The four pillars of cyber resilience:

Readiness checklist for SMBs

Assess your business's preparedness for cyber incidents and downtime using this quick yes/no checklist.

1. Risk awareness and assessment

- ☐ We have identified our critical business systems and data.
- ☐ We conduct regular vulnerability assessments, covering technical and human factors.
- ☐ We understand the potential financial and operational impact of downtime on our business.

2. Data protection

- ☐ We maintain secure, encrypted backups of all critical data.
- ☐ Backups are regularly tested to ensure successful recovery.
- ☐ Our backup strategy includes multiple storage locations (on-site and cloud).

3. Incident response plan

- ☐ A comprehensive incident response plan is documented and accessible.
- ☐ Roles and responsibilities are clearly defined in case of a cyberattack.
- ☐ Communication procedures for internal and external stakeholders are defined.

4. Testing and training

- ☐ Regular simulations or tabletop exercises are conducted to test our response.
- ☐ Employees receive training to recognize phishing and other cyberthreats.
- ☐ We review and update our incident response plan at least annually.

Your cyber resilience score

- ✓ **12–15 checks:** Strong resilience readiness. Keep testing and improving.
- ! **7–11 checks:** Moderate readiness. Focus on addressing the gaps.
- × **0–6 checks:** High risk. Immediate action is necessary to protect your business.

Next steps

Building cyber resilience is an ongoing process, not a one-time task. If you've identified gaps in your readiness, now's the time to address them.

Book a Cyber Resilience Readiness Assessment with our experts to get personalized insights and recommendations. You'll be better equipped to protect your business from cyberthreats and ensure continuity in the face of potential disruptions.

Cubical http://www.cubical.ec
+59325142100
soporte@cubical.ec