12 ACTIONS TO SECURE YOUR BUSINESS

1 CYBERSECURITY CULTURE

To establish a strong cybersecurity culture at all levels of the organization, along with appropriate protection processes and systems.

2 TRAINING AND AWARENESS

Continuous and effective training with regard to one's role, with no one excluded. Everyone contributes to the security of our information.

3 THIRD PARTIES, SUPPLIERS

They must be monitored to ensure adequate security levels. Their risks are also ours!

4 INCIDENT MANAGEMENT

You must have incident response procedures, they should be documented, and, if necessary, communicated. Learn lessons from incidents!

5 SECURE SYSTEMS

Access to systems and information must occur with strong, not easily discoverable credentials, using multiple factors. Let's keep the keys secure!

6 SECURE SYSTEMS WITH THE RIGHT PRODUCTS AND CONFIGURATIONS

A system needs security products (antivirus, encryption, etc.) and proper management to be secure: continuous system and application updates, use of only necessary software.

7 SECURE NETWORK

Implement products to secure the access network to your systems, the internet browsing network (e.g., firewalls, etc.) differently

8 PHYSICAL SYSTEMS

Protect physical access to your systems and information, set up automatic locks on systems (computers, servers, phones, etc.) in case of non-use.

9 PERFORMING AND SECURING BACKUPS

They must be planned and executed automatically, monitored and verified, adequately protected, and if necessary, replicated on different systems/sites.

10 THE CLOUD SIMPLIFIES, BUT IT MUST BE MANAGED CORRECTLY

It is necessary to pay attention to where (contractually) the data resides, the replication, service levels, and data protection and analysis systems (e.g., logs, access alerts).

11 ONLINE SECURELY

It is necessary to use secure protocols for both sites and services, handle information carefully, and conduct regular security tests.

12 SHARING HELPS PROTECT US

It is helpful to share experiences and network on security aspects.