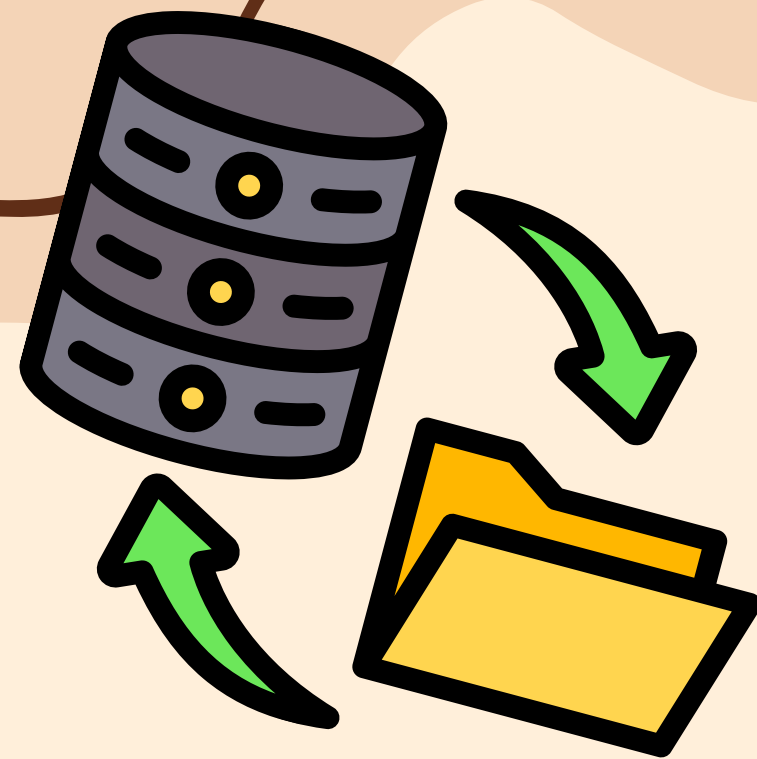


TIPI DI BACKUP

Corso Tecnico Software
2024/2025



INTRODUZIONE

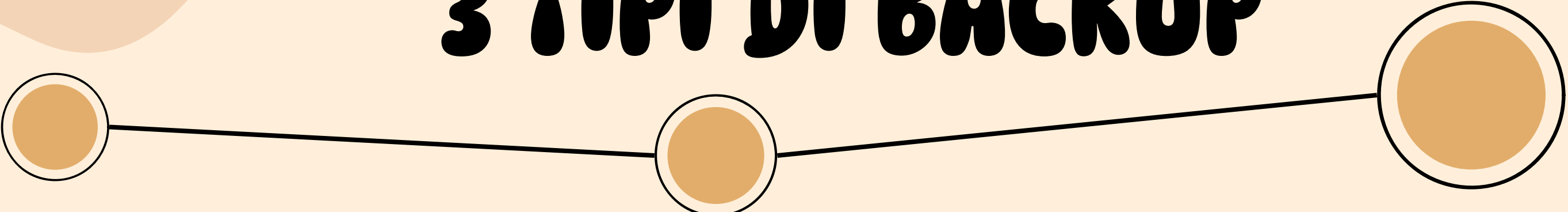
La perdita di dati rappresenta una delle sfide più critiche per aziende e individui. Può derivare da guasti hardware, attacchi informatici, errori umani o eventi catastrofici, con conseguenze economiche e operative significative.

Un backup efficace non è solo una misura di protezione, ma un requisito essenziale per garantire la continuità operativa. Il recupero dati, d'altra parte, consente di ripristinare rapidamente le informazioni perdute, minimizzando i tempi di inattività e i danni.

1. TIPI DI BACKUP

Per garantire la protezione ottimale dei dati, è importante conoscere le diverse modalità di backup disponibili e scegliere quella più adatta alle proprie esigenze.

3 TIPI DI BACKUP



COMPLETO

Un backup completo copia tutti i dati selezionati ogni volta che viene eseguito. Vantaggi:

- Copertura completa dei dati.
- Semplicità di ripristino, in quanto i file sono contenuti in un'unica copia completa.

Svantaggi:

- Richiede molto tempo e spazio di archiviazione.
- Può risultare inefficiente se eseguito frequentemente.

INCREMENTALE

Il backup incrementale salva solo i dati modificati o aggiunti dall'ultimo backup (sia completo che incrementale).

Vantaggi:

- Utilizza meno spazio di archiviazione rispetto al backup completo.
 - Più veloce da eseguire dopo il primo backup completo.
- Svantaggi:
- Ripristinare i dati richiede la combinazione del backup completo iniziale e di tutti gli incrementi successivi.
 - Maggiore complessità nei processi di recupero.

DIFFERENZIALE

Un backup differenziale copia i dati modificati dall'ultimo backup completo.

Vantaggi:

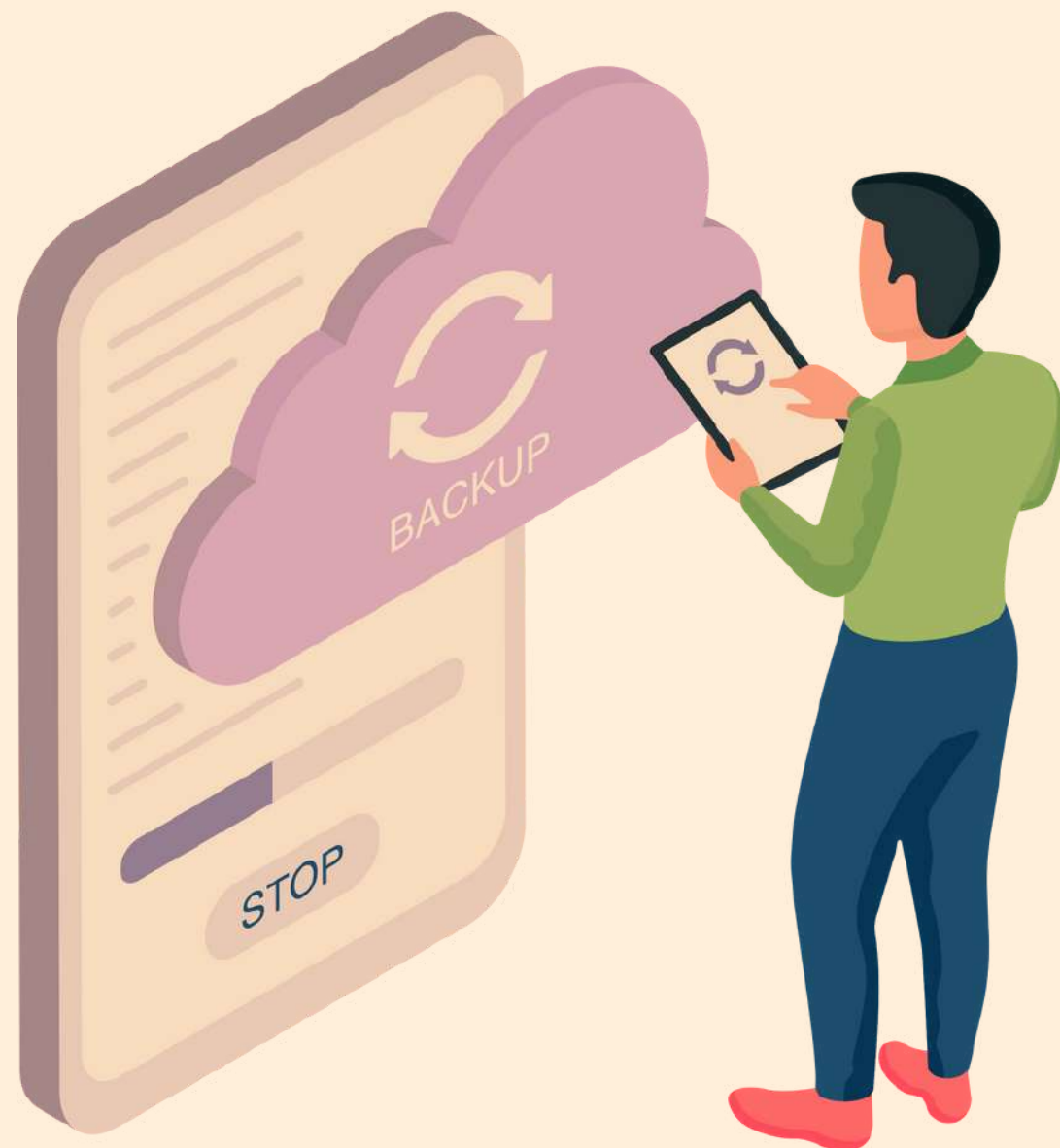
- Più rapido del backup completo.
 - Più semplice da ripristinare rispetto a un backup incrementale.
- Svantaggi:
- Con il tempo, può richiedere più spazio di archiviazione rispetto al backup incrementale.

2. STRUMENTI E TECNOLOGIE

Per eseguire backup e recupero dati in modo efficace, è essenziale scegliere gli strumenti e le tecnologie più adatti alle proprie esigenze. Questa sezione esplora le principali opzioni disponibili.



SOFTWARE DI BACKUP



I software di backup consentono di automatizzare, pianificare e monitorare i processi di copia dei dati. Alcuni dei più diffusi sono:

- Acronis Cyber Protect**
- Veeam Backup & Replication**
- EaseUS Todo Backup**
- Bacula**
- Duplicati**

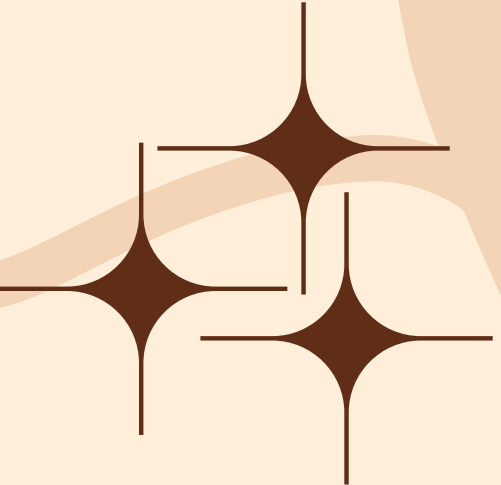
SOLUZIONI CLOUD VS ON- PREMISES

- **Backup Cloud:** I dati sono archiviati su server remoti accessibili tramite internet.
- **Backup On-Premises:** I dati vengono archiviati localmente su dispositivi fisici come NAS o server locali.



HARDWARE PER IL BACKUP

Hard Disk Esterni, NAS, Tape Drive e SSD sono le principali soluzioni di archiviazione.



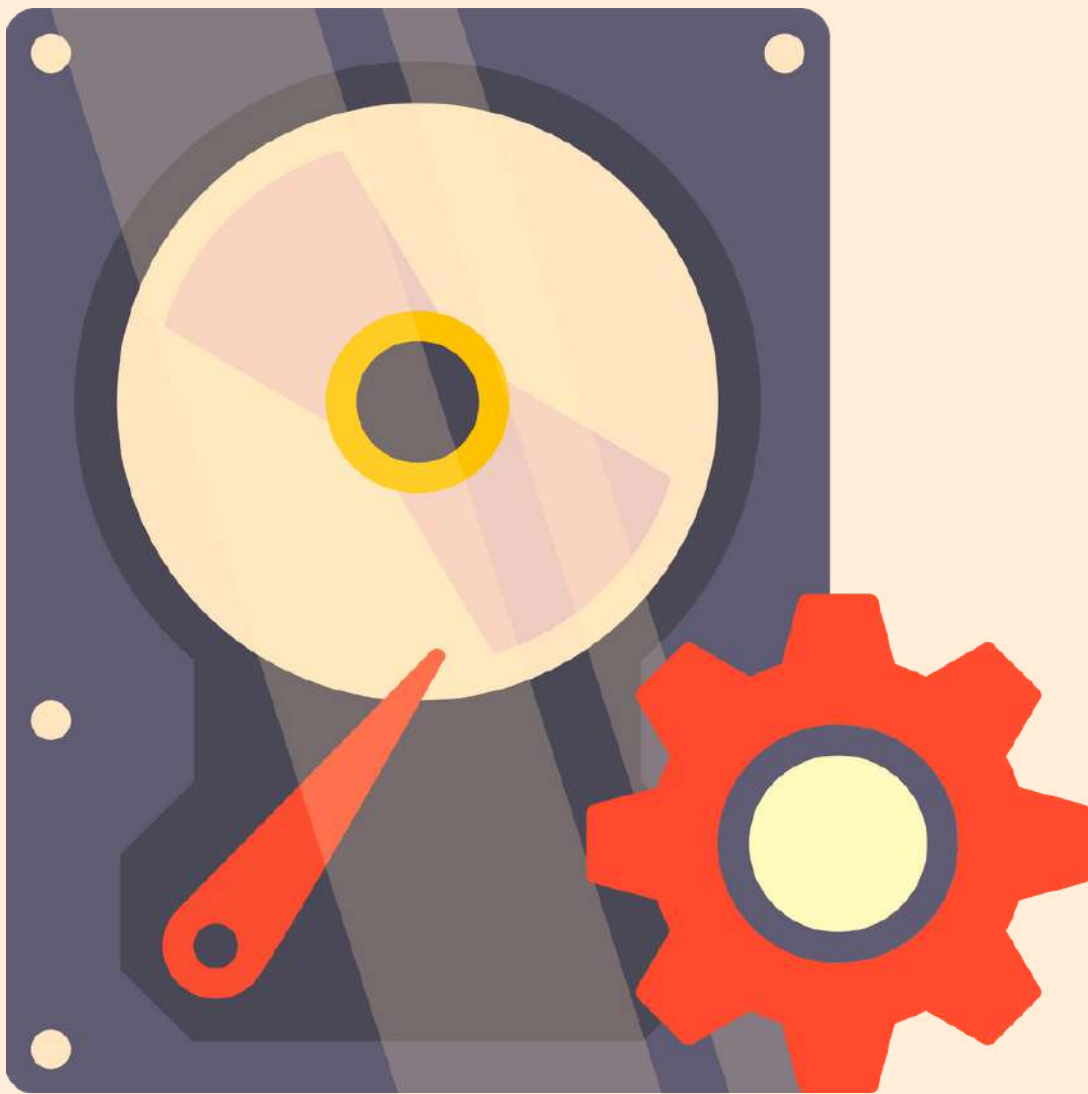
3. BEST PRACTICE PER IL BACKUP

Per garantire un backup efficace e sicuro, è fondamentale adottare un insieme di pratiche consolidate.



FREQUENZA E PIANIFICAZIONE DEL BACKUP

- Determinare la frequenza del backup in base alla criticità dei dati.
- Pianificare i backup in orari di basso utilizzo per ridurre l'impatto sulle risorse di sistema.



LA REGOLA DEL BACKUP 3-2-1

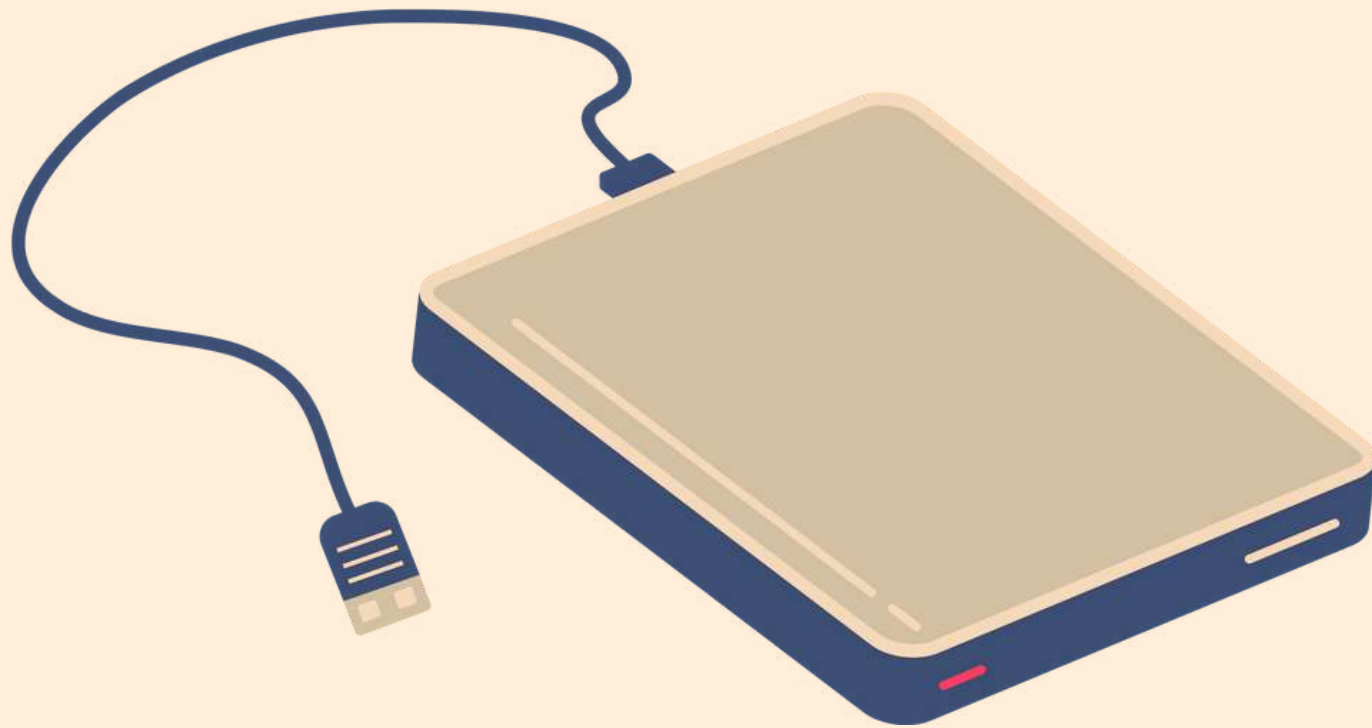
Un principio fondamentale per la sicurezza dei dati: 3 copie dei dati, su 2 supporti diversi, e una copia offsite.

AUTOMAZIONE E VERIFICA DEI BACKUP

**Configurare backup automatici e
verificare regolarmente la validità
dei backup per assicurarsi che
siano completi e funzionanti.**

4. RECUPERO DATI

Il recupero dati è una fase cruciale per garantire la continuità operativa in caso di perdita di informazioni.



DEFINIZIONE DI UN PIANO DI RECUPERO



- **Valutare i dati critici.**
- **Creare procedure documentate per il ripristino dei dati.**

TEST PERIODICI DEI PROCESSI DI RIPRISTINO

**Simulare scenari di
perdita di dati per
verificare l'efficacia delle
procedure di recupero.**



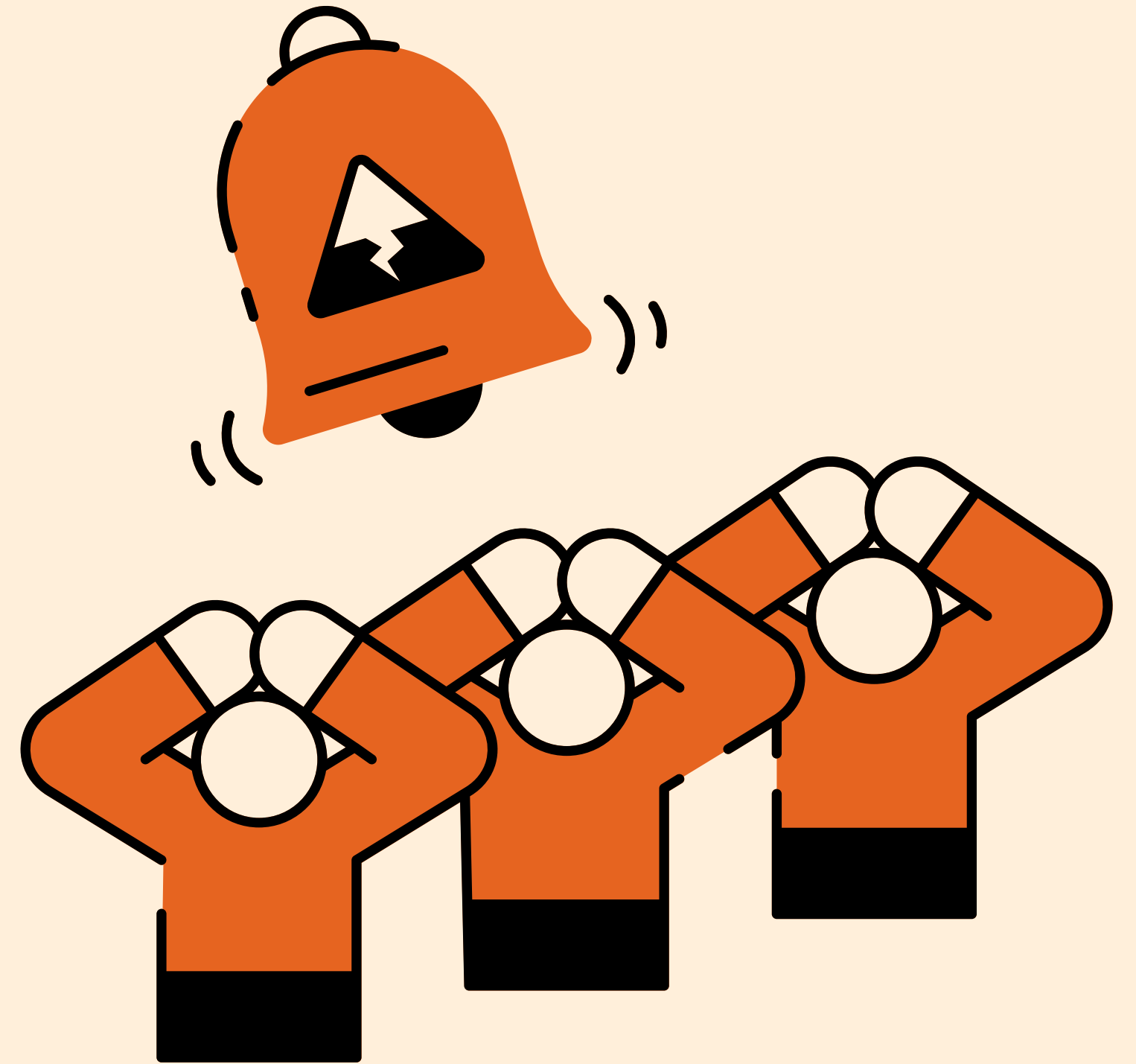
STRUMENTI PER IL RECUPERO DATI

- Software come Recuva, EaseUS, R-Studio e servizi professionali per il recupero.



5. DISASTER RECOVERY E SICUREZZA

Il disaster recovery è un aspetto fondamentale per garantire la continuità operativa in caso di eventi catastrofici.



DIFFERENZA TRA BACKUP E DISASTER RECOVERY

- Il backup è una copia dei dati, mentre il disaster recovery è un piano completo per il ripristino dei sistemi e delle operazioni aziendali.



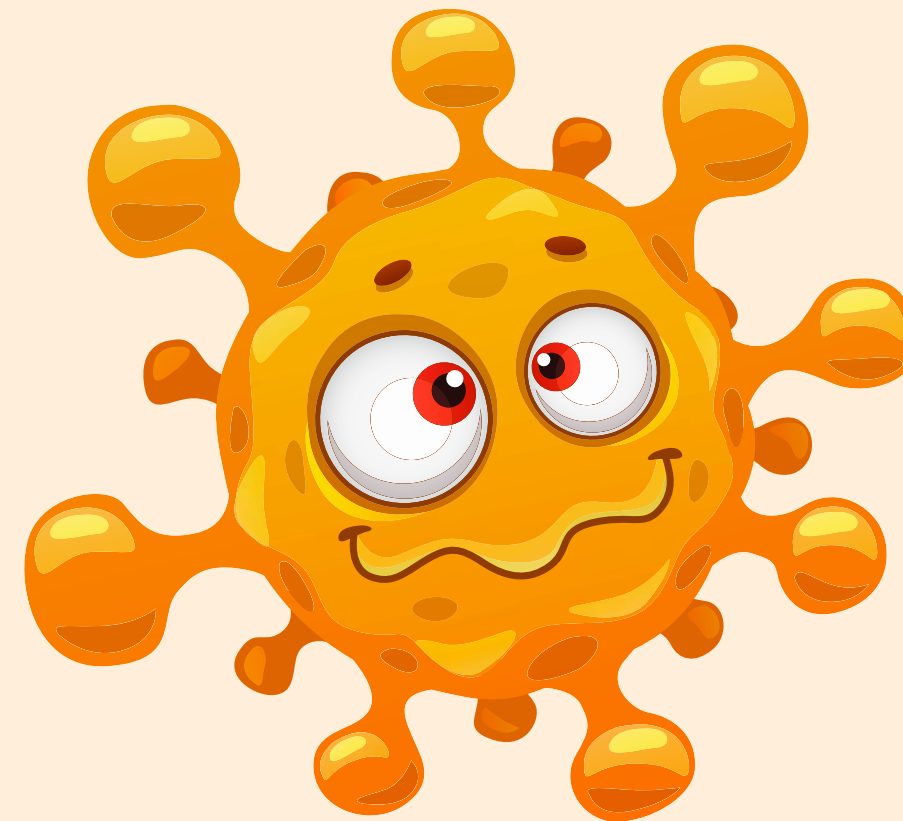
STRATEGIE DI DISASTER RECOVERY

- Utilizzo di Hot, Cold e Warm Sites.
- Soluzioni Cloud-based come AWS e Azure.



PROTEZIONE CONTRO RANSOMWARE

- Segmentazione della rete e backup immutabili per proteggere i dati da attacchi esterni.



6. CASI PRATICI



Esistono vari scenari reali e ipotetici per illustrare l'importanza di backup e disaster recovery.

CASO 1: GUASTO HARDWARE IN UN'UFFICIO

- L'azienda aveva un solo backup settimanale, perdendo 6 giorni di dati.
- Soluzione: backup incrementali giornalieri.**



CASO 2: ATTACCO RANSOMWARE A UN ENTE PUBBLICO

- Backup non aggiornati. Soluzione:
backup immutabili e protezione contro
ransomware.



CASO 3: DISASTRO NATURALE IN UNA ZONA SISMICA

- **Dati locali persi. Soluzione: backup cloud e piano di disaster recovery con cold site.**



CASO 4: RECUPERO DATI DA DISCHI DANNEGGIATI

- Dati persi per guasto del disco.**

**Soluzione: recupero professionale e
backup multipli.**



7. CONCLUSIONE E CONSIGLI FINALI

La protezione dei dati è una priorità fondamentale per aziende e individui. Attraverso l'implementazione di backup regolari e un piano di recupero dati ben strutturato, è possibile ridurre significativamente i rischi.

CONSIGLI FINALI:



- **Pianificazione è la chiave.**
- **Automazione e monitoraggio.**
- **Test regolari.**
- **Adotta la regola del 3-2-1.**
- **Proteggi i backup.**
- **Mantieniti aggiornato.**





CORSO TECNICO SOFTWARE 2024/2025