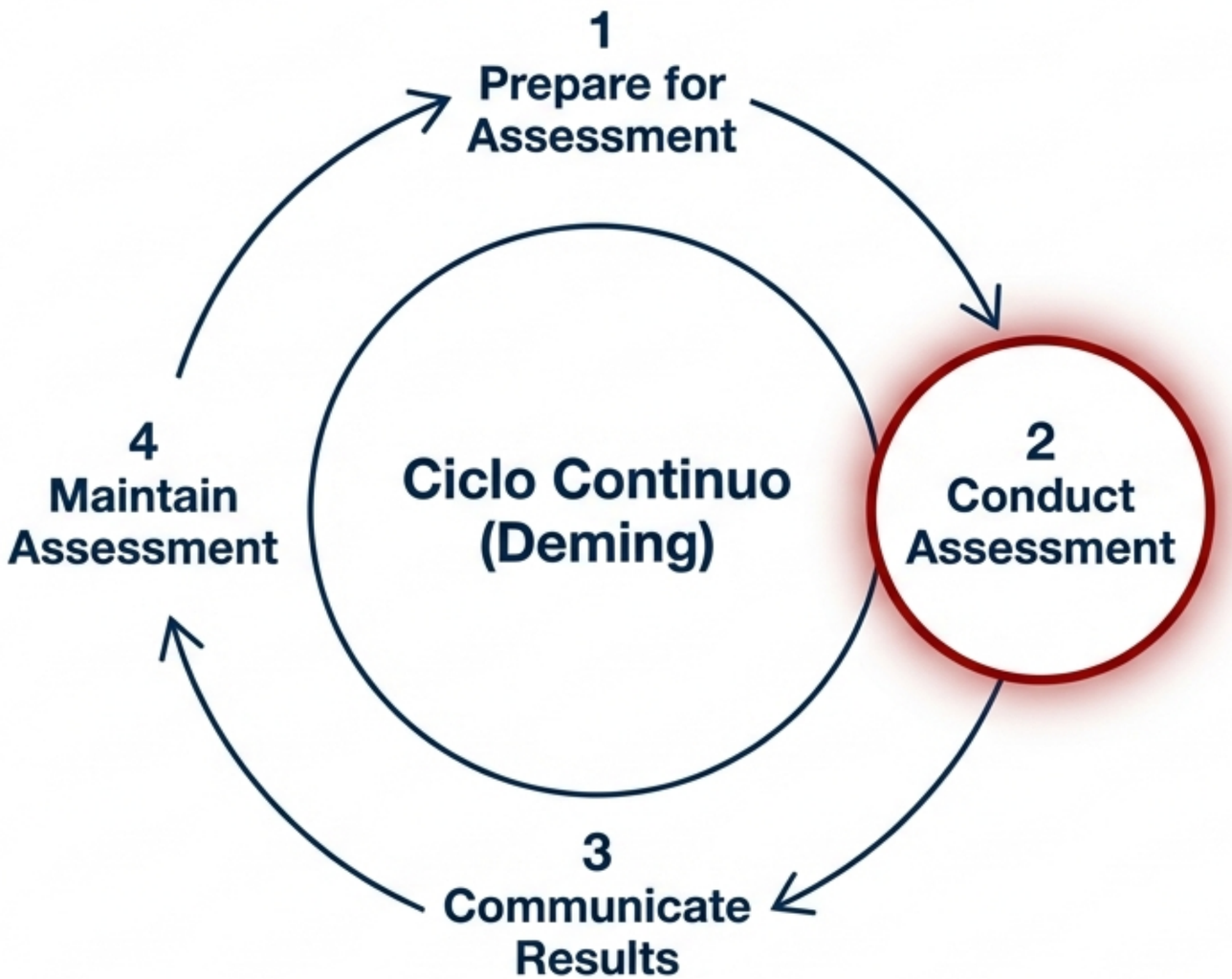
Ambiguità nell'Analisi Qualitativa

	Basso - Medio - Alto
Certezze Quantitative	Categorie Qualitative

Il Paradosso Matematico: Mentre la matematica è univoca, i metodi qualitativi producono categorie non numeriche soggette a interpretazione.

Il Fattore Umano: L'assessment dipende da individui con competenze eterogenee. Un rischio 'Medio' per un esperto potrebbe essere 'Alto' per un altro.

Lo Standard di Riferimento: NIST SP 800-30r1



Definizione: Valutare il rischio significa analizzare minacce e vulnerabilità per determinarne probabilità e impatto.

Continuità: Il processo non termina con l'assessment; deve essere aggiornato ciclicamente (Step 4).

Step 1: Identificazione delle Minacce

La causa scatenante di un evento negativo.

Minacce Esterne (Prevalenti / Non Controllabili)

Eventi indipendenti dalla volontà dell'organizzazione.

- Sviluppo di nuovi Ransomware
- Campagne di Phishing massive
- Evoluzione delle tecniche di attacco (AI)

Minacce Interne (Sporadiche)

Eventi legati al perimetro organizzativo.

- Dipendenti scontenti
- Furto di dati
- Sabotaggio

Step 2: Identificazione delle Vulnerabilità

Definizione: Debolezza interna all'infrastruttura tecnologica che una minaccia può sfruttare per penetrare il sistema.

Fattore di Controllo: A differenza delle minacce, le vulnerabilità sono **controllabili** e **interne**.

Mitigazione Attiva:

- *Tecnologica:* Installazione Firewall, patch management, aggiornamento Antivirus.
- *Umana:* Formazione del personale contro il social engineering.

"Non possiamo impedire a un attaccante di scrivere un malware, ma possiamo chiudere la falla che userebbe per entrare."

Step 3 & 4: Stima dei Parametri

Step 3: Determinazione della Probabilità

Stima della possibilità che una minaccia sfrutti una vulnerabilità.

- **Vincolo:** La stima deve riferirsi a un **periodo finito** (es. 6 mesi, 1 anno).

Step 4: Determinazione dell'Impatto

Stima dell'entità delle conseguenze se l'evento si verifica.

- **Metrica:** Espressa in termini **economici/monetari**.

Step 5: La Determinazione del Rischio

$$R = P \times I$$

Valore Dimensionale (€)
Perdita economica attesa

Adimensionale
Numero puro (0 → 1)

Valore Dimensionale (€)
Danno monetario

Il rischio rappresenta una perdita economica attesa, pesata dalla probabilità di accadimento.

Analisi delle Variabili: Il Peso dell'Impatto

$$0 \leq P \leq 1$$

La Probabilità è limitata all'unità.

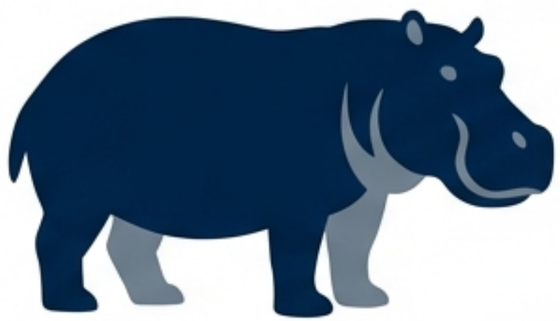
Conseguenza Matematica:

Quantitativamente, la variabile dell'impatto influenza il risultato finale molto più della probabilità. Per questo motivo, il Rischio viene spesso definito informalmente come "il cugino dell'Impatto'.

$$0 \leq I \leq \infty$$

L'Impatto è potenzialmente illimitato.

Casi Limite e Paradossi del Rischio



L’Ippopotamo

Scenario: Incontro per strada.

Impatto: **Altissimo** (Mortale).

Probabilità: ≈ 0.

RISULTATO: Rischio Basso

Lo Spazzolino

Scenario: Contrarre malattia lavandosi i denti.

Impatto: **Irrilevante** (Basso).

Probabilità: ≈ 1 (Uso quotidiano).

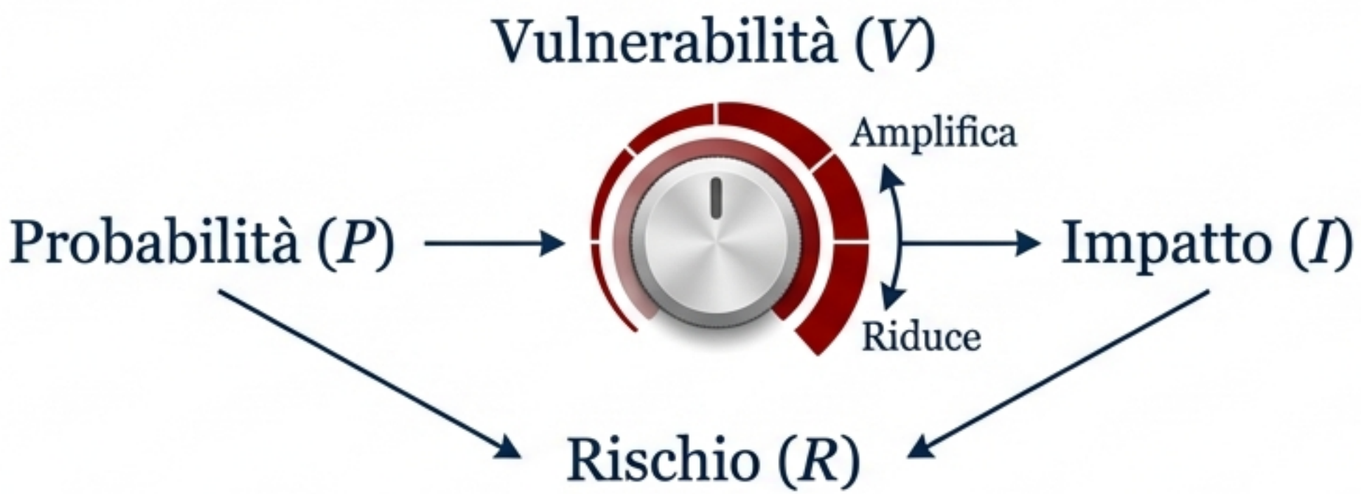
RISULTATO: Rischio Basso

Il rischio è elevato solo quando entrambe le variabili sono significative.

Formulazioni Complesse e Fattori di Peso

Oltre la semplice moltiplicazione ($P \times I$), esistono modelli che integrano la **Vulnerabilità** (V) come variabile indipendente.

$$R = f(P, I, V)$$



Ruolo della Vulnerabilità:

Agisce come un 'fattore di peso' che può amplificare o ridurre il rischio calcolato, basandosi sull'effettiva esposizione del sistema a quella specifica minaccia.

Standardizzazione: Common Vulnerability Scoring System (CVSS)

Obiettivo: Ridurre la soggettività assegnando punteggi oggettivi alle vulnerabilità note.
Utilizzo: Fornisce un linguaggio comune standardizzato per classificare la severità dei punti deboli.

Sintesi del Modulo

1. **Natura dell'Assessment:** Un processo soggettivo ma strutturato (NIST 800-30r1) necessario per gestire l'incertezza.
2. **Dinamica delle Variabili:** Le minacce sono spesso esterne/incontrollabili; le vulnerabilità sono interne/controllabili.
3. **Il Calcolo:** Il modello $R = P \times I$ trasforma stime qualitative in valori economici, dove l'impatto gioca il ruolo matematico preponderante.
4. **Obiettivo Finale:** Utilizzare standard come CVSS e framework metodologici per rendere il rischio misurabile e gestibile.

Riferimenti e Bibliografia

- **NIST SP 800-30r1**
  Guide for Conducting Risk Assessments - National Institute of Standards and Technology.
- **ISO 31000:2018**
  Risk Management — Guidelines - International Organization for Standardization.
- **CVSS Standards**
  Common Vulnerability Scoring System - FIRST.org.