GUIDA GRATUITA · KIBIT

10 controlli per proteggere i dati della tua azienda

Una checklist pratica per aziende e studi professionali: in mezz'ora capisci se backup, password, aggiornamenti e rete sono davvero al sicuro.

KIBIT

www.kibit.it

Come usare questa guida

Leggi ogni controllo e rispondi alle domande. Spunta la casella solo se la risposta è un "sì" sicuro. Ogni casella vuota è un punto su cui conviene intervenire, e prima lo si fa, meno costa.

Non servono competenze tecniche: se una domanda non ha una risposta chiara, considerala una casella vuota.

01 Backup secondo la regola 3-2-1

Tieni almeno **3 copie** dei dati, su **2 supporti diversi** (per esempio PC e NAS), di cui **1 fuori sede** o in cloud.

- [ ] I backup partono in automatico, senza che qualcuno debba ricordarsene?
- [ ] Esiste una copia fuori dall'ufficio?

02 Prova a ripristinare, non solo a salvare

Un backup che non si riesce a ripristinare non serve. Ogni tanto prova a recuperare un file o una cartella.

- [ ] Quando è stata l'ultima prova di ripristino?
- [ ] Sai quanto tempo serve per ripartire dopo un guasto?

03 Una copia al riparo dal ransomware

I virus che cifrano i file colpiscono anche i dischi di backup collegati. Serve almeno una copia **scollegata** o **immutabile**.

- [ ] Almeno una copia non è raggiungibile dai PC dell'ufficio?
- [ ] Il NAS ha le snapshot attive?

04 Aggiornamenti sempre installati

Sistemi operativi e programmi non aggiornati sono la porta d'ingresso preferita dagli attacchi. Attenzione ai PC con sistemi non più supportati, come Windows 10.

- [ ] Gli aggiornamenti si installano regolarmente su tutti i PC?
- [ ] Ci sono computer con sistemi operativi fuori supporto?

05 Antivirus moderno e controllato

Un antivirus gestito avvisa chi si occupa dei PC quando qualcosa non va, invece di restare in silenzio su un computer.

- [ ] Tutti i dispositivi sono protetti, compresi i portatili?
- [ ] Qualcuno riceve gli avvisi quando viene bloccata una minaccia?

06 Password robuste e verifica in due passaggi

La verifica in due passaggi blocca la grande maggioranza dei furti di account. Attivala su posta, gestionali online e banca.

- [ ] Le password sono diverse per ogni servizio?
- [ ] La verifica in due passaggi è attiva sulle caselle email?

07 Un account per ogni persona

Utenti condivisi e password scritte sui post-it rendono impossibile capire chi ha fatto cosa. Ognuno deve avere il suo account e solo i permessi che servono.

- [ ] Ogni collaboratore ha credenziali personali?
- [ ] Chi lascia l'azienda viene disattivato subito?

08 Riconoscere le email truffa

Mittenti strani, urgenza, allegati inattesi, richieste di cambio IBAN: sono i segnali tipici del phishing. Nel dubbio, si verifica con una telefonata.

- [ ] Il personale sa riconoscere un'email sospetta?
- [ ] I cambi di IBAN vengono sempre verificati per telefono?

09 Rete e Wi-Fi in ordine

Router e firewall aggiornati, password Wi-Fi robuste e una rete separata per ospiti e clienti, che non veda i PC dell'ufficio.

- [ ] Il Wi-Fi per gli ospiti è separato dalla rete aziendale?
- [ ] La password del router è stata cambiata da quella di fabbrica?

10 Accesso da remoto sicuro

Collegarsi all'ufficio da casa è comodo, ma va fatto tramite VPN o strumenti di teleassistenza sicuri, mai lasciando servizi esposti su internet.

- [ ] Chi lavora da remoto usa una VPN?
- [ ] Ci sono porte aperte sul router per il desktop remoto?

Se qualcosa va storto: i primi minuti

1. Scollega dalla rete il PC sospetto (cavo e Wi-Fi), ma non spegnerlo.
2. Non pagare riscatti e non cancellare nulla.
3. Avvisa subito chi si occupa dell'informatica e cambia le password da un dispositivo sicuro.
4. Verifica quali backup sono intatti prima di ripristinare.

Vuoi una verifica fatta da un tecnico?

Richiedi il check-up informatico gratuito: controlliamo noi questi punti e ti consegniamo un riepilogo con le priorità.

kibit.it/check-up-informatico-gratuito · 347 383 6763 · info@kibit.it