Interreg
España - Portugal

CIBERIA

2025

# CIBERIA

## GOOD PRACTICE GUIDE

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

| ACRONM | DEFINITION |
|---|---|
| 2FA | Two Factor Authentication |
| ABAC | Attribute-Based Access Control |
| AEPD | Spanish Data Protection Agency |
| AD | Active Directory |
| AI | Artificial Intelligence |
| BCP | Business Continuity Plan |
| CNCS | National Cybersecurity Center |
| CNPD | National Data Protection Commission |
| DAC | Discretionary Access Control |
| DRP | Disaster Recovery Plan |
| EDR | Endpoint Detection System |
| HTTP | Hypertext Transfer Protocol |
| ICMP | Internet Control Message Protocol |
| IDS | Intrusion Detection System |
| IGMP | Internet Group Message Protocol |
| INCIBE | National Cybersecurity Institute |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| IRP | Incident Response Plan |
| ISO | International Standards Organization |
| IT | Information Technologies |
| MAC | Mandatory Access Control |
| MFA | Multi-Factor Authentication |
| OSI | Open Systems Interconnection |
| RBAC | Role-Based Access Control |
| GDPR | General Data Protection Regulation |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| SIEM | Security Information and Event Management |
| SMTP | Simple Mail Transfer Protocol |
| SNMP | Simple Network Management Protocol |
| SSL | Secure Sockets Layer |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| UDP | User Datagram Protocol |
| EU | European Union |

**Comentado [MT1]:** The Portuguese National Cybersecurity Center

**Comentado [MT2]:** Which country?

**Comentado [MT3]:** The Spanish National Cybersecurity Institute

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

# 1. Introduction

In an increasingly digital world, cybersecurity has become a crucial aspect of everyday life. From personal devices to corporate networks, protecting data and systems from unauthorized access, cyberthreats, and malicious attacks is essential.

Cybersecurity is not an exclusive concern of the "computer scientists». Everyone has a role to play in keeping their information safe. Adopting good cybersecurity practices can significantly reduce risks.

This guide aims to provide an overview of cybersecurity best practices that organizations and individuals can follow. Regardless of the level of cybersecurity expertise, this guide offers practical advice for improving digital security and resilience.

The practices described here are designed to address a range of important cybersecurity issues, from using strong passwords to email management to more technical aspects such as network monitoring and server usage.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

# 2. Concepts

## 2.1 Introduction

The main objective of this chapter is to explain the most relevant technical concepts for interpreting this guide. However, these explanations will be succinct, so that the reader can understand the different concepts throughout the document.

## 2.2 Model OSI

The Open Systems Interconnection (OSI) network reference model [1, 2] was developed by the International Standards Organization (ISO) with the aim, first of all, of standardizing the approach to developing a solution for the exchange of data between networks and within the network itself.

This model attempts to standardize the way data is transmitted on the network. This allows for the development of systems that are compatible with each other, even if they come from different manufacturers. The term "Open" in the model's name implies the idea of a system open to communication with other systems.

The OSI model is based on seven layers, each of which solves a specific problem related to data transmission on the network.

Figure 1 shows the OSI model.

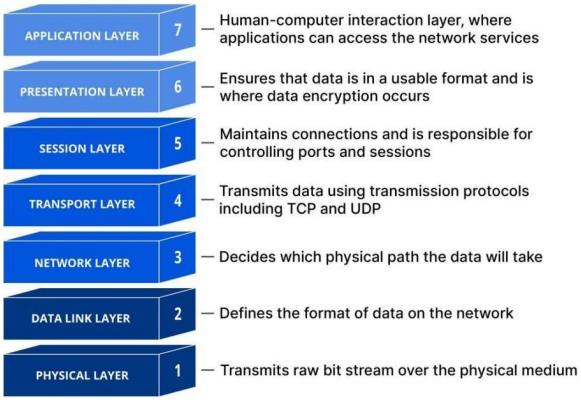


*Figure 1: OSI model, with a brief explanation of the layers (Image adapted from [3]).*

**Comentado [MT4]:** Presentation Layer 6 - Ensures that data is in a usable format. It is where data encryption occurs.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

- **Physical Layer -Layer 1**

The physical layer refers to the physical medium of communication and the technologies for transmitting data over that medium. Essentially, data communication is the transfer of signals, digital and electronic through various physical channels, such as fiber optic cables, copper pipes, and air. The physical layer includes standards for technologies and metrics strictly related to channels, such as Bluetooth, NFC, and data transmission speeds.

- **Data Link Layer -Layer 2**

The data link layer is very similar to the network layer, except that the data link layer facilitates the transfer of data between two devices of the same network. The data link layer receives packets from the network layer and divides them into smaller parts, called plots. Similarly to the network layer, the data link layer is also responsible for flow and error control for communications within the network (the transport layer only performs flow and error control for communications between networks).

- **Network Layer -Layer3**

The network layer is responsible for facilitating data transfer between two different networks. If the two communicating devices are on the same network, the network layer is unnecessary. The network layer divides the transport layer segments into smaller units, called packages at the sending device, and reassembles these packets at the receiving device. The network layer also finds the best physical path for the data to reach its destination, which is known as routing. Network layer protocols include IP, ICMP, IGMP and the IPsec suite.

- **Transport Layer -Layer4**

Layer 4 is responsible for end-to-end communication between two devices. This includes collecting data from the session layer and dividing it into parts called segments before sending them to layer 3 (network layer).

The transport layer is also responsible for flow and error control. Flow control determines an optimal transmission rate to ensure that a sender with a fast connection does not overload a receiver with a slow connection. The transport layer performs error control at the receiving end, ensuring that received data is complete and requesting retransmission if not. Transport layer protocols include TCP and UDP.

- **Session Layer -Layer5**

The session layer is responsible for opening and closing communication between two devices. The time between opening and closing the communication is called *session.* The session layer ensures that the session remains open long enough to transfer all the data being exchanged, and then closes it immediately to avoid wasting resources. The session layer also synchronizes data transfer with checkpoints.

- **Presentation Layer -Layer6**

This layer is primarily responsible for preparing data for use by the application layer; in

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

other words, the presentation layer makes the data presentable for consumption by applications. This layer is responsible for processing, encrypting, and compressing the data.

This layer is also responsible for compressing the data it receives from the application layer before delivering it to the session layer (layer 5). This helps improve communication speed and efficiency by minimizing the amount of data transferred.

- **Application Layer -Layer7**

This is the only layer that interacts directly with the data of the user.

Software applications, such as web browsers and email clients, rely on the application layer to initiate communications. However, it should be clear that client software applications are not part of the application layer.

The application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user.

- **Application layer protocols include HTTP and SMTP.**

### 2.3 Network Protocols

In networking, a protocol [4] is a set of rules for formatting and processing data. They provide computers with a common language. Computers on a network can use very different software and hardware, yet the use of protocols allows them to communicate with each other regardless of these differences.

On the Internet, there are different protocols for different types of processes. In the previous section, we mentioned some protocols found at different layers of the OSI model.

Below are the definitions of the aforementioned protocols. These definitions are very brief, as the focus of this document is not on network protocols.

Hypertext Transfer Protocol (HTTP)
The Hypertext Transfer Protocol [5] (HTTP) is used to load pages on the Internet via hyperlinks. HTTP is a communication protocol (at the application layer of the OSI model) used for distributed and collaborative hypermedia information systems. This protocol is the communication basis of the World Wide Web (WWW), where hypertext documents include hyperlinks to other resources that the user can easily access. In short, the HTTP protocol is used to load pages on the Internet via hyperlinks.

Simple Mail Transfer Protocol (SMTP)
The Simple Mail Transfer Protocol [6] (SMTP) is a communications protocol used to send and receive email messages over the Internet. Email servers and other message transfer agents use this protocol to send, receive, and transmit email.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

Transmission Control Protocol (TCP)

The *Transmission Control Protocol* [8] (TCP) is one of the core protocols in the TCP/IP suite. It sits between the application and network layers, which are used to provide reliable delivery services. This protocol ensures secure and efficient data transmission over the Internet. TCP plays a vital role in managing the flow of data between computers, ensuring that information is delivered accurately and in the correct sequence.

User Datagram Protocol (UDP)

The User Datagram Protocol [9] (UDP), a transport layer communication protocol, is a very common protocol for voice and video traffic. Unlike TCP, it is connectionless and does not guarantee delivery, order, or error checking, making it a lightweight and efficient option for certain types of data transmission.

Internet Group Message Protocol (IGMP)
The Internet Group Message Protocol [11] (IGMP) is a protocol that allows multiple devices to share an IP address so they can all receive the same data. IGMP is a network layer protocol used to configure multicasting on networks using IP version 4 (IPv4); specifically, this protocol allows devices to join a multicast group.

Internet ntrol Message Protocol (ICMP)Co
The Internet Control Message Protocol [10] (ICMP) is a network layer protocol. It is mainly used in network equipment, such as routers, and used for error handling at the network layer. Since there are several types of errors at this layer, ICMP can be used to communicate and resolve these errors.

Internet Protocol (IP)

The Internet Protocol [7] (IP) is a set of requirements that allows devices to communicate with each other over the Internet. Every device connected to the Internet has a unique IP address that allows data to be sent and received accurately. This protocol can be used with several transport protocols, such as TCP and UDP.

IPsec

IPsec [12] is a group of protocols for securing connections between devices. This protocol helps keep data sent over public networks secure. It is often used to create virtual private networks (VPNs) and works by encrypting IP packets and authenticating their origin.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

## 2.4 Other important definitions

There are other definitions that may be important throughout the guide and are not covered in the previous sections.

These definitions are presented in this section.

VPN

A Virtual Private Network (VPN) is an encrypted connection over the internet from a computer to a network. The encrypted connection helps ensure that sensitive data is transmitted securely, prevents unauthorized parties from eavesdropping on traffic, and allows the user to work remotely.

Secure Sockets Layer (SSL)

The Secure Sockets Layer (SSL) is a security protocol that provides privacy, authentication, and integrity to Internet communications.

Transport Layer Security (TLS)

Transport Layer Security (TLS) is a security protocol that provides privacy and data integrity for Internet communications. Implementing this protocol is standard practice for building secure web applications.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

# 3. Cybersecurity Laws and Standards in Portugal and Spain

The growing digitalization of services and the rise in cyberthreats have led governments around the world to develop specific legislation to protect critical infrastructure, sensitive data, and their citizens. In both Portugal and Spain, cybersecurity legislation and regulations have evolved to address these threats, with the aim of protecting the integrity of digital infrastructure, ensuring data privacy, and strengthening resilience to cyber incidents.

Both countries, as members of the European Union (EU), follow common guidelines established in European legislation, especially concerning the General Data Protection Regulation (GDPR) and the European Directive on Network and Information Systems (NIS). However, each country also has its own specific laws and regulations that reflect its legislative specifics and the challenges facing today's society in the field of cybersecurity.

This chapter examines cybersecurity laws and regulations in Portugal and Spain, covering both national regulations and obligations arising from European directives. The analysis provides a comprehensive overview of each country's preparedness to address cyber threats, as well as the similarities and differences in their legislative approaches.

## 3.1 CNCS

The National Cybersecurity Center (CNCS) acts as operational coordinator and expert authority on cybersecurity for state entities, operators of National Critical Infrastructures, essential service operators and digital service providers, guaranteeing the use of the cyberspace as a space of freedom, security and justice, for the protection of the sectors of society that embody national sovereignty and the democratic rule of law.

**Comentado [MT5]:** I suggest including a clarification: "The Portuguese National Cybersecurity Center (CNCS, from its Portuguese acronym) "

The CNCS acts in various areas, such as the management of cyberspace incidents of national interest, through the Center for Studies on Computer Incident Response Team (CERT.PT), national cooperation, standardization, awareness-raising, and training. To this end, it provides frameworks and tools to help organizations mature in cybersecurity, provides technical recommendations, conducts inspections, courses, and awareness-raising activities, along with content on best practices and reports that analyze the country's state-of-the-art in these areas.

For more information, click here.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

### 3.2 INCIBE

The National Cybersecurity Institute (INCIBE, from its Spanish acronym) works to strengthen digital trust, increase cybersecurity, and foster resilience in order to contribute to the digital market and promote the safe use of the cyberspace in Spain.

Comentado [MT6]: The Spanish National Cybersecurity Institute

INCIBE is an institute dependent on the Ministry of Digital Transformation and Public Service through the State Secretariat for Digitalization and Artificial Intelligence. It has established itself as a benchmark for the development of cybersecurity and digital trust for citizens, academic and research networks, professionals, businesses, and especially for strategic sectors.

With its activities based on research, service provision, and liaison with relevant stakeholders, INCIBE contributes to building cybersecurity at the national and international levels.

INCIBE's main missions are the following:

- Improving cybersecurity and digital trust among citizens and institutions, Spanish public companies and private companies in Spain.
- Protect and defend citizens, Spanish public institutions and private companies in Spain.
- Strengthen the Spanish cybersecurity sector.
- Promote Spanish R&D&i (Research + Development + Innovation) in the field of cybersecurity.
- Identify, generate, attract, and develop professionals in the cybersecurity sector.

For more information, click here.

### 3.3 Law No. 46/2018

According to the Official State Gazette, Law No. 46/2018, of August 13 [13, 14] establishes the legal framework for cyberspace security, transposing Directive (EU) 2016/1148of the European Parliament and of the Council of 6 July 2016 on measures for achieving a high common level of network and information security across the Union.

The Cybersecurity Legal Framework applies to Public Administration bodies, critical infrastructure operators, essential service operators, digital service providers, as well as any other entities that use information networks and systems, particularly in the area of voluntary incident reporting.

Chapter II establishes the National Cybersecurity Structure, which includes the High Council for Cybersecurity as a specific advisory body to the Prime Minister on cybersecurity matters. This chapter also establishes the National Cybersecurity Center as the National Cybersecurity Authority and the CERT.PT as the National Computer Security Incident Response Team.

Chapter III determines the entities to which the Cybersecurity Legal Framework applies,

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

and which must adopt security requirements and notify the National Cybersecurity Center of incidents with a significant impact on the security of their networks and information systems.

Finally, Chapter IV establishes the supervisory and sanctions regime, and Chapter V establishes the final provisions, highlighting the identification regime for essential service operators and digital service providers.

### 3.4 Decree-Law No. 65/2021

Decree-Law No. 65/2021 of 30 July [15] defines the Legal Framework for Cybersecurity in Portugal, listing the obligations of entities covered by cybersecurity certification and transposing Regulation (EU) 2019/881 of the European Parliament (17 April 2019) into national law. This Decree-Law also regulates Law 46/2018, presented previously.

Therefore, all Public Administration Agencies, Critical Infrastructure and Essential Service Operators, and Digital Service Providers are required to:

- Inform the CNCS of the identity and contact information of your organization's security officer and permanent contact person.
- Develop an information security plan.
- Prepare an inventory of all assets and communicate it to the CNCS.
- Prepare annual information security reports and submit them to the CNCS.
- Conduct a risk assessment of all assets that ensure the continued operation of networks and information systems.
- Report security incidents to the CNCS as soon as possible.

### 3.5 Regulation No. 183/2022

Regulation 183/2022 of the Security Office establishes a technical instruction on communication and information related to permanent points of contact, the security officer, asset inventories, annual reports, and incident reporting.

### 3.6 National Data Protection Commission

The National Data Protection Commission (The CNPD is an independent administrative body, with legal personality under public law and powers of authority, endowed with administrative and financial autonomy, which works alongside the Portuguese Parliament.

Comentado [MT7]: Which country?

The CNPD watches and supervises the compliance of the General Data Protection Regulation (described immediately below) and other laws, as well as other legal and regulatory provisions on the protection of personal data, in order to defend the rights, freedoms and guarantees of natural persons in the processing of their personal data.

### 3.7 General Data Protection Regulation

The General Data Protection Regulation (GDPR) [16, 17] is a European law (EU 2016/679) that establishes rules on the protection, processing and free movement of

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

personal data of natural persons in the countries of the European Union.

The General Data Protection Regulation (GDPR) strengthens existing rights, establishes new ones, and gives citizens greater control over their personal data. It includes the following measures:

- Easier access for citizens to their own data: This includes providing more information about how data is processed and ensuring that this information is available in a clear and understandable manner;
- A new right to data portability: Facilitates the transmission of personal data between service providers;
- Clarification of the right to data deletion: Whenever a person does not allow their data to be processed further and there are no legitimate reasons for retaining it, it will be deleted;
- Right to know when a personal data breach has occurred: Companies and organizations must notify the competent data protection supervisory authority and, in cases of serious data breaches, also the affected individuals.

The GDPR can be applied when:

- An entity is established in the European Union (EU) (applies regardless of whether processing takes place in the EU);
- An entity not established in the EU provides goods or services (even free of charge) to EU citizens. The entity is a government body, a public or private company, a natural person, or a non-proft organization;
- An entity not established in the EU but which monitors the behavior of persons located in the EU, provided that such behavior takes place in the EU.

Organizations also have the obligation to COMPLY with the following:

1. Appoint a data protection officer;
2. Adopt information privacy and security policies;
3. Conduct a Data Protection Impact Assessment;
4. Obtain consent from interested parties for specific processing purposes;
5. Process the data collected for specific, explicit and legitimate purposes;
6. Maintain records of data processing activities;
7. Provide information to interested parties;
8. Guarantee the rights of access, rectification, deletion and opposition;
9. Guarantee the rights to restriction of processing and data portability;
10. Keep data only as long as necessary;
11. Apply the principles of privacy by design and privacy by default;
12. Apply good practices and appropriate security measures;

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

13. Sign written contracts with subcontractors;
14. Report data breaches and security incidents;
15. Request, where appropriate, prior consultation with the CNPD for data processing;
16. Conduct compliance audits.

It should also be noted that it is the entities themselves that must demonstrate their compliance with the regulations, and not, as was previously the case, where it was the regulator who had to demonstrate non-compliance.

### 3.8 ISO/IEC 27000

ISO 27000 is a set of certifications for information security and data protection for businesses and public organizations. The ISO 27000 family of certifications was developed in collaboration between ISO and the International Electrotechnical Commission, another organization dedicated to standards, hence the name ISO/IEC 27000.

They serve as the basis for creating an Information Security Management System (ISMS) in small, medium-sized, and large organizations. The ISMS brings together an organization's information protection policies, procedures, guidelines, and resources. The system must be aligned with business objectives and jointly managed by the company.

### 3.9 NIS 2 Directive

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 [18]—currently under transposition—on measures for a high common level of cybersecurity across the Union, amends Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repeals its predecessor, Directive (EU) 2016/1148 (NIS 1 Directive).

In this context, the NIS 2 Directive aims to achieve the same three objectives as its predecessor, namely:

- Require Member States to ensure a high level of cybersecurity;
- Strengthen European cooperation between authorities responsible for cybersecurity;
- Require key operators in key sectors of our society to adopt the necessary security measures and notify the relevant authorities of any incident that has a significant impact on the provision of their services.

The central objective of the NIS 2 Directive is also to eliminate the deep differences that have arisen in the context of the implementation of the NIS 1 Directive among Member States, seeking greater harmonization by establishing minimum standards on the functioning of a coordinated regulatory framework, among other measures.

The main differences between the NIS 2 Directive and the NIS 1 Directive are summarized below:

- The scope of NIS 2 has been greatly expanded as new sectors and new types of entities within existing sectors have been added;

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

- The structure of the sectors covered has changed. There are two groups of sectors: Critically Important Sectors and Other Critical Sectors;
- The categorization of covered entities has changed in this Directive, covered entities are divided into essential entities and important entities;
- Greater precision and reinforcement of the cybersecurity risk management measures that organizations must adopt;
- Consideration of supply chain cybersecurity;
- More detailed, specific and optimized rules for reporting cybersecurity incidents;
- Further specification of the supervisory powers of cybersecurity authorities;
- Attribution of liability to the individuals responsible for the covered entities and concern for their cybersecurity training;
- Harmonized sanctioning framework at EU level, more robust and with higher fines.

### 3.10 Cyber Resilience Act

The Cyber Resilience Act (CRA) is a European legal directive that imposes a series of requirements and obligations that will oblige all manufacturers, software developers, importers, suppliers and other parties involved in the supply of digital products in Europe to take security seriously and efficiently.

Applying the CRA to the entire lifecycle of this product category requires stakeholders to include effective cybersecurity measures or use secure development practices ranging from security by design and construction to personal data protection (in line with GDPR), as well as risk management and incident management, leading the entire supply chain to devise rapid and efficient mitigation processes to address vulnerabilities and other security-related issues in their products.

Also, in the context of the CRA, if a manufacturer becomes aware of a cybersecurity risk, they must take immediate steps to address it, including notifying users and Computer Security Incident Response Teams (CSIRTs) as soon as possible. In these cases, they must also cooperate with national authorities in the investigation and resolution of cybersecurity incidents related to their products.

These directives complement a whole series of laws and measures that, in isolation, address or mitigate specific problems.

### 3.11 What is the applicable legislation?

Since this directive is not transcribed into Portuguese law, the directive approved by the European Parliament is indicated as a reference.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

### 3.12 What is the motivation for this measure?

Nowadays, the main vectors used in cyberattacks are based on vulnerabilities and defects in products, both hardware and software.

In today's globalized world, with organizations interconnected and connected to the global network, a cybersecurity incident affecting a single product tends to impact the entire organization and can quickly spread to the entire supply chain and customers, ultimately spreading across the country or even across borders in just a few minutes.

Therefore, it is essential to have control and also to be able to react quickly to any vulnerability or flaw identified or reported by researchers. In this context, effective response policies by software manufacturers or developers are essential.

Consumers will be better equipped to make informed and secure decisions when products are designed to be updated and patched to address potential vulnerabilities, and when they have access to all relevant information about the product's cybersecurity features.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

## 4. Update of Software and Patches

In the information age, the era we live in, the use of electronic devices such as computers and mobile phones has become essential. All the devices we use daily are based on operating systems and applications. These are software systems developed and implemented by humans and, as such, can contain errors, which are subsequently detected and corrected.

Software updates and patches are therefore crucial practices for system security [19, 20, 21, 22, 23].

As long as the errors are not corrected, they can lead to two different types of situations:

- System or application malfunction, which may lead to unexpected results;
- Even if the system is working properly, the flaw may have already been exploited by someone who has detected it before. This flaw can be used in a disguised manner to compromise credentials or other information on the system in question. This misuse can extend to using a compromised system for spying or stealing the credentials of other players connected to the same network.

Patches correct these vulnerabilities and protect against cyberthreats. A software update improves functionality and user experience, fixes issues, introduces new features, and optimizes performance. Over time, vulnerabilities are eliminated.

While updating software is often a nuisance, ignoring these updates can have serious consequences, as known vulnerabilities are often exploited by hackers to gain access to systems, as explained above.

Reasons why it is important to update your software:

- Troubleshooting security flaws: Security is the main reason to update software immediately. Software vulnerabilities can be considered open doors for hackers to enter a computer and, for example, install malware on systems. Security patches block these doors in the software and protect a device from attacks;
- New features: Software updates often add new features and may remove old features that are no longer needed;
- Data protection: Updating software helps mitigate security vulnerabilities, allowing for better data protection;
- Improve performance: Not all patches are security-related. Bugs may be found in a program, or it may need to be improved, and there are patches that help with this, ultimately resulting in improved software performance.
- Ensure compatibility: Software vendors release updates to ensure their software is compatible with the latest technology, otherwise compatibility issues may occur.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

A series of tips for updating the software are as follows:

- Configure automatic updates: Nowadays, most programs already offer the option of automatic updates and this is the easiest way to keep your software up to date without having to check for updates manually;
- Check for updates regularly: If you prefer to update the software manually, you must check for updates regularly;
- Update all software: You should not only update the operating system, but also all the software and applications on a device.
- You should be aware of fake update scams.

This is a type of attack in which attackers try to trick users into downloading and installing a malicious file that pretends to be a software update. The best way to avoid these scams is to never download or install software updates from unknown or suspicious sources.

## 5. Secure Passwords

A password serves as an authentication mechanism [24], providing proof of knowledge of a secret that enables the user to authenticate. Passwords protect accounts and electronic devices from unauthorized access and help keep sensitive information secure.

The complexity of the password plays a crucial role, since the more complex it is, the more difficult it is to decipher, protecting the user's information from cyber threats and hackers more effectively. Below are some aspects to keep in mind when creating a strong password:

- Password complexity: Passwords should be complex, i.e., at least 8 characters and a combination of uppercase, lowercase, and special characters [25]. The use of personal information such as date of birth, name, etc. should be avoided;
- Using unique passwords: Passwords should not be reused across multiple accounts If a password is compromised, the potential impact is limited to a single account, reducing the overall risk.

Comentado [MT8]: Mentioned below

Another important aspect is the use of the two-factor authentication(2FA). This is an essential security measure that adds an extra layer of protection to the use of strong passwords. 2FA requires a second authentication factor, such as a code sent by SMS, email, or a code generated by an application that generates tokens for this purpose.

Using two-factor authentication is very important because if a password is compromised and that account has implemented this mechanism, the risk of the account being compromised is lower.

This method is fairly easy to implement, as many services already offer built-in 2FA options, and the setup process is straightforward. 2FA is recommended for all accounts, but especially for the sensitive and most important ones, such as email accounts, accounts

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

in financial systems, etc.

In addition to the above advice, there are also behaviors that should be avoided, such as the following:

- Using the same passwords on different accounts. It is a practice to avoid, since once one of these passwords is discovered, multiple platforms and accounts could be compromised;
- Writing down passwords on paper is a poor practice. Even if disguised, this practice is unsafe and should not be used;
- Another common method is storing passwords in text documents or spreadsheets. While more secure than the previous methods, this practice should still be avoided since these files can also be accessed.
- Storing credentials in the browser is not a good practice, as most browsers do not incorporate two- or multi-factor authentication features, meaning all an attacker would have to do is gain access to your device.

Comentado [MT9]: I suggest deleting this as it has just been mentioned.

As more and more applications and systems are used, it becomes difficult to memorize all the passwords, especially if they are complex (as they should be). To solve this problem and avoid the above behaviors, it is advisable to use password managers.

A password manager is very useful for securely storing passwords, automatically filling in login credentials when needed, and can also generate secure passwords (where you can change the password length, use of special characters, etc.).

The following list presents several suggestions for password managers:

- Bitwarden ;
- Proton Pass ;
- KeePass ;
- 1Password.

To ensure proper credential and access management, it is crucial to scrutinize any request for access data that falls outside the normal context of application use. Even if the request appears legitimate, whether by email or any other means, resource or application managers never need to know the user's credentials. Therefore, this data should never be shared with third parties.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

# 6. Access Control

Access control is a fundamental component of data security [26, 27, 28]. It determines who can access certain data, applications and resources and under what circumstances. Just as keys and pre-approved guest lists protect physical spaces. Access control policies protect digital spaces. Access control policies rely heavily on techniques such as authentication and authorization, which allow organizations to explicitly verify that users are who they say they are and that they are granted the appropriate level of access based on context, such as device, location, role, and so on. Access control prevents sensitive information from being stolen by malicious actors or other unauthorized users.

Rather than managing permissions manually, most security-minded organizations rely on identity and access management solutions to enforce access control policies.

There are four main types of access control. Each of which manages access to confidential information in a unique way:

- Discretionary Access Control (DAC): In this type of model, each object in a protected system has an owner, and the owner grants users access to its description. DAC allows resources to be controlled on a case-by-case basis;
- Mandatory Access Control (MAC): In this type of model, access is granted to users in the form of authorization. A central authority regulates access rights and organizes them into tiers, the scope of which is uniformly expanded. This model is very common in government and military contexts;
- Role-Based Access Control (RBAC): In this type of model, access rights are granted based on defined business roles, not on an individual's identity or level of experience. The goal is to provide users with only the data they need to perform their roles, and nothing more.
- Attribute-based access control (ABAC): In this type of model, access is granted flexibly, based on a more granular combination of access control attributes, and helps reduce the number of role assignments.

## 6.1 Good practices in access control

There are several practices to consider when implementing access control. This section outlines access control best practices.

- **Connect access rights to user roles**

Role-based access control: Simplifies the complex challenge of access control and increases security. This type of access control configuration associates organizational roles with appropriate access privileges.

Role-based access systems improve operational efficiency. There is no need to assign access rights to individual employees. New employees receive privileges according to their role in the organization.

Automated access controls provide the correct privileges and can remove obsolete access

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

rights when workers change roles or leave the organization.

Role-based access control also helps avoid the problem of shared accounts. Users often share accounts to manage projects or access administrative tools, which is extremely insecure and can expose the entire network to external attacks. To avoid this problem, clearly define user roles and ensure each user can access the tools they need.

### 6.2 Use the principle of least privilege to guide access control

The principle of least privilege is a fundamental concept of access management. According to this idea, network users should have minimal access to data and applications. Users should be able to access the resources they need for their professional tasks, but everything else should be out of their reach.

- Restricting access within the confines of the network is a fundamental aspect of cybersecurity systems. If attackers gain access, they will not be able to easily move within the network. Security teams can more easily contain threats and protect sensitive systems.
- Design a multi-level access control system

Role-based controls and minimum access principles are only part of the access control challenge. Authentication and network security layers also help to control access and protect resources. This strengthens network boundaries and reduces the risk of malicious attacks.

Implementing multifactor authentication (MFA) for critical assets. MFA requires more than one authentication factor before granting access, making it much more difficult to breach network defenses.

Firewall access control lists provide additional resilience to access controls, and it is also possible to combine role-based controls with attribute-based controls. This allows IT teams to add additional protection to critical assets.

Training adds another layer of security. It is important for employees to receive training on password hygiene and secure remote work. It is also important to understand how access controls work.

- **Understanding the user environment**

Access control is based on knowledge. Organizations need to know who uses your systems, when they use them, and what resources they use.

It is important to create and maintain a complete user database. Each user profile should contain clear information about their role in the organization, which must be reflected in their access privileges according to control policies.

User management applies not only to employees but also to third parties, clients, and consumers, ensuring proper access control and security across all user types.

Avoid duplicate user accounts and delete unused profiles when employees leave. Authorized users should be uniquely identified. This allows you to securely authenticate them and track their activity while they use company resources.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

- **Continuously manage the access system**

Automation reduces the workload of access control, but regardless, the security officer must still monitor user access patterns. In addition, periodic audits should be conducted to ensure access controls are functioning properly.

It is essential to focus on auditing important access control tasks:

- Technical audits: Identify user experience problems: This allows administrators to optimize privileges and authentication processes;
- Security audits: Identify alerts and potential attacks, and suggest ways to strengthen controls over critical resources;
- Account audits: Check for orphaned accounts, shared privileges, or unduly high access levels.

**Tip 1 - Centralize access management**

Avoid regularly using access control lists managed by resource owners. This makes it more difficult to restrict user privileges. Instead, create a central database of access rights before implementing access controls.

Centralization makes it easier to control the privileges associated with roles or individuals. Administrators can provide access policies for all users and change settings instantly. They can add attribute-based controls to documents or data and easily add or remove users.

**Tip 2 - Automate unlinking to improve security**

User privileges should terminate when employees leave an organization. But without proper management, profiles can remain active for weeks or months. External attackers take advantage of orphaned profiles to mount attacks that are very difficult to detect. That Is why it Is important to remove all privileges immediately.

Automated profile management solves this problem. Connect your access controls to systems that eliminate all user rights. This extends beyond on-premises network resources to cloud services, third- party applications, and physical access control barriers.

**Tip 3 -Consider flexible access controls**

Users may need temporary access to specific databases, or they may need to write privileges to edit documents that are normally denied to them. Security officials may want to geographically limit resources if they are concerned about attacks from a specific country.

Role-based controls tend to be quite inflexible. But administrators can supplement RBAC with granular controls as needed. Context-based controls take into account location, device types, access time, and many other factors.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

**Tip 4 - Ensure access systems have reporting tools**

Access control is an important part of compliance strategies. But controls are useless if they do not generate evidence that regulators can review. Choose systems with audit capabilities that log all access events.

Automated, rule-based tools create reports tailored to regulatory needs. For example, an e-commerce retailer may need data on access to cardholder information. A robust access control system will provide this information upon request.

**Tip 5 - Cloud-native access systems**

Modern businesses often turn to SaaS tools to store information, share documents, and manage customer data. Employees can create new cloud resources instantly, sometimes without IT teams' knowledge.

Implement systems that automatically discover new cloud applications and seamlessly integrate them with existing access systems. Your central identity registry must be cloud-compatible. And all cloud applications must be subject to your authorization controls. This approach helps secure your network architecture and take advantage of the benefits of cloud computing.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

# 7. Network Monitoring Systems

Network monitoring systems include software and hardware tools that can monitor various aspects of a network and its performance, such as traffic, bandwidth utilization (i.e., the rate at which data flows through the network), and uptime [29, 30, 31]. These systems can detect devices and other elements that connected to or interact with the network and can provide status updates.

Network administrators rely on these types of systems to help them quickly detect device or connection failures or problems, such as traffic congestion that limits data flow. The ability to detect problems extends to parts of the network that traditionally lie beyond its boundaries. These systems can alert administrators of problems via email and present reports through network analysis.

## 7.1 Intrusion Detection System (IDS)

An intrusion detection system (IDS): It is a network security tool that monitors network traffic and devices to detect known malicious activity, suspicious activity, or security policy violations.

IDSs can help accelerate and automate threat detection on the network, alerting security administrators to known or potential threats or sending alerts to a centralized security tool. Such a tool can combine data from other sources to help security teams identify and respond to cyberthreats that may bypass other security measures.

An IDS cannot prevent security threats on its own. Currently, IDS capabilities are integrated or incorporated into an Intrusion Prevention System.

## 7.2 Intrusion Prevention System

An Intrusion Prevention System (IPS) monitors network traffic to detect potential threats and automatically blocks them by alerting the security team, terminating dangerous connections, removing malicious content, or activating other security devices.

IPS solutions evolved from IDSs; such a system provides the same threat detection and intelligence capabilities as an IDS, plus automated threat prediction capabilities.

## 7.3 Endpoint Detection and Response

Endpoint detection and response (EDR) is software that uses real-time analytics and AI-powered automation to protect an organization's users, end devices, and assets from cyberthreats that go beyond antivirus or other traditional endpoint security tools [36, 37, 38].

An EDR analyzes data and, if it identifies anything suspicious, it can automatically respond to, prevent or minimize the damage from any threats it may encounter.

## 7.4 Security Information and Event Management

Security Information and Event Management (SIEM) is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

they have the opportunity to disrupt business operations. SIEM systems help enterprise security teams detect anomalies in user behavior and use AI to automate many of the manual processes associated with threat detection and incident response.

### 7.5 Main Advantages of Network Monitoring Systems

The main advantages for companies to use network monitoring systems are as follows:

- Clear network visibility: By monitoring the network, administrators can get a clear picture of all the devices connected to the network. They can also see how data moves between devices and quickly identify and correct problems that could jeopardize performance and cause outages
- Increasing complexity: Modern businesses depend on a range of business-critical and internet-dependent services. This includes cloud service providers, internet service providers, and others. Each service operates over the internet, making it susceptible to performance fluctuations caused by internet outages or routing issues. Insight into network components beyond your control allows you to monitor issues that could affect employees or customers;
- Better utilization of IT resources: the hardware and software tools of the network monitoring systems reduce manual workloads for IT teams. This means valuable IT staff have more time to focus on critical projects for the organization;
- Early perception of future infrastructure needs: Network monitoring systems can provide reports on the performance of network components over a defined period. By analyzing these reports, network administrators can anticipate when the organization will need to consider upgrading or implementing a new IT infrastructure;
- Ability to identify security threats more quickly: Network monitoring helps organizations understand how their network is performing normal network activity. This way, when unusual activity occurs, such as an unexplained increase in network traffic, it is easier for administrators to quickly identify the problem and determine if it could be a security threat.

### 7.6 Network Monitoring Protocols

Earlier in this guide, we briefly discussed network monitoring protocols. For a recap, please refer to section 2.3.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

# 8. Backup and Data Recovery

Data backup and recovery together comprise the process of duplicating data and storing it in a secure location so that it can be restored in a usable manner in case of loss or damage [41, 42, 43, 44]. Ideally, this backup should be immutable, i.e., not altered after it has been created, in order to protect against mutations such as ransomware1 and other types of attacks.

It is important to emphasize that data backup systems should only be turned on during backup and turned off afterward.

The main difference between the backup and recovery of data is that the process of backup is a means of saving and storing data securely so that it can be accessed later if needed. Recovery is a process by which data is recovered and restored from backup to production systems. Reliable backups and rapid recovery ensure business continuity and resilience.

Why are data backups and recovery important?

Data is essential to every organization and can provide a competitive advantage. The primary, and perhaps most important function of data backup and recovery is to preserve critical data in the event of loss or damage.

Furthermore, in the event of a disaster, only with such a strategy can operations be maintained and the company continue to function. Another reason why it is important to have such a plan is to preserve records, which can also be important from a legal perspective.

Developing a data backup and recovery strategy is essential. A database can be rendered unusable by a hardware failure, a software failure, or both. You may also encounter storage issues, power outages, or other failures, and each failure scenario requires a different data recovery approach, so having a well- defined data recovery strategy is very important.

## 8.1 Types of Backup Data

Evaluating which type of backup is appropriate for specific business needs is very prudent.

There are three main types of backups for backing up digital assets:

- Full Backup (full backup) - the most basic and complete method, in which all data is sent to another location;
- Incremental Backup: All the files that have changed since the last backup are copied;
- Differential Backup: Copies are made of all the files that have changed since the last full backup.

[1] Ransomware is a type of malware that holds the victim's sensitive data or device hostage, threatening to lock it (or worse) if the victim does not pay a ransom to the attacker.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

Not all organizations can support all types of backups, as network capacity can vary from organization to organization.

Choosing the right backup method requires a tactical approach, a choice that can help organizations achieve the best level of data protection without placing excessive demands on the network.

However, before determining which backup method best suits a business's needs, it is worth understanding the advantages and disadvantages of the three main backup types mentioned above.

***Full Backup***

A full backup consists of creating a complete copy of an organization's files, folders, data, and hard drives. It is the perfect protection against data loss when you consider the speed and ease of recovery. However, the time and resources required to copy all data can make this option less desirable for many organizations.

**These are the advantages of making a copy of backup:**

- Fast restoration time;
- Storage management is simple, as all data is stored in a single version;
- Simple version control allows to maintain and restore different versions without effort;

***Searching for files is very easy.***

**Listed below are the disadvantages of performing a full backup:**

- Requires more storage space than other methods;
- Depending on its size, it can take a long time to make a backup from the archives;
- The need for additional storage space makes the method of backup more expensive;
- The risk of data loss is high, as all data is stored in a single location.

**In what situations should a full backup be made?**

Small businesses that handle a small amount of data regularly may find a full backup a good option, as it does not consume much storage space or take a long time to back up.

### 8.2 Incremental Backup

Incremental backup consists of making a backup of all the files, folders, data and hard drives that have changed since the last backup activity. Only one backup is performed of the most recent changes, which consumes less storage space and results in a fast backup. However, recovery time is longer because more files need to be accessed.

The advantages of this method are as follows:

- Efficient use of storage space, as files are not fully duplicated;
- Extremely fast backups;

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

- They can be run as often as desired, with each increment being an individual recovery point.

The disadvantages of incremental backups are as follows:

- Restoration is time-consuming, as data has to be compiled from multiple backups;
- Recovery is only possible if all files in the backup are safe from corruption;

Searching for files becomes more complicated, as you must go through multiple backup sets to restore a specific file.

When should you use incremental backup? Companies that handle large volumes of data and cannot dedicate time to the backup process will find incremental backup methods effective, as they take up less storage space and facilitate faster backups.

### 8.3 Differential Backup

Differential backup is a cross between a full backup and an incremental backup. This method backs up files, folders, and hard drives that have been created or modified since the last full backup.

Only a small amount of data is backed up between the last backup and the current one, which consumes less storage space and requires less time and investment.

The advantages of a differential backup are listed below:

- It takes up less space than full backups;
- Faster restoration than incremental backups;
- Much faster backups than full backups.

The disadvantages are as follows:

- Possibility of failed recovery if any of the backup sets are incomplete;
- Compared to incremental backups, incremental backup takes longer and requires more storage space;
- Compared to a full backup, restoration is slow and complex.

When should differential backup be used? Small and medium-sized organizations that want to process large volumes of valuable data but cannot perform consistent backups will find the differential backup method useful.

### *8.4* Frequency of *Backups*

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

The frequency of backups depends on the importance of the data and how often it changes [4 5].

Ideally, data backups should be done regularly, for example, daily, weekly or monthly, depending on the type of data.

Important files that are frequently changed may require more frequent backups to prevent potential data loss.

### 8.5 The 3-2-1 *Backup Rule*

The 3-2-1 Backup Rule is designed to help simplify backup procedures and reduce the risk of data loss [46]. This rule helps to quickly recover data and resume operations by minimizing downtime.

This rule involves duplicating data three times, storing it on two different devices, and keeping a copy of the data off-site.

**Three copies of the data**

The first element of the 3-2-1 backup rule emphasizes having three backup copies of your data. This redundancy ensures that even if one copy becomes inaccessible or corrupted, there are still two additional copies available to restore your data. By maintaining multiple copies, you significantly reduce the risk of permanent data loss.

**Two Different Devices**

The second aspect of the 3-2-1 backup rule suggests storing backups in two different formats or devices. This diversification provides an additional layer of protection against specific types of failures.

For example, by having one copy on a physical external hard drive and another copy in the cloud, your data is protected against hardware failures and online security breaches. Diversifying your storage devices minimizes the chances of losing all your copies simultaneously.

**A copy stored off-site**

The final element of the 3-2-1 backup rule is to keep a copy of the data off-site. This backup should be in a location other than the primary area where the data is created or maintained.

This helps protect backups from physical hazards such as fire, flood, theft, or other disasters that could affect the location where the backup is stored.

This standard establishes a solid foundation that balances diversity, redundancy, and off-site storage, ensuring the availability and resilience of key information. It is therefore a reliable method for organizations looking to improve their data backup practices.

Throughout the explanation of the standard, some of the advantages of applying it have already been mentioned. The main benefits of this standard are listed below:

- Data redundancy and protection against power failures and hardware issues;
- Mitigating data loss risks;

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

- Improving disaster recovery capabilities;
- Protection against ransomware attacks.

Failure to comply with the 3-2-1 data backup standard exposes organizations to unnecessary and significant risks, including:

- Vulnerability to data loss and corruption;
- Greater impact of natural disasters;
- Increased susceptibility to ransomware attacks.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

# 9. Disaster Recovery Plan

A Disaster Recovery Plan (DRP for short) is a detailed document that describes how an organization should effectively respond to an unforeseen incident and resume operations [47, 48]. These plans help ensure businesses are prepared for various types of disasters, such as power outages, ransomware and malware attacks, natural disasters, and more.

A solid DRP helps to restore connectivity quickly and efficiently, and to repair data loss after a disaster.

Similarly to DRP, a Business Continuity Plan (BCP) is part of a disaster recovery process that helps businesses restore normal operations after a disaster. BCPs typically take a broader view of threats and resolution options than DRPs, focusing on what a company needs to restore basic business functions after an incident.

An Incident Response Plan(IRP) is a type of disaster recovery plan that focuses exclusively on the cybersecurity and the threats to information systems.

An IRP clearly outlines an organization's emergency response from the moment it detects a threat through mitigation and resolution. Such a plan addresses the specific damage caused by a cyberattack and focuses exclusively on preparing for threats to technology, IT infrastructure, business operations, and reputation.

## 9.1 Importance of a Disaster Recovery Plan

Disaster recovery plans play a key role in developing a comprehensive security plan that helps assure stakeholders, customers, and investors that a company is operating responsibly. Companies that fail to take the necessary steps to ensure their preparedness face a range of risks, including costly data loss, operational downtime, financial penalties, and reputational damage.

The benefits that companies that invest in creating a solid DRP can enjoy are the following:

- Less downtime: Many companies depend heavily on technology for their day-to-day operation, so when an incident occurs, it can have serious consequences. Disaster recovery plans, when robust and rigorously tested, help businesses get back up and running as quickly as possible after an incident;
- Lower recovery costs: Recovering from an incident can be expensive. According to an IBM report [49], the average cost of a failure in 2023 was around four million dollars, 15% more than in the previous three years. Companies with DRPs can significantly reduce business recovery costs and other consequences of an unforeseen incident.

## 9.2 5 Steps to Developing a Disaster Recovery Plan

Developing a Disaster Recovery Plan begins with a business process analysis, a risk analysis, and clearly defined recovery objectives.

While there's no single model, there are several steps organizations or companies— regardless of size— can take to ensure they have a process in place to address a variety of incidents.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

**Step 1 - Conduct a business impact analysis**

A business impact analysis (BIA) is a careful assessment of each threat a company may face and its potential ramifications. A robust BIA examines how a potential threat could affect aspects such as daily operations, communication channels, and employee safety.

**Step 2 - Analyze the Risks**

Different sectors and types of companies face different threats, so analyzing the risks is key to determine how to respond to each of them. Each risk can be assessed separately, considering both its likelihood and potential impact.

There are two widely used methods for determining risk: qualitative and quantitative analysis. Qualitative analysis is based on risk perception, while quantitative analysis is based on verifiable data.

**Step 3 - Create an Asset Inventory**

To recover from a cyber incident, it is important to have a comprehensive understanding of the company's assets. Conducting a periodic inventory helps identify hardware, software, IT infrastructure, data, and other assets that are critical to the company's operations. Various labels can be used to categorize data, which will be discussed later in the document.

**Step 4 - Establish Roles and Responsibilities**

The roles and responsibilities section of the disaster recovery plan is quite important. Without this section, it would be difficult to know what to do when an unforeseen incident occurs.

Although actual roles and responsibilities vary greatly depending on the type of business, below are some typical roles and responsibilities contained in most disaster recovery plans:

- Incident Reporting: You should designate a person (or persons) in each department whose sole responsibility is to communicate with management, stakeholders, and all relevant authorities when disruptive incidents occur.
- PRM Management: A PRM supervisor must be designated to ensure that team members carry out their assigned tasks and that the PRM is functioning properly.
- Asset Protection: Someone should be tasked with securing and protecting your most important assets when a disaster occurs and communicating their status to management and stakeholders.
- Communication with third parties: A person should be responsible for coordinating with the third- party providers you have contracted as part of your disaster recovery plan. This person should provide ongoing updates on the progress of the disaster recovery plan to all relevant stakeholders.

**Comentado [MT10]:** Please include full term and PRM in brackets (). I don't know what this stands for.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

**Step 5 - Test and Refine**

To ensure that the disaster recovery plan runs smoothly during a real incident, it must be implemented regularly and updated based on significant changes within the business. For example, if the company acquires a new asset after developing the disaster recovery plan, it will need to incorporate it into the plan to ensure its protection in the future.

The process of testing and refining the disaster recovery plan can be simplified into three stages:

- Creating an accurate simulation: It is important to create an environment that closely resembles the real scenarios the company may encounter.
- Problem identification: Throughout the test, failures and inconsistencies in the DRP should be identified and an attempt should be made to resolve the identified issues in the next iteration of the disaster recovery plan;
- Test backups: It is also important to test procedures for restoring critical systems after the incident has passed. Network connectivity, recovery of lost data, and, ultimately, the resumption of normal operations should all be tested.

## 9.3 Management of data resources in the company

Although remote work is not a common practice in non-tech companies, this work model is becoming increasingly common and accepted as a natural way of working. However, this may not apply to all areas of a company. A common approach in such cases is to directly expose certain services or resources so that remote employees can access these contents.

This practice is inadvisable, as it exposes the company to unnecessary risks of attack. One solution is to establish a VPN support system, allowing all users with access to work securely from another location. This way, employees work as if they were physically on-site.

As already mentioned, it is very important to implement a backup system that ensures that all company information can be partially or completely restored in the event of a disaster or a simple failure. A simple way to do this could be to copy the data to disks or network shares on separate servers.

However, one of the global threats that has emerged in recent years—ransomware—has exposed the fragility of this approach, compromising these methods of data protection.

The solution to this problem is to ensure that the backup storage is on another layer or on a different network, to which there is no direct network access from other servers. There are several software programs that help with this process.

It is important to emphasize that these backups must be easily accessible, as in an emergency situation they must be accessed as quickly as possible and also so they can be tested frequently to ensure their integrity and usefulness.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

# 10. Assets

An asset is something that has value to the organization and must be protected from its perspective [50, 51, 52, 53]. According to Law No. 46/2018 of 13 August (already mentioned HERE - INSERT), which establishes the Legal Framework for the Security of Cyberspace and outlines measures to ensure a high common level of security for information systems and networks throughout the territory of the European Union (EU), an asset is defined as “any information and communications system, equipment and other physical and logical resources (software applications and platforms) considered essential, managed or owned by the organization, which directly or indirectly support one or more services”.

An information system comprises not only hardware and software, but also assets of the following categories:

- Technological (hardware, software, systems and network devices);
- People;
- Information;
- Physical environment and locations;
- Contractual dependencies internal or external to the service;

## 10.1 Classification Levels

To effectively protect the information handled by each organization, it is necessary to define a set of categories that describe the data and quantify the level of protection required. Based on existing literature, five categories have been defined into which data can be divided and classified:

- Top secret;
- Restricted/Secret;
- Confidential;
- Internal;
- Public.
- Public

Information that may be disseminated without restrictions as to its content, audience, or time of publication. Its dissemination does not violate any relevant law (particularly privacy laws).

- Internal

Information accessible only to members of the organization. Information disclosed at this classification level should not be made available to the public without prior review to avoid repercussions.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

- **Confidential**

Information that is confidential and requires specific authorization to be accessed and processed. Disclosure of this type of information can cause personal injury, disruption to a subset of the organization, damage to business relationships, and loss of competitive advantage.

- **Restricted/Secret**

Restricted or highly confidential information that requires the utmost care in its handling. Disclosure of this type of information could result in significant privacy breaches, security risks for an individual or group of people, significant financial losses (fines, termination of contractual relationships), or legal action.

- **Top Secret**

The Top Secret level encompasses the same properties as the next level down (Restricted/Secret) and is the highest sensitivity category, requiring the highest levels of protection and access control. This category is used when strictly necessary, as unauthorized disclosure of such information could have extremely serious consequences, such as irreparable damage to the entity, lawsuits or claims, risk to life, and significant compromise to national security.

### 10.2 Documentation Management

Document management, regardless of its content and classification, requires the implementation and adherence to certain principles and best practices that guarantee sound document management, both for physical and digital documents. Proper document management not only facilitates efficient information retrieval but also ensures compliance with data protection regulations, such as the GDPR.

It is essential that all employees, workers, and collaborators understand the established policies and procedures to ensure the protection of information and minimize the risks associated with improper document handling.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

# 11. Email Management and Practices

## 11.1 Email Management

Email management refers to the practice of organizing, prioritize and manage emails in order to optimize productivity and efficiency [54, 55, 56]. It involves strategies for managing incoming emails, responding promptly, and organizing email archives for easy retrieval.

Some proven email management tactics and strategies include:

### Spend time on email

Just as one allocates time for other tasks, it is essential to do the same for managing one's email account. This approach ensures that one does not check email constantly throughout the day. The most effective strategy is to designate a specific block of time each day to address email account matters. While handling email once a day may be sufficient, it is more efficient to schedule multiple blocks of time for email throughout the day. Additionally, it is important to avoid multitasking while checking email in order to minimize distractions.

### Create tags, folders, and categories

One way to simplify email management is through organization, which involves creating labels, folders, and categories. There are no rules about how this organization should be done; it simply needs to be tailored to each individual. The key is to prioritize, group, and categorize emails. The greatest advantage of this is that it is easier to locate more specific emails with just a few clicks.

### "Touch-it-once"

The "touch-it-once" principle is based on making quick decisions when managing emails. The idea behind this method is that checking the same email multiple times is a waste of time. The idea is to only touch each email once, taking the appropriate action for that email (it can also be based on the 4 Ds—delete, delegate, defer, do).

Although the concept is easy to understand, it can be difficult to follow when it comes to email, because we tend to postpone responding. But adopting this strategy is important and can increase productivity.

### Minute rule

The minute rule is based on a simple concept: if responding to an email takes less than a minute, do it immediately. By handling such messages right away, you can quickly respond and archive them, helping to clear your inbox more efficiently.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

**Read from top to bottom, write from bottom to top**

Atish Davda, CEO of EquityZen, proposes a unique way to check your inbox. He tries to read emails in reverse chronological order and respond to them in chronological order. Atish explains: "This trick takes into account the fact that some people respond to emails immediately, which is sometimestriggers a "tennis match" of emails, consuming that hour you've set aside to deal with your entire inbox and leaving you behind.

If you respond to emails in chronological order, you're less likely to get caught up in back-and-forth emails and more likely to stay up to date.

**Knowing when to send emails**

Knowing how to manage email has as much to do with the type and volume of emails you receive as with what you send. One way to send fewer emails is to choose which conversations to have by email and which by phone. If you just need to provide simple information, an update, email works. But if you need to provide more complex information, it may be easier to communicate by phone, because if the topic is discussed via email, it can lead to a lot of back and forth exchange.

**Turn group email accounts into shared inboxes**

Most companies have group email accounts, which make it easy for people outside the company to get in touch with their brand. But this may not be the most ideal solution. These accounts experience a large flow of incoming emails, which is compounded by the fact that there is no easy way to assign emails to individuals and track these tasks. Incoming emails need to be organized so that each team member is clear about what they need to do.

One way to manage email is through the use of email management software. Email management software is a tool that helps users manage, prioritize, send, track, and organize emails. This type of software includes a variety of solutions that can be used by both individuals and businesses.

These are just a few of the most essential tips for better email management. In addition to these recommendations, there is a mnemonic that can be associated with email management: the 4 Ds.

The 4 D's of email management are as follows:

- Delete – immediately delete irrelevant or unimportant emails;
- Delegate – assign to the appropriate person the emails that another person may handle;
- Do – respond to emails that require immediate action;
- Defer – postpone handling emails that require more time or consideration for later.

In summary, for better email management, you should follow the tips described above, i.e. check your email at specific times of the day, use the 4Ds method to quickly process and

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

prioritize incoming emails, use email management tools or software to automate repetitive tasks and organize your inbox.

Consider grouping similar tasks together to increase efficiency and focus on handling high-priority emails first and postpone less urgent ones for later.

### 11.2 Protection against Phishing

Phishing is an attempt to steal someone's money or identity by getting them to reveal personal information (credit card numbers, bank details, passwords, etc.) through websites or emails that appear legitimate. Cybercriminals impersonate trusted companies in messages, often including fake links designed to capture sensitive information.

**How to recognize a message or email from phishing?**

*Phishing* is a popular form of cybercrime due to its effectiveness. Phishing techniques have become increasingly sophisticated, so you should be very vigilant about the emails you receive. The best defense is awareness and knowing what to look for.

**Some ways to recognize a phishing email include the following:**

- Urgent calls to action or threats: Emails or messages that claim you need to click or open an attachment immediately should make you suspicious. Creating a false sense of urgency is a common trick of phishing attacks and scams;
- Senders: Although it is not unusual to receive emails for the first time, specially if the person is not part of your organization, this could be a sign of phishing. Be extra cautious at these times. When you receive an email from someone you do not recognize, take a moment to examine it more closely;

> Advice
>
> Whenever you see a message that demands immediate action, you should stop for a moment and analyze it carefully. Are you sure it is real? Be cautious and stay safe.

**Incorrect spelling and grammar:**

- If an email contains obvious spelling or grammatical errors, it could be a scam. These errors are often the result of an incorrect translation from a foreign language, and are sometimes deliberate in an attempt to circumvent filters intended to block these attacks;
- Generic greeting: If the email starts with a generic “Dear Sir or Madam,” it is a warning sign that it might not actually be your bank or shopping site;
- Incompatible email domains: If the email claims to be from a trusted company, such as Microsoft or your bank, but is sent from another domain, it is likely a scam. Pay attention to subtle misspellings in the domain name, as this is a very common trick;
- Suspicious links or attachments: If you suspect an email may be a phishing attempt, do not open any links or attachments, as they may contain harmful content.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

Although these techniques are quite common in phishing emails, always be alert for other signs that may be suspicious. As mentioned, phishing techniques are becoming increasingly sophisticated, so you can never be too cautious.

### 11.3 Other practices

Using personalized institutional company email addresses for accounts that manage or handle information transactions is a best practice. In addition to increasing credibility, this helps other partners and customers better identify any attempts to impersonate the company.

An additional measure in this context is to include qualified digital signatures in emails, such as those appearing on a citizen's identity document, since these signatures allow the sender to be unequivocally validated.

In compliance with the rules defined by the GDPR, company employees with a "personal" email address on the company domain are restricted from being accessed by anyone other than the employee themselves.

This limitation prevents the email address from being accessed (and therefore used) by another member of the company. Therefore, it is recommended that addresses related to company areas or services be created in an anonymous format, without mentioning the names of the people who may manage that email address.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

## 12. Use of Servers

A server is a hardware or software device that processes and responds to requests sent over a network. A client is a device that sends a request and waits for a response from the server. This setup is known as the client-server model.

Servers play an important role in any network [57, 58, 59]. A server is typically a high-performance computer that uses specialized software or operating systems to store data and centralize resources in an office or business.

The role of servers is increasingly essential. Whether you are a small business or an established company, investing in a server can bring significant benefits that go beyond simple data storage. Some of the advantages of using servers include:

- Centralized data management: A server acts as a centralized hub for storing and managing company data, meaning that data is stored in one place, simplifying access and facilitating data management;
- Greater security: Businesses handle sensitive data, so security is a priority. A server offers security features, such as firewalls, encryption, and user authentication, that protect data from unauthorized access;
- Improving collaboration: With centralized file storage and sharing features, employees across a company can collaborate and work simultaneously on projects and access shared documents efficiently;
- Reliable backups: Data loss can have disastrous consequences for a business. A server offers reliable backup solutions, ensuring that a company's data is regularly backed up and can be easily restored in the event of an incident;
- Scalability: A server offers scalability, allowing the infrastructure to expand and adapt to the growing needs of a company without affecting performance;
- Remote access and mobility: In an age where remote work is becoming more common, a server provides remote access to company resources.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

## 13. Active Directory Account Management

Active Directory (AD): It is a directory service implementation that stores information about objects on computer networks and makes this information available to network users and administrators [60, 61, 62, 63, 64, 65, 66, 67]. It is a Microsoft software used in Windows environments.

An Active Directory stores information about objects on the network and makes this information easy to find and use for administrators and users. Active Directory uses structured data storage as the basis for a logical, hierarchical organization of directory information.

Security is integrated into Active Directory through login authentication and access control to directory objects. Administrators can manage directory data and organization across the network, and authorized network users can access resources from anywhere on the network.

**Active Directory also includes:**

- A set of rules, or schema, that defines the classes of objects and attributes contained in the directory, the restrictions and limits on the instances of these objects, and the format of their names;
- A catalog containing information about all objects in Active Directory. This allows users and administrators to find information about the directory, regardless of the domain in which the data is actually located;
- A query and indexing mechanism, so that objects and their properties can be easily published and found by users or network applications;
- A Business Continuity Plan that distributes directory data across a network. All domain controllers participate in replication and contain a complete copy of all directory information for their domain. Any changes to directory data are replicated to all domain controllers in the domain.

**The Active Directory structure incorporates the following components:**

- Computers and Users - Self-explanatory. Each account is described by attributes such as name, title, email address, and so on;
- Organizational units - elements that organize users, groups, computers, and other resources;
- Domains - a set of objects grouped into a client-server network and authenticated in a single database;
- Trees - a domain tree is made up of several domains that share a common schema or configuration;
- Forest - a hierarchical extension of a tree. It is an administrative boundary used to facilitate the management and authentication of multiple trees, domains, and objects.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

### 13.1 Trust Terminology (or Relationships)

- *Active Directory:* It relies on trust relationships to moderate access rights to resources between domains. There are different types of trust relationships, which are presented below.
- One-way trust: It occurs when a first domain allows access privileges to users in a second domain, but the second domain does not allow access to users in the first domain.
- Two-way trust: Occurs when there are two domains, and they allow access to both.
- External trust: Trust that connects domains in separate forests or non-AD domains. These connections can be non- transitive, one-way, or two-way.
- Privileged access management (PAM): One-way trust created by Microsoft Identity Manager between a production forest and a bastion forest.
- Trusted domain: It is a unique domain that allows users to access another domain.
- Transitive trust: A connection that can extend beyond two domains and allow access to other trusted domains in a forest.
- Intransitive trust: One-way trust that is limited to two domains.
- Explicit trust: It is a one-way, non-transitive trust created by a network administrator. Cross-link trust is a type of explicit trust. This type of trust relationship exists between domains within (1) the same tree, with no parent-child relationship between the two domains, or (2) different trees.
- Forest trust: It applies to domains within the entire forest and can be one-way, two-way, or transitive.
- Shortcut: Joins two domains belonging to different trees. These can be unidirectional, bidirectional, or transitive.
- A domain: Trust that is transitive, intransitive, unidirectional or bidirectional.

### *13.2* Advantages of using *Active Directory*

AD provides more than a unified service: It is an invaluable asset for organizations looking to simplify their IT operations and strengthen their security. The key advantages of AD are:

- Centralized resource management:
- Simplified resource sharing: Active Directory allows IT administrators to manage network resources (users, computers, shared files, printers) from a central point, simplifying resource management;
- Simplified user management: AD simplifies user account management by providing a centralized platform to create, modify, or delete users across the network;
- Enhanced Security: Strong AD security features protect confidential data from cyberthreats. Group policies and access controls enforce strict password

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

requirements and limit user access to specific files or applications based on their specific roles in the company;

- Scalability and Flexibility
- Scalable architecture: AD can manage both small networks and large complex business environments, making it flexible for organizations of different sizes;
- Multiple domains and forests: Active Directories support the creation of multiple domains, forests, and organizational units, offering flexibility in managing different parts of an organization independently while maintaining centralized control;
- Role-based access control: Administrators can define access permissions based on roles, groups, or specific user criteria. This ensures that users only have access to the resources they need based on their roles, thus minimizing the risk of unauthorized access;
- Detailed logs of user activity and system events.

### 13.3 Active Directory Accounts

There are several types of accounts that serve different purposes in an Active Directory. The main types are analyzed below:

#### User Accounts

- Standard User Account: User accounts are created for individual users to allow access to network resources. Typically, each user has a unique username and password. Permissions are assigned based on the user's needs;
- Administrator Account: This is a special user account with elevated permissions, typically used to manage the AD infrastructure. Administrators can create, delete, and manage other accounts and resources within Active Directory;
- Guest Account: Normally disabled by default, the guest account is intended for temporary or limited access by users who do not have a dedicated account on the domain.

#### Team Accounts

- Domain-linked computer accounts: These are created when a device joins the domain and represent devices such as workstations and servers. They help authenticate and manage devices on the network;
- Domain Controller Accounts: They are specialized computer accounts that represent domain controllers, which are critical servers that host the services of Active Directory.

#### Service Accounts

- Local Service Account: This account has limited permissions and is used for run services locally on a computer, primarily on non-domain controllers;
- Network Service Account: Similar to the previous one, but with additional permissions

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

for accessing network resources, used for services that need to connect through the network;

- Managed Service Account: Managed service accounts are designed to run services with automatic password management. They are typically used to run services on individual servers;
- Group Managed Service Account: An account of this type can be used inmultiple servers, allowing a shared service account with automatic password management, which is advantageous for high availability services or server farms.

**Group accounts**

- Security groups: Are used to manage resource permissions within a domain. Security groups are typically used to assign access control permissions to files, folders, and other resources;
- Distribution groups: These are mainly used for mailing lists in Microsoft Exchange environments and do not have security permissions associated with them by default.

**Integrated accounts**

- Standard administrator account: A highly privileged account created by default in all AD environments, often used for initial installation and configuration.
- Local System Account: A powerful system account that can virtually access all system resources; used primarily by the operating system and some critical services.
- KRBTGT Account: A system account used by the Kerberos Distribution Center (KDC) for issuing tickets in AD environments. This is essential for Kerberos authentication and is automatically created during AD setup;
- Application accounts: These are service or user accounts created specifically for applications to access network resources. They typically require specific permissions to interact with AD objects and can be configured as managed services or group-managed service accounts to simplify credential management.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

## 14. Other recommendations

In conclusion, this chapter summarizes the recommendations formulated throughout this guide. The list below summarizes the various points [68]:

- Always keep operating systems and software regularly updated, applying the patches and security updates provided by the manufacturer;
- Use antivirus and firewalls on all devices, including desktops, laptops, smartphones, and tablets;
- Only open emails from known senders (by address, not name) and reject any suspicious email, especially those containing suspicious or unsolicited links or attachments;
- Activate automatic device locking, never leaving your devices unlocked for long periods or when you are away;
- Use passwords with more than 8 characters, including uppercase, lowercase, digits, and special characters;
- Change passwords regularly and do not reuse them across different sites; Use your organization's VPN on public networks or outside your normal workplace;
- Enable two-factor authentication (2FA) whenever possible;
- Keep backup copies stored in secure locations and protected from unauthorized access;
- Enable disk encryption on computers and removable devices such as USB flash drives, external drives, or memory cards;
- Anonymize or make available strictly necessary personal information on various online services, such as social networks, platforms or websites;
- Check the settings and access permissions of the different applications, whether on the computer or on the mobile phone, at regular intervals (for example, quarterly);
- Do not install programs from unknown or dubious sources;
- Cover or disable webcams and microphones, activating them only when necessary;
- Make sure you use the HTTPS protocol when browsing the Internet, especially on websites where you enter credentials or personal information, such as home banking, email, and healthcare access;
- Report and delete messages that attempt to impersonate you or exfiltrate credentials;
- Maintain a critical attitude and good computer literacy;

If you have any questions, please contact the IT support team of the company or service in question, requesting additional information for each query.

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

# 15. References


AW Services. What is the OSI model? [On-line]. Available: https://aws.amazon.com/pt/ what-is/osi-model/

Cloudflare. What is the OSI Model? [On-line]. Available:https://www.cloudflare.com/ learning/ddos/glossary/open-systems-interconnection-model-osi/

What is the OSI Model? [On-line]. Available:https://www.cloudflare.com/learning/ ddos/glossary/open-systems-interconnection-model-osi/

Or what is a protocol? | Definition of network protocol. [On-line]. Available: https:// www.cloudflare.com/pt-br/learning/network-layer/what-is-a-protocol/

What is HTTP? [On-line]. Available:https://www.cloudflare.com/learning/ddos/ glossary/hypertext-transfer-protocol-http/

What is the Simple Mail Transfer Protocol (SMTP)? [On-line]. Available:https:// www.cloudflare.com/learning/email-security/what-is-smtp/

What is the Internet Protocol? [On-line]. Available:https://www.cloudflare.com/ learning/network-layer/internet-protocol/

What is TCP/IP? [On-line]. Available:https://www.cloudflare.com/learning/ddos/glossary/ tcp-ip/

What is UDP? [On-line]. Available:https://www.cloudflare.com/learning/ddos/ glossary/user-datagram-protocol-udp/

Clouflare. What is the Internet Control Message Protocol (ICMP)? [On-line]. Available:

https://www.cloudflare.com/es-es/learning/ddos/glossary/internet-control-message-protocol-icmp/

Cloudflare. What is IGMP? | Internet Group Management Protocol. [On-line]. Available: https:// www.cloudflare.com/learning/network-layer/what-is-igmp/

What is IPsec? | How IPsec VPNs work. [On-line]. Available:https://www.cloudflare . com/learning/network-layer/what-is-ipsec/

D. of the Republic. Law No. 46/2018, of August 13. [On-line]. Available:https: // diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384

CNCS. Legal Regime. [On-line]. Available:https://www.cncs.gov.pt/pt/regime-juridico/

WeSecure. REGIME LEGALDA SECURITY DO CYBERSPACE (DL65/2021). [On-line]. Available:https://www.wesecure.pt/ regime_juridico_da_seguranca_do_ciberespaco_dl_65_2021/

IGFEJ. General Data Protection Regulation (RGPD). [On-line]. Available: https://igfej.justica.gov.pt/Sobre-o-IGFEJ/Regulamento-Geral-de-Protecao-de-Dados-RGPD

EUR-Lex. General Regulation on Data Protection (RGPD). [On-line]. Available: https://eur-lex.europa.eu/PT/legal-content/summary/general-data-protection-regulation-gdpr.html

CNCS. NIS 2 Directive. [On-line]. Available: https://www.cncs.gov.pt/pt/ diretivasri-2-nis-2/ #collapse1Two

TechTarget. 5 Reasons Software Updates are Important. [On-line]. Available: https:// www.techtarget.com/whatis/feature/5-reasons-software-updates-are-important


This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

Medium. The Importance of Regular Software Updates And Patches. [On-line]. Available: https://medium.com/%40findmyservices/the-importance-of-regular-software-updates-and-patches-c2f362cef981

pplware. 5 reasons to keep your devices and software updated. [On-line]. Available:https://pplware.sapo.pt/internet/ 5-razoes-para-manter-os-seus-dispositives-esoftware-atualizados/

LinkedIn. WHY REGULAR UPDATING OF SOFTWARES IS IMPORTANT-TE? [Online]. Available:https://www.linkedin.com/pulse/why-is-it-important-to-update-regular-software-gofix/

U. of Idaho. Why keeping your software up to date is important for cybersecurity? [On-line]. Available: https://support.uidaho.edu/TDClient/40/Portal/KB/ArticleDet?ID=2770

W.University. Cybersecurity 101: Why Choosing a Secure Password Is So Important. [On-line]. Available: https://www.waldenu.edu/programs/information-technology/resource/cybersecurity-101-why-choosing-a-secure-password-in-so-important

NI of Standards and Technology. NIST Password Guidelines 2024. [Online]. Available: https://www.auditboard.com/blog/nist-password-guidelines/

Microsoft. What is access control? [On-line]. Available:https://www.microsoft.com/ enus/security/business/security-101/what-is-access-control

Citrix. What is access control? [On-line]. Available:https://www.citrix.com/glossary/ what-is-access-control.html

Medium. Authentication, control of access and Analysis of vulnerability. [Online]. Available: https://medium.com/@celionormando/ autentica%C3%A7%C3% A3o-e-controle-de-acesso-e-an%C3%A1lise-de-vulnerabilite- f68726d203c2

Cisco. What Is Network Monitoring? [On-line]. Available: https://www.cisco.com/c/en/us/solutions/automation/what-is-network- monitoring.html

M. Engine. Basics of Network Monitoring. [On-line]. Available: https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html

NordLayer. The comprehensive guide to network security monitoring. [On-line]. Available: https://nordlayer.com/blog/the-guide-to-network-security-monitoring/

G. for Geeks. Intrusion Detection System (IDS). [On-line]. Available:https://www.geeksforgeeks.org/intrusion-detection-system-ids/

IBM. What is an intrusion detection system (IDS)? [On-line]. Available:https://www.ibm.com/topics/intrusion-detection-system

G. for Geeks. Intrusion Prevention System (IPS). [On-line]. Available:https://www.geeksforgeeks.org/intrusion-prevention-system-ips/

IBM. What is an intrusion prevention system (IPS)? [On-line]. Available:https://www.ibm . com/topics/intrusion-prevention-system

What is endpoint detection and response (EDR)? [On-line]. Available:https:// www.ibm.com/topics/edr

Cisco. What Is Endpoint Detection and Response (EDR)? [Online]. Available: https://www.cisco.com/c/en/us/products/security/endpoint-security/ endpoint-detection-response-edr-medr.html

Microsoft. What about EDR (extremity detection and response)? [On-line]. Available:https://www.microsoft.com/pt-br/security/business/security-101/whatis-edr- endpoint-detection-response

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

IBM. What is security information and event management (SIEM)? . [On-line]. Available: https://www.ibm.com/topics/siem

Microsoft. What es SIEM? [On-line]. Available:https://www.microsoft.com/en-us/security/ business/security-101/what-is-siemCohesity. Data backup and recovery. [On-line]. Available:https://www.cohesity.com/ glossary/backup-and-recovery/

AW Services. Or what is data backup? [On-line]. Available: https://aws.amazon.com/ pt/what-is/data-backup/

Veritas. Data backup and recovery: the essential guide. [On-line]. Available: https://www.veritas.com/pt/ br/information-center/data-backup-and-recovery

IBM. What is backup and restoration? [On-line]. Available:https://www.ibm.com/br-pt/ topics/backup-and-restore

Lenovo. What is backup? [On-line]. Available:https://www.lenovo.com/us/en/glossary/ backup/

Veritas. Backup Regra 3 2 1: guaranteeing the protection and recovery of data. [On-line]. Available: https://www.veritas.com/pt/br/information-center/3-2-1-backup-rule

IBM. What is a disaster recovery plan (DRP)? [On-line]. Available:https://www.ibm.com/ topics/disaster-recovery-plan

G. Cloud. What is a disaster recovery plan? [On-line]. Available: https://cloud.google.com/learn/what-is- disaster-recovery?hl=pt-BR

IBM. Cost of a Data Breach Report 2024. [Online]. Available:https://www.ibm.com/ reports/data-breach

B. OR. Policies. Data Classification Policy. [On-line]. Available: https://www.bu.edu/policies/ data-classification-policy/

R. Portuguese. Classified Information. [On-line]. Available:https://www.gns.gov.pt/docs/questes-sobre- informao-classifica.pdf

U. of Hong Kong. Information Security and Data Management Policy. [On-line]. Available: https://isdm.hku.hk/

U. of Arkansas. Data Lifecycle and Management Policy/Procedures. [On-line]. Available: https://uada.edu/docs/policies/UADA_920_1.pdf

R. Content. 7 Best Practices and Tips to Effective Email Management. [On-line]. Available: https://rockcontent.com/blog/email-management/

Winter. 23 Email Management Best Practices and Tips. [On-line]. Available:https://hiverhq.com/blog/email-management

ZenDesk. Best 13 email management software of 2024. [Online]. Available:https://www.zendesk.com/service/ticketing-system/email-management-software/

Medium. 8 Reasons Why Your Business Needs a Server. [On-line]. Available:

https://docs.rackspace.com/docs/create-manage-and-delete-users-and-groups-in-active-directory

ZDNET. 5 Reasons Your Business Needs to Server. [On-line]. Available: https://www.zdnet. com/paid-content/article/5-reasons-your-business-needs-a-server/

HP. How to Set Up to Server for Small Business. [On-line]. Available: https://www.hp.com/ us-en/shop/tech-takes/how-to-set-up-server-for-small-business

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.

Microsoft. Active Directory accounts. [On-line]. Available:https://learn.microsoft.com/ en-us/windows-server/identity/ad-ds/manage/understand-default-user-accounts

Rockspace. Create, manage, and delete users and groups in Active Directory. [On-line]. Available: https://docs.rackspace.com/docs/create-manage-and-delete-users-and-groups-in-active-directory

S.Space. How to Manage User Accounts in Active Directory. Part 1: Creating and Deleting User Accounts. [On-lie]. Available:https://serverspace.io/support/help/how-to-manage-user-accounts-in-active-directory- part-1-creating-and-deleting-user-accounts/

Wikipedia. Active Directory. [On-line]. Available:https://en.wikipedia.org/wiki/Active Directory

Microsoft. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview. [On-line]. Avail-able: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/ virtual-dc/active-directory-domain-services-overview

Quest. What is Active Directory and how does it work? [On-line]. Available:https://www.quest.com/solutions/active-directory/what-is-active-directory.aspx

TechTarget. What is Active Directory and how does it work? [On-line]. Available: https://www.techtarget.com/searchwindowsserver/definition/Active-Directory

proofpoint. What Is Active Directory? [On-line]. Available:https://www.proofpoint.com/ us/threat-reference/active-directory

CNCS. Cybersecurity Practices. [On-line]. Available:https://www.cncs.gov.pt/ docs/1626335247.pdf

This project has been funded by the European Regional Development Fund (ERDF). DER) within the framework of the Interreg VI-A Spain – Portugal POCTEP 2021-2027 programme Project: CIBERIA - Digitalisation and cross-border resilience by promoting a cyber-secure CENCYL zone (0192_CIBERIA_3_E.