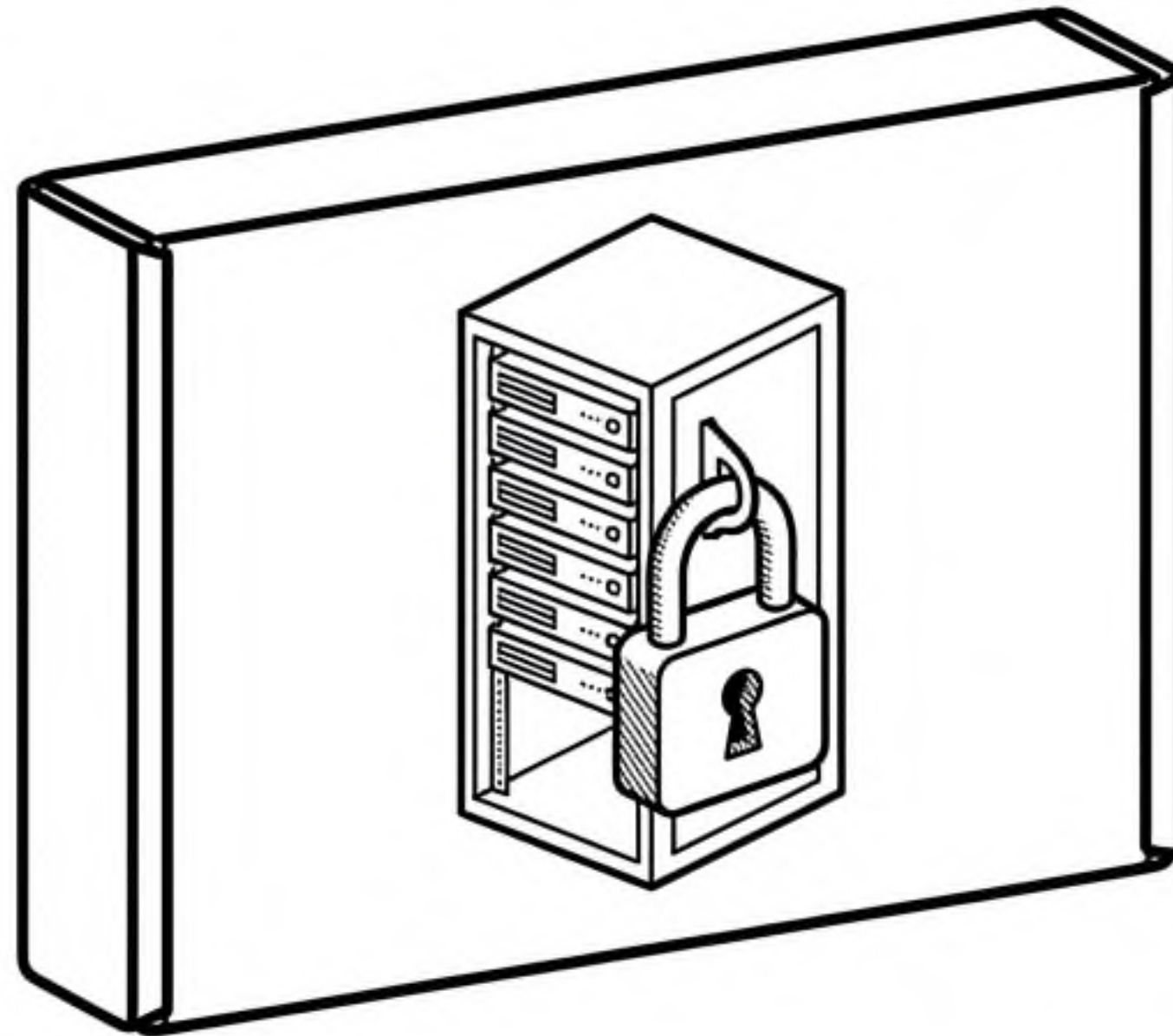


SÄKERHET

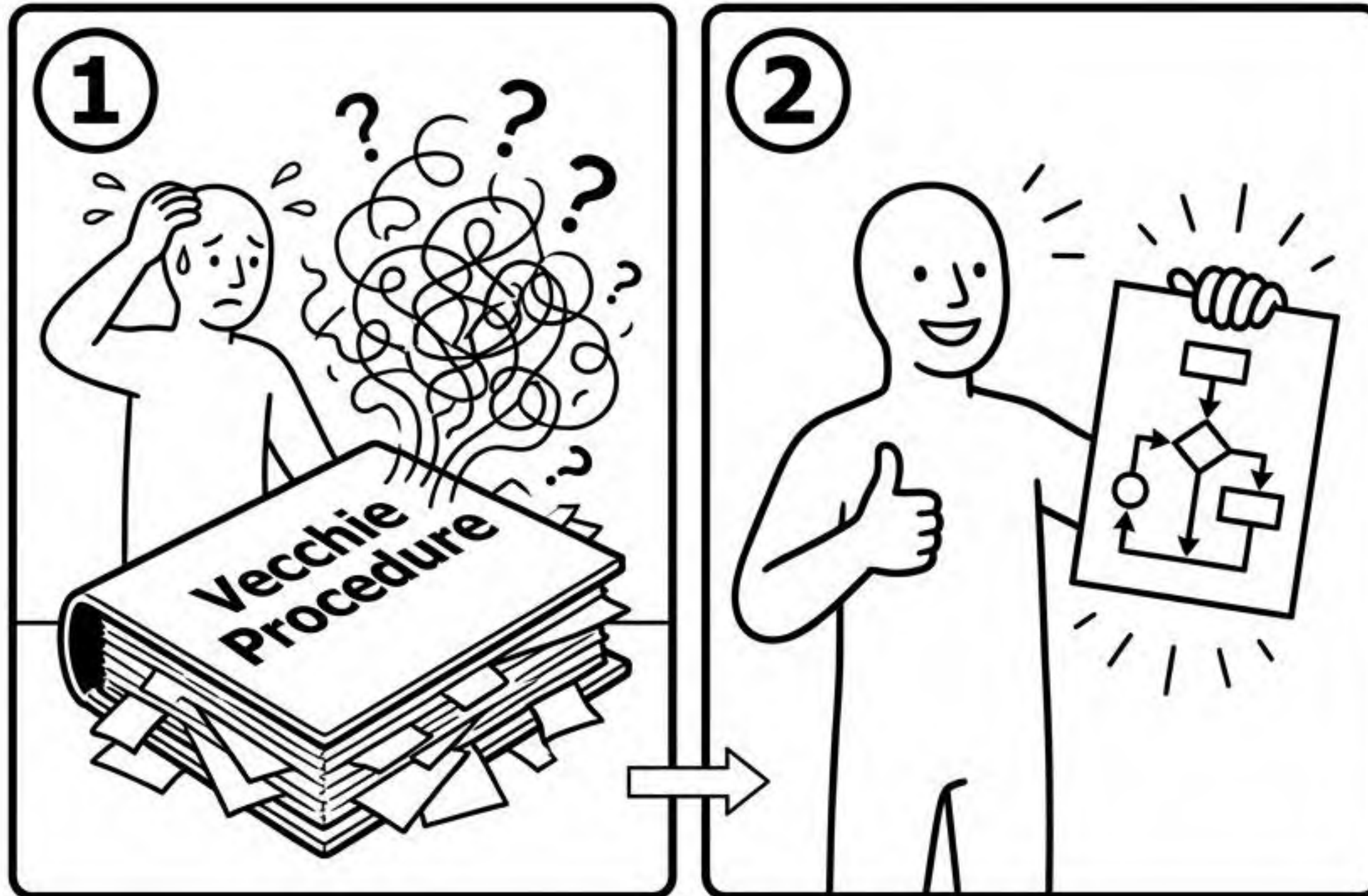
Manuale di Istruzioni per l'Assemblaggio: Sicurezza delle Informazioni



Design by Cesare Galletti (con contributi di Massimo Cottafavi e Stefano Ramacciotti)
Versione Gennaio 2026 (ISO/IEC 27001 Edition)



Importanti Avvertenze: La Semplicità è Sicurezza

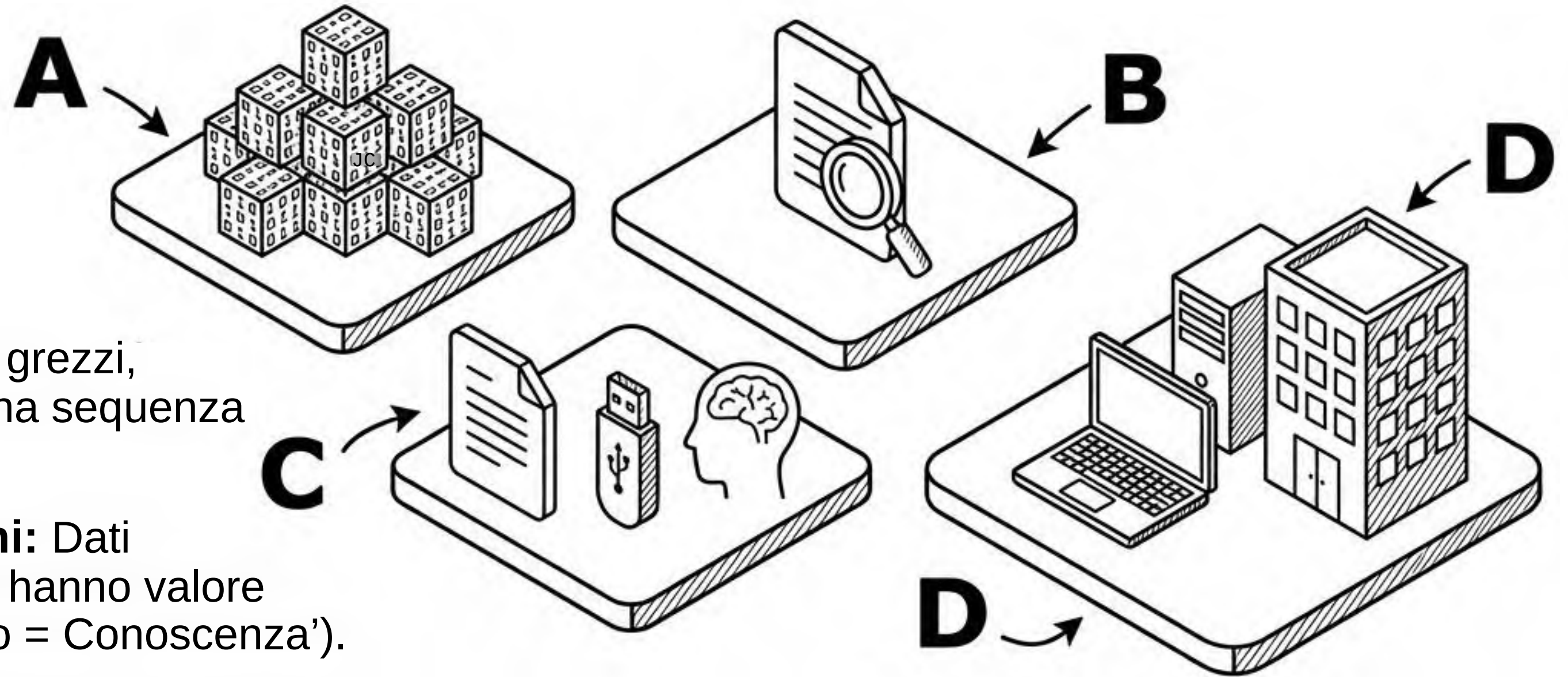


«Le istruzioni di IKEA, anche se costituite soprattutto da disegni... sono ottimi esempi di come scrivere procedure.»

(Fonte: Cesare Callotti, Sez. 12.1.2)

- Le procedure devono essere chiare, precise e sintetiche.
- Evitare la complessità inutile: la sicurezza non è burocrazia.
- Obiettivo: Usabilità per tutti gli operatori.

Inventario dei Componenti (Sez. 2.1 e 6.1)



A - I Dati: Elementi grezzi, numeri o fatti (es. una sequenza di bit).

B - Le Informazioni: Dati contestualizzati che hanno valore (es. 'Dati + Contesto = Conoscenza').

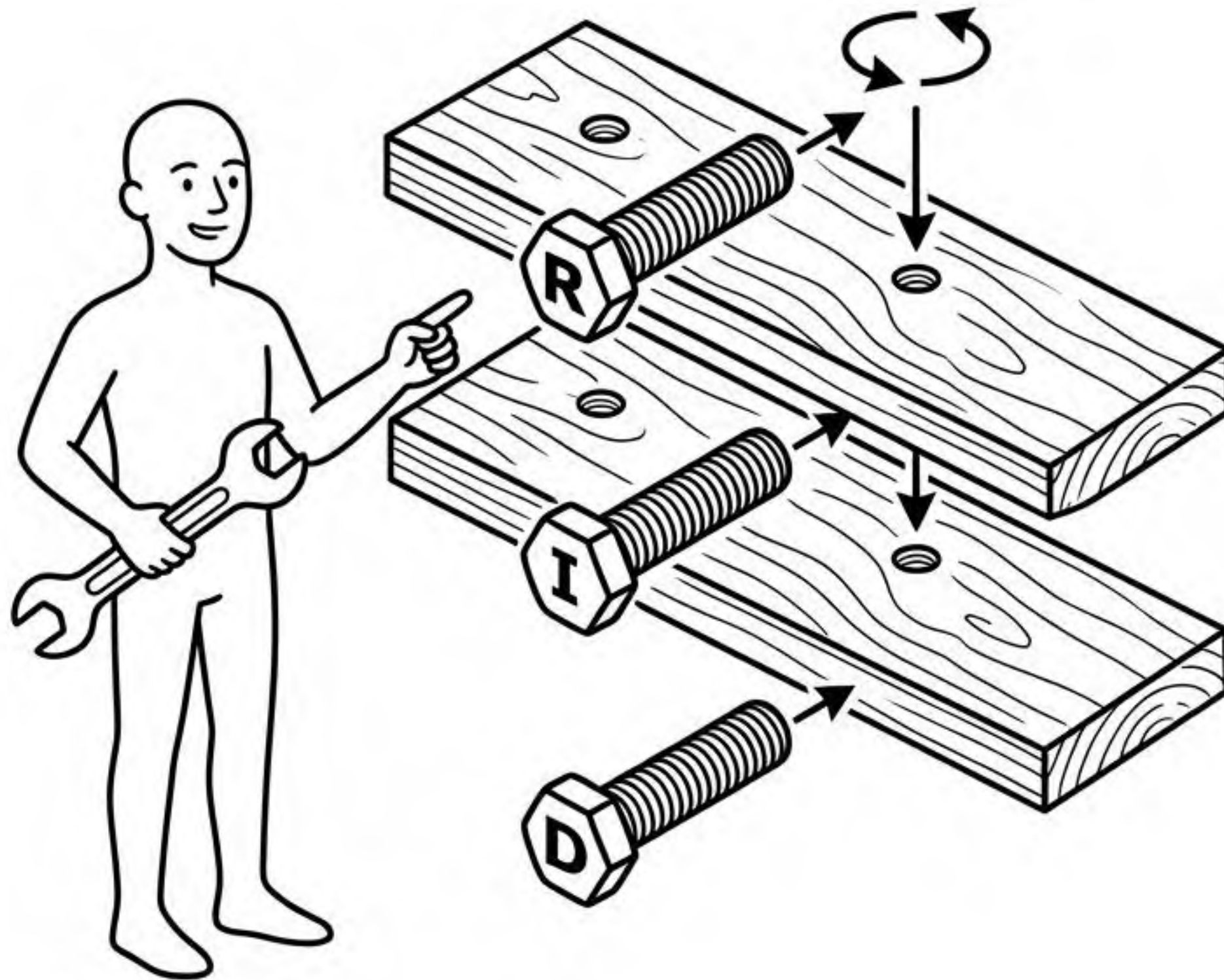
C - I Supporti: Dove risiede l'informazione (Carta, Digitale, La mente umana).

D - Gli Asset: Qualsiasi cosa abbia valore per l'organizzazione.



Attenzione: La sicurezza non riguarda solo l'informatica (IT), ma tutte le forme in cui le informazioni sono create, conservate e trasmesse.

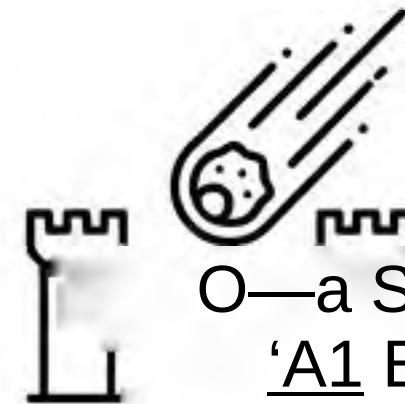
Specifiche di Integrità Strutturale: I Parametri RID



R - Riservatezza (Confidentiality):
L'informazione è accessibile solo a chi è autorizzato (Need to know).

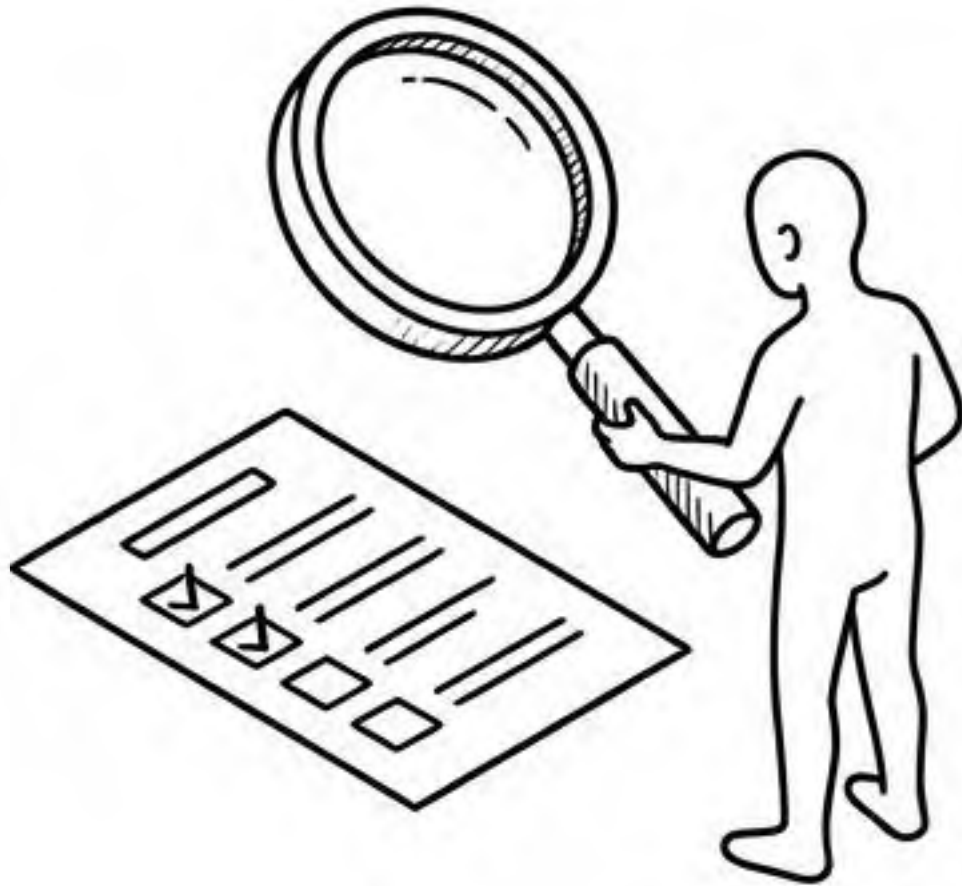
I - Integrità (Integrity):
Accuratezza e completezza. I dati non sono stati alterati.

D - Disponibilità (Availability):
Accessibile e utilizzabile entro i tempi previsti.



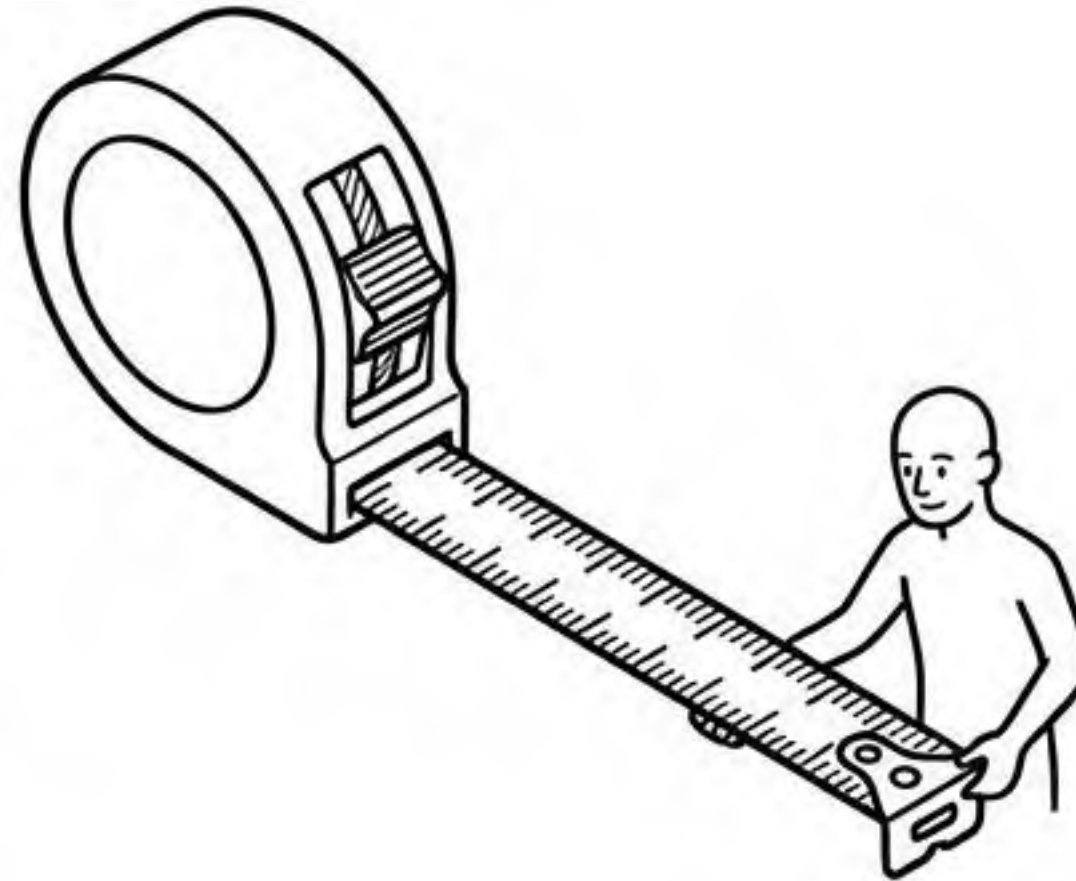
O—a Sicurezza assoluta non esiste.
'A1 Esiste solo il rischio gestito.

Strumenti Necessari: Valutazione del Rischio (Cap. 4 e 7)



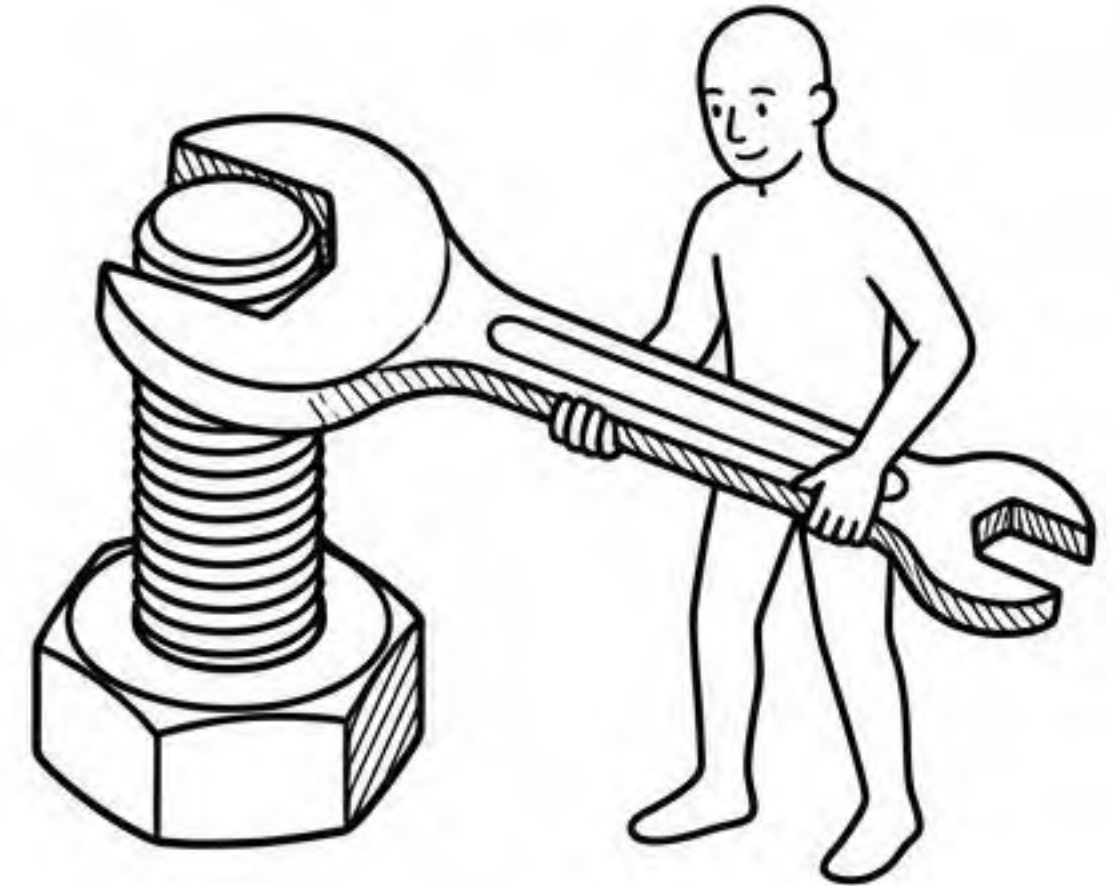
Tool 1: Identificazione

Individuare Asset,
Minacce e Vulnerabilità.



Tool 2: Analisi (La Misurazione)

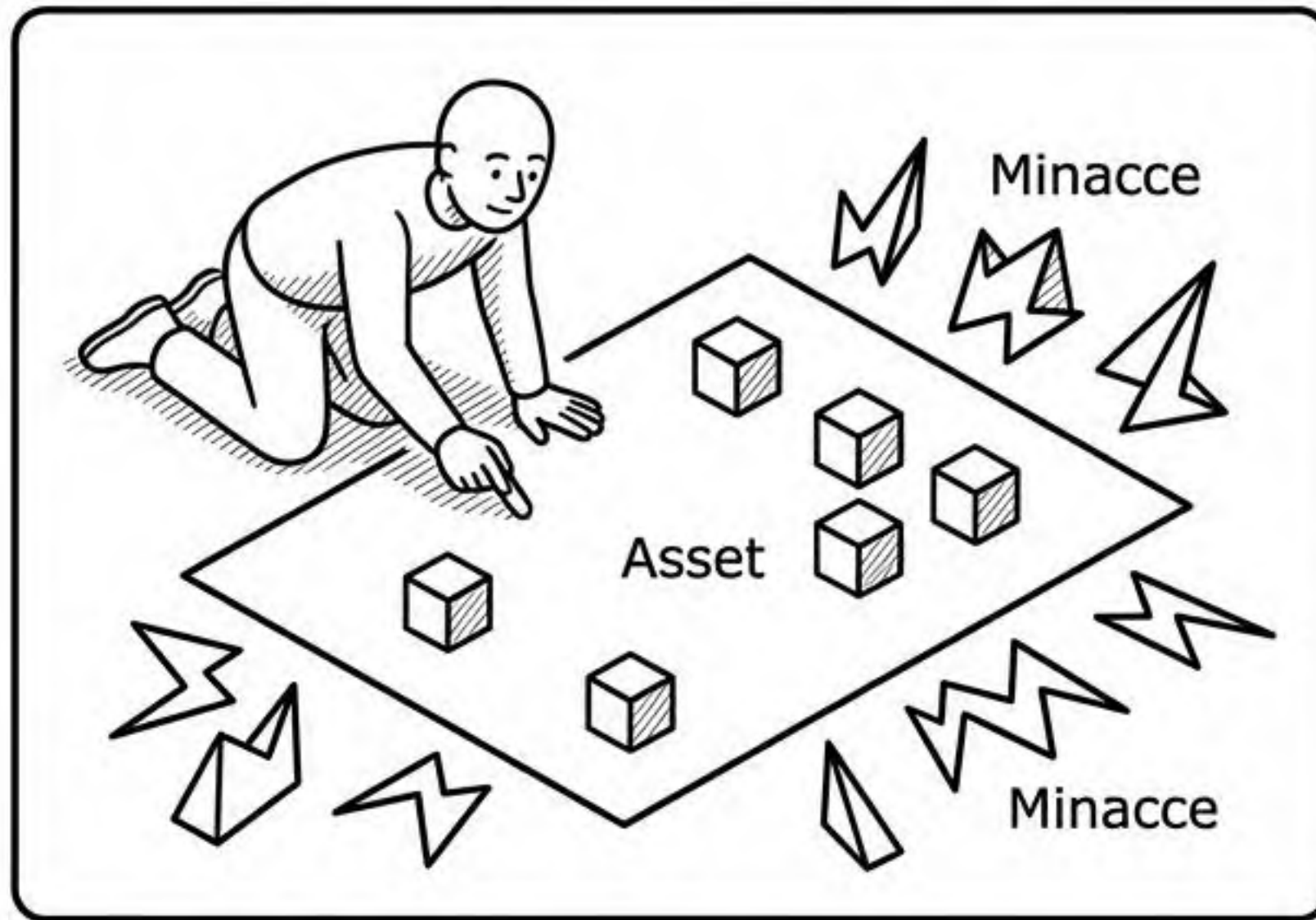
Formula: $\text{Rischio} = \text{Probabilità} \times \text{Impatto}$.
Stimare le conseguenze
sui parametri RID.



Tool 3: Trattamento (L'Azione)

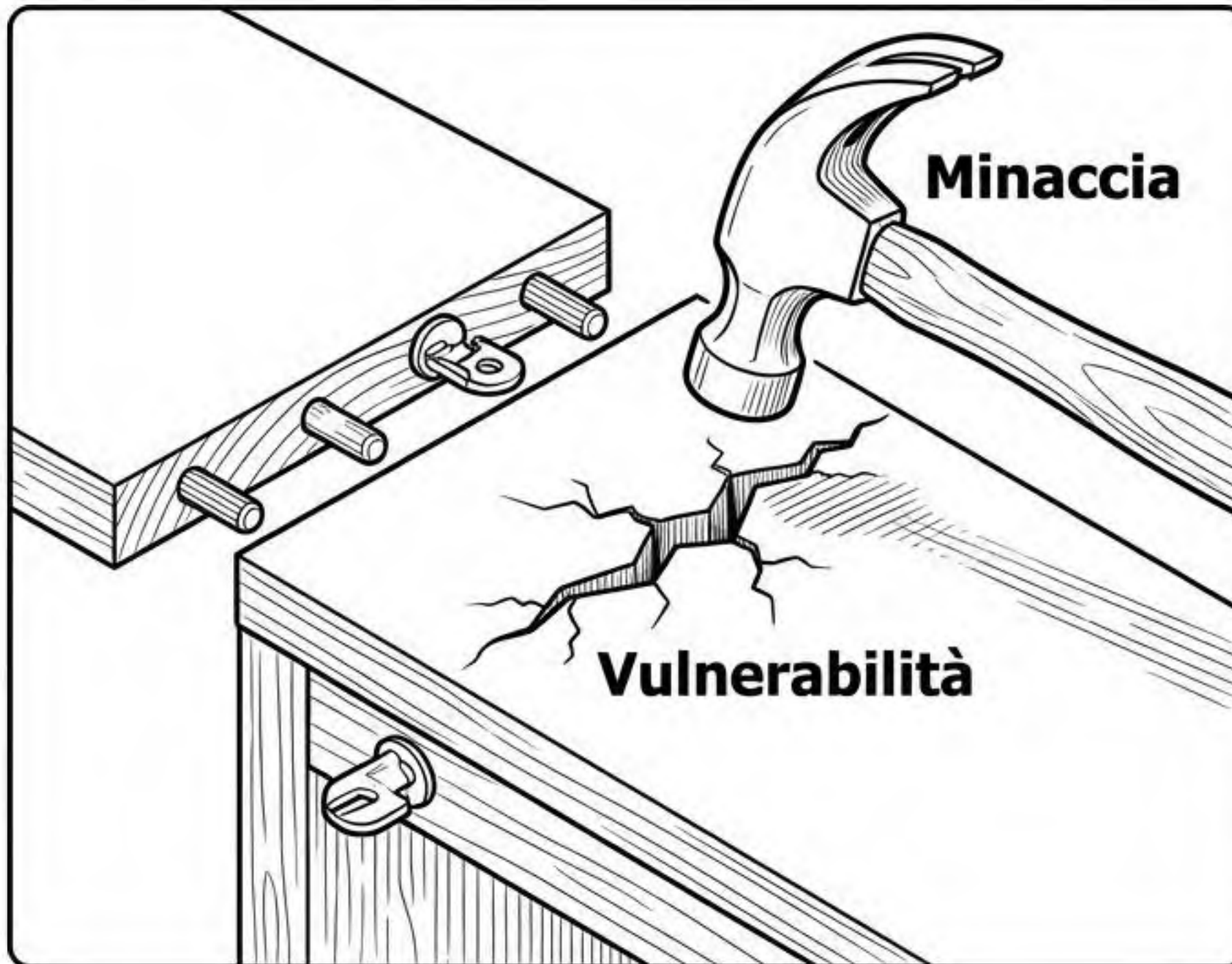
- Evitare (Eliminare la fonte)
- Modificare (Ridurre probabilità o impatto)
- Condividere (Assicurazioni)
- Accettare (Decisione consapevole)

Passo 1: Definire il Perimetro (Contesto e Ambito)



1. Contesto Interno ed Esterno: Dove operiamo?
2. Parti Interessate: Cosa si aspettano Clienti, Fornitori e Leggi?
3. L'Ambito (Scope): Cosa è incluso nel Sistema?

Passo 2: Analisi dei Punti Deboli



- **Minaccia (Threat):** Causa potenziale di incidente (es. Hacker, Incendio, Errore umano).
- **Vulnerabilità:** Debolezza che può essere sfruttata (es. Software non aggiornato, Porta aperta).
- **Il Rischio:** Quando una Minaccia incontra una Vulnerabilità.



- Umane: Errori, ingegneria sociale.

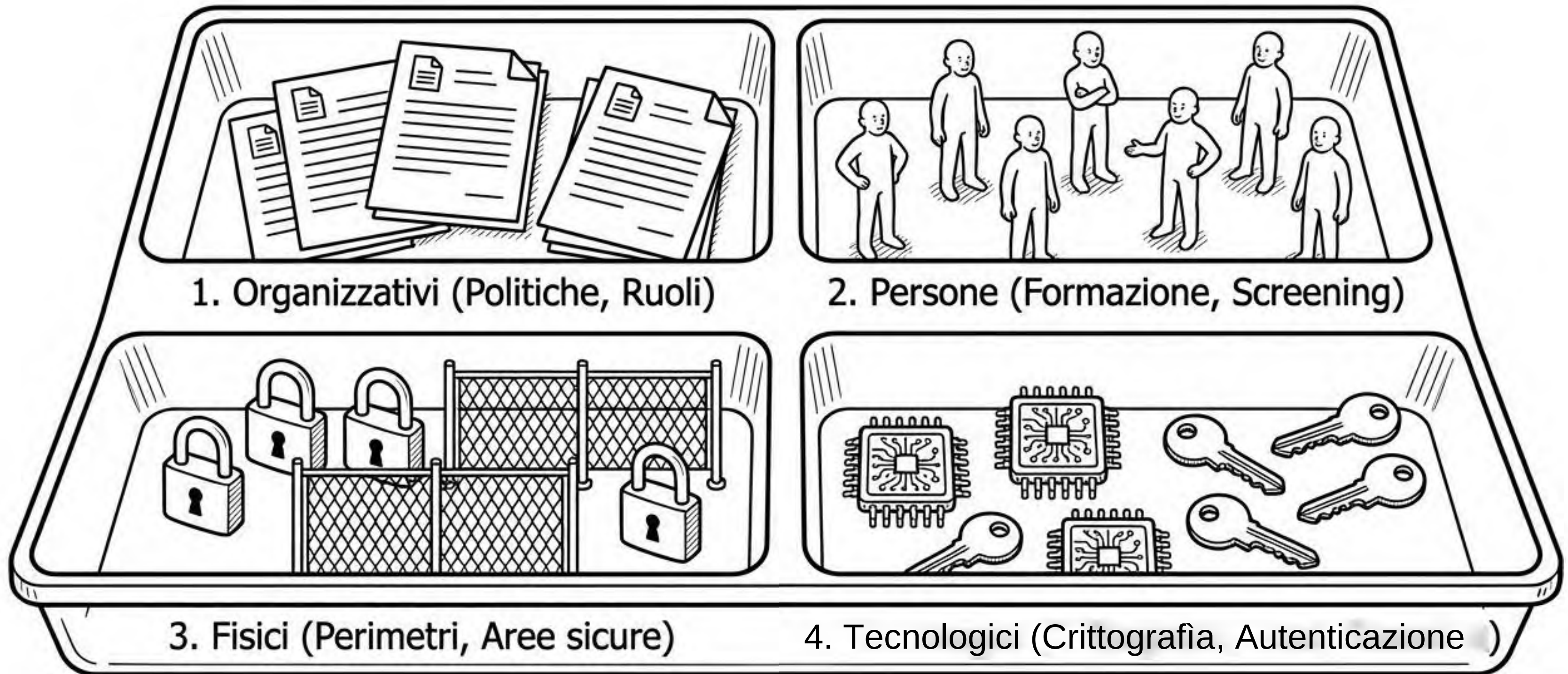


- Tecnologiche: Malware, guasti.



- Fisiche: Incendi, allagamenti.

Passo 3:1 Controlli di Sicurezza (ISO/IEC 27002:2022)



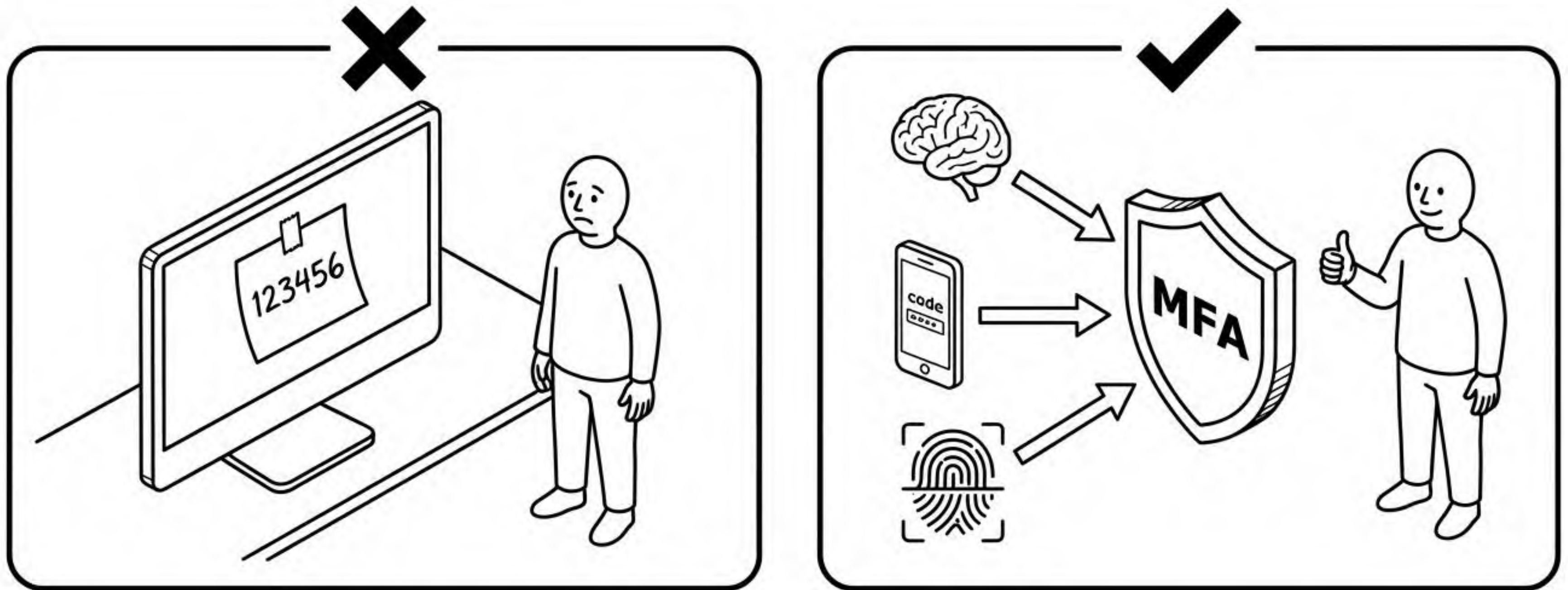
Obiettivo: Minimizzare il rischio a un livello accettabile stringendo le viti giuste.

Dettaglio Montaggio: Sicurezza Fisica



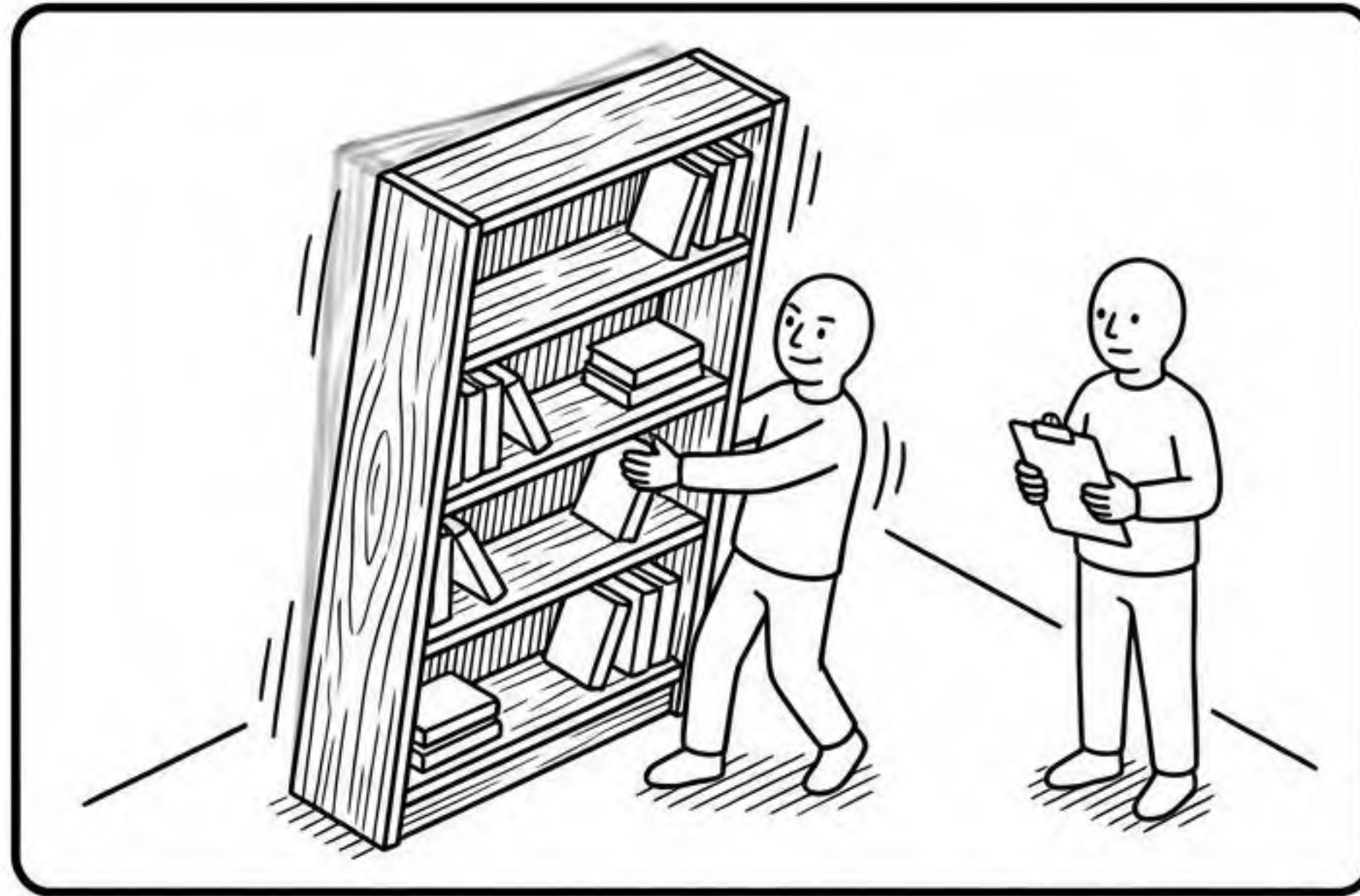
- Chiudere a chiave gli archivi riservati.
- Mai lasciare estranei non accompagnati (Tailgating).
- Proteggere i dispositivi fuori sede.

Dettaglio Montaggio: Sicurezza Logica



- Identificazione vs Autenticazione: 'Chi sei' vs 'Provalo'.
- MFA (Autenticazione Forte): Qualcosa che sai + Qualcosa che hai + Qualcosa che sei.
- Principio del Privilegio Minimo: Dare solo gli accessi strettamente necessari.

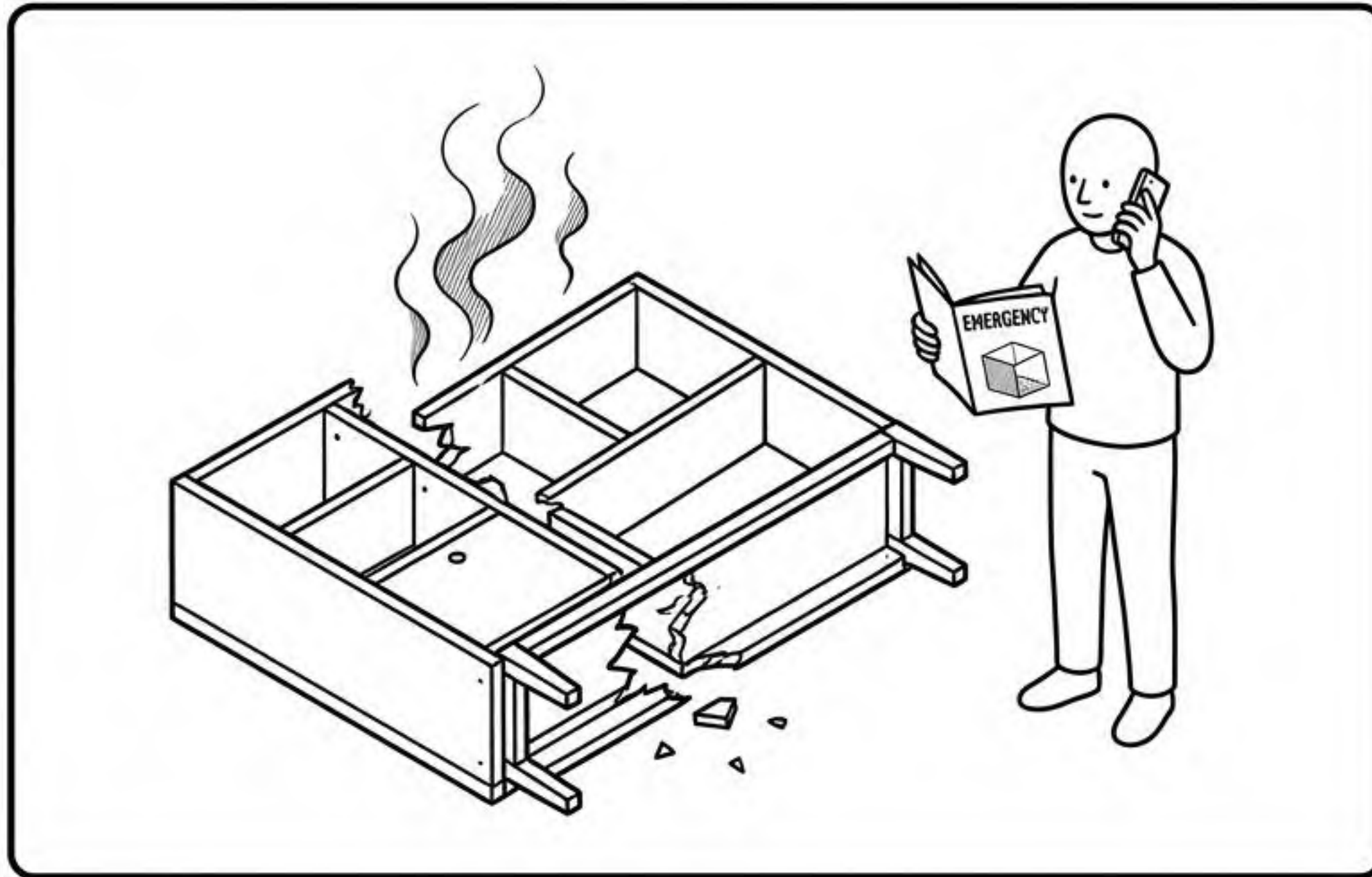
Verifica di Stabilità: Monitoraggio e Audit



1. Audit Interno: Verificare che le procedure siano rispettate (Regole interne + Norma).
2. L'Auditor: Trattare con trasparenza (Ospite, Partner o Ispettore).
3. Riesame della Direzione: Il management conferma che il sistema è efficace.

Non si può gestire ciò che non si misura.

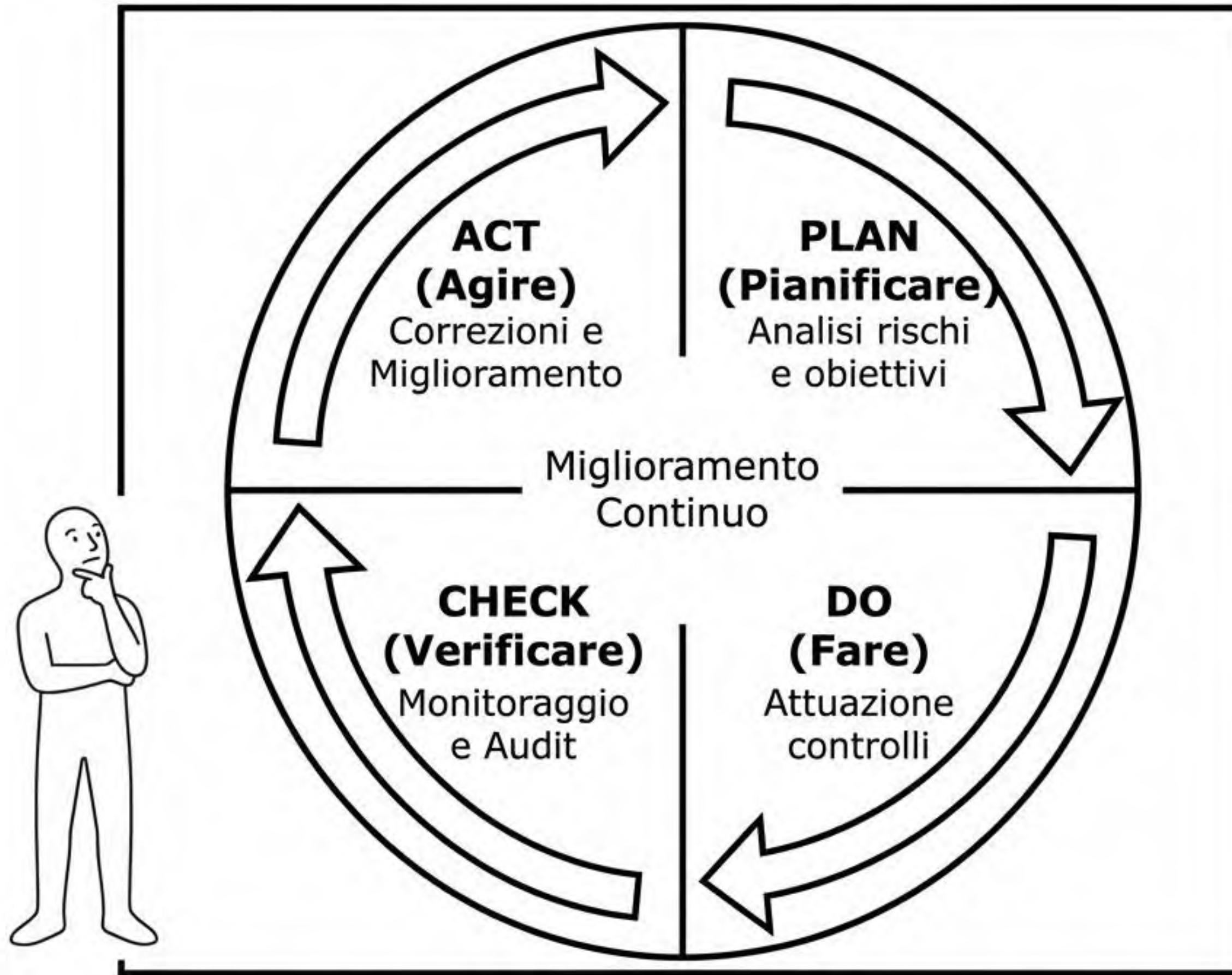
Risoluzione Problemi: Gestione Incidenti



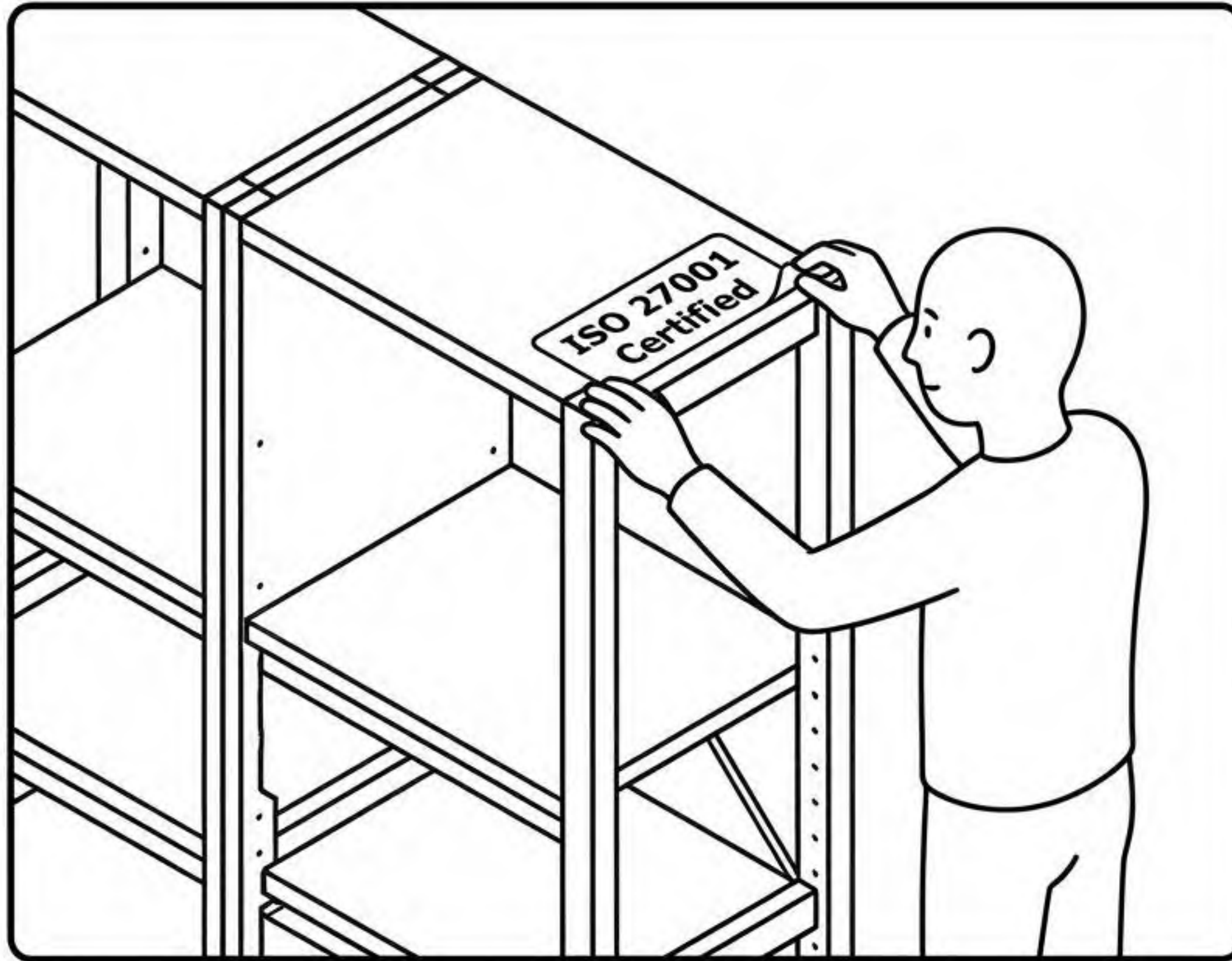
1. Rilevazione: Falso allarme o incidente reale?
- © Contenimento: Fermare l'emorragia.
3. Eradicazione e Recupero: Rimuovere la causa e ripristinare i dati.
- © Lezioni Apprese: Capire le cause (5 Whys) per evitare che ricada.

Non nascondere gli incidenti. Segnarli tempestivamente.

Ciclo di Manutenzione: PDCA (Miglioramento Continuo)



Il Sigillo di Qualità: La Certificazione



- Atto volontario che crea fiducia (Trust) con clienti e partner.
- Richiede un Auditor Esterno accreditato.
- Non garantisce l'impenetrabilità, ma dimostra una gestione strutturata e conforme dei rischi.

Godetevi il Vostro Prodotto



La sicurezza non è un prodotto che si compra, ma un processo che si vive.
Mantenete aggiornato il vostro manuale.