CCN-CERT

BP/29

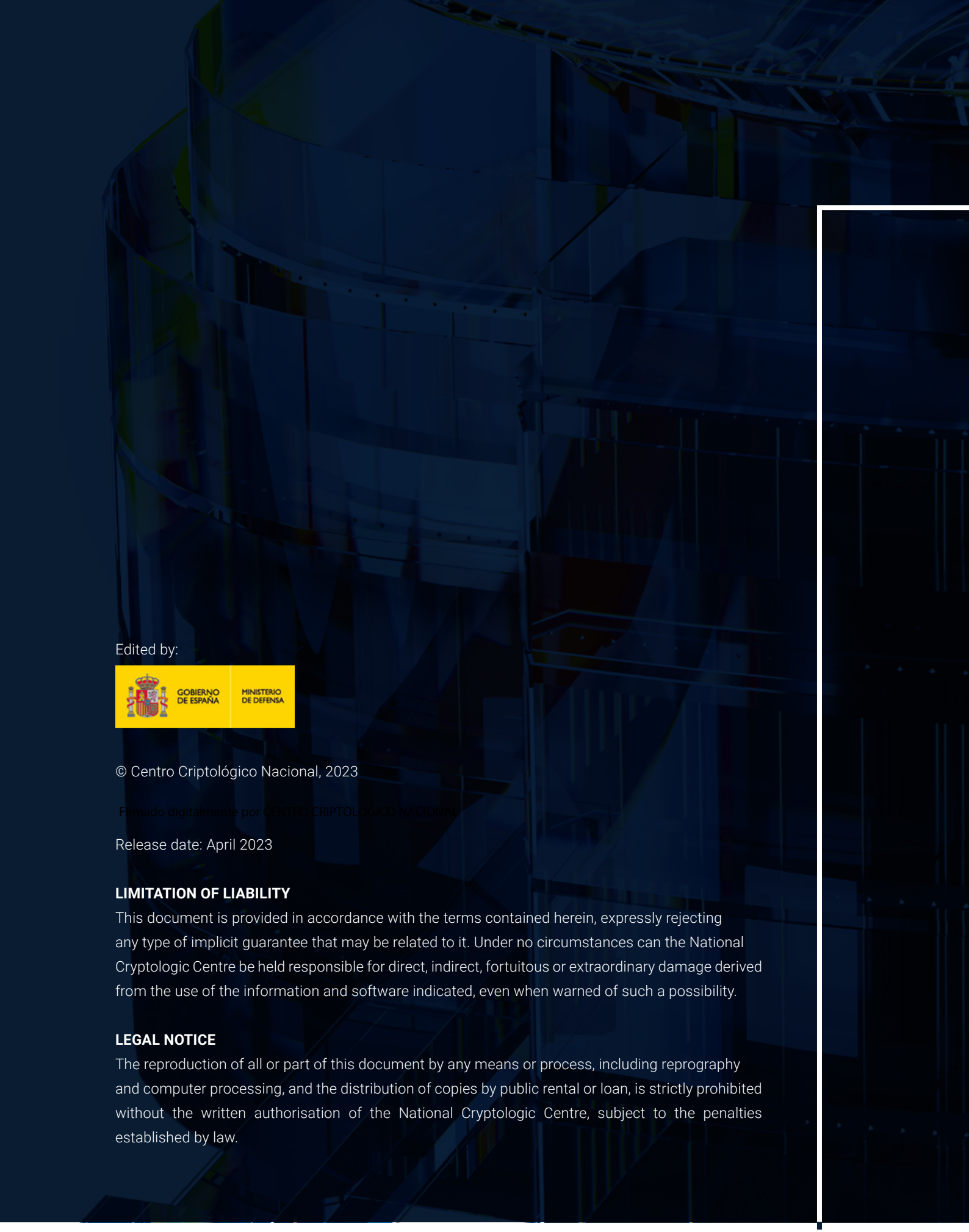
Crisis management for cyberincidents in local administrations

GOOD PRACTICES REPORT

APRIL 2023

ccn-cert centro criptológico nacional

CCN centro criptológico nacional



Edited by:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Release date: April 2023

Index

1. Introduction

We live in an increasingly complex and globalised world, more digitised and technologically dependent, in which cyber-attacks are on the rise. We must be aware of the challenge we face and that local administrations cannot remain aside.

In recent years, local councils, provincial councils, island councils, etc., have implemented measures to make more and more **public services available digitally,** they depend on the internet for daily interactions and transactions, they have a greater number of technological elements, from mobile applications and cloud services, as well as a wide range of electronic devices, staff carry out a large part of their activities telematically...

The increased use of electronic media by our local entities makes it essential to guarantee the protection of their technological capacities, the information processed and the services provided, which, due to their proximity to citizens, must remain fully operational.

Local administrations **are susceptible to a cyber-attack,** it is not a question of if it will happen, but when and whether we will be sufficiently prepared to respond adequately and in an organised manner by then. We cannot be complacent: attackers will continue to try to breach security barriers to steal data, damage systems and/or block administrative management and the provision of services to citizens.

Much progress has been made recently in the field of cybersecurity, the National Security Framework (ENS) has defined principles and requirements, guides have been produced to assist in implementation, security, incident management (the CCN-STIC-800 Series sets out the appropriate policies and procedures for the implementation of the measures contemplated in the National Security Framework),

The growth of digital services in local authorities makes cybersecurity and appropriate cyber crisis management essential. This guide helps to prepare for and respond in an organised manner to a possible cyber-attack.

however, **less work has been done to prepare those responsible for local administrations for the "during".** The crisis management model presented in this Guide is aligned with the National Security Framework (ENS), for its application in local administrations[1] .

Cybersecurity is essential, but **proper cyber-crisis management is also vital for citizens to trust their local councils:** they all need to continuously review, update and strengthen their cybersecurity, but they also need to develop their cyber-crisis management skills.

This document is aimed especially at the offices and governing bodies of local administrations, whether they are elected or civil servants (Mayor, President of the Provincial Council, Deputy Mayors, Local Government Board, Councillors, Communication Officers, Secretaries, Comptrollers and Treasurers).

This Guide is expected to contribute to improve the capacities of local administrations to respond to a relevant and high impact cyber security incident, to manage a cyber crisis and to return to normality with the least consequences for local administrations, citizens and their other stakeholders.

This **preparation** needs to be carried out in order to **build confidence** and provide assurances that, in the event of a cyber crisis, there is readiness to make decisions, to coordinate with all actors involved in the response and to communicate appropriately.

In short, it is intended to be read and taken into consideration by all those who, from the highest levels of government of a local authority, are responsible for making the public administration more secure and reliable and the **response in the event of possible cyber-attacks more efficient and effective.**

1. The National Security Framework (ENS) determines the security policy to be applied in the use of electronic media by public sector entities (and those private sector organisations that provide them with services), being made up of the basic principles and minimum requirements for adequate protection of the information processed and the services provided, of obligatory observance by the entities within its subjective scope of application, to ensure access, integrity, availability, authenticity, confidentiality, traceability and conservation of the data, information and services used in electronic media that they manage in the exercise of their competences.

2. Scope of the guide

The objective of any local authority must be to move towards resilience, understood as the capacity to anticipate, adapt and respond in order to recover the initial state when the disturbance to which it had been subjected has ceased.

Resilience is essential for local entities, which implies the ability to anticipate, adapt and recover from shocks.

This Guide focuses on one of the pillars of resilience: the need to design, develop and implement a crisis management model, which complements the capacities that the local administration has developed in risk prevention, security and continuity of services (see **Figure 1**).

Figure 1. The Pillars of Resilience

On the other hand, a resilient local administration must look at the whole cycle: prevention, preparedness, detection, **response**, recovery and learning. This Guide shows **an approach** to crisis management

when crises occur, i.e. it focuses on the response, the *during* (see **Figure 2**), by focusing on the key elements that need to be prepared in advance and that shape the capacities to respond appropriately to a high-impact incident.

The Guide has **two (2) parts:**

- The first part proposes a **basic organisational model** for managing cyber crises and its key elements:
  - **Crisis Committee:** who should be part of it and what they should do.
  - Roles of the different officers: the **Mayor, President of the Provincial Council, Deputy Mayors, Local Government Board, Councillors, Communications Officer, Secretary, Financial Controller and Treasurer.**
- The second part proposes a **model action protocol in the event of** an incident that may lead to a crisis:
  - Evaluation **criteria**.
  - **Actions** during the different **phases** of crisis governance.

Finally, the contents of this Guide are complemented with examples, lessons learned and best practices in crisis management, the result of the analysis of more than 100 real cases at national and international level and the result of the **lessons shared by local entities that have** recently **experienced** a VERY HIGH or CRITICAL cyber-attack.

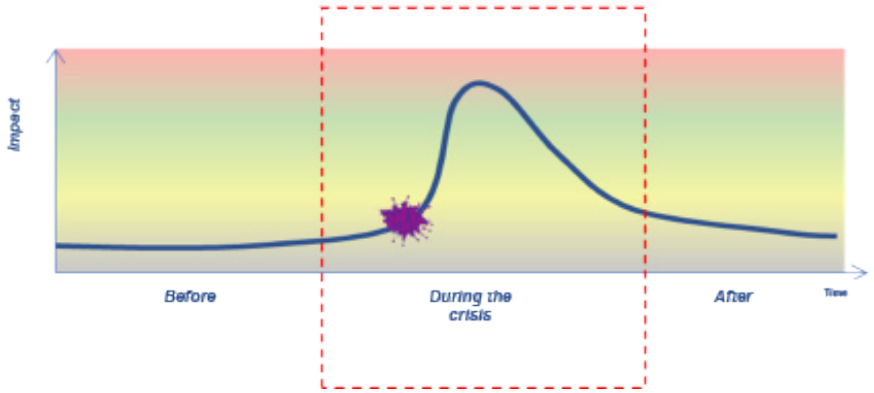


Figure 2 Time cycle of an incident turning into a crisis

2. More information in the report CCN-CERT BP/20 Best practices in Cyber Crisis Management.

2. Scope of the guide

Resources for the implementation of the National Security Framework, CCN 800 Series and reports:

- **Approach to the Cybersecurity Governance Framework (CCN).**
- **Directory of Cybersecurity for Local Authorities, by the Centro Criptológico Nacional (CCN) and the Federación Española de Municipios y Provincias (FEMP).**
- **CCN-STIC 800** Glossary of ENS terms and abbreviations.
- **CCN-STIC-801** Responsibilities and Roles in the ENS.
- **CCN-STIC-802** ENS Audit.
- **CCN-STIC-803** Assessment of Systems in the ENS.
- **CCN-STIC-804 ENS.** Implementation guide.
- **CCN-STIC-805** Information Security Policy.
- **CCN-STIC-806** ENS Compliance Plan.
- **CCN-STIC-808** Verification of compliance with measures in the ENS.
- **CCN-STIC-809** Declaration, certification and provisional approval of conformity with the ENS and compliance marks.
- **CCN-STIC-815** Indicators and metrics in the ENS.
- **CCN-STIC-821** Security Standards in the ENS.
- **CCN-STIC-822** Security Procedures.
- **CCN-STIC-882** Risk Analysis Guide for Local administrations.
- **CCN-STIC-883** ENS Implementation Guide for Local Entities.

2. Scope of the guide

Incident management resources:

- **National Cyber Incident Notification and Management Guide** approved by the National Cyber Security Council.
- **CCN-STIC 817.** National Security Framework. Cyber incident management.

Crisis management resources:

- **CCN-CERT BP/ 20** Best Practices in Cyber Crisis Management.
- **CCN-CERT BP/29** Crisis Management for Cyber Incidents in Local Entities.

I. Crisis Management Organisation:

Basic Model

3. What do we mean by crisis and by cybercrisis?

In a general way, we define **a crisis** as a **low-probability** situation which, when it happens, generates a **large impact** and whose effects **last** over time. These effects produce an impact:

- on the dynamics of the local administration or on the activities it carries out and the services it provides,
- on the reputation and image of the local administration, and
- on citizens in general or on a particular group depending on where the attack took place.

Moreover, crises caused by cyber-incidents **(cyber-crises), deliberate or not, have one characteristic: the local authority** is under **attack**, there are "bad guys" who intentionally and from their advantageous position seek to harm the entity and take advantage of it.

Every crisis involves **decision-making under great pressure,** in a short **time** and probably with **incomplete information**, on several **fronts in parallel** and with many groups and individuals intervening.

In particular, cyber-incident crises are characterised by the time and expertise required for analysis and recovery, and it is often **difficult to manage priorities** between the investigation of the incident and the need for recovery of the services provided by the entity.

Likewise, in this type of crisis it is often difficult to reconcile the different languages and break down the silo culture that usually exists between teams.

It is therefore necessary to have an outline of what the response will look like and who will be involved in it.

3.1. Basic organisational model: crisis committee, technical team and communication team

Regardless of the origin of the crisis, it is clear from the previous definition that its resolution involves a **management component. Therefore,** in any crisis, **two (2)** distinct **spheres of action** are identified (see **Figure 3**):

- **Organisational and strategic** insofar as its impact affects different areas of the local administration (services, attention to citizens, image and reputation, relationship with stakeholders, presence in social networks, etc.) and requires a coordinated response at a high level.

- **Operational and technical response to the incident:** the one which has to do with the reason for the incident and whose immediate effects must be contained and resolved by a specialised response team. Management that falls to an **Incident Response Team (IRT).**

Actions in the organisational and strategic sphere are to be taken primarily by the **Governing Board, which** becomes the core of the **Crisis Committee (CoC)** set up specifically for each crisis.

In addition to these two spheres (technical and management-coordination), communication management must be added and given importance. Crises caused by a cyber-incident usually have a very rapid impact on the media, i.e. they usually have a media component that requires coordinated action between internal and external communication.

In short, the management of a cyber crisis must be **led by the Governing Board, as the Crisis Committee,** which is **supported by two (2)** more technical and specialised **teams** that must be very well coordinated and aligned:

- the Cyber Incident Response Team, which will lead and take the initiative for action.
- the communication officer who, knowing the scope of the situation and the actions taken, will develop his or her communication activity.

This system of committees and teams is a BASIC MODEL whose application will undoubtedly depend **on the size of the local administration in question** and its capacities and resources, but it can be applied to any authority, as all of them have a **government team whose Mayor/ President or President and Local Government Board can constitute a Crisis Committee in case of need.** There is no one better than them to lead the City Council, the Provincial Council or the Cabildo in these moments of uncertainty and to transmit confidence to the public that they are acting appropriately, proportionately and in a coordinated manner.

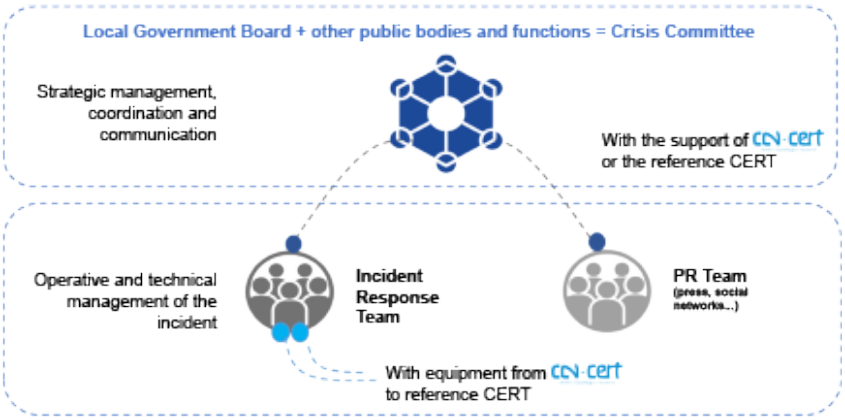


Figure 3. Basic organisational model

When the local administration is large, its size and complexity justify the existence of the Crisis Committee and the different teams, while in small or medium-sized municipalities there may be a single Crisis Team or Committee, or simply defining an action protocol led by the Mayor.

3.1.1. The Crisis Committee

The Cyber Incident Crisis Committee should have **well-defined members** and they should be assigned a role or responsibility in the exercise of their functions within the Crisis Committee.

In order to do this, it is necessary to have previously thought about and defined which managers are needed to cover all the fronts required to manage this type of crisis, which, in some cases, can paralyse everything for weeks or months at a time.

These functions or roles **are to be assigned to councillors, deputies or senior officials** in the institution's organisation chart, which, in turn, will be covered by elected or freely appointed positions, the assignment of which may change.

While their composition may **vary depending on** the nature of the incident or the situation, some roles are **preferably permanent,** such as the chair of the Committee, the coordination of the Committee, and those responsible at operational, communication and legal level.

It is recommended to **create a table with the correspondence** between the roles within the Crisis Committee and the positions that will assume that role in the event that the committee is convened. The table should include the contact details of the persons occupying that position, both incumbents and alternates, and should be constantly updated. In small or medium-sized organisations, some functions or roles may be assumed by the same person.

It is important that the roles of the Committee in general and of its members in particular **have been defined and shared** with its members, in order to align the approach and facilitate the functioning among them. In particular, it is key that the chairperson of the Committee - probably the Mayor or President - has a clear understanding of his or her role, as the leadership of the team and therefore the success of the management will depend to a large extent on him or her.

The composition of the Crisis Committee can be of variable geometry so that the permanent functions are always convened, while the rest depend on the specific characteristics of the crisis in question.

The appropriate organisation to deal with a crisis is not improvised when it arises, and it is therefore **essential to develop it in advance**

in order to have the necessary preparation at that moment. In this sense, it is essential that all of this is predefined in a Plan or Procedure and that this is regularly updated (Incident Response Plan, general or specific Crisis Management Plan for cyber-incidents...).

Anything **that is not foreseen is practically impossible to improvise during the emergency**, which is why one of the keys to effective crisis management is determined by the capacity to anticipate and identify the areas that may become critical situations. A constant foresight exercise is required to be aware of the weaknesses of local entities and thus be able to prepare and anticipate.

Have pre-defined plans and protocols.

In short, the ability to manage a crisis situation **depends to a large extent on the committees** that have been established, their organisation and functions, before the disaster caused by the "low probability, high impact" cyber event occurs.

Figure 4 shows the main roles and functions that should be covered in a Cyber Crisis Committee[3].

Figure 4. Composition of the Crisis Committee of the BASIC MODEL

3.1.2. Functions of the Crisis Committee

In the BASIC MODEL proposed in this Guide, the Governing Board, in whole or in part, **constitutes the core of the Crisis Committee** for the resolution of incidents that have been qualified as a crisis.

Indeed, the Governing Board is the body in which crisis management is built at a high level within the local authority, which provides greater capacity for a 360º and strategic vision, while at the same time having a greater capacity for dialogue and for mobilising extraordinary resources, if necessary.

It is the body responsible for **taking the decisions and coordinating** the actions necessary for the resolution of incidents that have been classified as crises, on all management fronts:

- Assuming responsibility for dialogue and communication with all affected and interested parties (citizens, the media, the City Council itself in plenary session...).

3. The positions mentioned are, mutatis mutandis, equally applicable to the Provincial Councils, Island Councils, etc.

The main roles and responsibilities of the Crisis Committee, mainly composed of the members of the Governing Board, are:

- Understanding the state of play and forecasting scenarios:
  - evaluate all information received about the incident, make an initial assessment of its impact (actual or potential) and the consequences on the affected local administration, its services and stakeholders,
  - keep a forecast of the potential impact and consequences for the organisation, considering the emerging risks and the scenarios towards which they may evolve in order to be able to undertake anticipatory measures.
- Coordinate and prioritise actions for their resolution and return to normality:
  - Determine and/or validate and monitor the strategies and measures previously implemented and/or proposed by the Incident Response Team IRT (for analysis, containment, mitigation and recovery of equipment, services, information...).
  - Determine priorities to recover activities and services in the shortest possible time, minimising impacts on stakeholders.
  - To support the technical response team, which is under a lot of stress and probably with little time for rest.
  - Activate the mobilisation of extraordinary resources when necessary.
  - Follow up on open points, e.g. by means of a "Cyber Attack Diary" document listing of relevant information regarding the daily management, the measures taken and the status (with time and date), and Action Plan tasks (with responsible persons and timeframe).
  - Act as an information reference centre during the incident response and subsequent recovery, both to internal and external actors involved in or concerned by the incident.
- Define positioning and direct internal and external communication:
  - Define the internal and external communication strategy: taking into account the service function of the local administration, the values of the elected government team and the need to ensure that trust, reputation and image as well as security are safeguarded.

- Assume responsibility for communication and ensure relations and dialogue with all affected and interested parties (citizens, media, the City Council in plenary session...).
- Designate the spokesperson and prepare him or her for the many occasions when it will be difficult to respond to requests for information...
- Ensure that the Communication Team carries out the communication measures previously designed, whether in the media, social networks, associative frameworks, etc.

Coordinate post-incident analysis actions:

- Extract lessons learned and points for improvement.
- Ensure that the resulting Action Plan is implemented.

4. Public decision makers in cyber-incident crisis management

In this proposed BASIC MODEL, it is worth highlighting the roles of the main public decision-makers.

4.1. Necessary organs

The first thing to point out is that, in the case of local councils, **the municipal government and administration**, except in those municipalities that legally operate under the Open Council system, **corresponds to the Town Council,** made up of the **Mayor and the Councillors of the Government Team.**

Mayor

Deputy Mayors

The Plenary

The Local Government Board

In municipalities with a population of more than 5,000 inhabitants, as well as in those with fewer than 5,000 inhabitants, when so stipulated in their organic regulations or agreed by the Plenary Session of their Town Council.

4.1.1. The Mayor

The Mayor is the president of the Local Agency and, among other attributions and, insofar as they may be applicable to the security of the information processed and the services provided by the entity, the **following functions and responsibilities** may be highlighted:

- To direct the municipal government and administration and, within the framework of the Organic Regulations, the organisation of the administrative services of the Local Agency, which also includes the governance of information security and crises caused, in this case, by a cyber-incident.
- To convene and chair the meetings of the **Local Government Board, the structure of which shall form the basis, in whole or in part,** of the Crisis Committee:
  - activate and deactivate the Crisis Committee.
  - designate other members from outside the Local Governing Board to join the Crisis Committee (whether they are council staff, members of the Information Security Committee, those responsible for Information, Services, System or Security, according to the National Security Framework, or other elected officials or external bodies necessary for the resolution of the cyber incident).
  - to steer the dynamics of the Crisis Committee.
- Assuming high-level interlocution and **representing the City Council**, also before the competent public entities in cybersecurity matters (for example, when ordering the notification of a security incident with significant impact) or before private entities (for example, encouraging, from its position as the highest representative of the institution, that the technicians responsible for the entity ensure that the information systems of the suppliers that provide services to the local authority are compliant with the provisions of the National Security Framework).
- **To convene and chair the meetings** of the Plenary and of any other municipal bodies to which he/she must keep duly informed of the situation and of the main actions being carried out.
- The **approval of extraordinary measures, projects and services** (when it is competent to contract or grant them) necessary and urgent for the prompt resolution of the incident.
- To oversee the data as the ultimate data controller in the Register of Processing established by the AEPD.

It should be remembered that the Mayor may **delegate powers to the Local Government Board (when it forms the Crisis Committee)**, as a collegiate body, so that the resolutions adopted by the latter in relation to the delegated matters will have the same value as the resolutions issued by the Mayor in the exercise of the powers that have not been delegated, without prejudice to their adoption in accordance with the rules of operation of the Local Government Board.

The Mayor may make so-called generic delegations in matters that he/she considers necessary for the resolution of the incident (e.g. those relating to the security of the entity's information systems) and may make special delegations to any councillor.

4.1.2. Deputy Mayor

The deputy mayors, who are appointed by the Mayor, replace the Mayor, in the order of their appointment and in cases of vacancy, absence or illness, and are freely appointed and removed by the Mayor from among the members of the Local Government Board and, where there is no Local Government Board, from among the councillors:

- **Deputising for** the Mayor in his role of chairing the Governing Board - Crisis Committee - during the crisis.

The Mayor may delegate the exercise of certain powers to the members of the Local Government Board (when it constitutes the Crisis Committee), and, where this does not exist, to the deputy mayors, without prejudice to the special delegations that, for specific tasks, may be made in favour of any councillors.

4.1.3. The Plenary

The Plenary is made up of all the Councillors (government team and opposition councillors) and is chaired by the Mayor.

Among other powers of the Plenary, and insofar as they may be applicable to cyber-incident crisis management, the following functions and responsibilities may be highlighted:

- **Ensure that it is duly informed** by appealing to the **sense of responsibility** that a cyber-attack requires, especially if it has caused damage to the activities and services provided by the City Council, or if there has been a breach of personal data, etc.

During the days or weeks that the management and resolution of a cyber-attack lasts, it is desirable that the Plenary trusts the Mayor and the Local Government Board, in its capacity as Crisis Committee, encouraging the Local Government Board to determine the extraordinary resources that may be necessary, with the particularities that correspond to the regulations applicable to large municipalities.

4.1.4. Local Government Board

Although the decisions and competences vary according to the regime of the municipality (large or not), for most of them the Local Government Board is composed of the Mayor, who chairs it, and a number of councillors freely appointed by him as members of the Local Government Board, which may not exceed one third of the legal number of members of the Local Agency.

The Governing Board must **be informed of all decisions of the Mayor,** prior to the adoption of the decision, whenever the importance of the matter so requires, and it is therefore especially necessary that they be part of the Crisis Committee as permanent members and that they meet. When there is a crisis, it is time to meet.

Thus, in the BASIC MODEL proposed in this Guide, the **Governing Board constitutes the essential backbone of the Crisis Committee** for the resolution of incidents that have been classified as a crisis, being the body in charge of high-level crisis management within the City Council that provides a strategic and 360º vision, while having a greater capacity for dialogue and for mobilising extraordinary resources, if necessary (see Crisis Committee section).

The Local Government Board has the following functions and responsibilities:

- They are permanent members of the Crisis Committee and therefore the main functions and responsibilities of the Governing Board are those of the Crisis Committee.
- **Permanent assistance to the Mayor** in the exercise of his powers and, consequently, as chairman of the Crisis Committee.
- Other powers delegated to it by the Mayor or the Plenary or attributed to it by law.

4.2. Complementary bodies

Depending on the population of the municipality, there are other complementary bodies whose responsibility should be highlighted for the duration of a cyber-attack: the councillors.

4.2.1. Councillors

Councillors in their capacity as heads of specific areas or departments are primarily responsible for the continuity of the activities and services provided by the council or local administration concerned.

Thus, during a cyber-attack, their main roles and responsibilities are:

- Provide **information and analysis of the affected areas** and the repercussions on assets, services, citizenship, ...
- **Coordinate actions,** teams and response plans for disrupted activities, continuity plans if any, ...
- Identify, **mobilise and organise the necessary resources** to try to maintain activities and service delivery, even if in a smaller way while the Incident Response Team is working towards the full recovery of systems and/or information, i.e. while the return to normality work is ongoing.

4.3. Public functions of nationally empowered persons: secretaries and financial controllers

These are necessary public functions in all local local agencies, whose administrative responsibility is reserved to Local Administration officials with national qualification:

Secretariat

Intervention

4.3.1. The Secretaries

In all local administrations there is a post called Secretary's Office, which is responsible for the administrative responsibility of the functions of public faith and mandatory legal advice with the scope and content provided for in the legal system.

Of the powers that fall within the public function of the Secretariat and as they may apply to the security of the information and services provided by the entity in the event of a crisis caused by a cyber incident, the following roles and responsibilities can be highlighted:

Regarding public faith:

- To prepare the items to be included on the **agenda of the meetings of** the Plenary, the Governing Board and the Crisis Committee.
- Attending and taking **minutes** of the meetings.
- Compile the **information and decisions taken:** transcribe into the **resolution book** those related to the incident and also those derived from the post-incident/ crisis analysis and its consequent improvement plan.
- Acting as a notary public in the formalisation of contracts, agreements and similar documents in which the local administration is involved, such as those signed with third party providers - public or private - of services aimed at guaranteeing the resolution of the incident affecting the local administration.
- To arrange for the **publication**, when mandatory and insofar as the cyber-attack allows, of the acts and agreements of the local authority in the official means of publicity, on the notice board and in the electronic office.
- To manage the **registry and archiving** of the local administration, including, in circumstances where cyber-attack permits, ensuring the availability of electronic files and the confidentiality, integrity, traceability and authenticity of the information contained therein.

Regarding legal advice:

- The issuing of prior reports in those cases in which this is ordered by the President or Mayor of the Local Agency or when requested by one third of the members of the Local Agency. Such reports must indicate the applicable legislation in each case and the compliance of the agreements in question with it. This would be the case, for example, of those reports relating to actions or initiatives related to the security of the entity's information.
- The issuing of prior reports whenever a legal or regulatory precept so provides or the issuing of a prior report whenever it matters for the approval of which an absolute majority of the legal number of members of the Municipal Agency or any other qualified majority is required.
- Issue reports when so provided for in sectoral legislation.
- To report at the meetings of the collegiate bodies that it attends and when expressly requested to do so by the person presiding, on the legal aspects of the matter under discussion, in order to collaborate in the legal correctness of the decisions to be adopted during the management and resolution of the cyber-incident.

4.3.2. The Financial Controllers

In Local administrations whose secretariat is classified as first or second class, there shall be a post called Financial Controller.

The internal control of the economic-financial and budgetary management includes during management and resolution, taking into account that it may require the extraordinary dedication of unforeseen economic resources.

Taking into account the exceptional conditions caused by a cyber-crisis and bearing in mind that financial resources may be needed in a hurry, the functions and responsibilities are:

- The **supervisory** function.
- **Financial control** (permanent control and public audit, both of which include efficiency control) will include the control actions attributed in the legal system to the financial control body required for the management and resolution of the cyber incident.
- The issuing of reports, opinions and proposals on economic-financial or budgetary matters that may be required during the management of the incident.

The accounting function comprises, among others:

- Organise an adequate archiving and conservation system for all the documentation and accounting information of the cyber incident to enable an economic analysis to be carried out:
  - of both the impact and the cost of the crisis, and
  - to the extent possible to draw the lessons learned on the benefit of investing in security or the impact of "delayed action".

4.4. Other figures to be included in the Crisis Committee

The BASIC MODEL proposed in this Guide proposes to integrate other local administration functions for an agile and effective response during the crisis:

- **Head of the area of information and communication technologies / information systems / IT / new technologies**
- **Head of communication**
- **Head of data / data protection**
- **Incident Response Team**

4.4.1. Responsible for Information and Communication Technologies, Information Systems

All cybersecurity incidents must have an incident manager assigned to them, and this responsibility may fall to different positions depending on the size and organisation of the local administration in question. This role is generally assumed by the person in charge of the Information and Communication Technologies, Information Systems, IT, New Technologies or, in the terminology of the National Security Framework: the System Administrator.

In any case, it is necessary to define an operational manager or incident manager, who will assume the functions related to the actual technical management of information security, cybersecurity, systems and technologies.

Specifically, your duties will be:

- Define, establish and monitor the Action Plan for the containment, eradication and recovery of breached networks, equipment and/or systems.
- To be **the liaison between the Crisis Committee and the Technical** Incident Response Team, playing a key role as **interpreter** between the two spheres of the City Council or local administration. This is the person on whom the Mayor and his team will rely to understand what is happening.
- Coordinate the Incident Response Team for the development of activities necessary for the containment, eradication and recovery of the cyber incident.
- Prepare and channel information on the state of play and the ongoing and planned Action Plan.
- Ensure the legal validity of evidence.

4.4.2. Head of Communication

Bearing in mind that communication is one of the axes of the management that the local authority must assume, in this organisational BASIC MODEL it is necessary to add the need to coordinate everything related to communication through **a person in charge who can be supported by a specific** Communication **team**.

Its main functions and responsibilities are:

- Define the external and internal and stakeholder Communication Plan.
- Manage media relations, channels, social networks, etc.
- Coordinate the Communication Team.
- Define external and internal communication messages.
- Monitor the information available in media, channels and social networks that may have an impact on the entity.
- Assist the spokesperson.
- Ensuring internal communication: Instructions.
- Ensure proactivity in relation to stakeholders, taking into account the context and their expectations (citizens, service users, suppliers, etc.).
- Ensure that what is communicated to local administration staff is perfectly aligned with the messages and explanations to the outside world.

4.4.3. Data Protection Officer (DPD)

Another of the key figures during the management of a cyber incident that has caused a crisis in the municipality is the Data Protection Officer (DPO). Current legislation establishes the presence of a DPO as mandatory. In certain cases, this figure may be delegated to a supra-municipal entity, from where the DPO service is provided (externally) or even to a private entity.

The essential functions of the DPO shall be to

- In the case of a cyber incident involving personal data, you must initiate the incident file with the Supervisory Authority within 72 hours of the incident and take responsibility for the incident until its completion.
- Inform and advise the Controller (Crisis Committee) or the Processor and the staff in charge of the processing of the obligations incumbent upon them by virtue of the Data Protection regulations in force.
- Supervise compliance with the provisions of current Data Protection legislation and the policies of the Controller or Processor, including the allocation of responsibilities, awareness and training of staff involved in processing operations, and related audits.
- Provide advice as requested on the data protection impact assessment and monitor its implementation in accordance with Article 35 of the GDPR.
- Cooperate with the supervisory authority (AEPD or Autonomous Data Protection Agencies).
- Act as a contact point for the supervisory authority for matters relating to processing, including prior consultation as referred to in Article 36 of the GDPR, and consult, as appropriate, on any other matter.

4.4.4. Incident Response Team

The Incident Response Team is the operational team and represents the tactical level of cyber incident management. It is the body in charge of **preventing, managing and** effectively **responding** to IT security incidents and carrying out actions aimed at the containment, eradication and recovery of breached networks, equipment and/or systems.

These teams are usually led by the System Administrator and consist of a group of experts who act according to predefined procedures and policies; experts in both preventive measures and in response measures to IT events/incidents and may be part of the local authority or a subcontracted team from a cybersecurity company.

The Incident Response Team will be responsible for identifying and classifying the level to which the incident will be assigned, using the classification criteria shown above, and responding quickly by implementing mitigation, containment, eradication and recovery measures.

It is advisable to have a reporting system (which will have been built within the preventive actions) to inform the top management of the local council or entity (the Governing Board) of any incident with a certain impact (potential or real), so as to ensure that the management team is aware of significant events and, therefore, can activate additional measures to those already taken by the operational layer.

Keeping the exposure area under control through safety diagnostics

4. Public decision-makers in cyber-incident crisis management

Within the framework of this Guide, the following three (3) functions should be highlighted:

- Communicate and coordinate with the National Cryptologic Centre or the reference CERT regarding security incidents considered as HIGH, VERY HIGH or CRITICAL.
- Ensure effective, efficient and secure investigation and cooperation with the National Cryptologic Centre or CERT of reference in case of a cyber incident.
- Coordinate and collaborate through the National Cryptologic Centre or reference CERT with other Incident Response Teams, if appropriate.

A key element in incident management is to subject pre-established plans, procedures and configurations to ongoing testing and verification, which will allow the assessment of the entities' exposure surface, identifying vulnerabilities, security gaps and configuration deficiencies associated with their services and applications.

II. Action Protocol:

Basic Model

5. From incident management to crisis management

The management of crises caused by cyber incidents must consider the specific characteristics of this type of event:

Cyber incident management should consider regulations, specialised bodies and phases.

- The threat can go far beyond the municipality or local administration.
- The existence of mandatory regulations to be followed in these circumstances, such as those relating to data protection.
- The involvement of public bodies specialised in the field - the CCN-CERT, in the case of public sector entities - which exercise constant vigilance and provide technical and operational support, both in the detection stages and in the reaction, containment, mitigation and recovery stages. In relation to local entities, they can provide technical solutions or even specialised technical staff to be integrated in the Incident Response Team and/or advise the Crisis Committee.

Taking into account these contextual conditions, this Guide proposes a sequence in four (4) stages or phases (**Figure 5**) with the objective of ensuring that certain incidents **are quickly escalated internally** and reach the decision-making level where they will be evaluated in order to determine whether they should be referred to the Crisis Committee to take control of the situation.

ICT Security Guide **CCN-STIC 817.** National Security Scheme. **Cyber incident management.**

Cyber Incident Crisis Management Guide for **Local Authorities**

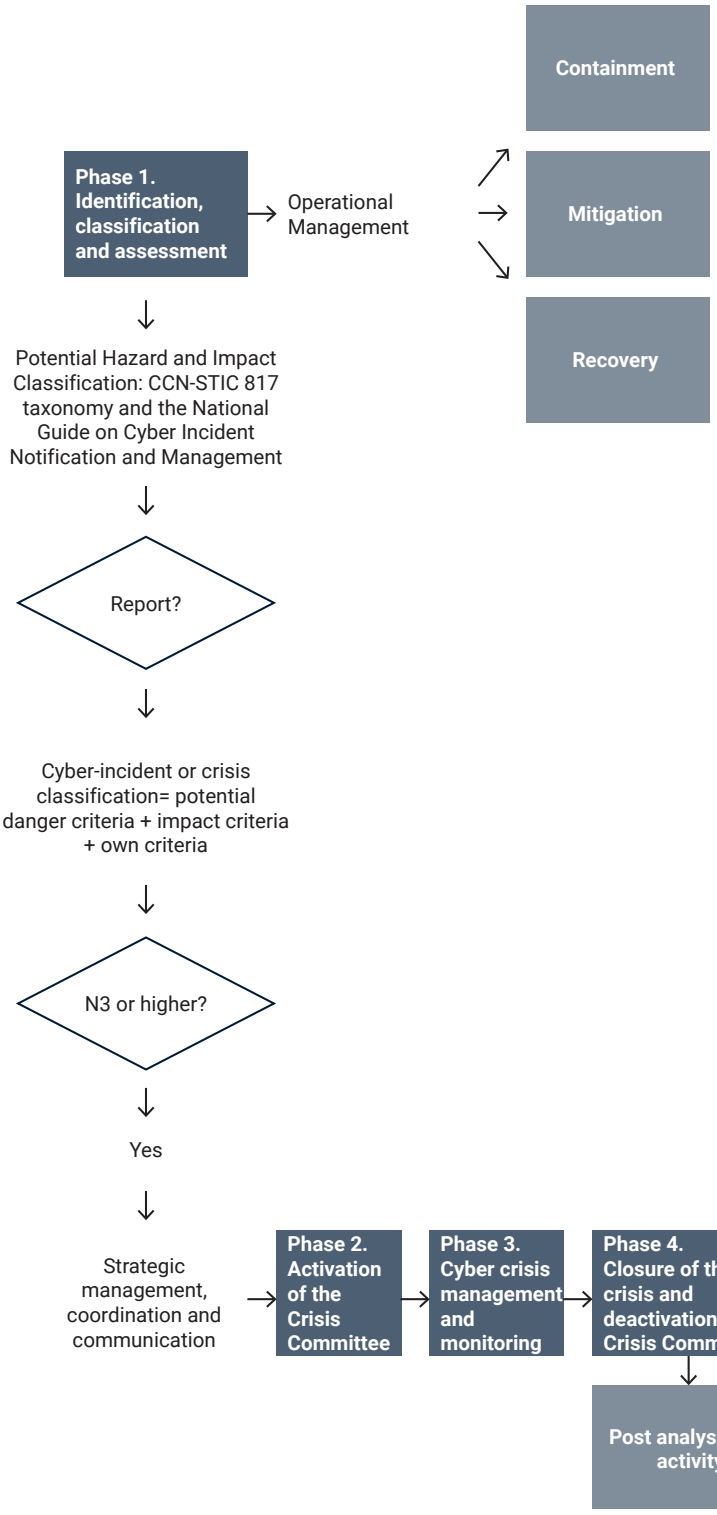


Figure 5. Phases of incident management in case it can be classified as a crisis

5. From incident management to crisis management

The chronological and natural order of crisis management, by virtue of the above phases, should allow:

- Address a **wide range of cyber incidents** that can be detected through different mechanisms internal and external to the local authority, and which need to be escalated and reported promptly to whomever is determined.
- Conduct the assessment using the defined criteria and classify the incident at a certain level of hazard and impact.
- **Activate the Crisis Committee**, to ensure adequate high-level decision-making and global vision in the local authority for the coordination of all technical actions (for resolution and return to normality), communication and attention to stakeholders, etc.
- Ensure that **existing operational plans** (information security, communication, business continuity, etc.) are **activated** or that they are designed ad-hoc according to the type of cyber incident.

As shown in **Figure 5**, the first step in dealing with a cyber incident is to perform a rapid initial classification and assessment to determine its nature and possible magnitude in order to correctly orientate the strategy to be followed.

In this sense, it is advisable to consider the provisions of the National Guide for Notification and Management of Cyberincidents and the ICT Security Guide CCN-STIC 817 when detecting a cyber incident. Likewise, it must be possible to apply the local authority's own criteria to assess the level of the emergency and the advisability of activating the Crisis Committee, so that it can lead the response on all fronts, coordinating all the people responsible/teams involved, including the incident response team itself.

Each of the phases of incident management is developed below, providing general guidelines and basic resources so that each local administration can adapt it to its circumstances.

6. Phase 1. Incident identification, classification and assessment

The cyber-attack finds the local authority focused on its day-to-day duties, yet it has to move quickly from its usual priorities to the crisis situation, without losing time that would give the attackers an advantage by not ensuring the rapid intervention of the reference CERT.

This is why it is so important that, at the first warning of a crisis, the organisation reacts quickly and forcefully by making an initial notification without undue delay and takes the initiative. It is therefore a matter of the local administration being proactive rather than reactive, making decisions quickly and positioning itself to take the lead in crisis management.

When a cyber-security incident is detected, there is no time to lose, but given the pressure and stress of a cyber-attack, it is advisable **not to improvise,** and therefore everything that has been planned in advance facilitates the necessary speed of action.

In this sense, **it is essential to have designed a detailed procedure to follow** if an incident occurs. For the purposes of this Guide, **it is assumed** that the local administration staff, when they become aware of the incident, will know how to escalate it to the person(s) identified internally, providing the necessary incident information for analysis, classification and notification to the reference CERT, if appropriate.

Cyber-attack requires rapid reaction and initial notification to lead crisis management. Classification of incidents important to activate Crisis Committee.

Take initiative and be proactive on the basis of established prevention mechanisms.

In this regard, it is essential to have previously defined an escalation protocol once it has been detected and an incident classification scheme based on the guidelines of the reference CERTs.

This scheme should **include levels of** potential hazard and impact, and should therefore include the **criteria for** hazard **classification and** impact **assessment** to place the incident at a certain level, thus facilitating rapid decision making in the early stages while helping to discern whether it is a crisis and therefore whether it will be appropriate to activate the relevant Crisis Committee.

The CCN-STIC 817 Incident Management Guide and the National Cyber Incident Notification and Management Guide (see **Figure 6**) provide a taxonomy and levels of danger that serve, in the first place, to clarify the obligatory nature of notification, but can also serve to guide whether or not it is appropriate to activate the Crisis Committee:

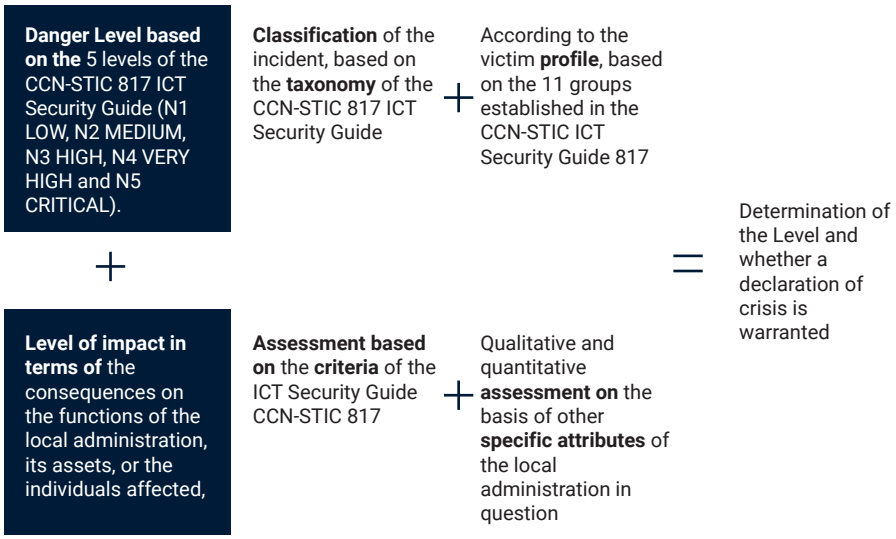


Figure 6. Guidelines for incident level determination and crisis declaration

Each entity should **develop its own table** and introduce specific concepts or attributes in order to facilitate the early classification of incidents. The more that are included, the better the scaling can be, but at the same time, the more difficult it will be to achieve. The table is intended to be a facilitating tool, but a perfectionist eagerness in its definition must be avoided so that it does not become a limitation that impedes progress.

Below are the evaluation criteria that can serve as a **reference**, taking as a starting point those established in the CCN-STIC 817 ICT Security Guide, to which are added, by way of suggestion, other possible concepts to be considered by local entities (see **Table 1**).

Source	Attribute / criterion
CCN-STIC 817	Affecting national security
	Affecting public safety
	Impact on critical infrastructure/essential service
	Affecting systems
	Service interruption
	Resources in person days
	Economic impact
	Geographical coverage
	Reputational impact
Other attributes that may be considered by the local administration	Affecting critical systems, processes or services, e.g. if they are critical by law.
	Affecting certain groups, for example, if it is a vulnerable group, ...
	Possible social alarm
	Impact on public security (e.g. if there has been theft of sensitive information...).

Source	Attribute / criterion
Other attributes that may be considered by the local administration	Affecting stakeholder relations and confidence
	Damage to third parties / environment
	Legal and contractual implications
	Timeliness criterion: depending on the day or time of the year when the incident occurred, e.g. if it is the period of a special campaign such as tax payment, school enrolment, elections,
	Others...

Table 1 . Criteria for assessing and classifying a cyber incident

The assessment and classification will be carried out by people with a cross-cutting vision and the ability to assess the scope and seriousness of the situation from different perspectives, based on the criteria adopted by the local administration. Thus, the person responsible for classifying an incident can be an individual or a small committee with knowledge of both cybersecurity aspects and of the organisation itself and the potential impact that the cyber-attack may have on it. For this purpose, it may be useful if the person(s) responsible for the assessment of the incident and its impact are the same as those who were assigned the responsibility for the information and services, in the terminology of the National Security Framework.

A case: Castellón City Council (I)

Castellón City Council detected a cyber-incident on 30 March 2021 that rendered its computer systems inoperative, notifying the City Council's management and carrying out a diagnostic phase by the Modernisation Department, which determined that it was a case of ransomware.

A work plan was created to restore normality in the IT Department and the CCN and CSIRT-CV were notified and travelled to Castellón to deal with the attack and mitigate the infection.

6.1. The importance of reporting

Bearing in mind that crises are not only the events that are happening but also **the way in which they are managed**, and bearing in mind that the first stages are often decisive, it is worth recalling now what the National Guide on Notification and Management of Cyber Incidents and the ICT Security Guide CCN-STIC 817 of the National Security Framework establishes in relation to notifications.

After determining the level of danger and impact of the cyber incident, the incident must be notified to the competent authority through the reference CERT in order to establish direct communication. In the case of public sector entities, cyber incidents must be notified to the CCN-CERT, if the level determined is HIGH (Level 3), VERY HIGH (Level 4) or CRITICAL (Level 5).

This notification can be made either through the e-mail address **"incidentes@ccn-cert.cni.es"**, including a detailed description of the incident, or, better, through the LUCIA tool (see CCN-STIC- 845 - User's Manual), containing:

- Collection of all relevant information concerning the incident.
- Document the incident and the actions taken so far by the Incident Response Team.

A model protocol for the data to be provided by the body concerned is set out in **Annex 1.**

The mandatory procedure for operators of essential services **is also highly recommended for local administrations as** it ensures rapid reaction, immediate availability of specialised response resources and early warning to other organisations that may also be affected. In particular, operators of essential services have to notify the respective competent authority, via the reference CSIRT, of incidents that may have a significant impact on these services and it is mandatory to report **the incident at least three (3) times** (see **Table 2**).

Operators shall make a first notification without undue delay as soon as sufficient information is available within 48 hours of becoming aware of the event. In addition, intermediate notifications shall be made as necessary to update the incident and its evolution until it is resolved, and a final notification shall be made after its resolution, providing details of the evolution of the event, the assessment of the likelihood of its recurrence and the corrective measures envisaged.

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

Table 2. Incident notification criteria according to the ICT Security Guide CCN-STIC 817

The CCN-CERT, in collaboration with INCIBE-CERT and ESPDEF-CERT, makes the **National Platform for Notification and Monitoring of Cyber Incidents** available to all the actors involved. This platform, based on the LUCÍA tool (Unified Incident and Threat Coordination List) allows the exchange of information and the monitoring of incidents between the operators of essential services or digital service providers, the competent authorities and reference CSIRTs in a secure and reliable manner, without prejudice to the specific requirements that apply in terms of personal data protection.

6.2. Action protocol: management and dialogue with the attacker

This is a key point to consider during cyber incident management, e.g. in case of ransomware.

As a general rule:

- the victim should not engage in dialogue with the attacker.
- the victim is recommended to file a complaint with the Law Enforcement Agencies (National Police, Guardia Civil or regional police).
- actions by the competent authorities:
  - FCSE (National Police, Guardia Civil or others): if the FCSE have been informed, they will act at their discretion, informing the entity also in case of dialogue with the attacker.
  - CCN-CERT or reference CSIRT: will act according to its criteria and practice, informing the entity in case of dialogue with the attacker, and if necessary sharing findings with other possible actors in the investigation.
- If the above-mentioned actions of the competent authorities result in any harm to the victim, the authority in question will take the necessary actions to restore or remedy the problem caused.

6.3. Incident response support

The determination of the actions to be taken for crisis management in the event of a cyber **incident includes the incident response support service based on the** identification and implementation of a strategy and measures for the management, containment and development of continuous improvement activities through the **use of automated reference tasks (playbooks) to support** the affected local authority.

Use of playbooks for the development of cyber incident planning, detection and response activities to minimise the impact of cyber incidents.

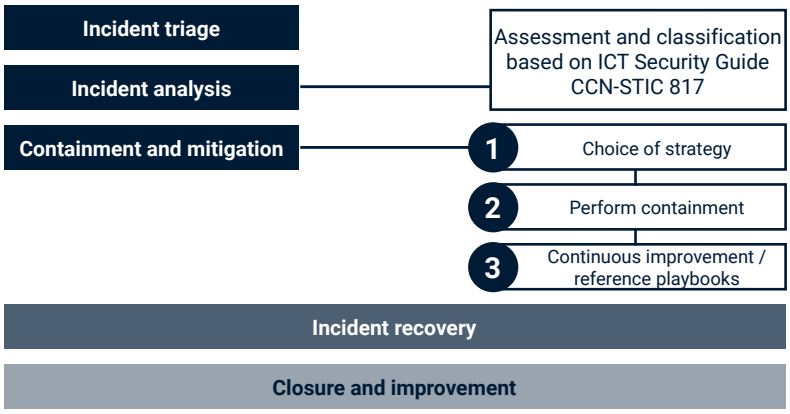


Figure 7 Incident Response Support Service Activities

As shown in Figure 7, **the triage** and **analysis of the incident** are the first activities that the local authority must carry out to determine the status of the cyber incident and identify its criticality. Regarding the containment and mitigation activity, the **response support service must contemplate the development of three (3) actions:**

- **Choice of strategy and selection of the applicable playbook** based on the analysis and characteristics of the incident. In the absence of a playbook associated with the management and containment of the incident, measures to contain and mitigate the impact must be identified and prepared.
- **Conduct containment in accordance with** the applicable playbook or, if not available, through the measures identified in the previous activity, including

the collection of evidence, documentation of activities performed and results obtained, in order to close the incident or to share findings with other possible actors in the investigation.

Continuous improvement of containment activities by updating and developing reference **playbooks based on** experience and results obtained during the incident response.

The **response service** will then imply that the playbooks are periodically updated by a multidisciplinary team within the entity to reflect changes in the context of the organisation in terms of controls implemented, services and technologies used, and integration of roles and responsibilities for incident handling, among others.

The playbooks should be updated periodically to reflect changes in the local administration context.

As shown in Figure 8, the development of **playbooks** should involve **three (3) stages: Planning, Detection and Response** for the determination of specific activities leading to effective incident analysis, detection and response.

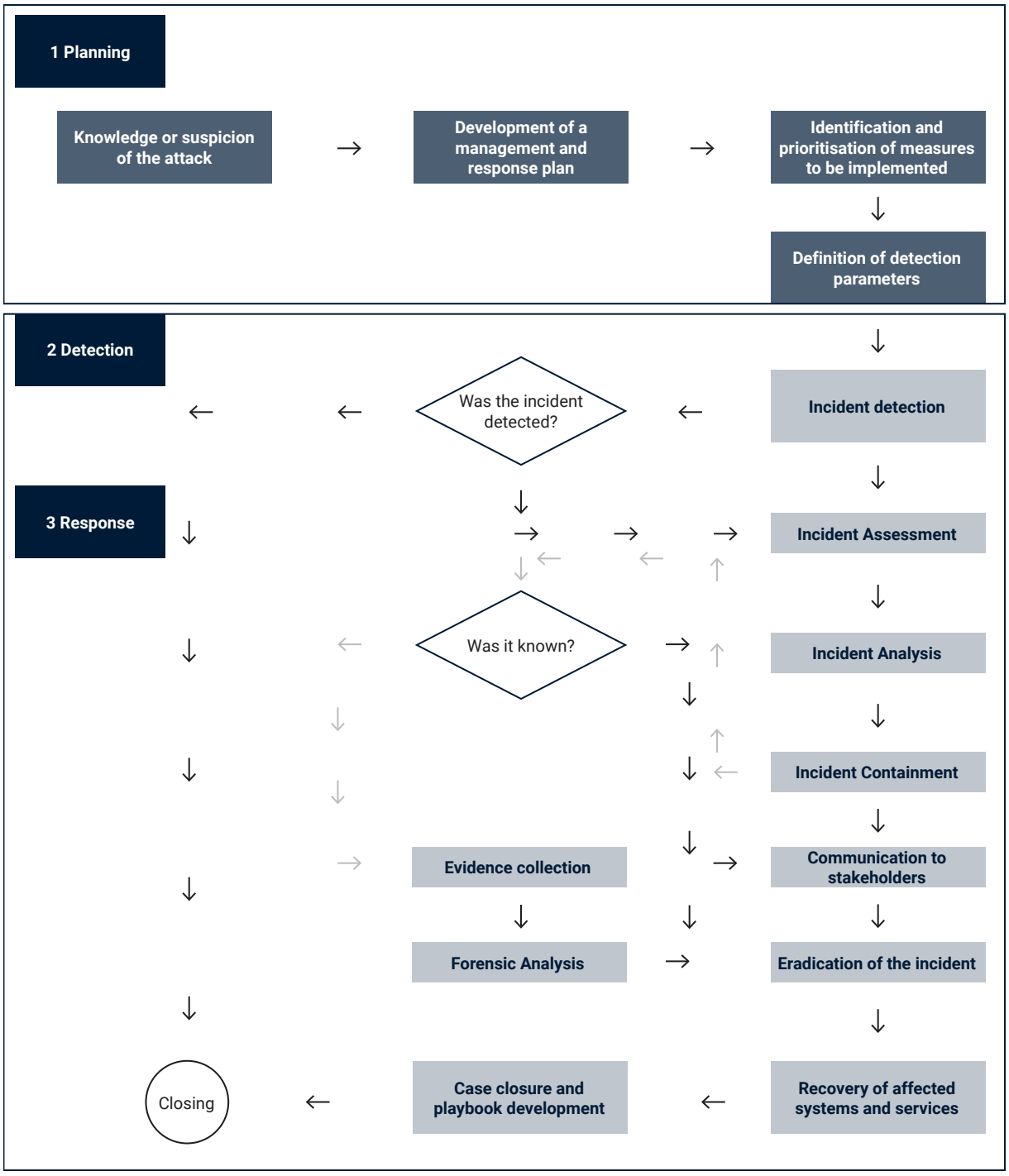


Figure 8 Stages and activities for playbook development

Taking into account the three (3) stages for the elaboration of playbooks, it is proposed to take as a basis for the management of cyber-incidents related to **data breaches, denial of service, malware and insider attacks** the playbooks annexed to this Guide.

7. Phase 2. Activation of the crisis committee

Continuing with the general flow of the event, once the incident has been detected and the first assessment has been carried out, the initial notification and consultation of the criteria defined in the classification and evaluation table, which also serve as escalation criteria, the crisis management mechanisms themselves will be set in motion.

Crisis management protocol: activation of the Crisis Committee according to level of danger and impact. Procedure for activation and development of defined meetings.

The decision to activate the local administration's Crisis Committee can be difficult in the early stages of an incident, as the level of stress and uncertainty about the incident itself means that it is not always obvious whether to escalate it to the government team. Experience shows that there may be several reasons for this:

- People tend to avoid conveying bad news, which seems catastrophic.
- Often there is an excess of voluntarism in thinking that it can be solved before it is reported to higher levels.
- There is a tendency to think that these higher instances can be an interference in the resolution and that their involvement is not necessary....
- Etc.

7. Phase 2. Activation of the crisis committee

It is therefore advisable for the local administration to have established the incident escalation protocol and the level at which the Crisis Committee is activated. In this sense, the determination of the Danger and Impact Level is key to determine whether it is appropriate to declare a crisis and, consequently, whether it is appropriate to activate the Crisis Committee:

- At first, Level 1 LOW and Level 2 MEDIUM incidents should not require the convening of the Crisis Committee as such. It will be the organisation, under the direct responsibility of the Information Security Officer, and the Incident Response Team that will be competent to solve the problem from an operational point of view: either because they have sufficient technical knowledge or with the help of the reference CSIRT teams.
- If the incident is Level 3 HIGH it would be optional.
- If the incident is a VERY HIGH Level 4 or a CRITICAL Level 5, a crisis declaration is considered appropriate and therefore the Crisis Committee would be activated.

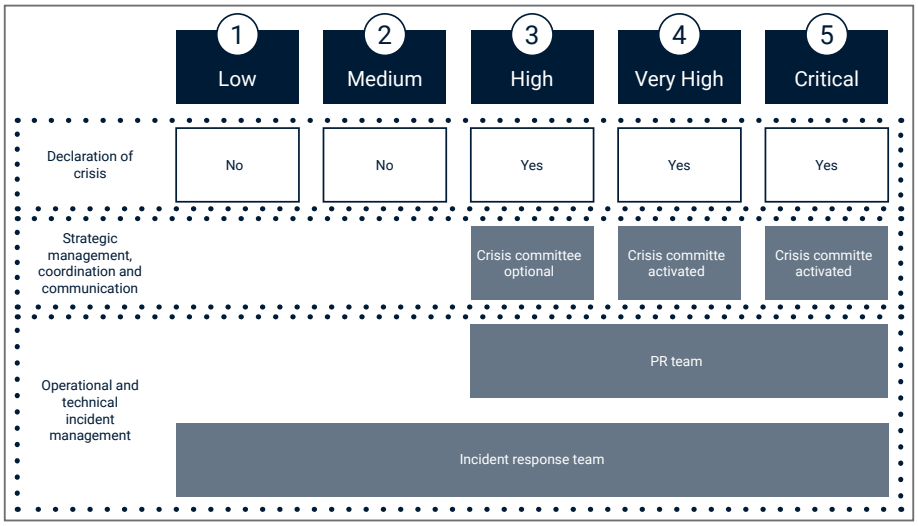


Figure 9. Committee and teams according to Level

Deciding on which level of the municipality and which committee or team to manage is also an element to consider when deciding on the level of the incident/crisis.

This configuration of committees (see **Figure 9**) is not exclusive; the constitution of one of the higher levels implies, in general, the maintenance of the activity of the previous ones. In other words, in a HIGH or VERY HIGH LEVEL cyber-attack, the local administration's top

management will make the final decisions within the Crisis Committee, according to the contributions of the Incident Response Team, the Communication Team and the teams made up of representatives from the functional areas.

It is important to have a well-defined **formal procedure for the activation of the Crisis Committee**, incorporating aspects such as:

- Which **members have the power** to activate it, in addition to the Mayor. In the event that, as mentioned above, there is a person or commission in charge of assessing incidents, it can be at the proposal of this person or commission.
- Which channels will be used to activate the Committee and convene the first meeting: email, phone call, social network group, mass communication application with the predetermined group, taking into account that the corporate network tools may not be operational.
- How meetings will be conducted: face-to-face, videoconference, multi-call, hybrid.
- What information should the activation statement contain: type of incident, first classification, known impacts, etc.

It is important to lead, take and maintain the initiative during an incident and, if the initiative is lost, to seek opportunities to regain it. Taking reasonable action is almost always better than doing nothing, based on preparation and an agreed plan.

Taking the lead, upholding one's own values and maintain control

8. Phase 3. Management and monitoring of the cybercrisis

Following the convening and activation of the Committee, the first action to be taken by the Crisis Committee is to meet.

There is a tendency to spend precious initial time waiting for more information (which rarely comes) or for the incident to deactivate itself (which never happens). This initial time is essential to make decisions in advance and to make a first diagnosis that will have a fundamental influence on subsequent work, as well as to dedicate time to possible scenarios of evolution.

Crisis management requires addressing several fronts at once as shown in Figure 10, which, in simplified form, will be developed throughout this document.

The Crisis Committee should meet and act early in the management of the crisis, coordinating with the reference CERT and developing a detailed mitigation plan. Successful resolution of the cyber incident requires coordination and external assistance.

Figure 10. Areas of action to be covered in a crisis

8. Phase 3. Management and monitoring of the cybercrisis

It is in this management phase that the mechanisms and procedures that have been defined in advance are applied. From a technical point of view:

- These mechanisms should provide for **rapid coordination with the reference CERT** so that a capable team is formed that can act quickly and whose tasks are taken on as a priority by the organisation. This work will provide more evidence and information to better assess the situation in the Crisis Committee.

- When the situation is under control by these technical teams, a **Mitigation Plan** should be drawn up and approved by the Crisis Committee. This plan should be very detailed and studied by all parties, including its implementers, before being carried out, ensuring a methodical, step-by-step execution, with two (2) objectives:

  - Decrease its execution time, since its execution will most likely lead to the temporary unavailability of the organisation's network.

  - Leave no loopholes for the attacker to stay inside the network, once the plan is executed.

A case: Castellón City Council (II)

One day after the incident was detected, on 31 March, three (3) courses of action were identified:

Containment:

The objective was to eliminate the malware and start the process of disinfecting the workstations. In this line of action, the type of attack was identified in order to determine the actions to be carried out.

In addition, the Spanish Data Protection Agency was notified and the attack was reported to the National Police.

Mitigation:

The network was redesigned, upgrading computers, wiping hard drives, changing domain-wide credentials and updating anti-spam and firewall rules in order to mitigate the impact of the incident.

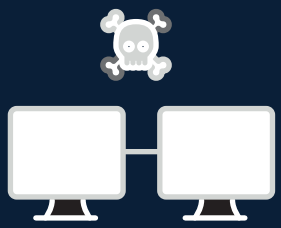
In this line of action, backups were also recovered, catalogued and secured in a stable and secure environment.

Recovery of services:

The databases, backup copies and file servers are recovered. In fact, on 5 April, the services are recovered, recovering a large part of the work tools and services of the City Council, among them:

- Recovery of the e-Office.
- Recovery of services without full operational capacity

Coordination between all involved and participants is one of the keys to the successful resolution of a cyber incident, and this often requires recognising that the situation is beyond one's capabilities and that external help is needed.



Ensuring coordination between the different departments involved is essential for the management of the cyber-attack

8.1. Dynamics of Crisis Committee meetings

The purpose of the first meeting is to assume the assigned functions, take control of the situation and start the formal decision-making process for the management of the cybercrisis. The meeting should be held as soon as possible (with its full or alternate members) and can be of various types (face-to-face, videoconference, etc.).

It is useful to plan the dynamics of the Crisis Committee both at the first meeting and between meetings during the crisis itself. To this end, it is recommended to include in the Crisis Plan or Manual a standard agenda and a checklist of issues to be addressed, in order to facilitate the dynamics and the decision-making process, ensuring that the key points are addressed.

To recall the main functions assigned to Crisis Committee members

As a guideline, t**he agenda** may contain the following points:

- Establish an estimate of the duration of the meeting.
- Review facts and ask for an update on the incident.
- Review the *checklist*.
- Quickly recall the role of each member: review their functions and the predefined actions to be carried out in the first moments.

8. Phase 3. Management and monitoring of the cybercrisis

- Assign responsibilities arising from the Action Plan and agreed first actions.
- Verify that actions are taken by those responsible, clarifying coordination issues between them.
- Set the next meeting and frequency of the following meetings of the Committee and of the checkpoints (the latter with a double purpose: informative and for review in case changes have occurred).
- To specify aspects to be included in the next meeting.
- Validate that all items on the *checklist* have been addressed.

The *checklist* should be drawn up in advance, in order to support the Crisis Committee in ensuring that all the issues to be addressed in a cybercrisis are dealt with in an orderly and systematic manner and to prevent any of them from being forgotten due to haste or the urgency of the situation. As can be deduced, it is important that it be comprehensive in the aspects it covers.

The first step in the management and subsequent resolution of an incident is to carry out a diagnosis of what is happening. Although, in the early stages of an incident, information is often unclear and incomplete, it is very important to understand what is happening and its possible short and medium-term effects (possible scenarios).

Conduct an initial diagnosis and possible scenarios.

It is important to continuously record the decisions taken by the Crisis Committee in a "Cyber Attack Diary" document that lists the relevant information regarding the daily management, the measures taken and their status (with time and date), and the tasks of the Action Plan (with responsible persons and deadline).

8.2. The Crisis Committee between meetings

The Crisis Committee must continuously monitor the situation, which implies maintaining an appropriate meeting dynamic to ensure regular and systematic review of the situation, as well as of the results and the response strategy adopted.

Therefore, it should be envisaged that while the Committee is active, a **meeting-pause process** will be used, so that its members can carry out the mandated actions and have time to coordinate their team and implement the actions in their area.

The following is a reminder of the main tasks to be carried out between meetings by the members of the Crisis Committee.

- Carry out the Action Plan tasks agreed at the previous meeting.
- Assign or undertake individual actions.
- Overseeing the development of the strategy.
- Gathering new information to be provided in real time to the Committee Coordinator who, in turn, has the responsibility to ensure that it is shared and reaches the other members of the Committee when they are not in session.

A case: Castellón City Council (III)

The Mayor called a meeting with the Municipal Operational Coordination Centre (CECOPAL) to address the attack, with the aim of neutralising it. Those attending the CECOPAL meeting included:

- The Mayor,
- The spokesperson of the government team,
- The Councillor for e-Government and Digital Innovation,
- Representatives of the municipal technical side,
- Representatives of the administration and the plenary, legal, urban and emergency services,
- Technicians from the technical team of the Department of Modernisation.

A total of 13 CECOPAL meetings were held and 4 meetings of spokespersons of a technical nature were held, in which the participants took part:

- The director of the service
- The councillor of the Castellón City Council
- The Head of Section.

8.3. Communication during the crisis

The management of communication in a crisis requires, as in other areas, **planning** and a strict application of the Communication Plan that has been previously defined, given that the internal and external noise that is produced in these situations jeopardises the success of this management and can place the local authority at the mercy of the situation.

Nowadays, any crisis is broadcast live on social networks, which in turn act as a source of information for the traditional media, which echo them. This circuit is exploited by multiple interlocutors who act as spokespersons or "alleged experts", inappropriately sizing up the crisis, **"if you don't say what you do, others will say what you don't do".**

In such a situation, the only option is proactivity, in the sense of taking the incident in hand, **setting one's own pace** without being at the mercy of internal or external pressure. In a crisis, it is always desirable that the main source of information should be the organisation itself. For this to be the case, it is essential to be proactive and take the initiative, without falling into haste.

In addition, it is very important that the Crisis Committee establishes clear messages that no one in the organisation should deviate from, so that whatever format and channel is chosen, the **information will be the same, without falling into contradictions.**

Be proactive, have a unified discourse and be the official source of information.

The first is to have a prior crisis communication **plan or protocol** that has "thought through" this type of scenario, which determines the information circuits, the necessary and recurrent arguments, the channels, the spokespersons, all the interlocutors involved and the actions to be taken.

The response time in today's crises is nil, which is why it is necessary to have the right **leadership** and decision-making capacity to take control of the situation. As mentioned above, the local administration must **decide who, at the communication level, is responsible for** managing the situation in all its internal and external dimensions.

In this sense, proactivity and a unified discourse are very important components of the communication policy that must take into account

not only external information (media, website, social networks, etc.) but also that this unified message is practised internally, towards staff, suppliers and/or customers.

Indeed, **internal communication is just as important as external communication** and begins by meeting the **information needs of the employees themselves**, who, in a society where social networks prevail, can in turn act as channels of communication, i.e. any employee can act - voluntarily or involuntarily - as a source of information about what is happening.

It is recommended to act quickly and **develop information to be passed on internally** to all staff, not only in relation to what they should do technically, but also by providing such information to help them deal with questions from their family and friendship circles.

8.3.1. Reflections on transparency, empathy and responsibilities

Disinformation, biased reporting, silence or passivity are the worst communication options when a cyber incident occurs. To protect the reputation of the entity, **uncertainty must be avoided**. This attitude is also relevant for the rapid notification of the CERT of reference, as this is of overall benefit.

In general, a mature society accepts that things in an organisation may not always work as desired and that imponderables may arise. What is not understood or accepted is that those in charge do not react in time or react inadequately.

However, maintaining transparency during a cyber scenario is not easy, but the damage can be compensated or minimised by adopting an **open and accountable policy** that, although in the short term may raise criticism, in the long run will lead to an improvement in the credibility and reputation of the local authority.

This approach **does not mean that absolutely** everything has to be **told**. As a general rule, it is necessary to gain time until the extent of the situation is better understood. Therefore, avoid mentioning the

causes of the incident, the person responsible for it, information that the investigation may reveal or the possible consequences for the organisation or another stakeholder.

As mentioned above, the way a crisis is managed is also based on the organisation's values. From this point of view, taking responsibility when there is a crisis is a sign that these values exist and are respected. Beyond that, in general, not taking responsibility generally works against the organisation and its governance team, when it becomes clear that by denying responsibility it was trying to avoid the consequences of its actions.

Have empathy and take responsibility.

It is therefore important to take special care to **balance what can be said** (over-communication may alert aggressors that the attack has been discovered and is being acted upon in a way that may not be desirable in the first place), with the need to meet the information expectations of stakeholders, such as the full council or opposition representatives.

8.3.2. Communication actions during the crisis

As with technical incident management and crisis management, communication management is a process that should start well before the incident and **end well after it,** but from the moment the incident is detected and leads to a crisis declaration, it is important to remember the following points:

- Gather all the information and understand the situation.
- Update and generate the arguments and messages: elaborate the most appropriate information taking into account time/priority and target group.
- Designate and prepare the spokesperson.
- Identify the related partners and possible new partners.
- Edit cross-platform content for messages.
- Manage, attend to and monitor the media and communication channels.
- Define a proper timetable and agenda with communication actions to be presented to the Crisis Committee.

Crises have many moments when, despite the intense work and the many simultaneous actions being carried out, there are still no results that can be presented to the public and stakeholders.

In a context such as the one described above of proactivity and transparency on the part of the local authority, when there is an appearance by the spokesperson or periodic communiqués, it is a good time to highlight the measures taken by the entity and its government team, both preventive measures in terms of cybersecurity (investments, coordination with the reference CERT, preparation of plans, technological changes, etc.) and corrective measures (people working on the incident, coordinated collaborators, etc.).

To highlight the value of the actions taken and resources used.

Any crisis represents an opportunity to demonstrate to public opinion the capacity of its closest administration -the City Council, the Provincial Council, the Cabildo, etc. - to resolve (alone or in coordination with other agents involved) a complex situation, demonstrating that the management of adversity has been adequately handled.

8.4. Stakeholder management

Stakeholder management, whether affected or not, is one of the pillars of cyber-incident management, which must be incorporated by the Crisis Committee among its functions, as all councillors and teams and all areas of the entity have their own groups to pay attention to.

Depending on the type of incident and the scenario caused, it will be necessary to review all stakeholders, their expectations and the strategy to be followed with each of them, and very importantly, to ensure that the main interlocutor is known.

For this reason, it is advisable to develop the so-called **"Stakeholder Map"** where the different areas of the local administration should identify those who may be affected by the situation and who require

information as well as solutions or alternative measures in case the situation is prolonged over time. The following is a list of stakeholders as a guideline, but not exhaustive:

- Citizens in general and neighbourhood organisations/associations through the district/neighbourhood councillors.
- The municipal plenary where all political forces are represented.
- Entities (cultural, sports, social, recreational, etc.).
- Economic sector of the municipality (industry, commerce) through their associations and their assigned councillor.
- Autonomous bodies of the Local Agency.
- Trade unions and bodies representing workers.
- Education and health sector.
- Supra-municipal bodies (Provincial Council, County Council).
- Suppliers of goods and services.
- Others...

All parties must make efforts to understand what the situation is, where the minimum threshold of responsibility lies and commit themselves to assume it, as well as to set up or create ad-hoc, agile and clear channels of dialogue to steer the return to normality.

9. Phase 4. Closure of the crisis and deactivation of the crisis committee

Organisations tend to close crisis files quickly, but it is important to dedicate efforts to close crises well because their effects and impacts last over time, and especially to avoid leaving unresolved issues that can be reproduced in the future.

It is important to close crises well and learn from them. Two parts: deactivation and post-crisis analysis.

In this phase, two (2) parts are differentiated: the deactivation of the Crisis Committee and the post-crisis analysis and adoption of lessons learned.

9.1. Deactivation of the Crisis Committee

Cyber-incident crises tend to be long and equipment and services are likely to be progressively restored in a secure manner, which entails working in a precarious/degraded manner for some time. In this case, the return to normality may take a long time and the deactivation of the Crisis Committee is only one of the necessary actions, but not the only

one: the closure of crises requires programmed and structured work that continues to involve different parts of the local administration.

In this regard, it is recommended that some criteria be incorporated to **help decide on the deactivation of** the Crisis Committee, for example:

- Si el Equipo de Respuesta a Incidentes puede continuar trabajando sin el apoyo del Comité.
- Si ya no es necesaria la implicación / dirección del personal del Comité y lo que queda pendiente puede ser ejecutado por otras personas de sus respectivos equipos.
- Si se dispone de un Plan de Acción que garantiza que todos los temas abiertos son tratados adecuadamente y se ha establecido un programa para actualizaciones periódicas.

Irrespective of whether the Crisis Committee has been called off, someone will be appointed to ensure the proper archiving of the information generated during the episode, paying particular attention to information that may be of use to the legal services in the following months and ensuring information security measures.

9.2. Post-crisis management and compliance with the ENS

Once the crisis is over, it is essential to carry out an analysis and assessment of everything that happened in order to identify those actions (best practices) that contributed to manage it properly and to identify weak points, all with the aim of designing measures that contribute to improve the local authority's response in the future, which should constitute the lessons learned from each crisis.

In many cases, day-to-day pressures mean that the incident is not closed in the most appropriate way. The best practice of successful closure is undoubtedly in dedicating time and resources to extracting lessons learned and implementing them in the reality of the organisation, as well as communicating closure, both internally and externally.

Bringing a crisis to a formal closure.

Consequently, carrying out the relevant analyses, drawing conclusions, defining an Action Plan and monitoring its implementation are indispensable steps in closing the cybercrisis and are often only half done.

In this final phase, the tasks to be carried out in order to **ensure a closure that provides value** to the local authority are:

- Produce **a post-crisis report**, with an in-depth analysis of the development of the crisis, its causes and the proposed measures to be implemented. The aim of this report is to learn from the experience, both to prevent other possible crises and to improve their management when they occur. To this end, it is important to have a critical spirit in order to generate best practices, lessons learned and define the measures to be implemented (with timeframe, cost and person in charge).

- Define the **ENS Compliance Plan** and the methodology for continuous improvement (monitoring of the measures adopted). The compliance with the ENS is key because it helps to reduce the exposure surface, to adopt a better security position, to strengthen (if not define) the figure of the Information Security Officer and the Crisis Committee.

- Hold a **meeting of the Crisis Committee** for this post-crisis analysis. The objective is to review the episode and the preliminary post-crisis assessment report made by the operational manager or coordinator, review the decisions taken and reflect critically to draw lessons learned and determine how they will be introduced in the organisation. The Mayor or President will decide which other members of the council or local administration should attend this meeting to complete and contribute their vision.

9. Phase 4. Closure of the crisis and deactivation of the crisis committee

To thank the staff of the local administration, the external collaborators who have intervened, the citizens in general, the members of the Plenary, whoever is considered appropriate, and to inform them that the crisis has been formally closed.

If it is determined that the crisis has caused reputational damage to the local administration, a Communication and Stakeholder Relations Plan will be defined to address the causes and restore the confidence of the parties.

Adopting lessons learned.

Treat an incident as a source of learning, drawing conclusions from what happened through in-depth analysis and adjusting those learnings to future action and investment plans.

9.3. ENS Compliance Plan and methodology for continuous improvement

For the effective adoption of the Adaptation Plan that allows compliance with the provisions of Royal Decree 311/2022, of 3 May, which regulates the National Security Framework (ENS), thirty-five (35) Essential Security Requirements are taken as a reference, as shown below, in the areas of Organisational Framework, Operational Framework and Protection Measures, whose assessment of compliance or state

of implementation in organisations using the INES governance tool provided by the National Cryptologic Centre, will make it possible to identify their state of progress with regard to compliance with the ENS and to identify possible deficiencies and existing risks, contributing to a reduction in the surface of exposure, the adoption of the ENS and the identification of possible deficiencies and existing risks, provided by the National Cryptologic Centre, will make it possible to identify their state of progress with respect to compliance with the ENS and the identification of possible deficiencies and existing risks, contributing to the reduction of the surface of exposure, the adoption of a better security position of the entity and the establishment or consolidation of a Crisis Committee and the figure of the Information Security Officer.

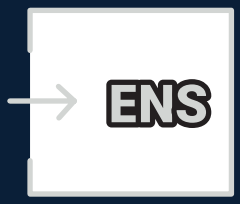
Organisational framework (4):	
[org. 1]	Security policy
[org. 2]	Safety regulations
[org. 3]	Security procedures
[org. 4]	Authorisation process
Operational framework (14):	
[org. pl]	Planning
[org. pl.1]	Risk analysis
[org. pl.2]	Purchase of new components
[org. acc]	Access control
[org. acc.1]	Identification
[org. acc.2]	Access requirements
[org. acc.4]	Access rights management process
[org. acc.6]	Authentication mechanisms (users of the organisation)
[org. exp]	Exploitation
[org. exp.1]	Inventory of assets
[org. exp.2]	Security settings
[org. exp.4]	Maintenance and security updates
[org. exp.6]	Protection against malicious code
[org. exp.7]	Incident management
[org. exp.8]	Activity logging
[org. exp.10]	Cryptographic key protection
[org. mon]	System monitoring
[org. mon.2]	Metrics system

Protective measures (17):	
[mp. per]	Personnel management
[mp. per.2]	Duties and obligations
[mp. per.3]	Awareness-raising
[mp. per.4]	Training
[mp. eq]	Protection of equipment
[mp. eq.1]	Uncluttered workstation
[mp. eq.3]	Protection of portable devices
[mp. eq.4]	Other devices connected to the network
[mp. com]	Protection of communications
[mp. com.1]	Secure perimeter
[mp. com.2]	Protection of confidentiality
[mp. si]	Protection of information media
[mp. si.3]	Custody
[mp. si.4]	Transport
[mp. si.5]	Deletion and destruction
[mp. info]	Protection of information
[mp. info.1]	Personal data
[mp. info.3]	Electronic signature
[mp. info.5]	Cleaning of documents
[mp. info.6]	Back-up copies
[mp. s]	Protection of services
[mp. si.1]	Protection of electronic mail
[mp. s.3]	Web browsing protection

Table 3. Essential Security Requirements:

Thus, for the effective implementation of a Plan of Adaptation to the ENS, which among others, frames some basic principles and minimum requirements that seek to give confidence to both citizens and the public administration in the use of electronic media, using measures and indicators to ensure the security of systems, data, communications and electronic services, it is proposed the development of a roadmap,

whose actions would have a maximum duration of six (6) months, distributed in the execution of two (2) groups of activities to be carried out consecutively, with deliverables associated with each of them in the areas of (i) **Governance and Compliance Model**, and **(ii) Security Tools**, complemented with the development of a technical analysis focused on obtaining the organisation's Exposure Surface, identifying possible vulnerabilities, security gaps, configuration deficiencies and existing risks.



Diagnosis of compliance and initiation of the ENS Adequacy Plan where appropriate.

Figure 11 and Figure 12 describe the activities for each area and the timeline (time estimate) associated with their implementation:

(i) Governance and Compliance Model: start of the application of the µCeENS Model on the basis of which a diagnosis is made as to whether the level of risk of the organisation is acceptable and an Adaptation Plan is established to contribute to the improvement of the security posture. Additionally, the needs are identified and the priority actions to be implemented are estimated, with respect to the framework of Governance, determination of roles and responsibilities, and compliance for the effective protection of information and data management.

(ii) Security Tools: based on the validation of the assumable risk and the analysis of the Exposure Surface, the critical services, systems and assets are determined for the development of technical audits in grey box, pentesting or ethical hacking exercises, together with the identification of the deployment of proactive measures that, based on the diagnoses of previous activities, contribute to adopting a better security posture appropriate to the potential threat.

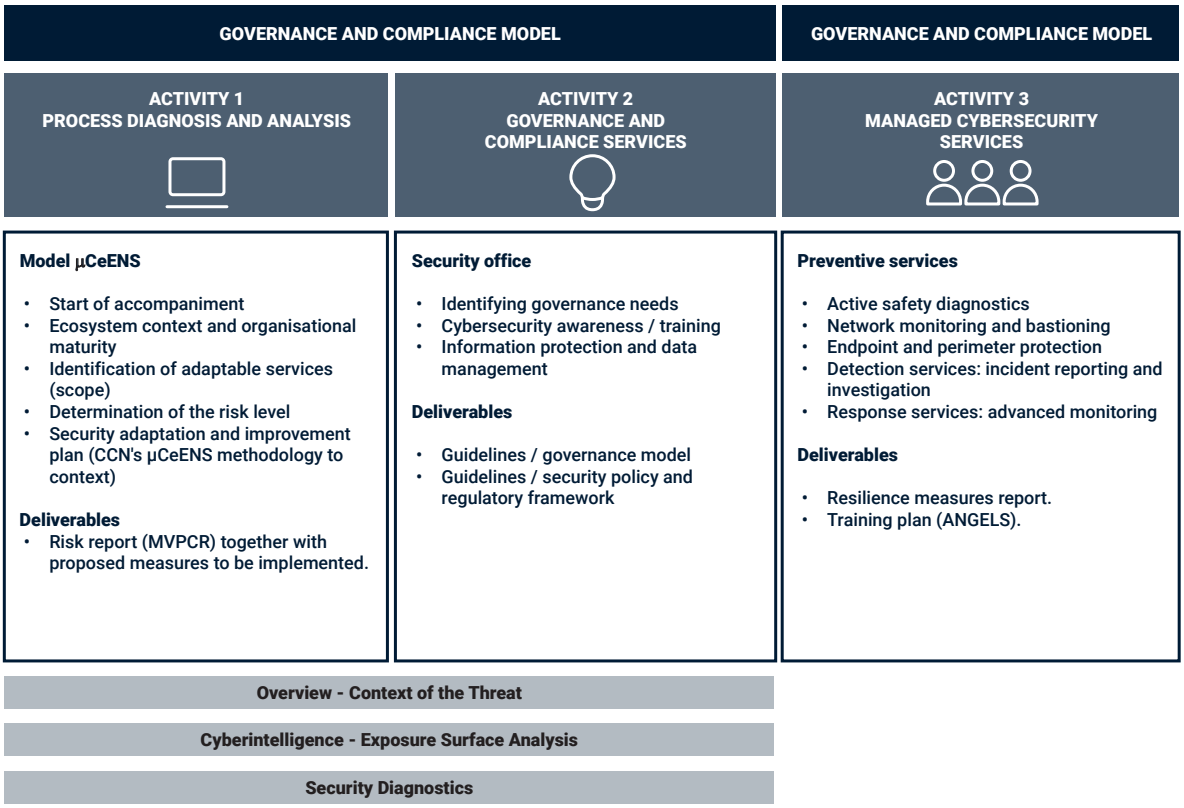


Figure 11. Activities and deliverables associated with each domain.

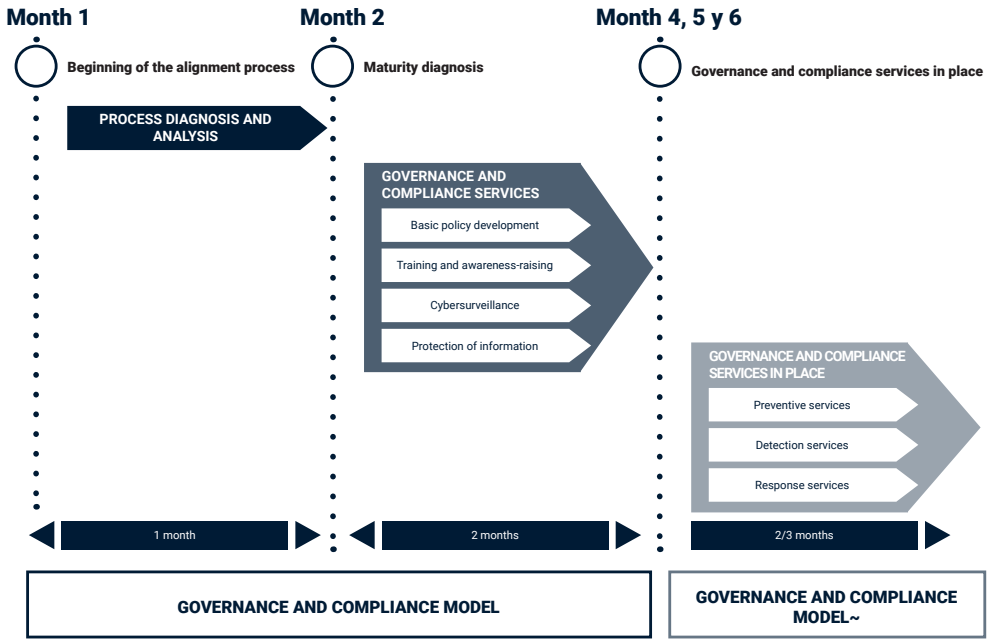


Figure 12 Timetable established for the development of activities

9. Phase 4. Closure of the crisis and deactivation of the crisis committee

The development of the proposed roadmap will facilitate both the entities' compliance with the ENS, as well as to organise and focus efforts on the following actions:

- **Global risk analysis** through the management of information systems security based on information on the organisation's assets and the assessment of the impact of their loss.
- **Identification of technical, regulatory and procedural measures** to achieve adequate protection of both information and critical systems of the entities to support the effective provision of services to citizens and to advance in the plan of adaptation to the ENS.
- **Support for the management of Proactive Prevention based** on the governance tools provided by the National Cryptologic Centre for the implementation of the governance and compliance service, in a staggered manner, in accordance with the entity's needs.

Annex 1. Data protocol to be provided by the body affected by ransomware

The entity shall provide the following information:

- The technical staff of the entity acting as POC and channelling the requests about the incident.
- The telephone number and e-mail address of the following staff of the entity:
  - Security Officer
  - Communications Officer
  - Systems Administrator
  - Responsible for the virtualisation system
- What and when has it been detected?
- How many teams are believed to be affected?
- Are the affected computers physical or virtual servers?
- If virtual, has it been encrypted at the machine level (i.e. files within the virtual machine) or at the hypervisor level (the whole virtual hard disk)?
- Sending of ransom note if received and available

Annex 1. Data protocol to be provided by the body affected by ransomware

- Are backups (especially of encrypted data) available, and if so, when was the last backup made?
- Is it known whether backup servers have been affected?
- Have mitigation actions been taken, and which ones?
- Is there remote access via VDI (Citrix type)?
- Is there remote access via VPN?
- Are all devices corporate?
- Credentials used or compromised. Protocols. Active directory
- Communications. Network monitoring. Network distribution.
- Is there a SOC deployed?
- Antivirus? EDR?
- Is two-factor remote access to the entity available (both VPN and VDI), and what is the log date for this?
- Provide an encrypted file
- List of critical services of the entity
- Does the entity have whitelists?

Annex 2. Reference playbooks for cyber incident response

Playbook			
	Stages	**Activities envisaged**	**Main actors involved**
Data breach	Planning	**Developing a Response Plan** Formation of a response team identifying roles and responsibilities for planning, detection and response. Development of a response plan for cyber data breach incidents, taking into account available resources and considering risk and recovery. Review and approval of the cyber data breach response plan. Development of an internal and external communication programme, including raising awareness of the incident and defining a spokesperson. Inventory of assets related to sensitive/critical data.	**Developing a Response Plan** Information Security Officer Information security manager, systems manager, legal team and business continuity. Mayor, information security manager, systems managers, legal team, business continuity and communications manager. Communications Officer and Information Security Officer. Information security manager and human resources manager.

	Stages	Activities envisaged	Main actors involved
Data breach	Planning	**Implementation of Preventive Measures** Use of basic and complementary tools to prevent information leakage (detection of unauthorised access or use, use of firewalls between networks to restrict traffic, intrusion prevention systems, etc.). Documentation and analysis of the incident. **Definition of detection parameters** Establishing indicators for detecting data breaches	**Implementation of Preventive Measures** Information Security Officer. Information security manager and systems manager. **Definition of detection parameters** Information Security Officer.
	Detection	**Incident detection** Monitoring and timely detection of anomalous events in network traffic (bounced emails, alert notification for disk saturation, identification of data publication outside the organisation, etc...). Monitoring of exposure of sensitive data on social networks and open sources. Review and analysis of information from internal and external users.	**Incident detection** Information Security Officer Information Security Officer Information security officer and legal team.
	Response	**Incident assessment** Categorisation of the cyber incident as a data breach attack and determination of the level of criticality. **Incident analysis**	**Incident assessment** Information Security Officer. **Incident analysis**

	Stages	Activities envisaged	Main actors involved
Data breach	Response	Verification of the legitimacy of the leaked data/information. Analysis of different sources of information to understand the target of the attack. **Incident containment** Implementation of physical and logical quarantine measures for infected assets, restricting and limiting their access to networks. Implementation of additional measures for internet browsing, use of removable devices and whitelisting. Suspension of login credentials of compromised users' accounts and disabling of affected services on servers. Verification of antivirus and malware signatures on computers. **Documentation and evidence control** Copies of files (logs) of perimeter security elements and affected devices. Identification and analysis of network packets to identify IP addresses, ports, protocols, agents, etc. **Forensic analysis**	Information Security Officer. Information security manager and systems manager. **Incident containment.** Information Security Officer and Physical Security Officer. Information Security Officer. Information Security Officer. Information Security Officer. **Documentation and evidence control** Information Security Officer. Information Security Officer. **Forensic analysis** Information Security Officer. Information Security Officer and Communications Officer. **Eradication of the incident**

	Stages	Activities envisaged	Main actors involved
Data breach	Response	Forensic analysis of the threat to identify the motivation of the attack and its target, the method used and possible actor involved, etc. Communication of the status of the incident and its management to stakeholders. **Eradication of the incident** Installation of security patches that mitigate the exploitation of the vulnerability associated with the attack. Implementation of customised security configurations and controls on servers, applications and network segments. **Recovery of affected services** Recovery of the availability of compromised devices and systems. **Closure of the incident** Report generation and identification of improvement activities.	Information Security Officer. Information Security Officer. **Recovery of affected services** Information Security Officer. **Closure of the incident** Information security manager and systems manager.

Playbook			
	Stages	**Activities envisaged**	**Main actors involved**
Denial of service (DDoS)	Planning	**Developing a Response Plan** Formation of a response team identifying roles and responsibilities for planning, detection and response. Development of a response plan, taking into account available resources and considering risk and recovery. Review and approval of the plan including verification of compliance and effectiveness of activities, responsibilities and escalation flow. Development of an internal and external communication programme, including raising awareness of the incident and defining a spokesperson. **Implementation of Preventive Measures** Protection of services published or exposed on public networks, such as e-mail, web portal and DNS services among others. Inclusion of denial of service (DDoS) attack mitigation techniques in the design stage of projects for changes or new services, Strengthening the infrastructure configuration (network, servers,	**Developing a Response Plan** Senior management. Information security manager, systems manager, legal team and business continuity. Mayor, information security manager, systems manager, legal team, business continuity and communications manager. Communications Officer and Information Security Officer. **Implementation of Preventive Measures** Information Security Officer. Information Security Officer. Information security manager and systems manager. Information Security Officer.

	Stages	Activities envisaged	Main actors involved
Denial of service (DDoS)	Planning	applications and operating systems) that could be affected by a denial of service (DDoS) attack, Documentation and analysis of the incident. **Definition of detection parameters** Definition of indicators for the detection of anomalous events related to denial of service attacks (DDoS) based on average traffic and maximum tolerable limit. Definition of the structure of records (logs) that need to be enabled in the infrastructure elements (servers, routers, among others), perimeter protection (firewall, IPS, among others) and detection probes that allow visibility of connections (source and destination IP address, protocol), traffic volume, among others. Configuration and analysis of anomalous events passing through outgoing traffic, mainly in IRC, P2P and HTTPS protocols.	**Definition of detection parameters** Information Security Officer. Information Security Officer. Information Security Officer.
	Detection	**Incident detection** Monitoring and timely detection of anomalous events in network traffic (unknown or unidentified packets coming from unknown sources, increase in the volume of encrypted data, anomalous increase in bandwidth usage, etc...).	**Incident detection** Information Security Officer Information Security Officer Information Security Officer. Information Security Officer.

	Stages	Activities envisaged	Main actors involved
Denial of service (DDoS)	Detection	Review and analysis of alerts from perimeter security components (Firewall, IPS, Anti DDoS systems, etc...). Review and analysis of notifications from suppliers. Review and analysis in cyber intelligence sources of new trends in relation to denial of service (DDoS) attacks.	
	Response	**Incident assessment** Categorisation of the cyber incident as a denial of service (DDoS) attack and determination of the level of criticality. **Incident analysis** Obtaining and analysing different sources of information/data necessary to understand details of the cyber-attack. Communicate the analysis of the incident to the CERT of reference. Implementation of the response plan / playbook available. **Incident containment** Identification of which traffic to discard or allow based on the source history of malicious or legitimate traffic. Communication and request for blocking of malicious traffic to the internet provider. If the level of criticality of the incident requires it, use the business continuity plan and disaster recovery procedure to move IT operations to alternative sites.	**Incident assessment** Information Security Officer. **Incident analysis** Information Security Officer. Information Security Officer. Information security manager and systems manager. **Incident containment.** Information Security Officer. Information Security Officer. Information Security Officer. **Documentation and evidence control**

	Stages	Activities envisaged	Main actors involved
Denial of service (DDoS)	Response	**Documentation and evidence control** Copies of log files of perimeter security components and affected devices. Identification and analysis of network packets to identify IP addresses, ports, protocols, agents, etc. **Forensic analysis** Forensic analysis of the threat to identify the motivation of the attack and its target, the method used and possible actor involved, etc. Communication of the status of the incident and its management to stakeholders. **Eradication of the incident** Installation of security patches that mitigate the exploitation of the vulnerability associated with the attack. Implementation of customised security configurations and controls on servers, applications and network segments. **Recovery of affected services** Recovery of the availability of compromised devices and systems. **Closure of the incident** Report generation and identification of improvement activities.	Information Security Officer. Information Security Officer. **Forensic analysis** Information Security Officer. Information Security Officer and Communications Officer. **Eradication of the incident** Information Security Officer. Information Security Officer. **Recovery of affected services** Information Security Officer. **Closure of the incident** Information security manager and systems manager.

Playbook			
	Stages	**Activities envisaged**	**Main actors involved**
Malware	Planning	**Developing a Response Plan** Formation of a response team identifying roles and responsibilities for planning, detection and response. Development of a response plan, taking into account available resources and considering risk and recovery. Review and approval of the plan including verification of compliance and effectiveness of activities, responsibilities and escalation flow. Development of an internal and external communication programme, including raising awareness of the incident and defining a spokesperson. **Implementation of Preventive Measures** Protection of all your devices (desktops, laptops and servers) through anti-virus and anti-malware software, Implementation of mitigation tools to detect and stop malware attacks. Documentation and analysis of the incident.	**Senior management.** Information security manager, systems manager, legal team, and business continuity. Mayor, information security manager, systems manager, legal team, business continuity and communications manager. Communications Officer and Information Security Officer. **Implementation of Preventive Measures** Information Security Officer. Information Security Officer. Information security manager and systems manager. **Definition of detection parameters** Information Security Officer. Information Security Officer. Information Security Officer.

	Stages	Activities envisaged	Main actors involved
Malware	Planning	**Definition of detection parameters** Definition of indicators for the detection of anomalous events related to malware attack. Enabling infrastructure components (servers, routers, etc...) and perimeter protection (firewall, IPS, etc...) logs to obtain visibility of packets, volume, origin, destination, protocols, among others. Analysis of anomalous events generated by unknown or unexpected services and applications.	
	Detection	**Incident detection** Monitoring and timely detection of anomalous events in network traffic (unknown or unidentified packets coming from unknown sources, increase in the volume of encrypted data, anomalous increase in bandwidth usage, etc...). Review and analysis of alerts from perimeter security elements (Firewall, IPS, anti-DDoS systems, among others) to identify possible malware attacks, e.g. ICMP viruses, Trojans, spyware, RAT, ransomware, rogueware, peripheral malware, among others. Review and analysis of notifications from suppliers. Review and analysis in cyber intelligence sources of new trends in malware attacks.	**Incident detection** Information Security Officer Information Security Officer Information Security Officer. Information Security Officer.

	Stages	Activities envisaged	Main actors involved
Malware	Response	**Incident assessment** Categorisation of the cyber incident as a malware attack and determination of the level of criticality. **Incident analysis** Obtaining and analysing different sources of information and data necessary to understand details of the cyber-attack. Communicate the analysis of the incident to the CERT of reference. In case the incident is between the MEDIUM and LOW criticality levels, verify whether a specific response plan for this type of incident (malware attack) is in place, and continue with containment and eradication activities. **Incident containment** Initiate quarantine (physical or logical) of infected assets, restrict or limit access to networks through perimeter security devices and to facilities through physical controls. Termination of unwanted connections or services on servers. Suspend login credentials of compromised users' accounts and disable affected services on servers.	**Incident assessment** Information Security Officer. **Incident analysis** Information Security Officer. Information Security Officer. Information security manager and systems manager. **Incident containment.** Information Security Officer. Information Security Officer. Information Security Officer. Information Security Officer. Information Security Officer.

	Stages	Activities envisaged	Main actors involved
Malware	Response	Adequacy of behavioural rules in the SIEM, Firewall and anti-virus/ anti-malware software, and continue to monitor the network for any new infections that may be spreading in the network. Verification that the anti-virus/anti-malware on all devices have the latest signatures available. **Documentation and evidence control** Copies of log files of perimeter security components and affected devices. Identification and analysis of network packets to identify IP addresses, ports, protocols, agents, etc. Back up the Malware affecting the devices, and perform the simulation in SandBox tools. **Forensic analysis** Forensic analysis of the threat to identify the motivation of the attack and its target, the method used and possible actor involved, etc. Communication of the status of the incident and its management to stakeholders. **Eradication of the incident**	**Documentation and evidence control** Information Security Officer. Information Security Officer. Information Security Officer. **Forensic analysis** Information Security Officer. Information Security Officer and Communications Officer. **Eradication of the incident** Information Security Officer. Information Security Officer. **Recovery of affected services** Information Security Officer. **Closure of the incident** Information security manager and systems manager.

	Stages	Activities envisaged	Main actors involved
Malware	Respuesta	Installation of security patches that mitigate the exploitation of the vulnerability associated with the attack. Implementation of customised security configurations and controls on servers, applications and network segments. **Recovery of affected services** Recovery of the availability of compromised devices and systems. **Closure of the incident** Report generation and identification of improvement activities.	

Playbook			
	Stages	**Activities envisaged**	**Main actors involved**
Insider Attacks (Insiders)	Planificación	**Developing a Response Plan** Formation of a response team identifying roles and responsibilities for planning, detection and response. Development of a response plan, taking into account available resources and considering risk and recovery. Review and approval of the plan including verification of compliance and effectiveness of activities, responsibilities and escalation flow. Development of an internal and external communication programme, including raising awareness of the incident and defining a spokesperson. **Implementation of Preventive Measures** Implementation and use of identity and access management (IAM) solutions by also implementing segregation of duties and privileged identity management (PIM) solutions. Implementation of identity governance solutions that define and enforce role-based access control and the principle of least privilege.	**Developing a Response Plan** Senior management. Information security manager, systems manager, legal team and business continuity. Mayor, information security manager, systems manager, legal team, business continuity and communications manager. Communications Officer and Information Security Officer. **Implementation of Preventive Measures** Information Security Officer. Information Security Officer. Information Security Officer. **Definition of detection parameters** Information Security Officer. Information Security Officer. Information Security Officer.

	Stages	Activities envisaged	Main actors involved
Insider Attacks (Insiders)	Planning	Implementation of complementary tools to help mitigate unauthorised access (authentication factors, host-based firewall, use of application whitelisting (Applications Control, etc...). **Definition of detection parameters** Definition of indicators for the detection of anomalous events related to unauthorised access attacks. Enabling in infrastructure components (servers, routers, etc.) and perimeter protection (firewall, IPS, etc.) the logs to obtain visibility of packets, volume, origin, destination and protocols, among others. Analysis of anomalous events generated by unknown or unexpected services and applications, which are started automatically at system start-up.	
	Detection	**Incident detection** Monitoring and timely detection of anomalous events in network traffic (unknown or unidentified packets coming from unknown sources, increase in the volume of encrypted data, anomalous increase in bandwidth usage, etc...). Review and analysis of alerts from perimeter security elements (Firewall, IPS, DLP systems, among others) to identify possible attacks by Insiders. Review and analysis in cyber intelligence sources of new trends in relation to Insider attacks, considering new threats or variants of existing ones, new vulnerabilities or incidents in the national and international context.	**Incident detection** Information Security Officer Information Security Officer Information Security Officer.

	Stages	Activities envisaged	Main actors involved
Insider Attacks (Insiders)	Response	**Incident assessment** Categorisation of the cyber incident as an Insider attack and determination of the level of criticality. **Incident analysis** Obtaining and analysing from different sources the information and data necessary to understand details of the cyber-attack. In case the incident is between the MEDIUM and LOW criticality levels, check if a specific response plan for this type of incident is in place, and continue with containment and eradication activities. **Incident containment** Initiate quarantine (physical or logical) of infected assets, restrict or limit access to networks through perimeter security devices and to facilities through physical controls. Termination of unwanted connections or services on servers. Suspend login credentials of compromised users' accounts and disable affected services on servers. Implementation of additional restrictions on internet browsing, on the use of removable devices and whitelisting for application control.	**Incident assessment** Information Security Officer. **Incident analysis** Information Security Officer. Information Security Officer. **Incident containment.** Information Security Officer. Information Security Officer. Information Security Officer. Information Security Officer. Information Security Officer. Information Security Officer.

	Stages	Activities envisaged	Main actors involved
Insider Attacks (Insiders)	Response	Adequacy of behavioural rules in the SIEM, DLP tool, Firewall and anti-virus/anti-malware software, and continue to monitor the network for any new threats from Insiders. Verification that the anti-virus/anti-malware on all devices have the latest signatures available. **Documentation and evidence control** Copies of log files of perimeter security components and affected devices. Identification and analysis of network packets to identify IP addresses, ports, protocols, agents, etc. **Forensic analysis** Forensic analysis of the threat to identify the motivation of the attack and its target, the method used and possible actor involved, etc. Communication of the status of the incident and its management to stakeholders. **Eradication of the incident** Installation of security patches that mitigate the exploitation of the vulnerability associated with the attack. Implementation of customised security configurations and controls on servers, applications and network segments.	**Documentation and evidence control** Information Security Officer. Information Security Officer. **Forensic analysis** Information Security Officer. Information Security Officer and Communications Officer. **Eradication of the incident** Information Security Officer. Information Security Officer. **Recovery of affected services** Information Security Officer. **Closure of the incident** Information security manager and systems manager.

CCN
centro criptológico nacional

CCN-CERT
centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es