tnsolutions.it
FINE TECHNOLOGY



GUIDA 09 · STUDI PROFESSIONALI

Informatica per studi legali e professionali: sicurezza, riservatezza e continuità del lavoro

Per studi professionali e PMI: postazioni e mobilità, gestionali, documenti riservati, posta e Microsoft 365, accessi remoti e MFA, backup, ransomware, collaboratori e scelta tra assistenza a chiamata e MSP.

REVISIONE TECNICA **Marco Ursoleo** CEO TN Solutions

Per: Titolari e responsabili organizzativi di studi legali, commercialisti, notai, studi tecnici e altre realtà professionali

Versione 1.0 · 14/11/2026

IN QUESTA GUIDA

Uno studio professionale vive di fiducia: i clienti affidano documenti, informazioni e scadenze che non possono andare perse né finire nelle mani sbagliate. Questa guida aiuta a costruire un'infrastruttura che protegga la riservatezza senza rallentare il lavoro quotidiano.

1. Il problema: tanta informazione riservata, poca struttura IT 3

2. Postazioni, mobilità e gestionali professionali 5

3. Documenti riservati, posta elettronica e Microsoft 365 6

4. Accessi remoti, MFA e gestione degli utenti 7

5. Backup, ransomware e continuità operativa 8

6. Assistenza a chiamata o servizio gestito (MSP)? 9

7. Checklist per lo studio 10

A chi è rivolta

Titolari e responsabili organizzativi di studi legali, commercialisti, notai, studi tecnici e altre realtà professionali.

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. Il problema: tanta informazione riservata, poca struttura IT

Molti studi sono cresciuti aggiungendo persone e strumenti senza un vero progetto informatico: un PC per ogni nuovo collaboratore, un NAS per l'archivio, una casella di posta in più, l'accesso da casa improvvisato durante un periodo di emergenza. Funziona, finché un notebook viene smarrito, una casella viene compromessa o il NAS si guasta alla vigilia di una scadenza.

Rischi specifici di uno studio

Riservatezza
atti, pareri, documenti di clienti e controparti sono informazioni molto sensibili.

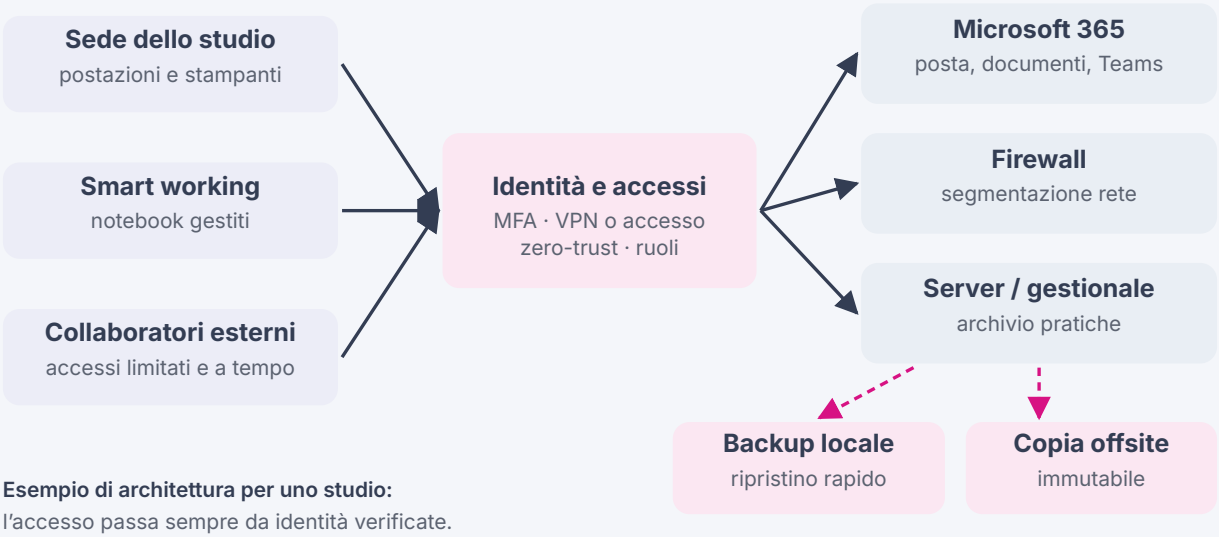
Scadenze
perdere l'accesso a documenti o calendari nel giorno sbagliato può avere conseguenze serie.

Frodi via email
gli studi gestiscono comunicazioni e talvolta indicazioni di pagamento, appetibili per chi compromette caselle di posta.

Collaboratori variabili
praticanti, consulenti esterni e personale che cambia richiedono accessi gestiti con attenzione.

Obblighi normativi: valutazione caso per caso

Il trattamento di dati personali è disciplinato dal GDPR, che richiede misure di sicurezza adeguate al rischio. Ulteriori obblighi possono dipendere dalla professione, dalle attività svolte e dai clienti assistiti: vanno verificati da ciascuno studio con i propri consulenti e gli ordini di riferimento. Questa guida si concentra sulle buone pratiche tecniche.



Esempio di architettura per uno studio:
l'accesso passa sempre da identità verificate.

Schema originale di un'architettura esemplificativa per uno studio professionale: tutti gli accessi passano da identità verificate.

2. Postazioni, mobilità e gestionali professionali

Postazioni e dispositivi mobili

Dispositivi aziendali gestiti
invece di PC personali per accedere ai dati dello studio.

Cifratura dei dischi
su tutti i notebook: un dispositivo perso non deve esporre documenti.

Aggiornamenti automatici
e protezione endpoint gestita.

Smartphone
con posta aziendale protetti da codice e, se possibile, gestiti centralmente con possibilità di cancellazione remota dei dati dello studio.

Gestionali professionali

Il gestionale dello studio (pratiche, scadenze, parcelle, archivio) è spesso l'applicazione più critica. Che sia installato su un server in sede o fornito in cloud, è importante sapere:

- dove risiedono i dati e chi ne fa il backup;
- come si accede da remoto e con quali protezioni;
- quali versioni sono supportate dal produttore;
- cosa succede se il servizio non è disponibile per un giorno.

3. Documenti riservati, posta elettronica e Microsoft 365

Gestione dei documenti

Struttura delle cartelle
coerente con l'organizzazione dello studio, con permessi per ruolo o per pratica.

Condivisioni esterne
controllate: link con scadenza, accesso nominativo, revisione periodica.

Archivio storico
separato dai documenti di lavoro, ma comunque protetto e incluso nel backup.

Posta elettronica e Microsoft 365

Per molti studi Microsoft 365 è la piattaforma di riferimento per posta, documenti e collaborazione. Le impostazioni che fanno la differenza:

- MFA per tutti gli account, amministratori compresi;
- protezione antispam e antiphishing configurata;
- regole che impediscano l'inoltro automatico della posta verso l'esterno senza controllo;
- gestione delle caselle condivise e dei permessi di delega;
- backup dedicato delle caselle e dei documenti, indipendente dalla piattaforma.

Approfondisci: Microsoft 365, Sicurezza e compliance in Microsoft 365, Backup di Microsoft 365.

Lo studio usa già Microsoft 365?

Una prima telefonata gratuita è utile per capire se configurazione, accessi e backup sono adeguati alla riservatezza richiesta.

Richiedi una prima consulenza per il tuo studio →

4. Accessi remoti, MFA e gestione degli utenti

Lavorare da fuori studio in sicurezza

Udienze, riunioni presso i clienti e lavoro da casa rendono indispensabile l'accesso remoto. Deve essere:

- protetto da **MFA** e da una VPN o soluzione equivalente;
- limitato alle risorse necessarie per ciascun ruolo;
- mai basato su desktop remoto esposto direttamente su Internet.

Approfondisci nella pagina dedicata all'autenticazione a due fattori.

Utenti e collaboratori

Situazione	Buona pratica
Nuovo collaboratore	Account nominativo, permessi per ruolo, dispositivo configurato prima del primo giorno
Praticante o stagista	Accessi limitati alle pratiche assegnate, scadenza definita
Consulente esterno	Account ospite o dedicato, accesso solo ai documenti necessari
Uscita dallo studio	Disattivazione immediata, recupero dei dispositivi, passaggio di consegne della casella
Cambio di ruolo	Revisione dei permessi, rimozione di quelli non più necessari

5. Backup, ransomware e continuità operativa

Backup

Il backup deve coprire server o NAS, gestionale, posta e documenti in cloud, con almeno una copia fuori sede e una copia immutabile o offline. E soprattutto deve essere **provato**: un ripristino di prova prima di una scadenza importante è la migliore assicurazione. Per approfondire, vedi la Guida 2 della collana.

Protezione dal ransomware

- MFA ovunque possibile e aggiornamenti puntuali.
- Protezione endpoint con avvisi gestiti.
- Permessi minimi: non tutti devono poter modificare tutto l'archivio.
- Backup immutabili, non raggiungibili con le credenziali dello studio.
- Attenzione del personale a email e allegati inattesi.

Continuità del lavoro

Uno studio dovrebbe sapere in anticipo come affrontare una giornata senza server, senza Internet o senza posta: dove reperire i documenti urgenti, come comunicare con i clienti, chi contattare per il ripristino.

INFRASTRUTTURA E SICUREZZA PER UNO STUDIO LEGALE

Tra i casi pubblicati da TN Solutions c'è il progetto di infrastruttura IT e sicurezza per uno studio legale, dedicato all'infrastruttura IT e all'accesso sicuro alle risorse dello studio da qualsiasi luogo. TN Solutions segue studi professionali con assistenza informatica e servizi di sicurezza.

6. Assistenza a chiamata o servizio gestito (MSP)?

Criterio	Assistenza a chiamata	Servizio gestito (MSP)
Quando si interviene	Su segnalazione	In modo continuativo e preventivo
Aggiornamenti e backup	Da verificare internamente	Pianificati e controllati dal fornitore
Costi	Variabili	Canone prevedibile
Conoscenza dello studio	Dipende dal tecnico disponibile	Referente che conosce l'infrastruttura
Adatto a	Studi piccoli, pochi sistemi	Studi che dipendono dall'IT ogni giorno

Per uno studio con più collaboratori, accessi remoti e un gestionale critico, la gestione continuativa riduce il rischio di scoprire i problemi nel momento peggiore. Approfondisci i servizi MSP.

7. Checklist per lo studio

Sicurezza, riservatezza e continuità	
☐ MFA attiva su posta, documenti e accessi remoti	Alta
☐ Backup di server, gestionale e Microsoft 365 con copia fuori sede	Alta
☐ Test di ripristino eseguito negli ultimi 6 mesi	Alta
☐ Dischi dei notebook cifrati	Alta
☐ Account disattivati il giorno dell'uscita di un collaboratore	Alta
☐ Nessun desktop remoto esposto su Internet	Alta
☐ Permessi sulle cartelle per ruolo o per pratica	Media
☐ Condivisioni esterne con scadenza e revisione periodica	Media
☐ Protezione antiphishing e controllo degli inoltri automatici	Media
☐ Procedura per lavorare in caso di fermo dei sistemi	Media
☐ Indicazioni al personale su phishing e frodi via email	Media
☐ Elenco aggiornato di dispositivi, licenze e fornitori	Bassa

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/

Microsoft 365
/it/microsoft-365/

Autenticazione a due fattori in azienda
/it/autenticazione-due-fattori-mfa-azienda/

Sicurezza Informatica
/it/sicurezza-informatica/

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

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

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 mettere in sicurezza l'infrastruttura del tuo studio? Richiedi una prima consulenza 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 9 · 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.