Acelera pyme

Cybersecurity for SMEs and freelancers: protect your business in the digital world and stay one step ahead of the curve

"Una manera de hacer Europa"
Fondo Europeo de Desarrollo Regional

Financiado por la Unión Europea NextGenerationEU

red.es

Plan de Recuperación, Transformación y Resiliencia

KIT DIGITAL

España | digital 2026

Contents

> Introduction 03.

> Cybersecurity awareness 04.

> Most common threats in cybersecurity 05.

> Data protection and practical tips for cybersecurity implementation 06.

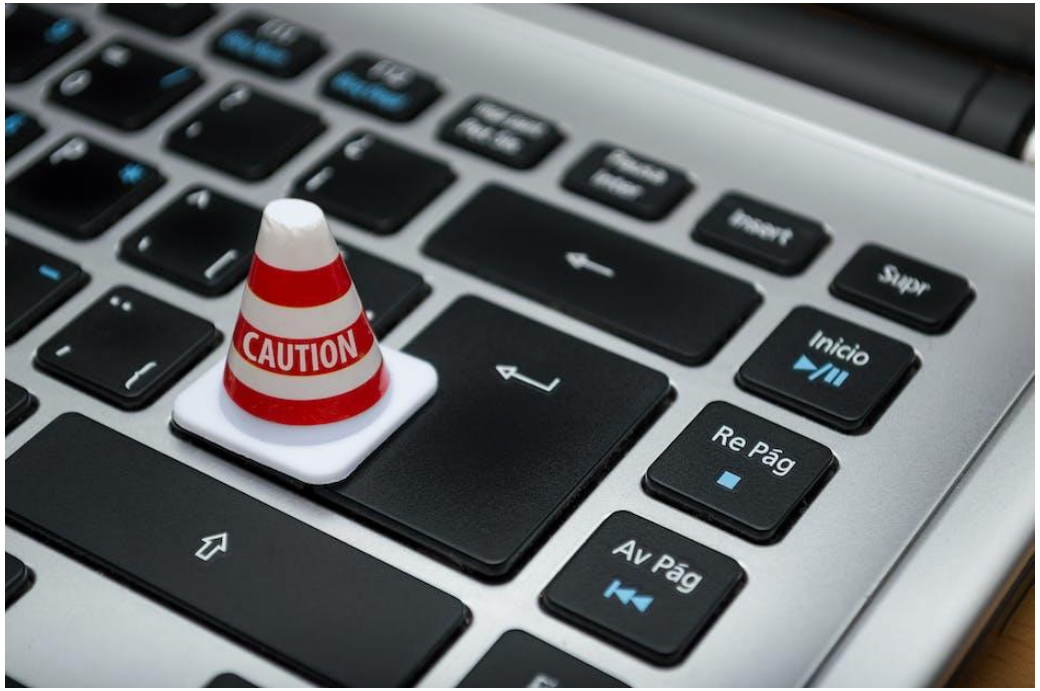
> Cybersecurity tools and technologies 09.

> Conclusions 10.

Introduction

Cybersecurity has become a **growing concern** in the business world and for society in general. Cyber attacks represent a **real threat** that can jeopardize **data security**, **reputation** and generate significant **economic losses**.

With increasing digitization, **SMEs** and **freelancers** have become more **vulnerable** to these attacks, so it **is essential that they are prepared** and have **adequate cybersecurity measures in place**.



Cybersecurity awareness

> The **process** of raising **awareness** of cybersecurity is something that can begin by **taking a number of actions**, such as those listed below:

Establish clearly stated **cybersecurity policies** and communicate them effectively and regularly.

Report risks with real cases to illustrate the consequences of lack of cybersecurity awareness and knowledge.

Educate and train employees of the SME so that they are aware of the most common risks and how to avoid them.

Exchange information with other agencies and associations to prevent the most common or most recent attacks.

Most common threats in cybersecurity

INCIBE - Guide to **prevent various attacks** and **how to act**:

1. Information leaks
2. Phishing attacks
3. CEO fraud (spear phishing)
4. HR fraud
5. Sextortion
6. Attacks against the corporate website
7. Ransomware
8. Fake Microsoft support scam
9. Malware email campaigns
10. Denial of service (DoS) attacks
11. Adware attacks
12. Vendor impersonation attacks

Data protection and practical tips for cybersecurity implementation

> **Data susceptible to theft** by cybercriminals:

CONFIDENTIAL OR PRIVILEGED CORPORATE INFORMATION

CUSTOMER INFORMATION

SUPPLIER INFORMATION

EMPLOYEE INFORMATION

PASSWORDS

Data protection and practical tips for cybersecurity implementation

Acelera pyme

BASIC GUIDELINES

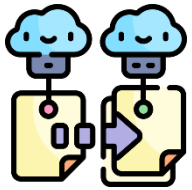
1. Use unique **passwords**
2. Multi-factor **identification**
3. Employ a **firewall**
4. Up-to-date **operating system** at all times
5. Avoid connecting to **public Wi-Fi** and activate **VPN**
6. Check that links have "**https**".
7. Enabling or increasing **privacy settings**
8. Be cautious about what **personal information** you share and where you share it
9. Only download **software** that is **verified** and from trusted sources
10. Regularly perform **backups**

Data protection and practical tips for cybersecurity implementation

> Applying cybersecurity measures must be accompanied by an organized and measured implementation. For this reason, the following **strategies** are proposed:

Developing a cybersecurity plan

Establish an incident response



Perform regular backups

Establish security policies

Implement technical security measures

Employee training and awareness

Keep software up to date

Reducing the digital footprint

Cybersecurity tools and technologies

Antivirus

- Bitdefender Antivirus Free
- Avast Free Antivirus

VPN

- Hotspot Shield
- ProtonVPN Free

Firewall

- Windows Defender
- ZoneAlarm
- Comodo Free Firewall

Password manager

- 1Password
- LastPass

Conclusions

In short, **SMEs and the self-employed must be prepared** to deal with **cybersecurity threats**. Awareness, understanding of common threats, data protection and implementation of appropriate security measures are key aspects to minimize risks.

Cybersecurity **must be a priority** for all companies, as attacks **can have serious consequences** both in terms of security and economic.

Acelera pyme

"Una manera de hacer Europa"

Fondo Europeo de Desarrollo Regional

Financiado por la Unión Europea NextGenerationEU

Gobierno de España · Vicepresidencia Primera del Gobierno · Ministerio de Asuntos Económicos y Transformación Digital · Secretaría de Estado de Digitalización e Inteligencia Artificial

red.es

Plan de Recuperación, Transformación y Resiliencia

KIT DIGITAL

España | digital 2026