www.ig.technology
info@ig.technology
+1 (786) 712-5226

CYBERSECURITY CHECKLIST

Protect your company in less than an hour

You don't need to be a tech expert to protect your company. This checklist is designed for managers, directors, and business owners. **Each action can be completed in less than an hour.** Check each box as you complete it.

Company Name	Cybersecurity Manager	Date

1 Access & Passwords

The #1 cause of breaches in companies

- [ ] **Enable two-factor authentication (MFA) on corporate email**
  Gmail, Outlook, and any cloud service have it for free in security settings.
- [ ] **Change all default passwords for routers, cameras, and servers**
  If the password is «admin» or «1234», anyone can enter. Change it today.
- [ ] **Delete accounts of employees who no longer work with you**
  Every active account without an owner is an open door for an attacker.
- [ ] **Use unique passwords per service, never repeat the same one**
  Consider a password manager like Bitwarden (free) for your team.

2 Email

90% of attacks arrive via email

- [ ] **Train your team to recognize phishing emails**
  Show them real examples of fake emails. 30 minutes can prevent a disaster.
- [ ] **Enable the anti-spam and anti-phishing filter on your mail server**
  Google Workspace and Microsoft 365 already include it, you just have to enable it.
- [ ] **Never open unexpected attachments, even from known contacts**
  If you weren't expecting that PDF or Excel, call the sender before opening it.
- [ ] **Verify your domain has SPF, DKIM, and DMARC configured**
  This prevents someone from spoofing your email. Ask your tech team to verify it.

3 Data Backup

If you lost everything today, could you recover it tomorrow?

- [ ] **Back up all critical data today**
  Include contracts, customer databases, invoices, and operational files.
- [ ] **Keep at least one copy outside the office or in the cloud**
  If there is ransomware or a fire, you need a copy that is not in the same place.
- [ ] **Test that you can restore your backups, making them is not enough**
  A backup that has never been tested can fail when you need it most.
- [ ] **Automate backups to occur without manual intervention**
  Manual backups are forgotten. Set up a daily or weekly automated task.

4 Devices & Software

Outdated software is an open invitation

- [ ] **Update all operating systems and applications this week**
  Updates close vulnerabilities that attackers already know and exploit.
- [ ] **Install an updated antivirus on all company computers**
  Ensure it is active and with up-to-date definitions on every computer.
- [ ] **Uninstall software that no one uses**
  Every installed program is a potential entry point. If it's not used, delete it.
- [ ] **Automatically lock computers after 5 minutes of inactivity**
  An unlocked screen in an office can compromise the entire company.

5 Network & Remote Access

Work from anywhere, but securely

- [ ] **Change the office router password to a strong and unique one**
  The router password should be changed periodically.
- [ ] **Separa la red WiFi de invitados de la red interna de trabajo**
  Clientes y visitas no deben estar en la misma red que tus servidores.
- [ ] **Use a VPN to connect to company systems from home or while traveling**
  Without a VPN, your connection is visible to anyone on the same public network.
- [ ] **Bloquea el acceso remoto directo desde internet si no lo necesitas**
  El acceso remoto expuesto es uno de los vectores más explotados en LATAM.

How many boxes did you check?

Add up your checked boxes and compare with the table. Repeat this checklist every quarter.

☐ / 20

0 – 8	9 – 14	15 – 20
High Risk	**Medium Risk**	**Low Risk**
≈ 70% probability of suffering an incident	≈ 40% probability of suffering an incident	< 15% probability of suffering an incident
Your company is exposed. Prioritize sections 1 and 2 this very week.	You are on the right track, but there are important gaps to close.	Good security baseline. Keep the habit and review every quarter.

Need help improving your security?

Our team can help you close every gap on this list, without technical jargon. Write to us and we will respond.

Contact Us →

www.ig.technology · +1 (786) 712-5226