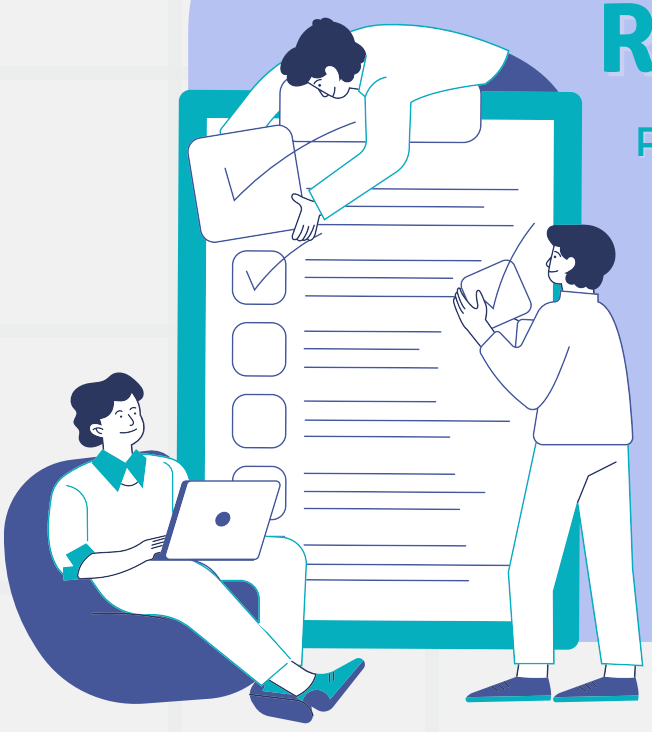

# RISCHIO CYBER

## PERCHÉ AUTOVALUTARSI

Scopri gli ambiti specifici in cui è maggiormente esposta la tua organizzazione e le relative pratiche di sicurezza migliori

## Domini di sicurezza del QUESTIONARIO

### Governance e Asset

Gestione della sicurezza dell'organizzazione con politiche, procedure, standard e certificazioni; controllo delle risorse aziendali attraverso l'inventario degli elementi della catena di valore.

### Security infrastructure

Adozione di misure di sicurezza per proteggere il patrimonio informativo dell'organizzazione (informazioni classificate o riservate, proprietà industriale, ecc.)

### Awareness e comunicazioni

Sensibilizzazione e formazione del personale per migliorare i presidi di sicurezza aumentando la consapevolezza sugli attacchi informatici e le loro possibili conseguenze

### Security update e monitoring

Aggiornamento frequente dei sistemi di sicurezza e monitoraggio costante degli eventi per migliorare la consapevolezza sul proprio livello di esposizione alle minacce informatiche e per consentire interventi di contrasto tempestivi

### Protezione del dato, Backup e Disaster Recovery

Impiego di soluzioni per la protezione del dato che ne garantiscano riservatezza, integrità e disponibilità in casi di possibili situazioni catastrofiche e di attacchi informatici distruttivi.

Il raggruppamento delle domande nei principali domini della *cyber security*, ci consente di fornire indicazioni chiare nell'esito finale riguardo gli interventi più urgenti da effettuare per diminuire il proprio livello di esposizione al rischio informatico.

Risorse utili:

- Standard ISO/IEC 27001 per la gestione della sicurezza informatica
- Guida alla cibersicurezza per le piccole e medie imprese - ENISA
- Vademecum Sicurezza Piccole e Medie Imprese – CYBER 4.0