tnsolutions.it
FINE TECHNOLOGY



GUIDA 01 · CHECK-UP IT

La tua infrastruttura IT è pronta a sostenere la crescita aziendale?

Check-up IT per PMI: 30 controlli su postazioni, server, rete e sicurezza, con indicatori di criticità e checklist delle priorità.

REVISIONE TECNICA **Marco Ursoleo** CEO TN Solutions

Per: Titolari, direzioni e IT Manager di PMI da circa 10 postazioni in su, studi professionali e aziende di servizi

Versione 1.0 · 14/11/2026

IN QUESTA GUIDA

Quando l'azienda cresce, l'IT cresce spesso per aggiunte successive: un PC in più, un NAS, una licenza, un accesso remoto. Questa guida ti aiuta a fermarti un momento e a verificare, con 30 controlli concreti, se l'infrastruttura regge il passo del business.

1. Perché fare un check-up IT proprio adesso 3

2. Microimpresa, piccola impresa e PMI strutturata: esigenze diverse 4

3. I 30 controlli: postazioni e server 5

4. I 30 controlli: rete, sicurezza e continuità 7

5. Gli indicatori di criticità: come leggere i risultati 8

6. Quando passare a un MSP 9

7. Checklist finale con priorità 10

A chi è rivolta

Titolari, direzioni e IT Manager di PMI da circa 10 postazioni in su, studi professionali e aziende di servizi.

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. Perché fare un check-up IT proprio adesso

Nella maggior parte delle PMI l'infrastruttura informatica non viene progettata in un giorno: si forma un pezzo alla volta, seguendo le urgenze. Funziona finché l'azienda resta piccola. Poi arrivano nuovi collaboratori, una seconda sede, clienti che chiedono garanzie sulla sicurezza dei dati, un gestionale che non può fermarsi. A quel punto le scelte fatte "per tamponare" diventano un freno.

Il problema di fondo raramente è un singolo guasto. È l'**assenza di visione d'insieme**: nessuno sa con certezza quanti dispositivi ci sono, chi ha accesso a cosa, quando è stato provato l'ultimo ripristino di un backup, cosa succede se il server principale si spegne di venerdì sera.

Il rischio, tradotto in termini aziendali

Fermi operativi
ogni ora di blocco del gestionale, della posta o dei file condivisi ferma persone pagate e rallenta i clienti.

Perdita di dati
documenti, contabilità, progetti e corrispondenza sono spesso il vero patrimonio dell'impresa.

Esposizione agli attacchi
sistemi non aggiornati e password deboli sono la porta d'ingresso più comune per il ransomware.

Costi imprevisti
gli interventi d'urgenza costano di più e arrivano sempre nel momento peggiore.

Crescita rallentata
inserire un nuovo collaboratore richiede giorni invece di ore, aprire una sede diventa un progetto complicato.

In sintesi

Un check-up non serve a trovare colpevoli. Serve a trasformare una situazione "che funziona finché funziona" in un quadro chiaro, con priorità e costi prevedibili.

Vuoi un parere su cosa è emerso finora?

Una prima telefonata con un incaricato TN Solutions è gratuita e senza impegno: ti aiuta a capire quali segnali d'allarme meritano attenzione subito.

Richiedi una prima consulenza telefonica gratuita →

2. Microimpresa, piccola impresa e PMI strutturata: esigenze diverse

Non esiste un'infrastruttura giusta in assoluto. Esiste quella adatta alla dimensione, al settore e al livello di dipendenza dall'IT. Per orientarsi è utile ragionare per fasce. Le soglie di micro, piccola e media impresa usate qui riprendono la definizione europea (Raccomandazione UE 2003/361), basata sul numero di dipendenti; "PMI strutturata" è una nostra etichetta per le realtà con più funzioni, sedi o applicazioni critiche.

Profilo	Situazione tipica	Cosa diventa indispensabile
Microimpresa (meno di 10 persone)	Pochi PC, posta in cloud, un NAS o cartelle condivise, un referente "informale"	Backup automatico e verificato, aggiornamenti, MFA sulla posta, password manager
Piccola impresa (10–49 persone)	Primo server o NAS centrale, gestionale, stampanti di rete, accessi remoti	Inventario, gestione utenti, firewall configurato, procedure di onboarding e uscita
PMI strutturata (50 persone e oltre, o più sedi)	Server virtualizzati, più reparti, collegamenti tra sedi, applicazioni critiche	Monitoraggio, segmentazione della rete, piano di continuità, budget e roadmap IT

Molte aziende si trovano "a metà": hanno 25 persone ma un'infrastruttura pensata per 8, oppure hanno 12 postazioni ma un'applicazione di produzione che non può fermarsi. Il check-up serve proprio a far emergere questi disallineamenti.



Schema originale TN Solutions: i quattro livelli di maturità IT. L'obiettivo non è arrivare subito al livello 4, ma sapere dove ci si trova.

3. I 30 controlli: postazioni e server

Per ogni controllo indichiamo che cosa verificare e il segnale che deve far scattare un approfondimento. Puoi segnare la risposta direttamente su questa pagina o nella checklist finale.

Postazioni di lavoro (controlli 1–8)

#	Controllo	Segnale d'allarme
1	Esiste un elenco aggiornato di PC e notebook, con utente assegnato	Nessuno sa dire quanti dispositivi ci sono
2	Il sistema operativo è ancora supportato dal produttore	Postazioni con sistemi fuori supporto
3	Gli aggiornamenti sono installati in modo automatico e controllato	Aggiornamenti rimandati da mesi
4	È attiva una protezione endpoint gestita centralmente	Antivirus diversi, scaduti o non monitorati
5	Gli utenti non lavorano con privilegi di amministratore	Tutti possono installare qualsiasi software
6	I notebook hanno il disco cifrato	Un notebook perso espone dati aziendali
7	I dati di lavoro non risiedono solo sul disco locale	Documenti importanti "sul desktop"
8	Esiste un piano di sostituzione per età e prestazioni	PC lenti che fanno perdere tempo ogni giorno

Server e servizi centrali (controlli 9–15)

#	Controllo	Segnale d’allarme
9	Sai quali servizi girano su ogni server e chi li usa	Server “che nessuno tocca perché funziona”
10	Hardware e sistemi operativi sono sotto garanzia o supporto	Server fuori garanzia o senza ricambi
11	Dischi e alimentatori sono ridondati dove serve	Un solo disco per dati critici
12	Lo spazio libero e le prestazioni sono monitorati	Ci si accorge del disco pieno quando si blocca
13	Il server è in un ambiente adeguato (temperatura, accesso fisico, UPS)	Server sotto una scrivania o in un ripostiglio caldo
14	Le credenziali amministrative sono custodite e note a più persone autorizzate	Solo un ex collaboratore conosce la password
15	La documentazione minima esiste (configurazione, licenze, contatti)	Ogni intervento parte da zero

4. I 30 controlli: rete, sicurezza e continuità

Rete e connettività (controlli 16–22)

#	Controllo	Segnale d'allarme
16	Il firewall è un apparato professionale, configurato e aggiornato	Si usa solo il router dell'operatore
17	La rete ospiti è separata da quella aziendale	Ospiti e fornitori sulla stessa rete dei server
18	Gli accessi da remoto passano da VPN o soluzioni equivalenti protette	Desktop remoto esposto direttamente su Internet
19	Il Wi-Fi aziendale usa cifratura e credenziali gestite	Password Wi-Fi mai cambiata e nota a tutti
20	La connessione Internet ha una linea di backup o un piano alternativo	Senza Internet l'azienda si ferma del tutto
21	Switch e apparati sono identificati e documentati	Cavi e apparati senza etichette né schema
22	Le stampanti e i dispositivi IoT sono aggiornati e inventariati	Telecamere e stampanti mai aggiornate

Sicurezza, backup e continuità (controlli 23–30)

#	Controllo	Segnale d'allarme
23	Il backup è automatico e copre server, PC critici e servizi cloud	Backup manuale "quando ci si ricorda"
24	Esiste almeno una copia fuori sede e protetta da modifiche	Unico backup sullo stesso NAS collegato in rete
25	Il ripristino viene provato periodicamente	Nessun test di ripristino negli ultimi 12 mesi
26	L'autenticazione a più fattori (MFA) è attiva su posta e accessi remoti	Solo password, spesso riutilizzate
27	Gli account di chi lascia l'azienda vengono disattivati subito	Account di ex collaboratori ancora attivi
28	I permessi su cartelle e applicazioni seguono i ruoli	Tutti vedono tutto
29	Il personale riceve indicazioni su phishing e uso sicuro	Nessuna formazione o comunicazione
30	Esiste un piano scritto su cosa fare in caso di incidente o fermo	In emergenza si improvvisa

5. Gli indicatori di criticità: come leggere i risultati

Dopo aver risposto ai 30 controlli, conta quante risposte rientrano nel “segnale d’allarme”. Non è un punteggio scientifico, ma un modo semplice e onesto per capire da dove partire.

Risposte critiche	Lettura indicativa	Cosa fare
0–5	Base solida	Mantenere, documentare e pianificare i rinnovi
6–12	Fragilità diffuse	Definire priorità e un piano di interventi a 6–12 mesi
13–20	Rischio operativo concreto	Intervenire subito su backup, accessi e aggiornamenti
oltre 20	Infrastruttura non governata	Serve una presa in carico strutturata e una roadmap

> ⚠ **Alcuni controlli pesano più degli altri**
>
> Se anche uno solo tra i controlli **23, 24, 25 e 26** è critico, consideralo comunque prioritario, a prescindere dal totale. Backup non verificati e accessi senza MFA sono tra le cause più frequenti di danni gravi e difficili da recuperare.

Backup, aggiornamenti, accessi e continuità: il nucleo minimo

Se le risorse sono limitate, quattro aree danno il miglior ritorno in termini di riduzione del rischio:

1. **Backup verificati**: automatici, con copia fuori sede e test di ripristino periodici.
2. **Aggiornamenti**: sistemi operativi, firmware di firewall e NAS, applicazioni esposte su Internet.
3. **Accessi**: MFA, privilegi minimi, gestione rapida di ingressi e uscite del personale.
4. **Continuità operativa**: sapere in anticipo chi fa cosa se un sistema si ferma, e in quanto tempo deve ripartire.

6. Quando passare a un MSP

Un **MSP** (Managed Service Provider) è un fornitore che prende in carico la gestione continuativa di una parte o di tutta l'infrastruttura IT, con un perimetro, delle attività ricorrenti e dei livelli di servizio definiti per contratto. È un modello diverso dall'assistenza "a chiamata", in cui si interviene solo quando qualcuno segnala un problema.

Assistenza a consumo si paga l'intervento	Servizio gestito (MSP) canone per perimetro concordato
• Chiami quando c'è un problema	• Monitoraggio e manutenzione continui
• Costi variabili, difficili da prevedere	• Canone prevedibile e SLA scritti
• Prevenzione affidata a te	• Patch, backup e verifiche pianificate
• Adatta a pochi sistemi e poco critici	• Adatto quando il fermo costa caro

Confronto tra assistenza a consumo e servizio gestito. Nessuno dei due è "giusto" in assoluto: dipende da quanto l'azienda dipende dall'IT.

Segnali che indicano che è il momento

- Le richieste di assistenza sono frequenti e i costi variano molto da un mese all'altro.
- Nessuno in azienda ha il tempo o le competenze per seguire aggiornamenti, backup e sicurezza.
- Un fermo del gestionale o della posta ha un impatto economico evidente.
- Clienti o partner chiedono garanzie documentate sulla gestione della sicurezza.
- L'azienda sta crescendo e deve inserire persone o aprire sedi in modo ordinato.

Cosa aspettarsi da un buon contratto gestito

- Perimetro chiaro: quali dispositivi, server e servizi sono inclusi.
- Attività pianificate: aggiornamenti, controllo dei backup, monitoraggio, verifiche periodiche.
- Tempi di risposta e canali di contatto scritti.
- Reportistica comprensibile anche per la direzione.
- Un referente tecnico che conosce l'azienda, non un call center anonimo.

ASSISTENZA E GESTIONE CONTINUATIVA

TN Solutions affianca le imprese con assistenza informatica, contratti di assistenza e servizi gestiti in modalità MSP, in Lombardia e da remoto su tutto il territorio nazionale. Nei casi studio pubblicati trovi esempi di interventi su infrastrutture di studi professionali e aziende strutturate.

7. Checklist finale con priorità

Usa questa checklist come piano di lavoro. Le priorità sono indicative: vanno sempre ricalibrate sulla realtà specifica dell'azienda.

Le 15 azioni che consigliamo di verificare per prime	
☐ Backup automatico con copia fuori sede e protetta da modifiche	Alta
☐ Test di ripristino eseguito e documentato negli ultimi 6 mesi	Alta
☐ MFA attiva su posta, accessi remoti e account amministrativi	Alta
☐ Nessun desktop remoto esposto direttamente su Internet	Alta
☐ Sistemi operativi tutti supportati e aggiornati	Alta
☐ Account degli ex collaboratori disattivati	Alta
☐ Inventario di dispositivi, server e licenze	Media
☐ Protezione endpoint centralizzata e monitorata	Media
☐ Firewall professionale con firmware aggiornato	Media
☐ Rete ospiti separata dalla rete aziendale	Media
☐ Permessi sulle cartelle basati sui ruoli	Media
☐ Documentazione minima e credenziali custodite in modo sicuro	Media
☐ Piano scritto per la gestione di incidenti e fermi	Media
☐ Piano di sostituzione di PC e server per età	Bassa
☐ Indicazioni periodiche al personale su phishing e uso sicuro	Bassa

I prossimi passi consigliati

1. Condividi i risultati con chi in azienda prende le decisioni di spesa.
2. Scegli al massimo tre interventi ad alta priorità da avviare subito.
3. Valuta se le attività ricorrenti possono essere gestite internamente o se conviene un servizio gestito.
4. Se vuoi un confronto tecnico, contatta TN Solutions per una prima telefonata 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

Assistenza Informatica
/it/assistenza-informatica/

MSP — Gestione IT per aziende
/it/msp-gestione-it-aziende/

Contratti di assistenza informatica
/it/assistenza-informatica/contratti-assistenza-informatica/

Consulenza IT
/it/consulenza/

Sicurezza Informatica
/it/sicurezza-informatica/

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

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/

> Hai individuato tre o più criticità ad alta priorità? Con una telefonata gratuita possiamo aiutarti a metterle in ordine.

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 1 · 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.