CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

INTECO (cert)

IDENTIFICATION AND REPORTING OF SECURITY INCIDENTS FOR STRATEGIC OPERATORS

A basic guide for the protection of critical infrastructures

INTECO Instituto Nacional de Tecnologías de la Comunicación

www.inteco.es

@intecocert

January 2014

CONTENTS

THE GUIDE'S OBJECTIVE 3

ACTIONS TO BE TAKEN IN THE EVENT OF AN INCIDENT 4

RESPONSE **4**

IDENTIFICATION 5

CONTAINMENT AND MITIGATION 6

DATA LEAKAGE AND EVIDENCE GATHERING 7

RECOVERY 8

DOCUMENTATION 9

REPORTING OF INCIDENTS 10

HOW TO REPORT **11**

REQUIRED INFORMATION **11**

CLASSIFICATION AND PRIORITISATION **12**

SCALE OF INCIDENTS **12**

TYPES OF INCIDENTS 14

CONCLUSIONS 15

Authors

Jesús Díaz Vico

Daniel Fírvida Pereira

Marco Antonio Lozano Merino

Coordination

Elena García Díez

1 THE GUIDE'S OBJECTIVE

This basic guide for the protection of Critical Infrastructures, regarding the identification and reporting of security incidents for Strategic Operators, is intended to serve as an action guide for the reporting and management of incidents related to Critical Infrastructures (CIs) and Strategic Operators, through INTECO's *Centro de Respuesta a Incidentes de Seguridad* (Computer Emergency Response Team) – (INTECO-CERT).

It should be emphasised that the response to incidents in CIs is carried out by INTECO in close collaboration with the National Centre for Critical Infrastructure Protection (CNPIC).

The operation of this service includes reporting security incidents to INTECO-CERT and CNPIC, the analysis of incidents, the extent to which their resolution needs managing, and a response on the part of INTECO-CERT, including recommendations to reduce the security risk such incidents may suppose to operators.

For easing the effective management of such incidents, this document sets out guidelines and procedures which those operators who suffer an incident may follow, along with an assessment of the severity of the incident. This information will be generated through the assessment of incidents through a system of incident management (in what follows RTIR – Request Tracker Incident Response).

In this guide for the identification and reporting of security incidents, although specific matters which deal with concrete cases are included, common criteria related to generally recognised good practices for the management of incidents are defined, such that they may serve as a reference for the design and implementation of this type of service on a wider scale.

This technical publication falls within the specific action framework set out by the Security and Industry CERT as defined by the agreement on Critical Infrastructure protection signed in October 2012 by the Secretaría de Estado de Seguridad (Secretary of State for Security, SES), organ dependent on the Ministerio del Interior (Interior Ministry), and the Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (the Secretary of State for Telecommunications and the Information Society, SETSI), organ dependent on the Ministerio de Industria, Energía y Turismo (Ministry for Industry, Energy and Tourism), for effective cooperation between CNPIC, law enforcement agencies and INTECO in cybersecurity matters.

2 ACTIONS TO BE TAKEN IN THE EVENT OF AN INCIDENT

In the event of a security incident, the main objective is to **recover the normal level of functioning of systems or services**, with respect to their quality and availability, minimising losses as much as possible.

The process of being able to recover this level of normal activity, along with actions to mitigate the incident's possible consequences, and the process of acquiring and analysing evidence, make up the set of actions that need to be carried out in the event of a security incident.

What follows here is a description of the actions to be carried out to mitigate the effects of security incidents and recuperate the affected systems, along with an illustrating flowchart.

RESPONSE

The main phases of response following an incident, shown in figure 1, can be summarised as: **identification, containment and mitigation, preservation of evidence and legal considerations, recovery and documentation**[1].

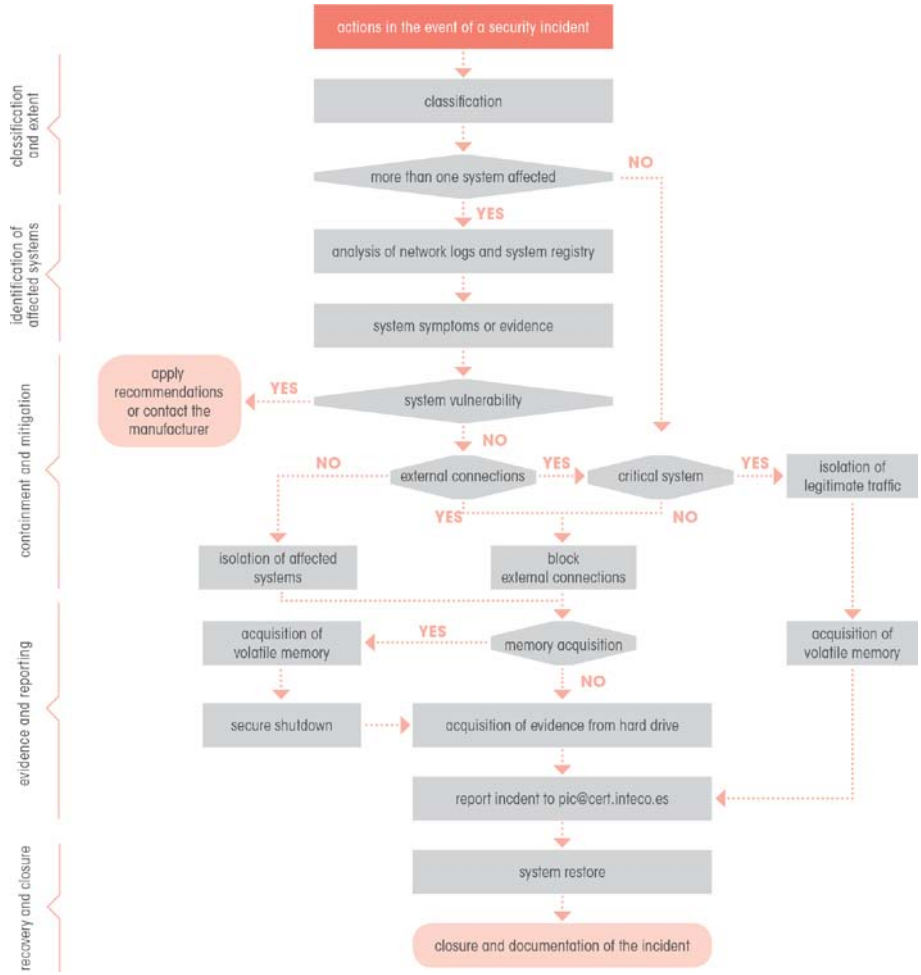

Figure 1: Action flowchart in the event of a security incident

[1] http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

IDENTIFICATION

To identify a security incident, determine its extent and the systems affected by it, evidence can be gathered in a variety of ways determined by the nature and type of the incident. One of the main methods is the analysis of logs and other sources of information for detecting anomalies. Such sources include:

- Anti-virus consoles.
- Intrusion Detection and Intrusion Prevention Systems (IDS/IPS).
- Security Information and Event Management (SIEM) warnings.
- Inspection of audit logs to identify attempts at unauthorized access.
- Logs of connections blocked by firewalls.
- Logs of connections made by corporate proxies.
- Data Loss Prevention (DLP) tool logs.
- Blocking of user accounts or other anomalies reported to the CAU or which imply risks such as loss of USB devices or laptops.
- Sudden and excessive use of memory or server disc space.
- Traffic anomalies, such as consumption peaks at unusual times.
- Network dumps, through, for example, port mirroring, which may allow the confirmation of a suspected incident.

The detection of these types of anomalies allows the identification of a possible security incident, along with its nature and extent. Should any of these records present anomalies, a more detailed analysis to determine whether there actually has occurred an incident will need to be carried out.

Such an analysis may be carried out, for example, through the detection of malicious network traffic, identifying the affected infrastructure, the host and destination addresses, the used port values, TTL, protocols, etc.

These actions will help to determine if there has really been a security incident, and its nature.

At a system level, ways of finding out if the incident has been having effects include:

- Unusual or especially privileged user accounts.
- Hidden files, or files that appear suspicious because of their size, file name or location, possibly indicating a data or logs leakage on the part of malware.
- Files with unusual permissions, with SUID or GUID, with unusual paths, orphan files, indicating the possibility of some kind of intrusion or rootkit.
- Suspicious registry entries, mainly in the case of Windows systems with malware infections, this being one of the main ways malware assures its persistence in the infected system.
- Unusual processes and services, not only listening services but those with connections to ports or hosts that are strange, unusual, or which appear on blacklists of Command and Control servers used by botnets.
- Excessive disc or memory loads, which may be provoked by a security incident involving malware, denial of service or intrusions.
- Sessions in a device opened by other devices, ARP table anomalies, unusual shared folders, an elevated number of anomalous active TCP connections, which may indicate a denial of service attack.

- In the case of user equipment or mobile devices, the following may indicate some kind of system infection, amongst others: anomalous sharing of applications, navigator pop-up windows, slow connections, reboots or applications which close without warning.
- Scheduled tasks or unusual activity in log files, which may indicate an abnormal system function or intrusion attempts into a given service through, for example, brute force.
- Alerts of the corporate anti-virus platform, or other tools normally deployed to identify rootkits, to carry out integrity checks on files, binary file signatures, etc. Installing such tools on possibly infected systems *ad hoc* is not recommended, since access dates may be altered, and evidence lost.

In addition to these measures to identify security incidents in affected devices, it cannot be ruled out that an incident may be identified by means of an external data source, a CERT report, or a report from another body, or from a user external to the organisation, etc.

CONTAINMENT AND MITIGATION

Once the incident has been identified, it is necessary, using the data already gathered, to contain it and mitigate its effects. In order to do this it is essential to define the extension of the incident, the kinds of devices affected, and their common characteristics in order to be able to isolate the incident according to this data.

In addition, it is important to be well prepared before the event. Tools such as an up to date inventory of assets, a map of the network architecture, IDS/IDP intrusion detection, event management tools (SIEM) and firewalls will help to determine more precisely the character of the incident and how to contain it.

Once the incident has been detected, it is key to define its extent, whether an infection is being dealt with, the type of equipment affected, identifying common characteristics (operating system platforms, the specific type of workplaces, single servers, etc.) in order to determine the extent of the infection and be able to take measures to isolate it according to the configurations identified.

The most important recommendations for the containment and mitigation of a security incident which may be applied at this stage are:

- Disconnecting the equipment or network segment from the rest of the organisation's networks. This can be done, in the case of an isolated device, by directly disconnecting the network cable, or isolating a network segment in a VLAN or similar.
- In the case of the infection occurring in a critical device, strictly necessary traffic may be isolated through setting up a firewall between this element and the rest of the network, allowing only traffic strictly necessary for the system's functioning.
- If the type of incident has been identified, and technical details are known, such as the malware's spread vectors, the behaviour pattern of a denial of service, or the characteristics of an intrusion attempt through brute force, it is possible to apply containment measures more appropriate for a given set of circumstances. For example, blocking specific emails, the access to shared equipment, outgoing connections, or any malware infection vector through firewall policies and rules. In the same way, it is possible to programme filter rules for denials of service or attempts at intrusion.
- In the case of a vulnerability which could result in intrusion or denial of service, all

the mitigating procedures recommended by the manufacturer have to be applied, and the recommended patches installed. If the system is a critical one, in which, for whatever reason, it is not possible to apply the patch or the threat mitigation measures, the manufacturer will need to be contacted so that alternative solutions may be evaluated and obtained.

DATA LEAKAGE AND ACQUISITION OF EVIDENCE

To avoid data leakage it is fundamental to identify the leak vector and then adopt the appropriate technical measures to limit its exploitation, whether these be restricting access to shared folders, disabling portable storage systems (USB devices, for example), blocking URLs or email, etc.

In addition, the repercussions of the leak will have to be quantified. It may result that the data leak is related to the access credentials of a given user of a given system in the organisation, which have been made public. In these cases, it may be necessary to consider involving the organisation's legal resources, and those of Human Resources and communication in order to outline a global strategy to deal with the leak.

Once the security incident and the equipment affected have been identified, and the latter isolated from the rest of the network, the next step is the preservation of data for forensic analysis of the incident. Volatile data will have to be extracted from memory before shutting down the system.

The data stored in the equipment's memory may turn out to be very important in analysing cases of malware or intrusions, and, on shutting the system down, they will be lost. Thus, as far as possible, measures for their acquisition will have to be taken before shutdown.

To acquire this data forensic tools designed for this end may be used. Nevertheless, neither the system nor its data should be altered in this process, since important data, such as file access dates, may be corrupted, or evidence lost.

Once this data has been acquired, mechanisms for preserving their integrity have to be put into effect, through the application of appropriate cryptographic hash functions. In doing this, there are various criteria that have to be taken into account.

On the one hand, most forensic analysis tools support the MD5 and SHA1 functions, while more advanced functions, such as those of the SHA2 family, are less widely supported. On the other hand, MD5 and SHA1 entail a lower computational cost, in return for a somewhat lower level of cryptographic security as well, while SHA2 functions are more collision resistant, at a cost of being more computationally intensive. This is an important factor, given that memory dumps are typically greater than 512 MB. Therefore, while the final decision will depend on the resources (tools and computing capacity) available, it will be necessary to balance cost and security. In most cases, obtaining both MD5 and SHA1 hashes for the data to be backed up will provide a solution acceptable both in terms of robustness and cost.

The main tools for the acquisition of volatile data from memory are:

- In the case of UNIX/Linux systems, LiME[2] run from a USB device connected to the compromised system, taking into account that the tool has to have the same kernel as the compromised system compiled and that the necessary libraries have to be included in the USB device.
- The Volatility[3] tool is also available for UNIX/Linux systems, and can also be run from a USB device. Again, the same kernel has to be compiled, and the necessary libraries included.
- For Windows systems, tools such as FTK Imager[4], DumpIT[5], Memory DD[6] o Memoryze[7] can carry out a system memory dump, or dumps of paging files and processes. Again, using Volatility, an analysis of the data extracted can be carried out.
- In virtual systems, RAM is found in .sav files in VirtualBox, and .vmen files in the case of VMWare.

Once the process of volatile data acquisition has been completed, the system can be shut down. In order to avoid any unexpected behaviour on the part of any malware or rootkit used for intrusion in doing this, cutting the power to the system, by directly unplugging the power cable, is recommended.

RECOVERY

Once evidence has been preserved and the incident reported, the next step to be taken is to recover the affected systems.

In the case of incidents caused by an intrusion or the introduction of malware into a non critical system, once the infection or intrusion vector has been detected and the opportune corrective measures to prevent the incident occurring anew established, the system affected by the incident may be restored using a backup carried out prior to the infection.

In the case of critical systems which are not high availability, the value of realising periodic copies of the whole system (and not just of data) may have to be included in business continuity plans. This would allow the recovery of normal activity in the case of incidents occasioned by malware or intrusions, taking into account that the original attack or infection vector will have to be prevented or blocked.

In any case, with critical systems, the manufacturer's instructions for recovery or reinstallation will have to be followed, programming the corrective maintenance and downtime necessary in order to recover from the incident.

In the same way, in incidents related to vulnerabilities the manufacturer's recommendations for mitigating or solving the vulnerability will have to be followed, applying the official patches released by the developer.

[2] LiME: http://code.google.com/p/lime-forensics/

[3] Volatility: http://code.google.com/p/volatility/

[4] FTK Imager: http://www.accessdata.com/support/product-downloads/ftk-download-page

[5] DumpIT: http://www.moonsols.com/wp-content/plugins/download-monitor/download.php?id=7

[6] Memory DD: http://sourceforge.net/projects/mdd/

[7] Memoryze: http://www.mandiant.com/resources/download/memoryze/

DOCUMENTATION

In the management of security incidents it is of great importance to document all that has been learned from previous incidents. These lessons learned may prove vital in avoiding future security incidents or resolving new incidents of similar characteristics

It is important that this documentation be detailed, such that it be known which tools were used and how, the investigations which were carried out and what their results were, the partnerships that were necessary, the documentation used to resolve the incident, the time line of actions followed, etc.

All this serves to identify with precision the nature and type of the incident, its characteristics, the malware or intrusion infection vectors, not only to be able to configure security systems adequately but also to carry out organisation-wide awareness campaigns focused on what the weak points of the system are and how to protect them.

In addition, this information allows the perpetrators of such attacks, their strategies, and denial of service patterns to be known. Identifying new vulnerabilities which affect the most critical systems of an organisation will also help in great measure to avoid and resolve possible security incidents.

All these technical and procedural steps of an organisation always have to take into account not only the legal considerations relevant for the organisation according to its sector and scope but also principles of privacy of communications and of persons, the penal code, etc. These considerations need to be taken into account throughout the resolution of an incident, and especially when acquiring data in the case of a forensic analysis.

3 REPORTING OF INCIDENTS

One of the tasks of INTECO-CERT and CNPIC is responding to security incidents reported as occurring in Critical Infrastructures by users of this service, and ensuring that the relevant information is stored in RTIR.

In what follows, a description is given of the information necessary both to correctly realise an information report on the part of the operators, and to facilitate communication between INTECO-CERT, CNPIC and the operators This description follows the scheme shown in Figure 2.

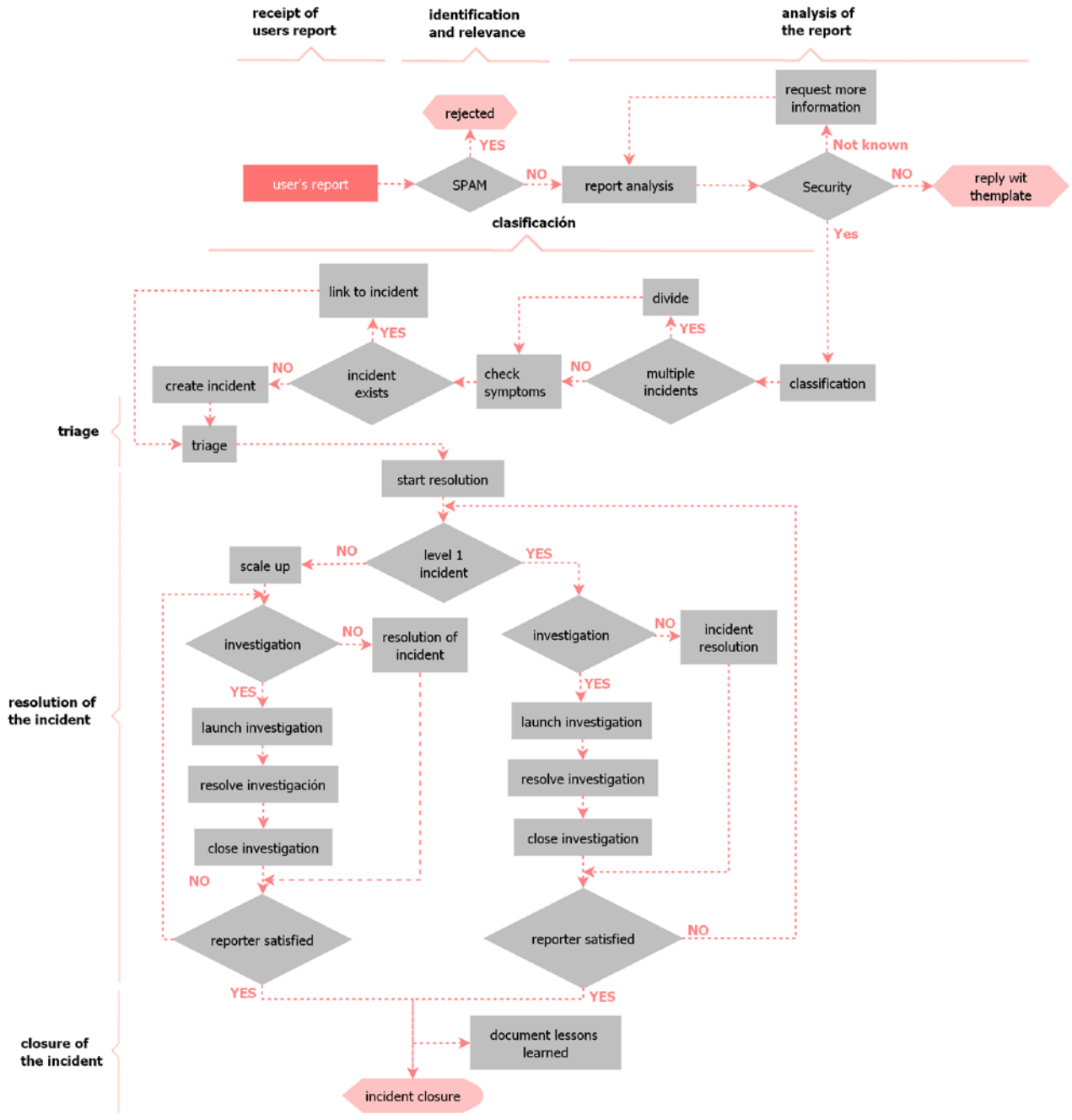

Figure 2. Steps to report an incident

HOW TO REPORT

Security incidents are reported through the user who, having been identified as a point of contact of the involved organisation, and acting as a representative of it, accesses the incident reporting service through an email sent to pic@cert.inteco.es. With this information an Incident Report will be generated in RTIR.

All information exchanges with the user will be performed by email from RTIR, from the address pic@cert.inteco.es. , with the standard subject-line field [INTECO-CERT/CNPIC #***] (*** being the report number created by the user). In this way, all exchanged emails will be stored in the same report, allowing their full monitoring.

As an exception, if the incident is considered sufficiently relevant, contact will be made with certain users by telephone. This contact will be considered complementary to the procedure detailed below.

All emails sent from the pic@cert.inteco.es account will be digitally signed with the private key that belongs to that account. In addition, when the exchanged information is confidential (logs containing credentials, confidential or personal information), the relevant emails will be encrypted by the INTECO-CERT technician who carries out the notification.

REQUIRED INFORMATION

The information that has to be included in a report of a security incident, so that a report be generated in the RTIR tool by the INTECO-CERT technician, has to include all the information that the user considers necessary for the incident's resolution; for example, a description of the incident, the elements involved, software versions, the nature and type of incident (if known), the IPs and hosts involved, etc.

With this information, the moderator of the RTIR incidents queue who has received and logged the report will create a new incident from the user's report. The incident will include the following data:

- **Subject**: This is a sentence which describes the incident in general form. This field will be inherited by all the investigations opened in association with the initial incident.

  By default, the subject field appears in the report from the point at which it is created, for which reason it can be either kept or replaced by a more explanatory name with the following format:

  - ***[Company name]* Textual description of the incident***

    - ** Only if identified*

- **Description:** This is a brief description of the incident. The moderator of the queue will use this field to make important comments about the incident.

- **Function:** Consultation or Incident. By default, Incident.

- **Classification:** This defines the incident according to the categories defined in the Types of Incidents section of this document.

- **Level:** This indicates the level of support the incident requires, according to the levels defined in the Scale of Incidents section of this document. By default, this is set to level 1.
- **Message:** By default, the body of the message reporting the incident sent by the user. The moderator will add comments if necessary and if necessary remove those fields left blank by the user.

  This message will also include all the information which the personnel of the strategic operator have been able to identify during the identification of the incident, including files, memory dumps, and any other information relevant to the incident.

- **Priority:** This indicates the level of priority of the incident. The levels of priority are defined in the Classification and Prioritisation section of this document.

CLASSIFICATION AND PRIORITISATION

For INTECO-CERT to be able to supply consistent and opportune responses/solutions to the user and ensure that sensitive information is managed appropriately, incidents have to be classified and prioritised correctly as soon as they are recorded in RTIR. Nevertheless, INTECO-CERT will be able to modify the classification and prioritisation of security incidents during their resolution, the values referred to remaining recorded in RTIR.

According to an incident's priority, the levels referred to are the following:

- **High:** Incidents which affect systems or data critical for the operator, and which may have a potential impact on the business.

  These incidents are typically: destructive malware, denial of services or compromised system, and certain cases of hacking and policy violations which affect critical systems.

- **Medium:** Incidents which affect systems or data which are not critical for the operator or whose impact does not have direct business repercussions.

  In this category are included the majority of hacking and phishing incidents, along with, in certain cases, policy violations and other consultations.

- **Low:** Possible incidents in non-critical systems, investigations requiring forensic analysis whose time scale is prolonged, or general consultations regarding security.

  This level includes the majority of consultations and invasive attacks, along with incidents of any other type which affects systems with a low level of importance or little business impact. The different types of incidents contemplated here are set out in the Types of Incidents section of this document.

SCALE OF INCIDENTS

Here it is defined the methodology of grading security incidents, so that support be given and incidents managed on the part of INTECO-CERT.

- **Level 1:** Level 1 security operators carry out primary care activities with respect to the reports and consultations that INTECO-CERT receives and take action in the cases of the most trivial incidents (incidents which do not require and expert security level).

They monitor all open reports and incidents and generate all necessary documentation.

They respond to and give support for attacks or incidents such as:

- Responses to requests for information (consultations).
- Known attacks or attacks whose identification is immediate.
- Monitoring and response to public vulnerabilities.
- Identification of defects and risks in the network topology or security systems.
- Identification of defects and incidences of internal security procedures and policies (systems, development, security, etc.).

Incidents which require a high level of expertise in security are classified at level 2.

- **Level 2:** This is an expert team which responds to incidents which require a high level of expertise in security. Incidents are scaled up from level 1 to level 2 by the level 1 team.

  The level 2 team analyses and responds to security attacks or incidences such as:

  - Unknown attacks, or attacks that are difficult to identify.
  - Analysis of suspicious vulnerabilities or incidents that require expert knowledge.
  - Support and consultation on existing network topology or the adequate configuration of security devices.
  - Identification of relations between incidents and defects in security and support procedures and policies.
  - Evaluation of risks and the impact of vulnerabilities and attacks.
  - Intrusion Tests.
  - Analysis of the impact and real risks of existing vulnerabilities.
- **CNPIC:** In addition, CNIPC's Servicio de Seguridad Lógica (Logical Security Service) will be informed by means of email, and may see itself involved in the management of an incident, contributing its specific experience in some of the main issues related to the protection of critical infrastructures, such as:
  - Previous experience in industrial control systems.
  - Providing contacts with other centres and operators in order to facilitate a more effective incident management.
  - Notifying contacts of people inside organisations, with whom there already exists a previous relationship, in case of need.
  - Legislation applicable to Critical Infrastructures Protection in Spain.

4 TYPES OF INCIDENTS

The incident's characteristics determine what actions have to be undertaken to resolve it. In general, the following types of incidents should be considered:

- **Denial of Service:** Incidents related to denial of service attacks (DoS) or distributed denial of service attacks (DDoS). These are very dangerous, since they are able to affect the availability of Strategic Operators' critical systems.
- **Malware infections:** Incidents provoked by malware (viruses, worms, trojans, logic bombs, spyware, rootkits, etc.). The severity of these depends on the malware; they can result in data theft, or can affect system availability. The most complicated aspect here is detection and identification, owing to the incorporation of rootkits.
- **Compromised systems:** Any computer system, piece of hardware or software, which is being or has been successfully attacked. Examples: theft of confidential information, changes in system configurations, etc.
- **Hacking:** Any suspicious activity or traffic which can alter the functioning of a system and which is related to an attempt at intrusion. Examples: attempted unauthorised system access or service scans
- **Malware distribution:** Incidents in which an organisation's public server is used to distribute malware. These incidents put third parties at risk.
- **Policy violations:** Inadequate use of system assets, such as unauthorised scaling of privileges or attempts to circumvent access controls systems.
- **Invasion attacks:** Any kind of attack against authorisations, authentications, permissions, rights over files or interception of email.
- **Vulnerability:** Any type of incident provoked by the exploitation of a system vulnerability.

In addition to these categories, which may be considered common, the evolution of technology and the complexity of attacks mean that other types of incidents will inevitably occur.

5 CONCLUSIONS

This guide has set out the steps that have to be taken in order to identify and manage security incidents. Concretely, the measures to take in the case of an incident are composed of its identification, containment, the preservation of evidence, and legal considerations.

The process to follow in order to report incidents has also been set out, using as a principal form of communication the pic@cert.inteco.es **mailbox**, which communicates with the RTIR (Request Tracker Incident Response) system. The user who reports the incident will include in the reporting email all the information considered necessary, which will in turn be used by the RTIR incidents queue moderator to create a new incident. The general steps that will be followed in the process from the initial reporting of the incident to its resolution are: **receipt** of the user's report, **identification and relevance**, **analysis** of the report, **classification, triage, resolution and closure** of the incident.

In addition, in order to assist in the management and reporting of incidents, a general classification, based on the main characteristics which possible security incidents may present, has been put forward. Concretely, incidents including those of denial of service, malware infection, compromised systems, hacking, invasion attacks and vulnerabilities have been defined.

As a guide for the identification and reporting of security incidents, although specific matters which can only be applied in concrete cases as they develop have been dealt with, the general criteria set out meet the standards of generally recognised best practices for the management of incidents, and, as such, may serve as a reference for the design and implementation of this type of service in other fields.