SECURITY LAB
sicurezza on line

📋 Checklist: Risk Analysis e Continuità Aziendale

Uno strumento pratico per valutare la resilienza della tua impresa.

🏢 1. Assetto Organizzativo (Art. 2086 C.C.)

- [ ] **Mappatura dei Processi:** Hai un diagramma chiaro di tutti i processi aziendali critici (vendite, produzione, logistica)?
- [ ] **Indicatori di Allerta:** Esistono KPI (indicatori di performance) monitorati mensilmente per rilevare cali di fatturato o ritardi d'incasso?
- [ ] **Organigramma e Responsabilità:** Sono definiti chiaramente i ruoli e chi deve intervenire in caso di anomalie?
- [ ] **Analisi di Mercato:** Viene effettuata almeno una volta all'anno un'analisi dei rischi legati alla concorrenza e ai costi delle materie prime?

🛡️ 2. Sicurezza Informatica e Protezione Dati (GDPR)

- [ ] **Inventario degli Asset:** Conosci esattamente dove sono salvati i dati sensibili (Server fisici, Cloud, PC portatili)?
- [ ] **Vulnerability Assessment:** Viene effettuata una scansione periodica delle falle di sicurezza della rete aziendale?
- [ ] **Data Minimization:** Hai rimosso i database obsoleti o i dati personali non più necessari alle finalità dichiarate?
- [ ] **Gestione degli Accessi:** Applichi il principio del "minimo privilegio" (ogni dipendente accede solo a ciò che gli serve)?

⚠️ 3. Business Continuity e Piani di Emergenza

- [ ] **Analisi d'Impatto (BIA):** Hai calcolato quanto costa all'azienda un fermo totale di 24 ore (o di una settimana)?
- [ ] **RPO e RTO Definiti:** Sono stati stabiliti i tempi massimi di recupero dati (RPO) e ripristino sistemi (RTO) in caso di disastro?
- [ ] **Backup Immutabili:** Esistono copie di sicurezza che non possono essere modificate o cancellate da un eventuale ransomware?
- [ ] **Test di Ripristino:** È stata fatta una simulazione di recupero dati negli ultimi 6 mesi per verificare che i backup funzionino davvero?

SECURITY LAB
sicurezza on line

⚖️ 4. Conformità Legale e Terze Parti

- [ ] **Audit Fornitori:** Hai verificato la solidità e la sicurezza dei fornitori critici (es. cloud provider o logistica esterna)?
- [ ] **Coperture Assicurative:** Le polizze attuali coprono i rischi cyber e i danni da interruzione di attività?
- [ ] **Formazione del Personale:** I dipendenti sono addestrati a riconoscere i rischi (phishing, truffe del CEO, procedure di emergenza)?

💡 Come interpretare i risultati

- **Da 0 a 4 "No":** La tua azienda ha una buona base di resilienza, ma richiede affinamenti tecnici.
- **Da 5 a 8 "No":** Sei in una zona di rischio moderato. Un imprevisto potrebbe causare danni economici rilevanti.
- **Oltre 8 "No": Critico.** L'assetto organizzativo non è adeguato all'Art. 2086 C.C. e il rischio di sanzioni o fermo aziendale è altissimo.

Il consiglio di SecurityLab: La Risk Analysis non è un documento statico da chiudere in un cassetto, ma un processo vivo. Iniziare dai rischi "Cyber" è oggi il modo più rapido per mettere in sicurezza il valore reale della tua impresa.
