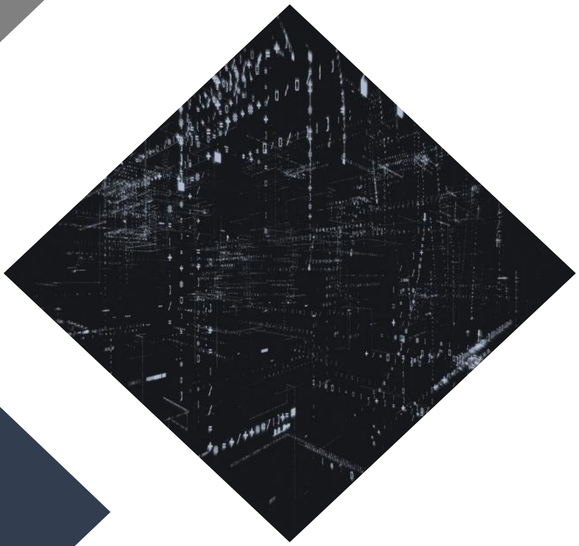
NATIONAL GUIDE FOR THE NOTIFICATION AND MANAGEMENT OF CYBER INCIDENTS



GOBIERNO
DE ESPAÑA

INDEX

1 INTRODUCTION

The Spanish Government attributes to different public institutions the competences in cyber security issues related to knowledge, management and reaction to cyber security incidents that happened to diverse information and communication networks of the country.

In particular, the Public Sector, the citizens and the companies, critical infrastructures and strategic operators, academic and research networks, as well as Spain's defence networks, have at their disposal a series of reference bodies on which the Spanish Government's response capacity to cyber security incidents (CSIRT) is based:

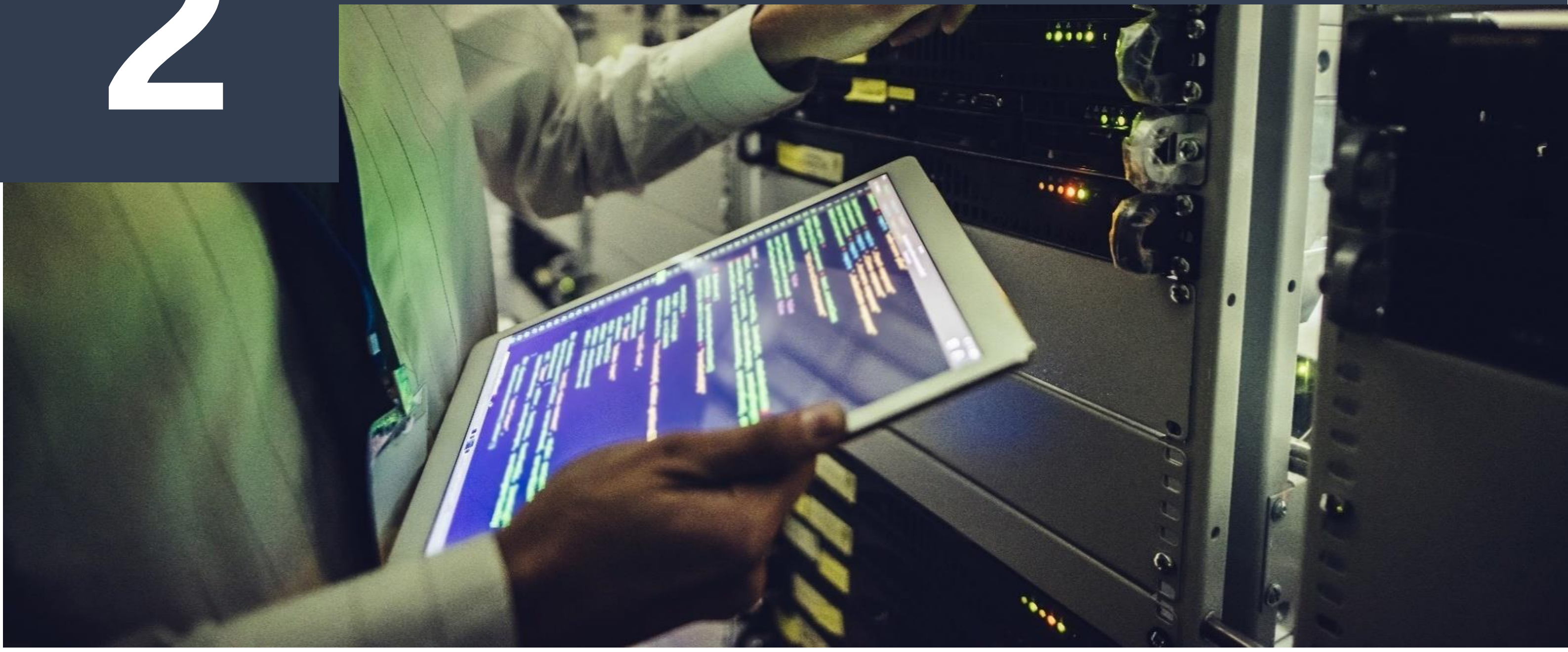
- **CCN-CERT, of the National Cryptologic Centre of the National Intelligence Centre**, with s competence area in the general, autonomous and local Public Sector, and systems that handle classified information.
- **INCIBE-CERT, of the National Institute of Cyber security of Spain**, with an area of competence in citizenship and the private sector. Likewise, INCIBE-CERT is the CERT that provides incident response services to institutions affiliated to RedIRIS, the Spanish academic and research network, in coordination with CCN-CERT regarding public bodies.
- **National Centre for Infrastructure Protection and Cyber security (CNPIC)**, with competence in critical infrastructures and critical operators, whose technical response capacities are materialized through the CSIRTs of reference. It is also the competent authority for those operators of essential services that are also critical, being in this case the Cyber Coordination Office the one that is responsible for the coordination in the cases provided for in the second paragraph of Article 11.2 of Royal Decree-Law 12/2018.
- **ESP-DEF-CERT of the Joint Command of Cyber Defence**, with competence in the networks and information and telecommunications systems of the Armed Forces, as well as those other networks and systems specifically entrusted to it that affect the National Defence, supporting operators of essential services and, necessarily, in those operators that have an impact on the National Defence and that are determined by regulation.

This National Guide to cybercrime notification and management is defined as the state reference for cybercrime notification (whether mandatory or optional communication), as well as for the demand for response to cyber security incidents.

Likewise, this document is also consolidated as a minimum benchmark in which any entity, public or private, citizen or agency, finds a scheme and precise guidance on to whom and how to report a cyber security incident within its sphere of influence.

This guide is aligned with Spanish regulations, European transpositions, as well as documents issued by supranational organizations that seek to harmonize the capacity to respond to cyber security incidents.

2 OBJETIVE OF THIS GUIDE



The purpose of this document is to generate a consensual framework of reference for national bodies competent in the field of cyber security incident notification and management. This includes the implementation of a series of minimum demanded standards and reporting obligations where required by law.

This National Guide for the notification and management of cyber incidents is especially aimed at:

- Information Security Officers (ISR), as Delegate Officers
- Response teams to cyber incidents and cyber security operation centers (SOC) internal to the organizations.
- CSIRT (*Computer Security Incident Response Team*)
- Information and/or Communication Systems Administrators
- Security staff
- Technical support staff
- Managers in the field of cyber security

This guide provides to the Responsible of the Information Security (RSI) the guidelines for the fulfillment of the obligations of reporting the cyber security incidents happened in the heart of the Public Administrations, the critical infrastructures and the strategic operators in their competence, as well as the rest of the entities included in the area of the Royal Decree-Law 12/2018 application. Here below it is shown an indicative scheme about the competent authorities and the CSIRT of reference:

COMPETENT AUTHORITY			
Operator type	**Subtype**	**Characteristics**	**Competent authority**
Essential services operator	Critical operator	-	**NACIONAL CENTER FOR INFRASTRUCTURE PROTECTION AND CYBER SECURITY (CNPIC)**
	No critical operator	Included in the scope of application of Law 40/2015, of October the 1st, on the Legal System for the Public Sector.	**NATIONAL CRYPTOLOGIC CENTER (CCN)**
		Rest	**SECTORAL AUTHORITY**
Digital services supplier	Private sector	-	**STATE SECRETARIAT FOR DIGITAL ADVANCEMENT**
	Public sector	Included in the scope of application of Law 40/2015, of October the 1st, on the Legal System for the Public Sector.	**NATIONAL CRYPTOLOGIC CENTER (CCN)**

Table 1. Competent authority

COMPUTER SECURITY INDICENT RESPONSE TEAM (CSIRT) OF REFERENCE		
Operator type	**Characteristics**	Competent authority
Essential services operator	Public Sector (entities included in the subjective scope of application of Law 40/2015)	**CCN-CERT**
	Private Sector (entities not included in the subjective scope of application of Law 40/2015)	**INCIBE-CERT**
Digital services supplier	Public Sector (entities included in the subjective scope of application of Law 40/2015)	**CCN-CERT**
	Private sector (entities that are not included in the subjective domain of the Law 40/2015 application)	**INCIBE-CERT**

Table 2. CSIRT of reference

Likewise, guidelines are referenced in the same sense, optional for the RSI of private companies that are not included in others already referenced above, of information and communication systems of institutions affiliated to the RedIRIS and citizens who, in a private decision, wish to contact the competent bodies.

From this document we can extract the following items:

- Homogeneous taxonomy in terms of classification, dangerousness and impact of cyber security incidents.

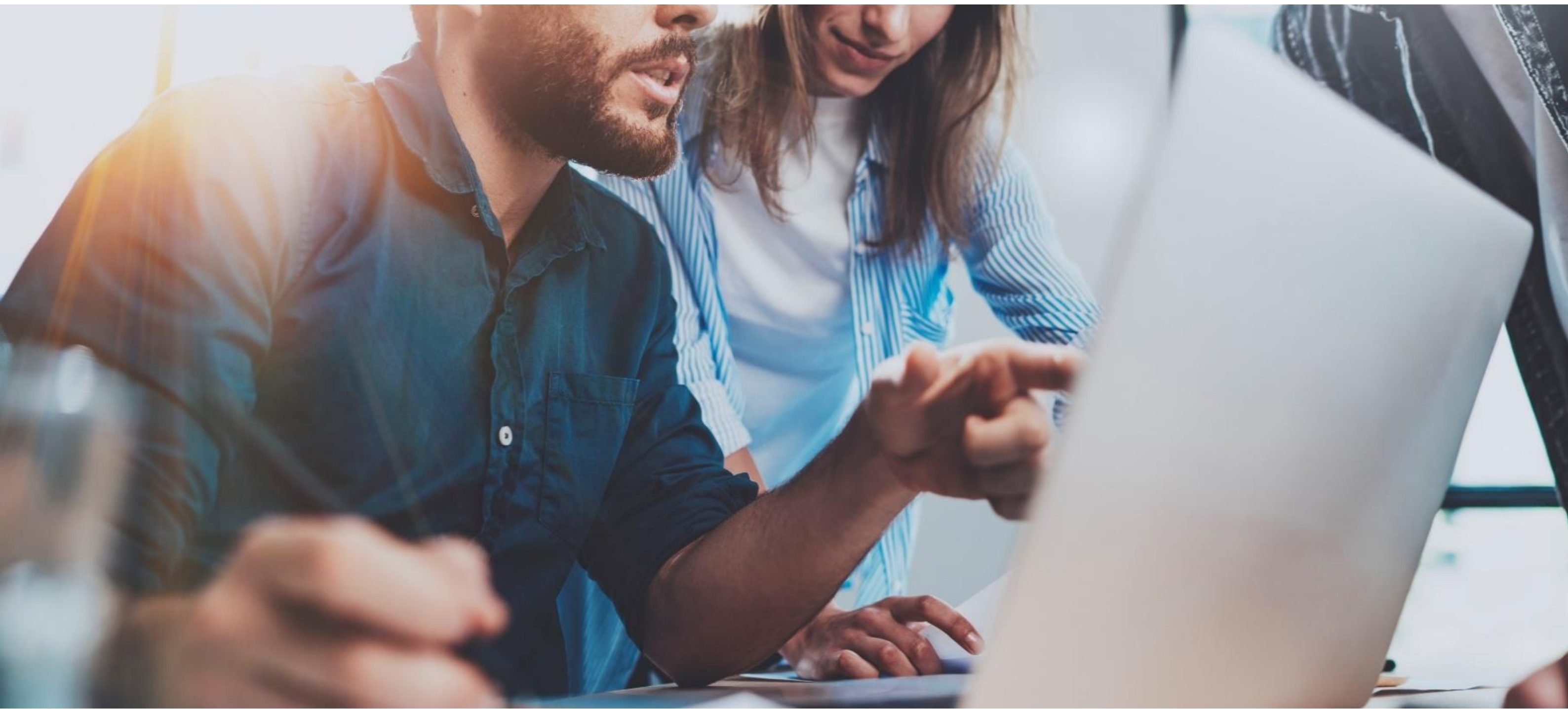
- Specifications of the competent authorities and CSIRT of reference at a national level, in terms of knowledge, management and resolution of cyber security incidents.

- Express definition of the cyber security incidents that must be notified to the competent authority as established by current legislation and through the channels defined for this purpose, depending on their danger and impact.

- Methodology for reporting and monitoring cyber security incidents (one-stop scheme).

- Specific requirements according to the particularity of the affected one, issued by the competent authorities.

The criteria included in this guide take into account generally recognized good practices in incident management and, as such, can serve as a reference in the design and implementation of this type of services in any other field.

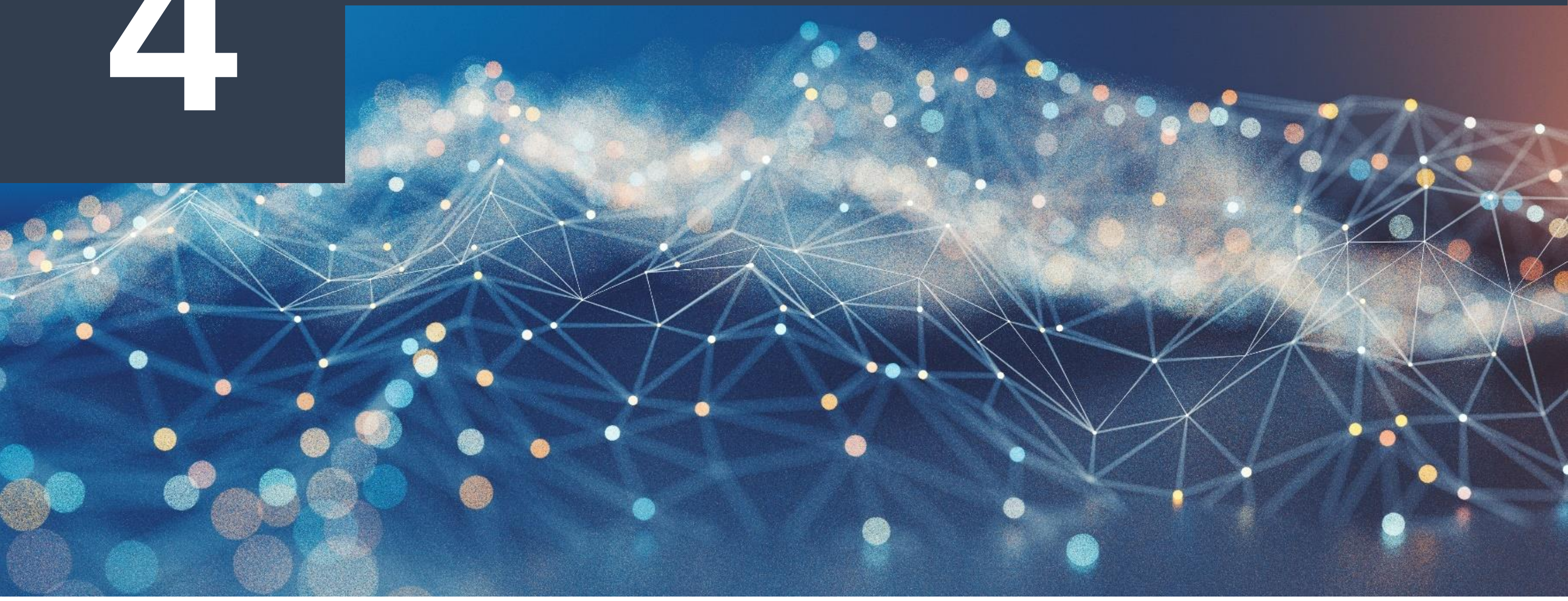


The public agencies or private companies obliged to notify a cyber incident under any regulation, must notify those cyber incidents occurred in its technological infrastructure that fall within the scope of the rule, the levels of danger and the levels of impact referenced in this document. Likewise, they may report other cyber incidents or cyber threats they judge appropriate, according to the following criteria:

- Need or convenience for the organization to have the support of the CSIRT of reference for the investigation or resolution of cyber incidents.
- Benefits or general interest for the security of the cyber security community as a whole, as well as for increasing situational awareness of the state of cyber security at the state level by the competent public agencies.

In relation to citizens and companies that are not included in the field of critical infrastructure protection, or of the public sector, or of the Royal Decree-Law 12/2018, the notification of cyber security incidents will have, in any case, a facultative and voluntary character. This target audience will find in this document a series of guidelines in the form of good practices.

4 ONE-STOP SCHEME NOTIFICATION



The information requested in each case, depending on the nature of the affected one, must be submitted in accordance with the channel established by its competent authority or CSIRT of reference. Based on all of the above, the reporting methodology will be as described in the following flow chart:

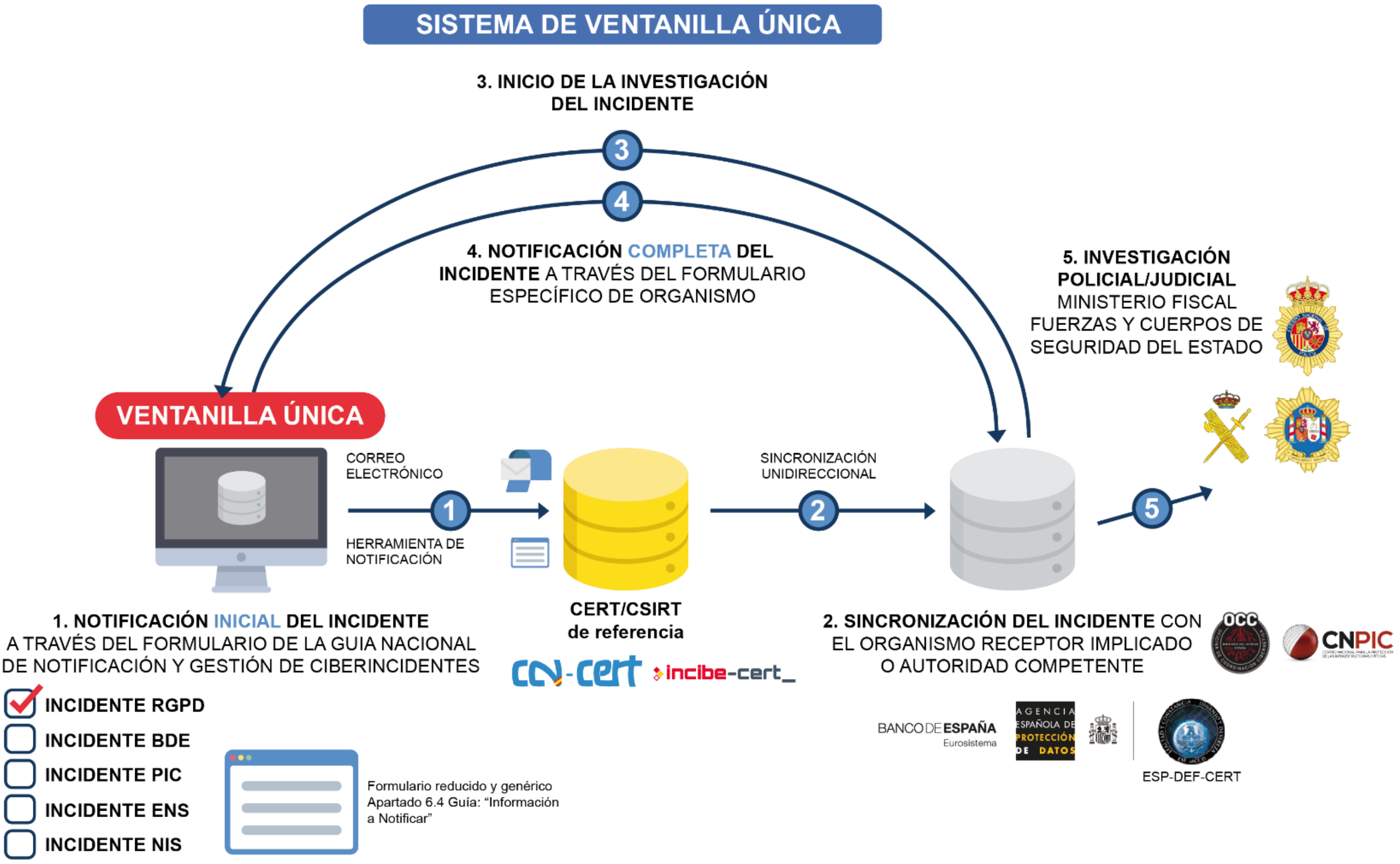

SISTEMA DE VENTANILLA ÚNICA
3. INICIO DE LA INVESTIGACIÓN DEL INCIDENTE
3
4
4. NOTIFICACIÓN COMPLETA DEL INCIDENTE A TRAVÉS DEL FORMULARIO ESPECÍFICO DE ORGANISMO
5. INVESTIGACIÓN POLICIAL/JUDICIAL
MINISTERIO FISCAL
FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO
VENTANILLA ÚNICA
CORREO ELECTRÓNICO
HERRAMIENTA DE NOTIFICACIÓN
1
SINCRONIZACIÓN UNIDIRECCIONAL
2
5
1. NOTIFICACIÓN INICIAL DEL INCIDENTE A TRAVÉS DEL FORMULARIO DE LA GUIA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES
CERT/CSIRT de referencia
ccn-cert
incibe-cert_
2. SINCRONIZACIÓN DEL INCIDENTE CON EL ORGANISMO RECEPTOR IMPLICADO O AUTORIDAD COMPETENTE
OCC
CNPIC
BANCO DE ESPAÑA Eurosistema
AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
ESP-DEF-CERT
☑ INCIDENTE RGPD
☐ INCIDENTE BDE
☐ INCIDENTE PIC
☐ INCIDENTE ENS
☐ INCIDENTE NIS
Formulario reducido y genérico
Apartado 6.4 Guía: "Información a Notificar"

Illustration 1.One-stop scheme system

ONE-STOP SCHEME SYSTEM

1. The affected subject will send an e-mail (or ticket) to the CSIRT of reference (INCIBE-CERT or CCN-CERT) notifying the incident.
2. The CSIRT of reference, depending on the incident, informs the receiving agency involved or thecompetent national authority about the incident.
   - If it affects the National Defence, the reference CSIRT ESP-DEF-CERT.
   - If it affects a Critical Infrastructure of Law PIC 8/2011, the CNPIC.
   - If it affects the RGPD, the AEPD
   - If it is an AAPP incident under the HIGH, VERY HIGH or CRITICAL ENS of danger, the CCN-CERT.
   - If it is a mandatory incident to report according to RD 12/2018, to the corresponding National Authority:
     - **RGPD**: refers to the URL of the AEPD portal.
     - **BDE:** the BDE .XLS notification template is sent.
     - **PIC:** the CNPIC .XLS notification template is sent
     - **ENS:** the .DOC notification template is sent to the CCN-CERT.
     - **NIS:** the notification template of the competent National Authority is sent.
3. The involved Receiving Agency or Competent National Authority contacts the person concerned with the aim of gathering information.
   - **RGPD**: refers to the URL of the AEPD portal.
   - **BDE:** the BDE .XLS notification template is sent.
   - **PIC:** the CNPIC .XLS notification template is sent
   - **ENS:** the .DOC notification template is sent to the CCN-CERT.
   - **NIS:** the notification template of the competent National Authority is sent.
4. The subject concerned communicates the needed data to the involved Receiving Agency or Competent National Authority.
5. If necessary, from the Cyber Coordination Office (CNPIC), the information can be made available to the State Security Forces and Corps and the Public Prosecutor's Office to initiate the police and judicial investigation (art. 14.3 RD Law 12/2018).

In accordance with Article 11.2 of RD Law 12/2018, of September the 7th, in cases of special gravity that are determined by regulation and that require a higher level of coordination than is necessary in ordinary situations, the CCN-CERT will exercise the national coordination of the technical response of the CSIRTs.

4.1. INCIDENT REPORTING TO CCN-CERT

It will be carried out as the preferred channel through the application enabled for this purpose: LUCIA[1], and secondarily through the email management of cyber security incidents incidentes@ccn-cert.cni.es preferably through messaging encrypted with the PGP key of this CERT[2].

4.2. INCIDENT REPORTING TO INCIBE-CERT

Cyber incidents are reported to INCIBE-CERT through a user who, as the final affected party or identified as the point of contact by the affected agency, accesses the response service through the means provided by this CERT.

If the report is made through e-mail, the generic mailbox for incident notification is incidencias@incibe-cert.es.

As responsible for early warning, preventive and reactive response to security incidents of the Spanish academic and research network (RedIRIS), the service is provided through mailbox iris@incibe-cert.es.

For their part, Operators of essential services will access the service through the account pic@incibe-cert.esor other mechanisms provided by INCIBE-CERT. The management of these incidents through INCIBE-CERT is operated jointly by INCIBE and the CNPIC.

In all cases, provided that the information sent to INCIBE-CERT is by e-mail, it will preferably be sent encrypted with the PGP key corresponding to each of the mailboxes of this CERT[3].

The report through e-mail is complementary to any other way that could be offered by INCIBE-CERT, such as contact forms, Application Programming Interface (API), web portal, etc.

4.3. INCIDENT REPORTING TOESP-DEF-CERT

CCN-CERT and INCIBE-CERT will cooperate with ESP-DEF-CERT, of the Ministry of Defence, in those situations that these require in support of essential services operators and, necessarily, in those operators that have an impact on the National Defence.

The communication with ESP-DEF-CERT will be carried out by e-mail by means of encrypted messaging with the public key PGP. In case of emergency, the Service Officer may be contacted. The specific data for communication can be found at the following link http://www.emad.mde.es/CIBERDEFENSA/ESPDEF-CERT/

[1] https://www.ccn-cert.cni.es/gestion-de-incidentes/lucia.html

[2] https://www.ccn-cert.cni.es/sobre-nosotros/contacto.html

[3] https://www.incibe-cert.es/sobre-incibe-cert/claves-publicas-pgp

5 CLASSIFICATION/TAXONOMY OF THE CYBER INCIDENTS

Since not all cyber incidents have the same characteristics or have the same implications, it is considered necessary to have a common taxonomy[4] of the possible incidents that are recorded, which will help later analysis, containment and eradication. *Table 3. Classification/Taxonomy of the cyber incidents* will be used to assign a specific classification for an incident recorded in networks and information systems when communication is made to the competent authority or CSIRT of reference.

CLASIFICATION/TAXONOMY OF CYBER INCIDENTS		
Classification	**Type of incident**	**Description and practical examples**
Abusive content	Spam	Unsolicited bulk email. The recipient of the content has not given valid authorization to receive a collective message.
	Hate crime	Defamatory or discriminatory content. E.g. cyber bullying, racism, threats to a person or directed against groups.
	Child pornography, inappropriate sexual or violent content	Material that visually represents content related to child pornography, advocacy of violence, etc.
Harmful content	Infected system	Infected system with malware. E.g.: system, computer or mobile phone infected with a rootkit.

[4] https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force

	C&C Server (Command and Control)	Connection to Command and Control (C&C) server via malware or infected systems.
	Malware distribution	Resource used for malware distribution. E.g. resource of an organization used to distribute malware.
	Malware configuration	Resource that hosts malware configuration files e.g. webinjects attack for Trojan.
Obtaining information	Network scanning	Sending requests to a system to discover possible weaknesses. Testing processes to collect information from hosts, services, and accounts are also included. E.g. DNS petitions, ICMP, SMTP, port scanning.
	Sniffing	Observation and recording of network traffic
	Social engineering	Collection of personal information without the use of technology. E.g. lies, tricks, bribes, threats.
Intrusion commitment	Exploitation of known vulnerabilities	Attempted compromise of a system or interruption of a service by exploiting vulnerabilities with a standardized identifier (see CVE). E.g. buffer overflow, backdoors, cross site scripting (XSS).
	Access attempt with credential violation	Multiple attempts to violate credentials. E.g. attempts to break passwords, brute force attack.
	Unknown attack	Attack using unknown exploit
Intrusion	Commitment of account with privileges	Commitment of a system where the attacker has acquired privileges.
	Commitment of account without privileges	Commitment of a system using accounts without privileges
	Commitment of applications	Commitment of an application by exploiting software vulnerabilities. E.g. SQL injection.

	Theft	Physical intrusion. E.g.: unauthorized access to Data Processing Center.
Availability	DoS (Service Denial)	Denial of Service Attack. E.g.: sending requests to a web application that causes the interruption or slowdown in the provision of the service.
	DDoS (Distributed denial of service)	Distributed denial of service attack. E.g. SYN packet flooding, reflection and amplification attacks using UDP-based services.
	Bad configuration	Wrong configuration of the software that causes problems of availability in the service. E.g. DNS server with the KSK of the root zone of obsolete DNSSEC.
	Sabotage	Physical sabotage. E.g. equipment wiring cuts or arson fires.
	Interruptions	Interruptions due to external causes. E.g.: natural disaster.
Commitment of the information	Unauthorized access to information	Unauthorized access to information. E.g.: theft of access credentials through traffic interception or through access to physical documents.
	Unauthorized modification of information	Unauthorized modification of information. E.g.: modification by an attacker using credentials stolen from a system or application or encrypted data using a ransomware.
	Loss of data	Loss of information e.g. loss due to hard disk failure or physical theft.
Fraud	Unauthorized use of resources	Use of resources for inappropriate purposes, including for-profit actions. E.g. use of email to engage in pyramid schemes.
	Copyright	Offering or installing unlicensed software or other copyrighted material. E.g. Warez.
	Impersonation	A type of attack in which one entity impersonates another for illegitimate gain.
	Phishing	The impersonation of another entity in order to convince the user to reveal his or her private credentials.

Vulnerable	Weak cryptography	Publicly accessible services that may have weak cryptography. E.g., web servers susceptible to POODLE/FREAK attacks.
	DDoS amplifier	Publicly accessible services that may be used for reflection or amplification of DDoS attacks. E.g. DNS open-resolvers or NTP servers with monlist monitoring.
	Services with an undesired potential access	E.g. Telnet, RDP or VNC.
	Revelation of information	Public access to services where potentially sensitive information may be revealed. E.g. SNMP or Redis.
	Vulnerable system	Vulnerable system. E.g. bad proxy configuration in client (WPAD), outdated system versions.
Others	Others	Any incident that has no place in any of the previous categories.
	APT	Attacks directed against specific organizations, based on very sophisticated mechanisms of concealment, anonymity and persistence. This threat usually employs social engineering techniques to achieve its objectives along with the use of known or genuine attack procedures.

Table 3. Classification/Taxonomy of the cyber incidents

6 NOTIFICATION OF CYBER SECURITY INCIDENTS

This section provides information regarding the notification to the relevant competent authority or CSIRT of reference of a registered cyber security incident. For this purpose, the criteria used and the tables to be consulted are included in order to assign the corresponding levels of hazard and impact in each case.

6.1. CRITERIA FOR NOTIFICATION

For the notification of cyber security incidents, the **Hazard Level** assigned to an incident will be used as a reference criterion, without prejudice to the fact that throughout the development, mitigation or resolution of the incident, it will be categorized with a certain **Impact Level** that makes it advisable to report the incident to the competent authority or CSIRT of reference.

In any case, when a certain event may be associated with more than one type of incident included in *Table 3.Classification/Taxonomy of cyber incidents* due to their potential characteristics, this will be associated with the one that has a higher Hazard Level according to the criteria set out in this section.

6.1.1. Cyber incident hazard level

The hazard indicator determines the potential threat posed by the materialization of an incident in the information or communication systems of the affected entity, as well as for the services provided or business continuity if any. This indicator is based on the characteristics intrinsic to the type of threat and its behaviour.

Incidents will be associated with one of the following hazard levels: **CRITICAL, VERY HIGH, HIGH, MEDIUM, and LOW.**

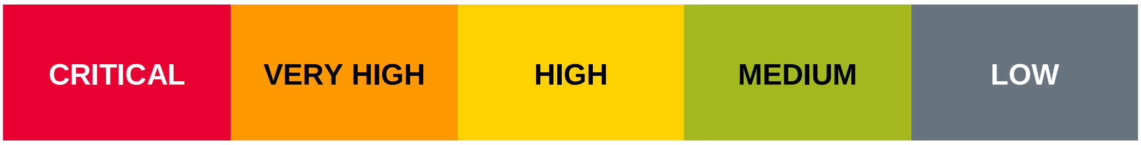


Illustration2.Cyber incident hazard level

Here below is included *Table 4. Criteria for the determination of the cyber incident hazard level*. By consulting this table, information reporting entities will be able to assign a certain hazard level with an incident.

CRITERIA FOR THE DETERMINATION OF A CYBER INCIDENT HAZARD LEVEL		
Level	**Classification**	**Type of incident**
CRITICAL	Others	APT
VERY HIGH	Harmful code	Malware distribution
		Malware configuration
	Intrusion	Theft
	Availability	Sabotage
		Interruptions
HIGH	Abusive content	Child pornography, inappropriate sexual or violent content
	Harmful code	Infected system
		C&C server (Command and Control)
	Intrusion	Applications commitment
		Commitment of accounts with privileges
	Intrusion attempt	Unknown attack
	Availability	DoS (Service Denial)
		DDoS (Distributed Denial of Service)
	Information commitment	Unauthorized access to information
		Unauthorized modification of information
		Loss of data
	Fraud	Phishing
MEDIUM	Abusive content	Hate speech

	Obtaining information	Social engineering
	Intrusion attempt	Exploitation of known vulnerabilities
		Attempted access with violation of credentials
	Intrusion	Commitment of non-privileged accounts
	Availability	Bad configuration
	Fraud	Unauthorized use of resources
		Copyrights
		Impersonation
	Vulnerable	Weak cryptography
		DDoS amplifier
		Services with unwanted potential access
		Disclosure of information
		Vulnerable system
LOW	Abusive content	Spam
	Obtaining information	Network scanning
		Packet analysis (sniffing)
	Others	Others

Table 4. Criteria for the determination of a cyber incident hazard level

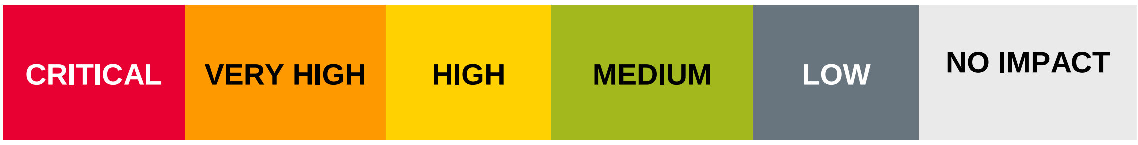
6.1.2. Level of impact of the cyber incident

The impact indicator of a cyber incident will be determined by evaluating the consequences that the cyber incident has had on the functions and activities of the affected organization, on its assets or on the affected individuals. According to this, aspects are taken into account such as the potential or materialized consequences caused by a certain threat in an information and/or communication system, as well as in the affected entity itself (public or private bodies, and individuals).

The criteria used to determine the level of impact associated with a cyber incident meet the following parameters:

- Impact on National Security or in Citizen Security
- Effects on the provision of an essential service or critical infrastructure
- Type of information or systems affected
- Degree of affectation to the organization's facilities.
- Possible interruption in the provision of the organization's normal service
- Personal and others time and costs until the recovery of normal operation of the facilities
- Economic losses
- Geographical extension affected
- Associated reputational damage

Incidents will be associated with any of the following impact levels::**CRITICAL, VERY HIGH, HIGH**, **MEDIUM, LOW** or **NO IMPACT.**



CRITICAL

VERY HIGH

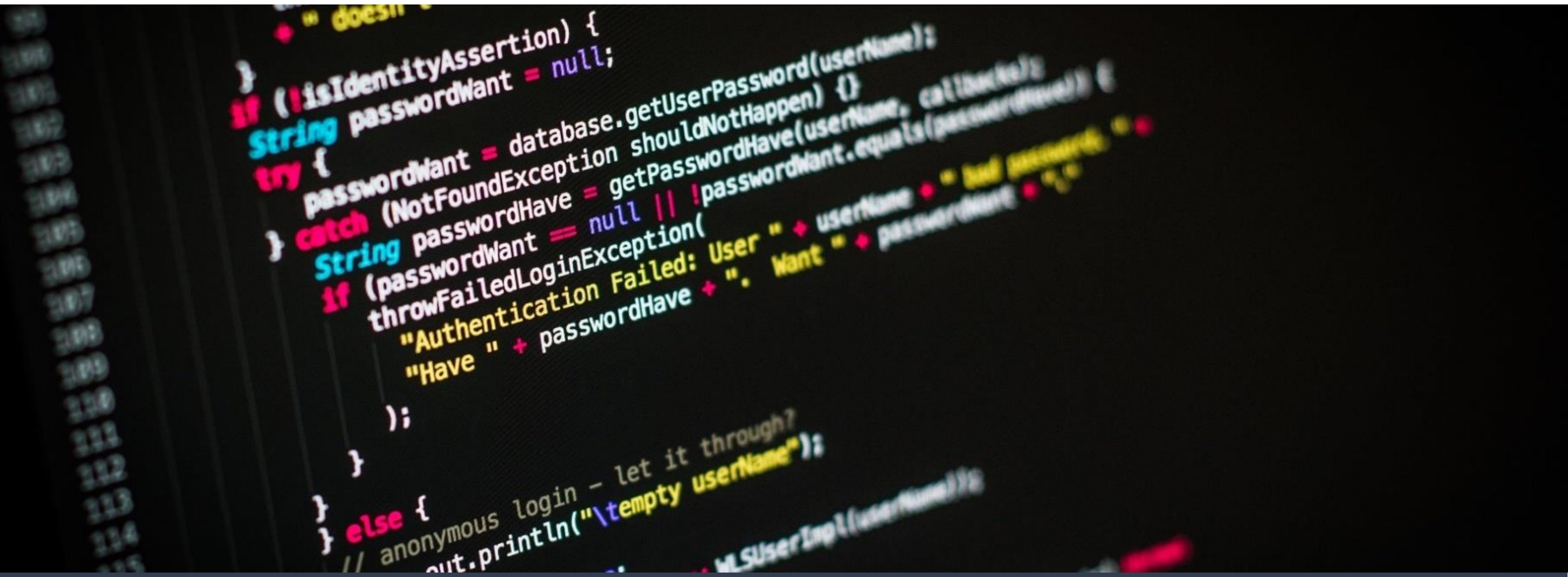
HIGH

MEDIUM

LOW

NO IMPACT

Illustration 3. Levels of impact of a cyber incident



```
                                  + " doesn'
        }
        if (!isIdentityAssertion) {
            String passwordWant = null;
            try {
                passwordWant = database.getUserPassword(userName);
            } catch (NotFoundException shouldNotHappen) {}
            String passwordHave = getPasswordHave(userName, callbacks);
            if (passwordWant == null || !passwordWant.equals(passwordHave)) {
                throwFailedLoginException(
                    "Authentication Failed: User " + userName + " bad password, Want " + passwordWant + ", "
                    "Have " + passwordHave + ".
                );
            }
        } else {
            // anonymous login - let it through?
            out.println("\tempty userName");
```

Here below is included *Table 5. Criteria for the determination of the impact level of a cyber incident*. By consulting this table, information reporting entities will be able to assign a certain hazard level with an incident.

CRITERIA FOR THE DETERMINATION OF THE IMPACT LEVEL OF A CYBER INCIDENT	
Level	**Description**
CRITICAL	It significantly affects national security.
	It affects citizen security, with potential danger to people's lives.
	It affects a Critical Infrastructure.
	It affects systems classified as SECRET.
	It affects more than 90% of the organization's systems.
	Interruption in service provision for more than 24 hours and more than 50% of users.
	The cyber incident needs more than 100 Person-Days to be resolved.
	Economic impact greater than 0.1% of the current GDP.
	Supranational geographical extension.
	Very high reputational damage and continuous coverage in international media.
VERY HIGH	It affects citizen security with potential danger for material goods.
	It significantly affects official activities or missions abroad.
	It affects an essential service.
	It affects systems classified as RESERVED.
	It affects more than 75% of the organization's systems.
	Interruption in service provision for more than 8 hours and more than 35% of users.
	The cyber incident needs between 30 and 100 Person-Days to be resolved.
	Economic impact between 0.07% and 0.1% of the current GDP.
	Geographical extension greater than 4 Autonomous Communities or 1 T.I.S.
	Reputational damage to the country's image (Marca España).
	High reputational damage and continuous coverage in national media.
HIGH	It affects more than 50% of the organization's systems.
	Interruption in service provision for more than 1 hour and more than 10% of users.
	The cyber incident needs between 5 and 30 Person-Days to be resolved.
	Economic impact between 0.03% and 0.07% of the current GDP.
	Geographical extension greater than 3 Autonomous Communities.
	Reputational damage that is difficult to repair, with media coverage (wide media coverage) and affecting the reputation of third parties.
MEDIUM	It affects more than 20% of the organization's systems.
	Interruption in service provision for more than 5% of users.
	The cyber incident needs to between 1 and 5 Person-Days to be resolved.
	Economic impact between 0.001% and 0.03% of the current GDP.
	Geographical extension greater than 2 Autonomous Communities.
	Appreciable reputational damage, with media coverage (wide media coverage).

LOW	It affects the organization's systems.
	Interruption of the service provision.
	The cyber incident needs less than 1 Person-Days to be resolved.
	Economic impact between 0.0001% and 0.001% of the current GDP.
	Geographical extension greater than 1 Autonomous Community.
	Reputational damage on a one-off basis, with no media coverage.
NO IMPACT	There is no appreciable impact.

Table 5. Criteria for the determination of the impact level of a cyber incident

T.I.S refers to "Territories of Singular Interest". The cities of Ceuta and Melilla and each of the islands that make up the archipelagos of the Balearic and Canary Islands are considered as such.

GDP refers to "Gross Domestic Product updated to 2017 is considered to be: 1,162,663 million Euros.

6.1.2. Levels with associated mandatory reporting

The incidents will be associated with one of the hazard and impact levels established in this section, taking into account the obligation to report all those that are categorized with a level **CRITICAL, VERY HIGH OR HIGH** for all those **obligated subjects** to whom it is applicable specific regulations in accordance with the provisions of this "National Guide for notification and management of cyber incidents" depending on their nature. In this case, **they must communicate, in time and form, the incidents they record on their networks and information systems and are required to notify because they exceed the impact or hazard thresholds established in this guide.**

6.2. INTERACTION WITH THE CSIRT OF REFERENCE

The CSIRTs of reference have incident notification and ticketing tools for a better incident management and follow-up with users. Each CSIRT can provide different methods of interaction with these tools to facilitate interaction throughout the life cycle of the incident.

However, if the tools provided by the CSIRTs of reference are not available, the use of e-mail is considered valid.

6.3. OPENING OF THE INCIDENT

Whenever the CSIRT of reference receives notification of a possible cyber incident, the technical team performs an initial analysis to determine whether the case is likely to be handled by them. This opening can be produced by a report of the affected party, by a detection of the CSIRT as part of the detection tasks performed, or by a third party reporting to the CSIRT an incident affecting its reference community.

If cyber incident management is applied by the CSIRT, the reported information will be recorded and an initial classification and values of hazard and impact will be assigned, which will be communicated to the sender, and the necessary actions for the resolution of the cyber incident will subsequently be initiated.

During the registration of a cyber incident, the CSIRT will assign to each case a unique identifier that will be present during all communications related to the incident. If communications are made by e-mail, this identifier appears in the "subject" field and should not be modified or deleted as this would slow down the management and final resolution of the cyber incident.

Throughout the cyber incident management process, the CSIRT may communicate with the sender or third parties to request or exchange additional information to expedite the resolution of the problem.

Likewise, the competent authorities may establish appropriate channels of communication as it legally develops.

6.4. INFORMATION TO BE NOTIFIED

For a correct management and treatment of a registered incident, it is necessary to have precise data and information about it. For this reason, *Table 6. Information to be notified in a cyber incident to the competent authority* specifies by way of guidance a series of points that the entity affected by the cyber incident may provide in its communication to the competent authority or CSIRT of reference.

However the provisions of the previous paragraph, all regulated entities to which specific regulations are applicable in accordance with the provisions of this "National guide for the notification and management of cyber incidents" shall communicate in time and form all information related to the registered incident that is required of them.

In any case, in the initial notification, the regulated entity shall communicate all the fields of which it is aware at that time, and all the fields of *Table 6. Information to be notified in a cyber incident to the competent authority* shall subsequently be filled in the final notification of the incident.

What to notify	Description
Subject	A sentence that describes the incident in a general way. This field will be inherited by all notifications associated with the incident.
OSE/PSD	Name of the essential services operator or digital service provider that reports.
Strategic sector	Energy, transport, financial, etc.
Date and time of the incident[5]	Indicate as precisely as possible when the cyber incident occurred.
Date and time of the detection of the incident	Indicate as precisely as possible when the cyber incident was detected.
Description	Describe in detail what happened.
Affected technological resources	Indicate the technical information about the number and type of assets affected by the cyber incident, including IP addresses, operating systems, applications, versions...
Origin of the incident	Indicate the cause of the incident if known. Opening a suspicious file, connecting a USB device, accessing a malicious website, etc.

[5] Indicating the time zone UTC format.

Taxonomy (classification)	Possible classification and type of cyber incident according to the taxonomy described.
Hazard level	Specify the level of hazard assigned to the threat. See Table 4. Criteria for determining the hazard level of a cyber incident.
Impact level	Specify the impact level assigned to the incident. See Table 4. Criteria for determining the level of impact of a cyber incident.
Cross-border impact	Indicate if the incident has cross-border impact in any Member State of the European Union. Specify.
Action plan and countermeasures	Actions taken so far in relation to the cyber incident. Indicate the Action Plan followed together with the countermeasures implemented.
Affectation	Indicate whether the affected party is a company or an individual and the effects according to the criteria indicated in Table 5. Criteria for the determination of the impact level of a cyber incident.
Means required for resolution (P-D)	Capacity used in the resolution of the incident in Person-Days.
Estimated economic impact (if known)	Costs associated with the incident, both direct and indirect.
Geographical area (if known)	Local, regional, national, supranational, etc.
Reputational damage (if known)	Effect on the operator's corporate image.
Attachments	Indicate the list of attached documents provided to help know the cause of the problem or its resolution (screenshots, information log files, e-mails, etc.).
Affected regulation	ENS / RGPD /NIS / PIC / Others
Action from the FFCCSE is required	Yes / No

Table 6. Information to be notified in a cyber incident to the competent authority

6.5. REPORT WINDOW

All reporting parties affected by an incident of obligatory notification to the competent authority, through the CSIRT of reference, shall submit, in due time and form, those initial, intermediate and final notifications required in accordance with *Table 7. Temporary reporting window for reporting parties.*

- The initial notification is a communication consisting of informing and alerting of the existence of an incident

- The intermediate notification is a communication through which the data available at that time relating to the reported incident will be updated

- The final notification is a final communication by which the final data relating to the reported incident are explained and confirmed

However, any additional intermediate or subsequent notifications deemed necessary shall be provided.

The communication will always be made in writing through the use of electronic mail or system provided by the operator's CSIRT of reference, taking the structure of *Table 6. Information to be notified in a cyber incident to the competent authority.*

Hazard or impact level	Initial notification	Intermediate notification	Final notification
CRITICAL	Immediate	24 / 48 hours	20 days
VERY HIGH	Immediate	72 hours	40 days
HIGH	Immediate	-	-
MEDIUM	-	-	-
LOW	-	-	-

Table 7. Temporary reporting window for reporting parties

The times reflected in *Table 7. Temporary reporting window for reporting parties* for "intermediate notification" and "final notification" refer to the time of submission of the "initial notification". The "initial notification" has as its time reference the moment of having knowledge of the incident.

6.6. CLOSING STATUS AND VALUES

During the different phases of management of a cyber incident, the CSIRT of reference will maintain the incident in an open status, carrying out in coordination with the affected party the necessary actions and the appropriate follow-ups.

A solution and the closure of the associated cyber incident do not always imply a satisfactory resolution of the problem. In some cases it is not possible to reach an adequate solution for different reasons, such as a lack of response from someone involved or the absence of evidence to identify the origin of the problem.

Table 8. States of cyber incidents shows the different status that a cyber incident may have, in a given instant, detailing the different types of closure.

Status	Description

Closed (Resolved and no response)	There is no response from the affected organism in a given period. However, the incident appears to be resolved.
Closed (Resolved and answered)	The affected organism has resolved the threat and notifies its CSIRT of reference the cyber incident closure.
Closed (No impact)	The detection is positive but the organism is not vulnerable or affected by the cyber incident.
Closed (False positive)	The detection was erroneous.
Closed (No resolution and no response)	If the affected organism has not resolved the cyber incident and it has not communicated with the CSIRT of reference, it is closed with this status.
Closed (No resolution and response)	A solution to the problem has not been reached or the affected person indicates that he does not know how to solve it even with the indications provided by the CSIRT.
Open	Status that goes from when the affected organism notifies the threat to the CSIRT of reference, or the latter communicates it to the affected person, until the closure of the same occurs due to any of the causes previously described.

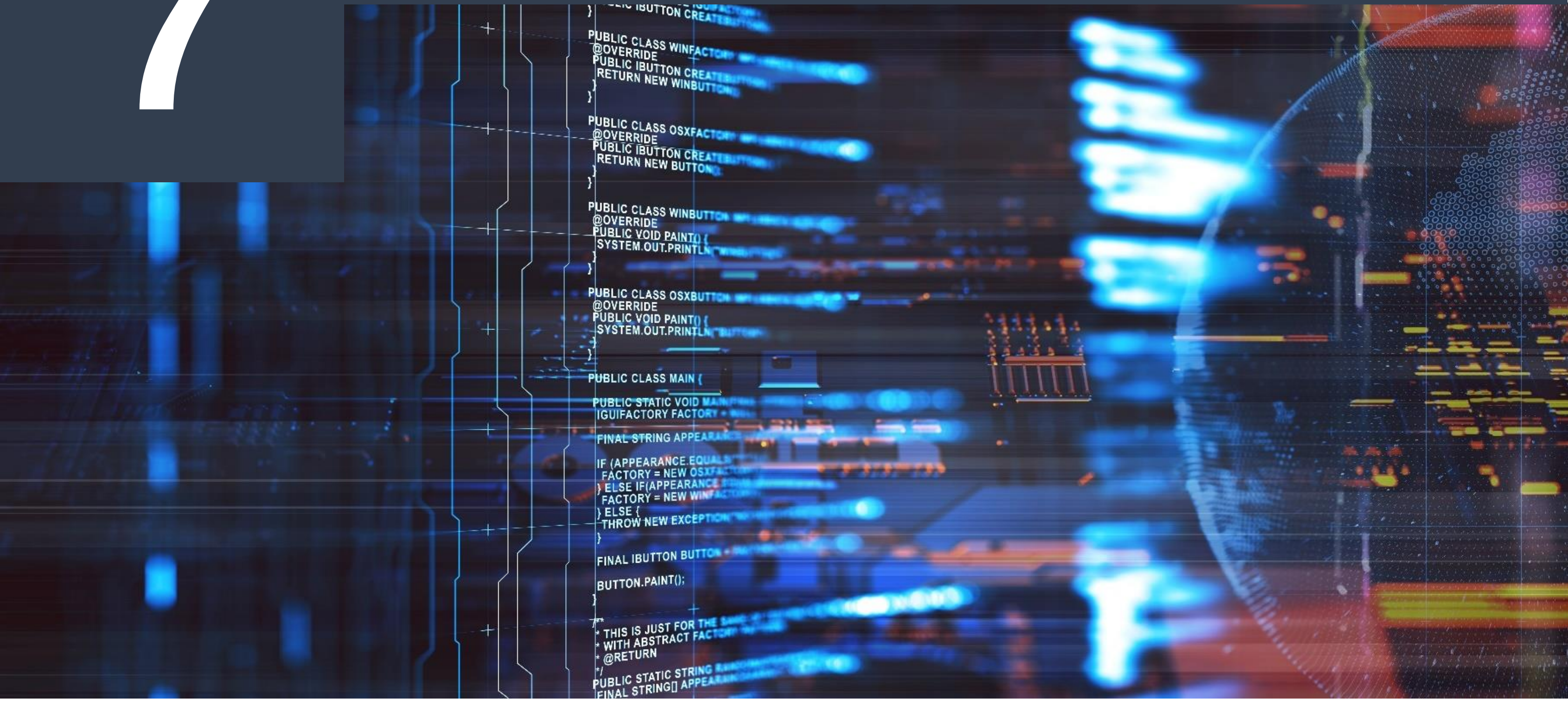
Table 8. Status of cyber incidents

Table 9. Cyber incident closure times without response shows the days after which a cyber incident without response will close, depending on its hazard or impact level.

Hazard or impact level	Cyber incident closure (calendar days)
CRITICAL	120
VERY HIGH	90
HIGH	45
MEDIUM	30
LOW	21

Table 9. Cyber incident closure times without response

7 CYBER SECURITY INCIDENTS MANAGEMENT



Cyber incident management is an orderly set of actions focused on preventing as much as possible the occurrence of cyber incidents and, if they occur, restoring operation levels as soon as possible. The incident management process consists of different phases and, although all are necessary, some may be included as part of others or treated simultaneously.

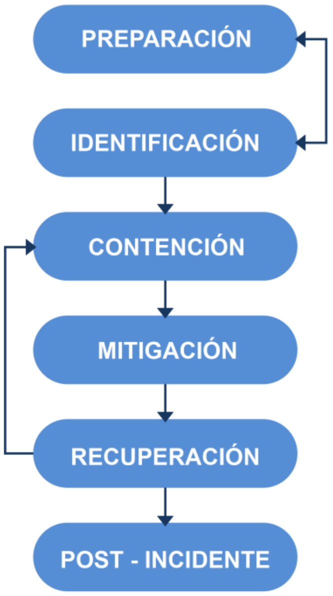


Illustration 4. Cyber incident management phases

The different phases of cyber incident management are briefly described below.

7.1. PREPARATION

This is an initial phase in which every entity must be prepared for any event that may occur. A good anticipation and previous training is key to carry out an effective management of an incident, for which it is necessary to take into account three fundamental pillars: people, procedures and technology.

Some of the most relevant points to take into account in this phase are:

- Have updated contact information, both internal and external personnel, to involve in other phases of cyber incident management, as well as the different ways of contact available in each case.
- Maintain updated policies and procedures. Especially all those related to incident management, evidence collection, forensic analysis or system recovery.
- Tools to be used in all phases of cyber incident management.
- Training of the human team to improve technical and operational capabilities.
- Perform risk analysis to have a risk treatment plan to control risks that can be mitigated, transferred or accepted.
- Execution of cyber exercises in order to train technical, operational, management and coordination capacities and procedures.

7.2. IDENTIFICATION

The objective of this phase is to have the capacity to identify or detect any cyber incident that an organism or entity may suffer and with the least possible delay, for which it is important to carry out as complete a monitoring as possible. Taking into account the maximum that not all events or cyber security alerts are cyber incidents.

Correct identification or detection is based on the following principles:

- Register and monitor network, system and application events.
- Collect situational information to detect anomalies.
- Have the capacity to discover cyber incidents and to communicate them to the appropriate contacts.
- Collect and securely store all the evidences.

- Share information with other internal and external teams in a bidirectional manner to improve detection capabilities.

7.3. CONTAINMENT

Once a cyber incident has been identified, the top priority is to contain its impact on the organization so that propagation to other systems or networks can be avoided as soon as possible, avoiding a greater impact, and the extraction of information from outside the organization.

This is usually the phase in which the evaluation of all the information available at that time is carried out, making a classification and prioritization of the cyber incident according to the type and criticality of the information and systems affected. In addition, possible impacts on the business are identified and, depending on the procedures, decisions are made with the appropriate business units and/or those responsible for the potentially affected services.

During this phase is due:

- Register and monitor network, system and application events. Record and monitor network event.
- Collect situational information to detect anomalies.
- Have the skills to discover cyber incidents and communicate them to the appropriate contacts.
- Collect and securely store all evidence.
- Share information with other internal and external teams in a bi-directional way to improve detection capabilities
- Share information with other internal and external teams.

7.4. MITIGATION

Mitigation measures will depend on the type of cyber incident, as in some cases it will be necessary to have support from service providers, such as in the case of a distributed denial of service (DDoS) attack, and in other cyber incidents may even include the complete deletion of the affected systems and the recovery from a backup.

Although mitigation measures depend on the type of cyber incident and the impact it has had, some recommendations at this stage are:

- Determine the causes and symptoms of a cyber incident to determine the most effective mitigation measures.

- Identify and remove all software used by attackers. Often, the way that offers the most guarantees of removing all trace of an incident passes through a new platform of the machine.

- Recovering the last clean backup.

- Identify the services used during the attack, as sometimes attackers use legitimate services of the attacked systems.

7.5. RECOVERY

The purpose of the recovery phase consists on returning the operating level to its normal state and for the affected business areas to resume their activity. It is important not to rush into the production of systems that have been involved in cyber incidents.

It is important to pay special attention to these systems during the production and look for any signs of suspicious activity, defining a period of time with additional monitoring measures.

7.6. POST-INCIDENT ACTIONS

Once the cyber incident is under control and the activity has returned to normal, it is time to carry out a process that is not usually given all the importance it deserves: the lessons learned.

It is convenient to reflect on what happened, analyzing the causes of the problem, how the activity has developed during the management of the cyber incident and all the problems associated with it. The purpose of this process is to learn from what happened and to take appropriate measures to prevent a similar situation from happening again, as well as to improve procedures.

Finally, there will be a cyber incident report that will detail the cause of the cyber incident and the cost (especially in terms of information commitment or impact on the services provided), as well as the measures that the organization must take to prevent future cyber incidents of a similar nature.

8 METRICS AND INDICATORS

With a view to evaluating the implementation, effectiveness and efficiency of the cyber incident management process by the competent authority or CSIRT of reference, the following tables are included for the assignment of recommended metrics and reference indicators to measure the level of implementation and efficiency of the incident management process of each organization.

8.1. IMPLEMENTATION METRICS

M1	**Indicator**	Scope of the incident management system	
	Objective	To know if all the information systems are attached to the service	
	Method	Services that are under control are counted. (If you knew how many services are there in total, you could calculate a percentage). # essential services for the organization # important services for the organization	
	Characterization	Object	100%
		Yellow threshold	Essential: 4/5 (80%) Important: 2/3 (67%)
		Red threshold	Essential: 2/3 (67%) Important: 1/2 (50%)
		Measurement frequency	Quarterly
		Reporting frequency	Annual

Table 10. Implementation metrics

8.2. CYBER INCIDENT RESOLUTION METRICS

M2	**Indicator**	Resolution of cyber incidents with HIGH / VERY HIGH / CRITICAL impact level.	
	Objective	To be able to promptly resolve high-impact incidents.	
	Method	It measures the time it takes to resolve an incident with a high impact on the organization's systems: from notification to resolution. T(50) time that it takes to close 50% of the incidents T(90) time that it takes to close 90% of the incidents	
	Characterization	Object	T(50) = 0 && T(90) = 0
		Yellow threshold	T(50) > 4d || T(90) > 5d
		Red threshold	T(50) > 14d || T(90) > 18d
		Measurement frequency	Annual
		Report frequency	Annual
M3	**Indicator**	Resolution of cyber incidents with LOW / MEDIUM impact level.	
	Objective	To be able to promptly resolve medium-impact incidents.	
	Method	It measures the time it takes to resolve an incident with a high impact on the organization's systems: from notification to resolution. T(50) time that it takes to close 50% of the incidents T(90) time that it takes to close 90% of the incidents	
	Characterization	Object	T(50) = 0 && T(90) = 0
		Yellow threshold	T(50) > 10d || T(90) > 30d
		Red threshold	T(50) > 15d || T(90) > 45d
		Measurement frequency	Annual
		Reporting frequency	Annual

Table 11. Cyber incident resolution metrics

8.3. RESOURCE METRICS

M4	**Indicator**	Resources consumed	
	Objective	To know if it is necessary to increase the workforce.	
	Method	It estimates the number of person-hours dedicated to resolving security incidents. Equation: #hours dedicated to incidents / #hours formally contracted for ICT security	
	Characterization	Object	<20%
		Yellow threshold	20%
		Red threshold	50%
		Measurement frequency	Quarterly
		Reporting frequency	Annual

Table 12. Resource metrics

8.4. INCIDENT MANAGEMENT METRICS

M5	**Indicator**	Closing status of the incidents	
	Objective	To be able to manage security incidents	
	Method	It measures the number of incidents that have been closed without response: Equation: # closed security incidents with no response / # total of notified incidents	
	Characterization	Object	<10%
		Yellow threshold	20%
		Red threshold	50%
		Measurement frequency	Quarterly
		Reporting frequency	Annual
M6	**Indicator**	Closing status of hazard incidents VERY HIGH / CRITICAL	
	Objective	To be able to manage high-risk security incidents	
	Method	It measures the number of incidents that have been closed without response: Equation: # closed security incidents with no response / # total of notified incidents	
	Characterization	Object	0%
		Yellow threshold	5%
		Red threshold	20%
		Measurement frequency	Quarterly
		Reporting frequency	Annual

Table 13. Incident management metrics

A1

ANNEX 1. NOTIFICATION IN THE FIELD OF CRITICAL INFRASTRUCTURE PROTECTION

Those entities whose competent authority for incident notification, in accordance with the current legislation, is the **National Centre for Infrastructure Protection and Cyber security (CNPIC)**, must comply with the provisions of this Annex regarding the notification of incidents occurring in the networks and information systems that support the essential services provided by their infrastructures.

For this purpose, the operator concerned must take into account the provisions of this annex regarding the notification obligations, depending on whether certain criteria relating to the hazard and/or impact level associated with the incident are met. It also includes the necessary information regarding the content of the communications to be made, the required temporary framework and the mandatory communications to the prosecution service or other agencies.

Likewise, those suppliers of the subjects bound by this annex who provide their products or services to them, and whose activities have a direct effect on the provision of an Essential Service, must comply with the same criteria required of operators. In any case, the affected operator shall be ultimately responsible for compliance with the requirements of this text.

MANDATORY COMMUNICATIONS

For the notification of cyber security incidents, the **Hazard level** assigned to an incident will be used as a reference criterion, without prejudice to the fact that throughout its development, mitigation or resolution, it will be categorized with a certain **Impact level** that requires the communication of the incident to the CNPIC through the CSIRT of reference.

Nevertheless, the provisions of the preceding paragraph, the Ministry of the Interior, through the Secretariat of State for Security, may require the communication of any incident occurring in the networks or information systems that support the essential services provided by its infrastructures in accordance with the application of a certain Antiterrorist Alert Level (NAA) or Critical Infrastructure Alert Level (NAIC).

Mandatory notification according to the level of hazard of the cyber incident

According to the criteria indicated in the body of this text, in which a certain level of hazard is assigned to an incident, the notification of all those that are categorized with a **CRITICAL, VERY HIGH or HIGH** level of hazard will be mandatory.

For a more precise definition of the hazard level associated with each incident recorded on the operator's networks and information systems, it will be used *Table 4.Criteria for the determination of the cyber incident hazard level* in which a given level of hazard is assigned based on the classification of the incident.

Mandatory notification according to the level of impact of the cyber incident

According to the criteria indicated in the body of this text in which a certain level of impact is assigned to an incident, the notification of all those that are categorized with a **CRITICAL, VERY HIGH or HIGH** impact level will be mandatory.

For a more precise definition of the impact level associated with each incident recorded, it will be followed *Table 5.Criteria for the determination of the impact level of a cyber incident* in which a determined level of impact is assigned based on a series of effects caused by the incident on the operator's networks or information systems.

COMMUNICATION TO THE PROSECUTION SERVICE AND OTHER AGENCIES

The Cyber Coordination Office (OCC) of the Ministry of the Interior, integrated into the structure of the National Centre for Infrastructure Protection and Cyber security (CNPIC) and functionally dependent on the Secretariat of State for Security (SES), is the competent body to coordinate and promote the operational response by the State Security Forces and Corps (FFCCSE), and especially by its technological units.

Therefore, when an incident is reported within the scope of this annex to the "National Guide for the notification and management of cyber incidents", and presents characters of criminal infraction, the National Center for Infrastructure Protection and Cybersecurity will report it, through the Cyber Coordination Office of the Ministry of the Interior to the Attorney General's Office and the FFCCSE for appropriate purposes, transferring all information in their possession in relation to the event.

The OCC is also in permanent contact with national and international agencies, with which it exchanges strategic and operational information to raise situational awareness of the state of cyber threats and to improve the level of cyber security at a global level.

REPORT FLOWCHARTS AND PIC OPERATIONAL RESPONSE

The following images show the informative flowcharts detailing the process of notification and management of an incident and the process of operational response to the communication of a cyber incident in the networks or information systems that support the essential services provided by the infrastructures of an operator.

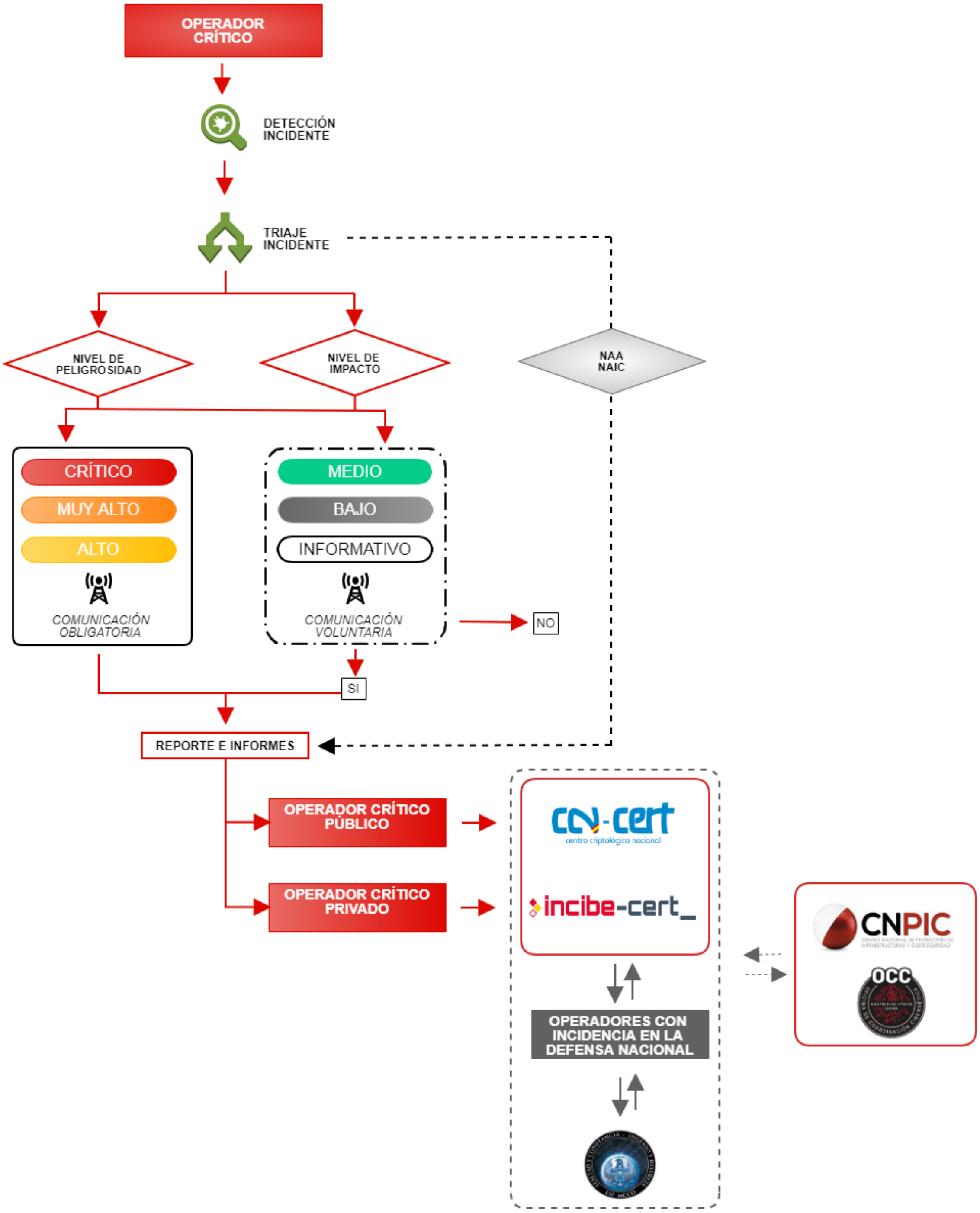


Illustration 5. Flowchart of management and notification at PIC level

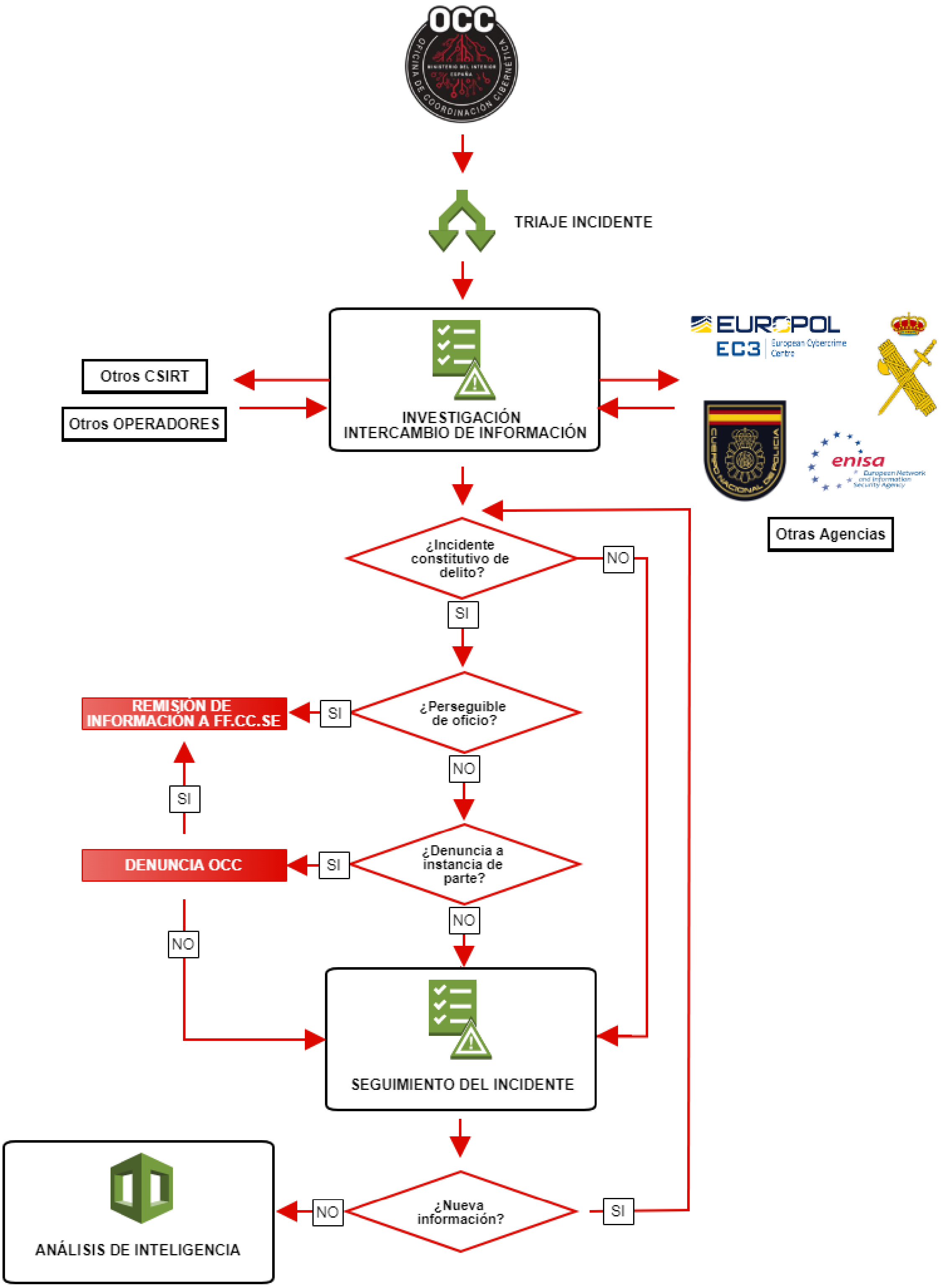

OCC
OFICINA DE COORDINACIÓN CIBERNÉTICA
TRIAJE INCIDENTE
INVESTIGACIÓN
INTERCAMBIO DE INFORMACIÓN
Otros CSIRT
Otros OPERADORES
EUROPOL EC3 European Cybercrime Centre
enisa
Otras Agencias
¿Incidente constitutivo de delito?
NO
SI
¿Perseguible de oficio?
SI
REMISIÓN DE INFORMACIÓN A FF.CC.SE
NO
SI
¿Denuncia a instancia de parte?
SI
DENUNCIA OCC
NO
NO
SEGUIMIENTO DEL INCIDENTE
¿Nueva información?
NO
SI
ANÁLISIS DE INTELIGENCIA

Illustration 6. Flowchart of operational response at PIC level

A2

ANNEX 2. NOTIFICATION IN THE PUBLIC SECTOR FIELD

The Public Sector agencies will notify the incidents as specified in the Technical Instruction on Security Notification of Security Incidents published in BOE No. 95 of 18 April 2018 and the Guide CCN-STIC 817 Management of Cyber incidents.

Mandatory notification in incidents with High, Very High and Critical impact level

The notifications made by the entities within the scope of the application of the aforementioned Technical Security Instruction to the National Cryptologic Centre (CCN) shall be made in the terms indicated in the articles 36 and 37 of the Royal Decree 3/2010, of 8 January.

To this end, security incidents that have a significant impact on the security of the information handled or the services provided in relation to the category of the system, determined in accordance with the provisions of the articles 43, 44 and the Annex I of the Royal Decree 3/2010, of 8 January, will be notified.

In any case, it will be mandatory to notify the CCN at the time they occur, the security incidents that by their level of potential impact are qualified with the level of CRITICAL, VERY HIGH or HIGH, through the use of tools developed for the purpose of incident reporting (LUCIA).

A3 ANNEX 3. NOTIFICATION IN THE PRIVATE SECTOR FIELD

Private law entities shall notify the INCIBE-CERT of cyber incidents, as set forth in the article 11 of the Royal Decree-Law 12/2018 of 7 September on the security of networks and information systems, through the channels and tools established by the INCIBE-CERT. The cases will be managed in accordance with the "Procedure for the management of cyber incidents for the private sector and citizens".

Citizens may notify the INCIBE-CERT of cyber incidents, in accordance with the article 11 of the Royal Decree-Law 12/2018, of 7 September, on the security of networks and information systems, in which it is stated that the INCIBE-CERT will also be a reference incident response team for citizens, private law entities and other entities not previously included in section 1 of the same article 11, and may use the channels and tools provided by the INCIBE-CERT. Case management will be carried out in accordance with the "Procedure for the management of cyber incidents for the private sector and citizens".

A4 ANNEX 4. REGULATORY FRAMEWORK

The management of cyber security incidents, and in particular the notification to your competent authority or CSIRT of reference, is a legal imperative for certain public and private organizations in Spain.

The preparation of this "National guide for the notification and management of cyber incidents" has taken as a reference the following regulations at a national level.

OF A GENERAL CHARACTER

- Organic Law 10/1995, of 23 November, of the Criminal Code
- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights.
- Law 9/2014, of 9 May, General of Telecommunications
- Royal Decree-Law 12/2018, of 7 September, on networks and information systems security
- Royal Decree 1720/2007, of 21 December, approving the Regulation and the development of the Organic Law 15/1999, of 13 December, on the protection of personal data
- Ninth additional provision. Management of cyber security incidents affecting the Internet network of the Law 34/2002, of 11 July, on information society services and electronic commerce.

OF PARTICULAR CHARACTER IN THE AREA OF PUBLIC SECTOR

- Law 11/2002, of 6 May, regulating the National Intelligence Centre
- Law 40/2015, of 1 October, on the Legal Regime of the Public Sector
- Royal Decree of 421/2004, of 12 March, regulating the National Cryptological Centre
- Royal Decree 3/2010, of 8 January, regulating the National Security Scheme for public sector entities within its area of application. Modified in the RD 951/2015.
- Technical Instruction on Security Notification of Security Incidents published in the BOE no. 95 of 18 April 2018.

OF PARTICULAR CHARACTER IN THE AREA OF CRITICAL INFRASTRUCTURES

- Law 8/2011, of 28 April, establishing measures for the protection of Critical Infrastructures.
- Royal Decree 704/2011, of 20 May, approving the Regulation for the protection of Critical Infrastructures.
- National Plan for the Protection of Critical Infrastructures (PNPIC) approved by the Instruction No. 1/2016 of the Secretariat of State for Security.
- Resolution of 8 September 2015, of the Secretariat of State for Security, approving the new minimum contents of the Operator Security Plans and the Specific Protection Plans.
- Framework Agreement for Collaboration on Cyber security between the Secretariat of State for Security and the Secretariat of State for Telecommunications and for the Information Society of 21 October 2015.

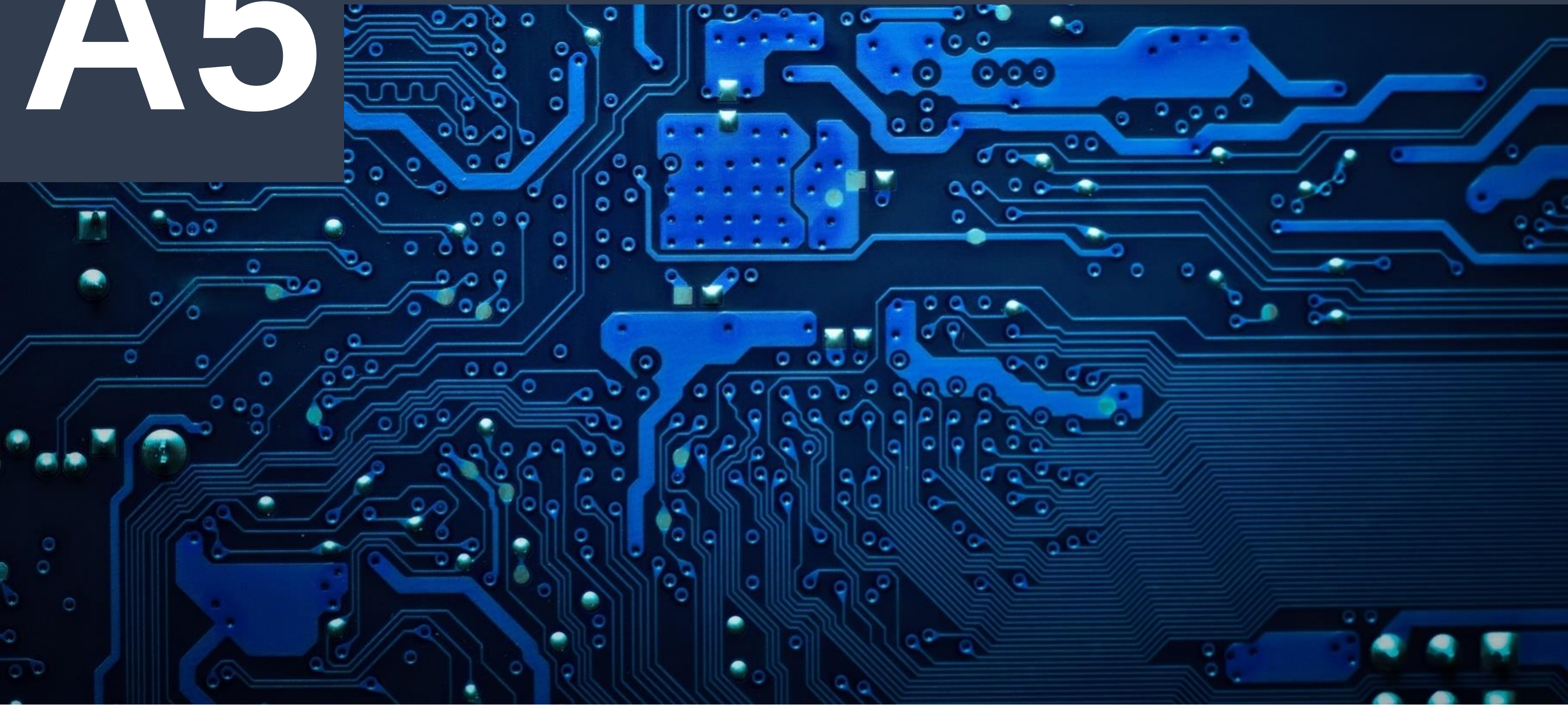
OF PARTICULAR CHARACTER TO MILITARY AND DEFENSE NETWORKS

- Royal Decree 998/2017, of 24 November, which develops the basic organic structure of the MDEF and modifies the Royal Decree 424/2016, of 11 November.

- Ministerial Order 10/2013, of 19 February, creating the Joint Command for Cyber Defence of the Armed Forces

- Order DEF 166/2015, of 21 January, developing the basic organization of the Armed Forces (repealing the Ministerial Order 10/2013)

A5 ANEXO 5. GLOSSARY OF TERMS



ABUSIVE CONTENT

- **Unsolicited bulk email (SPAM):** Unsolicited email that is sent to a large number of users, or a high rate of emails sent to the same user in a short space of time.

- **Harassment:** Refers to virtual or cyber harassment, it is the use of digital media to harass a person, or group of people, through personal attacks, disclosure of private or intimate information, or false.

- **Extortion:** Forcing a person or a company, through the use of violence or intimidation, to perform or omit acts with the intention of causing harm to it, or for profit of the one who causes it.

- **Offensive messages:** Unexpected or desired communications, as well as actions or expressions that injure the dignity of another person, undermining his fame or attempting against his own estimation.

- **Crime:** Any action classified as a crime in accordance with the provisions of the Organic Law 10/1995, of 23 November, of the Criminal Code.

- **Pedophilia:** Any behaviour related to those described in the Title VIII of the Penal Code, relating to the recruitment or use of minors or persons with disabilities in need of special protection in acts that threaten their indemnity or sexual freedom.

- **Racism:** Any criminal offence, including offences against persons or property, where the victim, the premises or the objective of the offence is chosen for its real or perceived connection, sympathy, affiliation, support or belonging to a social group, race, religion or sexual condition.

- **Apology of violence:** Exposure, in the presence of an audience of people or by any means of dissemination, of ideas or doctrines that praise the crime or praise its perpetrator.

HARMFUL CONTENT

- **Malware:** Word derived from the terms *malicious* and *software*. Any piece of software that performs actions such as data mining or other alteration of a system can be categorized as malware. So malware is a term that encompasses several types of malicious programs.

- **Virus:** A type of malware whose main purpose is to modify or alter the behaviour of a computer system without the user's permission or consent. It is disseminated by the execution in the system of software, files or documents with harmful load, acquiring the ability to replicate from one system to another. The most common methods of infection are through removable devices, Internet downloads and email attachments. However, it can also do so through scripts, documents, and XSS vulnerabilities present on the web. It is noteworthy that a virus requires human action to spread unlike other malware, see *Worm*.

- **Worm:** Malicious program whose main characteristic is its high capacity of spreading out. Its purpose is to replicate to new systems to infect them and continue replicating to other computers, taking advantage of all types of media such as email, IRC, FTP, P2P and other specific protocols or widely used.

- **Trojan horse:** A type of malware that is masked as legitimate software in order to convince the victim to install the part on their system. Once installed, the malicious software has the ability to engage in harmful activity in the background. A Trojan horse does not depend on a human action and does not have the ability to replicate, however it can have great damaging capacity on a system in the form of Trojans or exploiting software vulnerabilities.

- **Spyware:** A type of malware that spies on a user's activities without their knowledge or consent. These activities can include keyloggers, monitoring, data collection as well as data theft. Spyware can be spread out as a Trojan horse or through software exploitation.

- **Rootkit:** A set of malicious software that allows privileged access to areas of a machine, while at the same time it is hiding its presence by corrupting the Operating System or other applications. By machine it is meant the whole spectrum of IT systems, from smartphones to ICS. The purpose of a rootkit is to effectively mask payloads and allow their existence in the system.

- **Dialer:** A type of malware that is installed on a machine and, automatically and without the user's consent, it makes calls to a special rate telephone number. These actions entail economic costs for the victim by passing on the amount of the communication.

- **Ransomware:** It includes any malware that infects a machine, so that the user is unable to access the data stored in the system. Normally, the victim subsequently receives some type of communication in which he is coerced to pay a reward that allows access to the system and the blocked files

- **Harmful Bot:** A botnet is the name used to designate a set of remotely controlled machines with a generally malicious purpose. A bot is a piece of malicious software that receives commands from a main attacker who remotely controls the machine. The C&C servers enable the attacker to control the bots and to execute the orders remotely.

- **RAT:** Remote Access Tool, it is a specific function of remote control of an information system, which incorporates certain families or samples of harmful software (malware).

- **C&C:** Command and control, it refers to command and control panels (also referred to as C2), by which cyber attackers control certain zombie computers infected with samples from the same malware family. The Command and Control Panel acts as a point of reference, control and management of the infected computers.

- **Suspicious connection:** Any exchange of information at the local or public network level, whose origin or destination is not fully identified, as well as their legitimacy.

OBTAINING INFORMATION

- **Port Scanning:** Local or remote software analysis of the port status of a machine connected to a network. The purpose of this action is to obtain information regarding the identification of active services and possible vulnerabilities that may exist in the network.

- **Network Scanning:** Local or remote analysis through a software of the state of a network. The purpose of this action is to obtain information regarding the identification of active services and possible vulnerabilities that may exist in the network.

- **Scanning of technologies:** Local or remote analysis through a software, of the technologies present or available in a determined network or a concrete system of information, by means of which the references of the hardware/software present are obtained, as well as its version, and potential vulnerabilities.

- **DNS transfer area (AXFR IXFR):** Transaction of DNS servers used for a database replication between a first server and secondary servers. These transactions can be complete (AXFR) or incremental (IXFR).

- **Packet analysis (Sniffing):** Software analysis of network traffic in order to capture information. Traffic that travels unencrypted can be captured and read by an attacker.

- **Social engineering:** Techniques that seek the disclosure of sensitive information of a target, usually through the use of persuasive methods and with the absence of will or knowledge of the victim.

- **Phishing:** A fraud committed through a telematic way by which the fraudster attempts to obtain confidential information (passwords, bank details, etc.) from legitimate users in a fraudulent way using social engineering methods.

- **Spear Phishing:** A variant of phishing through which the attacker focuses his action on a specific objective.

INTRUSIONS

- **Exploitation:** Any practice by which a cyber attacker violates an information and/or communication system for illicit purposes or for which he or she is not duly authorized.

- **SQL injection:** Type of exploitation, consisting on the introduction of poorly formed SQL strings, or strings that the receiver does not expect or properly control; which cause unexpected results in the target application or program, and by which the attacker produces unexpected effects and for which he is not authorized in the target system.

- **Cross Site Scripting XSS (Direct or Indirect):** Attack that attempts to exploit a vulnerability that is present in web applications, by which an attacker injects badly formed sentences or strings that the recipient does not expect or controls properly.

- **Cross Site Request Forgery (CSFR):** Cross site request falsification. It is a type of harmful exploit of a website in which unauthorized commands are transmitted by a user in whom the website trusts. This vulnerability is also known by other names such as XSRF, hostile link, one-click attack, session override, and automatic attack. Unlike XSS attacks, which exploit a user's trust in a particular site, Cross Site Request Falsification exploits a site's trust in a particular user.

- **Defacement:** A type of attack on websites that implements a change in the visual appearance of the page. This is usually done using techniques such as SQL injections or some kind of existing vulnerability on the page or server.

- **File Inclusion (RFI and LFI):** Vulnerability that allows an attacker to show or run remote files hosted on other servers because of poor programming of the page containing file inclusion functions. Local File Inclusion (LFI) is similar to the Remote File Inclusion vulnerability, except that instead of including remote files only local files can be included, i.e. files on the current server for its execution.

- **Avoidance of control systems:** Process by which a sample of malicious software, or a set of actions orchestrated by a cyber attacker, manages to violate or circumvent the systems or security policies established by a particular information and communication system.

- **Pharming:** Computer attack that exploits vulnerabilities of DNS servers (Domain Name System). When the user tries to access the website, the browser will automatically redirect the user to an IP address where a malicious website is hosted that replaces the real one, and where the attacker will be able to obtain sensitive information from users.

- **Brute force attack:** Process by which an attacker tries to violate a validation system by access credentials, password or similar, through the use of all possible combinations, in order to access information and/or communication systems for which it has no privileges or authorization.

- **Dictionary Attack:** Process by which an attacker tries to violate a validation system by access credentials, password or similar, through the use of a dictionary previously generated with certain combinations of characters, in order to access information and/or communication systems for which it does not have privileges or authorization.

- **Theft of access credentials:** Unauthorized access or theft of access credentials to information and/or communication systems.

DISPONIBILITY

- **DoS (Denial of Service) o Service Denial Attack:** A set of techniques aimed at rendering a server inoperative. This type of attack seeks to overload a server and thus prevent legitimate users can use the services provided by it. The attack consists of saturating the server with service requests, until the server cannot attend to them, causing its collapse.

- **DDoS (Distributed Denial of Service):** Variant of the DoS in which the remission of requests is carried out in a coordinated manner from several points to the same destination. To do this, bots nets are used, generally without the users' knowledge.

- **Sabotage/Terrorism/Vandalism:** Attacks implemented with the aim of provoking the interruption or degradation of the provision of a service, causing relevant damage to the continuity of the service of an institution or relevant reputational damage committed for ideological, political or religious purposes.

- **Unintentional harmful disruption:** Actions that may cause the interruption or degradation of the provision of a service, causing significant damage to the continuity of an institution's service or relevant reputations.

- **SYN or UDP flooding:** Procedures used to carry out a DoS or a DDoS attack consisting of initiating a large number of sessions preventing the server from attending to bid requests.

- **Open-Resolver DNS:** DNS server capable of resolving recursive DNS consultations from any Internet source. This type of server is usually used by malicious users to carry out DDoS attacks.

- **Bad configuration:** Configuration failure in the software that is directly associated with a loss of a service availability.

INFORMATION COMMITMENT

- **Unauthorized access to information or cyber spying:** Process by which an unauthorized user accesses content for which he or she is not authorized.

- **Unauthorized modification of information:** Process by which an unauthorized user agrees to modify content for which he or she is not authorized.

- **Unauthorized deletion of information:** Process by which an unauthorized user agrees to delete content for which he or she is not authorized.

- **Exfiltration of information:** Process by which a user disseminates information in channels or sources in which the sharing of that information is not intended or authorized.

- **Unauthorized access to systems:** Process by which a user accesses without violating any service, system or network, information and/or communication systems for which he is not duly authorized, or does not have tacit or manifest authorization.

- **POODLE Attack / FREAK Attack:** Process by which a server makes use of an unsecured communication protocol, which was not originally intended, in order to be able to filter information.

FRAUD

- **Unauthorized use of resources:** Use of technologies and/or services by users who are not duly authorized by the competent Management or business.

- **Identity theft:** Malicious activity in which an attacker pretends to be someone else in order to commit some kind of fraud or harassment.

- **Intellectual property rights:** Intellectual property is the set of rights that correspond to authors and other owners (artists, producers, broadcasting organizations ...) in respect of the works and benefits resulting from their creation.

- **Other frauds:** Economic deception with the intention of making a profit, and with which someone is harmed.

VULNERABILITIES

- **Vulnerable technology:** Knowledge on the part of the administrators of technologies, services or networks, of vulnerabilities present in these.

- **Precarious security policy:** Deficient security policy of the organization, through which there is the possibility that during a certain period of time, cyber attackers made unauthorized access to information systems, not being able to reliably determine this extreme.

OTHERS

- **Cyber terrorism:** Computer crimes provided for in articles 197 bis and ter and 264 to 264 quarter of the Organic Law 10/1995 of the Criminal Code when such crimes are committed for the purposes provided for in the article 573.1 of the same text. These purposes are:

  - To subvert the constitutional order, or to seriously suppress or destabilize the functioning of political institutions or of the economic or social structures of the State, or to oblige the public powers to carry out an act or to abstain from doing so.

  - To seriously disturb public peace.

  - To seriously destabilize the functioning of an international organization.

  - To provoke a state of terror in the population or in a part of it.

- **Computer damage PIC:** Computer crimes foreseen in art. 264.2 3º and 4º of the Organic Law 10/1995 of the Criminal Code related to the erasure, damage, alteration, suppression or inaccessibility of data, computer programs or electronic documents of a Critical Infrastructure. As well as serious behaviours related to the foregoing terms that affect the provision of an Essential Service.

- **APT (Advanced Persistent Threat) / AVT (Advanced Volatility Threat):** Attacks directed against specific organizations, based on very sophisticated mechanisms of hiding, anonymity and persistence. This threat usually employs social engineering techniques to achieve its objectives along with the use of known or genuine attack procedures.

- **DGA Domains:** Procedure to dynamically generate domains where Command and Control servers will be hosted, a technique used in Botnet networks to make it difficult to stop them.

- **Cryptography:** Technique that consists on encrypting a message, known as clear text, converting it into an encrypted message or cryptogram, which is illegible to anyone who does not know the key by which it has been encrypted.

- **Proxy:** A computer, usually a server, used in communications between two other computers, normally used transparently by the user.

GENERAL

- **Cybersecurity:** Part of security that deals with crimes committed in cyberspace and their prevention.

- **Cyberspace:** Virtual space encompassing all ICT systems, both information systems and industrial control systems. Cyberspace relies on the availability of the Internet as a network of networks, enriched with other data transport networks.

- **Networks and information systems:** This concept means one of the following three points:

    - An electronic communications network within the meaning of Article 2(a) of the Directive 2002/21/CE.

    - Any device or group of interconnected or related devices in which one or more of them perform, by means of a programme, the automatic processing of digital data.

  - Digital data stored, processed, retrieved or transmitted by means of the elements referred to above for the purposes of their operation, use, protection and maintenance

- **Security in networks and information systems:** the ability of networks and information systems to withstand, with a given level of reliability, any action that compromises the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed, or the corresponding services offered by or accessible through such networks and information systems.

- **Essential services operator:** a public or private entity of one of the types listed in Annex II, meeting the criteria set out in the Article 5(2) of the Directive (EU) 2016/1148 of the European Parliament and of the Council.

- **Digital service:** a service within the meaning of Article 1(1)(b) of the Directive (EU) 2015/1535 of the European Parliament and of the Council of one of the types listed in Annex III.

- **Digital service provider:** any legal person providing a digital service.

- **Cyber-incident:** any event that has a real adverse effect on the security of networks and information systems.

- **Management of cyber incidents:** all procedures followed to detect, analyse, limit and respond to an incident.

- **Cyber threat:** Threat to systems and services present in or reachable through cyberspace.

- **Taxonomy:** Classification or arrangement in groups of objects or subjects that share common characteristics.

- **RGPD:** General Data Protection Regulation, regulation EU 2016/679.

- **Open PGP:** Standard based on the PGP program, from the English *Pretty Good Privacy*, whose purpose is to protect the information through the use of public key cryptography, as well as to facilitate the authentication of documents thanks to digital signatures.

- **Webinject:** A free open-source tool designed primarily to automate the testing of web applications and services.

- **Telnet:** Network protocol that allows access to another machine to operate it remotely as if we were sitting in front of it.

- **RDP:** Remote Desktop Protocol. Proprietary protocol developed by Microsoft that allows communication in the execution of an application between a terminal and a Windows server.

- **VNC (Virtual Network Computing):** Free software program based on a client-server structure that allows to remotely observing the actions of the server computer through a client computer.

- **SNMP (Simple Network Management Protocol):** Network protocol used for the exchange of messages for the administration of network devices.

- **Redis:** Database engine in memory, based on storage in hashes tables.

- **ICMP:** Internet message control protocol.

- **Clean backup**: Point of restoration of a system that has the security of not being compromised.

NATIONAL GUIDE FOR THE NOTIFICATION AND MANAGEMENT OF CYBER INCIDENTS

GOBIERNO
DE ESPAÑA