

ICT Security Guide CCN-STIC 817

NATIONAL SECURITY FRAMEWORK CYBER-INCIDENT MANAGEMENT



June 2018

Published by:



©National Cryptologic Centre, 2018

NIPO: 785-18-023-3

Publication date: June 2018

Mr. Carlos Galán, Mr. José Antonio Mañas and Innotec System all helped draw up and modify this document and its appendices.

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 a warning is provided concerning this damage.

LEGAL NOTICE

Without written authorisation from the **National Cryptologic Centre**, it is strictly forbidden, incurring penalties set by law, to partially or totally reproduce this document by any means or procedure, including photocopying and computer processing, or distribute copies of it by means of rental or public lending.

PROLOGUE

The current national and international scenario is dominated by developments in Information and Communication Technologies (ICT) and by risks emerging from their use. The Administration is fully aware of this scenario and it is necessary for this body to develop, acquire, conserve and secure use of ICTs to guarantee that its services run effectively for the citizen's and the country's best interests.

Working from the Centre's knowledge and experience on threats and vulnerabilities in terms of emerging risks, Law 11/2002, dated 6th May, regulating the National Intelligence Centre, entrusts the National Intelligence Centre the functions related to information technology security, according to the Article 4.e), and to the protection of classified information, according to the Article 4.f). It also gives, through the Article 9.2.f), its Secretary of State-Director the responsibility of managing the National Cryptologic Centre.

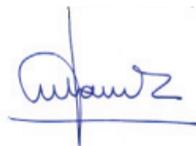
One of the most outstanding functions that it assigns to it, in Royal Decree 421/2004, dated 12th March, regulating the National Cryptologic Centre is to draw up and disseminate standards, instructions, guides and recommendations to guarantee security for the Administration's information and communication technologies.

Royal Decree 3/2010, dated 8th January, develops the National Security Framework (hereinafter called ENS) in the field of Electronic Administration which is also referred in the second section of Article 156 of Law 40/2015, dated 1st October, of the Public Sector Legal System. The National Security Framework establishes the security policy, in matters of use of electronic means, which ensures the protection of information.

Indeed, Royal Decree 3/2010, dated 8th January, updated by Royal Decree 951/2015, dated 23rd October, sets the basic principles and minimum requirements as well as any protection measures to be introduced in Administration systems. In article 29, it authorises the CCN to develop CIS guidelines to ease the fulfilment of these minimum requirements.

The CCN-STIC documents series was drawn up to comply with this function and the ENS, aware of the importance of establishing a frame of reference on this matter that can be used as support so that Administration staff can carry out their difficult and occasionally thankless task of providing security for ICT systems within their responsibility.

June 2018



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

TABLE OF CONTENTS

1. INTRODUCTION.....	5
2. AIM 6	
3. SCOPE	6
4. CYBER-INCIDENT MANAGEMENT DIAGRAM	7
5. CYBER-INCIDENT RESPONSE CAPABILITY	8
5.1 EVENTS AND CYBER-INCIDENTS	8
5.2 CYBER-INCIDENT RESPONSE	8
5.3 INFORMATION SECURITY POLICY AND CYBER-INCIDENT MANAGEMENT	9
6. CYBER-INCIDENT MANAGEMENT	10
6.2 CYBER-INCIDENT CLASSIFICATION	11
6.3 CYBER-INCIDENT DETECTION	14
6.4 CYBER-INCIDENT DANGER.....	15
6.4.1 CYBER-INCIDENT DOCUMENTATION.....	18
6.4.2 LEVEL OF IMPACT OF THE CYBER-INCIDENT ON THE ORGANISATION	18
6.5 MONITORING BY CCN-CERT	19
6.6 CLASSIFICATION OF CYBER-INCIDENT CAUSES AND FACTS	21
6.7 METRICS AND INDICATORS	22
6.8 COLLECTING AND SAFEKEEPING EVIDENCE	22
6.9 INFORMATION EXCHANGE AND NOTIFICATION OF CYBER-INCIDENTS	23
7. APPENDIX A. METRICS AND INDICATORS	25
7.1 IMPLANTATION METRICS.....	25
7.2 EFFICACY METRICS	25
7.3 EFFICIENCY METRICS.....	26
7.4 KEY RISK INDICATORS (KRIS)	27
8. APPENDIX B. ELEMENTS FOR THE CYBER-INCIDENT CLOSURE REPORT	29
9. APPENDIX C. INTRODUCTION TO THE LUCIA TOOL	30
9.1 AIMS	30
9.2 FEATURES	30
9.3 ARCHITECTURE	31
9.4 INTERCONNECTION: CONNECTORS	32
10. APPENDIX D. GLOSSARY	33
11. APPENDIX E. REFERENCES.....	42

1. INTRODUCTION

1. The National Cryptologic Centre (CCN) is developing and publishing this document in response to the order compiled in article 36 of Royal Decree 3/2010, dated 8 January, regulating the National Security Framework (ENS) in the field of Electronic Administration that states; *"The National Cryptologic Centre (CCN) will articulate its response to security incidents around the structure known as CCN-CERT (National Cryptologic Centre-Computer Emergency Response Team), that will act without affecting each public administration's capabilities to respond to security incidents and the CCN's national and international coordination role"* and RD 951/2015, dated 23 October, modifying RD 3/2010.
2. In accordance with article 37 of RD 3/2010, the CCN's missions include:
 - Support and coordination for processing **vulnerabilities and resolving security incidents** by the General State Administration, Regional Administrations, entities within Local Administration and Public Law Entities with their own legal form linked or dependent on any of the aforementioned administrations.
 - Research and dissemination of **best practices on information security** among all members of Public Administrations. For this purpose, the **document series by CCN-STIC (National Cryptologic Centre - Information and Communication Technology Security)**, drawn up by the National Cryptologic Centre, will offer **standards, instructions, guides and recommendations** to apply the National Security Framework and to guarantee security for information technology systems in the Administration.
 - **Training** intended for Administration staff specialising in the field of cyber-security, in order to make it easier to update Administration staff knowledge, raise awareness and improve skills for detecting and managing incidents.
 - Information on **vulnerabilities, alerts and warnings** concerning new threats to information systems, compiled from different sources with recognised prestige, including its own.
3. In turn, the **National Cyber-Security Strategy** gives the CCN-CERT a central role in developing its **Line of Action 2: Security for Information and Telecommunication Systems supported by Public Administrations**, as an essential figure in guaranteeing full implementation of the ENS, by means of reinforcing **CCN-CERT intelligence, detection, analysis and response skills and its Detection and Early Warning Systems**.
4. As part of these functions, missions and responsibilities, and as expressed in article 29 of the ENS, it gives the CCN the responsibility of drawing up and disseminating the corresponding **security guides** for information and communication technologies in order to best comply with the ENS, for which this

CCN-STIC-817 Guide on Cyber-Incident Management in the ENS¹ has been developed and published.

2. AIM

5. The aim of this Guide is to help public entities from the ENS field of application establish **cyber-incident response capabilities** and process them effectively and efficiently, particularly intended for:
 - Cyber-Incident Response Teams inside organisations,
 - CSIRTs (Computer Security Incident Response Team),
 - Network and Systems Administrators,
 - Security Staff,
 - Technical support staff,
 - IT Security Managers (CISO Chief Information Security Officer) and Delegate Managers,
 - Information System Managers (CIO Chief Information Officer) and in general,
 - Cyber-security programme administrators.
6. Specifically, this Guide will provide Security Managers from these public entities with:
 - An approach to classifying cyber-incidents.
 - Recommendations to determine the danger of cyber-incidents.
 - A methodology for notifying the CCN-CERT, focussing on the point in time and type of cyber-incident.

Important note: The content of this Guide is aligned with the LUCIA tool, developed by the CCN-CERT, to Handle Cyber-Incidents in organisations within the National Security Framework field of application, as mentioned in detail in Appendix C of this document.

Using the LUCIA tool, the organisation can handle three types of cyber-incident:

- Incidents originating from the SARA Network Early Warning System (SAT-SARA)
- Incidents originating from the Internet Early Warning System (SAT-INET)
- Any other type of general cyber-incident

3. SCOPE

7. Article 11 of the ENS mentions the obligation for public entities in its field of application to have an **Information Security Policy** that articulates a series of **Minimum Security Requirements**. For the purposes of this document, these

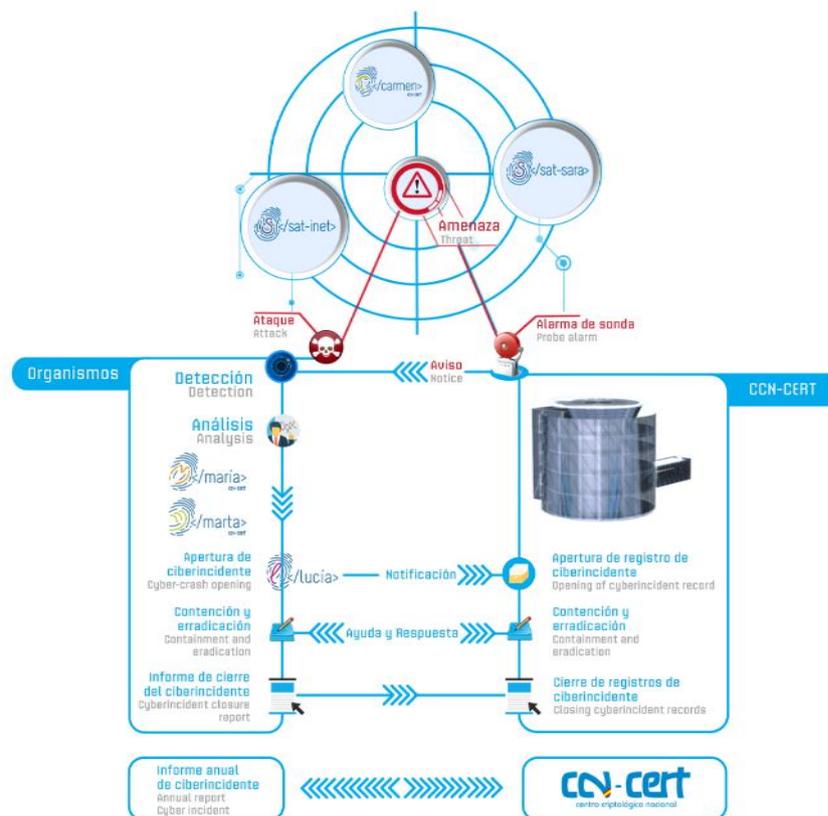
¹ Please consult the CCN-STIC-403 Guide on Security Incident Management for a more general description of Security Incidents and how to Manage them.

requirements include **Security Incident Management**, a requirement that is specified in article 24 of this legal body, stating that:

- A system to detect and react to malware will be set up.
 - Any security incidents will be registered plus any actions taken to process them. These records will be used to continuously improve system security.
8. Following the terminology used in the National Cyber-Security Strategy, the term **cyber- incident** will be used throughout this document as a synonym for a **security incident** in the field of Information and Communication Systems.

4. CYBER-INCIDENT MANAGEMENT DIAGRAM

9. The following picture shows a basic outline for how to deal with a cyber-incident.
10. Notice that once a threat has penetrated the organisation, DETECTION can be performed by the actual organisation and/or by probes used by CCN-CERT that will generate the corresponding warning.
11. In both situations, in the event of the cyber-incident being confirmed, the organisation will begin Formal Notification to CCN-CERT in parallel (using the LUCIA tool) plus actions from the CONTAINMENT phase that will include actions shown in the picture.
12. Once the threat has been ERADICATED, using the same tool, the organisation will notify CCN-CERT that the cyber-incident has been closed.



5. CYBER-INCIDENT RESPONSE CAPABILITY

5.1 EVENTS AND CYBER-INCIDENTS

13. Attacks against Information Systems are increasingly not only more numerous and diverse, but also more dangerous or potentially harmful. Although preventive actions and measures, adopted, based on results obtained from mandatory risk analyses that all public systems must undergo, doubtlessly help reduce the number of cyber-incidents, reality shows us that, unfortunately, not all cyber-incidents can be prevented.
14. Therefore, it has become necessary to have the appropriate **cyber-incident response capability** that, by detecting attacks and threats quickly, can minimise the loss or destruction of technological assets or information, mitigate harmful exploitation of weaknesses in infrastructures and manage to recover services as quickly as possible. This Guide offers guidelines on how to handle cyber-incidents and determine the most appropriate response to each type, independently of the underlying technology platform, hardware, operating systems or applications.
15. Given that it is complicated to manage cyber-incidents appropriately as this involves adopting methods to compile and analyse data and events, monitoring methodologies, procedures for classifying their danger and priority, as well as determining communication channels with other units or entities, inside or outside the organisation, achieving effective cyber-incident response capabilities requires **scrupulous planning** and corresponding **allocation** of appropriate and sufficient **resources**.
16. For the purposes of using common vocabulary, Appendix D of this Guide includes a Glossary featuring the terminology used in the text.

5.2 CYBER-INCIDENT RESPONSE

17. For public organisations, the most significant benefit of the right cyber-incident response capability is systematic management (following consistent and consolidated methodology), making it easy to adopt the right measures. Consequently, correct Cyber-Incident Response Capability helps security teams minimise the loss or exfiltration of information or service shut-off. Another benefit is the possibility of using information obtained during cyber-incident management to improve how we respond to security incidents in the future and, consequently, provide greater and better protection for systems.
18. In addition to claiming to provide better Electronic Administration services, the bodies and organisations from the ENS field of application should match their cyber-incident response capability to the legal standard that is applied in each case and for each regional or sector-based Administration involved. Among these regulations, due observance should be highlighted for the National Cyber-Security Strategy, Law 15/1999, dated 13 December, on Personal Data Protection

(and its subsequent standards), Law 11/2007, dated 22 June, on Citizen Access to Public Services, the National Interoperability Framework (and its derived standards), and the National Security Framework (and its derived standards), Law 9/1968, dated 5 April, on Official Secrets, among others.

5.3 INFORMATION SECURITY POLICY AND CYBER-INCIDENT MANAGEMENT

19. Security Policy

Article 11 of the ENS mentions minimum requirements that any Security Policy should consider including **Security Incidents**, necessarily specifying:

- The position of the Cyber-Incident Response Team (CIRT), its competences and authority, within the organisation structure and definition of roles and responsibilities for each unit.
- Departmental and personal responsibilities.

20. Security standard

- Definition of cyber-incidents considered according to the risk analysis and the terms of reference used.
- Criteria for informing about cyber-incidents and, when appropriate, information exchange, internally and externally.
- Cyber-incident danger level.

21. Operation security procedures

- Mechanisms to notify Cyber-Incident Reports.
- Notification, communication and information exchange forms.

22. Parts of the Cyber-Incident Response Plan

Organisations within the ENS field of application should have a **Cyber-Incident Response Plan** that responds appropriately to its specific requirements, including the organisation's mission, size, structure and functions. The Plan should also determine and ensure that it has the right human and material resources and should have essential Management support.

Once the organisation has drafted (and Management has approved) the Cyber-Incident Response Plan, it will be introduced. The Plan should be reviewed at least once a year to ensure that the organisation is following the Road Map for continuous improvement properly.

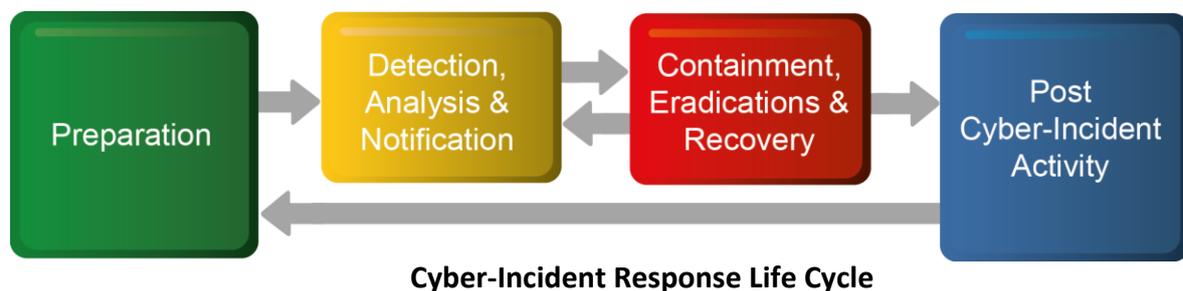
23. Cyber-Incident Response Procedures

Each organisation in the ENS field of application should draft and approve the **Cyber-Incident Response Procedures** that should be based on the Information Security Policy and the aforementioned Cyber-Incident Response Plan. They will

include developing technical aspects, control lists and specific forms, used by the Cyber-Incident Response Team (CIRT).

6. CYBER-INCIDENT MANAGEMENT

24. Cyber incident management involves several phases.
25. The initial phase contemplates setting up and training a **Cyber-Incident Response Team (CIRT)** and use of the necessary tools and resources.² During this **PREPARATION** phase, following Appendices I and II of the ENS, and after the corresponding risk analysis, the public organisation will have identified and laid out a determined set of security measures. However, it is well known that even after introducing such measures, a residual risk will remain that should be assumed by the organisation's Executive Management.
26. Appropriate introduction of the aforementioned measures will help detect and analyse any possible security gaps in the organisation's Information Systems, in the **DETECTION, ANALYSIS AND NOTIFICATION** phase, leading to possible notification processes.
27. In the cyber-incident **CONTAINMENT, ERADICATION AND RECOVERY** phases, the organisation (aware of the danger level) should firstly attempt to mitigate its impact, and then eliminate it from the affected systems and finally aim to recover the system to normal operation. During this phase, it will be necessary to continue analysing the threat in cycles and these results will gradually lead to new containment and eradication mechanisms.
28. After the incident, in the **POST CYBER-INCIDENT ACTIVITY** phase, the organisation's managers will issue a Cyber-Incident Report providing details on its original cause and its cost (particularly in terms of compromised information or impact on service provision) and the measures that the organisation should take to prevent similar cyber-incidents in the future.



(Preparation - Detection Analysis and Notification - Containment, Eradication and Recovery - Post Cyber-Incident Activity)

² For example, by joining the CCN-CERT Early Warning System (SAT) services both in the SARA (Application and Network Systems for Administrations) network (SAT-SARA) and on the internet (SAT-INET).

29. The *CCN-STIC-403 Guide Security Incident Management* develops these phases in detail.

6.2 CYBER-INCIDENT CLASSIFICATION

30. Given that not all the cyber-incidents have the same characteristics or the same danger level, it is necessary to classify cyber-incidents which will subsequently help to analyse, contain and eradicate them.
31. Factors that we can consider for classification criteria include:
- **Type of threat:** malware, intrusions, fraud, etc.
 - **Origin of the Threat:** Internal or external.
 - The security **category**³ of the affected systems.
 - The **profile of affected users**, their position in the entity's organisation structure and consequently their access privileges to sensitive or confidential information.
 - The **number and type of systems affected**.
 - The impact that the incident might have on the organisation, from the point of view of information protection, service provision, legal compliance and/or public image.
 - The **legal and regulatory requirements**.
32. The combination of one or several of these factors is determining when taking the decision to create a cyber-incident or determine its danger level and action priority.
33. The following table shows a **classification of cyber-incidents**, looking at the attack vector used. (See Glossary in Appendix D).

³ Looking at the criteria mentioned in Appendix I of the ENS, to categorize Information Systems.

CYBER-INCIDENT CLASSIFICATION		
Cyber-Incident Category	Description	Type of Cyber-Incident
Malware	Software intended to infiltrate or damage a computer, server or other network device, without its manager or user finding out, for a variety of purposes.	Virus
		Worms
		Trojans
		Spyware
		Rootkit
		Ransomware (computer hijack)
		Remote Access Tools (RAT)
Availability	Attacks intended to put systems out of service, to cause damage to productivity and/or the image of the institutions being attacked.	[Distributed] Denial of Service DoS / DDoS
		Failure (Hardware/Software)
		Human error
		Sabotage
Information Gathering	Attacks intended to collect fundamental information in order to launch more sophisticated attacks, through social engineering or identification of vulnerabilities.	Identification of assets and vulnerabilities (scanning)
		Sniffing
		Social Engineering
		Phishing
Intrusions	Attacks intended to exploit design, operation or configuration vulnerabilities in different technologies, in order to enter an organisation's systems fraudulently.	Compromising user accounts
		Defacement
		Cross-Site Scripting (XSS)
		Cross-Site Request Forgery (CSRF)
		SQL injection

		Spear Phishing
		Pharming
		Brute Force attack
		Remote File Injection
		Exploitation of software vulnerability
		Exploitation of hardware vulnerability
		Unauthorized access to a network
Information compromise	Incidents related to access and leaks (confidentiality), modification or erasing (integrity) of unpublished information.	Unauthorised access to information
		Unauthorised modification and erasing of information.
		Unauthorised publication of information
		Exfiltration of information
Fraud	Incidents related to fraudulent actions derived from identity theft, in all its variants.	Identity Theft / Spoofing
		Use of unauthorised resources
		Illegitimate use of credentials
		Infringements of intellectual or industrial property rights.
Abusive content	Attacks intended to damage the organisation's image or use its electronic resources for illicit uses (such as advertising, extortion or general cyber-crime).	Spam
		Bullying/extortion/offensive messages
		Paedophilia/racism/justification of violence/crime, etc.
Security policy	Incidents related to users infringing security policies approved by the organisation.	Abuse of privileges by users
		Access to unauthorised services.
		Non updated system
		Others
Others	Other incidents not included in the previous sections.	

Table 1.- Cyber-Incident Classification

6.3 CYBER-INCIDENT DETECTION

34. In any case, it is not easy to determine exactly whether a cyber-incident has occurred or not and if so, identify its type and assess its theoretical danger level. This difficulty lies in three essential factors:
- Cyber-incidents can be detected using different tools with different levels of detail and loyalty: **automated systems** for detection (including using network or server IDS/IPS,⁴ antivirus software and log analysers, among others) or **manual resources** (such as actual users reporting problems). In addition, some cyber-incidents appear with very clear signs of anomalies whilst others, on the contrary, are very difficult to detect.⁵
 - There is normally a considerable volume of signs of potential cyber-incident. For example, it is not unusual for an organisation to have to process thousands or even millions of daily warnings from intrusion sensors.
 - In-depth specialised technical knowledge and extensive experience are required to endorse an appropriate, efficient analysis of data related to the cyber-incidents.
35. Basically, signs that might point to a cyber-incident can come from two types of sources: *precursors* and *indicators*. A **precursor** is a sign that an incident *might happen* in the future. An **indicator** is a sign that an incident *might have happened or might be happening now*.
36. The majority of attacks do not have precursors that can be identified or detected from the TARGET's perspective. If an organisation detected the presence of precursors, it might have a chance of preventing the cyber-incident from taking place, adapting its security measures appropriately. Some examples of precursors are:
- Web server log inputs with vulnerability scanner results.
 - Announcement of a new exploit, aimed at attacking a possible vulnerability in the organisation's systems.
 - Explicit threats from specific groups or entities, announcing attacks on target organisations.⁶
37. Whilst precursors are relatively scarce, indicators are very common such as: a network intrusion sensor, sending out an alarm when there has been an attempt to bypass the buffer for a database server; alarms generated by antivirus software; the presence of a file name with unusual characters; a log record regarding a change that was not envisaged in a host's configuration; application logs reporting repeated failed login attempts from an unknown external system;

⁴ Intrusion Detection Systems and Intrusion Prevention Systems.

⁵ As in the case of the attacks on specific organizations, based on very sophisticated concealment, anonymity and persistence mechanisms: what are known as APTs (Advanced Persistent Threats)

⁶ This is the case of hacktivist groups broadcasting attacks for example.

detection of a significant number of bounced emails with suspicious content; unusual deviation of traffic from the internal network, etc.

38. Even if an indicator is accurate, this does not necessarily mean that there has been a cyber-incident. Some indicators - such as a server crashing or critical files being changed - might take place for different reasons, far from a cyber-attack, including human error. However, when an indicator shows signs of activity, it is reasonable to suspect that an incident could be taking place, and action should be taken. Determining whether a particular event is actually a cyber-incident is occasionally a matter of appreciation and judgement, as it is necessary to exchange information on the supposed cyber-incident with different members of the CSIRT and, when appropriate, from another unit (internal or external) to be able to make a reasonably appropriate decision.⁷
39. Although some cyber-incidents are easy to detect (for example, website defacement), many of them do not show clear symptoms. Occasionally, small signs (such as alterations to a system configuration file, for example) might be the only indicators that a cyber-incident is taking place.
40. CCN-CERT management and coordination of incidents for organisations in the Spanish public sector, using the **SARA Network Early Warning System (SAT-SARA)**⁸ and the **Internet Early Warning System (SAT-INET)**⁹ provides an appropriate response to these needs.

6.4 CYBER-INCIDENT DANGER

41. In addition to classifying cyber-incidents within a certain group or type, managing them (assigning priorities and resources, etc.) requires determining the potential danger¹⁰ posed by the cyber-incident. To do this, certain **Danger Determination Criteria** must be set to compare against the evidence available on the cyber-incident in its initial stages.
42. For the purpose of this Guide, the danger of a given cyber-incident will be assigned on a scale of five values. This scale, from least to most dangerous, is shown below.

DANGER	LEVEL
1	LOW

⁷ For these purposes, the CCN-CERT has been providing support and help to Spanish Public Administration organizations to determine authenticity and certainty of cyber-incidents.

⁸ Service run by CCN-CERT working with the Ministry of Finance and Public Administrations (organization in charge of the SARA network, System of Applications and Networks for Administrations). It aims to detect attacks and threats in real time by analyzing network traffic in the Public Administration Organization networks connected to the SARA network.

⁹ Service developed and introduced by CCN-CERT for real time detection of existing threats and incidents in the traffic flowing between the member organization's internal network and the Internet.

¹⁰ *Danger or riskiness*: attended with risk or danger. (Merriam Webster dictionary). Other texts might use the term 'critical level'.

2	MEDIUM
3	HIGH
4	VERY HIGH
5	CRITICAL

Table 2.- Danger Levels

This Danger Level will be used by the CCN-CERT when communicating with the affected entities, members of SARA (SAT-SARA) or Internet (SAT-INET) Early Warning Systems.

43. The chart below shows the **Cyber-Incident Danger Level**, focussing on the threat's potential repercussion on the information systems for entities within the ENS field of application.

CRITERIA FOR DETERMINING CYBER-INCIDENT DANGER LEVELS ¹¹			
LEVEL	MOST USUAL UNDERLYING THREAT(S)	ATTACK METHOD	POTENTIAL FEATURES OF THE CYBER-INCIDENT
CRITICAL	Cyber-espionage	<ul style="list-style-type: none"> - APTs, malware campaigns, service downtime, compromised industrial control systems, special incidents, etc. 	<ul style="list-style-type: none"> - Capacity to exfiltrate very valuable information, in considerable quantity over a short time. - Capacity to take control of sensitive systems, in quantity over a short time.
VERY HIGH	Shutting off IT services /Data exfiltration / Compromised services	<ul style="list-style-type: none"> - Confirmed high impact malware (RAT, Trojans sending data, rootkit, etc.) - Successful external attacks. 	<ul style="list-style-type: none"> - Capacity to exfiltrate valuable information, in an appreciable quantity. - Capacity to take control of sensitive systems, in considerable quantity.
HIGH	Taking control of systems / Theft and publication or sale of stolen information / Cyber-crime / Identity theft	<ul style="list-style-type: none"> - Medium impact malware (virus, worms, Trojans) - External attacks - compromising non-essential services (DoS / DDoS). - DNS traffic with domains related to APTs or malware campaigns. - Unauthorised access / Identity theft / Sabotage - Cross-Site Scripting / SQL injection. - Spear phishing / pharming 	<ul style="list-style-type: none"> - Capacity to exfiltrate valuable information. - Capacity to take over certain systems.
MEDIUM	Achieve or significant increase offensive capacities / Website defacement / Manipulating information	<ul style="list-style-type: none"> - Downloading suspicious files. - Contacts with suspicious domains or IP addresses. - Vulnerability scanners, - Low Impact malware (adware, spyware, etc.) - Sniffing / Social engineering. 	<ul style="list-style-type: none"> - Capacity to exfiltrate an appreciable volume of information. - Capacity to take control of a system.
LOW	Attacks on image or reputation / Ridicule / Errors and faults	<ul style="list-style-type: none"> - Policies - Spam with no attachments - Out of date software - Bullying / Coercion / offensive comments - Human error / HW-SW fault 	<ul style="list-style-type: none"> - Scarce capacity to exfiltrate an appreciable volume of information. - No or little capacity to take control of systems.

¹¹ Regarding entities in the ENS field of application.

6.4.1 CYBER-INCIDENT DOCUMENTATION

44. The LUCIA tool, available to organisations in the ENS field of application, and as explained in Appendix C of this Guide, uses a ticket monitoring system that documents how a cyber-incident develops and actions that have been carried out at all times corresponding to the detection, containment, eradication and recovery phases.

6.4.2 LEVEL OF IMPACT OF THE CYBER-INCIDENT ON THE ORGANISATION

45. The ENS highlights that the impact of a cyber-incident on a public organisation is determined by assessing this cyber-incident's consequences on how the organisation operates, on its assets and on affected individuals.
46. Consequently, cyber-Incident Management should be prioritised based on different criteria including:
- Functional Impact of the Cyber-Incident: the Cyber-Incident Response Team (CIRT) should consider how the cyber-incident might affect system operation.
 - The Impact of the Cyber-Incident on Information or Services: given that cyber-incidents can affect confidentiality and integrity concerning information processed by the organisation and/or the availability of services, the CIRT should consider how the cyber-incident might affect the organisation's skills-based developments or its public image.
 - Recovery from the cyber-incident: given that the type of cyber-incident and the surface area of assets being attacked will determine the time and resources that should be put into the recovery, the CIRT, with relevant help from other departments in the organisation, should consider the effort required to return to the situation prior to the cyber-incident and its opportunity.

These criteria can change if the cyber-incident's circumstances or knowledge of it changes during the management process.

47. The following chart shows how the organisation should determine **the Potential Impact**¹² of Cyber-incidents in the organisation.

Level	Description
I0 – IRRELEVANT	<ul style="list-style-type: none"> - There is no appreciable impact on the system. - There is no appreciable damage to reputation.

¹² Potential impact is defined as an estimation of the damage that a security incident might cause.

I1 – LOW	<ul style="list-style-type: none"> - The highest category of affected information systems is BASIC. - The cyber-incident must be resolved in less than 1 DP¹³ - One-off reputation damage, no repercussions in the media.
I2 – MEDIUM	<ul style="list-style-type: none"> - The highest category of affected information systems is MEDIUM. - This affects more than 10 machines with information whose maximum category is BASIC. - The cyber-incident must be resolved in between 1 and 10 DP - Appreciable damage to reputation, with media repercussions (wide press coverage)
I3 – HIGH	<ul style="list-style-type: none"> - The highest category of affected information systems is HIGH. - This affects more than 50 machines with information whose maximum category is BASIC. - This affects more than 10 machines with information whose maximum category is MEDIUM. - The cyber-incident must be resolved in between 10 and 20 DP - Damage to reputation that is difficult to repair, with media repercussions (widespread press coverage) affecting the reputation of third parties
I4 - VERY HIGH	<ul style="list-style-type: none"> - Affects systems classified as RESERVED - This affects more than 100 machines with information whose maximum category is BASIC. - This affects more than 50 machines with information whose maximum category is MEDIUM. - This affects more than 10 machines with information whose maximum category is HIGH. - The cyber-incident must be resolved in between 20 and 50 DP - Reputation damage to the country's image (Spain brand) - Appreciably affects official activities or missions abroad - Appreciably affects a critical infrastructure
I5 - CRITICAL	<ul style="list-style-type: none"> - Affects systems classified as SECRET - This affects more than 100 machines with information whose maximum category is MEDIUM. - This affects more than 50 machines with information whose maximum category is HIGH. - This affects more than 10 machines with information whose maximum category is RESERVED. - The cyber-incident requires more than 50 DP to be resolved - Appreciably affects national security - Seriously affects a critical infrastructure

Table 4.- Criteria for Determining the Level of Impact

6.5 MONITORING BY CCN-CERT

48. Once the affected organisation has been notified about the incident by the CCN-CERT SARA Network Early Warning System (SAT-SARA) or the Internet System (SAT-INET), it will be monitored, assigning it a certain Status.
49. The following table shows the different statuses that a cyber-incident might have at any given time.

¹³ DP - Day-person; estimation of the effort required to carry out a task whose unit is equivalent to an uninterrupted work day for an average worker.

Status	Description
Closed no activity	There is no answer from the organisation.
Request more information	The affected organisation requires more information from the CCN-CERT to close the incident correctly.
Closed (cyber incident took place)	Detection was positive and it has affected the organisation's systems.
Close (No impact)	Detection was positive but the organism is not vulnerable or not affected.
Closed (False positive)	Detection was mistaken.
Closed (No reply)	After a period of 60 days, if the cyber incident has not been closed by the organisation, it is closed by the corresponding Early Warning System, with this status.
Open	Usually this status appears when the ticket is not properly managed by the affected organisation. Cyber incidents with this status are moved into the right status (usually "closed no activity").

Table 5.- Statuses of cyber incidents notified by the CCN-CERT Early Warning System

50. This monitoring will depend on the danger level of the cyber-incident, based on the following table:

Danger Level	Obligation to notify the incident to CCN-CERT(*)	Cyber incident closure (calendar days)	Comments
LOW	No	15	- Automatically closed by Early Warning Systems after 60 days with the status "Closed - No reply".
MEDIUM	No	30	
HIGH	Yes	45	- The Early Warning System does not notify the affected organisation with a fresh warning.
VERY HIGH	Yes	90	- Should never be assigned the status "Closed – No reply". - The Early Warning System notifies the affected organisation with a fresh warning every seven days until it receives a reply.
CRITICAL	Yes	120	

Table 6.- Type of monitoring to be done by the CCN-CERT, according to Danger Level

6.6 CLASSIFICATION OF CYBER-INCIDENT CAUSES AND FACTS

51. Faced with the avalanche of data, it is advisable to have a few indicators that are sufficiently representative of the system's security to obtain metrics that can back up decision making, particularly on two aspects: meeting standards and running projects.
52. So, as compiled in the CCN-STIC-815 guide.¹⁴ it will be necessary to compile the following information for subsequent processing:

Relating to the time of the cyber-incident:

- Date and Time the cyber-incident was detected.
- Date and Time of notification,
- Date and time of resolution and closure.
- Impact or consequences.

Annually, the organisation will send the CCN-CERT a summary with the essential data concerning all cyber-incidents that took place in the considered period. Appendix B of this Guide contains a list of the most relevant information that should be included in this Annual Report.

In relation to the assets involved:

- Downgrading of the affected asset: high, medium or low.
- Affected security aspect: Confidentiality, Availability and Integrity (if traceability and authenticity dimensions are affected, it will be considered as a case where information integrity is affected).

Cause of the Cyber-incident:

Causes (root) of the cyber-incident (mark as necessary)		Appendix II of the ENS ¹⁵
Code	Description	
C.1	non-compliance or lack of security standard	org.1 org.2
C.2	non-compliance or lack of security procedures	org.3
C.3	non-compliance of the authorisation process	org.4
C.4	technical or operative fault in identification or authentication	op.acc.1 op.acc.5
C.5	technical or operative fault in access checks	op.acc.2 op.acc.4
C.6	unauthorised local access	op.acc.6
C.7	unauthorised remote access	op.acc.7

¹⁴ CCN-STIC-815 Metrics and Indicators in the ENS.

¹⁵ List used in the ENS compiling the three groups encompassing the security measures: organizational framework [org], operational framework [op] and protective measures [mp].

C.8	absent or deficient function and task segregation	op.acc.3
C.9	incorrect data entry not spotted in time	
C.10	inappropriate configuration	op.exp.2 op.exp.3
C.11	absent or deficient maintenance	op.exp.4
C.12	change made inappropriately	op.exp.5
C.13	lack of staff awareness	mp.per.3
C.14	staff training defects	mp.per.4
C.15	work stations not cleared	mp.eq.1
C.16	unauthorised surplus information	mp.si.5
C.17	defects in a SW application specification	mp.sw
C.18	defects in a SW application implantation	mp.sw.2
C.19	defective equipment operation entry (SW, HW, COMMS)	mp.sw.2
C.20	external service: caused by supplier negligence	mp.ext.2
C.21	external service: that was not communicated within the agreed lead times and channels	mp.exp.2
C.22	external service: the responsible supplier has not met their agreed obligations.	mp.exp.2

Table 7.- Incidents when resolving the Cyber-incident

6.7 METRICS AND INDICATORS

53. Appendix A of this Guide contains a set of Metrics and Indicators that organisations in the ENS field of application can use to assess **introduction, effectiveness and efficiency** of the cyber-incident Management process.

6.8 COLLECTING AND SAFEKEEPING EVIDENCE

54. Although the main reason for collecting evidence on a cyber-incident is to help resolve it, it might also be necessary to begin legal processes. In such cases, it is important to clearly document how the evidence was obtained and kept, always in compliance with what appears in the legislation in force.¹⁶
55. A detailed record should be kept of all evidence, including:
- Identification of the information (such as the location, series number, model number, host name, MAC address and IP addresses of affected computers).
 - Name, position and telephone number of each person who has collected or managed evidence during the cyber-incident investigation.

¹⁶ On this point, the CIRT would be well advised to discuss the matter of obtaining and safekeeping evidence with the organization's Legal Services, the CCN-CERT or specialized third parties, including, if necessary, Law Enforcement Agencies and Prosecutor's Office for Computer Criminality.

- Date and time of every occasion that each piece of evidence has been processed.
 - Locations where evidence is kept.
56. However, it is no simple task to collect evidence data. In general, it is always advisable to start by collecting evidence as soon as a cyber-incident is detected. On the other hand, from a probatory point of view, it is advisable to immediately obtain a snapshot of the system being attacked, making it inaccessible and guaranteeing its integrity,¹⁷ before processing copies of the system under attack, with different types of tools that might otherwise alter part of the information or the status of the compromised systems.¹⁸
57. Organisations from the ENS field of application should draft and approve standards on evidence safekeeping for a cyber-incident. Some of the most significant factors when determining the standard are shown below:
- Prosecution of a crime: If the attacker can be prosecuted as a consequence of the cyber-incident, it will be necessary to safe keep the proof of the crime properly until all legal action is complete.
 - Data retention: All organisations should have data retention policies stating how long certain types of data should be held, abiding in any case by the legislation in force for each type of information.
 - Cost of safekeeping: Safekeeping physical elements that might contain evidence (for example, hard disks, compromised systems, etc.) come at a cost that should be taken into account.

6.9 INFORMATION EXCHANGE AND NOTIFICATION OF CYBER-INCIDENTS

58. In addition to mandatory notification of cyber-incidents to the CCN-CERT, public organisations occasionally need to communicate with third parties (Law Enforcement Agencies and social media, specifically). All communication with other figures (ISPs, CSIRTs, software vendors, etc.) will take place through the CCN-CERT as part of its role as **Information Exchange Node concerning Cyber-Incidents in Public Administration Information Systems**.

¹⁷ And work, from then on, with system copies.

¹⁸ In order to obtain additional information on safekeeping evidence, please refer to the NIST SP 800-86 Guide, Guide to Forensic Techniques in Incident Response.



Reporting Cyber-Incident Information to Third Parties

59. Independently of the above, the Cyber-Incident Response Team should work with the organisation's Department of Institutional Relations, Legal Services and Top Management to analyse the criteria and procedures for information reporting to third parties before a cyber-incident takes place. If not, the case might arise that confidential information contained in the information on the cyber-incidents might be handed over to unauthorised third parties. In addition to damaging the organisation's image and a serious breach in legal compliance, it might lead to requiring patrimonial liability from the entity for damage caused to third parties.
60. As previously mentioned, coordination and information exchange with the right organisations can strengthen the organisation's capacity to respond effectively to cyber-incidents. For example, if an organisation identifies suspicious behaviour in its network and sends information on the event to the CCN-CERT, it is highly likely that there have been similar behaviour references in other organisations and it will be able to respond appropriately to the suspicious activity.
61. Another incentive to exchange information is the fact that the response capability for certain cyber-incidents might require using tools that are not available for just one organisation, particularly if this is a small or medium sized organisation. In these cases, the organisation in question can make the most of its network to exchange trustworthy information to effectively outsource the cyber-incident analysis to third party resources that do have the right technical capabilities to manage the cyber-incident appropriately.

7. APPENDIX A. METRICS AND INDICATORS

7.1 IMPLANTATION METRICS

M1	Indicator	Scope of the cyber incident management system		
	Aim	Find out if all information systems are signed up to the service		
	Method	<p>It counts how many services are under control. (If the total number of services is known, it will be possible to calculate a percentage).</p> <ul style="list-style-type: none"> • #HIGH category services (ENS Appendix I) • #MEDIUM category services (ENS Appendix I) 		
	Characterisation	Aim	100%	
		Yellow threshold	HIGH: 4/5 (80%) MEDIUM: 2/3 (67%)	
		Red threshold	HIGH: 2/3 (67%) MEDIUM: ½ (50%)	
		Measuring frequency	quarterly	
Reporting frequency		annual		

7.2 EFFICACY METRICS

M2	Indicator	Resolving cyber incidents with HIGH impact level (ENS Appendix I – affecting HIGH category systems)		
	Aim	Be capable of promptly resolving high impact incidents		
	Method	<p>The time is measured that it takes to resolve an incident with a HIGH category system impact: from notification to resolution</p> <ul style="list-style-type: none"> • T(50) time it takes to close 50% of incidents • T(90) time it takes to close 90% of incidents 		
	Characterisation	Aim	T(50) = 0 && T(90) = 0	
		Yellow threshold	T(50) > 5d T(90) > 10d	
		Red threshold	T(50) > 10d T(90) > 20d	
Measuring frequency		annual		
Reporting frequency	annual			

M3	Indicator	Resolving cyber incidents with MEDIUM impact level (ENS Appendix I – affecting MEDIUM category systems)	
	Aim	Be capable of promptly resolving high impact incidents	
	Method	The time is measured that it takes to resolve an incident with a HIGH category system impact: from notification to resolution <ul style="list-style-type: none"> • T(50) time it takes to close 50% of incidents • T(90) time it takes to close 90% of incidents 	
	Characterisation	Aim	T(50) = 0 && T(90) = 0
		Yellow threshold	T(50) > 10d T(90) > 30d
		Red threshold	T(50) > 15d T(90) > 45d
		Measuring frequency	annual
Reporting frequency		annual	

7.3 EFFICIENCY METRICS

M4	Indicator	Resources consumed	
	Aim	Find out if it is necessary to increase the workforce	
	Method	Estimation of number of man-hours spent on resolving security incidents formula: #hours spent on incidents / #hours formally contracted for ICT security	
	Characterisation	Aim	< 20%
		Yellow threshold	20%
		Red threshold	950%
Measuring frequency		quarterly	
Reporting frequency		annual	

7.4 KEY RISK INDICATORS (KRIS)

M5	Indicator	Staff rotation	
	Aim	Stability of the incident management team	
	Method	<p>A = number of persons who leave the incident response team during the counting period</p> <p>T = number of persons who form part of the team during the counting period</p> <p>formula: A / T</p>	
	Characterisation	Aim	0%
		Yellow threshold	20%
		Red threshold	50%
		Measuring frequency	annual
Reporting frequency		annual	

M6	Indicator	Staff maturity	
	Aim	Experience of the incident management team	
	Method	<p>$Q(x)$ = number of months experience in incident management of the x% newest team members</p> <p>e.g. if $Q(25) = 24m$, it indicates that 25% of staff have less than 24 month experience on the issue</p>	
	Characterisation	Aim	$Q(25) > 24m \ \&\& \ Q(50) > 36m$
		Yellow threshold	$Q(25) < 12m \ \ Q(50) < 24m$
		Red threshold	$Q(25) < 6m \ \ Q(50) < 12m$
		Measuring frequency	annual
Reporting frequency		annual	

M7	Indicator	Danger of access to external services	
	Aim	Measure whether going out of the plant is causing the organisation problems	
	Method	<p>We measure NI: the number of incidents with a VERY HIGH or CRITICAL danger level</p> <p>We measure NS: number of sessions on the Internet originating in the organisation</p> <p>formula: NI / NS</p>	
	Characterisation	Aim	0% annual growth
		Yellow threshold	10%
		Red threshold	30%
		Measuring frequency	quarterly
Reporting frequency		annual	

M8	Indicator	Danger of external access to the organisation's services	
	Aim	Measure whether allowing inputs from the outside is causing the organisation problems	
	Method	We measure NI: the number of incidents with a VERY HIGH or CRITICAL danger level We measure NS: number of web or ftp sessions where the organisation is the server formula: NI / NS	
	Characterisation	Aim	0% annual growth
		Yellow threshold	10%
		Red threshold	30%
Measuring frequency		quarterly	
Reporting frequency	annual		

M9	Indicator	Danger of email	
	Aim	Measure whether allowing email from the outside is causing the organisation problems	
	Method	We measure NI: the number of incidents with a VERY HIGH or CRITICAL danger level We measure NE: number of emails received formula: NI / NE	
	Characterisation	Aim	0% annual growth
		Yellow threshold	10%
		Red threshold	30%
Measuring frequency		quarterly	
Reporting frequency	annual		

8. APPENDIX B. ELEMENTS FOR THE CYBER-INCIDENT CLOSURE REPORT¹⁹

- **Cyber-incident danger level (final).**
- **Summary of actions performed for:**
 - Cyber-incident containment,
 - Cyber-incident eradication and
 - Recovery of the affected systems.
- **Cyber-incident impact measured in:**
 - Number of machines affected
 - Evaluation of the impact on the Organisation's public image
 - Affected security dimensions (Confidentiality, Integrity, Availability, Authentication, Traceability, Legality)
 - Percentage downgrade in services offered to citizens
 - Percentage downgrade in the Organisation's internal services
 - Evaluation of the incident cost that can be assigned directly to the incident:
 - in work hours
 - Cost of purchasing equipment or software required to manage the incident
 - Cost of contracting professional services to manage the incident.

¹⁹ For cyber-incidents with as HIGH, VERY HIGH or CRITICAL danger level.

9. APPENDIX C. INTRODUCTION TO THE LUCIA TOOL

LUCIA (Unified List to Coordinate Incidents and Threats) is a **ticket management** tool that allows the organisation in the ENS field of application to manage each of its cyber-incidents, whilst making it possible to integrate all tool instances installed in the different organisations within the instance installed in the CCN-CERT, thereby making it possible to consolidate and synchronise cyber-incidents registered for each organisation in the CCN-CERT Coordination Node.



9.1 AIMS

The LUCIA platform has the following aims:

- Equip organisations from the ENS field of application with a single, distributed platform for processing cyber-incidents, for separate management of security incidents in all member organisations.
- Comply with National Security Framework (ENS) requirements.
- Federate the LUCIA systems being deployed.
- Report context information (metadata) to the CCN-CERT for cyber-incidents identified in the organisations.
- Communicate and synchronise cyber-incidents between the CCN-CERT and its community of organisations, improving procedures with members of the Internet (SAT-INET) and SARA Network (SAT-SARA) Early Warning Systems.
- Make it possible to report on security incidents from external platforms in organisations that used other technology (e.g. Remedy).

9.2 FEATURES

LUCIA is based on implementing the Incident Manager Request Tracker (RT) open system including extending it to Request Tracker for Incident Response (RT-IR) incidents for response teams.

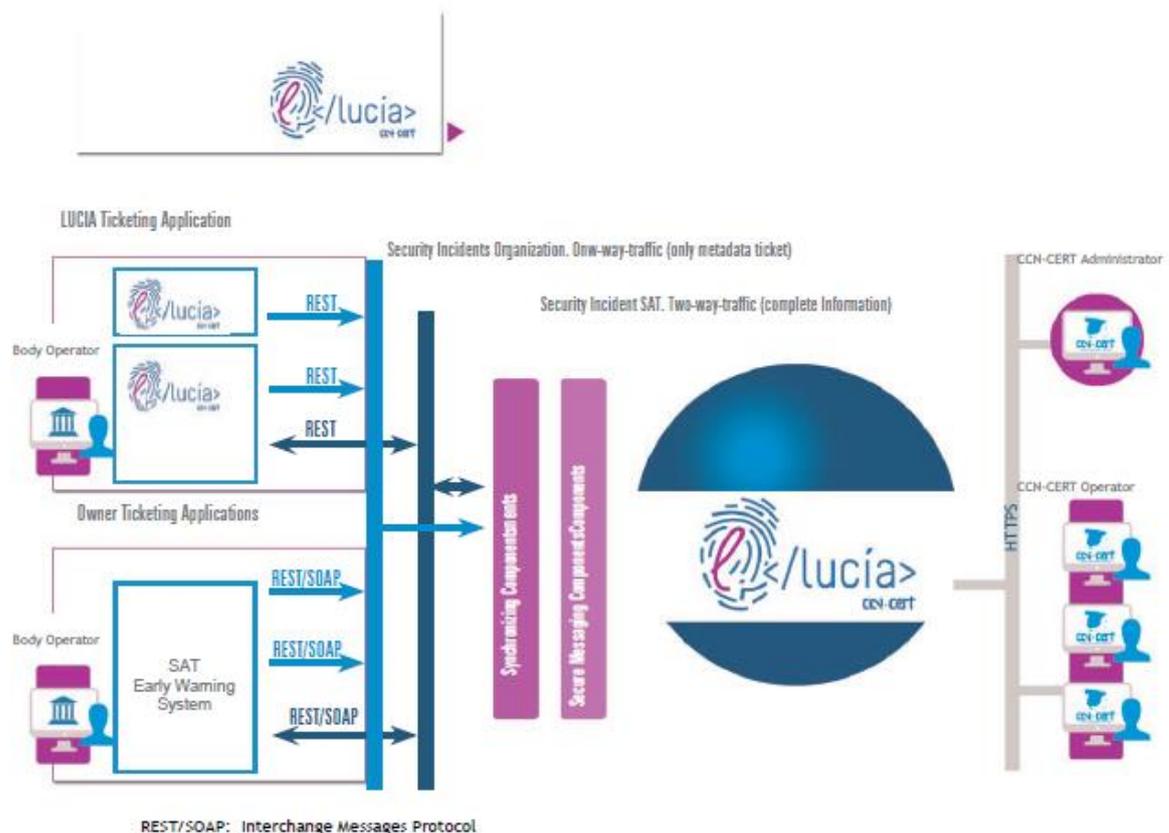
Its main features include:

- Personalised mode, meeting CCN-CERT requirements and procedures plus requirements derived from compliance with the ENS.

- Synchronised and shared information among the different member organisations.
- Based on the use of REST services, allowing greater flexibility and an improvement in RT integration and performance.
- Secure communication, based on a transactional model in order to guarantee correct reception and prevent loss of reported incidents.
- Single platform available for all member organisations:
- Distribution of a previously packaged virtual machine.
- Adaptable to each organisation's storage architecture.
- Traceability of incidents between organisations and the CCN-CERT.
- Classification of standardised incidents, providing a "common language" for management and processing.
- Registering response times between different incident statuses.

9.3 ARCHITECTURE

The following graphic shows the conceptual architecture diagram for the LUCIA system.



The different LUCIA instances are synchronised with the central CCN-CERT system as follows:

- One-way Synchronizing: the One-way Synchronising component allows any member organisation to call for creation, extended creation, modification, information update, adding comments and change in status of the tickets that reports to the central LUCIA server.

This component will allow any incident compiled locally in a LUCIA instance to be automatically replicated in the central server, guaranteeing that only information on the incident context is shared, with no additional data.²⁰

- Two-way Synchronising (organisations registered with the SAT-INET and SAT-SARA Early Warning Systems): the Two-way Synchronising component will give the system functional features developed in the One-way Synchronising Component from the actual LUCIA RT-IR central server towards certain LUCIAs deployed in organisations where CCN-CERT has probes.

This mechanism operates in both directions, making it possible to synchronise incidents created in the central system with others created at member organisations.

9.4 INTERCONNECTION: CONNECTORS

The platform can incorporate organisations that already have ticketing systems with the LUCIA instance from CCN-CERT.

To do so, it implements a SOAP²¹ integration layer for the connection with standard systems known as "SOAP Wrapper" allowing REST communication with the RT platform and SOAP communication with external platforms.

The existence of the REST integration layer allows custom-built developments for systems that do not have SOAP integration interfaces.

Currently, LUCIA has a BMC Remedy connector with the future possibility of incorporating other tools such as OTRS, HP Service Manager, Track, RedMine, Mantis, etc.

²⁰ Simple Object Access protocol (This is a protocol to access web services that defines how two objects in different processes can communicate by exchanging XML data (eXtensible Markup Language)).

²¹ Simple Object Access protocol (This is a protocol for access to web services that defines how two objects in different processes can communicate by means of exchanging XML data (eXtensible Markup Language)).

10.APPENDIX D. GLOSSARY

Term	Definition
<p>Brute force attack or exhaustive key search</p>	<p>STIC 401 GLOSSARY 2.97.1 EXHAUSTIVE KEY SEARCH</p> <p>1. Specific case of an attack only on encrypted text which the crypto analyst, knowing the encrypting algorithm, attempts to decipher by trying each password key by key. If the password is very long, the time invested in running through these combinations is enormous and chances of success are very low. [Ribagorda:1997]</p> <p>2.97.2 (EN) BRUTE FORCE</p> <p>(I) A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries a large number of possible solutions to the problem. (see impossible, strength, work factor) [RFC4949:2007]</p>
<p>APT (<i>Advanced Persistent Threat</i>)</p>	<p>STIC 401 GLOSSARY 2.47.1 ADVANCED PERSISTENT THREATS (APT)</p> <p>A selective cyber-espionage or cyber-sabotage attack, carried out under the auspices or managed by a country, for reasons that are not just financial/criminal or a political protest. Not all attacks of this type are very advanced or sophisticated, in the same way as not all complex and well-structured selective attacks are an advanced persistent threat. The opponent's motivation, rather than the level of sophistication or the impact, is what makes an APT stand out from others attack carried out by cyber-criminals or hacktivists.</p> <p>McAfee. Threat forecasts for 2011.</p>
<p>Cyber-incident</p>	<p>Action using networks of computers or other resources, that has a real or potentially adverse effect on an information system and/or the information that it processes or the services it provides.</p> <p>STIC 401 GLOSSARY 2.210.1 CYBER-INCIDENT</p> <p>Incident related to security of Information and Communication Technologies that takes place in Cyberspace. This term encompasses aspects such as attacks on ICT systems, electronic fraud, identity theft, abuse of Cyberspace, etc. [ISDEFE-6:2009]</p>
<p>CCN-CERT</p>	<p>National Cryptologic Centre-Computer Emergency Response Team</p> <p>STIC 401 GLOSSARY 2.185.1 CERT - COMPUTER EMERGENCY RESPONSE TEAM</p> <p>Organisation specialising in immediate response to incidents related to network or equipment security. It also publishes warnings on threats and vulnerabilities in systems. In general, it aims to raise the user system security and deal with any incidents that might arise.</p>

CIO	Chief Information Officer
CISO	<p>Chief Information Security Officer</p> <p>STIC 401 GLOSSARY 2.850.1 INFORMATION SECURITY OFFICER Person looking after the organisation's information security. Their work consists of being up to date on technology changes that might affect information security, spanning the gap between the corporate security manager and technology managers. Responsibilities do not usually include physical security, risk management or operation continuity.</p>
Cross Site Scripting (XSS).	<p>Vulnerability status that is created by insecure coding methods leading to validation of inappropriate inputs. It is usually used with CSRF (Cross-Site Request Forgery) or SQL injection (Structured Query Language).</p> <p>STIC 401 GLOSSARY 2.353.2 XSS Cross-site Scripting is a breach in security that occurs in dynamically generated websites. In an XSS attack, a Web application is sent with a script that activates when it is read by the user's browser or a vulnerable application. Given that dynamic sites depend on user interaction, it is possible to put a malicious script on the page, hiding it among legitimate requests. Common entry points include search engines, forums, blogs and all types of online forms in general. Once the XSS has begun, the attacker can change user configurations, hijack accounts, poison cookies, expose SSL connections, access restricted sites and even install advertising on the victim's site.</p> <p>http://www.inteco.es/glossary/Formacion/Glosario/</p> <p>2.353.3 XSS CROSS-SITE SCRIPTING is a breach in security that occurs in dynamically generated websites. In an XSS attack, a Web application is sent with a script that activates when it is read by a user's browser or a vulnerable application. Given that dynamic sites depend on user interaction, it is possible to put a malicious script on the page, hiding it among legitimate requests. Common entry points include search engines, forums, blogs and all types of online forms in general. Once the XSS has begun, the attacker can change user configurations, hijack accounts, poison cookies, expose SSL connections, access restricted sites and even install advertising on the victim's site.</p> <p>http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S</p> <p>2.353.4 CROSS-SITE-SCRIPTING VULNERABILITY This fault allows an attacker to enter a "script" (perl, php, javascript, asp) in the field of a form or code embedded in a page that when stored or shown in the browser can cause unwanted code to be run. http://www.vsantivirus.com/vul-webcamxp.htm</p>

CSIRT	Computer Security Incident Response Team, similar to a CERT.
CSRF /XSRF Cross site request forgery	<p>STIC 401 GLOSSARY 2.358 CROSS-SITE REQUEST FORGERY</p> <p>Acronyms: CSRF, XSRF</p> <p>2.358.2 CROSS SITE REQUEST FORGERY</p> <p>A CSRF (Cross-site request forgery) is a type of malicious exploit on a website where unauthorised commands are sent by a user that the website trusts. This vulnerability is also known by other names such as XSRF, hostile linking, one click attack, session riding, and automatic attack.</p> <p>http://es.wikipedia.org/wiki/Cross_Site_Request_Forgery</p> <p>2.358.1 CROSS SITE REQUEST FORGERY (CSRF)</p> <p>Vulnerability status that is created by insecure coding methods that allow unwanted actions to be run using an authenticated session. It is usually seen alongside XSS or SQL injection.</p> <p>http://es.pcisecuritystandards.org</p>
Defacement or Misrepresentation	<p>STIC 401 GLOSSARY 2.377 DEFACE 2.377.1 MISREPRESENTATION. Attack on a web server that changes its appearance. The change of image can benefit the attacker or be mere propaganda (benefiting the attacker or causing an embarrassing situation for the site owner).</p> <p>CCN-CERT IA_09-15 Threat Report. Deface or Defacement is a deformation or change caused intentionally on a legitimate website using some type of malware.</p>
DoS / DDoS (Denial of Service / Distributed Denial of Service)	<p>STIC 401 GLOSSARY 2.381.1 DENIAL OF SERVICE. Denial of Service, in computer security terms, is understood to be a set of techniques used to make a service inoperable. This type of attack aims to overload a server, thereby denying service to its legitimate users. The attack consists of saturating the server with service requests until it cannot deal with them, causing it to collapse.</p> <p>A more sophisticated method is the Distributed Denial of Service attack (DDoS) where requests are coordinated between several computers that might be being used for this purpose without their legitimate owners actually knowing. This can be done using malware programs that take control of the computer remotely, such as cases of certain types of worms or because the attacker has entered the victim's computer directly. http://www.inteco.es/glossary/Formacion/Glosario/</p> <p>2.382.1 DISTRIBUTED DENIAL OF SERVICE. Denial of service attack that is carried out using multiple attack points simultaneously.</p> <p>2.382.2 DISTRIBUTED DENIAL OF SERVICE</p> <p>DoS attack involving a large number of attacking computers. [CCN-STIC-612:2006]</p>
Event	STIC 401 GLOSSARY 2.476.3 EVENT

	<p>(Service Operation) A significant change in status for a Configuration Element or an IT Service.</p> <p>The term Event is used as a Warning or Notification created by an IT Service, Configuration Element or a Monitoring tool. Events normally require actions from IT Operations staff and often involve the Incident log [ITIL:2007]</p>
Security Event	<p>STIC 401 GLOSSARY 2.476.2 INFORMATION SECURITY EVENT</p> <p>Occurrence detected in a system, service or network status that indicates possible violation of the information security policy, a fault in the controls or an as-yet unknown situation that might be relevant to security. [UNE-ISO/IEC 27000:2014]</p>
Worm	<p>STIC 401 GLOSSARY 2.553.1 WORM Program that is designed to be copied and propagate itself using network mechanisms. Does not infect other programs or files. [CCN-STIC-430:2006]</p> <p>2.553.3 WORM This program is similar to a virus although differs in how it carries out infections. Whilst a virus will attempt to infect other programs by copying itself inside them, a worm will make copies of them, infect other computers and is automatically propagated in a network independently of human action.</p> <p>http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S</p>
IDS/IPS	<p>Intrusion Detection System/Intrusion Prevention System</p>
Incident	<p>An occurrence that, really or potentially, endangers the confidentiality, integrity or availability of an information system; or the information that the system processes, stores or sends; or that constitutes a violation or imminent threat of violation to the organisation's security policies, standards or procedures.</p> <p>STIC 401 GLOSSARY 2.574.2 INCIDENT</p> <p>(Service Operation) Unplanned shut-off of an IT Service or Quality failure for an IT Service. It also refers to a Configuration Element Fault that has not yet affected the Service. For example, a Fault in a mirror disk. [ITIL:2007]</p> <p>2.574.3 INCIDENT</p> <p>Any event that is not part of standard operation for a service that causes, or might cause, a shut-off or quality failure on this service (aligned to ITIL). [COBIT:2006]</p> <p>2.574.4 INCIDENCE</p> <p>Any anomaly that affects or might affect data security.</p> <p>Royal Decree 994/1999, dated 11 June, approving the Regulation on security measures for automated files containing personal data.</p>

Security incident	<i>See Cyber-incident</i>
Social Engineering	<p>2.601 SOCIAL ENGINEERING (SUBTERFUGE)</p> <p>2.601.2 SOCIAL ENGINEERING</p> <p>These are techniques based on swindles used to control a person's behaviour or obtain sensitive information. The affected person is incited to act in a certain way (clicking links, entering passwords, visiting pages, etc.) convinced that they are doing the right thing when really they are being tricked by social engineering.</p> <p>http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S</p> <p>2.601.4 SOCIAL ENGINEERING</p> <p>Euphemism used to refer to non-technical, low complexity technological means to attack information systems such as lies, identity theft, tricks, bribes and blackmail. [CCN-STIC-403:2006]</p>
Remote File Injection	<p>STIC 401 GLOSSARY 2.622.1 INJECTION ERRORS</p> <p>Vulnerability status that is created by insecure coding methods that results in validation of inappropriate inputs allowing attackers to transfer malware to the underlying system through a web application. This type of vulnerability includes SQL injection, LDAP (Lightweight Directory Access Protocol) injection and XPath injection.</p> <p>http://es.pcisecuritystandards.org</p>
SQL injection	<p>STIC 401 GLOSSARY 2.623.1 SQL INJECTION</p> <p>Type of attack on websites based on databases. A malicious person runs unauthorised SQL commands making the most of insecure codes from a system connected to the Internet. SQL injection attacks are used to steal injection that is normally not available from a database or to access the host computers of an organisation by means of the computer working as the database server.</p> <p>http://es.pcisecuritystandards.org</p>
DP Day - person	<p>Estimation of the effort required to carry out a task whose unit is equivalent to an uninterrupted work day for an average worker.</p>
Pharming	<p>STIC 401 GLOSSARY 2.747.1 PHARMING Computer attack that consists of modifying or replacing the domain name server file by changing the legitimate IP (Internet Protocol) address (commonly for a bank) so that when the user writes the entity's domain name in the address bar the browser will automatically redirect the user to another IP address hosting a false website that will assume the legitimate identity of the entity, illicitly obtaining access passwords for the entity's customers.</p> <p>http://www.inteco.es/glossary/Formacion/Glosario/</p>

<p>Phishing Spear phishing</p>	<p>STIC 401 GLOSSARY See: • http://en.wikipedia.org/wiki/Phishing 2.761.1 PHISHING. Attack method that seeks to obtain personal or confidential information from users by means of trickery or subterfuge, stealing the digital identity of an entity that is trusted in cyberspace. 2.761.2 PHISHING. Phishing is the name given to the trick carried out online where a scammer attempts to fraudulently get confidential information (passwords, bank details, etc.) from legitimate users. The scammer or phisher steals the identity of a trusted person or company so that anyone receiving apparently official electronic communication (email, fax, text message or phone call) believes that it is real and thereby provides the personal data requested by the scammer. http://www.inteco.es/glossary/Formacion/Glosario 2.761.3 PHISHING. "Phishing" attacks social engineering to fraudulently get personal information from users (mainly access to financial services). They use spam for distribution to reach the greatest possible number of victims and increase their chances of success. Once the mail reaches the recipient, they try to trick users to provide personal data, normally by taking them to fake places on the Internet, apparently official websites for banks and credit card companies that end up convincing the user to enter personal details for their bank account, giving their account number, password, social security number, etc. http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S 2.983.1 SPEAR PHISHING. Specific phishing that maximises the probability of the attack victim taking the bait (usually based on prior social engineering work on the victim) CCN-CERT IA-09-15 Threat Report. Identity theft. This consists of sending emails that seem to be reliable and that usually lead to false websites collecting confidential data from the victims. Attack method that seeks to obtain personal or confidential information from users by means of trickery or subterfuge, stealing the digital identity of an entity that is trusted in cyberspace.</p>
<p>Cyber-Incident Response Plan</p>	<p>Predetermined and ordered set of instructions and procedures to detect, respond and limit the consequences of a cyber-incident.</p>
<p>Ransomware</p>	<p>STIC 401 GLOSSARY 2.821.1 RANSOMWARE Ransomware is malware used to hijack data, a means of exploitation in which the attacker puts a price on the victim's data and demands payment to decipher the code. Ransomware is propagated through files attached to email,</p>

	<p>infected programs and compromised websites. A ransomware malware program can also be called a cryptovirus, cryptotrojan or cryptoworm. This consists of hijacking the computer (making it impossible to use it) or encrypting its files (cryptoware), promising to release them once a certain amount of money, or ransom, has been paid.</p> <p>CCN-CERT IA-09-15 Threat Report. This consists of hijacking the computer (making it impossible to use it) or encrypting its files (cryptoware), promising to release them once a certain amount of money, or ransom, has been paid.</p>
RAT (Remote Access Tool)	<p>Piece of software that allows an "operator" to remotely control a system as if they had physical access to it. Although it has perfectly legal uses, RAT software is usually associated with cyber-attacks or criminal or harmful activities. In these cases, the malware is usually installed without the victim knowing, frequently hiding a Trojan.</p>
Rootkit	<p>STIC 401 GLOSSARY 2.870.1 ROOTKIT This is a tool that is used to hide illegitimate activities in a system. Once installed, it gives the attacker the same level of privileges as the computer administrator. It is available for a wide range of operating systems. http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=5</p> <p>2.870.2 ROOTKIT Type of malicious software that, when installed without authorisation, is capable of going undetected and taking administrative control of a computer system. http://es.pcisecuritystandards.org</p>
Scanner (Scanning) Vulnerability scanning / Network security analysis	<p>STIC 401 GLOSSARY 2.461.1 VULNERABILITY SCANNER. Program that analyses a system searching for vulnerabilities. It uses a database of known defects and determines the vulnerability of the system being examined.</p> <p>2.461.2 NETWORK SECURITY ANALYSIS Process that searches for vulnerabilities in an entity's systems remotely using manual or automated tools. Security analysis that includes exploration of internal and external systems and generates reports on services exposed to the net. The analyses can identify vulnerabilities in operating systems, services and devices that might be used by malicious persons. http://es.pcisecuritystandards.org</p>
Sniffer/Sniffing	<p>2.977.1 NETWORK MONITOR Programs that monitor information on the net to capture information. Network interface cards have a system for verifying addresses telling them whether the information passing through is intended for its system. If not, it rejects it. A Sniffer consists of putting the network interface card in a mode known as promiscuous which deactivates the address</p>

	<p>verification filter and therefore all packets sent to the network come to this card (computer where the Sniffer is installed). There are Sniffers to capture any type of specific information. For example, passwords giving access to accounts, making the most of the fact that the user does not generally encrypt them. They are also used to capture credit card numbers or email addresses. Traffic analysis can also be used to determine relationships between several users (find out which users or systems relate to someone in particular). Good Sniffers cannot be detected although the immense majority can be spotted with a few tricks, because they are too closely related to the TCP/IP protocol.</p> <p>http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S</p> <p>Network packet capturing program Literally a sniffer. [CCN-STIC-435:2006]</p>
SOAP	<p>Simple Object Access Protocol. This is a protocol for access to web services that defines how two objects in different processes can communicate by exchanging XML data (eXtensible Markup Language).</p>
Spam	<p>STIC 401 GLOSSARY 2.969.2 SPAM Unsolicited emails that are sent randomly in batch processes. This is an extremely efficient and cheap way of marketing any product. The majority of users are exposed to spam as confirmed in surveys showing that over 50% of all emails are spam. This is not a direct threat but the quantity of emails generated and the time that it takes companies and individuals to deal with them and delete them is annoying for Internet users.</p> <p>http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S</p>
Spear Phishing	<p>STIC 401 GLOSSARY 2.983.1 SPEAR PHISHING. Specific phishing that maximises the probability of the attack victim taking the bait (usually based on prior social engineering work on the victim)</p>
Spyware "spy software"	<p>STIC 401 GLOSSARY 2.972.1 SPYWARE</p> <p>Type of malicious software that, once installed, intercepts or takes partial control of the user's computer without their consent. http://es.pcisecuritystandards.org</p> <p>2.972.3 SPYWARE</p> <p>Malware usually designed to use the infected user's work station for commercial or fraudulent purposes such as displaying advertising or stealing personal information from the user. [CCN-STIC-400:2006]</p> <p>2.972.4 SPY SOFTWARE</p> <p>Any form of technology that is used to collect information on a</p>

	<p>person or a company, or information referring to equipment or networks, without their knowledge or consent. It can also be implanted in their hardware. It can capture browsing habits, mail messages, passwords and bank details to send them to another destination on the Internet. Just as a virus can be installed by merely opening an infected mail attachment, clicking on an advertising window or camouflaged along with other programs that we install.</p> <p>http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S</p>
<p>SQL</p>	<p>Structured Query Language</p>
<p>Spoofing</p>	<p>STIC 401 GLOSSARY 2.992.2 SPOOFING</p> <p>Spoofing is a technique based on creating TCP/IP frames using a fake IP address; from their machine, an attacker simulates the identity of another machine in the network (obtained previously by a variety of methods) to get access to resources in a third system that has established some kind of trust based on the name or the IP address of the spoofed host.</p> <p>http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S</p> <p>2.992.3 SPOOFING</p> <p>As far as network security is concerned, spoofing is an identity theft technique using the Net, carried out by an intruder generally for malware or investigation uses. Security attacks on the net using spoofing techniques endanger user privacy on the Internet, as well as data integrity.</p> <p>Depending on the technology used, various types of spoofing can be distinguished:</p> <ul style="list-style-type: none"> • IP spoofing: This consists of impersonating the original IP address for a TCP/IP packet with another IP address you wish to impersonate. • ARP spoofing: This is identity theft by forging the ARP. ARPs (Address Resolution Protocol) are network level protocols that relate a hardware address with the computer's IP address. Therefore, when the victim's ARP is forged, everything they send will be sent to the attacker. • DNS spoofing: This is identity theft concerning the domain name which consists of a fake relationship between the IP and the domain name. • Web spoofing: The attacker uses this technique to create a fake website, very similar to what the affected person usually uses in order to obtain information from this victim such as passwords, personal information, data provided, pages that they

	<p>frequently visit, user profile, etc.</p> <ul style="list-style-type: none"> • Mail spoofing: Email identity theft either from persons or entities in order to carry out massive phishing or spam. <p>http://www.inteco.es/glossary/Formacion/Glosario/Spoofing</p>
Trojan	<p>STIC 401 GLOSSARY 2.155.1 TROJAN HORSE. Someone or something intended to defeat or subvert from within usually by deceptive means. Merriam Webster dictionary.</p> <p>2.155.2 TROJAN Also known as a "Trojan Horse". A type of malware that, once installed, allows the user to run functions normally whilst the Trojans run malicious functions without them knowing. http://es.pcisecuritystandards.org</p> <p>2.155.3 TROJAN Program that does not replicate itself or make copies of itself. It appears to be a useful or innocent program but it actually has harmful purposes such as allowing intrusions, deleting data, etc. [CCN-STIC-430:2006]</p> <p>2.155.4 TROJAN HORSE Program that apparently or really runs a useful function but hides a harmful subprogram that abuses the privileges granted to run the aforementioned program. For example, a program that reorders a file properly and, using the writing rights that have to be granted to it, copies it into another file that can only be accessed by the creator of this program. [Ribagorda:1997]</p> <p>CCN-CERT IA_09-15 Threat Report. Trojan Horse or Trojan is malware that looks like an inoffensive program but, when run, gives the attacker remote access to the infected computer, normally by installing a backdoor.</p>
Virus	<p>STIC 401 GLOSSARY 2.1049.1 VIRUS Program that is designed to copy itself with the intention of infecting other programs or files. [CCN-STIC-430:2006]</p>

11.APPENDIX E. REFERENCES

- RD 3/2010, dated 8 January, regulating the National Security Framework in the field of Electronic Administration.
- RD 951/2015, dated 23 October, modifying RD 3/2010, dated 8 January, regulating the National Security Framework in the field of Electronic Administration.
- CCN-STIC-403 Guide. Security incident management.
- CCN-STIC-815 Metrics and Indicators in the ENS.

- NIST SP 800-61 (Rev 2) Computer Security Incident Management Guide (Aug., 2012).
- NIST SP 800-150 (Draft) Guide to Cyber Threat Information Sharing (Oct., 2014).