✓ SETTORE — 2 REPORT

RISK ASSESSMENT LIGHT

Technology & ICT

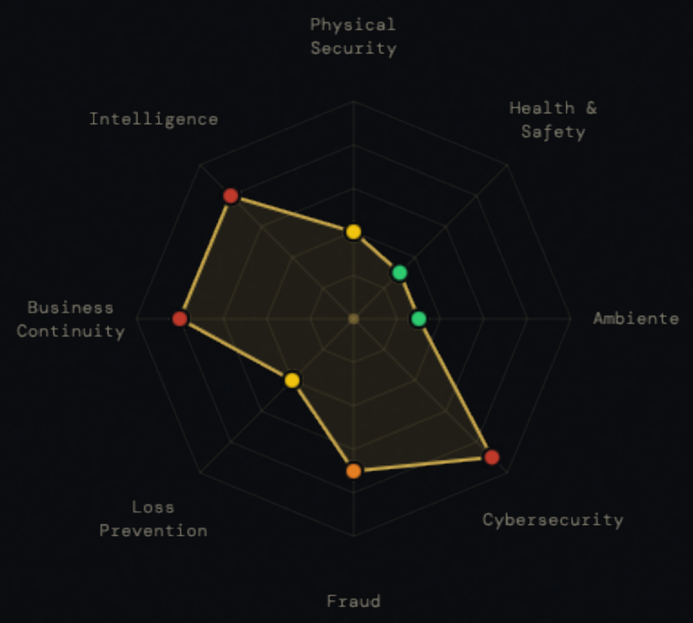
DATA ANALISI
26 maggio 2026

METODOLOGIA
ISO 31000 / Light

AREE ANALIZZATE
8 domini di rischio

LIVELLO GLOBALE
Alto

● LIVELLO DI RISCHIO GLOBALE: ALTO



67 /100

Il settore tech è dominato da rischi cyber e intelligence competitiva. La business continuity dei sistemi IT è critica. L'esposizione alla proprietà intellettuale e alle frodi digitali è elevata.

3	1	2	2
CRITICI	ALTI	MEDI	BASSI

ANALISI PER DOMINIO DI RISCHIO

4

Physical Security

MEDIO

Esposizione moderata. Controllo accessi e videosorveglianza raccomandati.

AZIONI RACCOMANDATE

- → Sistema TVCC perimetrale
- → Controllo accessi elettronico
- → Piani di risposta a intrusioni

3

Health & Safety

BASSO

Ambiente di lavoro a basso rischio infortunistico. Adempimenti base D.Lgs 81/08 sufficienti.

AZIONI RACCOMANDATE

- → DVR aggiornato
- → Formazione base lavoratori

3

Ambiente

BASSO

Impatto ambientale ridotto. Adempimenti standard ISO 14001 applicabili.

AZIONI RACCOMANDATE

- → Registro rifiuti
- → Formazione ambientale

9

Cybersecurity

CRITICO

Rischio cyber critico. Target ad alto valore per attaccanti. Richiesta difesa in profondità.

AZIONI RACCOMANDATE

- → CISO dedicato
- → Zero trust architecture
- → Red teaming continuo

7

Fraud

ALTO

Alta esposizione a frodi interne ed esterne. Richiesto programma anti-frode strutturato.

AZIONI RACCOMANDATE

- → Analisi dati per anomalie
- → Investigazioni interne
- → Fraud risk assessment

4

Loss Prevention

MEDIO

Esposizione moderata a perdite. Ottimizzazione dei controlli di magazzino raccomandata.

AZIONI RACCOMANDATE

- → Sistemi antitaccheggio
- → Controllo inventario real-time
- → Formazione personale

8

Business Continuity

CRITICO

Business continuity critica. Interruzioni hanno impatto sistemico. DRP completo indispensabile.

AZIONI RACCOMANDATE

- → Resilienza multi-sito
- → Esercitazioni crisi
- → Certificazione ISO 22301

8

Intelligence

CRITICO

Target ad alto valore per intelligence. Richiesta controintelligence e threat assessment continuo.

AZIONI RACCOMANDATE

- → Counterintelligence program
- → Monitoraggio dark web
- → Intelligence officer dedicato

NOTA METODOLOGICA

Il presente documento costituisce un'analisi preliminare di risk assessment di tipo "light", basata su profili di rischio tipici per categoria di settore. Non sostituisce un'analisi di rischio approfondita, personalizzata e condotta in loco da professionisti qualificati. Benedetti Group S.r.l. declina ogni responsabilità per decisioni operative adottate sulla base esclusiva di questo report indicativo. Per un'analisi completa e certificata, contattare il nostro team di esperti.

← NUOVA ANALISI

© 2026 Benedetti Group S.r.l. — Tutti i diritti riservati