CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Cybersecurity Risk and Crisis Communication Framework

v1.0
April 2024
Centro Nacional
de Cibersegurança

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Funded by the European Union
NextGenerationEU

Observatório de Cibersegurança

CONTENTS

LIST OF ABBREVIATIONS

ANACOM – National Communications Authority

ANEPC – National Emergency and Civil Protection Authority

ANSSI – Agence Nationale de la Sécurité des Systèmes d'Information

APPA – American Public Power Association

CCN – National Cryptologic Centre

CNPD – National Data Protection Commission

CSC – Cyber Security Coalition

ENSC – National Strategy for Cyberspace Security 2019-2023

GCS – Government Communication Service

ISAC – Analysis and Information Sharing Centres

ISO – International Organization for Standardization

PSC – Public Safety Canada

QNRCS – National Cybersecurity Reference Framework

RJSC – Legal Framework for Cyberspace Security

1. EXECUTIVE SUMMARY

The Cybersecurity Risk and Crisis Communication Framework (Framework) is a set of cybersecurity risk and crisis communication guidelines and recommendations for national Organizations.

The Framework is intended to serve as a support document for the development of the cybersecurity sector, assisting other Organizations in communicating risk management internally, as well as in developing communication plans to be followed in situations of cybersecurity crisis, listing steps, identifying essential elements and functions in the communication team created for such situations, encouraging the continuous improvement of communication plans.

In accordance with the National Strategy for Cyberspace Security 2019-2023, the Framwork is intended to assist Organizations in their capability to respond to cybersecurity crisis situations, during which communication is critical.

With these goals in mind, the Framework should be interpreted as a starting point for developing strategies, policies, and plans that should be tailored to the context and needs of each Organization.

2. INTRODUCTION

Various security surveys are published year after year, highlighting significant losses for Organizations as a result of the evolution of cyberthreats and cyberattacks. This evolution requires approaches and response capabilities to adapt, allowing for organizational growth in the context of cybersecurity. It should be noted that nowadays greater care and attention is being paid to the Organization's employees in terms of information security technology awareness and training.

It is therefore necessary for Organizations to prepare for risk and crisis communication situations in the context of information and systems security, given its growing importance in recent years.

The contents of this Framework are intended to guide Public Administration, critical infrastructure operators, essential service operators, and digital service providers, as well as all small, medium, and large Organizations, in complying with the requirements proposed within the applicable legislation and adopting best practices in communicating cybersecurity risks and crises.

This document was based on various national frameworks and practices on planning and managing the communication of cybersecurity risks and crises implemented by various countries, including Belgium, Canada, Spain, the United States of America, France, and the United Kingdom, as well as the international standard ISO 22361:2022, which is dedicated to crisis management. The goal was to compile a list of processes for identifying and communicating risks and crises to competent authorities that already exist in other countries, that are considered good practices, and which could be applied in a national context.

The goal of this document is to provide a reference for cybersecurity risk management and crisis communication planning and management for all Organizations that require such a reference.

2.1. SCOPE

Taking into account Law No. 46/2018 of August 13, 2018, which establishes the Legal Framework for Cyberspace Security, transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6, 2016, on measures to ensure a high common level of network and information security across the Union, the National Cybersecurity Centre (CNCS) seeks to contribute to the use of cyberspace in a free, reliable, and secure manner, by promoting the continuous improvement of national cybersecurity and international cooperation, in articulation with all competent authorities.

Considering the terms of the National Strategy for Cyberspace Security 2019-2023, which was approved by the Council of Ministers on May 23, 2019, and published by Resolution 92/2019 on June 5, 2019, it was deemed necessary to elaborate a cybersecurity risk and crisis communication framework.

In this sense, the Framework provides a body of knowledge for identifying key aspects in the field of cybersecurity risk and crisis communication, serving as a support document for the development of the cybersecurity sector and contributing to the definition and formulation of cybersecurity communication policies and plans.

2.2. OBJECTIVES

Considering the Framework's legal and strategic scope, and with its practical utility in mind, the Framework's conceptualization had the following goals underlying it:

- To identify and to capitalize on the strengths of various national and international frameworks on risk and crisis communication in cybersecurity, standardizing the various communication phases as well as the steps associated with each phase;
- To take advantage of synergies between the frameworks, minimizing conceptual differences and maximizing interoperability.
- To facilitate the Framework's updating and continuous improvement.

2.3. FRAMEWORK'S CONTEXT

For the development of this Framework, the following documents served as the primary external references:

- "*Crisis of Cyber Origin: The Keys to Operational and Strategic Management*" - Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), **France**;[1]
- "*Cyber Security Incident Management Guide*" - Cyber Security Coalition (CSC), **Belgium**;[2]
- "*Cybercrisis Management. Good Practices in Cybersecurity Crisis Management*" - Centro Criptológico Nacional (CCN), **Spain**;[3]
- "*Developing an Operational Technology and Information Technology Incident Response Plan*", Public Safety Canada (PSC), **Canada**;[4]
- *"Public Power Cyber Incident Response Playbook* - American Public Power Association (APPA)/Nexight Group, **United States**;[5]
- "*Emergency Planning Framework*" - Government Communication Service (GCS), **United Kingdom**;[6]
- "*ISO 22361:2022 - Security and resilience - Crisis management - Guidelines*"**, International Organization for Standardization.**[7]

[1] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), "*Crisis of Cyber Origin: The Keys to Operational and Strategic* Management", March 2022, https://cyber.gouv.fr/sites/default/files/2022/05/20220516_np_anssi_guide_gestion_crise_cyber_en1.pdf.

[2] Cyber Security Coalition (CSC), "*Cyber Security Incident Management Guide*", January 2016, revised September 2021, https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf.

[3] Centro Criptológico Nacional (CCN-CERT), "*Gestión de Cibercrisis. Buenas Prácticas en la Gestión de Crisis de Ciberseguridad",* 2020, https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5428-ccn-cert-bp-20-buenas-pra-cticas-en-la-gestio-n-de-cibercrisis- 1/file.html.

[4] Public Safety Canada (PSC), "*Developing an Operational Technology and Information Technology Incident Response Plan*", 2020, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dvlpng-ndnt-rspns-pln/index-en.aspx.

[5] American Public Power Association (APPA) and Nexight Group, "*Public Power Cyber Incident Response Playbook',* August 2019, https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf.

[6] Government Communication Service (GCS), "*Emergency Planning Framework',* 2018, https://gcs.civilservice.gov.uk/wp-content/uploads/2020/04/Emergency-planning-framework-1.pdf.

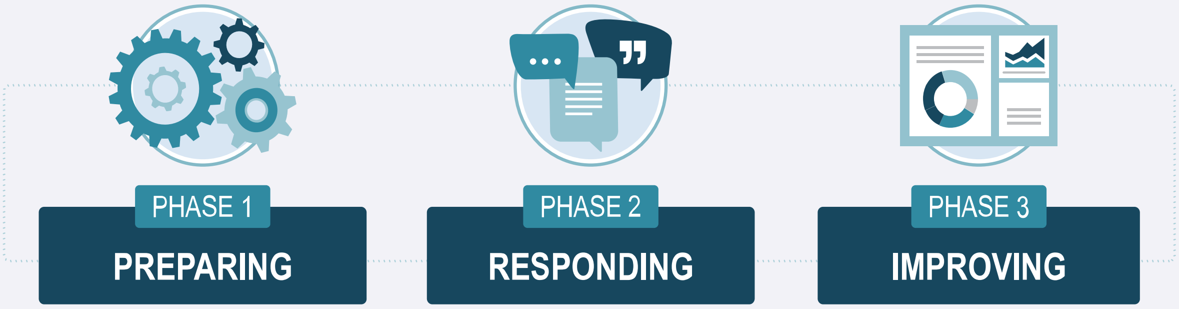
[7] International Organization for Standardization, "*ISO 22361:2022 - Security and resilience - Crisis management - Guidelines",* https://www.iso.org/standard/50267.html.

2.4. DOCUMENT STRUCTURE

The essential part of this Framework can be found in point 3 - "Cybersecurity Risk and Crisis Communication Framework" – of the document.

This section outlines three phases that will assist Organizations that follow these guidelines in communicating about cybersecurity risks and crises.

Figure 1: Document structure



PHASE 1 – "PREPARING THE COMMUNICATION OF A CYBERSECURITY CRISIS" deals with the preparation and drafting of a communication plan, along with the necessary steps required for this purpose, while also addressing the need to survey risks and communicating them to stakeholders.

PHASE 2 – "RESPONDING EFFECTIVELY" focuses on the practicalities and execution of communication in a context of crisis, addressing the activation of the communication team, the requirements for reporting the crisis and notifying the CNCS, as well as the requirements for communicating the impact of the crisis, its formal closure, and indications that could help restore the Organization's reputation if it has been affected.

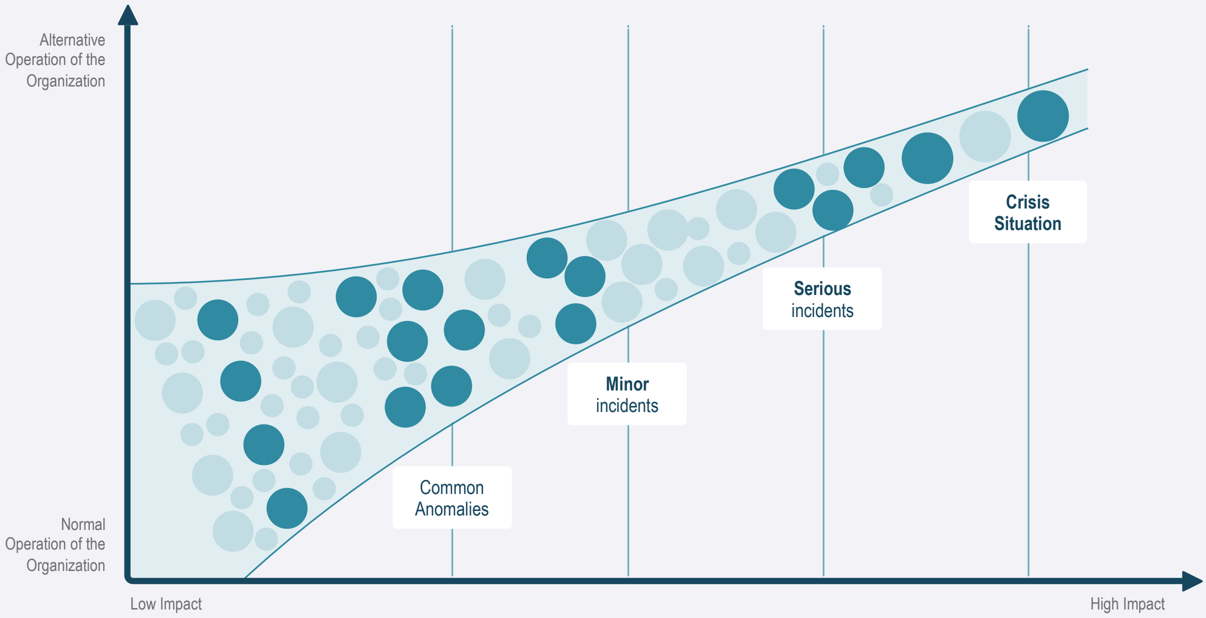
PHASE 3 – "LESSONS LEARNED AND IMPROVEMENT" is intended to prompt a review of the process of analysing the situation that occurred, allowing conclusions to be drawn about what was positive, as well as opportunities for improvement in the communication plan's implementation. This will make it easier to improve the plan, as well as the assessing of the risks to which the Organization is vulnerable.

A table detailing the expectations pertaining to each phase outlined in this Framework is provided within the points of each phase. The expectations are categorized into three levels of capability: Initial, Intermediate, and Advanced. The aforementioned levels align with those that have been established in the National Cybersecurity Reference Framework (QNRCS) and the Cybersecurity Capabilities Assessment Framework.

3. CYBERSECURITY RISK AND CRISIS COMMUNICATION FRAMEWORK

The Framework is presented below, being based on a structured and phased set of steps to be taken in order to effectively communicate about cybersecurity risks and crises, streamlining procedures and improving Organizations' ability to respond in crisis situations.

Figure 2: The evolution of an incident's impact to a crisis situation



What is Crisis Communication?

Crisis communication encompasses all forms of communication that an Organization can use to deal with a problem that affects its internal organization and reputation are referred to as crisis communication. A crisis is a situation in which an Organization's normal functioning is affected, disrupting its processes and operating environment.

Crisis communication aims above all to mitigate the negative impact of a crisis on an Organization's services, products or reputation. Prevention, rapid response, and immediate decision-making are critical in the event of a crisis. Having a communication plan in place may turn out to be crucial for effectively managing communication and avoiding potential controversies.

Crisis communication should also be a key component of any Organization's communication strategy, as it affects all communication channels, from internal to external, as well as public relations, including interactions with the press and social media.

Furthermore, crisis communication is an essential component of crisis management, which entails ongoing consultation with members of an Organization's management and with members of the crisis or incident response unit.

There are two widely acknowledged components of crisis communication:

- Communication during crisis management, which consists of alerting stakeholders and coordinating operations (QNRCS: RS.CO-2);
- Communication on how the crisis was handled and what was done to overcome it in order to maintain or restore the Organization's reputation[8] (QNRCS: RC.CO-2).

Why communicate during a crisis?

Effective and efficient communication is critical during a crisis, both for handling and resolving it. Without an appropriate response to the crisis, individual employees and other stakeholders are left to interpret the situation, which can lead to even more confusion and disorganization in the resolution process. An Organization experiencing a crisis because of a cyberattack should consider communicating the relevant aspects of the crisis to its stakeholders, reducing the possibility of divergent interpretations and misaligned messages.

The primary goals of crisis communication should be to alleviate any public concerns about the situation and to protect the Organization's image and reputation. Given the situation, there should be a concern in this process to convey genuine, truthful, and consequential information[9].

Different Organizations must act differently

Organizations are not all created equal. They differ in a variety of ways, including size, activity sector, available resources, the type of data and information they value most, and even their level of cybersecurity maturity. Given these differences, presenting a single approach to crisis communication would be inappropriate for many Organizations' realities. **It was thus decided, within the points of the phases included in this Framework, to establish what is expected of Organizations within different levels of capabilities, according to the CNCS Cybersecurity Capability Assessment Framework's three levels - Initial, Intermediate, and Advanced.**

[8] C-Risk, "*Crisis Communication: How to manage crisis communication after a cyberattack?*", August 2, 2021, updated May 2, 2023, https://www.c-risk.com/en/blog/crisis-communication/.
[9] C-Risk, "*Crisis Communication*".

Table 1

EXPECTATIONS BY CAPABILITY LEVEL - OVERVIEW	
Initial Level	- Although there are processes/measures/activities, these are not structured or defined in a plan, and are mainly carried out on an *ad hoc* basis in isolated, non-formal initiatives.
Intermediate Level	- The processes/measures/activities are planned, documented and formalized, and are carried out and reviewed with some regularity.
Advanced Level	- The processes/measures/activities are planned, documented and formalized, and involve continuous monitoring, recurring evaluation and revision at defined intervals, taking into account changes, incidents, tests and exercises, in order to proactively improve them.

It is critical to emphasize that, while there are different expectations depending on the level of capacity of the Organizations, there are fundamental elements that must be observed at all levels, including the initial level.

After laying the groundwork, Organizations must strive to achieve higher levels of capability through continuous improvement in order to increase their resilience and capacity to respond to crisis situation

PHASE 1

PREPARING THE COMMUNICATION OF A CYBERSECURITY CRISIS

PHASE 1: PREPARING TO COMMUNICATE A CYBERSECURITY CRISIS

1. DEFINING CYBERSECURITY INCIDENT AND CRISIS

To make the communication of a cybersecurity crisis more efficient at any capability level, it is necessary to define what a cybersecurity incident is and what a cybersecurity crisis consists of.

What is a cybersecurity incident?

A cybersecurity incident is an event that has a significant negative impact on the security of networks and information systems[10] .

What is a cybersecurity crisis?

ISO 22361:2022 defines a crisis as "an abnormal or extraordinary event or situation that threatens an organization (3.13) or community and requires a strategic, adaptive and timely response in order to preserve its viability and integrity"[11] .

A cybersecurity crisis can be similarly defined, with the addition that the abnormal or extraordinary situation or event is the result of one or more incidents originating in the cyberspace of interest to the Organization and that have the potential to affect the confidentiality, integrity, and availability of its information systems and technological structure.

To respond appropriately to a cybersecurity crisis, it is critical to develop communication procedures for dealing with such situations. Because it is difficult to predict the duration of a crisis and calculate the impact it may have on an Organization, it is essential that communication during a crisis be agile and effective. Therefore, adequate preparation is required during crisis management to ensure that the action process is successful, that it is carried out simply and frequently, and that it keeps the entities involved and affected by the crisis informed of the progress of the recovery of the impacted systems.

[10] Law no. 46/2018, of August 13.
[11] International Organization for Standardization, "*ISO 22361:2022*", 2.

1.1. CARRYING OUT A RISK ASSESSMENT

An assessment of the risks to which the Organization is exposed must be performed prior to developing a crisis communication plan.

According to the **Guide for Risk Management in matters of Information Security and Cybersecurity**, a Risk Assessment procedure seeks to identify, quantify and describe risks and enable Organizations to prioritize them according to their perceived severity or other established criteria[12] .

This procedure is broken down into three major stages:

1. Risk identification;
2. Risk analysis;
3. Risk assessment.

The goals of this assessment are to determine the value of information assets, to identify the threats and vulnerabilities associated with them, to identify existing controls and their effects on the identified risk, to determine potential consequences or impacts, and, lastly, to prioritize the derived risks.

This analysis will be critical in understanding which scenarios and risks may occur and which should be focused on in order to communicate effectively when they do.

1.2. RISK COMMUNICATION

Once the risks have been identified, analysed, and comprehended, it is time to apply this knowledge to develop a communication strategy tailored to each of the risk scenarios identified.

According to the **Guide for Risk Management in matters of Information Security and Cybersecurity**, risk communication is an activity that aims not only to achieve consensus on how to manage information security and cybersecurity risks, through the exchange and/or sharing of risk information between those responsible and other stakeholders, but also to promote awareness of the importance of the risk management process throughout the Organization.

[12] National Cybersecurity Centre (CNCS), "*Guide to Information Security and Cybersecurity Risk Management*", version 1.1, December 2022, 10, https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11 .pdf.

Table 2

EXPECTATIONS REGARDING RISK ASSESSMENT AND COMMUNICATION BY CAPABILITY LEVEL	
Initial Level	• Risks are identified, but there is no formal process for risk treatment; • There is a generic list of threats, with no mapping or documentation in the risk management methodology; • There is no dedicated risk management team; • Risks are communicated arbitrarily and/or *ad hoc*.
Intermediate Level	• Risks are identified and typified in relation to the information assets; • There is a risk management process that monitors assets according to current and new risks; • There is a map of known threats associated with each type of asset; • There is an indication of the treatment for each mapped threat; • Risks are prioritized according to established treatment criteria, based on the perceived level of exposure and the importance of the asset to the Organization; • Risks are systematically communicated, documented and made available for consultation.
Advanced Level	• There is a formal process for reviewing and analysing identified risks on a recurring basis; • Risks and vulnerabilities are identified automatically by dedicated vulnerability scanning systems; • The risk management process is established with defined criteria and its results and treatment strategies are reviewed at regular intervals; • The risk management process is evaluated and tested for its effectiveness; • Risks are categorized on a scale of importance in order to prioritize treatments; • The treatment of risks takes into account the financial and operational cost between the expected damage and the financial and operational cost of implementing the defined controls. • Risks are communicated in a systematic way, documented, made available in an accessible form and defined and approved by top management.

2. DEFINING A COMMUNICATION PLAN FOR VARIOUS RISK AND CRISIS SCENARIOS

Taking into account the various aspects of a crisis, from its unpredictability to the speed with which everything can change, it is critical that the Organization establishes the appropriate levels of criticality and categorization for different crisis scenarios, for a correct and flexible application of the crisis communication plan, as indicated in the QNRCS (RS.CO-4).

Given this unpredictability, here are some presuppositions to consider when developing a crisis communication plan that can be tailored to a variety of situations.

Presuppositions to consider when developing the communication plan

Although no two crises are alike, some presuppositions must be considered when developing a communication plan for a cybersecurity crisis scenario.

- **Speed**
  During a cybersecurity incident, it is critical that communication is done quickly and reaches the appropriate personnel with responsibility for action. This can only happen if the type of crisis and key employees are identified ahead of time.

- **Transparency**
  It is a presupposition that must be included when developing a cybersecurity crisis communication plan and must be followed throughout the crisis. Organizations in both the private and public sectors should be as transparent and informative as possible.

- **Flexibility**
  Although crisis response planning is extremely useful, unforeseen situations do occur, and so it is critical to ensure that the plan is flexible so that it can be adapted to those unforeseen situations[13].

- **Message unity**
  In times of crisis, it is critical that Organizations communicate with a single voice. By communicating with a single voice, it is meant communicating the same message while maintaining the Organization's cohesion and coherence, without alternative versions or additions. Regardless of who is contacted within the Organization, the message must be consistent. To protect its reputation and mitigate the potential consequences of the crisis, the Organization should communicate what is most important, and it should control the flow of communication (QNRCS: RC.CO-1).

2.1. EXAMPLES OF CYBERSECURITY CRISIS SCENARIOS

The following table provides some examples of scenarios that could lead to a cybersecurity crisis, examples of possible targets, and what should be considered when communicating, including indications of the stakeholders that should receive communications about the crisis in question.

[13] GCS, "*Emergency Planning Framework*", 7.

Table 3

TYPE OF SCENARIO	MOST FREQUENT TARGETS	CONSIDERATIONS ON WHAT TO COMMUNICATE	WHO TO COMMUNICATE
Compromise of systems specific to remote work	Banking, Health, streaming services, postal and transport services, operators of essential services, Public Administration and Sovereign Bodies	• What needs to be said, to whom, and why? • How can the content of the message vary according to the audience and how will this distinction be made? • Does it make sense to define different types of communication for internal and external contacts? • Who needs to be involved in developing the message? • If a crisis has occurred in the past, did communication channels used by the Organization work or were they affected by the crisis? • What communication channels are available at the moment? • What is the best way to reach the audience in a crisis? • How serious is the crisis? • Who might be affected? • What are the possible consequences of this crisis for each of the stakeholders? • How likely is it that the impacts of the crisis on customers will be widely reported in the media? • What is the current number of requests for information from customers? Is it beyond "normal"? • Are we obliged to share information with the affected population? • What are the current and potential reputational impacts? • Do we need to proactively issue communications to key stakeholders? Do we know how to prioritize communications / notifications? • Do we know what timelines we need to meet for communications / notifications?	Management Employees
Cyberespionage	Operators of essential services, Public Administration and Sovereign Bodies		Victims of the crisis Authorities CNCS Management
Compromise of the supply chain	Operators of essential services, Public Administration and Sovereign Bodies		Suppliers Employees Management
Compromise of user accounts	Operators of essential services, Public Administration, Public Bodies, Sovereign Bodies and citizens in general		Customers Suppliers Employees Management
DDoS (Distributed Denial of Service)	Operators of essential services, Public Administration and Sovereign Bodies		Management Customers Suppliers Employees CNCS
Defacements	Operators of essential services, Public Administration and Sovereign Bodies		Management Customers Suppliers Employees CNCS
Exploitation of vulnerabilities	Operators of essential services, Public Administration, Public Bodies, Sovereign Bodies and citizens in general		Management Victims of the crisis CNCS
Intrusion	Operators of essential services, Public Administration and Sovereign Bodies		Management Victims of the crisis CNCS
Phishing, mass phishing and spear phishing	Banking, health, streaming services, postal services and transport operators, operators of essential services, Public Administration, Sovereign Bodies and citizens in general		Management Victims of the crisis CNCS Suppliers
Ransomware and/or cybersabotage	Banking, health, streaming services, postal services and transport, operators of essential services, Public Administration and Sovereign Bodies		Management Customers Suppliers Employees CNCS Authorities
Abuse of AI (Artificial Intelligence)	Public Administration, Sovereign Bodies and citizens in general		Management Victims of the crisis CNCS Suppliers
Deep fakes and varied disinformation	Public Administration, Sovereign Bodies and citizens in general		Management Customers Suppliers Employees CNCS

Source: National Cybersecurity Centre and Cybersecurity Observatory, *"Cybersecurity in Portugal Report: Risk and Conflicts"*, 4th edition, June 2023..

2.2. CREATING A CYBERSECURITY CRISIS COMMUNICATION TEAM

Roles and responsibilities must be assigned and documented in the plan for a communication plan to truly work and be useful during a cybersecurity crisis. It is recommended that the roles listed below be assigned, though more than one role can be assigned to the same person. The following should be defined:

- The **point of contact for** cybersecurity **incidents/crises** and how to contact it[14] ;
- The **incident/crisis response tasks** to be carried out and **who carries out each task**;
- The **person responsible for managing the overall response to the incident/crisis** (must belong to the Organization and have decision-making authority);
- The **person responsible for contacting and passing on information to senior management**;
- The **person responsible for contacting external incident response partners**;
- The **person responsible for reporting the situation to the authorities** (e.g.: police, CNCS, National Security Authority);
- The **person responsible for communication with the media and external partners**;
- Who **will act as spokesperson** (there may be more than one person in this role, according to the needs of the Organization).

Table 4

EXPECTATIONS OF THE INCIDENT REPORTING TEAM BY CAPABILITY LEVEL	
Initial Level	• There is no defined team, but there is informal and unstructured knowledge of the roles of each player in the Organization.
Intermediate Level	• The team is defined. • Employees are aware of the procedures to be followed and the responsibilities to be fulfilled.
Advanced Level	• The team is defined and training exercises to implement the plan are carried out regularly. • Employees are aware of the procedures to be followed and the responsibilities to be fulfilled. • The relevant external stakeholders are involved in the communication activities.

[14] It is important to recall that Public Administration, critical infrastructure operators, operators of essential services, and digital service providers are required by Decree-Law No. 65/2021, of July 30, to designate a permanent point of contact for the security of their network and information systems. This provision ensures uninterrupted communication with the appropriate authorities in the case of a cybersecurity incident.

2.3. IDENTIFYING STAKEHOLDERS

Because a crisis rarely involves just one Organization, it is critical to identify who else will be interested in resolving the crisis and to find ways to make that resolution a collaborative effort.

In a crisis, the relationships and protocols established with other Organizations can be of great assistance. Knowing who to contact within each external entity is critical during a crisis, as it allows Organizations to spend less time making the necessary contacts and more time focusing on resolving the crisis.

As new relationships and protocols are established and others are terminated, it is critical to keep the list of relevant stakeholders up to date in order to avoid both contact with Organizations that are no longer relevant in the current context, and to avoid not reaching out to the Organizations that really should be contacted, informed, and included in the crisis communication and resolution.

It is also critical to consider the Organization's target audience, as they may react unexpectedly to a crisis.

Table 5

EXPECTATIONS REGARDING THE IDENTIFICATION OF STAKEHOLDERS BY CAPABILITY LEVEL	
Initial Level	• The Organization is able to identify internal and external stakeholders and does so on an *ad hoc* basis, with no set interval for updating this record. • The identification is not widely publicized and is not known by all essential workers.
Intermediate Level	• The Organization is able to identify internal and external stakeholders and does so with some regularity. • The identification is publicized and known to all essential workers.
Advanced Level	• The Organization is able to identify internal and external stakeholders, which are reviewed at regular intervals. • The identification is publicized and known to all workers. • Relationships and protocols with internal and external stakeholders are reviewed at regular intervals, keeping the record up to date.

2.4. DEVELOPING A 24/7 CONTACT LIST FOR EMPLOYEES AND RESPONSE PARTNERS

It is critical to have a list of key people who are involved in cybersecurity crisis management and are aware of the crisis in question in order to have an effective communication plan.

These key people may be sorted into internal and external contact lists, making the list easier to manage. The Organisation should ensure that it possesses the correct contact information for each of these people, as well as an indication of the best way of contacting them.

The **internal contact list** should include:

- Leaders of the departments included in the incident/crisis response team (senior management, IT security, operations staff, public relations, legal representatives, etc.);
- CISO (*Chief Information Security Officer*) and the IT security department;
- Individuals in charge of handling communication;
- Employees with operational responsibilities[15] .

The Organization should ensure that it has an up-to-date contact list, prioritized by the main people in charge, and a person in charge of communication. This list should include the times when employees will be absent and their contact information, which should include their names, roles, contact and backup information, and possible alternatives for each role. It is suggested that this list be kept both online and offline, and that it be distributed to members of the cybersecurity incident/crisis response team.

The **external contact list** should include:

- Suppliers of critical systems, who can provide information on the importance of log entries or help identify false positives for certain intrusion detection signatures;
- Internet service providers, which can provide requested information on the main attacks on the network, identify potential origins or potentially block communication paths as necessary;
- Contracted security service providers for monitoring, forensic investigation and analysis, and incident/crisis response, if applicable;
- Insurance brokers and other legal or commercial resources to support business continuity;
- Media[16] .

[15] APPA and Nexight Group, "*Public Power Cyber Incident Response Playbook*', 10.
[16] APPA and Nexight Group, "*Public Power Cyber Incident Response Playbook*',10-11.

Once all relevant stakeholders for an incident/crisis response have been identified, it is critical to identify the contacts of incident response partners from the same sector as the Organization and the government, such as:

- Contacts with authorities (e.g.: local agencies);
- Contacts for organizations to report incidents/crises and share information through the Information Sharing and Analysis Centres (ISAC);
- Contacts for cybersecurity assistance (e.g.: CERT.PT);
- Contact with clients/users.

Maintaining positive relationships with key stakeholders is critical. Even if it is not possible to ensure this good relationship ahead of time, it is critical that communication reflects this goal during a crisis.

Communicating with stakeholders is more than a formality; it is a priority. Communicating information to stakeholders prevents the spread of false information and keeps them informed and reassured. The Organization must ensure that the most effective method of communicating with stakeholders is identified. When an Organization has large departments, it may be beneficial to divide them into areas so that they can be contacted more easily in a crisis[17].

It is recommended that one or more people be designated as **spokespersons**, in accordance with the Organization's size, responsible for **communicating important aspects with the media**. The communication handlers' primary responsibilities are to manage information and support spokespeople in order to protect the Organization's reputation and ensure that all messages are consistent. It is not recommended to wait until a crisis occurs to train the Organization's spokespeople, who should be trained ahead of time. Organizations should make time to prepare and train the approach that will be used when necessary.

[17] GCS, "*Emergency Planning Framework",* 9.

Table 6

EXPECTATIONS REGARDING THE 24/7 CONTACT LIST BY CAPABILITY LEVEL	
Initial Level	• There is a list of internal contacts and a list of external contacts and these are updated from time to time. • The internal list is hierarchical.
Intermediate Level	• There is a list of internal contacts and a list of external contacts that are updated on a regular basis. • The lists are hierarchical and include times of absence and alternative methods of contact during those times.
Advanced Level	• There is a list of internal contacts and a list of external contacts that are updated at set regular intervals. • The lists are hierarchical and include times of absence and alternative methods of contact during those times. • The lists include alternative contacts (people) for situations where the primary contacts are unavailable. • The spokespeople have been trained for potential crisis situations.

2.5. DEFINING COMMUNICATION TEMPLATES FOR THE DIFFERENT STAKEHOLDERS

The incident/crisis response team should develop appropriate communication templates and guidelines for the type and level of information that should be provided to both technical teams and middle managers, senior management, industry partners, CERT.PT, the public, and other relevant entities ahead of time. Appropriate review and approval protocols should also be established to allow information to be disseminated to other participants, partners, and based on their relationship to the crisis and its consequences.

The pre-established communication templates should define:

- What to communicate: what content, what needs to be said immediately (e.g.: how the cybersecurity crisis was handled) to internal and external contacts, how the content can/should differ depending on the audience, and how this distinction should be made;
- What message: form and format, what type of means will be used, from short texts to images, metaphors, videos, etc.;
- Who should communicate: a responsible person/spokesperson should be appointed with the authority and autonomy to communicate, particularly with external Organizations;
- Who to communicate to: recipients of communication;
- How to communicate: which channels should be used for the most effective dissemination of the message (e.g.: emails and screensavers) [18].

[18] GCS, "*Emergency Planning Framework*", 17.

Examples of communication templates can be found in Annex 1.

Table 7

EXPECTATIONS REGARDING COMMUNICATION TEMPLATES BY CAPABILITY LEVEL	
Initial Level	• The Organization has defined a generic communication template for use in crisis situations; • The general template is used both internally and externally.
Intermediate Level	• The Organization has defined different communication templates for internal and external use; • The Organization has defined different communication templates for internal and external use and for different degrees of crisis severity.
Advanced Level	• The Organization has defined different communication templates for internal and external use; • The Organization has defined different communication templates for internal and external use and for different degrees of crisis severity; • The Organization has defined different communication templates for internal and external use, adjusted to the target audiences it wishes to address (e.g.: internal - different departments, such as human resources, legal department, financial department, among others; external - clients, media, business partners, among others).

2.6. DETERMINING THE MEANS BY WHICH COMMUNICATION WILL BE CARRIED OUT

When a crisis occurs, it is critical to have quick and effective means of communication in order to quickly make aspects of the event known to stakeholders. One should consider what the best and quickest methods of disseminating information within the Organization are, and to ensure that all necessary contact information is correct and available.

At this point it is important to consider the following questions:

- If the Organization has already been through a crisis, were the channels used effective? Or were they impacted by the crisis?
- What communication channels does the Organization currently have at its disposal?
- What is the best way to reach the Organization's relevant audiences in a crisis?

Different Organizations and types of crises have different communication requirements. For moments of crisis, it is recommended that appropriate spaces, such as meeting rooms, be identified to serve as situation rooms. The Organization should be aware that cybersecurity incidents and crises can have an impact on the digital systems that normally support communications.

It is recommended that the communication plan include several viable communication alternatives for the incident/crisis response team members. It is recommended that it also includes specific instructions for each alternative in the event that the primary communication system fails during an incident or crisis.

Secure internal communication channels such as e-mail and encrypted chat messages should be used for direct internal actions and the dissemination of necessary information – not all details will be shared with external stakeholders.

Some examples of alternative communications include:

- Secure web portals accessible via the public network with separate authentication systems;
- Secondary and tertiary Internet connections, such as mobile data or satellite;
- E-mail with the previously defined incident/crisis response distribution lists;
- Internet-based collaboration systems and/or audio communication channels;
- Cell phones;
- Landlines;
- Satellite phones;
- VHF/UHF (Very High Frequency/ Ultra High Frequency) radio systems[19] .

[19] PSC, "*Developing an Operational Technology and Information Technology Incident Response Plan",* 28-29.

Table 8

EXPECTATIONS REGARDING ALTERNATIVE MEANS OF COMMUNICATION BY CAPABILITY LEVEL	
Initial Level	• The Organization has alternative means of communication for e-mail and telephone communications.
Intermediate Level	• The Organization has alternative means of communication for secure and encrypted e-mail and telephone communications. • The Organization has its own alternative website or social media profile that serves as a single point of communication for the general public.
Advanced Level	• The Organization has all the above means at its disposal, supported by redundancy systems, such as satellite communication systems that ensure the viability of communications in a crisis.

2.7. DEFINING COMMUNICATION STRATEGY DURING MITIGATION

During a crisis, an organization's primary goal is to mitigate and overcome that situation. To this end, the Organization must define and implement systematic processes and procedures for resolving and dealing with incidents and crises (QNRCS: RS.MI-2).

Once it has been determined who to communicate with and what to communicate, the Organization must decide **when** to communicate. The moments when an incident or crisis is communicated to the relevant stakeholders are critical, as is knowing how to identify the moments when silence is a more prudent option.

In other words, **to avoid alerting the attacker(s) that the Organization is aware of their actions, it may be necessary to define a non-communication phase** from the time the incident is detected until a complete picture of the incident/crisis has been obtained and a plan to mitigate it has been devised. If the attacker(s) are alerted, they may abandon the attack and attempt to wipe out any trace, or they may attempt to cause final damage, such as stealing the Organization's most sensitive information or installing backdoors.

To avoid information leaks during this period of silence, a list of everyone who is aware of the cybersecurity incident or crisis should be kept. If a leak occurs, this list will help identify the person responsible so that legal action can be taken.

As a result, the timing of communication must be determined by the aforementioned objectives, the Organization's mitigation needs, and the needs of the various stakeholders.

[20] CSC, "*Cyber Security Incident Management Guide",* 31.

Table 9

EXPECTATIONS REGARDING ALTERNATIVE MEANS OF COMMUNICATION BY CAPABILITY LEVEL	
Initial Level	• Communication during the incident/crisis mitigation phase is reactive and unstructured.
Intermediate Level	• Communication during mitigation follows predefined procedures. • Mitigation procedures and communication actions during mitigation are documented.
Advanced Level	• Communication is carried out efficiently until the incident/crisis is mitigated. • An analysis is made of communication actions taken during the handling of incidents/crises for the purposes of continuous improvement.

2.8. TESTING THE COMMUNICATION PLAN THROUGH EXERCISES

To respond effectively to a crisis, the response must first be tested. It is critical to include relevant stakeholders in this training process in order to ensure and strengthen the relationship between both parties.

It is difficult to guarantee that a cybersecurity crisis plan will work in a crisis until it has been thoroughly tested.

Preparing and testing the components of an emergency plan are critical steps in preparing for a crisis in order to identify existing flaws and assist the Organization and employees in becoming aware of them, and thus identifying measures to address them.

Why are plan testing exercises so important? Because they permit:

- Training;
- Testing;
- Validating the plan.

What kind of exercise is best for the Organization? The type of exercise chosen will be determined by a variety of factors such as duration, cost, facilities, and participant availability.

The following are three options for training exercises, along with the benefits and drawbacks of each:

Table 10

DISCUSSION-BASED EXERCISES	TABLE-TOP EXERCISES	LIVE EXERCISES
These provide opportunities to talk through plans in a group context, enabling the approach to be checked and amended and ensuring everyone has a clear sense of the strategy.	These exercises are simulated exercises that often revolve around testing a specific scenario. They are good for validating plans and exploring potential weaknesses.	These involve a full, live rehearsal of the implementation of a plan and work well for testing logistics, communications and physical capabilities.
PROS		
• Low cost, quick and relatively easy to set up. • Useful at development stage to refine plans. • They ensure that everyone has a clear sight of the plans.	• Useful for stress-testing plans and helping those involved to understand their role. • Can identify potential weaknesses in the approach. • Help strengthen working relationships in a practical way.	• Teams gain direct, hands-on experience of scenarios, learning by doing. • Tests how staff and systems can respond in an actual crisis situation. • Tests logical and operational challenges as well as strategy.
CONS		
• More difficult to test logistical and operational challenges that may arise during crisis. • Does not test how staff or systems might respond in “real” life.	• Requires careful planning to develop appropriate scenarios. • Identifying the format and venue can be a challenge. • Does not test how staff or systems might respond in “real” life.	• Can be very expensive and take a long time to plan and deliver. • They can have unintended consequences, such as undermining staff confidence.

Source: GCS, “*Emergency Planning Framework*”.

Recommendations for crisis communication plan testing exercises:

The Organization should establish clear objectives for the exercises to be carried out. Attempting to test all aspects of a plan in a single exercise may be overly ambitious, if not downright counterproductive. It is therefore recommended that the exercises be designed to test the ability to carry out the functions defined and assigned in the plan, with these functions distributed across several exercises to be completed at different times[21].

Having several exercises that test different capabilities rather than a single exercise that attempts to test all aspects of the plan does not imply that the exercises are oversimplified. The crisis scenario defined for each exercise should be appropriately challenging, complex, and realistic, reflecting the general characteristics of a crisis that is likely to occur within the Organization[22].

2.8.1. EXERCISE EVALUATION

Following the completion of each exercise, the Organization must assess whether the performance recorded during the exercise corresponds to the desired performance. If it falls short, any observed flaws should be identified and recorded so that they can be corrected and improved upon at a later stage[23].

Organizations must conduct a rigorous analysis of the performance obtained in an exercise during the evaluation process and not ignore any shortcomings. A false sense of security in an Organization's ability to respond to crises can have serious consequences. It is also prudent to consider not only human flaws, but also whether the crisis communication plan itself meets the needs of the Organization during a crisis, or whether it should be improved.

After analysing the performance during the exercise and identifying the failures, an action plan should be developed and implemented to correct these failures. Once these failures have been corrected (and their correction tested in subsequent exercises), this correction can be labelled as "lessons learned"[24] .

[21] International Organization for Standardization, "*ISO 22361:2022*", 33.

[22] International Organization for Standardization, "*ISO 22361:2022*", 33.

[23] International Organization for Standardization, "*ISO 22361:2022*", 34.

[24] International Organization for Standardization, "*ISO 22361:2022*", 34.

Post-exercise activities should include:

- Structured questionnaires for those involved in the exercise;
- Scrutiny and evaluation of decisions and their implementation;
- Identification of the strengths observed and opportunities for improvement;
- Analysis of compliance with the objectives set for the year in question;
- Lessons identified and their relevance to the Organization's capacity building;
- Action plans for implementing the lessons and a mechanism for confirming implementation.

2.8.2. VALIDATION OF THE EXERCISES AND THE PLAN

Finally, exercises should be used to validate the crisis communication plan.

This validation should take place only after the exercises have been completed and the identified improvements have been implemented, including testing of these improvements in subsequent exercises.

Once the plan's ability to be implemented at the desired level has been demonstrated, as well as its suitability for the Organization's needs in a crisis context, it must be validated by the Organization's top management.

After the plan has been validated, it must be tested on a regular basis to ensure that its execution capacity is maintained and that it is up to date.

It should be emphasized that exercises should contribute to the development of capabilities on both a collective and individual level, with the goal of continuous improvement within the Organization. The exercises should allow to capitalize on previously identified strengths and provide opportunities for improvement over time[25] .

[25] International Organization for Standardization, "*ISO 22361:2022*", 34-35.

Table 11

EXPECTATIONS REGARDING THE TESTING OF THE COMMUNICATION PLAN BY CAPABILITY LEVEL	
Initial Level	• Simple exercises (mainly discussion exercises) are carried out to test the communication plan on a one-off basis, with no set regularity.
Intermediate Level	• Exercises simulating specific crisis scenarios are carried out with some regularity. • Strengths and opportunities for improvement are identified during the exercises. • An action plan is drawn up for implementing the improvements, and these improvements are tested in new exercises.
Advanced Level	• Real exercises are carried out to test the strategy adopted, the actual reaction of the staff and the systems that may be affected at set regular intervals. • Strengths and opportunities for improvement are identified during the exercises. • All decisions made during the exercise are scrutinized and evaluated. • Questionnaires are given to all those involved in the exercises. • An action plan is drawn up for implementing the improvements, and these improvements are tested in new exercises.

PHASE 2

RESPONDING EFFECTIVELY

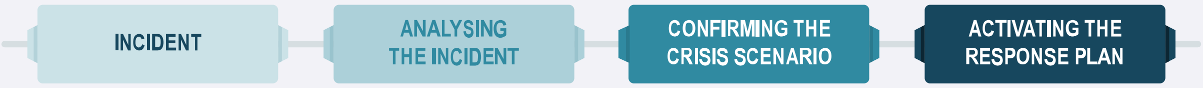
PHASE 2: RESPONDING EFFECTIVELY

Employees, particularly those involved in crisis resolution, must know their roles and carry out their activities correctly in order to respond effectively to a crisis, according to the NRCS (RS.CO-1).

1. ACTIVATING THE COMMUNICATIONS TEAM

When a cybersecurity incident is detected, it must be investigated and confirmed. If it is determined that the detected incident is indeed a crisis, the incident/crisis response team, including the crisis communication team, should be activated.

Figure 3: Response plan activation procedure



Depending on the severity of the situation, it may not be necessary to mobilize all resources and employees to respond to the crisis. To put it another way, a low-severity crisis may only require the deployment of an IT technical support team, a public relations team, and legal representatives to contain and investigate it, whereas a high-severity incident or crisis may require the immediate deployment of all elements with incident/crisis response responsibilities to launch a response operation with all available capacity.

The Organization's cybersecurity crisis response plan should outline the process for activating the response team as well as all the logistics that will be required to support it. The incident/crisis response team should determine how frequently the team meets and is briefed, how crisis updates are provided (e.g.: email, face-to-face meetings), and communication methods to be used if core systems have been compromised by the cybersecurity crisis.

In this regard, the items mentioned in Phase 1 should be prepared for the coordination of the incident/crisis response team, such as:

- One or more dedicated meeting rooms (war rooms), centralizing communications and coordination and a dedicated communication channel for team members to exchange information;
- Cipher messaging systems or other secure systems for crisis communication;
- Dedicated cell phones for members of the incident/crisis response team for "after hours" support and workplace communications;
- Printed copies of incident/crisis response procedures, contact lists and incident/crisis handling forms;
- Secure storage infrastructures to protect evidence and other confidential materials;
- Secure filing systems, applications or databases with restricted access to store confidential incident/crisis handling forms and information[26] .

2. REPORTING INCIDENTS AS REQUIRED BY REGULATIONS AND CONTRACTS

Organizations are required to report cybersecurity incidents for two reasons.

The first reason is compliance - legal, regulatory, and contractual - in order to avoid violating current laws, regulations, or contracts.

The second reason is the Organization's reputation. Organizations that postpone reporting an incident or crisis to the appropriate stakeholders, or that allow those stakeholders to learn about the incident or crisis from other parties rather than themselves, suffer the greatest reputational losses. Organizations that notify stakeholders of incidents/crises, on the other hand, tend to perform better in terms of maintaining their reputation and customer trust intact.

For these reasons, the aim of informing stakeholders and reporting an incident must be included in the Organizations' communication plan, which must be supported by the respective communication strategies outlined in the QNRCS (DE.PD-4, RS.CO-2, RS.CO-3).

[26] APPA and Nexight Group, "*Public Power Cyber Incident Response Playbook*', 16.

There are, however, precautions to be taken before reporting an incident or crisis to stakeholders. It is critical to consider:

- Consulting the Organization's legal department (or lawyers) before making any reports outside the Organization;
- Determining and authorize in advance which circumstances are acceptable for making the notification;
- Reviewing information protection and confidentiality agreements in place before voluntarily sharing information;
- Working with the legal team to review and sign confidentiality agreements in advance;
- Identifying clearly what kind of information can be shared regarding the incident/crisis with other entities;
- Identifying contacts and building relationships with authorities in advance. Understand the expectations from authorities regarding the level of information and access to be given to them if the Organization reports a cybercrime and how to coordinate with law enforcement during response and recovery[27].

2.1. REPORTING CYBERSECURITY INCIDENTS TO THE CNCS:

As stated in Article 11(1) of Decree-Law No. 65/2021, of July 30, Public Administration, critical infrastructure operators, operators of essential services and digital service providers notify the CNCS of the occurrence of incidents with a relevant or substantial impact under the terms of Articles 15, 17 and 19, respectively, of the Legal Regime for Cyberspace Security (Law No. 46/2018, of August 13).

There are three types of notification to take into account:

a) Initial notification (Article 13 of Decree-Law 65/2021);

b) Notification of end of relevant or substantial impact (Article 14 of Decree-Law 65/2021);

c) Final notification (Article 15 of Decree-Law 65/2021).

[27] APPA and Nexight Group, "*Public Power Cyber Incident Response Playbook*', 17.

a) Initial notification

The initial notification must be sent as soon as the entity can conclude that there is or may be a relevant or substantial impact, and no later than two hours after such verification, and the entity must prioritize mitigating and resolving the incident, without prejudice to compliance with this deadline.

The initial notification must include the following information:

1. Name, telephone number, and e-mail address of an entity representative, if different from the permanent point of contact referred to in Article 4, for possible contact by the CNCS;
2. Date and time of start of the incident or, if this cannot be determined, of its detection;
3. A brief description of the incident, including an indication of the root cause category and the effects produced, in accordance with the taxonomy defined in Article 16 and, where possible, the respective detail;
4. Estimate of the impact, considering:
   - i) Number of users affected by the service's disruption;
   - ii) Duration of the incident;
   - iii) Geographical distribution, with regard to the area affected by the incident, including an indication of cross-border impact;
5. Other information that the entity considers relevant.

b) Notification of end of relevant or substantial impact

The notification of end of relevant or substantial impact of the incident must be submitted to the CNCS as soon as possible, within a maximum of two hours after the loss of relevant or substantial impact.

The notification of end of a material or substantial impact must include the following information:

1. Updating the information transmitted in the initial notification, if any;
2. A brief description of the measures taken to resolve the incident;
3. Description of the situation of the impact existing at the time of the end of relevant or substantial impact, namely:
   - i) Number of users affected by the service disruption;
   - ii) Duration of the incident;
   - iii) Geographical distribution, with regard to the area affected by the incident, including an indication of cross-border impact;
   - iv) Estimated time for full recovery of services.

c) Final notification

The final notification must be sent within 30 working days of the incident's conclusion.

The final notification must include the following information:

1. Date and time when the incident had a relevant or significant impact;
2. Date and time when the incident ceased to be relevant or significant;
3. Impact of the incident, considering:
    i) Number of users affected by the service disruption;

    ii) Duration of the incident;

    iii) Geographical distribution, with regard to the area affected by the incident, including an indication of cross-border impact;

    iv) Description of the incident, indicating the root cause category and the effects produced, according to the taxonomy defined in the following article, and the respective detail;
4. Indication of the measures taken to mitigate the incident;
5. Description of the residual situation of the impact existing on the date of the final notification, in particular:
    i) Number of users affected by the service disruption;

    ii) Geographical distribution, with regard to the area affected by the incident, including an indication of cross-border impact;

    iii) Estimated time for full recovery of the services still affected;
6. Indication, where applicable, of the submission of notification of the incident in question to the competent authorities, namely the Public Prosecution Service, ANEPC, ANACOM, CNPD, the Portuguese Criminal Investigation Police, and other sectoral authorities, in accordance with the applicable legal and regulatory provisions;
7. Other information that the entity considers relevant.

In cases where there is a residual situation of the impact on the date of the final notification, as described in point 5, the entities must communicate the full recovery of this residual situation to the CNCS as soon as possible.

How to notify the CNCS?

Incident notifications and additional information must be sent to the CNCS via the CNCS *website* – **https://www.cncs.gov.pt** – in the "Incident Notification" section, by filling in the reporting template established for this purpose, or via the API (Application Programming Interface) made available by the CNCS. If, as a result of the incident or for another duly justified reason of an eminently technical nature, the entity does not have the operational capacity to ensure notification on the CNCS website, or if it is unavailable, notification may be made via:

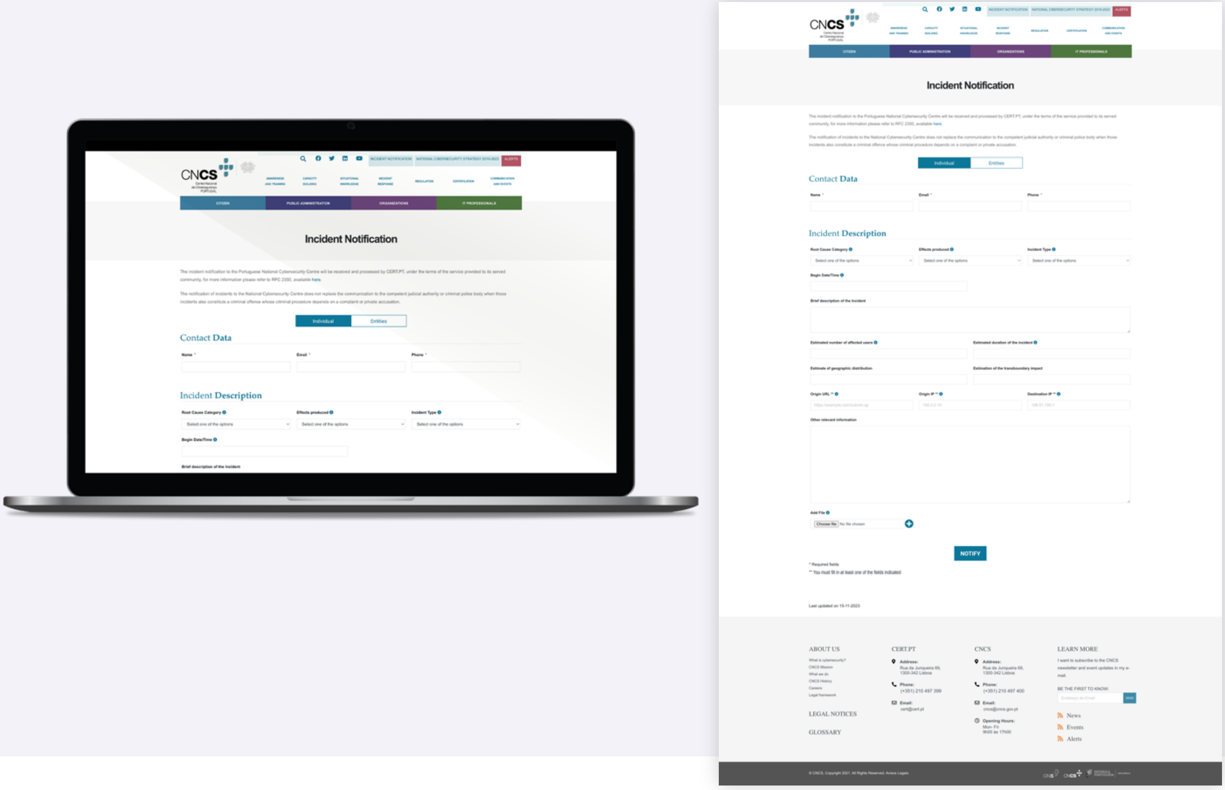
– Email to the following address: **cert@cert.pt**;

– Telephone number **(+351) 210 497 399**;

– Telephone number **(+351) 910 599 284**, available 24 hours a day, seven days a week.

If the entities wish to send the notification protected by a cryptographic method, they can protect the information using the PGP public key, associated with the aforementioned email address – **cert@cert.pt** –, published on the CNCS website. The public key is available at **https://www.cncs.gov.pt/pt/certpt/chave-pgp/**.

Figure 4: CNCS Incident Notification Form.



Incident Notification

The incident notification to the Portuguese National Cybersecurity Centre will be received and processed by CERT.PT, under the terms of the service provided to its served community, for more information please refer to RFC 2350, available here.

The notification of incidents to the National Cybersecurity Centre does not replace the communication to the competent judicial authority or criminal police body when those incidents also constitute a criminal offence whose criminal procedure depends on a complaint or private accusation.

Contact Data

Name *

Email *

Phone *

Incident Description

Root Cause Category: Select one of the options

Effects produced: Select one of the options

Incident Type: Select one of the options

Begin Date/Time

Brief description of the incident

Estimated number of affected users

Estimated duration of the incident

Estimate of geographic distribution

Estimation of the transboundary impact

Origin URL **: https://example.com/submit.cgi

Origin IP **: 192.0.2.14

Destination IP **: 198.51.100.1

Other relevant information

Add File: Choose file No file chosen

* Required fields

** You must fill in at least one of the fields indicated

Last updated on 15-11-2023

CERT.PT
Address: Rua da Junqueira 69, 1300-342 Lisboa
Phone: (+351) 210 497 399
Email: cert@cert.pt

CNCS
Address: Rua da Junqueira 69, 1300-342 Lisboa
Phone: (+351) 210 497 400
Email: cncs@cncs.gov.pt
Opening Hours: Mon- Fri 9h00 às 17h00

LEARN MORE
I want to subscribe to the CNCS newsletter and event updates in my e-mail.
BE THE FIRST TO KNOW:

© CNCS. Copyright 2021. All Rights Reserved. Avisos Legais.

It should also be noted that, in addition to the previously mentioned entities, any entity may voluntarily notify incidents that have a significant impact on the continuity of the services it provides. This voluntary notification cannot impose obligations on the notifying entity that would not have existed if the notification had not been made.

It should also be highlighted that the notification of incidents to the CNCS does not exempt entities from other notification obligations, such as notification obligations arising from the General Data Protection Regulation (GDPR), to the supervisory authority and/or to data subjects, in the event that the incident resulted in a personal data breach and the circumstances of that breach require such notifications, nor does it replace communication to the competent judicial authority or criminal police body when such incidents also constitute a criminal offense whose prosecution depends on a complaint or private accusation.

Benefits of early incident notification

i) Identifying coordinated attacks or attack trends by correlating incidents across the industry. When suspicious or confirmed incidents are reported to government entities, these partners can analyse the report in relation to other reports and threat intelligence, allowing for the early detection of a more coordinated and widespread attack;

ii) Mitigation measures. Organizations can recommend mitigation steps for cybersecurity incidents or conduct malware or threat analysis to identify and mitigate the incident;

iii) Assistance with incident investigation. Various external response groups, either remotely or locally, can assist with forensic analysis and investigation of an incident;

iv) Preparing resources for response and coordination. Notifying external response groups in advance can assist in initiating coordination between sectors, preparing response teams for potentially serious incidents, and supporting message coordination between response partners[28] .

Table 12

EXPECTATIONS REGARDING INCIDENT REPORTING BY CAPABILITY LEVEL	
Initial Level	• There's informal and unstructured awareness of incident reporting channels.
Intermediate Level	• The ability to report incidents is guaranteed; • Incident reporting criteria have been established.
Advanced Level	• Criteria have been established for involving external stakeholders in the handling of incidents; • Incidents are reported in an integrated manner.

[28] APPA and Nexight Group, "*Public Power Cyber Incident Response Playbook*', 17.

3. DOCUMENTING THE INCIDENT

A detailed and accurate record of the information relating to the suspected incident should be started as soon as possible, and the documentation of the incident should be constantly updated during the response action.

The person in charge of coordinating the response to cybersecurity incidents must lead the team in the information-gathering function, which will allow the response to be documented during the incident's course; inform the incident response team and/or other stakeholders; and conduct the necessary reports or other notifications, such as:

- The type of incident;
- The date and time of the incident;
- Whether the incident is still active;
- How the incident was identified and the employees who identified it;
- The affected devices, applications or systems;
- The current or future impacts of the incident, in the internal and external context of the Organization;
- The type and sensitivity of the data stored on the affected systems;
- Any mitigation measures planned or already taken;
- Logs or other records of the incident;
- List of stakeholders already contacted or other resources involved;
- Details of the points of contact between the incident response team and the Organization[29] .

Keeping records of incident information requires the use of a secure application or database, access to which must be restricted according to the sensitivity of the data contained therein.

[29] APPA and Nexight Group, "*Public Power Cyber Incident Response Playbook*', 29.

Table 13

EXPECTATIONS REGARDING THE DOCUMENTATION OF INCIDENTS BY CAPABILITY LEVEL	
Initial Level	• The incident is documented in a loosely structured way and without uniformity of information.
Intermediate Level	• Incident documentation practices are in place; • Information about the incident is collected in a structured and uniform way.
Advanced Level	• Templates are defined for documenting the incident; • The templates record all the points mentioned above; • The structure of the information collected allows for the incident documentation to be easily read by the relevant stakeholders.

4. COMMUNICATING THE FORMAL CLOSURE OF THE CRISIS

Most of the time, the pressure of a crisis causes Organizations to want to get out of that crisis as soon as possible, which can lead to falling short of taking all necessary steps to resolve it. One step that is frequently overlooked is communicating the formal closure of the crisis.

Communicating the formal closure of the crisis entails communicating its end both internally and externally. At this stage, communication includes, in addition to announcing the end of the crisis, communicating the activities undertaken to overcome it, as well as conveying to stakeholders and public opinion in general the message that the Organization has learned from what happened and is now better prepared for the future and better able to withstand similar events. This is also an appropriate time to thank everyone who has contributed to the crisis' resolution, both individually and institutionally.

This communication is important at both an internal and external level. Messages should be sent thanking everyone for their efforts and emphasizing the importance of everyone being prepared for situations like this, emphasizing the need for all Organization members to be on alert[30] .

[30] CCN-CERT, "*Gestión de Cibercrisis*", 25.

Table 14

EXPECTATIONS REGARDING FORMAL CRISIS CLOSURE ACTIVITIES BY CAPABILITY LEVEL	
Initial Level	• There is no defined procedure for communicating the formal closure of the crisis. • The closure of the crisis is communicated internally and externally by means of a general and simple message, for example by email, internally, and by publishing on the Organization's website or social network page, externally.
Intermediate Level	• Procedures are defined for communicating the formal closure of the crisis. • The closure of the crisis is formally communicated internally and externally, following the defined procedures, mentioning, as far as possible, the reasons for the crisis and the measures taken to resolve it.
Advanced Level	• Procedures have been defined for the formal closure of the crisis. • The closure of the crisis is formally communicated internally and externally, following the defined procedures, mentioning, as far as possible, the reasons for the crisis and the measures taken to resolve it, expressing thanks and demonstrating the Organization's commitment to becoming more resilient to similar situations that may occur in the future. • Procedures are in place to review incidents/crises and the communication made during their resolution.

5. RECOVERING REPUTATION

Just like the formal closure of the crisis, recovery activities are frequently overlooked as the final stage in crisis communication, as Organizations and teams seek to resume normal routines as soon as possible.

The Organization must ensure that all stakeholders (internal and external) are kept up to date on recovery efforts (NRCS: RC.CO-2).

Following a crisis, communication is critical in assisting the Organization in redefining relations with those affected and rebuilding any reputational losses that may have occurred[31] .

Here are six activities that can help the team and the Organization rebuild and repair its reputation and/or relationships[32] .

[31] ANSSI, "*Crisis of Cyber Origin: The Keys to Operational and Strategic* Management", 20.
[32] GCS, "*Emergency Planning Framework",* 33.

Considering recovery from the start

Recovery must be prioritized from the beginning of a crisis. If a crisis ends without a plan for recovery, the immediate opportunity to repair any damage to the Organization's reputation may be lost.

RECOMMENDATIONS:

- Assign one or two team members to work closely with legal colleagues on recovery while the crisis is still ongoing;
- Establish clear objectives on rebuilding reputation that can help inform action while the crisis is still being managed.

Building trust through actions, not words

A crisis can fundamentally alter one or more stakeholders' opinion of the Organization. As a result, demonstrating that the Organization's performance is once again in line with the expectations of the stakeholders regarding the Organization's activities and services can be a good way to rebuild this trust.

RECOMMENDATIONS:

- Reputation is demonstrated through actions. The best way to restore reputation is to show how commitments have been and will continue to be met;
- For communicators, this means demonstrating what is being done. In other words, any communication must be supported by evidence that can be presented to stakeholders.

Involving the Organization's employees

Maintaining internal cohesion during a crisis is critical to its resolution. Employees should therefore be kept as up to date as possible on the crisis, from its inception to its resolution.

RECOMMENDATIONS:

- Making sure that internal communication is an integral part of any recovery plan - the employees themselves are the Organization's greatest advocates;
- Communicating with senior management about the challenges of engaging and reconnecting with staff after a crisis - their visibility is vital.

Redefining the agenda through active communication

It is critical not to allow the Organization to be constrained by a crisis. As a result, communication must be proactive, coherent, and based on decisions made to make the Organization more resilient to future crises.

RECOMMENDATIONS:

- Developing a coherent and proactive communication plan that supports the Organization's decisions;
- Reflecting on how the Organization can demonstrate its leadership capacity and overcome the crisis by redefining its priorities.

Keeping promises and meeting deadlines

During a crisis, Organizations often choose to make promises or guarantees in order to reduce criticism of those responsible for the crisis.

RECOMMENDATIONS:

- Following up on all the commitments made publicly during the crisis and make sure that the deadlines for these commitments are met;
- Making sure that the teams keep in touch with those responsible for fulfilling their commitments, so that they can manage them proactively and reduce the risk of loss of reputation.

Using windows of opportunity to deliver lasting change

During a crisis, Organizations should take advantage of any "window of opportunity" to change their direction, values, or strategy.

RECOMMENDATIONS:

- Reflecting on what unintended consequences can be exploited (for example: a drought can be an opportunity to change the target audience's attitudes towards water consumption);
- Reflecting on how the crisis may have changed the communication scenario.

It should be noted that these indications and recommendations cannot guarantee the restoration of an Organization's reputation, but they can serve as a good starting point[33] .

[33] GCS, "*Emergency Planning Framework",* 33-34.

Table 15

EXPECTATIONS REGARDING REPUTATION MAINTENANCE/RECOVERY ACTIVITIES BY CAPABILITY LEVEL	
Initial Level	• *Ad hoc* measures are adopted to mitigate reputational impacts or losses.
Intermediate Level	• Activities/measures are defined to maintain/recover the Organization's reputation; • The Organization is proactive in communication, making commitments (e.g., providing status updates at regular intervals) and following through on them with reasonable rigor.
Advanced Level	• A strategy for recovering/maintaining the Organization's reputation has been established; • The Organization is proactive in communication, establishing commitments and meeting them within the established deadlines; • The Organization has the capacity to, if necessary, redefine priorities and strategies, communicating these changes to the relevant stakeholders.

PHASE 3

LEARNING LESSONS AND IMPROVING

PHASE 3: LEARNING LESSONS AND IMPROVING

The moments after a crisis provide an opportunity to learn and improve procedures. As a result, establishing a feedback process on the actions and activities undertaken in resolving the crisis is critical for learning lessons and improving the response to similar situations in the future.

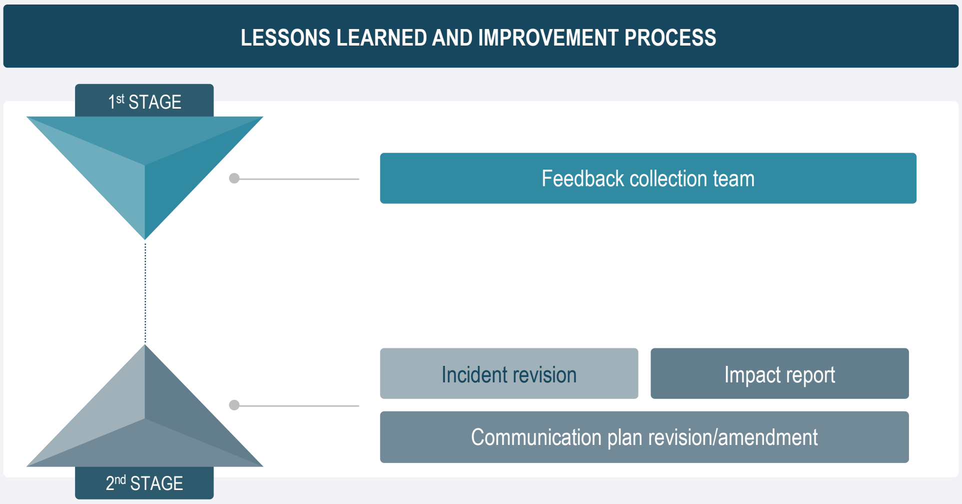
The feedback process should be divided into two stages based on the strategic component of the Organization.

The first stage of the process should begin with the Organization's strategic unit identifying the team responsible for collecting feedback on crisis management.

Once this team has been formed, the people who will be interviewed about the crisis and crisis management should be identified, as should the order in which they will be interviewed. It is also recommended that the practical aspects of the round of interviews be structured (timetable, form, summary, documentation, coordination)[34] .

After collecting feedback, which must be structured and organized so that it can be presented to the Organization's strategic and operational components, the feedback process must be completed within the maximum timeframe defined by the Organization, between the end of the crisis and the end of the feedback process, by requesting an investigation report and its summary (for management teams) from the providers of the services mobilized.

Figure 5: Process for gathering feedback, lessons learned and improvements


LESSONS LEARNED AND IMPROVEMENT PROCESS

1st STAGE

Feedback collection team

Incident revision

Impact report

Communication plan revision/amendment

2nd STAGE

[34] ANSSI, "*Crisis of Cyber Origin: The Keys to Operational and Strategic* Management", 64.

The information obtained from the crisis review can help the operational response in several ways:

- It must keep the crisis response team on track by reminding them of their communication objectives;
- It must allow the content and dissemination channels to be adapted quickly in response to any feedback;
- It should show whether important messages are reaching the intended audience and where additional investment is required to inform or persuade the intended audience.

1. CRISIS REVIEW AND COMMUNICATION PLAN GLOBAL ASSESSMENT

The cybersecurity crisis management plan should include a post-crisis review and lessons learned (QNRCS: RC.ME-1).

A crisis review is a detailed retrospective that allows an Organization to understand every aspect of the crisis from beginning to end. It is a step in the incident/crisis response process that allows for the full comprehension of the cause and scope of the incident/crisis.

Evaluating the communication plan – or evaluating its execution and the impact of the selected messages – is critical for the Organization to verify the adequacy of the existing plan and to understand the expectations of the media and other stakeholders, allowing it to improve its communication processes, mechanisms, and strategies for future circumstances.

To do so, it is necessary to assess whether the information of the main contacts was available from the start of the crisis, as well as whether the communication channels defined for crisis situations operated without any issues. This assessment enables the Organization to update and improve its information on crisis contacts, as well as to update the best communication channels to use in these situations.

It is also necessary to evaluate whether the developed message had the desired effects on the intended target audiences. This allows the Organization to determine whether the message should be modified for future occasions or not.

Checking with stakeholders to ensure there has been a formal closure of the crisis is critical to reassuring them that the crisis has been resolved. Carrying out this activity could make the difference between the Organization and its partners maintaining trust.

It is also important to determine whether the Organization's reputation has been harmed, whether it has been preserved, or whether it has had to be restored. This validation is required in order to apply the appropriate resources to each situation.

After performing these evaluations and verifications, as well as any others that may be considered relevant, it is critical to review and/or reformulate the communication plan in order to correct any flaws that may have been identified, so that they are not repeated at a later date.

A good crisis review should result in a list of practical actions that address each of the factors that contributed to the attacker's success. The practical actions listed should improve the Organization's resilience to attack attempts, response capacity, and communication.

The updated communication plan should reflect the list of practical actions resulting from the crisis review. All those involved in incident/crisis response activities should be kept up to date on any changes[35].

Table 16

EXPECTATIONS REGARDING THE LESSONS LEARNED AND IMPROVEMENT PROCESS BY CAPABILITY LEVEL	
Initial Level	• The Organization carries out an informal review of the crisis. There is no formal method for reviewing and evaluating the failures that may be identified; • The communication plan is updated in line with the faults detected.
Intermediate Level	• Metrics relating to recovery plans exist and are evaluated; • The teams (internal and external) involved in incident/crisis recovery are trained and managed, and communication flows are established between them; • The communication plan is formally updated according to lessons learned and applicable improvements identified.
Advanced Level	• Procedures are in place for the periodic review of recovery strategies by top management; • The analysis of lessons learned to improve incident/crisis response procedures includes: ○ Support documents for the incident/crisis response plan; ○ Records of meetings and other interactions, in the context of continuous improvement; ○ Records of the treatment of vulnerabilities resulting from incidents/crises that have occurred. • Recovery plans are updated according to the improvements identified and with the involvement of top management.

[35] Cybereason, "*Post-Incident Review: Examining the Importance of Post-Incident Review for Security Teams*", https://www.cybereason.com/resources/post-incident-review.

2. MONITORING AND REVIEWING RISKS

Even in the absence of a cybersecurity crisis, Organizations should conduct regular risk monitoring and reviews.

However, there is always the possibility that a crisis will occur, which is why Organizations must review and reassess not only the crisis and existing response plans, but also the risks, following a crisis. This review and reassessment enable Organizations to change the classifications and levels assigned to the risks identified during the crisis, as well as to identify new risks not previously identified in the Organization (NRCS: RS.MI-3).

This review, duly documented, is required due to the constant change in the probability and impact of the risks known to the Organizations, as well as the emergence of new risks that impact their business continuity.

After the post-crisis risk review and reassessment has been completed and documented, it is critical to return to the risk communication and consultation process in order to reach a new consensus on how to manage the new information security and cybersecurity risks.

The communication of the risk review and reassessment should include the sharing of risk information between those responsible in the Organization and the relevant stakeholders (NRCF: RC.CO-2) in order to alert staff to new risks and promote awareness of them throughout the Organization if they are discovered.

Table 17

EXPECTATIONS REGARDING THE MONITORING AND REVISION OF RISKS BY CAPABILITY LEVEL	
Initial Level	• Monitoring and review is carried out on an ad hoc and unstructured basis.
Intermediate Level	• There is an established vulnerability/risk management process; • There are defined criteria for mitigating vulnerabilities/risks.
Advanced Level	• The vulnerability/risk assessment process is well-defined and constant. • There is a process for formalizing and accepting vulnerabilities/risks; • New risks/vulnerabilities are communicated to the Organization's managers and its stakeholders.

4. METHODOLOGICAL NOTES

The primary goal of this document is to prepare Organizations for crisis situations and to advise them on how to report them to the appropriate authorities, including the CNCS.

As such, the methodology used in the creation of this document began with the collection of data and information from various reference documents on the preparation and communication of cybersecurity crises, which are used by various countries whose cybersecurity maturity is comparable to or greater than that of Portugal. This was followed by a phase of data and information analysis, culminating in a revision of the text produced.

The data was provided by the CNCS, and PwC, CNCS's partner, performed the analysis and subsequent drafting and production of this document.

5. BIBLIOGRAPHY

5.1. MAIN REFERENCES:

1. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). "*Crisis of Cyber Origin: The Keys to Operational and Strategic Management*". March 2022.
https://www.ssi.gouv.fr/uploads/2022/05/20220516 np anssi guide gestion crise cyber en.pdf

2. American Public Power Association (APPA) e Nexight Group. "*Public Power Cyber Incident Response Playbook*". August 2019.
https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Play book.pdf

3. Centro Criptológico Nacional (CCN-CERT). "*Gestión de Cibercrisis. Buenas Prácticas en la Gestión de Crisis de Ciberseguridad'.* 2020.
https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5428-ccn-cert-bp-20-buenas-pra- cticas-en-la-gestio-n-de-cibercrisis-1/file.html.

4. Cyber Security Coalition (CSC). "*Cyber Security Incident Management Guide*". January 2016, reviewed in September 2021.
https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide- EN.pdf

5. Government Communication Service (GCS). "*Emergency Planning Framework*'. 2018.
https://gcs.civilservice.gov.uk/wp-content/uploads/2020/04/Emergency-planning-framework-1.pdf

6. International Organization for Standardization, "*ISO 22361:2022 - Security and resilience — Crisis management — Guidelines* ".
https://www.iso.org/standard/50267.html

7. Public Safety Canada (PSC). "*Developing an Operational Technology and Information Technology Incident Response Plan* ". 2020.
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dvlpng-ndnt-rspns-pln/index-en.aspx

5.2. OTHER REFERENCES

1. National Cybersecurity Centre (CNCS). "*Guide to Risk Management in Information Security and Cybersecurity Matters*". Version 1.1, December 2022.
   https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf

2. National Cybersecurity Centre (CNCS) and Cybersecurity Observatory. "*Cybersecurity in Portugal: Risks and Conflicts Report*" 4th edition: June 2023.
   https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf

3. C-Risk."*Crisis Communication: How to manage crisis communication after a cyberattack?*". August 2, 2021, updated May 2, 2023.
   https://www.c-risk.com/en/blog/crisis-communication/

4. Cybereason. "*Post-Incident Review: Examining the Importance of Post-Incident Review for Security Teams".*
   https://www.cybereason.com/resources/post-incident-review

5. Government Communication Service Behavioural Science Team. "*Crisis communication: A behavioural approach*". Cabinet Office, August 2022.
   https://gcs.civilservice.gov.uk/publications/crisis-communication-a-behavioural-approach/

5.3. LEGISLATION

1. Law no. 46/2018, of August 13.

2. Decree-Law no. 65/2021, of July 30.

6. ANNEXES

A1: Communication template examples

Communication templates should define what to communicate (content), what message to use (short text, metaphors, images, videos), who should communicate, who to communicate to (which stakeholders will receive the information), and how to communicate, as stated in the Framework (channels to be used to disseminate the message, such as e-mail or SMS).

The template examples presented in this Framework are just that: examples, so Organizations should try to adapt them to their communication needs in a crisis as best they can. Organizations should also consider the need for new communication moments with their stakeholders.

To adapt the examples provided, Organizations should try to anticipate potential crisis scenarios as much as possible and define their communication templates based on the anticipated scenarios and the Organization's communication objectives.

Example 1: Generic template (for internal and external use)

Communication recipients: Internal and external stakeholders

Recommended means of communication: SMS, e-mail, publication on website/social networks

"Hello, everyone.

(Name of Organization) would like to inform you of a recent cybersecurity incident that has affected the Organization.

Since the incident was discovered at (insert time) on (insert day and month), our teams have been working tirelessly to resolve it.

We place the highest priority on your security, as well as the security of our and your data.

Our incident response plan was immediately activated, and containment measures were promptly implemented.

(If the type of incident/attack has already been determined and it is safe to reveal it:)

We believe this is a (insert type - malware, ransomware, Denial of Service, etc.) attack. The scope and magnitude of the attack covered (mention what was affected) / is still unknown (select depending on the reality of the incident).

We recognize the gravity of the situation and are committed to resolving it as soon as possible.

We will keep you updated as the incident's resolution progresses.

If you have any questions or concerns about this matter, please contact (insert person/department/division/directorate and contact information).

Thank you for your patience and cooperation during this trying time.

Sincerely,

(Author of the communication/The Organization)."

Example 2: Template for use with client (external use)

Communication recipients: Clients (individual and collective)

Recommended means of communication: SMS, e-mail.

"Dear Client,

We regret to inform you that (name of Organization) has recently been affected by a cybersecurity incident, and we would like to keep you updated on the situation.

Since the incident was discovered at (insert time) on (insert day and month), our teams have been working tirelessly to resolve it.

Our incident response plan was immediately activated and containment measures were promptly implemented.

(If the type of incident/attack has already been determined and it is safe to reveal it:)

We believe this is a (insert type - *malware, ransomware, Denial of Service,* etc.) attack. The scope and magnitude of the attack covered (mention what was affected) / is still unknown (select depending on the reality of the incident).

Your data's security is of the utmost importance to us, and we are doing everything we can to deal with this situation in order to ensure its safety. We understand the concerns that this situation may cause, and we are committed to keeping you updated on the incident's resolution. Any concerns or questions should be directed to (insert person/department/division/directorate name and contact information).

We apologize for any inconvenience this may cause and appreciate your trust in (name of Organization).

Sincerely,

(Author of the communication/Organization)"

Example 3: Template for use with the media (external use)

Target audience: Media

Recommended means of communication: SMS, e-mail.

"(name of the Organization), has issued a statement on a recent cybersecurity incident to ensure transparency with its interlocutors.

(Name of Organization) regrets to inform that it has recently been affected by a cybersecurity incident.

Our teams discovered the incident at (insert time) on (insert day and month) and have been working tirelessly ever since to resolve it.

Its incident response plan was immediately activated and containment measures were promptly implemented.

(If the type of incident/attack has already been determined and it is safe to reveal it:)

The (Organization name) believes it is an attack by (insert type - *malware, ransomware, Denial of Service,* etc.). The scope and magnitude of the attack covered (mention what was affected) / is still unknown (select according to the reality of the incident).

(Name of Organization) reiterates its commitment to resolving this incident, emphasizing the importance of keeping the public informed and committing to take all necessary precautions to prevent future incidents.

(You could supplement the press release with a quote from a senior manager or spokesperson of the Organization, such as: (Name of person), (position of person), stated that at (name of Organization), "We are fully committed to resolving this incident and to ensuring the security of our systems and data." Our top priority continues to be the safety of our assets, our partners and employees, and the general public.

For press inquiries or interviews, please contact:

(Name of person responsible)

(e-mail address)

(telephone/mobile number)

Thank you for your attention to this matter. We will keep you informed as we make progress in resolving this incident.

Sincerely,

(Author of the communication/Organization)"

VISIT OUR WEBSITE

www.cncs.pt

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

PRR
Plano de Recuperação
e Resiliência

REPÚBLICA
PORTUGUESA

Funded by
the European Union
NextGenerationEU

Observatório
de Cibersegurança