

TECHNICAL INFORMATION FOCUSED ON BUSINESS TRENDS AND THE CREATION OF NEW TECHNOLOGICAL-BASED COMPANIES

DIGITAL SECURITY

IN NEW BUSINESSES



IAPMEI



Powered by CAPACITAR PARA EMPREENDEDOR

TABLE OF CONTENTS

INTRODUCTORY NOTE DIGITAL SECURITY CHALLENGES Increasingly sophisticated threats require organizations to constantly and expensively invest in IT security to protect their data and information. The pressing need for legal regulation in the digital world requires companies to adapt to complex processes with the adoption of new technologies.	4
CHAPTER 1 THE INTERNET AND NEW BUSINESSES The web presence is a differentiating factor for any business, as it provides an agile and borderless means of communication. Small businesses should be encouraged to ensure their presence on the Internet from the start.	6
CHAPTER 2 DATA AND INFORMATION 'Data' is a raw element that, without the correct interpretation, does not express any meaning. Information can be understood as data within a context that allows for the attribution of meaning, abstracting the simple mathematical symbol and elevating it to an understanding at the level of logical and human reasoning.	10
CHAPTER 3 GENERAL DATA PROTECTION LAW General Data Protection Regulation (GDPR) presents a unique set of rules regarding the protection of individuals related to the processing of personal data and the free movement of the same. Companies established in the EU are subject to its application, irrespective of their location.	17
CHAPTER 4 DIGITAL SECURITY Digital Security (DS) describes the features used to protect online identities, data, and other assets. These tools include web services, antivirus software, smartphone SIM cards, biometrics, and secured personal devices. Digital security is the process used to protect an online identity or other sensitive information.	19
CHAPTER 5 THREATS AND RISKS The more the company depends on Information Technologies, the more important it is to identify and control the risks related to its IT assets to avoid potential damage to its business.	21

TABLE OF CONTENTS

CHAPTER 6 | SOLUTIONS AND TRENDS In the digital age, the need for digital security implies the search for effective security solutions (updated platforms and software packages) that guarantee the trust of those responsible for companies regarding their businesses and their data. A set of solutions and trends are referred to as investments in the area of digital security.

33

CHAPTER 7 | CASE STUDIES Examples of case studies of startups linked to the area of digital security, in which their businesses are related to services in terms of Security, Fraud, and Validation. These cases are related to Portuguese, European, and Brazilian startups.

37

GLOSSARY

42

REFERENCES

45

TABLE OF CONTENTS OF PHOTOGRAPHS, FIGURES, AND TABLES

47

INTRODUCTORY NOTE

The challenges of Digital Security

History shows that society experiences technological leaps that allow a change in the way of life, namely through the creation of innovative products, processes, and services. Some discoveries leveraged a rapid development of society: the steam engine was one of the great leaps, which allowed the industrial revolution in 18th century England, and which aimed to replace human labor with machines that performed the same functions with greater efficiency.

Since then, new technologies have emerged and are part of the change in the daily life of the human species. A new technological leap was given with the discovery of semiconductors and their evolution, implying the appearance of computers.

The use of computers and their computing power are increasingly present in commercial and industrial operations and personal life, implying a **fast-growing consumption of data processing**, storage, and transport resources (information).


Information is a necessity to be **accessed anytime and anywhere**. People and companies invest in information and communications technology (ICT) equipment and services to be used in their personal and professional activities, from simply storing travel photos to the financial control of an organization.

Maintaining an **ICT infrastructure** is not a simple task and often has relatively high costs. This type of infrastructure requires investments in communication equipment, storage, and other systems which, in addition to the initial cost of their acquisition, imply complexity in their implementation, management, and maintenance, requiring qualified professionals and, consequently, also operating costs.

Some companies stand out in the development of products and systems to support personal and professional activity, and/or their implementation and maintenance, such as, e.g., operating systems, text editors, applications, written communication systems (spoken and television), specific platforms (for niche markets), etc., favoring the performance of companies in new types of business.

On the other hand, there are tools and complete platforms distributed in open source, free to use, with models and architectures in the cloud that can perfectly fulfill the designed functions with a high degree of quality and a relatively low cost.

In the digital context, computer security is a topic in constant development. Threats are increasingly sophisticated and require organizations to make a constant and costly investment to protect data and information. The emergence of a regulatory system has an impact on the management of technologies, requiring companies to adapt to complex processes with the adoption of (typically) high-cost technologies.

Investments in data protection are often leveraged, either by the growing concern about threats in the digital universe, as explained in the '[Report – Cybersecurity in Portugal – 2020 Society](#)' (CNCS - 2020 Society Report, [s.d.]), or by the obligations in the compliance with rules, laws, and regulations. Regardless of the reasons, the fact is that family businesses, small businesses, and, in a very special scenario, Startups, have to adapt to offer the necessary security to their customers and their business. 

In this e-book, **Digital Security (DS)** will be addressed as a set of measures necessary to **guarantee the integrity of information**, whose theme may interest the most diverse professional profiles (promoters, managers, and employees) and businesses, including 'small companies ', 'family businesses' and 'Startups'.

It is important to point out that any **Information Security** work must be conducted through a careful analysis to be developed specifically for the target environment. The tips, examples, and recommendations presented in this e-book are intended to provide knowledge to perform critical analysis in each environment, identify potential weaknesses, and help find effective protection solutions for your data and that of your customers.

Keywords: antimalware, antivirus, authentication, cybersecurity, data classification, data, encryption, information, malware, organizations, data protection, digital security, startups.

1. THE INTERNET AND NEW BUSINESSES

The presence on the internet is a differentiating factor for any business, as it provides an agile and borderless means of communication. Small businesses should be encouraged to ensure their presence on the Internet from the start.

Photo by [Pickawood](#) on [Unsplash](#)

News, digital marketing, and personal and commercial communications are a constant with information that is broadcast all over the world. Currently, information flows at high speeds due to the entire existing **communication infrastructure** (from fixed to land mobile and satellite systems). Online products and services generate, daily, a veritable avalanche of information.

Society has changed behaviors as a result of the democratization of mobile technologies and the internet and is, therefore, increasingly interconnected. As an example, until 2008, a typical audience at a musical show carried the memories of the event with them. With the insertion of smartphones and the growing connectivity of these devices with the world wide web, and the Internet, public participation in events began to be disseminated in real-time, thus generating a flow of transmission of images and personal data unprecedented in the history of technologies.

Care and responsibilities with copyright, image rights, and personal information must always be taken care of so that they are not the subject of future claims and legal proceedings.

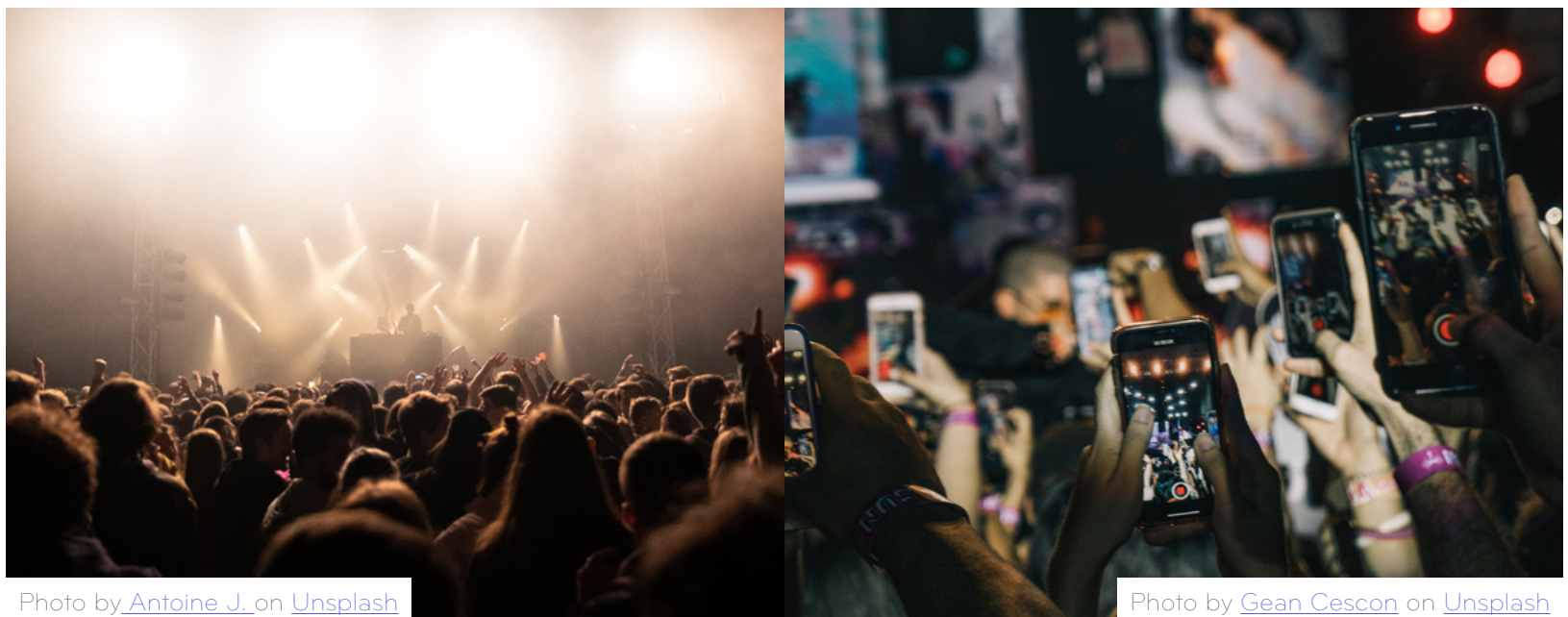


Figure 1.1. Digital access between 2005 and 2013

The perception of connectivity in current events is remarkable. The digital age is consolidated in this period. Some people are **browsing the "net"** and with access to a huge amount of information in close to real-time, opening a universe of opportunities, on the other hand, due to the volume and value of information, more complex **digital threats** also arise and robust.

Internet presence is an enormous value for any **business** and **e-commerce** has grown at an accelerated pace, as shown by statistics published by [INE](#).



In 2020, 61.5% of companies with 10 or more employees have a website.

Source: Instituto Nacional de Estatística

The presence on the internet is a differentiating factor for any business, as it provides an **agile and borderless means of communication**. Small businesses should be encouraged to ensure their presence on the Internet from the start.

However, small businesses cannot always make the necessary investment to have their digital presence infrastructure or platform. As a solution to this scenario, **cloud-based e-commerce tools**, commonly referred to in English as cloud, share resources between several customers, offering products and services at more affordable prices.

Sales of goods and services carried out through **e-commerce**, as a % of the total turnover of companies with 10 or more employees, for Portugal and the EU-27.

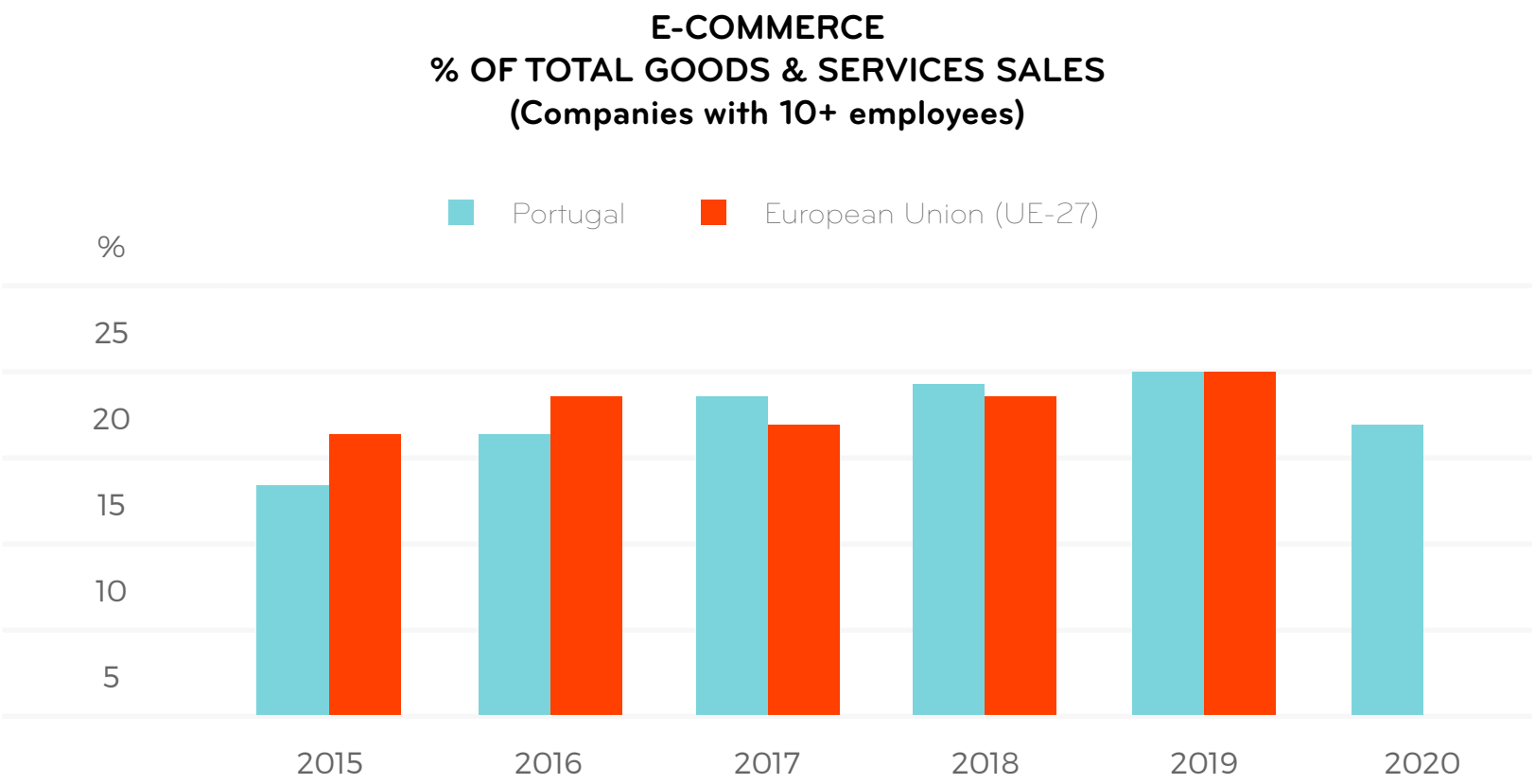


Figure 1.2. Information and Communication Technologies usage in Enterprises.
Source: INE & Eurostat,

The description of products or services and price lists was the most available feature on the websites.

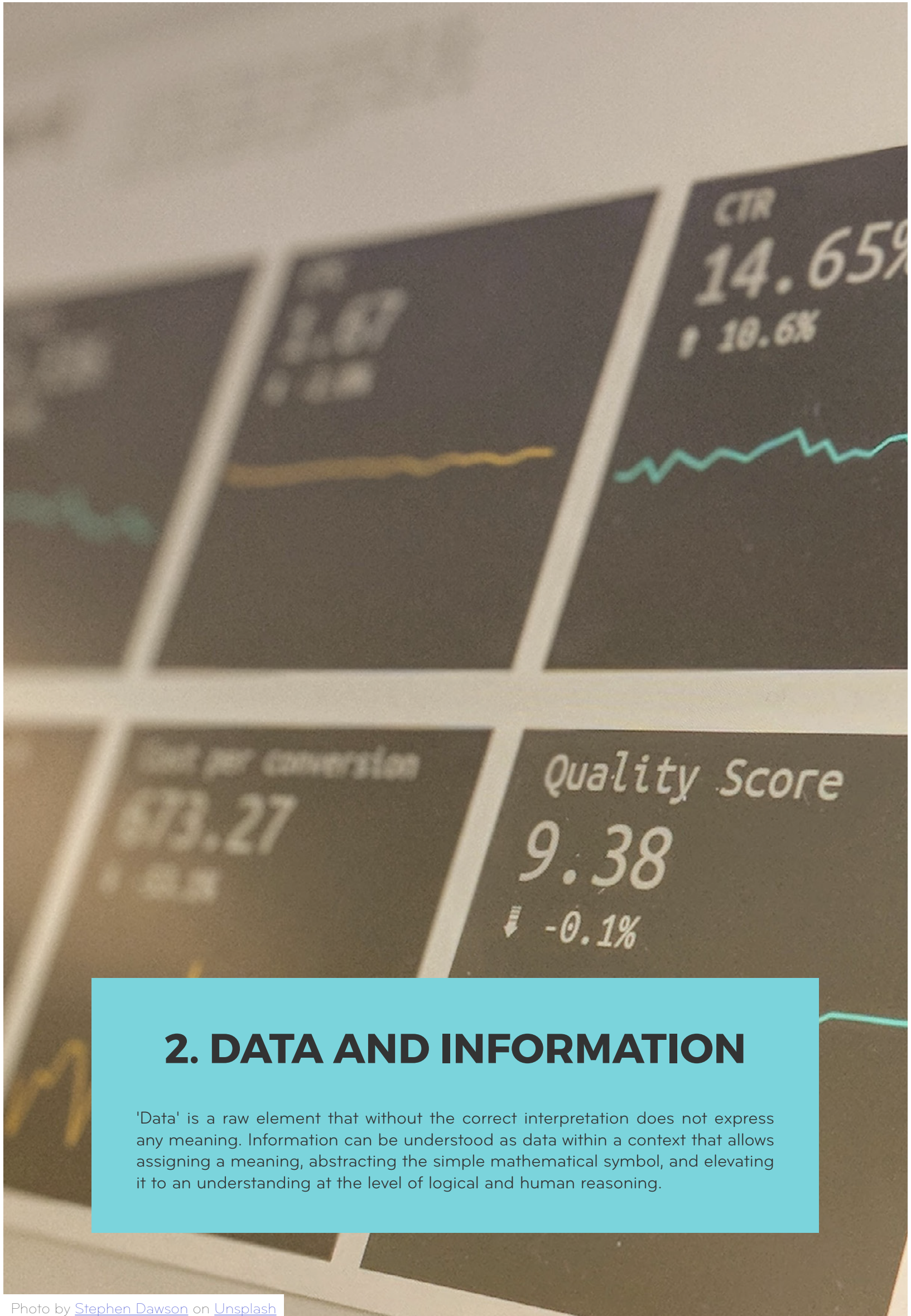
Source: Instituto Nacional de Estatística

Note: In 2020, in the context of the COVID-19 pandemic, 21.3% of companies started or increased efforts to sell goods or services via the Internet and 24.0% increased their investment in ICT. However, sales of goods and services through e-commerce in Portugal represented 17.0% of total turnover in 2020, 2.8 p.p. less when compared to the previous year. This result was influenced by the reductions observed in accommodation and transport services and by the reduction of transactions between companies, reflecting the contraction of economic activity because of the pandemic.

In general, the term information is closely linked to knowledge. It will be said that whoever has access to a greater amount of information has greater knowledge. In terms of business and relationships between organizations, this translates into obtaining advantages over other organizations, which may be of a political, financial, economic, or technological nature.

Threat prevention contributes decisively to the **security of an organization** and therefore assumes (in this context) a central role; effective prevention makes it possible to take all the necessary actions **to prevent or combat any threat**, and this is only possible through a **well-structured information service**.

In addition to financial factors, digital insecurity, derived from widely publicized events, e.g., the **unauthorized collection of personal data**, **hacker movements**, and **threats such as viruses**, triggers in customers the need to look for companies with specialized skills in information security recognized, through **certification seals** and disclosed in public bulletins, which offer trust and guarantee in the services and confidentiality in the treatment of data.



2. DATA AND INFORMATION

'Data' is a raw element that without the correct interpretation does not express any meaning. Information can be understood as data within a context that allows assigning a meaning, abstracting the simple mathematical symbol, and elevating it to an understanding at the level of logical and human reasoning.

Photo by [Stephen Dawson](#) on [Unsplash](#)

To contextualize the security landscape, it is necessary to understand what data and information are. In the article by SETZER, entitled "Data, Information, Knowledge and Competence", data is defined as:

«...a sequence of quantified or quantifiable symbols. Therefore, a text is data. Letters are quantified symbols... a datum is necessarily a mathematical entity and, therefore, is purely syntactic. This means that data can be fully described through formal, structural representations. Being still quantified or quantifiable, they can be stored in a computer and processed by it.»

Setzer, 2021

Therefore, data is a means of encoding, storing, and transporting information. Data may contain personal and sensitive information.

From this approach, it is understood that **data is a raw element**, represented mathematically and that, without the correct interpretation, does not express any meaning, being the data capable of containing information.

The concept of **information** finds several definitions in the academic literature, but it is consensual to assume that, within companies, it can be understood as a **set of data integrated** into a context, which allows attributing a meaning, abstracting from the simple mathematical symbol, which then raises an understanding at the level of logical and human reasoning.

2.1. Personal data


Personal data must be especially observed and protected. According to [European Comission](#) (What is personal data?, [n.d.]), personal data contain "information relating to a living, identified or identifiable person. Personal data is also the set of distinct information that can lead to the identification of a particular person." (Table 2.1) 

Table 2.1 Data: Personal, Sensitive and Common

PERSONAL DATA		
What are personal, sensitive and common data		
PERSONAL DATA	SENSITIVE DATA ¹	COMMON DATA
<ul style="list-style-type: none">• Name• e-mail (jhon.doe@acme.com)• Phone number• Home address• IP Addresses• Cookies	<ul style="list-style-type: none">• Criminal records• Medical records• Race or ethnicity• Sexual orientation• Religion	<ul style="list-style-type: none">• Business phone number• e-mail (info@acme.com)• Anonymized data• Company information• Data of a dead person

¹ Sensitive data is personal data that requires special treatment.

2.2. Data classification

The **information can be classified** based on its domain, that is, grouped according to the target audience, the relevance of its content and the restrictions applied, finding in the literature, several models, and information segmentations.

Information is all knowledge that can be communicated, and which has been assigned a security rating to protect against unauthorized disclosure.

The disclosure of classified information, irrespective of its material format or mode of transmission, may have generally adverse consequences for the interests of the organization.

The **classification of information** (*Data Classification, 2016*) consists of identifying the type of data and defining the levels of protection that each data should receive, e.g., **open data**, **internal data**, **industry data**, and **confidential data**.

Several models were created to establish a classification of data that allows the process of the information and applies the appropriate control. An example classification might contain the following levels of information:

PUBLIC	Information that can be made public, without significant harmful consequences for the normal functioning of the company, so its integrity is not vital.
INTERNAL	Free access to this type of information should be avoided, although the consequences of unauthorized use are not serious. Integrity is important, even if it's not vital.
CONFIDENTIAL	Information restricted to the company's limits, the disclosure or loss of which may lead to operational imbalance and, eventually, to financial or reliability losses vis-à-vis external customers.
SECRET	Critical information for the company's activities, whose integrity must be preserved at any cost, and its access must be restricted to a small number of people. The security of this type of information is vital for the company.

A base policy for a data classification model should minimally meet the following criteria:

- Be direct and avoid ambiguity. However, the policy used must be generic enough to apply to **different assets in various contexts**;
- Be clear and **written simply**;
- Be aligned with the **organization's business**;
- Contain few pages and have no more than three or four **rating levels**;
- Contain the point of contact for the most diverse cases and situations that employees may face;
- Contain a **review agenda**.

2.3. Data protection

Data protection consists of creating **security controls** for classified data of a personal nature, or any other sensitive data for the business. For example, the company's financial reports must have access control and be kept in the custody of protection technologies.

Especially after the approval of the [General Data Protection Law \(LGPD\)](#) in [Brazil](#) and the entry into force of the [General Data Protection Regulation \(GDPR\)](#) in [Europe](#), some countries require extraordinary data protection measures, on the part of partners and investors who collect information from their citizens.



To minimize risks, data strictly necessary for the business must be collected, kept securely, with access records, and **transmitted only by secure means**. In cases of disaster, data recovery must be performed to have all the information restored in time to minimize the impact on the business.

2.4. Business continuity and disaster recovery

Organizations that have a [business continuity plan](#) (well thought out and structured) guarantee their ability to respond in the event of unexpected events and, consequently, the sustainability of their business.

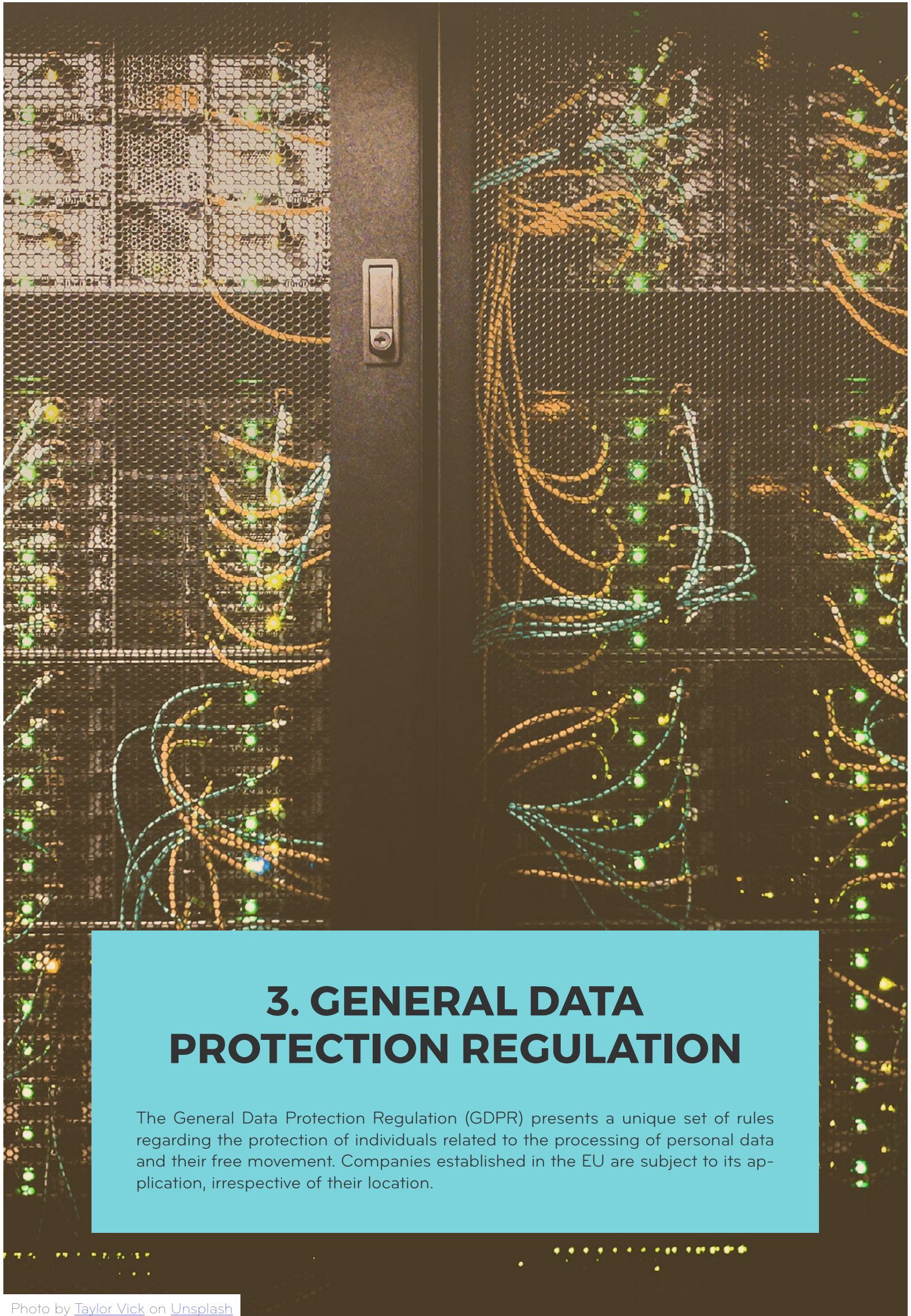


There are no closed formulas that guarantee an “**effective antidote**” in case an organization is affected by a **cyberattack**, a **natural catastrophe**, or a **terrorist attack**. But there are investment decisions that can only be taken if there is knowledge of the resources available so that a manager can consciously prepare his company better for the eventualities of the future.

2.5. IT Architecture

The alignment of business needs with technologies depends on the structure of the IT Architecture as an information technology competence that ensures that processes and technological solutions are adequate to the needs of organizations, generating compliance and alignment with strategic objectives and, therefore, on the other hand, ensuring that the IT area is contributing to quickly benefit the **design of the business model**, processes and technologies, namely to:

- Plan **appropriate infrastructure** architectures for the business;
- Dealing with already implemented systems and integrating them with **new technologies**;
- Implement a new storage system with **data classification**;
- Ensuring responsible handling of **data in the organization**;
- Implement and manage **efficient and innovative solutions**;
- Implement physical and virtual networks, routers, firewalls, and servers.



3. GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) presents a unique set of rules regarding the protection of individuals related to the processing of personal data and their free movement. Companies established in the EU are subject to its application, irrespective of their location.

Photo by [Taylor Vick](#) on [Unsplash](#)



- ✍ The [General Data Protection Regulation](#) (GDPR) presents a unique set of rules regarding the protection of individuals, the **processing of personal data**, and the free movement of such data. Companies established in the EU are subject to its application, regardless of their geographical location (*IAPMEI - General Data Protection Regulation*, [s.d.]).
- ✍ In [article 30](#), the GDPR defines the obligation to **register personal data processing activities**. This means that, whenever a business relationship is established, and an entity requests personal data from users/customers, a process must be launched to record the data collected and indicate the purpose for which these data will be used, with the **respective registration of the consent of the data subject**.
- ✍ In Portugal, the [Portuguese Data Protection Authority](#) (CNPD) is the body responsible for **controlling and supervising compliance with the RGPD** and the law that implements it in the Portuguese legal system, as well as other legal and regulatory provisions in terms of **data protection of personal data**, to **defend the rights, freedoms, and guarantees of natural persons** in the context of the processing of personal data.

Specific rules and legislation such as the GDPR bring complex variables to the insertion of companies in the market, especially when they are in the digital environment.



4. DIGITAL SECURITY

Digital Security (DS) describes the features used to protect online identities, data, and other assets. These tools include web services, antivirus software, smartphone SIM cards, biometrics, and secured personal devices. Digital security is the process used to protect an online identity or other sensitive information.

Photo by [Immo Wegmann](#) on [Unsplash](#)

Digital Security (DS) describes the features used to protect online identities, data, and other assets. These tools include **web services**, **antivirus software**, smartphone **SIM cards**, **biometrics**, and secured personal devices. Digital security is the process used to protect online identity. DS is applied as a component of **Information Security**.

Information Security is a set of areas that refers to the protection of information of a company or person. Information is understood to mean any data that, when properly interpreted, carries with it some knowledge, it is important to know your **data models**, the information that is encoded in these models, and classify them properly to apply the most appropriate treatment.

Security is based on three traditional pillars:

The Confidentiality

It is a property that aims to ensure that access to certain information is given only to those who have the right to it.

The Availability

It is a property that aims to ensure that data is accessed when requested (only for duly authorized users).

The Integrity

It is a property defined to guarantee that the information kept has all its characteristics, from its generation to the end of its life cycle. After identifying and mapping all data, it is necessary to prepare a security policy and select how the company's information will be kept.

The Security Policy must contain at least:

- Analysis of the internal environment;
- Responsibility matrix;
- SWOT analysis;
- Business impact analysis;
- Training and awareness plan;
- Key performance indicators.



Photo by [Luther.M.E. Bottrill](#) on [Unsplash](#)

For each security control applied, it is important to identify and map the impact of that component on the business.



5. THREATS AND RISKS

The more the company depends on Information Technologies, the more important it is to identify and control the risks related to its IT assets to avoid potential damage to its business.

Photo by [Setyaki Irham](#) on [Unsplash](#)

In many countries, **Startups** aggregate a considerable part of the intellectual capital and play an important role in the growth and resilience of the economy. It is not uncommon for these companies to face financial and personnel constraints and, as a consequence, place [cybersecurity](#) (Cybersecurity, 2020) as a low priority in products or services. Unfortunately, it only takes one successful **attack or security breach** to **destroy a startup's reputation**, even before it is deployed to the market.



As with small businesses, *startups* face unique challenges and cybersecurity is no exception. From understanding their exposure to risk to locating and mobilizing the appropriate resources to mitigate it, many entrepreneurs struggle to keep their business safe on a limited budget and to build **customer trust** as they build their business.

These companies are seen as "easy prey" and interesting by cybercriminals because, in addition to having information that they can use, **they often do not have the security infrastructure that larger companies have**. On the other hand, a small company is seen as a possible vehicle for attacking a larger company with which it has a relationship.

Cybersecurity should be top of mind for most startup owners, especially in times when **cybercrime** and **data privacy attacks** have become routine. Establishing and maintaining a trusting relationship with customers is an ongoing challenge and built business by business, transaction by transaction, but this can be compromised in the event of a security incident.

By prioritizing **cybersecurity**, the **entrepreneur** will have the opportunity to see his company grow robust and capable of withstanding increasingly sophisticated and frequent cyber threats and attacks.

The more a business relies on Information and Communication Technologies (ICT), the more important it is to identify and control risks related to its technology assets. The risks associated with ICT refer to the probability of the occurrence of events or incidents (equipment failures, power outages, or **malicious hacker attacks**, among others) that have the potential to interrupt critical systems supporting business processes or allow unauthorized access to the information assets of your organization, its suppliers or customers.

Within the scope of cybersecurity, there are five important recommendations for protection. (Table 5.1)

Table 5.1. Recommendations for cybersecurity protection

TIPS FOR PROTECTING AGAINST CYBER THREATS				
REVISION	SOFTWARE	PASSWORDS	DO NOT ANSWER	DO NOT OPEN
Review your online accounts and set up alerts for unusual logins	Install an anti-malware and keep the system up to date	Create complex passwords with letters, numbers and special characters	To emails, SMS and phone calls from unknown sources	Attachments or links sent by unknown emails

Security breaches can devastate even the most resilient companies. Events of this nature may result in financial losses arising, among other factors, from:

- **Theft of funds** and strategic or financial information;
- **Sales losses** due to the interruption of business processes;
- Damage to the company's reputation: **reduced sales** and profits due to **loss of trust** on the part of customers, suppliers, or business partners;
- Fines and regulatory sanctions resulting from non-compliance with legal requirements applicable to your business segment or data protection and privacy laws;
- Individual or collective legal actions for failure to protect customer or partner information;
- Costs associated with repairing affected systems, networks, and devices, or other activities or services necessary for business processes to return to their normal operational state, which may include even the payment of ransom to [hackers](#) (hackers, 2021).



Cyber risk management is a **central business priority** so that the probability of negative events occurring is reduced, their possible consequences are eliminated or controlled, and the return to normal operation takes place in the shortest possible time. Next, we will present the **basic steps of the cyber risk management process**, the main threats to which organizations are exposed, and strategies to eliminate or mitigate their consequences.

5.1. Cyber risk management



Photo by [Michael Geiger](#) on [Unsplash](#)

Currently, many of the services associated with information technologies can be contracted to third parties, including those related to **cybersecurity**. Purchasing cybersecurity services does not mean transferring all responsibility for security (or the survival of the company) to the contractor. In this sense, an agreement between the business and the risks underlying it is necessary, to design and validate a plan with the various phases for its implementation, so that organizations are prepared for **cyber risk**.

As a first step, startups should consider structured approaches to risk. The NIST Cybersecurity Framework, Figure 5.1, provides a common language for understanding, managing, and expressing cyber risk. In this sense, it is important to identify and track technology (hardware, software) and information assets (customer and supplier data; intellectual property, financial data, company strategy) and understand the value of these assets to the business. Without this asset tracking, access and configuration control and **security management** policies will lose effectiveness. On the other hand, it is necessary to verify that the technology and information assets (previously identified) are properly protected and if the company uses cloud-based services, it is important to ensure that your contract with the provider of these services has the scope and responsibilities related to **cybersecurity**, clearly defined and in line with business requirements.

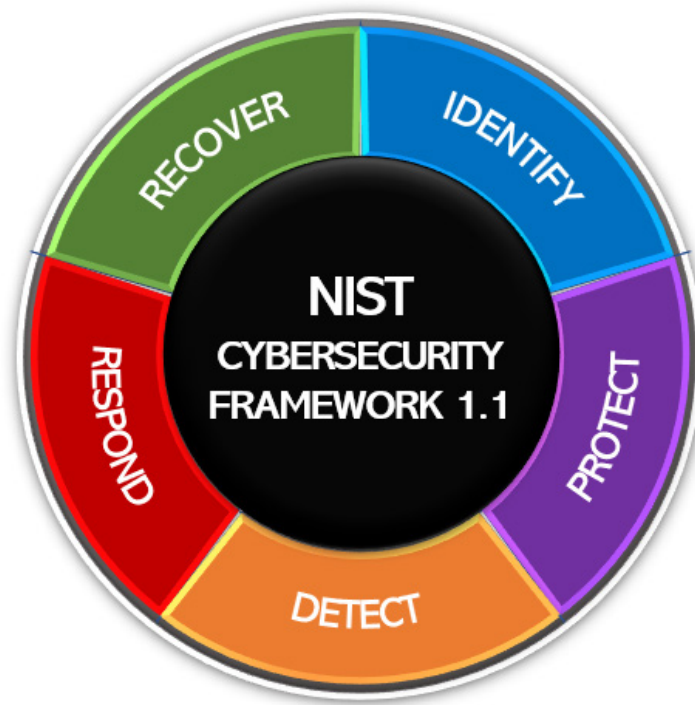


Figure 5.1 NIST Framework

From this point on, actions should be taken to resolve the identified deviations, always from the perspective of business needs and investment capacity. Below are the general stages of a cyber risk management process, based on the general definition of risk and the need for permanent control and updating.

✎ In [ISO 31000:2018](#), the risk is defined as “the effect of uncertainty on objectives”. Risk can be characterized according to its origin (source), potential events, consequences, and the possibility of occurrence. Its effect on objectives can be positive, negative, or both, and address or create threats or opportunities for an organization or business process.

Risk management, in general, is the process that identifies, assesses, and controls threats to an organization's resources, capital, and earnings. In **cyber risk management**, the general principles of risk management are applied to the IT organization, through policies, procedures, and technologies to **reduce threats, vulnerabilities** of technological assets, and **unprotected data** and their respective consequences.

Risk management consists of several processes to build resilience and develop the company's ability to prevent, detect and respond to events related to assets and data, to minimize business interruption and consequent financial loss. These processes include the following steps:

- Identify the **technological and data assets** that can become targets of **cybercriminals** or be impacted by natural events, due to the vulnerabilities they present;
- Identify as many risks as possible to which the business is exposed in its operating environment. **Cyber or IT risks** include **software and hardware failures, malicious attacks (viruses, spam, among others)**, human error, and natural disasters (e.g., floods, fires, storms);
- Analyze each identified **risk factor** to determine its scope and its relationship to the different factors within the organization and map which business processes are affected by a given risk and the magnitude of the impact caused. Factors that impact an organization's cyber risk include, among others, regulations and other legal requirements affecting the industry segment and location in which it operates, its business model, products or services offered, technology platform adopted, and customer location and Providers;
- Classify and **prioritize risk**. There are risks that, if they materialize, can **paralyze the entire business**, while there are risks that will only be minor inconveniences and, therefore, acceptable. Risk classification allows the organization to obtain a holistic view of risk exposure to be used in prioritizing the actions and investments to be made to address them;
- Address risks with measures that can be eliminated or contained to the extent possible. In the case of **cyber risks**, the **necessary cybersecurity** measures must be implemented, whether of a technical nature (technology acquisition), procedural, or for the people of the organization (technical training, cybersecurity awareness campaigns);
- Monitor and analyze risk, as risks are not static and the **effectiveness of treatment measures** can be negatively impacted by changes in the organization's internal or external environment. The processes and indicators associated with the **treatment of risks** must be defined and monitored, and any deviations identified must be used for adjustments and/or creation of preventive or corrective measures for the treatment of risks.

Currently, a company has the opportunity to choose to implement a **cyber risk** management system to implement best practices in the prevention of **cyber-attacks** and obtain **certification**, to assure customers that measures or best practices are adopted for cybersecurity management systems.

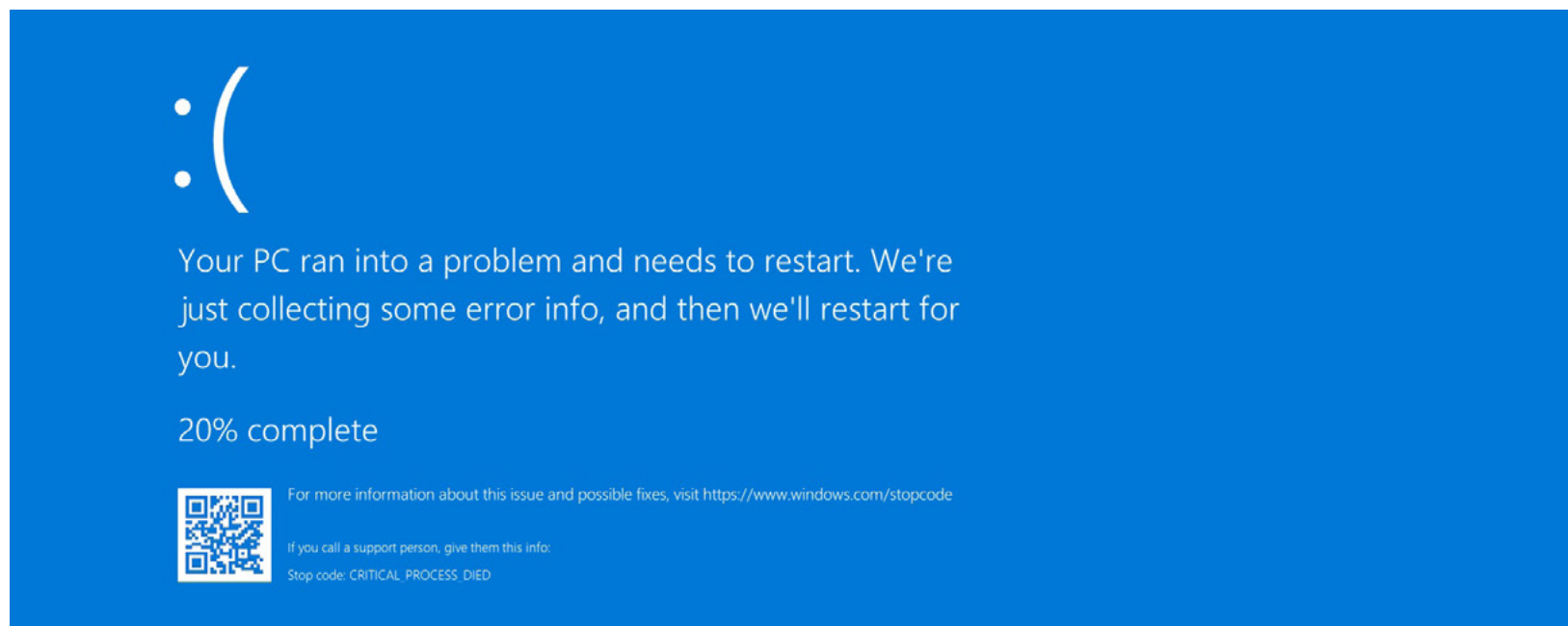
 [ISO 27001](#) (ISO 27001, 2013) is an international standard that describes best practices for information security management systems. This standard is part of the ISO 27000 family, whose objective is to help keep a company's **information assets** protected. The ISO 27001 standard specifies the essential control to maintain security, namely: **security policy, classification, and control of assets, physical and environmental security** - physical control of access to information and equipment, security of the work environment, **identity and access control**, system development and maintenance, business continuity management and compliance with relevant national and international laws.

5.2. Most common cyber threats for small businesses

The two most common types of threats for small businesses are social engineering and [malware](#) (malware, 2021). Social engineering is the manipulation of individuals, usually via email, phone, or text message (SMS), to obtain confidential information (e.g., login credentials) or induce an action, e.g., click on a link and download a file or visit a malicious webpage where the **hacker** can deploy [ransomware](#) (ransomware, 2021) or other *malware*.




5.2.1. Malware





Malware is an umbrella term that refers to software designed to **harm a computer, server, client, or computer network** to give cybercriminals access to a victim's system. *Malware* can include viruses and *ransomware*.



Viruses are malicious programs that spread from computer to computer (and other connected devices). Viruses are designed to give cybercriminals access to a victim's system.


 [Ransomware](#) is a specific type of malware that **locks down a victim's computer** or encrypts all of their data until the ransom is paid. Ransomware is usually delivered via a malicious link via an email and exploits unpatched vulnerabilities in the software. Often, data or system is not restored even after the ransom is paid.

5.2.2. Threats by email

 [Phishing](#) is one of the oldest used by hackers to obtain information and create channels of interaction with users. It is a type of [social engineering](#) attack that uses email, or a **malicious website**, to infect a machine with malware or gather sensitive information. Phishing emails appear as if they were sent by a known person or a legitimate organization, tricking users into clicking a link or opening a file that contains malicious code. 

5.2.3. Threats in videoconferencing environments

 Historically, small businesses have had tools to support virtual offices and remote workers. Some examples of the most widespread tools are [Zoom](#), [Google Meeting](#), [Microsoft Teams](#) and [Jitsi](#), the latter being an [Open Source](#) platform. 

With the COVID-19 crisis, a large number of people turned to videoconferencing platforms (VTC) to interact with others on a personal or professional level. Some reports of [conferences interrupted](#) by **pornographic** and/or **hateful images** and **threatening language** have become more frequent in recent months. Virtual events are an environment in which social engineering techniques can be applied to information that could facilitate a future **cyber-attack**. 

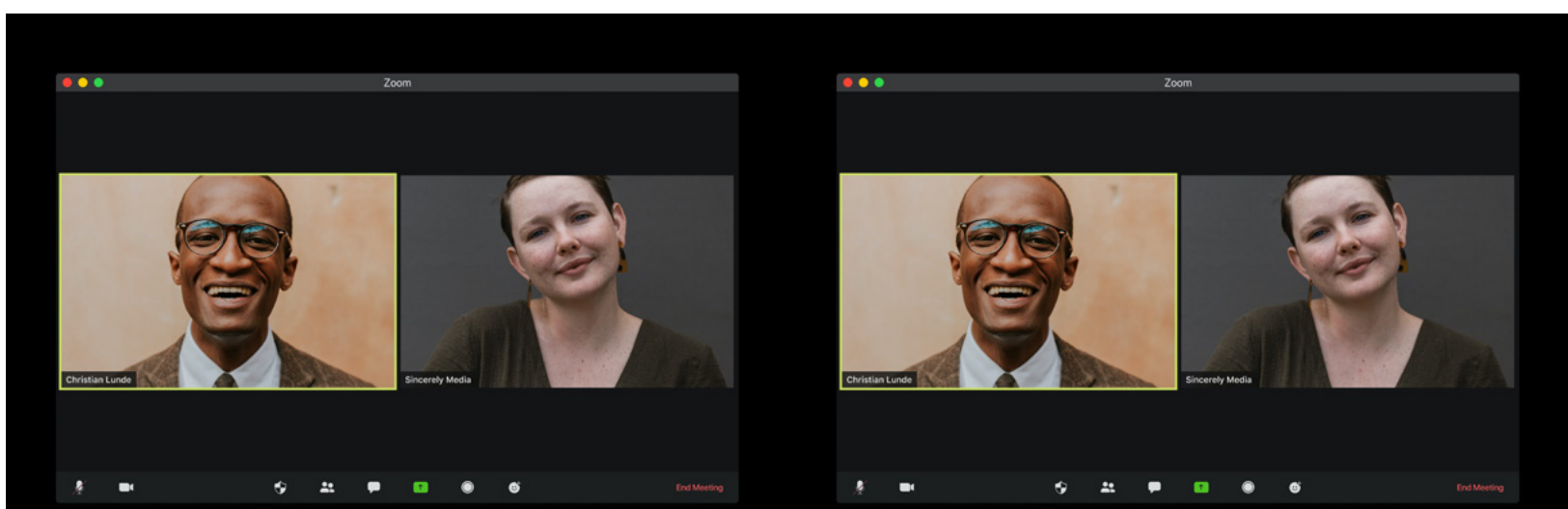


Photo by [visuals](#) on [Unsplash](#)

Photo by [visuals](#) on [Unsplash](#)

5.3. Cyber vulnerabilities

A vulnerability is a weakness that can be exploited by a malicious actor to gain access or perform unauthorized actions on a system or device. The **vulnerabilities** could allow **hackers** to run programs, install **malware**, and copy, modify, encrypt or destroy data. The most common vulnerabilities (for small businesses) include behavioral, **code injection**, **sensitive data exposure**, **endpoint protection**, and **identity management**.

Vulnerabilities increase an organization's attack surface, that is, the points with potential for exploitation by malicious actors. Public websites, personal devices, and people are key elements of an **attack surface**. To reduce it, organizations must regularly assess their vulnerabilities and identify security weaknesses, in addition to monitoring network and server anomalies.

The analysis of vulnerabilities, weaknesses, and mitigation procedures must be a constant, cyclical, and perennial routine in the IT environment of companies.

5.3.1. Behavioral vulnerabilities

The security of certain information can be affected by behavioral factors and the use of those who access it, by the environment or infrastructure that surrounds it, or by malicious people who aim to **steal**, **destroy** or **modify** such information.

End-user error is the number one security threat action and is a significant issue for organizations of any size. Behavioral **vulnerabilities (weaknesses)** include:

- Use of "weak" passwords;
- Entering malicious links received by email;
- Browsing unsafe websites;
- Execution of malicious file downloads;
- Failure to comply with prescribed measures to protect confidential information;
- Failure to update the system software.

The best way to mitigate behavioral vulnerabilities is through end-user training and **security awareness**. Information security awareness is one of the hottest topics in recent years, especially given the rise of the *Internet of Things (IoT)* devices and remote work.

- ✍ The action of making the [organizational community aware](#) of the nature of the company's business, specifically about the **potential threats, risks, and behaviors** that promote a safer environment is to promote information security through awareness campaigns for the involvement of all employees in the identification of threats, *phishing* campaigns to identify points of improvement in communications and specific training to increase the maturity level of workers.

Without enough resources to invest in sophisticated cybersecurity tools and systems, security training will provide the best results for small businesses. [Many training programs](#) are available to help reinforce security concepts. It is essential to track a user's success or failure rates in testing, as well as in "real fire" testing with **phishing** emails and **other tactics**.

Security is the duty of all employees towards the organization and its information assets. Each individual must observe security rules and conduct when handling the organization's data. For this reason, it is important to keep the organizational community always aware of threats, ways to identify them, and with a direct channel of communication with the management of information technologies, to report any indication of risk and potential attacks (anticipating greater impacts on the business).

5.3.2. Code injection

Code injection attacks are among the most common. Some vulnerabilities allow **cybercriminals to inject malicious code** into a victim's system by exploiting applications that allow user input into databases, **shell** commands, or the operating system.

Monitoring patterns of abnormal behavior of input data in computing systems is an effective mitigation strategy for code injection attacks. There is an antivirus (state-of-the-art) that looks for actions that are not consistent with the patterns of data entry made by humans and also patterns of behavior that are used by malicious actors. These types of tools provide a comprehensive analysis of **malicious behavior**, as well as more flexible prevention and detection options.

5.3.3. Confidential data protection

Human failure to take prescribed precautions to protect sensitive data also adds a layer of vulnerability. Data are written to storage devices, as well as data in transit, must be protected. **Security experts** recommend that data, whether confidential or sensitive, be stored in an **encrypted format**. However, even encrypted data is susceptible to a **ransomware** attack.

Encrypting data is not an expensive undertaking, and small businesses should follow best practices for using **encryption** to protect data. Using a VPN to encrypt data (as it is transmitted) is a common and effective solution, as is keeping **encrypted data at rest**, even when access control, at the level of users and passwords, fails.

Additionally, it is recommended to implement multi-level encryption, e.g., on the database and on the physical storage device where the database resides. Data **encryption keys** must be updated regularly and stored separately from the data.



One solution that many small businesses find satisfactory for protecting data in transit is the use of [encrypted flash drives](#). If encrypted data is needed at a remote location, physically moving the information on an [encrypted drive](#) may be the right solution in some circumstances.



To protect data from ransomware, a [multifaceted backup](#) and recovery strategy is recommended that includes system data, database backups, and end-user data. The main operating systems, such as [Windows](#), [Linux](#), and [macOS](#), natively have some capacity to perform backups.



5.3.4. Endpoint devices


Laptops and desktops, tablets, and mobile phones connected to the organization's network are potential vectors for **malware**. **The update level of the software** installed, the applications installed (on each endpoint device) and its compliance with security policies will define the level of exposure, even in small businesses.

Developing and implementing policies that require all applications and **operating systems** on any **endpoint** (connected to the business network) to be updated and patched is the most effective and least expensive endpoint protection measure.

Setting clear expectations for *endpoint* security is vital to preventing future misunderstandings and policy non-compliance in both personal and business use of the same *endpoint* device.

5.3.5. Credential management

One of the most common causes of system compromise is the lack of **robust credential management**. Using the same password for multiple accounts, even reusing passwords for personal accounts in commercial systems, represents one of the most exploited vulnerabilities by hackers who can use credentials obtained in previous breaches to **attempt logins** to a wide variety of websites.

 For most organizations, satisfactory results can be achieved by implementing strict password control, e.g., using longer, more complex passwords, forcing more frequent password changes, or a combination of these principles. Currently, [Multi-Factor Authentication \(MFA\)](#) is used in various services as an additional mechanism for authenticating a user. MFA is the use of two or more factors, or methods, to verify the authenticity of something or a person.

Social networks (with Facebook) and the main e-mail services (Gmail from Google) and even in the physical world, such as ATM terminals (in some countries), already use more than one means to certify that the user who is trying to access the service is authorized. Some alternatives can be adopted as a second, third, or nth authentication factor, e.g.,

Table 2.1 Data: Personal, Sensitive and Common

BIOMETRY	VERIFICATION CODES	TOKENS	DIGITAL CERTIFICATES
Fingerprint, iris or retina reading and facial recognition	Sent to an email or SMS account	Generated by specific applications or <i>hardware</i>	Embedded in smartcards or protected files

The use of password management tools helps and facilitates the adoption of password management policies. These tools eliminate the need for users to remember a large number of passwords.



6. SOLUTIONS AND TRENDS

In the digital age, the need for digital security implies the search for effective security solutions (updated platforms and software packages) that guarantee the trust of those responsible for companies regarding their businesses and their data. A set of solutions and trends are referred to as investments in digital security.

Photo by [Diego PH](#) on [Unsplash](#)

As described above, **data cleansing** can incur significant costs, both financial and reputational. Protecting company and customer data is a key part of the **cybersecurity business plan**, and it may not be expensive, but requires effort and diligence in execution.

An effective security platform has, at its base, components that are simple to implement and relatively affordable. In this sense, some investment suggestions are indicated:

Reliable antivirus and antimalware

A compromised device means exposure to attacks. Every action, from logging in to your email to checking your company's bank account balance, is a potential exposure situation. Install reliable [anti-virus and anti-malware software](#) on every laptop, desktop, or mobile phone used by each employee.



Multi-Factor Authentication (MFA)

As discussed above, the [MFA](#) introduces one or more additional identification requirements for accessing services, requiring, e.g., a password and code, which can be sent as a text message to a user-specified telephone number. For all major cloud services, activation is important. Google, Amazon, and Microsoft provide (step-by-step) guidance for setting up and using MFA.



Encryption to protect sensitive data

If a company stores any type of customer data, whether regulated information (e.g., credit card numbers, or simply personal data, delivery addresses), it is convenient to encrypt the database throughout the entire process from entry to exit. It is convenient to use strong [criptografia](#) in production and logistics systems.



Safety as part of organizational culture

One of the weakest links in any security system is not technological, but human. The most convenient and frequent way to attack the security of most organizations is through the team; 93% of all attacks start with an email used to deliver malware to a device. The best approach, in these cases, is to [make the team aware of the risks](#) and that the company's leadership takes security seriously, and the defined protocol for handling suspicious emails or phone calls, and even attempts to enter the physical premises.



Table 6.1. Eight tips for safe browsing

TIPS FOR PROTECTING AGAINST CYBER THREATS			
HEADS UP	SAFE SITE	HEADS UP	STRONG PASSWORD
To fake websites and suspicious links	Check on the web browser	To <i>phising</i> mails	Create complex passwords
SOCIAL NETWORKS	ADWARE	BANKS	SOFTWARE
Validate all access to social accounts	Install an anti-adware tool	Configure secure access and MFA	Keep all software up to date

Seek help

It is especially important for startups or anyone working with sensitive data to look for tools that automate threat detection that can reduce the time and effort to identify security breaches. It is better, and almost always less, the cost of prevention than remedy, i.e., prevention and repair. The inclusion of specific platforms in the cybersecurity arsenal, such as [IDS/IPS](#), can be an asset to the company. However, cybersecurity tends to become a complex topic as the company grows and the probability of being attacked increases. There are several companies focused on providing automated “threat intelligence”, alongside more traditional services and tools that handle security monitoring and management on an “as a service” basis. In Portugal, [REDSTOUT](#) has an assessment program. The portfolio of security services of these companies may include, e.g., risk assessment; risk management; training and awareness; endpoint protection; email security; cloud security management; access management (physical and/or digital); firewall and network; data encryption; security incident monitoring, detection, and response; penetration testing (pentest); etc.

Cyber Insurance

Cybersecurity insurance, **cyber liability** insurance, or **cyber insurance** is a type of insurance that a company can purchase to help reduce the financial risks associated with doing **business online**, by transferring (for a fee) part of the risk to the insurer.

In general, **policies include primary coverage** for losses that apply directly to a business, and **third-party coverage applicable to losses suffered by a third party** in a cyber event or incident, based on the existing business relationship with the business that purchased the insurance.

Cyber insurance policies help cover financial losses resulting from cyber events and incidents and the costs associated with remediation, including payment for legal assistance, investigators, institutional communication management activities, and customer reimbursements.

Many **cybersecurity policies** exclude preventable human-caused security issues such as **poor configuration management** or **careless mishandling of digital assets**.

The cost of improving technology systems, including enhancing security in systems or applications, maybe the reason for exclusions from **cyber insurance** coverage. Improved security of technology systems, including strengthening security in systems or applications, and pre-existing (or previous) cyber breaches or events, maybe considered incidents that occurred before the purchase of insurance.

Cybersecurity insurance is a new and emerging sector and is now available in Portugal. However, unlike traditional insurance modalities, insurers have limited data to formulate risk models and determine the coverage, rates, and **premiums of insurance policies**. For this reason, a careful analysis must be made before deciding on the acquisition. As it is a relatively new product on the market, it is recommended that they be evaluated with the help of specialized consulting.



7. CASE STUDIES

Examples of case studies of startups linked to the area of digital security, in which their businesses are related to services in terms of Security, Fraud, and validation. These cases are related to Portuguese, European, and Brazilian startups.

Photo by [Mimi Thian](#) on [Unsplash](#)

This chapter refers to a case study of startups linked to the area of **digital security**, in terms of **Security, Fraud, and Validation**.

✎ [FullFace Biometric Solutions](#) aims to identify people. With the increase in digital processes, **authentication mechanisms based** on logins and passwords are not the best way to guarantee information security. In this sense, FullFace Biometric Solutions is specialized in the identification of people through **real-time facial biometrics** and in the development of **biometric platforms** involving the web and mobile applications.



Photo by [FullFaceBiometric Solutions](#)

Other services and further details of the company's products and services can be found [here](#) (FullFace, 2021). ✎

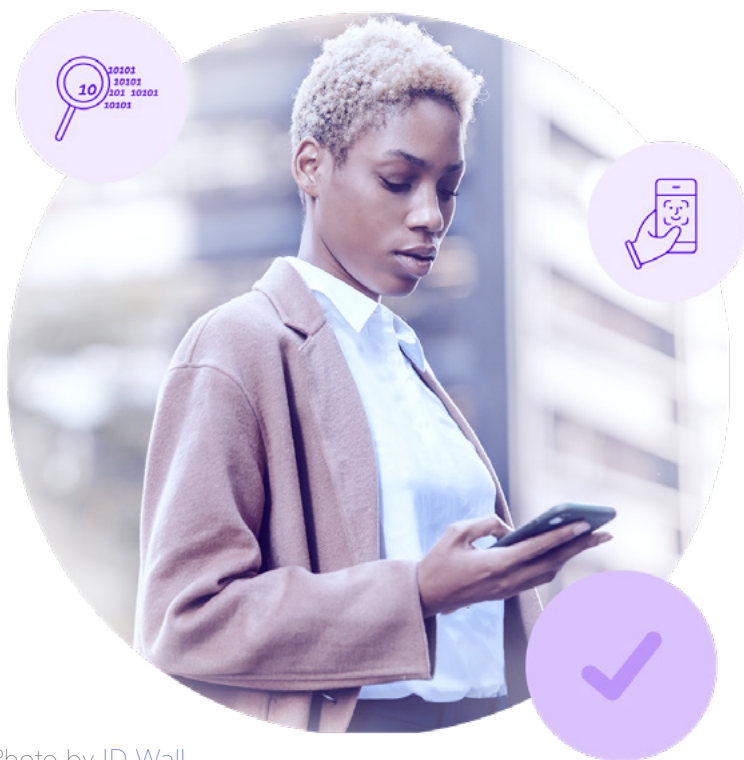


Photo by [ID Wall](#)

✎ [ID Wall](#) (ID Wall, 2021) develops several services in the security area, where the verification of OCR (**Optical Character Recognition**) documents stands out - in which the type of document is identified and the data from it are extracted automatically. Data extraction is performed using different technologies, e.g., **Face Match**, which recognizes the image by comparing a selfie with the photo of the document; the *Background check*, which allows you to search more than 200 data sources from "Individual and Legal Persons" (to speed up the process of digital onboarding of customers and partners, considering the security of your business to be essential); the *Mobile SDK*, which allows to integrate solutions quickly and securely, and the approval of customers without compromising security; "**Documentoscopy**", which allows triggering the analysis of a document, and verifying and confirming whether the document

was produced by the person, public or private organization (entity that is supposed to have produced the document) and if it underwent alterations after it was finalized, or if it was "manufactured" improperly, by a third party that seeks to assume the identity of the author; *Professional Services* integrates onboarding and user validation consulting services.

✍ [REDSTOUT](#) (REDSTOUT, 2021) is an information technology company, based in Lisbon, focused on open-source cybersecurity solutions and services. The company was born from the union of ideas and studies of a group of students, as a result of the first RED (REDSTOUT Enterprise Defense) project that has its scope is defined to support **low-cost security solutions** for Small Businesses and Families Businesses.



When exploring market solutions, the company identified that investments to keep up with legislation and threats (increasingly sophisticated) represented a significant cost for small businesses.


The studies developed within the scope of the M.Sc. in Telecommunications and Computer Engineering and Ph.D. in Science and Information Technology at ISCTE-IUL allowed the knowledge to be applied in the development of products **based on open-source software** for **data protection**. At its inception, the company had the support of the [AUDAX-ISCTE](#) Innovation and Entrepreneurship Center (*Audax-ISCTE*, [2021]) in incubating ideas and integrating them into the business environment in Portugal.

In addition to systems, the company has established itself as a multidisciplinary consultancy with doctors and masters, in management, finance, projects, and technologies that accumulate vast experience to support any type of business and provide more modern and secure processes and tools. From strategy to implementation and support, REDSTOUT offers cybersecurity expertise that goes beyond traditional compliance solutions. REDSTOUT consulting services help **reduce your business risk** by addressing your organization's unique opportunities and challenges. Experts assess and guide the remediation of information security compliance gaps at all levels of the enterprise to help focus your organization's resources, time, and budget on areas that add value or significantly reduce risk exposure.

REDSTOUT has broadened its horizons and is also present in Angola (www.redstout.co.ao), exploring a market full of opportunities in information security.

✍ [Noleak Behavior Recognition](#) (NoLeak, 2021) is a system based on **artificial intelligence** to identify **suspicious** actions and **behaviors**, captured through RGB camera sensors. The system correlates events from multiple cameras (in real-time), creating a risk score for monitored environments. The system can be adapted to detect human behavior, in various markets and sectors, when solving problems.



 [XLabs on security](#) (XLabs, 2021) is a company, where more than 100 million people pass through the systems daily. This company has four main products:

Penetration test

It uses several techniques to check for vulnerabilities (in terms of targeted attacks, compromising the availability, integrity, and confidentiality of information on your systems) and risks on internal networks or even on the web.

Web Application Firewall

This application protects web applications against the Top 10 threats of [OWASP](#) 2021 (OWASP, 2021) and others such as database access, redirects, execution of remote commands, denial of service, and inclusion of ads. It also detects and blocks threats before they reach data centers without compromising enterprise application performance and responds to targeted attacks with the ability to pinpoint locations.

Content Delivery Network

This performance tool geographically distributes the platform's content, implying an improvement in performance and security as well.

The *Content Delivery Network* is an information distribution network that increases speed through the use of multiple servers that direct content to the user according to the proximity of the server. The main mission is to shorten the physical distance between the client and the server, improving the rendering speed (processing or digital creation of an image with detail and definition) and the performance of the website.

Security Operations Center

It is a product that centralizes the entire security operation. This center can monitor internal and external environments in terms of people, processes, and technologies to detect security incidents, through the analysis, detection, prevention, and mitigation of vulnerabilities in organizations' systems and platforms.

In any organization, it is necessary to identify and understand the cyber risks and threats to which organizations are exposed (as a first step to protecting information assets). It is important to take a proactive and comprehensive approach to identify the level of risk and vulnerabilities before they can be exploited. Cybersecurity assessment results can be used to determine the budget to improve cybersecurity in the organization, estimate benefits, and prioritize investments.

The assessment impacts cybersecurity awareness and knowledge (at all levels of the organization) and drives accountability and creates a more effective and efficient work culture. By making cybersecurity a priority, employees can support each other in the safe use of technology. The assessment action has positive results in terms of processes, tools, and behaviors to quickly prevent, resolve/mitigate cybersecurity incidents (avoiding data loss/theft) and, consequently, downtime in business and operations, loss of revenue, legal exposure, and negative publicity.

As an initial step in the process of creating a secure infrastructure, capable of protecting critical data, accesses, and users, an initial analysis of the state of Information Security is recommended, to carry out a high-level survey of Security solutions. of Information implemented, identify points of attention, and propose improvements in infrastructures and processes based on architectures and validation models of the disciplines of protection of information assets.

REDSTOUT is a company incubated at AUDAX-ISCTE that offers an assessment and proposes recommendations for improvements that can promote an increase in the degree of maturity in a short period and with relatively little effort, to direct actions and promote visibility on returns. investment in the area.

Glossary

- **CNCS**
National Cybersecurity Center.
- **CNPD**
National Data Protection Commission.
- **Cybercriminal**
An unethical *hacker* who crosses legal boundaries gathers unauthorized information and performs electronic transactions anonymously.
- **Cyber Risk**
Technological events that can cause business losses are caused by weaknesses and vulnerabilities, to which technological assets are exposed.
- **Data**
Set of characters or symbols that encode information.
- **DS**
Digital Security.
- **Endpoint**
Access points to information in a computer network, e.g., Notebooks, PCs, Tablets, and mobile phones, among others.
- **Framework**
The model aims to solve recurring problems.
- **GDPR**
General Data Protection Regulation (GDPR).
- **Hacker**
A person with computer knowledge is capable of exploiting security weaknesses and vulnerabilities.
- **ICT**
Information and Communication Technologies.

- **IoT**

Internet of Things. The concept describes the connectivity and exchange of information between physical objects such as cars, appliances, and industrial equipment, endowed with the ability to send data.

- **ISO**

International Standardization Organization.

- **IT Architecture**

The IT architecture is responsible for planning the technologies and transporting the business needs to the technological environment.

- **Malware**

Software package designed to cause intentional harm.

- **Personal data**

Set of data that encodes personal information.

- **Personal information**

Any information that makes it possible to identify a natural person.

- **Phishing**

Technique for collecting information and disseminating *malware* using the email service.

- **Ransomware**

A group of *malwares* that hijacks data and encrypts the content, is usually used to demand ransom for stolen information.

- **Shell**

Command interpreter for the Linux operating system.

- **Startup**

English language term that defines an "emerging company".

- **Technological assets**

All components of the information technology infrastructure.

- **Token**

An electronic key is used to identify a user, an application, or an endpoint.

- **Video conference**

A platform for making group voice and video calls.

- **VPN**

Virtual Private Network, or private network, where data is encrypted and sent over a public network such as the Internet.

References

Anderson, C. (2008), A Cauda Longa, Editora Campos.

Anderson, D., (2019), Storytelling: Manipulation of the Audience - How to Learn to Skyrocket Your Personal Brand and Online Business Using the Power of Social Media Marketing, Including Instagram, Facebook and YouTube, Independently Published.

(Audax–ISCTE, 2021), AUDAX-ISCTE, <https://audax.iscte-iul.pt/>, (Accessed: October 2021).

(Cibersegurança, 2020), Você sabe o que é a cibersegurança?, <https://www.youtube.com/watch?v=CU2yQxzkvFg> (Accessed: October 2021).

(CNCS, 2020), CNCS - Relatório Sociedade 2020, <https://www.cncs.gov.pt/pt/relatoriosociedade-2020/>, (Accessed: September 2021).

(CNPd, 2021), Comissão Nacional de Proteção de Dados, <https://www.cnpd.pt/>, (Accessed: September 2021).

(Cybersecurity, 2021), The History of Cybersecurity, CompTIA's Future of Tech., <https://www.futureoftech.org/cybersecurity/2-history-of-cybersecurity/>, (Accessed: September 2021).

(Data Classification, 2016), Data Classification – Why Is Data Classification Essential For All Businesses?, <https://www.youtube.com/watch?v=fkHkmdgyYW8> (Accessed: September 2021).

(European Commission, 2021), O que são dados pessoais?, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt, (Accessed: September 2021).

(hackers, 2021), What is a hacker?, <https://searchsecurity.techtarget.com/definition/hacker> (Accessed: October 2021).

(IAPMEI, 2021), IAPMEI - Regulamento Geral de Proteção de Dados, <https://www.iapmei.pt/PRODUTOS-E-SERVICOS/Assistencia-Tecnica-e-Formacao/Regime-Geral-de-Protecao-de-Dados.aspx>, (Accessed: September 2018).

(INE, 2021), Portal do INE, https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=415621360&DESTAQUESmodo=2, (Accessed: September 2021).

(ISO 27001, 2013), ISO 27001 definition: What is ISO 27001?, <https://www.itgovernance.co.uk/iso27001>, (Accessed: October 2021).

(ISO 27001, 2021) ISO - ISO/IEC 27001—Information security management, <https://www.iso.org/isoiec-27001-information-security.html>, (Accessed: September 2021).

(ISO 31000, 2021), ISO - ISO 31000—Risk management, <https://www.iso.org/iso-31000-risk-management.html>, (Accessed: September 2021).

(Keller, 2013), Cybersecurity Framework, NIST, <https://www.nist.gov/cyberframework>, (Accessed: September 2021).

(malware, 20219), What is malware? Types and dangerous of malware, <https://searchsecurity.techtarget.com/definition/malware> (Accessed: October 2021).

(Ministros, 2019), Resolução do Conselho de Ministros 41/2018, Diário da República Eletrónico, de <https://dre.pt/home/-/dre/114937034/details/maximized>, (Accessed: September 2021).

(Noleakdefence, 2021), Action/Behavior Recognition, <https://www.noleakdefence.com>, (Accessed: October 2021).

(OWASP, 2021), OWASP Top 10 - 2021, <https://owasp.org/Top10/>, (Accessed: October 2021).

(phishing , 2021), How phishing works?, <https://searchsecurity.techtarget.com/definition/phishing>, (Accessed: October 2021).

(ransomware , 2021), How do ransomware attacks work?, <https://searchsecurity.techtarget.com/definition/ransomware>, (Accessed: October 2021).

(Redstout, 2021), REDSTOUT ENTERPRISE DEFENSE, <https://www.redstout.com>, (Accessed: October 2021).

(Regulamento, 2016), Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, Pub. L. No. 32016R0679, 119 OJ L (2016), <http://data.europa.eu/eli/reg/2016/679/oj/por>, (Accessed: September 2021).

(Setzer, 2021) Setzer V., Dado, Informação, Conhecimento e Competência <https://www.ime.usp.br/%7Evwsetzer/dado-info.html>, (Accessed: September 2021).

(XLABs, 2021), Produtos/soluções, <https://www.on-security.com/pentest>, (Accessed: October 2021).

Photos

Capa: Photo by [Getty Images Signature](#) on [Canva](#)
Photo by [Pickawood](#) on [Unsplash](#)
Photo by [Taylor Vick](#) on [Unsplash](#)
Photo by ricochet64. Credits: Getty Images/iStockphoto.
Photo by [Immo Wegmann](#) on [Unsplash](#)
Photo by [Setyaki Irham](#) on [Unsplash](#)
Photo by [Diego PH](#) on [Unsplash](#)
Photo by [Mimi Thian](#) on [Unsplash](#)
Photo by [ID Wall](#)
Photo by [FullFaceBiometric Solutions](#)
Photo by [Michael Geiger](#) on [Unsplash](#)
Photo by [Luther.M.E. Bottrill](#) on [Unsplash](#)
Photo by [Stephen Dawson](#) on [Unsplash](#)
Photo by [Gean Cescon](#) on [Unsplash](#)
Photo by [Antoine J.](#) on [Unsplash](#)
Photo by [tagedstudio](#)
Photo by [visuals](#) on [Unsplash](#)
Photo by [visuals](#) on [Unsplash](#)

Figures

[Figure 1.2. Information and Communication Technologies usage in Enterprises](#)
[Figure 5.1. NIST Framework](#)

Tables

[Table 2.1. Data: Personal, Sensitive and Common](#)
[Table 5.1. Recomendations for cybersecurity protection](#)
[Table 6.1. Eight tips for safe browsing](#)

AUTHORS

Marcio Santos
Cláudio Perim and
Pedro Sebastião

**PROMOTING
ENTITY**

IAPMEI, Agência para a Competitividade e Inovação, I.P.
Departamento de Empreendedorismo e Financiamento
Departamento de Valorização e Capacitação Empresarial

**COORDINATION &
REVISION**

AUDAX – Centro de Inovação e Empreendedorismo do ISCTE-IUL
Luís Gonçalves

GRAPHIC DESIGN

I AM - The Creative House

DATE OF ISSUE

October 2021

COPYRIGHT

2021, IAPMEI

PRODUCTION

audax _iscte



ISBN: 978-972-8191-66-5

Co-financed by



UNIÃO EUROPEIA

Fundo Social Europeu