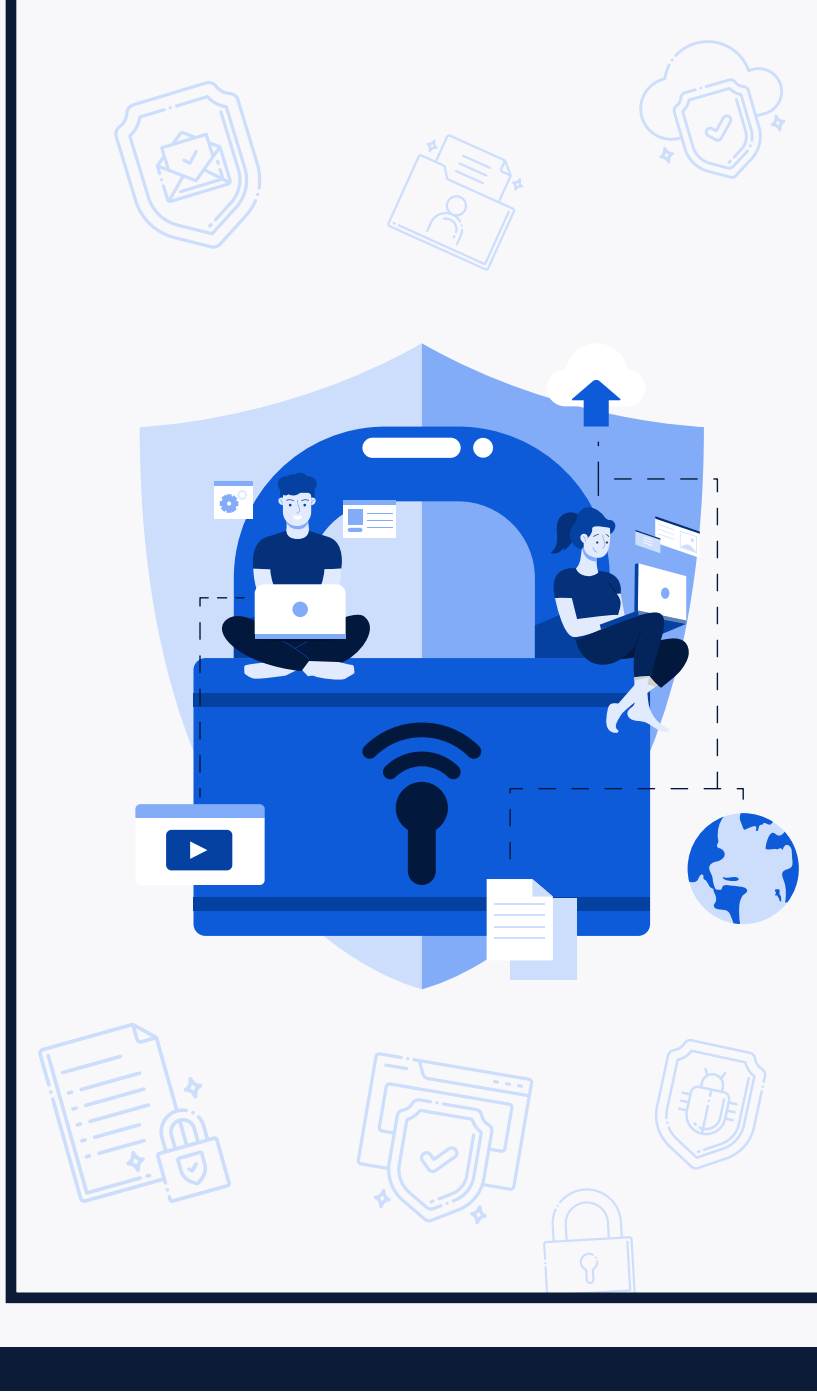
CCN-CERT

BP/01



Basic principles and recommendations in Cybersecurity

BEST PRACTICES REPORT

MARCH **2021**

cn-cert centro criptológico nacional

CCN centro criptológico nacional

Edit:

National Cryptologic Centre, 2021

Release date: march 2021

LIMITATION OF RESPONSIBILITY

This document is provided in accordance with the terms compiled in it, expressly rejecting any type of implicit guarantee that might be related to it. In no case can the National Cryptologic Centre be considered liable for direct, indirect, accidental or extraordinary damage derived from using information and software that are indicated even when warning is provided concerning this damage.

LEGAL NOTICE

Índice

1. About CCN-CERT

The CCN-CERT is the Information Security Incident Response Capability of the National Cryptologic Centre.

The CCN-CERT (www.ccn-cert.cni.es) is the Information Security Incident Response Capability of the National Cryptologic Centre, CCN (www.ccn.cni.es). This service was created in 2006 as the Spanish **Governmental/National CERT** and its functions are set out in Law 11/2002 regulating the National Intelligence Centre, RD 421/2004 regulating the CCN and RD 3/2010, of 8 January, regulating the National Security Scheme (ENS), modified by RD 951/2015, of 23 October.

According to all of them, the CCN-CERT is responsible for managing cyber incidents that affect **public sector systems**, **companies and organisations of strategic interest** to the country and any classified system. Its mission, therefore, is to contribute to the improvement of Spanish cybersecurity, being the national alert and response centre that cooperates and helps to respond quickly and efficiently to cyber-attacks and to actively face cyber-threats.

2. Introduction

Awareness, common sense and good practice are the best defences to prevent and detect mishaps in the use of Information and Communication Technology (ICT) systems.

It can be said that there is no system that guarantees 100% security of the service it provides and the information it handles, largely due to the vulnerabilities presented by the technologies and, more importantly, the impossibility of having sufficient resources to deal with them. Therefore, a risk must always be accepted; the so-called residual risk, assuming a compromise between the level of security, the available resources and the desired functionality.

Security implementation involves planning and taking into account the following elements:

Awareness, common sense and good practice are the best defences.

Risk Analysis

Studying possible risks and assessing their consequences on assets. (Information and service).

Risk Management

Assess the different protection measures and decide on the solution that best suits the entity. (Determination of residual risk).

Governance

Adapt the institution's normal operations to security measures.

Monitoring

Continuous observation of security measures, as well as their adaptation to the emergence of new technologies.

Contingency plans

Determination of the measures to be taken in the event of a security incident.

The combination of these practices helps to provide the minimum level of protection to keep data safe.

3. Threat factors

The widespread use of electronic media in the normal course of society has increased the area of exposure to attacks and, consequently, the potential benefits derived from them, which is undoubtedly one of the greatest incentives for attackers.

This trend has continued in recent years, with an increase in the number, type and seriousness of attacks against the information systems of the public sector, companies and institutions of strategic interest or those with important intellectual and industrial property assets and, in general, against all types of entities and citizens.

Cyber espionage actions are still present, consisting of cyber-attacks originated or sponsored by states and perpetrated by themselves or by other paid actors, and always with the intention of appropriating politically, strategically, security or economically sensitive or valuable information.

To summarise, cyber espionage has the following general characteristics:

- **Origin in states, industries or companies.**
- **Generally using targeted attacks (Advanced Persistent Threats).**
- **Against the public (political or strategic information) and private sectors (economically valuable information).**
- **Extremely difficult to attribute.**
- **Pursuing political, economic, strategic or social advantage.**

The security of their activities makes it more difficult to analyse these attacks. In fact, in recent years, tactics, techniques and procedures have become increasingly professionalised, clearly demonstrating a new type of criminal behaviour, which we could call *Crime-as-a-Service*. This makes it possible for third parties to carry out high-impact cyber-attacks, generally with the aim of obtaining illicit economic benefits.

3. Threat factors

Another element to take into account is the use of cyberspace in so-called ***Hybrid Warfare***, which by combining different tactics seeks to destabilise and polarise the society of states by avoiding armed conflict, but at the same time making such actions appear deliberately ambiguous.

Hybrid Warfare seeks to destabilise and polarise the society of states.

For the purpose of categorising the threat, the following figure shows the *Harm Pyramid,* according to the greater or lesser danger of cyberthreats, depending on their origin.

Hazard Level of Threats

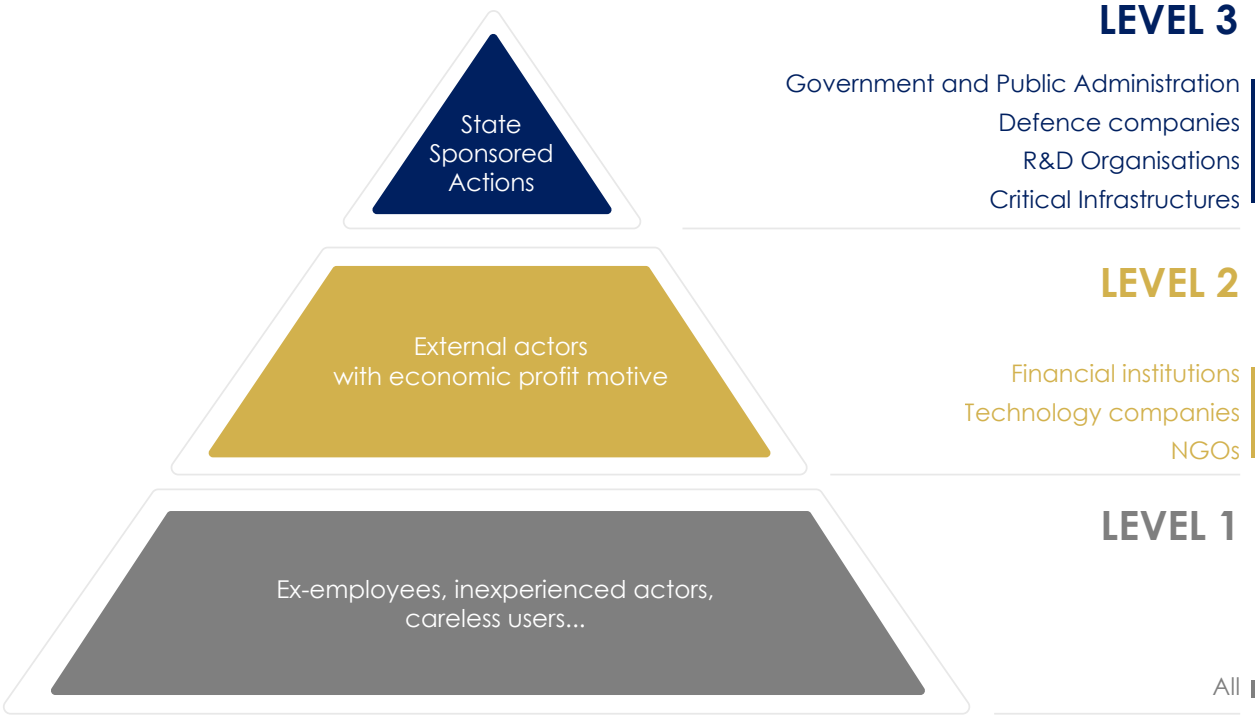


Figure 1. Damage Pyramid

3.1 Targeted attacks (APT)

Cyber-attacks have become a real alternative to conventional intelligence tools, due to their low cost, the difficulty of proving authorship and the significant volume of information that can be obtained in this way.

In this sense, APT[1] (Advanced Persistent Threat) groups seek to gather as much useful information as possible from the victim in order to prepare the most effective attack possible.

Figure 2.- Phases of an APT

1. Advanced Persistent Threats.

3. Threat factors

The parameters characterising the attack techniques (APT) are based on:

Development capacity
Exploits[2] and vulnerabilities used.

Persistence
After reboots, updates and even formatting activities.

Encryption
Encryption methods and key strength to exchange the exfiltrated information.

Exfiltration techniques
Protocols used for information extraction.

Stealth
rootkit[3], *bootkit* techniques used to hide.

Resistance to reverse engineering
Techniques that make it difficult to analyse the code.

The information exfiltrated, depending on the motivation of the attackers, can be of a very varied nature: economic, sensitive, intellectual property, industrial or state secrets, etc.

2. Program or code that exploits a vulnerability in an application or system to cause unwanted or unexpected behaviour.
3. A tool used to hide illegitimate activity on a system. Once installed, it allows the attacker to act with the privilege level of the computer's administrator.

4. The Deep internet

The Internet has been divided into the deep web and the shallow web.

The Internet has been divided into the deep web and the shallow web. The shallow web is composed of static or fixed pages, while the deep web is composed of dynamic pages where the content is placed in a database that is provided at the user's request.

The main reason for the existence of the deep Internet is the impossibility for search engines (Google, Yahoo!, Bing, etc.) to find or index much of the information on it.

A subset of the deep Internet is only accessible using certain web browsers. This is the case, for example, of the *TOR* network, where users must have the appropriate browser software in order to access domains that are inaccessible from a conventional browser.

In addition, users must know in advance the address to which they have to go.

There are lists with some public domains of the TOR network that users can consult (The Hidden Wiki, Silk Road, Agora, Evolution, Middle-Earth, etc...) and search engines such as *"Grams"* (the Google of the *dark web*).

4.1 The TOR network

The Onion Router **(TOR) was a project designed and implemented by the US Navy, launched in 2002, to strengthen Internet communications and ensure anonymity and privacy.**

Unlike conventional Internet browsers, TOR allows users to surf the web anonymously. Data does not travel directly, but through several nodes that facilitate the anonymity of communications. There is a directory of intermediate nodes with associated public keys in order to establish encrypted communication.

TOR creates virtual circuits composed of three (3) nodes randomly chosen from its network. Thus, the communication between the source, our computer and the destination, for example, a website, has to go through the three (3) assigned nodes, through which the information will be transmitted in encrypted form.

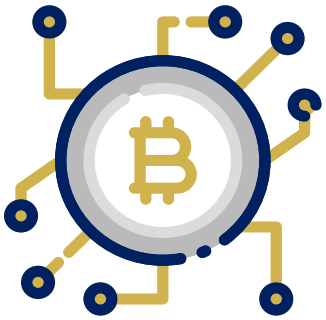
The source element encrypts the communication with the public key of the last node of the chosen route so that it is the only element that can decrypt the message and the instructions (intermediate nodes and their associated public keys) to reach the destination.

Random paths are chosen where data is encrypted in layers and once the last layer is processed by an exit node, the connection to the destination web page is made.

Unlike conventional Internet browsers, TOR allows users to surf the web anonymously.

4.2 Bitcoins

A string of cryptographic characters that are exchanged through digital wallets between the user and the seller (P2P exchanges), which makes it beyond the control of any government, institution or financial institution.



***Bitcoin* is an encrypted, decentralised, peer-to-peer electronic currency controlled indirectly by the users themselves through P2P exchanges.**

Instead of minting a coin or printing a banknote, it uses a string of cryptographic characters that are exchanged through digital wallets between the user and the seller (P2P exchanges), which makes it beyond the control of any government, institution or financial institution.

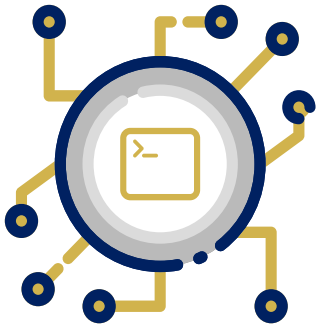
Every bitcoin transaction is recorded in a large database called the "BlockChain". The data is stored in blocks and each new block must contain the hash of the previous block. Therefore, each new block that joins the chain has the entire history of the transaction.

This protocol is based on a network of "miners" who control the currency. The miners make computing resources available to the network and are rewarded with bitcoins. These miners protect the system so that there are no reversal transactions (return of money already spent).

This currency is international, easy to use, allows anonymous transactions, ATMs are available and more and more vendors/ merchants accept it. As risks, it represents a very practical mechanism for money laundering and tax evasion (tax exemption).

5. Applications

The installation of software may affect the performance and security of devices/equipment. The integrity of the devices/equipment must be maintained and authorised software provided directly by the manufacturer must always be installed.



The use of **legitimate software** offers warranty and support, regardless of the legal implications of using non-legitimate software.

Certification of the software for compatibility with the operating system and other applications.

Installation and maintenance of **security patches and updates**, with special attention to those of a critical nature.

Consider the area of exposure associated with ***legacy* systems**, especially those older than a decade because of their extreme vulnerability.

5. Applications

Users should **be aware** that the introduction of unauthorised software can cause infection of the most protected system. Here are some good practices:

- **Usually work on the system as an unprivileged user, not as an "Administrator".**
- **Never run programs of dubious or unknown origin.**
- **If you use an office software package capable of running macros, make sure that the automatic execution of macros is disabled.**

When it comes to printing documents, it is important to be aware that printed **documents and transactions are susceptible to security breaches.** Therefore, it is essential to employ good practices to comply with each entity's existing regulations and to ensure that printed information is secure and not accessible by unauthorised personnel.

> **The introduction of unauthorised software can cause infection of the most protected system.**

5.1 Data encription

Encrypting data means converting plain text into unreadable text, so-called ciphertext, preventing the information from being accessed by unauthorised third parties. This requires an **encryption algorithm** and the **existence of a key**, which enables the data transformation process to be carried out and which must be kept in secret.

There are multiple commercial solutions for encrypting computer hardware, which can be classified into three (3) types according to the level at which they act on the file system:

Disk encryption

It is a technology that encrypts the entire disk, so that the operating system is responsible for decrypting the information when the user requests it.

Folder encryption

Encryption is performed at the folder level. The encryption system will take care of encrypting and decrypting the information when the protected folder is used.

Encryption of documents

The system is responsible for displaying and allowing access to the document only to authorised users, rendering the content unreadable to unauthorised users.

Encrypting data means converting plain text into unreadable text, so-called ciphertext, preventing the information from being accessed by unauthorised third parties.

4. See **CCN-STIC-955B Guide GPG Recommendations for Use** (https://www.ccn-cert.cni.es/series-ccn-stic/900-informes-tecnicos/1816-ccn-stic-955b-recomendaciones-de-empleo-de-gpg/file.html)

5.2 Personal firewalls

Personal *firewalls*[5] are programs that monitor incoming and outgoing connections to the computer.

They are designed to block unauthorised access to the computer, while still allowing authorised communications. The most complicated part of a firewall is configuring it correctly, so that legitimate connections (web browsing, updates, email, etc.) are not blocked.

As a generic criterion, connections from unknown sources should not be allowed. Therefore, they should block all incoming connections and only allow those that are explicitly indicated on the basis of an established set of rules and criteria.

A properly configured firewall adds necessary protection that makes unauthorised lateral movement through the network more difficult, but should in no case be considered as sufficient.

5. See **Guide CCN-STIC-408 Perimeter Security-Firewall** (https://www.ccn-cert.cni.es/pdf/guias/1297-indice-series-ccn-stic/file.html)

5.3 Anti-Malware Applications

Actions that can be caused by malicious code or malware include: **deletion or alteration of files, consumption of computer resources, unauthorised access to files, remote infection of computers,** etc.

The minimum functions that can be expected in a good **anti-malware tool**[6] (better known as **antivirus**) are incoming and outgoing filtering of malicious content, protection in email, browsing and connections of all kinds in professional or home networks. They must also be able to scan files on removable devices such as external disks or USB sticks and allow for the scheduling of exhaustive scans from time to time.

Anti-malware applications should have regular updates (latest definitions and search engines) and be products of reputable vendors that allow a combination of the following methods:

Access scanner: allows to examine files when they are opened.

On-demand scanner: analysis based on a set schedule.

Email scanner: on perimeter protection devices or mail servers.

Signature control: allows the detection of non-legitimate changes to the content of a file.

Heuristic methods: search for anomalies in files and processes based on previous experience of malware behaviour.

But, an anti-malware application alone is not enough; a centralised (client-server) approach must be provided to protect all endpoints (servers, desktops, laptops, smartphones, etc.) connected to the network. Some vendors offer *Endpoint Security* systems that include antivirus, firewall and other security software.

---

6. The CCN-CERT has available for registered users of its portal the **multi-antivirus platform MARIA** for static analysis of malicious code through multiple antivirus and antimalware engines for Windows and Linux platforms (https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/maria-publico.html)

5.4 Secure data erasure[7]

You might think that simply formatting a hard drive would prevent the data stored on it from being recovered. However, there are applications that allow you to undo the formatting of a drive and there are even methods to recover data from disks, even if they have been overwritten.

In order to ensure that sensitive information is not being distributed, data must be overwritten in a method (erasure pattern) that does not allow it to be recovered in any way.

For this purpose, it is necessary to perform several write passes over each of the sectors where the information is stored. To simplify the task, the easiest way is to use a specialised application that allows the information to be easily deleted.

In the case of digital photographs, audio or video files and office documents, there is metadata[8] that may store hidden information that is not visible using standard application settings, requiring specific configuration or even specific software to reveal that data.

This metadata is useful as it facilitates the search for information, enables interoperability between organisations, provides digital identification and supports document lifecycle management.

However, the erasure of metadata or hidden data through document/file review and cleaning procedures and tools is essential to minimise the risk of sensitive information being revealed in the storage and exchange of information.

---

7. See **CCN-STIC-305 Guide Destruction and Sanitisation of Computer Storage Media** (https://www.ccn-cert.cni.es/series-ccn-stic/300-instrucciones-tecnicas/60-ccn-stic-305-destruccion-y-sanitizacion-de-soportes-informaticos/file.html)

8. See **Guide CCN-STIC-835 Erasure of Metadata in the framework of the ENS** (https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2031-ccn-stic-835-borrado-de-metadatos-en-el-marco-del-ens/file.html)

6. Safe navigation

Communication on the Internet is based on a basic idea: clients (computers, telephones, tablets, etc.) call servers (web, databases, etc.) that provide (serve) information. This communication is carried out through a protocol (http, https[9], ftp, etc.).

The client is identified in the network through an IP address (TCP/IP) and every time it connects to a website, it automatically knows the IP address, hostname, the page from which the client came, etc. There is an exchange of information that is usually not visible, where the web browser provides most of this data.

A high percentage of users are unaware of the amount of information they disclose to third parties when using the Internet. discloses to third parties when using the Internet.

A high percentage of users are unaware of the amount of information they are inadvertently and unwittingly disclosing to third parties when using the Internet.

Each time a website is visited, information is routinely provided which may be archived by the site administrator.

It is trivial for the website to find out the Internet address of the machine from which you are accessing, operating system, etc.

With the help of *cookies*, the information collected about visitors can be further personalised by recording the most visited pages, preferences, time of visit, software installed, etc.

---

9. See **Best Practice Report CCN-CERT BP-01/17 HTTPS Implementation Recommendations** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html)

6. Safe navigation

A web browser, in favour of maximum usability, allows seemingly harmless information to be accessed.

- The public IP address to which the user connects.
  - Your IP address is xxx.xxx.xxx.xxx.
  - Your browser is using 128 bit SSL secret key.
  - The server is using 1024 bit SSL public key.
- Screen resolution.
- Which pages are read and which are not, which figures are looked at, how many pages have been visited, which was the most recently visited "*Referer*" site.
- The value of the "*User-Agent*" field.
  - Mozilla/5.0 (Windows NT 6.1; rv:16.0) Gecko/20100101 Firefox/16.0
- The language and GMT zone of the operating system.
- Whether or not to accept ***cookies***.
- Fonts loaded on the system or ***plugins*** installed and activated.

Some **recommendations** for **safe navigation**[10] are as follows:

- Access only trusted sites.
- Keep the browser updated to the latest version available from the manufacturer.
- Configure the security level of the browser according to your preferences.
- Download software from official sites to avoid malicious impersonation.
- Configure your browser to prevent pop-up windows.
- Use a user without "Administrator" permissions to browse the Internet and prevent the installation of programs and changes to system settings.

---

10. See **Best Practice Report CCN-CERT BP-06/16 Safe Navigation** (https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1801-ccn-cert-bp-06-16-navegadores-web/file.html)

- Delete *cookies*, temporary files and history when using other people's computers in order to leave no trace of browsing.
- Disable *scripting* in web browsers, such as Firefox (NoScript) or Chrome (NotScript), to prevent scripting by unknown domains.
- HTTPS (SSL/TLS) is recommended over HTTP even for services that do not handle sensitive information. Features such as HSTS and extensions such as *HTTPS Everywhere* will help to ensure that HTTPS is used in preference to HTTP when browsing the web.
- As far as possible, use virtual machines for surfing the Internet.

Furthermore, it should be noted that anonymous browsing systems allow the use of some Internet services, mainly those based on web browsing (http/https), in a way that is not linked to the IP address from which the communication originates.

Anonymisers

They act as a filter between the browser and the website you want to visit.
When you connect to the anonymiser, you enter the URL to be visited and it then enters the network, filtering cookies, javascripts, etc.

Proxy servers

A proxy server acts as a gateway between the client machine and the Internet.
The proxy server acts as an intermediary, retrieving web pages instead of the user who is navigating.

Encryption Tunnels (TOR, VPS and Darknets)

A network of "tunnels" through which navigation data, duly encrypted, passes through multiple nodes until it reaches its destination.

7. E-Mail

Currently, email[11] is still one of the most widely used tools in any corporate environment for the exchange of information, despite the fact that in recent years a multitude of technologies and collaborative tools have emerged to facilitate communication and file exchange.

The increase and effectiveness of social engineering to deceive users via email has changed the paradigm of corporate security.

Today, perimeter firewalls and the securitisation of services exposed to the Internet are not sufficient countermeasures to protect an organisation from external attacks.

Here are some **recommendations**[12] for the safe use of **email**:

- **Do not open any link or download any attachment from an email that shows any unusual pattern.**
- **Do not rely solely on the name of the sender. The user should check that the domain of the email received is trustworthy. If an email from a known contact requests unusual information, contact the sender by telephone or other means of communication to corroborate the legitimacy of the email.**
- **Before opening any file downloaded from email, be sure of the file extension and do not rely on the icon associated with it.**
- **Do not enable macros in office documents even if the file itself requests it.**

11. See **Guide CCN-STIC-814 Email Security** (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/524-ccn-stic-814-seguridad-en-servicio-de-correo/file.html)
12. See **Best Practice Report CCN-CERT BP-02/16 E-mail** (https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1598-ccn-cert-bp-02-16-correo-electronico/file.html)

- **Do not click on any link requesting personal or bank details.**
- **Always keep your operating system, office applications and browser (including installed *plugins/extensions*) updated.**
- **Use security tools to mitigate *exploits* in a complementary way to antivirus software.**
- **Avoid clicking directly on any link from the email client itself. If the link is unknown, it is advisable to search for information about it in search engines such as Google or Bing.**
- **Use strong passwords for email access. Passwords should be periodically renewed and if possible use two-factor authentication.**
- **Encrypt emails containing sensitive information.**

The increase and effectiveness of social engineering to deceive users via email has changed the paradigm of corporate security.

8. Virtualisation

Virtualisation is understood as the recreation of a physical (hardware) or logical (software) resource, by means of a hypervisor that allows it to be executed by more than one environment at the same time.

In the virtual machine environment, the hypervisor allows the simultaneous use of the hardware in more than one operating system.

The heyday of virtualisation has come with the **use of the cloud**[13], where this system of resource sharing has become almost indispensable. Although there were already multiple systems from many manufacturers, their development and advances have increased exponentially. Currently you can choose, among others, XenServer from Citrix, VMware ESXi from Dell, VirtualBox from Oracle, Oracle VM Server and Hyper-V from Microsoft.

Security in virtualisation has the same premise as any other system, which is to *minimise the attack surface*. However, it has particularities that make security more difficult, such as, for example, the multitude of shared resources or the operating systems that run simultaneously with their own applications on the same physical machine.

13. See **Guide CCN-STIC-823 Security in Cloud Environments** (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-entornos-cloud/file.html)

8. Virtualisation

As a general rule, **the following guidelines should be followed** when setting up a virtual machine *host*:

- **Have the latest security updates installed on the operating system.**
- **Have the latest available rollback of the virtualisation software.**
- **If possible, have at least one network adapter exclusively for the virtualisation infrastructure.**
- **Create a laboratory environment isolated from the production environment.**
- **Have a security group to manage the security platform.**
- **Protect the storage devices on which the virtual machine definition and resource files are stored.**
- **Keep guest administrators separate from *host* administrators.**

8. Virtualisation

For *guest* creation, the following rules are recommended:

- **Make a preliminary outline of what the virtualisation infrastructure will look like.**
- **Size the creation of virtual machines to the actual needs and hardware resources available on the *host*.**
- **Encrypt virtual machine files, snapshots and virtual hard disks for virtualisation platform storage.**
- **Install the latest security updates for each *guest* operating system.**
- **Consider installing hypervisor agents, such as Guest Additions, and if so, keep them updated.**
- **Secure all guest operating systems with anti-malware and firewalls.**
- **Connect DVDs, CDs and external storage media only when necessary and switch off after use.**
- **Keep only essential virtual machines active.**
- **Use a separate virtual network interface for connection to the corporate network or the Internet, which should be deactivated when it is not in use.**
- **Encrypt external storage media containing backup virtualisation files and secure them appropriately.**

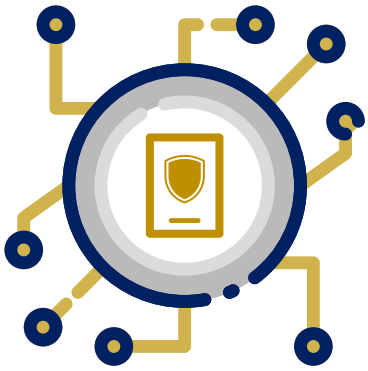
9. Mobile devices Security

The increased possibilities and capabilities associated with today's mobile devices[14] ealso imply increased security risks.

It is very important that users are aware of the importance of security on mobile devices and the dangers that can be associated with their misuse.

It is advisable to follow these **tips**[15]:

The increased possibilities and capabilities associated with today's mobile devices[14] also imply increased security risks.



- **Establish a secure method to unlock the terminal, e.g. using a strong *passphrase*.**
- **It is advisable to delete message previews and take extra precautions when the phone is not within reach.**
- **Disable wireless connections (WiFi, Bluetooth, etc.) and all unnecessary connections when not in use.**

14. See various **CCN-STIC Guides 450-451-452-453-454 and 455 Security on Mobile Devices** (https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6-ccn-stic-450-seguridad-en-dispositivos-moviles/file.html)
15. See **Best Practice Report CCN-CERT BP-03/16 Mobile Devices** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1807-ccn-cert-bp-03-16-dispositivos-moviles-1/file.html)

9. Mobile devices Security

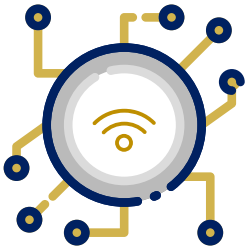
- **Keep the device software up to date and use security settings approved by the entity's ICT manager.**
- **Be careful about access and permission requests from applications running on the phone.**
- **Ignore and delete messages (SMS, MMS or other) of unknown origin that invite you to download content or access websites.**
- **Enable PIN access to Bluetooth connections and set the device to stealth mode. Do not accept connections from unknown devices.**
- **Download applications only from official markets. Under no circumstances download software from unreliable sites and in any case request the necessary applications from the entity's ICT manager.**
- **Avoid *jailbreaking* or *rooting* the handset, as it may compromise and considerably reduce the security of the phone, although it may be tempting to access specific applications or services.**
- **Use a virtual private network (VPN[16]) to protect data traffic from the mobile device to the organisation's infrastructure. This is always a good practice to avoid possible monitoring by intruders.**
- **Avoid as much as possible the use of printers, fax machines or public WiFi networks, such as those offered in hotels or airports, unless you have the necessary tools to secure your communications.**
- **Many mobile phones and digital cameras add GPS coordinates in the information of the images taken, so it is advisable to limit the sharing of images on the network or to use applications that remove this information.**
- **Separating personal and professional communications is a good security practice. Having watertight compartments in a single device will increase security.**
- **Implement centralised management of mobile devices using *MDM* (Mobile Device Management).**
- **For handling sensitive information, use only solutions approved by the entity's ICT security officer.**

---

16. See **Guide CCN-STIC-836 Virtual Private Network (VPN) Security** (https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2299-ccn-stic-836-seguridad-en-vpn-en-el-marco-del-ens/file.html)

10. Wireless networks Security

If you are working with a wireless network, to maximise the security of your WiFi network you should pay attention to the following **recommendations**[17]:



Change the default access password for Access Point administration.

Modify the default SSID by not using names that could identify the entity and allow it to go unnoticed in the environment.

Hiding the SSID identifier from the outside makes it difficult to obtain the name of the network, although client traceability is still possible regardless of SSID hiding.

Enable MAC address filtering of WiFi devices to allow devices with the specified MAC addresses to connect to the network.

Configure WPA2-AES in data confidentiality mode, obtaining strong authentication and data encryption.

---

17. See **Guide CCN-STIC-816 Security in Wireless Networks** (https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2317-ccn-stic-816-seguridad-en-redes-inalambricas-en-el-ens/file.html)

Limit WLAN coverage. A multi-directional antenna located in the centre of the house/office is the most common option.

Disconnect the network when not in use. While it is not practical to do this on a daily basis, it is highly recommended during long periods of inactivity.

Disable UPnP (Universal Plug and Play) when its use is not necessary, to prevent malicious code in the network itself from using it to breach the router's firewall to allow other attackers to gain access.

Update the router's *firmware* on a regular basis, as many of the updates and patches that are added affect security.

Use static IP addresses or limit the number of reserved addresses (DHCP) where possible, to prevent unauthorised users from obtaining an IP address from the local network.

Activate the router's firewall, so that only authorised users and services can access the network.

Activate the *login* option for the router and periodically analyse the access history.

It is advisable to change the router's default DNS configuration to one that preserves the user's privacy and improves security, for example, *DNSCrypt*.

11. Instant messaging

Instant messaging applications allow text messages to be sent via an Internet connection (WhatsApp[18] and Telegram[19] are the most popular).

WhatsApp, launched in 2009, for example, currently handles around 100 billion messages per day.

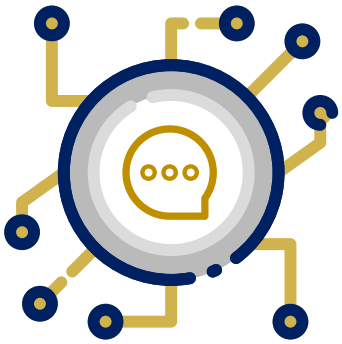
These are platforms that can behave in a similar way to conventional social networks and are prone to expansion. In addition, the sharing of personal information and the low perception of security risk among users have made them an attractive environment for intruders and cyberattackers trying to obtain data and information from their users.

One of the most common flaws in messaging applications is the way they use to delete conversations stored on the phone, as it does not involve the direct deletion of messages, but rather they are marked as free, so that they can be overwritten by new conversations or data when necessary and made accessible by forensic techniques.

In addition, there are the implications of having the backup option active (storing a possible deleted conversation) that could be recovered in the future.

During the establishment of a connection to the servers, sensitive information about the user can be exchanged in clear text and exposed to anyone when using public WiFi networks or networks of dubious origin.

The sharing of personal information and the low perception of risk among users have made instant messaging applications an attractive environment for cyberattackers.



18. See **CCN-CERT IA-21/16 WhatsApp Usage Risks** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1746-ccn-cert-ia-21-16-riesgos-de-uso-de-whatsapp/file.html)
19. See **CCN-CERT IA-23/17 Telegram Usage Risks** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2443-ccn-cert-ia-23-17-riesgos-de-uso-de-telegram-1/file.html)

11. Instant messaging

Client operating system

Version of the application in use

Registered telephone number

By using a VPN-based connection, all data sent and received is encrypted between the sender and receiver, adding a new layer of security to prevent attackers from intercepting network traffic (*man-in-the-middle*).

On the other hand, the database of conversations, files, messages and other data handled by this type of application is stored locally on the phone, regardless of whether the cloud backup option is activated on the device.

Although the information is stored encrypted locally, there are many applications[20] that, for example for WhatsApp, allow the information contained therein to be decrypted in a simple way, both in a local version for a computer and through an application on the phone or web interface.

To prevent an attacker from gaining access to all private information stored on the phone, special attention needs to be paid to which third-party applications are installed, as well as physical access to the handset by another person.

In the case of data sharing with social networks, such as *WhatsApp* and *Facebook*, and although messages, photos and profile information will not be targeted for sharing, other information such as phone number, contacts, last connection time, as well as your app usage habits, may be shared.

20. WhatCrypt: http://whatcrypt.com/

11. Instant messaging

In line with the **recommendations** for mobile devices, certain precautions should be taken when using instant messaging applications such as:

- **Keep the phone locked. This will reduce the risk if the device falls into the wrong hands.**
- **It would be advisable to delete message previews and take extra precautions when the phone is not within reach.**
- **Where possible, it is recommended to configure the applications to only receive messages from authorised persons.**
- **Disabling additional connectivity on the phone when it is not in use, such as WiFi or Bluetooth, not only reduces battery consumption, but also reduces the potential attack surface on the device.**
- **Use instant messaging applications whose source code is open to the community and has been reviewed. In this sense, there are alternatives that also ensure the confidentiality of communications by encrypting end-to-end traffic (e2e), for example *Signal*.**

12. Social networks

Social media have not only changed the way citizens inform and communicate with each other, but also the way governments and organisations convey their messages to citizens and how citizens respond.

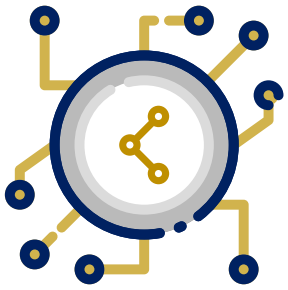
Communicating, sharing information, maintaining contact based on interest or affinity, relating, forming an identity and reputation, asserting claims, protesting, manipulating... there are multiple objectives sought when using one or another social network.

However, the success achieved, the enormous possibilities they offer and their massive use have put them in the spotlight of cyberattackers, who do not hesitate to exploit the risks and vulnerabilities of both the platforms that support these social networks and the people or organisations that use them.

Once again, the weakest link in this chain is the human factor due to low awareness and overconfidence in the use of these networks.

In general, the risks associated with social networks are the same as with other activities and/or services on the Internet: great difficulties in removing uploaded information, future access by third parties (the right to change one's mind is null and void and it will be very difficult to delete any opinion, photograph or video uploaded) and the difficulty of discerning between truthful information and propaganda or manipulation.

At this point, it is important to remember the importance of the security settings of the device (operating system and browser) used to connect to the Internet and, in this way, access social networks.



The success, possibilities and massive use of social networks have put them in the spotlight of cyberattackers.

12. Social networks

The following are the **main tips** that can be given as good practices in the use of **social networks**:

- **Careful creation of profile and privacy settings. Do not rely on the default settings provided by the platforms.**
- **Reflect on everything you post and use a pseudonym. Assuming that everything you post on a social network is permanent, even if you delete your account.**
- **Choose your friends carefully.**
- **Avoid revealing your friends' email addresses, do not allow social networking services to scan your email address book.**
- **Pay attention to location-based services and mobile phone information.**
- **Caution with links. Avoid clicking on hyperlinks or links of dubious origin.**
- **Type the address of your social networking site directly into your browser to prevent a fake site from stealing your personal information.**
- **Be cautious when installing additional elements on your site as these applications are sometimes used to steal personal information.**
- **Review the information you post. Avoid giving out too much information about yourself, such as your birthday, hometown, high school class, etc., to prevent people from hacking into your account.**
- **Password security, use complex passwords that include numbers, symbols and punctuation marks. It is important not to share the same password for all social networks and other services used on the Internet (use password managers such as *keepass*).**
- **Increase the security of account access by adding a second factor authentication (*2FA*) to prevent a potential attacker who has obtained the password from accessing the service.**

13. Internet of Things (IoT)

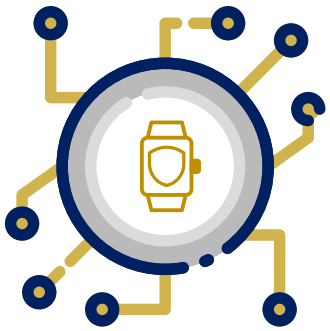
In essence, IoT[21] (*Internet of Things*) refers to networks of physical objects, artefacts, vehicles, buildings, appliances, clothing, implants, etc. that carry within them electronic components, software, sensors with network connectivity that allows them to collect information to achieve a contextualisation of the situation through Big Data techniques impossible to perform by other means.

It is a network that interconnects thousands of physical objects offering data in real time, becoming the sensors of the physical world. At this point we must consider the cultural change involved, as technology influences the way we make decisions and this affects people's capacity for action, privacy and autonomy.

The IoT is the first real evolution of the Internet, a leap that could lead to revolutionary applications with the potential to dramatically change the way we live, learn, work, entertain or socialise.

Everyday items are no longer isolated items, devices that can be connected to other devices. The cybersecurity experts' nightmare can become armies of *botnets* using smart toasters to develop *DDoS* attacks or to hide information and executables away from the view of researchers.

The IoT could lead to revolutionary applications with the potential to dramatically change the way we live, learn, work, entertain or socialise.



21. See **Good Practice Report CCN-CERT BP-05/16 Internet of Things** (https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2258-ccn-cert-bp-05-16-internet-de-las-cosas/file.html)

13. Internet of Things (IoT)

Security, interoperability and manageability of such systems are **vital aspects** to consider in the IoT:

Web interface.

Authentication mechanisms.

Network services.

Unencrypted transport.

Protection of privacy.

Security settings.

Software/firmware integrity.

Physical security of devices.

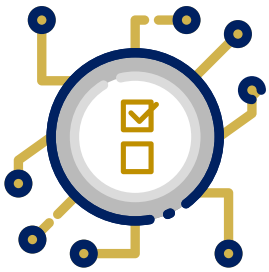
13. Internet of Things (IoT)

The challenge comes down to establishing a monitoring and control base to reduce risk exposure and applying smart techniques to the growing population of IoT devices.

- **Change default passwords on devices and use really strong passwords.**
- **Keep devices up to date with the latest available software and firmware versions.**
- **Disable all remote (internet) connectivity of devices when it is not strictly necessary.**
- **Keep only those communication ports open that are really necessary and modify the listening ports if possible.**
- **If IoT devices do not allow configuration of their security, always operate them on a local area network (LAN) behind a properly configured device (router) that does provide such security.**
- **As far as possible, ensure authenticity, confidentiality and integrity in all local (LAN) communications, especially if these are made via radio links (WiFi, Bluetooth, etc.).**
- **Periodically check the security configuration of all elements of the IoT architecture and their communication with the outside.**
- **Keep unnecessary components, such as microphones, video cameras, etc., disabled.**
- **Check the visibility of own devices in IoT device search engines such as Shodan.**

14. Security Policy

The design of a security strategy within an organisation generally depends on the activity of the organisation, its size, the scope of its activities and the interconnection with external users (clients, suppliers, end-users, etc.). However, in general terms, some basic steps can be considered when developing a strategy:



Create a Security Policy.

Conduct a risk analysis.

Implement appropriate safeguards.

Raise awareness among users.

The **Security Policy**[22] sets out the state of information and services within the entity and defines what is to be protected and the corresponding security objectives, providing a basis for security planning.

It describes user responsibilities and how the effectiveness of the measures implemented is monitored. In short, it is a set of rules that are decided to be applied to the system activities and communications resources belonging to an organisation.

---

22. See **CCN-STIC-805 Information Security Policy** (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/508-ccn-stic-805-politica-de-seguridad-de-la-informacion/file.html)

14. Security Policy

These rules include areas such as physical, personnel, administrative and network security. In addition, it should state the importance of IT to the organisation, the period of validity of the policy, the resources available and the specific objectives to be covered.

Risk analysis[23] identifies the risks to which the organisation is exposed and the impacts, potential threats and vulnerabilities that can be exploited.

Once the security policy is established, determining the residual risk that it is willing to accept, **safeguards** must be put in place to comply with it.

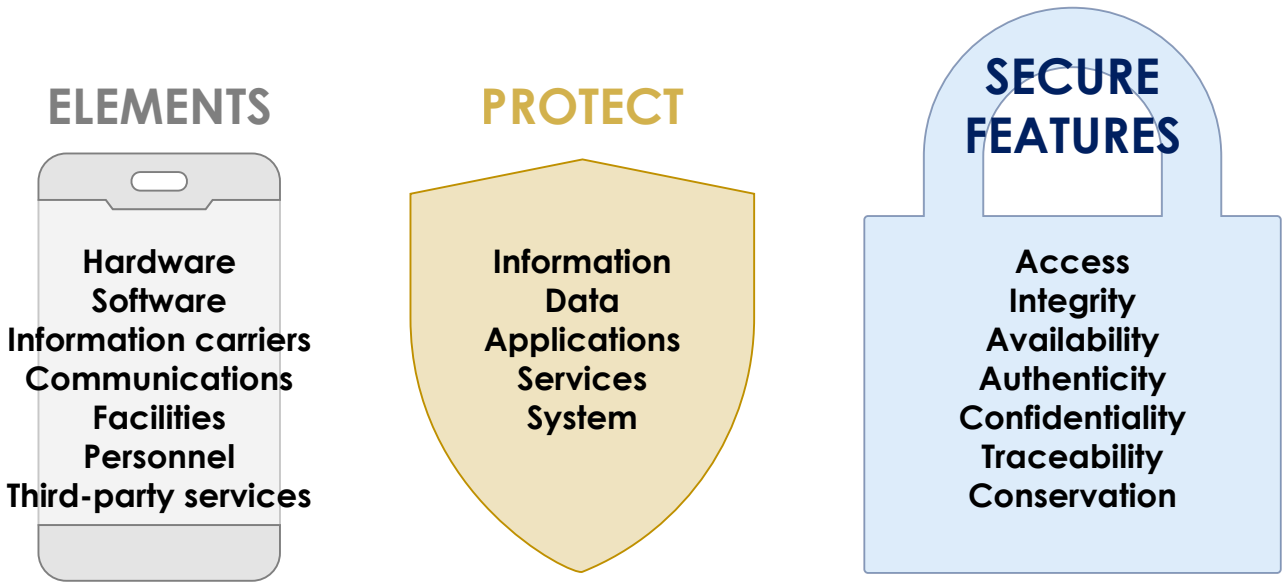


Figure 3. Elements to consider in the Security Policy

23. CCN-CERT makes the **PILAR Risk Analysis tool** available to the Public Sector (https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html)

14. Security Policy

Risk management uses the results of the risk analysis to select and implement appropriate security measures to control the identified risks, which can be divided into the following:

- **Preventive: aimed at reducing risk.**
  - **Physical protection:** guards, access control, hardware protection...
  - **Technical Measures:** firewalls, intrusion detectors, cryptography...
  - **Procedural measures:** awareness-raising courses, refresher courses, rules on access to information, sanctions, etc.
- **Analysis: aimed at risk identification.**
  - **Physical protection:** surveillance systems, motion detectors...
  - **Technical measures:** logical access control, authentication session...
  - **Procedural measures:** log management, audit monitoring...
- **Corrective: aimed at preventing or reducing the impact on assets.**
  - **Physical Protection:** Power Supply Backup (UPS)...
  - **Technical measures:** anti-virus software, audits, security backup...
  - **Procedural measures:** contingency plans...

14. Security Policy

The most serious threat to an information system is people, so their **training and awareness** is one of the fundamental objectives to be pursued when implementing a cybersecurity culture programme.

The awareness and sensitisation programme should make clear not only how to protect systems, but also why it is important to protect them and how users become the first security barrier for them.

Finally, it is very important to define, document and disseminate a security policy that demonstrates the organisation's commitment to security, as well as the development of regulations that set out the obligations to which users are subject with regard to the processing and security of information.

The most serious threat to an information system is people, so their training and awareness is one of the fundamental objectives.

14.1. Governance

Professionals are the foundation of a successful security operation. For this reason, aspects such as governance, structure, experience, training and certification of personnel must be considered in any organisation.

Security management and **administration** mechanisms must be established, including support for operations, escalation levels in accordance with the classification and remediation of incidents, frequency and types of notification, etc. In this sense, it is advisable to implement the so-called **ISMS (Information Security Management System)**, a set of information administration policies, where a set of processes are defined, implemented and maintained to efficiently manage the accessibility of information, seeking to ensure the confidentiality, integrity and availability of information assets while minimising information security risks.

In this way, the **structure** should make it possible to identify the people who have the level of authority and responsibility for the different tasks.

The necessary areas of expertise are those that will allow the roles and profiles necessary for the operation of the services to be defined, and it is important to consider training plans and certifications that allow for adaptation to changes, the incorporation of new technologies and the growth of the services.

14. Security Policy

Consideration should be given to establishing a security office to assist in the implementation of policies, procedures and regulations that provide the basis for directing, managing, communicating, assessing, monitoring and improving the security of information related to the entity's own activities in accordance with applicable regulations and best practices:

- **Review and support the implementation of the governance model.**
- **Regulatory analysis and adequacy.**
- **Analysis and management of the risks associated with the assets (assumable residual risk).**
- **Analysis and definition of scorecards (measures and indicators).**
- **Compliance audits.**
- **Support to security governance bodies.**
- **Monitoring and improvement of security status and management.**

14.2 Configuration management

Effective implementation of **configuration** control **and software management** is critical, as it is the only way to ensure that operating systems and applications are properly updated following the release of required patches.

The following should be considered:

The security provided by passwords depends, to a large extent, on their confidentiality.

All shared executable files and document templates must be placed in a read-only directory.

Each user should have his own personal directory on the network with read/write access and restricted read access for other users to prevent foreseeable spread of malicious software from the local machine to the network.

Directories shared by several users is a common way of working, so the spread of possible infections must be prevented.

Passwords are the main authentication mechanism used by individuals to access information systems. The security provided by passwords depends, to a large extent, on their confidentiality.

- **It may not be easily associated with any information relating to the user of the account.**
- **It shall have a minimum length of eight (8) characters with different types of typefaces.**
- **Change the password periodically.**
- **Do not share accounts and passwords with other users.**
- **Do not write down passwords in easily accessible places or store them in unprotected files on the computer.**
- **Limit the possibility of *"Remember Password"* offered by some web browsers.**

There are programmes that allow you to store all passwords with associated usernames in one place, so that they are always available and you don't have to remember them all. Usually, these programmes also have a password generator, so that passwords can be generated securely.

Removable media is one of the main threats of data leakage as well as malware infection. Limiting the use of USB devices may be a measure too drastic. However, the possibility of blocking these ports and removing optical media reader/writer drives from user equipment should be considered.

14.3 Surveillance

Along with software configuration control and management, a continuous process of vulnerability scanning, either automatic or manual, should be assessed.

Automatic vulnerability analysis:
deployment of tools to perform vulnerability scans of infrastructures and services.

Manual vulnerability analysis:
a group of analysts regularly reviews the different applications, mainly those exposed to the Internet, from a black-box and white-box perspective.

Cybersecurity Operations Centre (SOC)

DETECTION

Early Waning System

ANALYSIS

Malicious Code Analysis

RESPONSE

Incident Management

COORDINATION

Cyber Threat Information

It should not be overlooked that the establishment of a **Security Operations Centre (SOC)** improves surveillance and incident detection capabilities and optimises the ability to react and respond to any attack.

Consider deploying a block of services based on:

The establishment of a SOC allows improvementr incident detection and monitoring capabilitiesas well as optimiser the ability to react and respond to any attack.

Security monitoring

Deployment of high-capacity probes that receive a copy of both incoming and outgoing Internet traffic. Processing of events generated by a security information and event management system (SIEM).

Machine learning modules should also be considered for event analysis and alerts to detect new threats.

Protection and filtering of malicious content

Protecting users surfing the Internet from this type of threat. New generation devices, which have, in addition to traditional firewall capabilities, intrusion prevention and control of applications.

Incident Response

Advanced incident management support service through professionals who can coordinate, remotely or on-site, with the entity's staff in order to perform forensic analysis, collaborate in the mitigation and/or recovery strategy, etc.

Vulnerability Analysis

Periodic analysis of vulnerabilities, both automatically and manually. To this end, technologies for scanning systems and web applications will be provided to facilitate the performance of these tests on a regular basis, both automated and manual.

14.4 Business Continuity / Back-up Policies

The term "Business *Continuity*" implies thinking about and having an alternative plan in the event of a disaster occurring in the organisation's ICT systems. This plan must be documented so that, in the event of a disaster, the steps to be taken to mitigate the problem and return to the previous situation of normality as soon as possible are clear.

In addition, where possible, continuity plans should be **tested** to confirm that they are up to date and respond effectively to the need.

Regular **backups** are essential to ensure the integrity/availability of the system. Backing up involves creating a copy of the data on a different medium from the one on which it is located so that it can be used to restore the original copy after a data loss.

Data loss can be due to theft, system failure, natural disasters or simply system hardware failure. There are many different types of data storage devices used for backups, with advantages and disadvantages to consider in their choice.

Finally, it is highly recommended to verify backups relatively frequently by actually restoring data to a test location.

14.5 Incident management

Incident management[24] is part of the risk management culture.

When a security incident[25] occurs, it is critical for an organisation to have an effective response protocol in place to help security teams minimise the loss or leakage of information, prevent the spread of the incident, or even the disruption of service itself. The speed with which the incident is recognised, analysed and responded to will limit the damage and minimise the cost of recovery.

Organisations need to become accustomed to reporting and sharing incidents with relevant organisations, especially as patterns are often repeated. It is essential to establish good practices on reporting, use of a common taxonomy and procedures for reporting incidents, including those where the impact is unknown.

Organisations need to become accustomed to reporting and sharing incidents with relevant organisations, especially as patterns are often repeated.

Figure 4. Cyber Incident Response Life Cycle

24. See **CCN-STIC-817 Guide Incident Management** (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html)
25. Unexpected or undesired event with consequences detrimental to the security of networks and information systems.

In this regard, the competent authorities and the reference CERT/CSIRT[26] shall use a common platform to facilitate and automate the incident notification, communication and reporting processes.

The entities concerned shall make an initial notification without delay. Subsequently, they shall make further notifications as necessary to update information on the evolution of the incident until it is resolved. Once the incident is resolved (networks and systems have been restored and service is operating normally), they shall send a final notification of the incident.

CSIRTs monitor networks to detect potential incidents early[27], disseminate alerts about them and provide solutions to mitigate their effects. CSIRTs should be the gateway for incident notifications, which will allow rapid organisation of incident response.

Security incident management shall take into account:

- **The establishment of systems for detecting and reacting to malicious code.**
- **The logging of security incidents that occur and the actions taken to deal with them.**
- **Support and coordination for vulnerability treatment and security incident resolution.**
- **Provide information on vulnerabilities, alerts and warnings of new threats. Includes research and dissemination of information security best practices.**
- **Train to improve incident detection and management capabilities.**

26. Both terms are used to refer to a Team of Incident Management Experts. CERT: Computer Emergency Response Team and CSIRT: Computer Security Incident Response Team. The former is registered by CERT CC, the first such team at Carnegie Mellon University in the United States.
27. An example of this is the CCN-CERT Early Warning System (SAT INET and SAT SARA).

14. Security Policy

A basic outline of how to deal with a cyber incident could be as follows:

- **The DETECTION of the threat can be carried out by the entity itself and/or by the probes deployed by the Cyber Incident Response Team (CSIRT) of reference, which will generate the corresponding warning.**

- **In case the cyber incident is confirmed, the agency will make the formal notification (e.g. LUCIA tool) to the competent authority, via the reference CSIRT, and the actions of the CONTENTION phase.**

- **Once the threat has been ERADICATED, the entity, using the same tool, will notify the competent authority, through the reference CSIRT, of the closure of the cyber incident.**

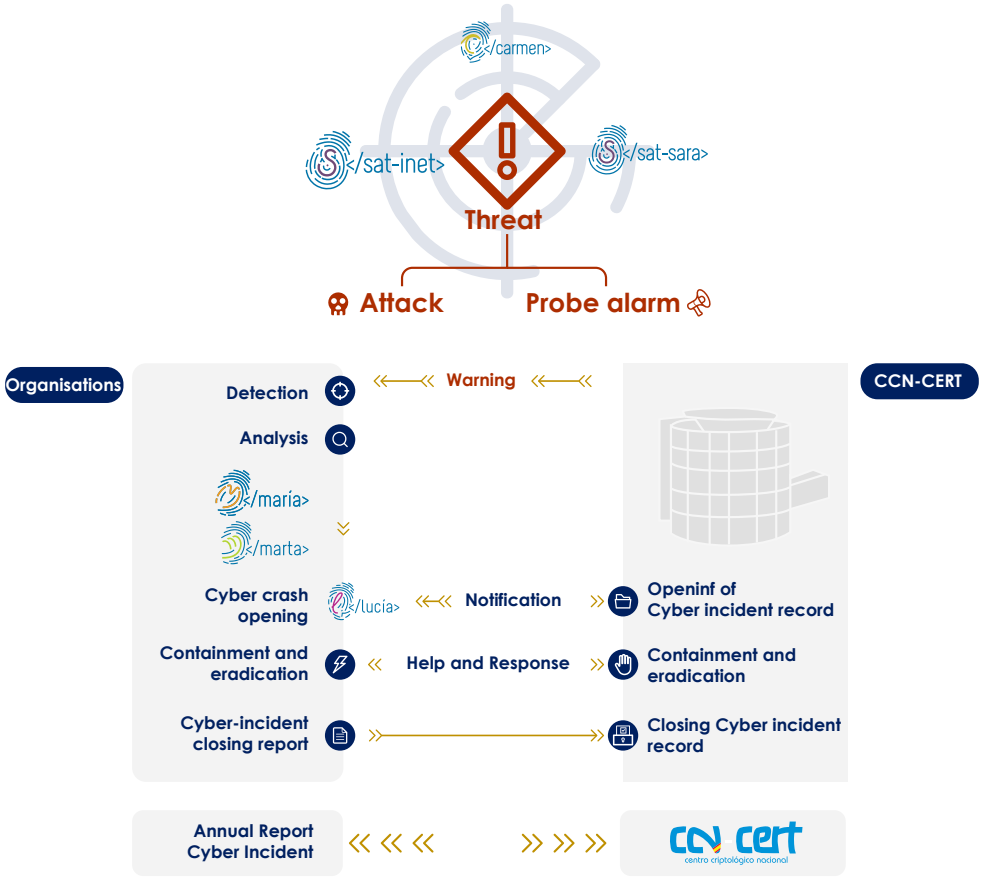


Figure 5. Basic outline of action in the event of a cyber incident

14. Security Policy

The management of cyber incidents (prioritisation, allocation of resources, etc.) requires the determination of the potential danger of the cyber incident. To do this, it is necessary to establish the criteria for determining the threat against which to compare the available evidence of the cyber incident in its early stages.

15. Basic Security Decalogue

This Decalogue of good practices aims to lay the foundations for establishing a culture of security.

Basic Security Decalogue

1. **Cybersecurity culture**, employee awareness, must be one of the pillars on which the cybersecurity of any organisation is built.

2. **Do not open** any link **or download** any attachment from an email that shows any **unusual pattern**.

3. The use of **security software, anti-virus and anti-malware tools**, personal **firewalls**, **secure deletion tools**, etc. should be a must when using an **ICT system**.

4. **Limit the area of exposure to threats**, not only by implementing security measures to protect access to information, but also by determining which services are strictly necessary.

5. **Encrypt sensitive information**, there is no alternative.

6. Use **passwords adapted** to the functionality, being aware that two-factor authentication is already a necessity.

7. **Secure deletion of information** once it is no longer needed or the media in question is to be withdrawn from use.

8. **Make regular backups**, there is no alternative in case of ransomware-type malicious code infection, data loss, storage hardware failure, unintentional deletion of information by the user, etc.

9. **Keeping your applications and operating system up to date** is the best way to avoid enabling the potential threat.

10. Regularly review **applied security settings**, **application permissions** and **security options**.

CCN centro criptológico nacional

CCN cert centro criptológico nacional

Figure 6. Security Decalogue

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es