tnsolutions.it
FINE TECHNOLOGY



GUIDA 02 · BACKUP E DR

Backup e Disaster Recovery: quanto è preparata la tua azienda a un'interruzione IT?

Per le PMI: regola 3-2-1 e sue evoluzioni, RPO e RTO, immutabilità contro il ransomware, test di ripristino e piano di continuità operativa.

REVISIONE TECNICA **Marco Ursoleo** CEO TN Solutions

Per: Direzioni, IT Manager e responsabili amministrativi di PMI, studi professionali e aziende con server e servizi critici

Versione 1.0 · 14/11/2026

IN QUESTA GUIDA

Quasi tutte le aziende fanno qualche forma di backup. Molte meno sanno quanto tempo servirebbe per ripartire davvero dopo un guasto o un attacco. Questa guida spiega come passare da “abbiamo il backup” a “sappiamo ripristinare”.

1. Backup, disaster recovery e continuità: tre cose diverse 3

2. Backup locale, esterno e cloud 4

3. RPO e RTO: i due numeri che guidano le scelte 5

4. Immutabilità e ransomware 6

5. Backup di server fisici e macchine virtuali 7

6. Test di ripristino: l’unica prova che conta 8

7. Il piano di continuità operativa 9

8. Checklist aziendale 10

A chi è rivolta

Direzioni, IT Manager e responsabili amministrativi di PMI, studi professionali e aziende con server e servizi critici.

Come usarla

Leggi i capitoli nell’ordine, poi compila la checklist finale: le voci con priorità alta sono quelle da affrontare per prime.

Download libero

Questa guida è gratuita e non richiede registrazione. Puoi condividerla con il tuo team.

Contenuti verificati da Marco Ursoleo, CEO di TN Solutions

Revisione tecnica completata il 14/11/2026. TN Solutions opera con sistema di gestione certificato ISO 9001 e ISO/IEC 27001. Per domande su questa guida: info@tnsolutions.it · 02 95 17 550.

1. Backup, disaster recovery e continuità: tre cose diverse

Il primo passo è usare le parole giuste, perché ognuna risponde a una domanda diversa.

Concetto	Domanda a cui risponde	Esempio
Backup	Ho una copia dei dati da cui ripartire?	Copia giornaliera di server, file e caselle di posta
Disaster Recovery (DR)	Come e in quanto tempo rimetto in funzione i sistemi dopo un evento grave?	Ripristino del server su hardware alternativo o in un ambiente remoto
Continuità operativa	Come continua a lavorare l'azienda mentre i sistemi tornano disponibili?	Procedure alternative, priorità dei reparti, comunicazione ai clienti

Un backup senza un piano di ripristino è come un'assicurazione di cui non si conoscono le condizioni: c'è, ma non si sa cosa copre. Il disaster recovery trasforma la copia dei dati in un **tempo di ripartenza prevedibile**.

Perché il tema è diventato urgente

- Il **ransomware** non si limita più a cifrare i dati di produzione: cerca attivamente i backup raggiungibili dalla rete per cifrarli o cancellarli.
- Sempre più dati vivono in **servizi cloud** (posta, documenti condivisi) che molte aziende considerano "già protetti", ma che richiedono comunque una strategia di backup dedicata.
- I **server virtualizzati** concentrano più servizi su meno hardware: un guasto non gestito ha un impatto più ampio.
- Clienti, partner e assicurazioni chiedono sempre più spesso evidenze sulla capacità di ripristino.

2. Backup locale, esterno e cloud

Non esiste un'unica destinazione ideale: ogni posizione ha punti di forza e limiti. La strategia corretta di solito li combina.

Destinazione	Punti di forza	Limiti da considerare
Locale (NAS, storage dedicato)	Ripristini veloci, ideale per file e VM di grandi dimensioni	Esposto agli stessi rischi della sede (furto, incendio, attacco in rete)
Supporto esterno rimovibile	Separazione fisica dalla rete quando scollegato	Dipende dalla disciplina delle persone; rischio di dimenticanze e smarrimento
Cloud o datacenter remoto	Copia fuori sede automatica, protezione da eventi locali	Tempi di ripristino legati alla banda; costi ricorrenti; scelta del fornitore

La regola 3-2-1 e le sue evoluzioni

La regola 3-2-1 è il riferimento più diffuso: **tre copie** dei dati, su **due supporti** diversi, di cui **una fuori sede**. Con la diffusione del ransomware si è affermata un'evoluzione spesso indicata come **3-2-1-1-0**: almeno una copia **immutabile o offline** e **zero errori** nei test di verifica.

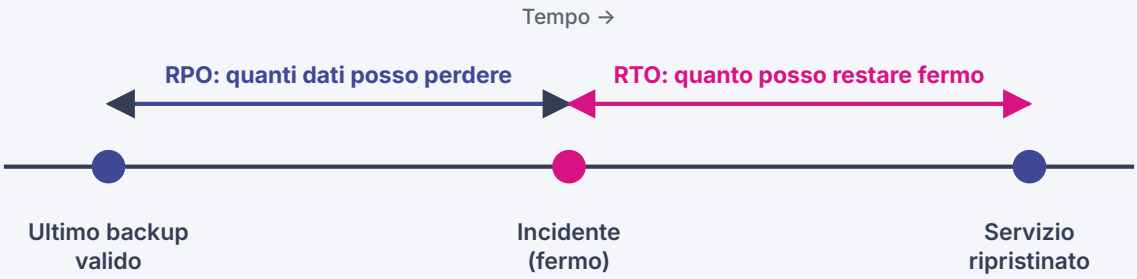


Schema originale: la regola 3-2-1 e la sua evoluzione. Le ultime due cifre spostano l'attenzione dalla copia al ripristino.

3. RPO e RTO: i due numeri che guidano le scelte

Prima di scegliere tecnologie e prodotti bisogna rispondere a due domande, sistema per sistema.

- **RPO (Recovery Point Objective)**: quanti dati posso permettermi di perdere? Se l'ultimo backup è di ieri sera e il guasto avviene alle 17, si perde una giornata di lavoro.
- **RTO (Recovery Time Objective)**: per quanto tempo posso restare fermo? È il tempo massimo accettabile tra l'incidente e la ripresa del servizio.



Schema originale: l'RPO guarda indietro (dati persi), l'RTO guarda avanti (tempo di fermo).

Esempio illustrativo di classificazione

I valori seguenti sono esempi per spiegare il metodo, non raccomandazioni valide per tutti.

Sistema	Impatto del fermo	RPO di esempio	RTO di esempio
Gestionale / ERP	Blocca ordini, fatture, magazzino	Poche ore	Entro la giornata
Posta elettronica	Rallenta clienti e fornitori	Poche ore	Entro poche ore
File server documentale	Ferma uffici tecnici e amministrativi	Un giorno lavorativo	Uno o due giorni
Archivio storico	Impatto limitato nel breve	Una settimana	Alcuni giorni

Più RPO e RTO sono stretti, più la soluzione diventa sofisticata e costosa. Il valore di questo esercizio è proprio rendere esplicito il compromesso tra costo e rischio, invece di scoprirlo durante un'emergenza.

RPO e RTO non sono mai stati definiti?

In una prima telefonata gratuita possiamo aiutarti a capire quali sistemi sono davvero critici e da dove partire.

Richiedi una prima consulenza telefonica gratuita →

4. Immutabilità e ransomware

Un backup **immutabile** è una copia che, per un periodo definito, non può essere modificata né cancellata, nemmeno da un amministratore. È una delle contromisure più efficaci contro gli attacchi che puntano a distruggere i backup prima di chiedere un riscatto.

Come si ottiene, in pratica

Storage con blocco degli oggetti
(object lock) in cloud o su appliance che lo supportano.

Repository protetti
con credenziali separate, non raggiungibili con gli account del dominio aziendale.

Copie offline
o con separazione di rete (air gap), anche con supporti rimovibili gestiti con procedure rigorose.

⚠ Errori frequenti

Usare le stesse credenziali di amministratore per server e backup. Lasciare il NAS di backup montato come cartella di rete sui PC. Conservare un solo punto di ripristino recente: se l'infezione è iniziata giorni prima, anche il backup può essere compromesso. Non ricevere o non leggere gli avvisi di backup fallito.

Il backup fa parte della sicurezza, non la sostituisce

L'immutabilità permette di ripartire, ma non impedisce l'attacco né la possibile esfiltrazione dei dati. Va affiancata a MFA, aggiornamenti, protezione degli endpoint e monitoraggio: ne parliamo nella Guida 3 della collana dedicata alla cybersecurity.

5. Backup di server fisici e macchine virtuali

Server fisici

Per i server fisici si usano in genere agenti installati nel sistema operativo, che consentono backup a livello di file o di immagine completa del disco. L'immagine permette il ripristino "bare metal" su hardware nuovo, utile quando il guasto riguarda la macchina intera.

Macchine virtuali

Negli ambienti virtualizzati il backup avviene spesso a livello di hypervisor, senza agente in ogni VM. Alcuni aspetti da verificare:

Coerenza applicativa
database e posta vanno salvati in uno stato coerente, non solo "fotografati" mentre scrivono.

Backup incrementali
basati sui blocchi modificati, per ridurre tempi e spazio.

Snapshot
utili per operazioni brevi (ad esempio prima di un aggiornamento), ma **non sono un backup** se restano sullo stesso storage della VM.

Ripristino granulare
poter recuperare un singolo file o una singola casella senza ripristinare l'intera VM.

Servizi cloud e Microsoft 365

Le piattaforme cloud garantiscono la disponibilità del servizio, ma la responsabilità sulla conservazione e sul recupero dei dati dell'azienda resta in larga parte del cliente: cancellazioni accidentali, errori di sincronizzazione o account compromessi possono propagarsi. Per questo è consigliabile un backup dedicato di Microsoft 365 con conservazione indipendente.

6. Test di ripristino: l'unica prova che conta

Un backup non testato è un'ipotesi. I test vanno pianificati, documentati e ripetuti, con difficoltà crescente.

Tipo di test	Cosa verifica	Frequenza indicativa
Ripristino di file singoli	Integrità dei dati e permessi	Mensile
Ripristino di una casella o di un database	Coerenza applicativa	Trimestrale
Avvio di una VM da backup in ambiente isolato	Capacità di ripartenza del sistema	Trimestrale o semestrale
Simulazione di disastro su un servizio critico	RTO reale, procedure, ruoli	Annuale

Ogni test produce un breve verbale: cosa è stato provato, quanto tempo è servito, cosa non ha funzionato, chi deve correggere. È anche un documento utile da mostrare a clienti e partner che chiedono garanzie.

BACKUP PROFESSIONALE CON ACRONIS

Tra i casi pubblicati da TN Solutions c'è un progetto di backup professionale con Acronis. Un altro caso riguarda la virtualizzazione dei server fisici di un'azienda strutturata, con un sistema di alta affidabilità. Approfondisci i servizi di Backup e Disaster Recovery.

7. Il piano di continuità operativa

Il piano di continuità operativa traduce la tecnologia in decisioni e responsabilità. Non deve essere un documento enorme: per una PMI bastano poche pagine chiare e aggiornate.

Gli elementi essenziali

1. **Analisi dell'impatto**: quali processi si fermano se un sistema non è disponibile, e con quali conseguenze.
2. **Priorità di ripristino**: in che ordine si riattivano i servizi.
3. **Ruoli**: chi decide, chi interviene, chi comunica con personale, clienti e fornitori.
4. **Procedure alternative**: come si lavora in modalità ridotta (ad esempio ordini registrati manualmente).
5. **Contatti e accessi di emergenza**: numeri, credenziali custodite, fornitori da allertare.
6. **Comunicazione**: messaggi già preparati per clienti e collaboratori.
7. **Revisione**: aggiornamento dopo ogni test, cambiamento organizzativo o incidente.

8. Checklist aziendale

Backup, disaster recovery e continuità	
☐ RPO e RTO definiti per ogni sistema critico	Alta
☐ Backup automatico di server, VM e servizi cloud	Alta
☐ Almeno una copia fuori sede	Alta
☐ Almeno una copia immutabile o offline	Alta
☐ Credenziali del backup separate da quelle del dominio	Alta
☐ Avvisi di backup fallito ricevuti e gestiti da una persona definita	Alta
☐ Test di ripristino documentato negli ultimi 6 mesi	Alta
☐ Backup dedicato per Microsoft 365 o altri servizi SaaS	Media
☐ Coerenza applicativa verificata per database e posta	Media
☐ Più punti di ripristino conservati nel tempo (retention)	Media
☐ Piano di continuità scritto con ruoli e priorità	Media
☐ Simulazione annuale di disastro su un servizio critico	Media
☐ Documentazione delle procedure di ripristino	Bassa

I prossimi passi consigliati

1. Elenca i sistemi critici e assegna a ciascuno un RPO e un RTO realistici.
2. Verifica che almeno una copia sia fuori sede e protetta da modifiche.
3. Pianifica un primo test di ripristino entro il prossimo mese.
4. Per un confronto tecnico, contatta TN Solutions: la prima telefonata è gratuita.

COME LAVORIAMO

Dal download alla soluzione, senza impegno nei primi passi

1 Download gratuito

Hai scaricato questa guida senza registrazione: usala per una prima autovalutazione.

2 Telefonata gratuita

Un incaricato TN Solutions ascolta le tue esigenze e ti aiuta a capire le priorità. È conoscitiva e senza impegno.

3 Audit avanzato (facoltativo, a pagamento)

Se serve un'analisi approfondita, con sopralluogo concordato, ricevi prima un preventivo dedicato. L'audit parte solo dopo che hai accettato il preventivo.

4 Proposta commerciale

Ricevi una proposta per i soli servizi necessari, con priorità e fasi di intervento.

Parla con noi
Prima telefonata gratuita e senza impegno

02 95 17 550 · info@tnsolutions.it · www.tnsolutions.it

Chi è TN Solutions

System integrator B2B con sede a Melzo (MI), operativo in Lombardia e da remoto su tutto il territorio nazionale. Dal 2001 progettiamo, integriamo e gestiamo infrastrutture IT per PMI, studi professionali, aziende di servizi, startup e imprese manifatturiere. L'azienda è guidata da **Marco Ursoleo**, CEO di TN Solutions.

Il sistema di gestione aziendale di TN Solutions è certificato **ISO 9001** (qualità) e **ISO/IEC 27001** (sicurezza delle informazioni). Le certificazioni riguardano i processi dell'azienda, non i singoli prodotti di terze parti citati in questa guida.

Servizi collegati a questa guida

Backup e Disaster Recovery
/it/centro-recupero-dati/backup-disaster-recovery/

Backup di Microsoft 365
/it/centro-recupero-dati/backup-office-365-servizio-aziendale-in-cloud/

Assistenza Informatica
/it/assistenza-informatica/

Virtualizzazione server
/it/virtualizzazione-server/

Infrastruttura IT sicura e resiliente
/it/infrastruttura-it-aziendale-sicura-resiliente/

Sicurezza Informatica
/it/sicurezza-informatica/

PROSSIMO PASSO

Vuoi capire come migliorare l'infrastruttura IT della tua azienda?

TN Solutions può aiutarti a valutare le esigenze, individuare le priorità e progettare la soluzione più adatta.

Richiedi una prima consulenza telefonica gratuita →

tnsolutions.it/it/contatti/

> Vuoi sapere se i tuoi backup reggerebbero un incidente reale? Parliamone in una prima telefonata gratuita.

TELEFONO 02 95 17 550

EMAIL info@tnsolutions.it

SITO WEB www.tnsolutions.it

SITO WEB CONTATTI

tnsolutions.it
FINE TECHNOLOGY

TN Solutions · Viale Svezia 3, 20066 Melzo (MI) · 02 95 17 550 · info@tnsolutions.it · www.tnsolutions.it

Contenuto realizzato con il supporto dell'intelligenza artificiale. Revisione e supervisione tecnica: Marco Ursoleo, CEO TN Solutions.

TN Solutions — Guide tecniche per le imprese · Guida 2 · Versione 1.0 · 14/11/2026. Le informazioni hanno carattere divulgativo e non sostituiscono un'analisi tecnica specifica. Le tabelle economiche sono esempi illustrativi, non offerte né medie di mercato. I marchi citati appartengono ai rispettivi titolari.