# La tua azienda è protetta dai ransomware?

Checklist di autoanalisi in 12 domande — Stampa e compila

**Come usare questa checklist:** per ogni domanda, segna una sola casella tra **SÌ**, **NO** o **Non so**. Se non sei sicuro della risposta, segna **"Non so"** (nel calcolo del punteggio vale come un "NO"). Alla fine, somma i punti delle risposte **NO** e **Non so** per scoprire il tuo livello di protezione.

| # | Domanda | ✅ SÌ | ❌ NO | ❓ Non so |
|---|---|---|---|---|
| 1 | I backup sono conservati in un luogo separato dalla rete aziendale (es. cloud esterno o disco non sempre connesso)? | ☐ | ☐ | ☐ |
| 2 | Hai effettuato un test di ripristino dei backup negli ultimi 6 mesi? | ☐ | ☐ | ☐ |
| 3 | I dipendenti utilizzano account utente standard (senza privilegi di amministratore) per le attività quotidiane? | ☐ | ☐ | ☐ |
| 4 | Tutti gli account aziendali (email, gestionale, server) sono protetti con autenticazione a due fattori (2FA)? | ☐ | ☐ | ☐ |
| 5 | I dipendenti usano password diverse per ogni servizio aziendale? | ☐ | ☐ | ☐ |
| 6 | Gli ex dipendenti non hanno più accesso a sistemi o account aziendali? | ☐ | ☐ | ☐ |
| 7 | I sistemi operativi e i software sono aggiornati alle ultime patch di sicurezza? | ☐ | ☐ | ☐ |
| 8 | È installato e aggiornato un antivirus/antimalware su tutti i dispositivi? | ☐ | ☐ | ☐ |
| 9 | Il firewall aziendale è configurato e monitorato attivamente? | ☐ | ☐ | ☐ |
| 10 | I dipendenti hanno ricevuto formazione sul phishing negli ultimi 12 mesi? | ☐ | ☐ | ☐ |
| 11 | Esistono procedure scritte su come comportarsi in caso di sospetta infezione? | ☐ | ☐ | ☐ |
| 12 | Esiste un piano scritto di risposta agli incidenti informatici, con ruoli e contatti definiti? | ☐ | ☐ | ☐ |

### 📊 Come calcolare il punteggio

Assegna **1 punto** per ogni risposta "NO" e **1 punto** per ogni "Non so". Le risposte "SÌ" valgono 0 punti.

**Il mio punteggio totale:** _____ / 12



Ivan De Biasio | +39 347 888 3386

# Il tuo risultato

Cosa significa il tuo punteggio e cosa fare adesso

## 🛡 AZIENDA PROTETTA

**0–3 punti**

**Complimenti!** La tua azienda ha una buona base di sicurezza informatica. Hai implementato le misure fondamentali contro i ransomware.

**Cosa fare ora:**

- Mantieni aggiornate le procedure
- Ripeti questa autoanalisi ogni 6 mesi
- Valuta un audit esterno per identificare vulnerabilità nascoste

## ⚠ AZIENDA A RISCHIO

**4–7 punti**

**Attenzione!** La tua azienda presenta diverse vulnerabilità che potrebbero essere sfruttate da un attacco ransomware. Non è troppo tardi per intervenire, ma è importante agire con metodo.

**Azioni prioritarie:**

- Metti in sicurezza i backup (sono la tua ultima linea di difesa)
- Attiva l'autenticazione a due fattori su tutti gli account critici
- Pianifica una formazione base per i dipendenti sul phishing
- Documenta almeno una procedura di risposta agli incidenti

## 🔥 AZIENDA CRITICA

**8–12 punti**

**Situazione seria.** La tua azienda è altamente esposta a un attacco ransomware. Un singolo errore o una email di phishing potrebbero bloccare l'intera operatività per giorni o settimane.

**È urgente:**

- Effettuare un audit completo dell'infrastruttura IT
- Implementare immediatamente una strategia di backup isolato
- Rivedere accessi e permessi di tutti i sistemi
- Formare il personale sulle minacce informatiche
- Definire un piano di risposta agli incidenti

### Non sai da dove iniziare?

Non devi affrontare tutto da solo. Una breve chiacchierata può aiutarti a capire quali sono le priorità per la tua azienda, senza impegno e senza costi nascosti.

**+39 347 888 3386** ✉ **i.debiasio@dbsi.it** 🌐 **www.dbsi.it**

Ivan De Biasio — Consulente informatico per PMI
Friuli Venezia Giulia & Veneto