Acelera pyme

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

April 2023

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

Acelera pyme

Contents

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA

Acelera pyme

1. Introduction

In the field of cybersecurity, the **risk of cyberattacks** is a reality that is increasingly **present** in the business world and in the public at large. These attacks can not only **jeopardize the security of data and confidential information of the SME**, but can also **affect its image and reputation**, as well as **generate significant economic losses**. Moreover, with the acceleration of digitization in all sectors, exposure to these types of threats has also increased. Therefore, it is **imperative** that SMEs and freelancers are **prepared to deal with these attacks** and have adequate cybersecurity measures and tools in place to minimize risks.

According to the Cybersecurity Balance 2022 **[REF-01]** published by the National Cybersecurity Institute (INCIBE), queries from companies mainly originate from phishing, smishing or extortion techniques (20.8%), CEO fraud or Business Email Compromise, BEC (15.3%) and employee awareness and good cybersecurity practices (12.5%). It is worth noting that, **in 2022**, INCIBE managed a total of **118,820 incidents**, an increase of 8.8% compared to 2021. **Several reasons may have influenced this**, such as the **increased degree of digitalization** in the country by both citizens and companies, which has generated a higher number of cyber incidents, and the Russia-Ukraine conflict, which has allowed cybercriminals to perpetrate more cybercrime **[REF-02]**. According to S21sec, Spain ranks seventh in the ranking of the countries most cyberattacked by ransomware in 2022 **[REF-03]**. As the DESI 2022 result indicates **[REF-04]** although Spain is not the country with the highest degree of digitalization, it is in the top 10 countries that have received the most ransomware attacks this year. It is therefore essential that citizens, companies, public administration and trainers give cybersecurity the importance it deserves, since suffering an attack of this type can have serious consequences.

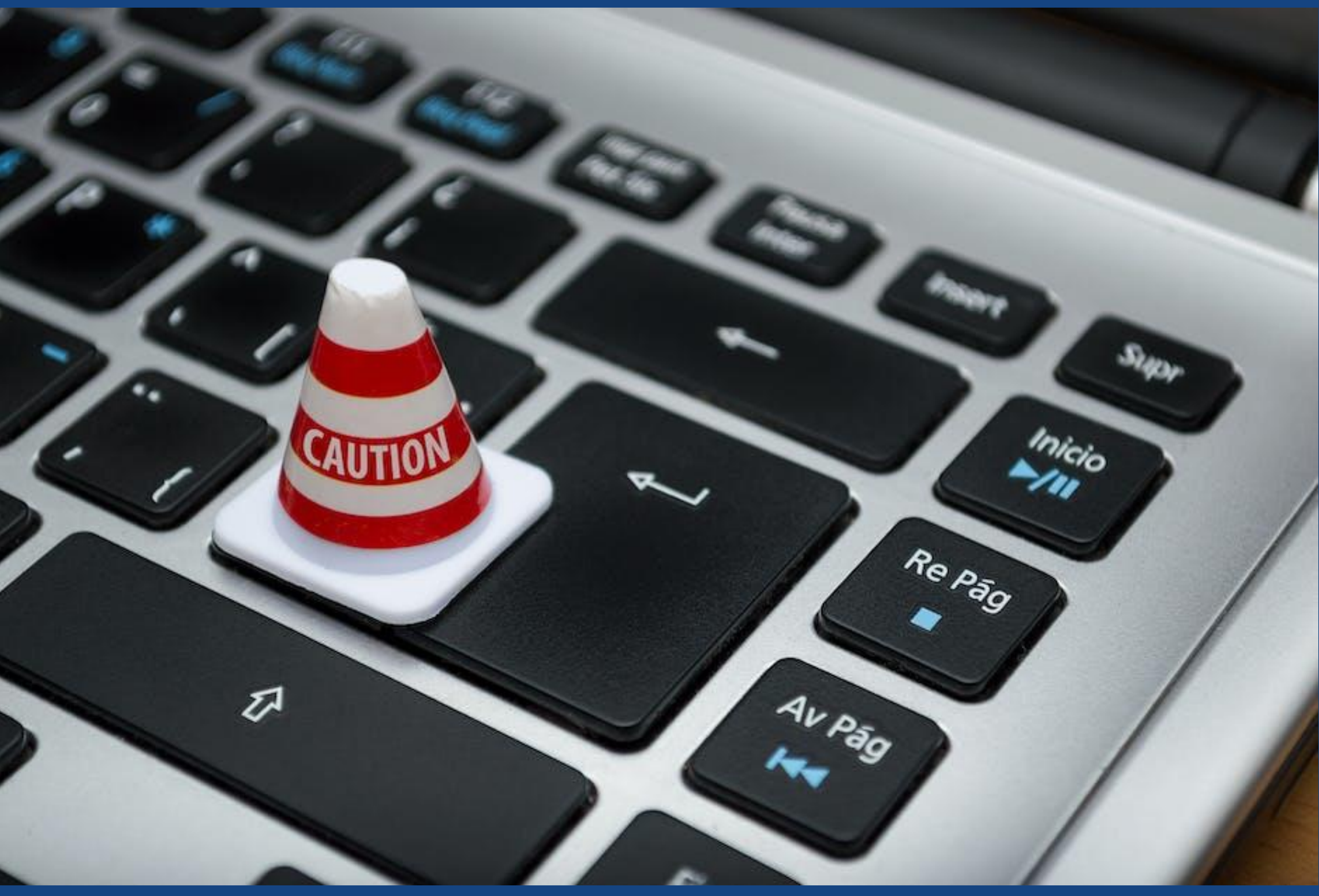
Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA

Acelera *pyme*

The **objectives of this monograph** are to **provide** SMEs and freelancers with a clear and concise **overview of the main risks and threats** in the field of cybersecurity, as well as to **offer guidelines and practical advice** to reduce risks and protect their data and information. It focuses on the current situation of cybersecurity in the business environment and is aimed at those companies that do not have sufficient resources in cybersecurity or have limited knowledge in this area. It will address topics such as data protection, the most common threats, the **importance of awareness** and **good practices**, as well as the description of accessible and more effective cybersecurity tools and technologies for SMEs and freelancers to protect themselves from risks and threats.



Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA

Acelera pyme

2. Cybersecurity awareness

Now, and increasingly so, it is **essential to raise awareness** of the importance of cybersecurity among all users. Cybersecurity is not something that should only **concern** large companies, but **all types of businesses**, large or small. For all businesses it should be crucial to protect the personal data of the company, customers and suppliers, avoid financial losses, secure the reputation of the business while complying with regulations. No one is completely safe from a cyber attack, however, **different measures can be implemented to minimize the risks as much as possible**. For example, well-known institutions and companies [REF-05] such as the Spanish Public Employment Service (SEPE) have suffered attacks, paralyzing the entire computer system and, consequently, causing delays in managing appointments and delaying unemployment benefit payments. The Spanish home delivery company, Glovo, also suffered a cybersecurity attack, in which they were able to access customer and delivery drivers' account data. Similarly, cybercriminals gained access to sensitive data of the chain's customers. All this led to **reputational damage** for these companies, which may also **seriously affect** their **revenues**. More recently, in March 2023, the Hospital Clínic de Barcelona suffered a ransomware cyberattack in which patient and employee data was stolen and a ransom was demanded in exchange for not publishing the data **[REF-06]**. Currently the Catalan Data Protection Authority (Autoritat Catalana de Protecció de Dades (Apdcat) has initiated a preliminary investigation in order to determine whether appropriate measures have been implemented to safeguard the security of the data they held **[REF-07]**.

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA

Acelera pyme

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

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

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

Exchange information with other agencies and associations to prevent the most common or most recent attacks. This is also very important, as there are constantly new and increasingly ingenious threats.

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

Fondo Europeo de Desarrollo Regional

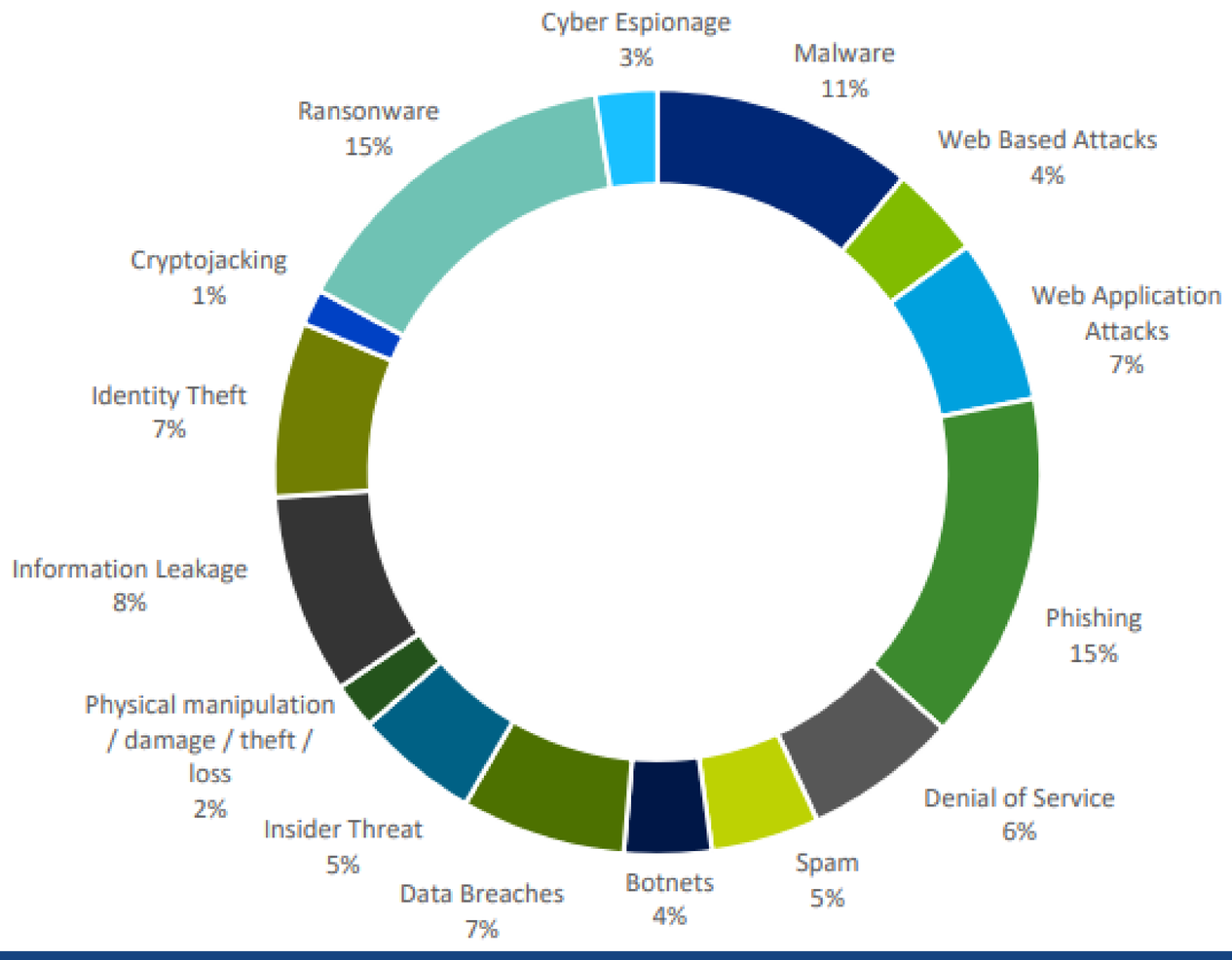
"Una manera de hacer Europa"

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA

3. Most common cybersecurity threats:

After establishing actions to promote cybersecurity awareness, it is important to understand the **common threats faced by SMEs and the self-employed**. A Deloitte study entitled "The State of Cybersecurity in Spain 2023" **[REF-08]**, indicates that the three most common threats are ransomware (15%), phishing (15%) and malware (11%). In addition to these three threats, there are many more types of cyber threats that SMEs and freelancers can suffer. It is therefore essential that they are **familiar** with the different types of existing threats so that they can **take appropriate measures** to prevent possible attacks by cybercriminals.

Porcentaje de ocurrencia de ciberamenazas en 2022



The state of cybersecurity in Spain. Deloitte Spain. https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html

Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"
GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA

For its part, **INCIBE** makes available to anyone interested **free** of charge on its website different guides **to prevent different attacks** and **how to act** in the event of suffering one. In this regard, there is a guide published entitled "Ciberamenazas contra entornos empresariales - Una guía de aproximación para el empresario" **[REF-09]**. This guide includes the **main types of threats** that exist and what they mean:

1. **Information leaks:** this refers to the unauthorized or accidental disclosure of a company's confidential data, which can result in loss of data privacy, reputational damage and potential legal consequences.

2. **Phishing attacks:** these attacks are intended to trick users into revealing personal information, such as passwords, credit card or bank account details, through forged communications that appear to come from a known and legitimate source, such as a bank or well-known company.

3. **CEO fraud (spear phishing):** as the name suggests, this fraud involves the well-planned impersonation of a senior executive for the purpose of stealing corporate funds.

4. **HR fraud:** similar to CEO fraud, this is identity theft, but this time of an employee, the victim being the human resources department of a company.

5. **Sextortion:** this threat is better known and involves threatening the victim to share compromising images of the victim with his or her entourage unless payment is received.

6. **Attacks against the corporate website:** this consists of attacking a company's website in order to damage its image, obtain economic benefits or steal personal data, for example.

Acelera pyme

7. **Ransomware:** this attack locks information on an electronic device, quickly propagates and requests an economic ransom in order to free the information.

8. **Fake Microsoft support fraud:** it starts with a call from a supposed Microsoft employee reporting device security errors with the aim of gaining access to confidential company information.

9. **Email campaigns with malware:** they include files or links with hidden malware to introduce different types of malware in the devices.

10. **Denial-of-service (DoS) attacks:** these are cyber attacks that seek to interrupt or block access to a system, service or network by overwhelming it with a large number of requests or traffic, exhausting its resources and making it inaccessible. They can end up generating economic losses and damage to the reputation of the affected organization. Methods used include mass mailing of requests, flooding network traffic and exploiting vulnerabilities in the target software.

11. **Adware attacks:** as the name suggests, these are attacks that intrusively display advertisements in order to generate revenue.

12. **Vendor spoofing attack:** in this case it is also a spoofing attack, however, to a service provider, getting the victims to transfer money to the cybercriminals instead of to the real provider.

It also explains in more detail what these threats consist of, how to identify them and how to act in the event of suffering any of these attacks.

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA

4. Data protection and practical tips for cybersecurity implementation

When talking about cybersecurity, many people are not fully aware of what data can be subject to attack by **cybercriminals**, however, it is **crucial to know** them, in order to be able to protect themselves adequately. Below is a list of **data that is susceptible to theft** by cybercriminals:

Confidential or privileged corporate information

Customer information (contact details, order history and purchasing preferences, bank account details, etc.)

Supplier information (company information, details of business transactions, financial information, confidential business contracts and agreements, etc.)

Employee information (employee personal information, work lives, social security data, payroll, etc.)

Passwords

Now, knowing this information, what measures can SMEs and freelancers carry out to protect such data? In this regard, there are a series of **basic guidelines** proposed by Panda Security, a company specialized in offering cybersecurity products and services, which **should be followed by any SME or freelancer**, such as **[REF-10]**:

Acelera pyme

1. **Use unique passwords** (at least 12 characters long, containing uppercase, lowercase, numbers and special characters (%&$#) and containing no personal or company information in it) for each type of account and try to change them at a recommended frequency of at least 45 days.

2. Where possible, use **multi-factor authentication** to ensure advanced identity verification.

3. **Use a firewall** to prevent unwanted access to the SME's devices.

4. Ensure that the **operating system is always up to date**, as well as the browsers and software used to reduce the risk of cyber-attacks.

5. If possible, **avoid connecting to public Wi-Fi, and activate the VPN** (there are many free and available) in order to have a secure connection at all times and minimize risks.

6. Check that the links accessed on the web always have "**https**" at the beginning of the link instead of "http".

7. In all the installed programs that allow it, to **enable the privacy configuration or to increase it** in those that it is possible.

8. Be **cautious about what personal information you share and where**, as it can give cybercriminals clues to guess passwords.

9. Of course, **only download verified software from trusted sources**, as pirated programs often contain malware and are not legal.

10. Make sure to **regularly perform backups** to the cloud or external drives in order to prevent ransomware and data loss.

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA

Regardless of the above, starting to apply cybersecurity measures has to be accompanied by an organized and measured implementation in order to ensure that it is carried out correctly. Therefore, the **following strategies** are proposed:

- **Develop a cybersecurity plan:** preferably a comprehensive plan should be created that addresses policies, procedures and actions to protect the company's systems and data.

- **Establish an incident response:** Similar to the cybersecurity plan, an incident response plan should be prepared and practiced to quickly and effectively address any security incidents that may occur.

- **Establish security policies:** Define and clearly communicate the SME's security policies, such as the appropriate use of devices and resources, information privacy and staff responsibilities in terms of security.

- **Implement technical security measures:** Establish security protocols and measures, such as two-factor/multi-factor authentication, data encryption, regular software and operating system updates, and regular backups of relevant data.

- **Train and raise employee awareness:** Inform employees about good cybersecurity practices, such as the correct identification of phishing attacks, secure use of passwords and identification of potential threats.

- **Keep software up to date:** Ensure that all systems, applications and devices used are up to date with the latest security patches and updates provided by the vendors of these softwares.

- **Perform regular backups:** Make regular backups of important data and store the backups in secure locations outside the main business network.

Within these measures, it is essential to **reduce the digital footprint** as much as possible, thus limiting the personal information of the self-employed or SME shared on the Internet, and controlling well the information that is shared (consciously or unconsciously) on the Internet and social networks. This helps to **mitigate the risk of exposure of sensitive dat**a and contributes to **strengthening cybersecurity** in SMEs and freelancers. While it is true that it is not possible to eliminate the digital footprint completely, INCIBE recommends following a **series of steps to help minimize it as much as possible [REF-11]:**

1. **Do not upload images of compromised places** in the office (server rooms, security access, etc.).

2. **Avoid taking pictures of the workstation** and less of the computer screen on.Delete data from documents before uploading them to the network.

3. **Use browsers [REF-12] that have features to minimize the digital footprint** as much as possible (e.g. Firefox, Brave, DuckDuckGo, Tor).

4. **Employ** a **VPN to better protect information**.

5. **Raise awareness among employees** to prevent information leaks (they are the main source of leaks due to malpractice and lack of knowledge).

In addition, INCIBE also provides users with information, guidelines and specific advice **[REF-13]** according to the type of sector they belong to (from education, health, tourism and leisure to retail, for example).

In summary, **data protection and the implementation of cybersecurity measures are key issues** for SMEs and the self-employed at this time. Aspects such as reducing the digital footprint, increasing employee awareness and adopting security tools such as VPNs are essential actions to safeguard confidential information and strengthen the cybersecurity of an SME. By following these tips and taking advantage of available resources, SMEs and freelancers will be **better prepared to face existing cybersecurity threats** and will be able to **better protect their business and customer data**.

5.Cybersecurity tools and technologies

There are different options available to companies and freelancers that INCIBE publishes completely free of charge, such as the Glossary of cybersecurity terms - An approach guide **[REF-14]** for the entrepreneur that includes a definition of all the terms of the subject.

On the one hand, on the INCIBE website, there is a risk analysis test [REF-15] that can be taken by anyone that is going to help them assess their cybersecurity status. On the other hand, on the Acelera pyme platform itself, after logging in, any user can carry out a cybersecurity self-assessment [**REF-16]** to find out the state of maturity of cybersecurity in their company.

In terms of **specific tools**, the following is a list of free or low-cost firewall, antivirus, etc. software:

Antivirus [REF-17]:

- **Bitdefender Antivirus Free [REF-18]**: Enables outstanding anti-malware protection, with high threat detection and efficient blocking of malicious web pages. It also offers strong anti-phishing protection, blocking a high percentage of illegitimate pages. It is a free antivirus that is easy to use and does not slow down computer performance.

- **Avast Free Antivirus [REF-19]**: It stands out for its high detection of viruses and malicious web pages, reaching 99.96% and 99.67% respectively. It also offers great protection against phishing, blocking 93% of attempts. However, it is ad-heavy and lacks additional features such as parental control, VPN, password manager and banking protection. Nevertheless, it can be combined with other tools listed in this section.

Firewall [REF-20]:

- **Windows Defender:** this firewall comes by default installed in the Windows 10 operating system, so it already has many basic benefits.

- **ZoneAlarm [REF-21]**: is compatible with Windows systems and is a free solution that monitors the activity of programs on computers. It protects users' identities from hackers and offers security tools for surfing unsecured networks. Its Web Secure feature, which provides additional protection while surfing the Internet, is particularly noteworthy.

- **Comodo Free Firewall [REF-22]**: allows you to monitor traffic, detect suspicious connections and disinfect your PC if necessary. In addition, it offers features such as custom DNS servers, ad blocker and protection against suspicious activity. It has a simple interface and has the ability to hide ports and block suspicious software.

VPN [REF-23]:

- **Hotspot Shield [REF-24]**: one of the most recommended and popular free VPNs, which allows the service to be used on up to five devices with a single account and offers up to 500 MB per day. It stands out for its ease of use and secure data encryption. However, the free version has ads and does not allow you to select the server location, as it connects randomly.

- **ProtonVPN Free [REF-25]**: this VPN is indicated for those cases in which the amount of data is a priority, since it has unlimited data in its free version, however, it can only be used on one device at a time and only has three locations for its servers. On the other hand, it is not necessary to log in to use it, thus minimizing the digital footprint even more.

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA

Password Manager [REF-26]:

- **1Password:** a secure, easy-to-use password manager with a wide range of features and offers a 14-day free trial. It provides affordable plans for both individual users and families. In addition, it offers a version designed specifically for businesses, which is priced at $7.99 per month. This enterprise version not only has secure password management, but also seamless integration with other tools used in corporate environments.

- **LastPass [REF-27]:** has a 14-day free trial and its basic paid enterprise version is priced at €3.90 per user per month and includes a number of additional features, such as the ability to have up to 50 users, password-free login, shared folders, multi-factor authentication (MFA), a security dashboard and the ability to monitor hacking attempts.

6. Conclusion

In conclusion, this monograph explained the importance of cybersecurity for SMEs and the self-employed, offered indications on how to promote **awareness in the field of cybersecurity**, giving **real examples** of attacks on the State Public Employment Service (SEPE) and the Spanish home delivery company, Glovo. In addition, emphasis was placed on the importance of knowing the **different types of existing threats** and their **consequences**, such as **ransomware**, **phishing** and **malware**.

Further on, it has been specified which data can be subject to **theft by cybercriminals** such as **personal**, **financial** and **commercial** information that can have serious repercussions for both the company and the affected individuals. In terms of measures to be taken, specific advice has been provided for SMEs and the self-employed. These include implementing a **cybersecurity plan**, using **strong passwords**, performing **regular backups**, **updating software** or **even reducing the digital footprint**. In addition, the importance of having cybersecurity tools such as **antivirus**, **firewalls** and **VPNs** has been highlighted, and some free or low-cost options that SMEs and freelancers can use have been mentioned.

SMEs and freelancers need to be aware that cybersecurity is a **critical aspect** that cannot be ignored. Implementing protective measures, raising employee awareness, protecting data and keeping up to date with the latest threats are **fundamental steps to safeguard information** and ensure business continuity to avoid serious consequences. In this regard, it should be emphasized that cybersecurity should be seen as an investment, not an expense, as the costs associated with a **security breach** can be much higher. With a **solid cybersecurity strategy** in place, SMEs and freelancers will be better prepared to face the challenges and protect their business in the digital era.

Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"
GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA

7. References

[REF-01] – INCIBE. +118.820 incidentes gestionados fraude online. https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2022_incibe.pdf

[REF-02] – CSO España. El cibercrimen crece en España y se profesionaliza en 2022. (1 November, 2022). https://cso.computerworld.es/reportajes/el-cibercrimen-crece-en-espana-y-se-profesionaliza-en-2022

[REF-03] – Group, I. D. M. España es el séptimo país más ciberatacado por ransomware en 2022. (7 December, 2022). https://www.itreseller.es/seguridad/2022/12/espana-es-el-septimo-pais-mas-ciberatacado-por-ransomware-en-2022

[REF-04] – Índice de la Economía y la Sociedad Digitales (DESI). (2022) https://espanadigital.gob.es/sites/espanadigital/files/2022-08/DESI%202022%20Espa%C3%B1a.pdf

[REF-05] – Unión Alcoyana Seguros. Ejemplos de ciberataques en empresas españolas y consecuencias. (13 July 2022). https://unionalcoyana.com/consecuencias-ciberataques-en-empresas-espanolas/

[REF-06] – Fontserè, C. B., Sara. El ciberataque que sufre el Hospital Clínic de Barcelona procede del extranjero y obliga a anular 3.000 visitas. El País. (6 March, 2023). https://elpais.com/espana/catalunya/2023-03-06/el-ciberataque-que-sufre-el-hospital-clinic-de-barcelona-procede-del-extranjero.html

[REF-07] – Press, E. La Apdcat abre un expediente por el ciberataque al Hospital Clínic y sus entidades. Www.europapress.es. (22 June, 2023). https://www.europapress.es/catalunya/noticia-apdcat-abre-expediente-ciberataque-hospital-clinic-entidades-20230622141451.html

[REF-08] – El estado de la ciberseguridad en España. Deloitte España. https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html

[REF-09] – Ciberamenazas contra entornos empresariales. https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberamenazas_contra_entornos_empresariales.pdf

[REF-10] – Panda Security Mediacenter. 10 consejos de seguridad en el Mes de la Concienciación sobre la Ciberseguridad. (10 October, 2018) https://www.pandasecurity.com/es/mediacenter/panda-security/consejos-mes-ciberseguridad/

[REF-11] – INCIBE. Como Evitar Que La Huella Digital Afecte Nuestras Empresas | Empresas https://www.incibe.es/empresas/blog/como-evitar-que-la-huella-digital-afecte-nuestras-empresas

[REF-12] – AndroidTR. *Cómo minimizar tu huella digital*. (9 March, 2023). https://androidtr.es/como-minimizar-tu-huella-digital/

[REF-13] – INCIBE. Sectoriza2 | Empresas (https://www.incibe.es/empresas/sectoriza2

[REF-14] – Glosario de términos de ciberseguridad. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

[REF-15] –INCIBE. Instituto Nacional de Ciberseguridad. Adl.incibe.es. Autodiagnóstico ligero, https://adl.incibe.es/

[REF-16] – Acelera pyme. ¿Quieres conocer el grado de digitalización de tu pyme? https://www.acelerapyme.es/quieres-conocer-el-grado-de-digitalizacion-de-tu-pyme

[REF-17] – Proteger el ordenador con antivirus gratuitos. https://www.ocu.org/tecnologia/antivirus/consejos/antivirus-gratuitos

[REF-18] – Bitdefender. Líder mundial en software de seguridad informática. https://www.bitdefender.es/

[REF-19] – Avast. Descargar Free Antivirus y VPN | 100 % gratis y sencillo. https://www.avast.com/es-es/index

[REF-20] – ADSLZone. Los mejores cortafuegos para tu ordenador Windows 10. https://www.adslzone.net/listas/mejores-programas/cortafuegos-firewall/

[REF-21] – ZoneAlarm. *PC and Mobile Security Software*. https://www.zonealarm.com/

[REF-22] – Comodo. Free Firewall | Get Award Winning Comodo Firewall Today. https://www.comodo.com/home/internet-security/firewall.php

[REF-23] – Fernández, Y. Xataka. VPN gratis: las 7 mejores con las que conectarte ocultando tu IP o desde otro país. (28 June, 2022). https://www.xataka.com/basics/vpn-gratis-mejores-que-conectarte-ocultando-tu-ip-otro-pais

[REF-24] – Hotspotshield. Descargue ya la VPN de Hotspot Shield para navegar por Internet de forma privada y segura, acceder a sitios web bloqueados y mucho más. https://www.hotspotshield.com/es/

[REF-25] – Proton VPN. VPN gratuita sin anuncios ni límites de velocidad. https://protonvpn.com/es/free-vpn

[REF-26] – SafetyDetectives. Los 7 mejores gestores de contraseñas (GRATIS) en 2023. (12 April, 2021). https://es.safetydetectives.com/blog/the-best-free-password-managers-es/

[REF-27] – LastPass. Precios por plan. https://www.lastpass.com/es/pricing?pill=business

Acelera pyme

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

UNIÓN EUROPEA