Best Practices

for Establishing a National CSIRT

Organization of
American States

More rights
for more people

The Organization of American States (OAS) is the main political forum of the Region that promotes and supports Democracy, Human Rights, Multidimensional Security and Integral Development in the Americas. The OAS seeks to prevent conflicts and to bring political stability, social inclusion and prosperity to the region through dialogue and collective action such as cooperation, the implementation of follow-up mechanisms of the Member States' engagements and the enforcement of Inter-American Law and International Law.

This guide was created thanks to the financial support of the Government of Canada.

Important Notice

The contents of this publication do not necessarily reflect the views or policies of the OAS, its Member States or partner organizations. This guide has been submitted for consideration to a number of international cyber security experts and members of the OAS hemispheric network of CSIRTs. The guide is subject to periodic updates.

This document is an initiative of the OAS Cyber Security Program, which receives financial support from the governments of Canada, the United Kingdom and the United States.

April 2016
© General Secretariat of the Organization of American States (OAS)
1889 F Street, N.W., Washington, D.C., 20006
United States of America
www.oas.org/cyber/

Best Practices
for Establishing a National CSIRT

Organization of American States | More rights for more people

A **Computer Security Incident Response Team** (CSIRT) is an organization whose primary purpose is to provide information security incident response services to a particular community.

Several types of CSIRTs are analyzed in this guide, including National-level CSIRTs, which respond to incidents at the nation-state level.

This guide discusses the process of managing a project for the creation and deployment of a National CSIRT, including approaches and considerations necessary to define its constitution, mission, vision, scope, services, timeframe, legal, and institutional or organizational aspects. This includes an examination of the human resource requirements – both in terms of hiring and continued training – necessary to staff a national incident response team.

The guide also outlines detailed descriptions of infrastructure, covering hardware, software, and technical procedures.

Finally, it analyzes different policies and procedures necessary for fluid CSIRT operation. In this regard, the guide reviews and highlights elements of existing CSIRT frameworks such as those developed by ENISA and GÉANT. Guidelines for membership and participation in certain international bodies, such as the Forum of Incident Response and Security Teams (FIRST), are also discussed.

Content

How to use this guide 08

1 PLANNING

Definition 12

CSIRT Action Areas 14
The Role of a National CSIRT 16
Stakeholders 17

Establishment 28

Document of Establishment 29
Institutional Framework 34
Legal Framework 36

Scope 38

Target Community 39
Services 41
Reactive Services 42
Proactive Services 43
Value Added Services 44
Evolution of CSIRT Services 44

Organization and HR 45

Organizational Structures of the Response Centers 46
Organization Size 47
Roles and Responsibilities 48
Organizational Structure 50
Size and Quantity of Resources 56

Timeline 58

Conclusion of Preliminary Planning 62

2 IMPLEMENTATION

Human Resource Selection 66

Management 68
Operations 68
Research & Development 69
Information Technology 69

Training 70

Training in Cyber Security 72
Training in Cyber Security Incident Response 72
Forensics and Malware Analysis Courses 73

IT Facilities and Infrastructure 74

CSIRT Facilities 75
CSIRT Network Basic Design 77
Suggested Basic Equipment 78

Operational Policies and Procedures 80

Mandatory Minimum Policies 81
Other policies 81

3 CLOSURE

Formal Closure 85

ANNEXES

Sample Acceptable Use Policy 88
Disclosure Policy 90
Incident Response Forms 92
Works cited 103

How to use this guide

This guide analyzes several types of CSIRTs, including National-level CSIRTs, which respond to incidents at the nation-state level. These usually monitor and respond to incidents in government networks, and also serve as a coordinator of information security for the private sector or other sectors and institutions. They may or may not provide incident response services to the private sector or end users.

All things CSIRT-related, much like information security in and of itself, require a broad understanding of a number of different disciplines aside from networking or computing. They involve such additional considerations as human resource management, legal processes, financial planning, procurement, and many others. Project oversight and management are particularly important in CSIRT creation and deployment as they need to work in a structured, phased, and strategic manner during planning phases, which necessitates collaboration among diverse stakeholders.

In essence, this is a support guide on managing a project for the creation of a National CSIRT. It is specifically directed to the project manager to use as an aid and reference throughout the implementation process. It is divided into 3 main sections: Planning, Implementation and Closure, and describes the principal objectives and outcomes of each phase and present supporting materials for the process. Nevertheless, as is shown in each chapter, project managers must create a multidisciplinary team to assist throughout the process where specialization is needed.

Each country has a different political structure, culture, geography, legal framework and resources. As such, this guide is not meant to serve as a definitive template, but is meant to be adapted to local conditions, where necessary.

1 PLANNING

A Definition

What is a CSIRT?

Traditionally, a CSIRT is defined as a team or an entity within an agency that provides services and support to a particular group[1] (target community) in order to prevent, manage and respond to information security incidents. These teams are usually comprised of multidisciplinary specialists who act according to predefined procedures and policies in order to respond quickly and effectively to security incidents and to mitigate the risk of cyberattacks.

Over time, the concept of the Computer Security Incident Response Team evolved to meet the growing services required by the target community. While early teams provided basic services to respond to basic attacks and incidents, more recently, some CSIRTs have tried to keep pace with larger and more nebulous adversaries by offering advice in risk analysis, business continuity plans, malware analysis, and many other areas. When expanding CSIRT services, the European Union Agency for Network and Information Security (ENISA)[2] recommends including forensic analysis and vulnerability management. Again, the level and type of services offered will differ based on who the CSIRT serves and what its mandates are.

Teams that arose primarily to respond to incidents have evolved and are now frequently oriented to a comprehensive model of information security management. Indeed, whereas the purview of CSIRTs was largely confined to “response” services, today they increasingly adopt a proactive stance, focusing on incident prevention and detection, achieve through a mix of skills and awareness training, alerts and monitoring, dissemination of information related to information security, development of business continuity plans, development of best practices documents and vulnerability analysis, among others.

CSIRT Action Areas

There are hundreds of CSIRTs in the world that vary in mission and scope. One of the chief ways to classify CSIRTs is to group them by the sector or community they serve. Below are some of the main types of CSIRTs in operation:

ACADEMIC CSIRTs

These response teams assist academic communities, universities, colleges, schools or institutes. Their size and facilities vary depending on the size of the community, and they frequently partner with other academic CSIRTs and may specialize in research.

COMMERCIAL CSIRTs

For a variety of reasons, including human resource limitations or a host of others, some companies elect to outsource CSIRT services instead of internally creating and managing incident response functions. This has spawned a robust market for commercial CSIRTs, which offer incident response services to paying customers. The relationship between a commercial CSIRT and its client is often governed by service level agreements (SLAs), which are necessary to establish incident response guidelines and to ensure information is handled according to the client's needs.

CRITICAL INFRASTRUCTURE CSIRTs

In some cases, there are CSIRTs specifically established for the protection of critical information assets and the critical infrastructure of a nation, regardless of whether it is operated by the public or private sector, or administering transport, power generation, communications or other processes. Since institutions reporting to of this type of CSIRT can pertain to more than one community (for example, both military and critical infrastructure), it is vital to establish protocols for interaction with other teams involved.

GOVERNMENT CSIRTs

Government CSIRTs serve state institutions in order to ensure that government IT infrastructure and the services it facilitates to citizens have an adequate level of security. Government CSIRTs adapt their structures to the Government. They can meet local, regional or sector-specific government communities. Government CSIRTs can operate independently or interact to combine strategies and efforts and share resources and knowledge. Within a country, for example, the Ministry of Education and the Ministry of Tourism might operate independent CSIRTs, but regularly collaborate and share information.

NATIONAL CSIRTs

In addition to serving a defined community, a country's National CSIRT usually takes on the role of national coordinator for incident response, and is the contact point[3] for national and international incidents. The role and target community of a national CSIRT varies depending on its roles and the existence of other response centers. For example, if there is no CSIRT designated for critical infrastructure, the national CSIRT could assume responsibilities normally assigned to a critical infrastructure response team.. It can be considered as a "last resort CSIRT," or one which takes charge of incident response matters that are not under the purview of another body[4]. It is very common for various CSIRTs to be part of the community the National CSIRT serves.

MILITARY SECTOR CSIRTs

Military CSIRTs provide services to the military institutions of a country. Their activities are usually limited to the defense, or offensive cyber capabilities, of a nation. In addition to standard incident response technologies, they often have specific ICT knowledge for military use including, for example, weapons and radar systems.

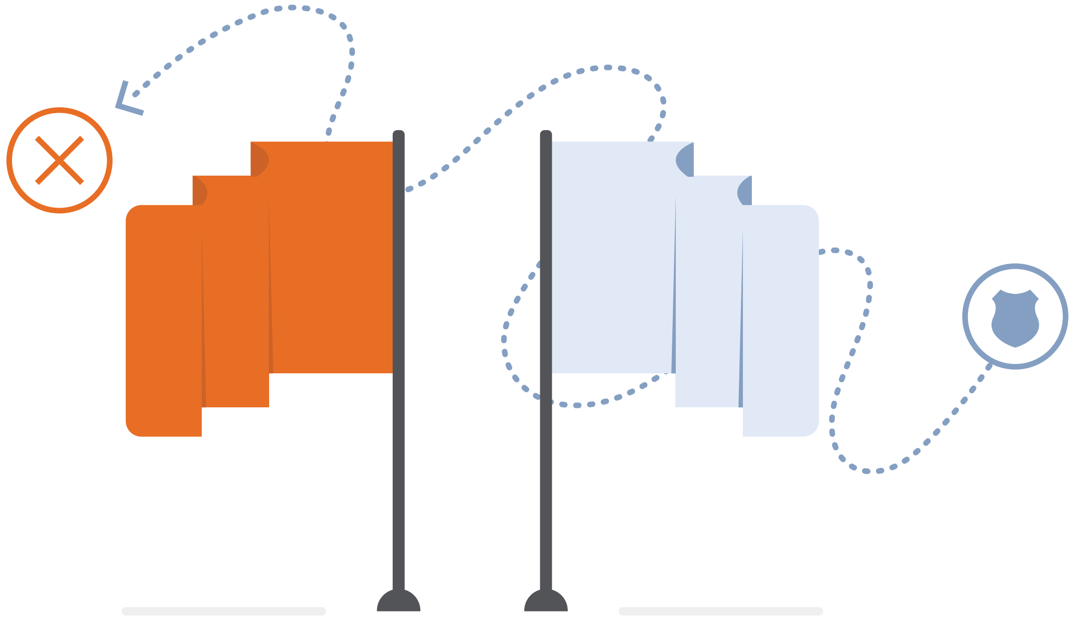
PROVIDER CSIRTs

Provider CSIRTs render services relating to specific products from a manufacturer, developer or service provider. The purpose of this type of CSIRT is to mitigate the impact of vulnerabilities or security issues related to their products. Examples include HP CSIRT (Hewlett Packard), Banelco CSIRT (Banelco Bank), or Adobe PSIRT (Adobe) among others.

SMALL/MEDIUM-SIZED ENTERPRISE (SME) SECTOR CSIRTs

The size and nature of SMEs often do not allow them to implement individual incident response teams. Therefore, there is a need to create CSIRTs that understand and address the needs of this business community, such as the one implemented in Spain by the INTECO-CERT Corporation, which focuses on assisting SMEs and citizens.

The role of a National CSIRT



A CSIRT is a team of people whose job is to prevent and respond to computer security incidents. Of course, the level and type of response effected by a particular CSIRT will depend on many factors.

A frequently referenced analogy, one first put forth by Carnegie Mellon University, draws comparison between CSIRTs and firefighters. As explained by CMU's CSIRT Handbook, in the same way that a team of firefighters responds to a fire emergency, so must a CSIRT respond to and manage a computer incident. Going further, the analogy holds that in addition to their response duties, fire crews perform preventive activities such as education, risk analysis or the promotion of regulations. CSIRTs also carry out these types of preventative activities. Finally, fire crews often investigate how and why a fire occurred in order to prevent it from happening again. Almost all CSIRTs perform investigative functions, regardless of their classifications.

As mentioned above, a CSIRT can have different organizational forms: it may be an independent institution, private or public, a department of another organization or just a group of people distributed in different organizations.

Each CSIRT defines how it will perform its activities. It may need to go to the scene of an incident to perform a response, or otherwise can remotely oversee incident management by coordinating with other stakeholders and obtaining evidence and log files through means other than physical transfer.

As previously described, a National CSIRT acts as a country's point of contact at the international level. For example, if a CSIRT from country "A" detects malicious traffic originating from a bank in country "B," it would send a communication to the National CSIRT from country "B," which would then work directly to address the source of the malicious traffic and resolve the issue. In this example, it is also important to note that in addition to receiving the request from CSIRT "A," CSIRT "B" then coordinates the incident response process that takes place within its own stakeholder community. These are the two most important roles of a National CSIRT: to act as the country's contact point internationally for cyber security matters and to coordinate and perform computer security incident response activities nationwide.

In establishing a CSIRT, officials often focus solely on technical incident response capacities as opposed to broader organizational concerns. To ensure that both principal objectives of National CSIRTs are addressed, significant portions of this guide are dedicated to planning and developing a model in which the National CSIRT effectively partners with necessary stakeholders. Indeed, to lead, articulate and coordinate incident response actions and norms, a National CSIRT must first devise clear goals, objectives, and strategies, and subsequently inform all relevant parties of the same.

Stakeholders

Input	Tools	Output
- Project team	- Brainstorming - Mental maps - Analysis of stakeholders	- List of stakeholders and their roles, interests, support and influence over the project

To plan a National CSIRT, the first step a team must take is to identify stakeholders.

As explained before, the main role of a national CSIRT is to coordinate with stakeholders in the country on cyber security incident the response activities. For this reason it is essential to clearly identify the stakeholders.

Stakeholders are the people or organizations that will be affected in some way by the implementation of a National CSIRT. These parties will have different levels of interest in the project, a specific role in the lifecycle of the national CSIRT, and a given level of power over the project implementation and operation of the CSIRT.

Once the stakeholders are identified, they can be classified according to their role, responsibilities and interest regarding the CSIRT initiative. Then, a strategy will be developed to engage with and manage them.

Stakeholders are people or organizations that will be affected in some way by the implementation of a National CISRT

Although others may be identified, the main stakeholders[5] in Cyber Security activities are:

Executive Power of the State

The government participates as a stakeholder in several roles. It processes highly sensitive information for the country: of its citizens and of the financial, public security, defense, health, and education sectors, among others. Due to the importance of the information it manages, government needs to keep its systems secure, and is usually the main "client" for a National CSIRT, since it may be the victim of an attack that would have potentially serious consequences.

At the same time, governments are responsible for regulation and generating laws, standards, and other initiatives of national importance. In this sense the government is an extremely important instrument for regulatory activities and norms for the prevention of cyber security incidents. Government has the responsibility of determining acceptable risk levels in the aforementioned sectors, including those associated with computer incidents. As such, government acts as a both a CSIRT sponsor and promoter.

Legislative Power of the State

Besides being a client – in that the National CSIRT may safeguard its networks and information – the legislature creates laws promoting information security, establishes limits for a CSIRT, and is also a key strategic partner.

Judicial Power of the State

In addition to strengthening the legal aspects for the criminalization of cybercrime, judicial institutions provide clarity in the areas of law that may affect the operations of the CSIRT. In this sense it is a key stakeholder.

Law Enforcement

Law enforcement should ensure that cybercrime legislation is implemented in a country. The police conducts cybercrime investigations and often liaise with a National CSIRT in this regard. They can provide valuable information from malicious cyber activity and cooperate with counterparts from other nations' law enforcement agencies. Law enforcement bodies often maintain a specialized cybercrime unit with procedures and tools needed to collect evidence from cyberattacks.

Ministry of Defense

In many countries, the Ministry of Defense administers the country's most valuable or sensitive information. Furthermore, it oversees cyber defense issues, making it a key partner in incident response and CSIRT operations.

Academia

The academic community has much to contribute to a CSIRT. For one, it is often the de facto sector that leads efforts to develop human resources and train young people in various facets of information and computer security. It can also conduct research in the same areas. It is a key partner throughout the lifecycle of a National CSIRT.

Internet Service Providers

ISPs allow governments, businesses and citizens to connect to and use the internet. As such, they have a wide range of responsibilities related to internet use and web hosting. They are critical assets in maintaining information security and responding to cyber security incidents. ISP cooperation is key to CSIRT operation, especially where modifications to Internet networks, contingency planning, or identifying threats and vulnerabilities are needed.

Private Sector

The private sector is involved from two points of view. On one side are the private companies operating in sectors critical to the state. Their compromise would result in negative consequences to the economy, public safety, and/or national security. On the other side are the many enterprises that manufacture and develop technologies used in IT and information security. Companies that operate critical infrastructures will be key customers, often becoming trusted partners with whom incident response will be closely coordinated. Meanwhile, technology manufacturers collaborate on training, support, updates and vulnerability patching. In both cases interaction with them is essential.

Financial Sector

The financial sector can be subdivided into several subgroups, including: Banks, Central Banks (or regulators), brokerage firms and exchanges. Each of these sectors has particular requirements as partners, customers, and even sponsors.

Civil Society

Civil society includes professional associations, nonprofit organizations and user groups, among others. These groups not only bring together specific profiles of technicians and professionals but also provide training and guidance and can help with awareness-raising efforts. They are often influential strategic partners.

National and international specialized groups

Specialized groups may exist as private or specific CSIRTs at the local and international level, international forums such as FIRST, or multilateral organizations performing cyber security activities like the OAS.

All stakeholders will play slightly different roles in the creation, development, and operation of a National CSIRT. They can be roughly grouped according to their contributions:

Sponsors or promoters
Persons or organizations that promote the existence of a National CSIRT, and will support it either politically or financially.

Clients
Organizations that will use the services of the National CSIRT.

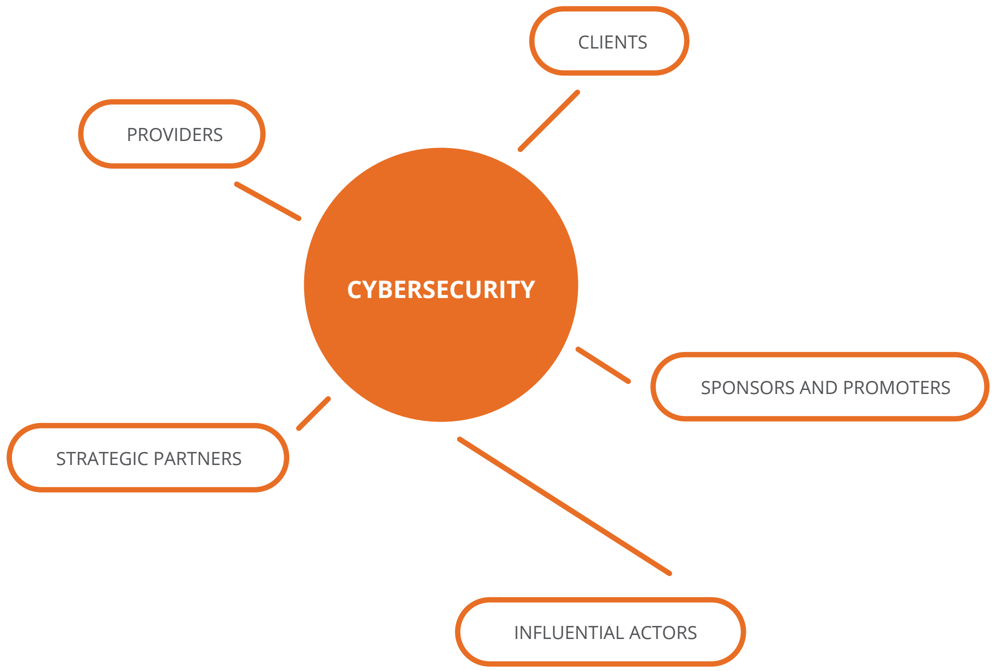
Providers
Organizations that provide products and/or services to the national CSIRT, such as tools, professional services, training, etc.

Strategic Partners
Personnel or organizations that are strategic to the proper development of the CSIRT. In general, these allies execute activities of interest to the CSIRT that it cannot perform on its own. An example might be academia or sector-specific regulators.

Influential
Individuals or organizations that informally influence different sectors. An example would be civil society actors such as user groups or with nonprofit organizations.

The role of each interested party is important to identify, considering that it will define the way in which a CSIRT engages with it. The relationship between the CSIRT and each of its stakeholders will be different and thus imply a different style of interaction. For example, collaboration with an ISP or law enforcement will likely be guided by contracts or official agreements. Partnerships with civil society or government institutions, on the other hand, may be more informal, though no less important. Indeed, they likely require their own type of nuanced interaction.

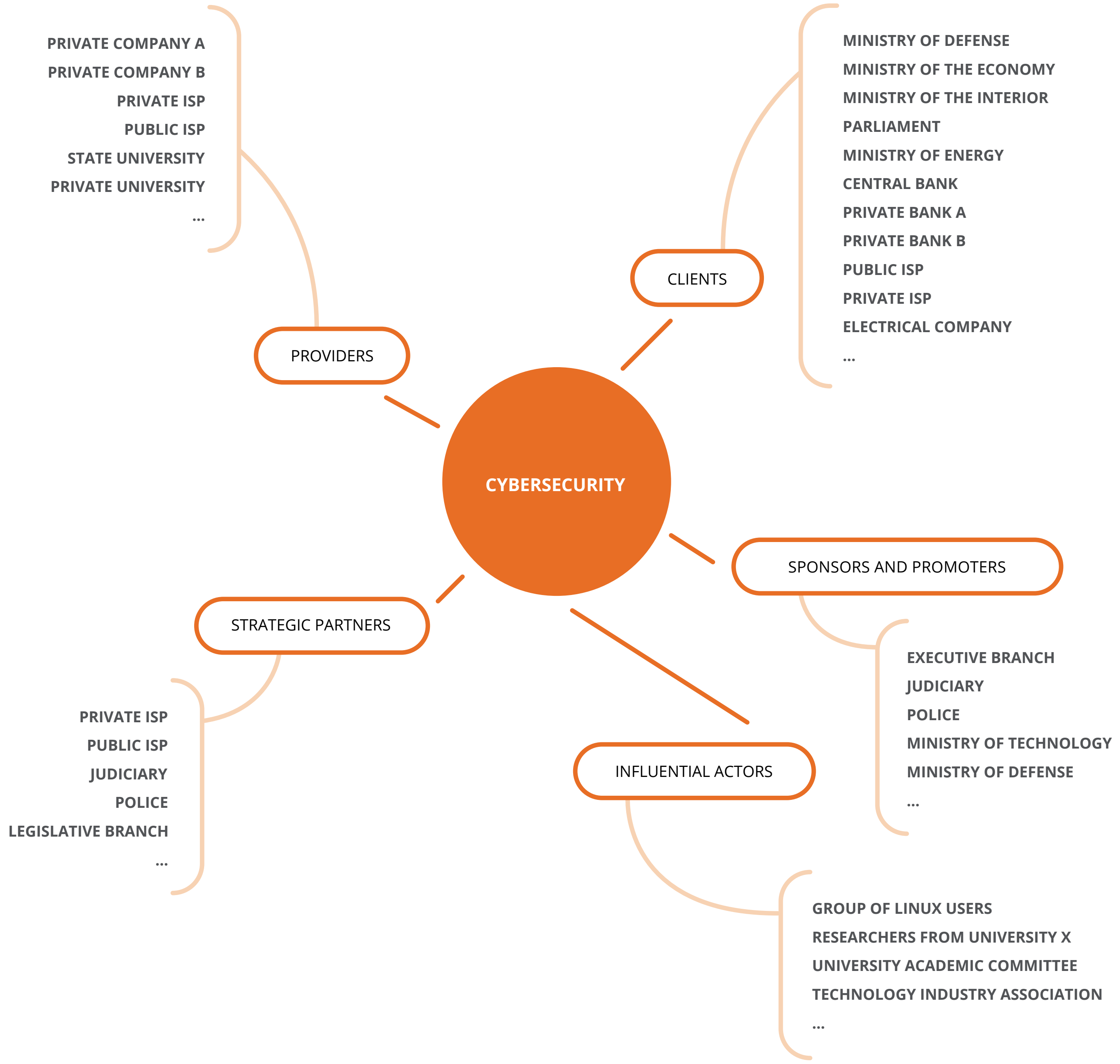
Methodology to identify stakeholders



To identify stakeholders, the CSIRT project manager must recruit a small team that represents a variety of interests and organizations. This is to ensure that multiple perspectives and specializations are incorporated into the stakeholder selection and engagement process. If possible, in an effort to preserve objectivity there should be at least one person on the team who is more neutral, or not necessarily a part of the stakeholder community. The actual process of determining stakeholders should consist of a preliminary brainstorming session followed by informational interviews.

As explained above, the stakeholders can be grouped according to the role they will play. The first step is to list the different groups., Mind maps can be used as a tool to sort this information, which will help the project team visualize the information more easily.

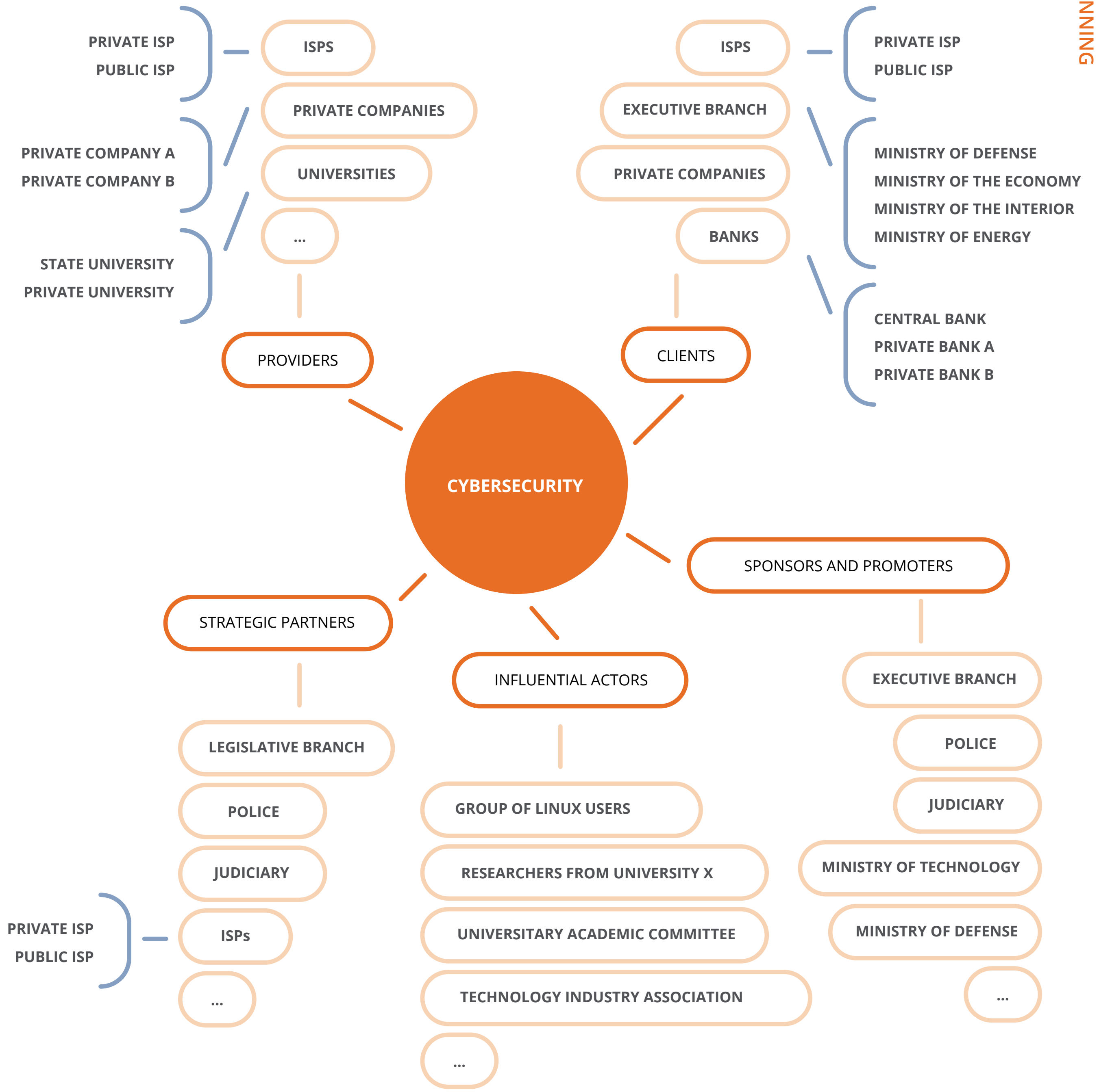
The diagrams on pages 22-23 shows the initial structure of a mental map to begin brainstorming and identifying stakeholders.



Once the groups are defined, brainstorming helps to categorize the nominated actors in each group.

The diagram above shows an example of a mind map midway through the organization process.

As seen in the diagram, a stakeholder may occupy several roles simultaneously. This situation will often present itself both within government and with the private sector, academia and civil society. The clearest example of this is within an ISP and the Government. These groups are strategic partners without whom it would be almost impossible to establish and operate a national CSIRT. At the same time, they are recipients of CSIRT services since they may become a victim of a cyberattack or cyber security incident. The groupings can be further broken down into subgroups, as seen below:



Finally, a list of the stakeholders and their roles will be generated in a formal document.

This list should contain each of the groups involved, the justification for their participation in the CSIRT project, and an officially designation point of contact.

These groups are strategic partners without whom it would be almost impossible to establish and operate a national CSIRT

Interviews with stakeholders

Once the list of the stakeholders, roles and subgroups is prepared, there will be meetings with each of the subgroups as a way to approach them and better understand their needs, what they expect from the national CSIRT, and generally where they stand in terms of cyber security. Meeting each subgroup individually provides a rich environment for exchange of opinions and allows for transparency during the creation process.

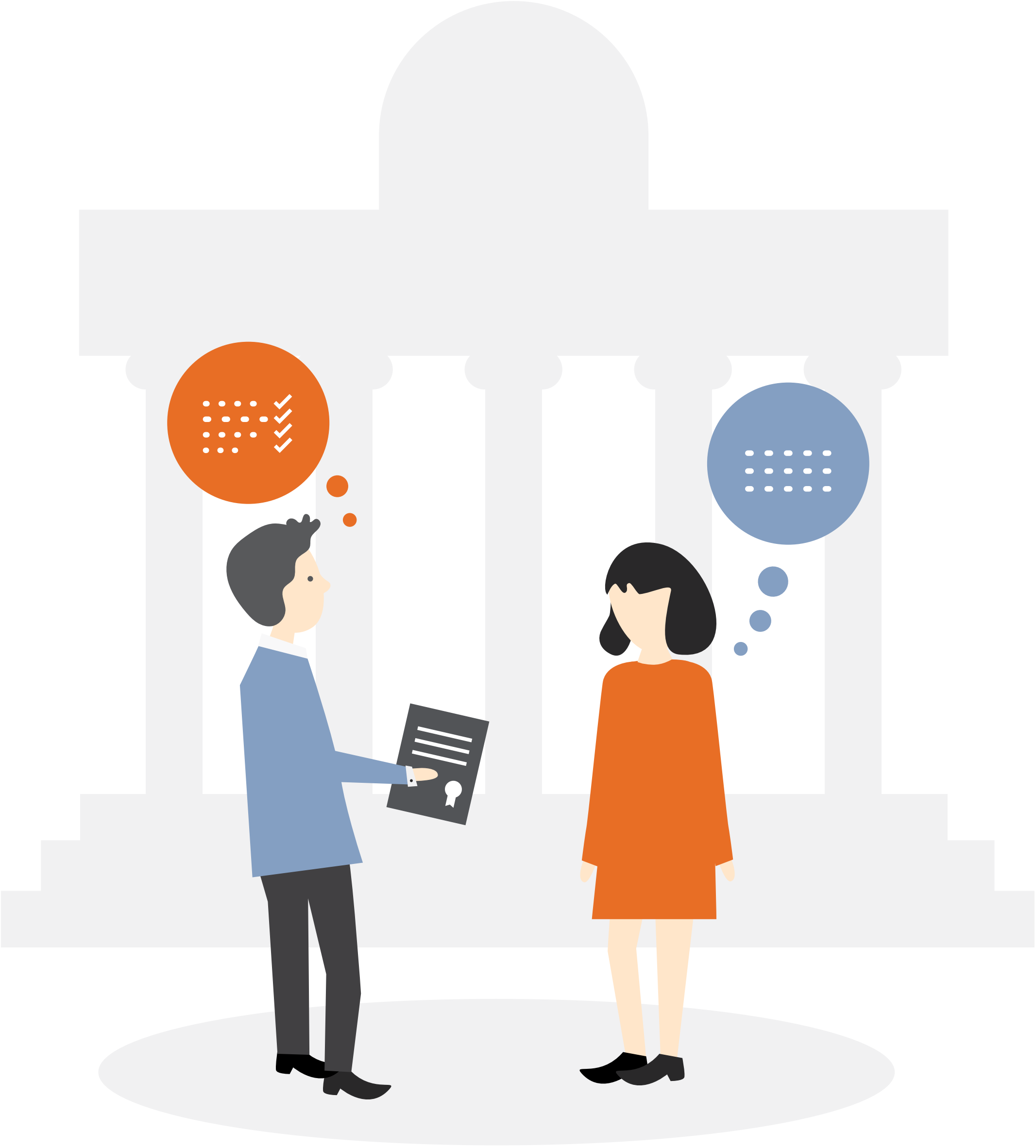
During these interviews, it is important to introduce the stakeholders to the subject of CSIRTs, since many of them may not have experience in the subject, especially depending on the audience and general level of cyber security development within a country and government. The CSIRT project manager and team should prepare questions to help stakeholders elaborate their position, such as:

- Do you feel there is a need to create a National CSIRT? Why or why not?
- What should the role of a National CSIRT be?
- What services should a National CSIRT provide?
- Is there any particular part of government where the National CSIRT should be located?
- How would a National CSIRT potentially benefit your organization?
- How might working with a National CSIRT be difficult for your organization? Would the relationship be governed by a contract, NDA, SLA, or some other means?
- Is your organization willing to actively cooperate with a National CSIRT? What are the limits to cooperation?
- What other organizations or individuals do you think should be involved?

After holding discussion sessions, the project team could circulate a questionnaire, allowing stakeholders to contribute thoughts privately.

Meeting each subgroup individually provides a rich environment for exchange of opinions and allows for transparency during the creation process.

Information would be analyzed following discussions and the collection of surveys, allowing the project team to create a more robust and clear stakeholder map. This entire process could be repeated to ensure that all stakeholders are engaged and the map of roles and responsibilities of collaborating institutions is complete and precise.



Stakeholder analysis

Stakeholder analysis identifies each stakeholder's attitude towards the implementation of the National CSIRT. A picture will naturally emerge that shows how much each stakeholder is invested in the CSIRT project and how each has the ability to influence the response team's development. The results of the analysis will yield guidelines that outline the most appropriate way to manage the project and project partners for better results.

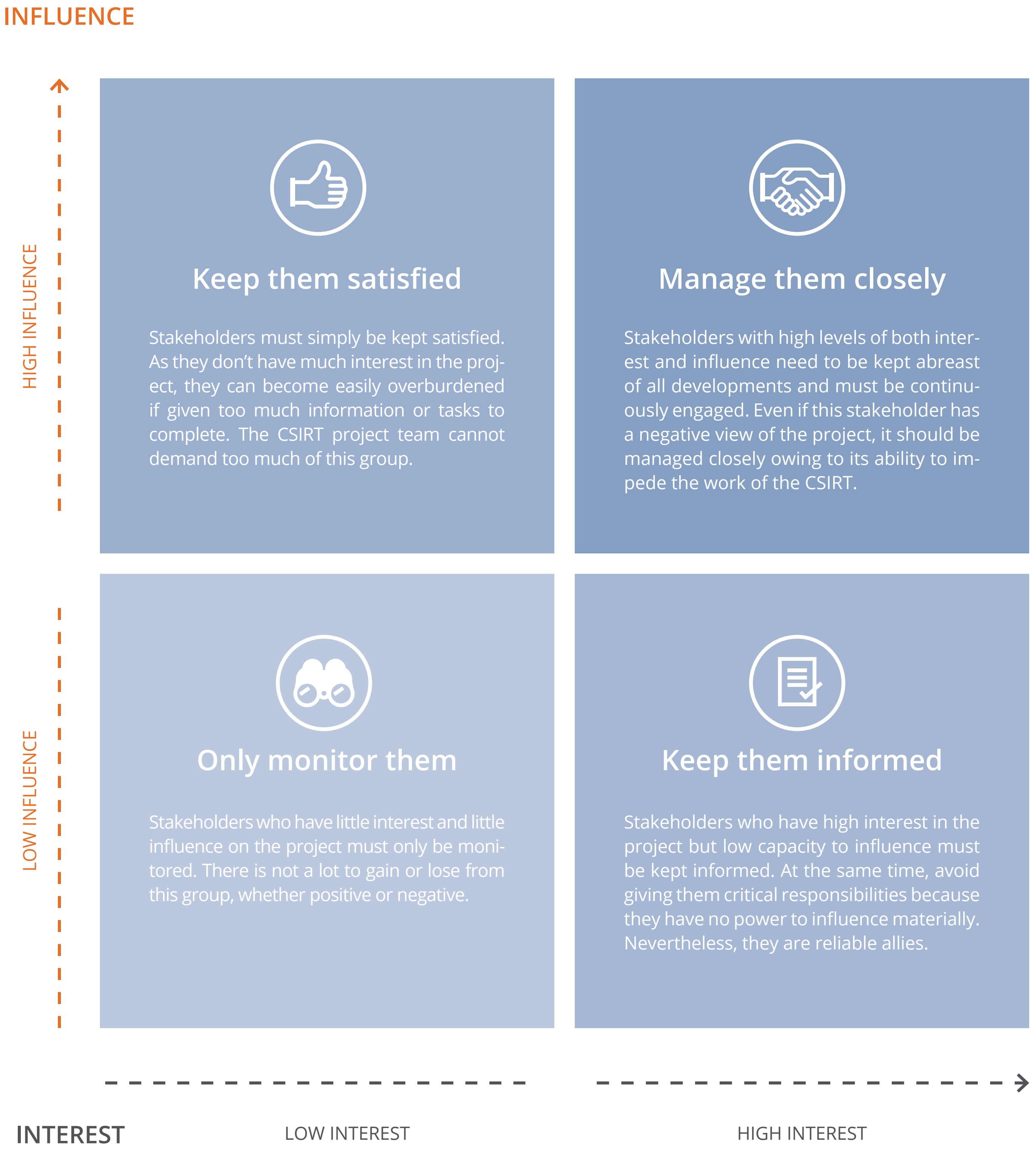
There are two popular methods for classification.

The first is to establish a scale with the stakeholder's level of support for the project based on the interviews, for example, by defining three simple levels of support: opposes initiative; is neutral; or supports the initiative.

Another technique is to establish a map of quadrants where the concerned stakeholder will be classified according to their level of interest in the project, and the level of influence it has on it.

Once stakeholders are located in their respective quadrants, there will be a clear map for how to effectively manage each. At this point there is a map with identified stakeholders, their interest in the project, their attitude toward giving support to the initiative, good or bad, and their level of influence. The stakeholders can then be managed using the following diagram.[6]

Once the stakeholder-identification and analysis process has ended, you will have a structured list of all stakeholders, their respective roles, levels of interest in the project, their attitude towards it, as well as each of their abilities to influence the CSIRT. Ultimately, this information will be useful to allow the project team to identify sources of assistance, funding, advice, or anything else beneficial to the development of the CSIRT. Simultaneously, it will highlight any potential "unhappy customers" or institutions that could complicate CSIRT activities.



Keep them satisfied

Stakeholders must simply be kept satisfied. As they don't have much interest in the project, they can become easily overburdened if given too much information or tasks to complete. The CSIRT project team cannot demand too much of this group.

Manage them closely

Stakeholders with high levels of both interest and influence need to be kept abreast of all developments and must be continuously engaged. Even if this stakeholder has a negative view of the project, it should be managed closely owing to its ability to impede the work of the CSIRT.

Only monitor them

Stakeholders who have little interest and little influence on the project must only be monitored. There is not a lot to gain or lose from this group, whether positive or negative.

Keep them informed

Stakeholders who have high interest in the project but low capacity to influence must be kept informed. At the same time, avoid giving them critical responsibilities because they have no power to influence materially. Nevertheless, they are reliable allies.

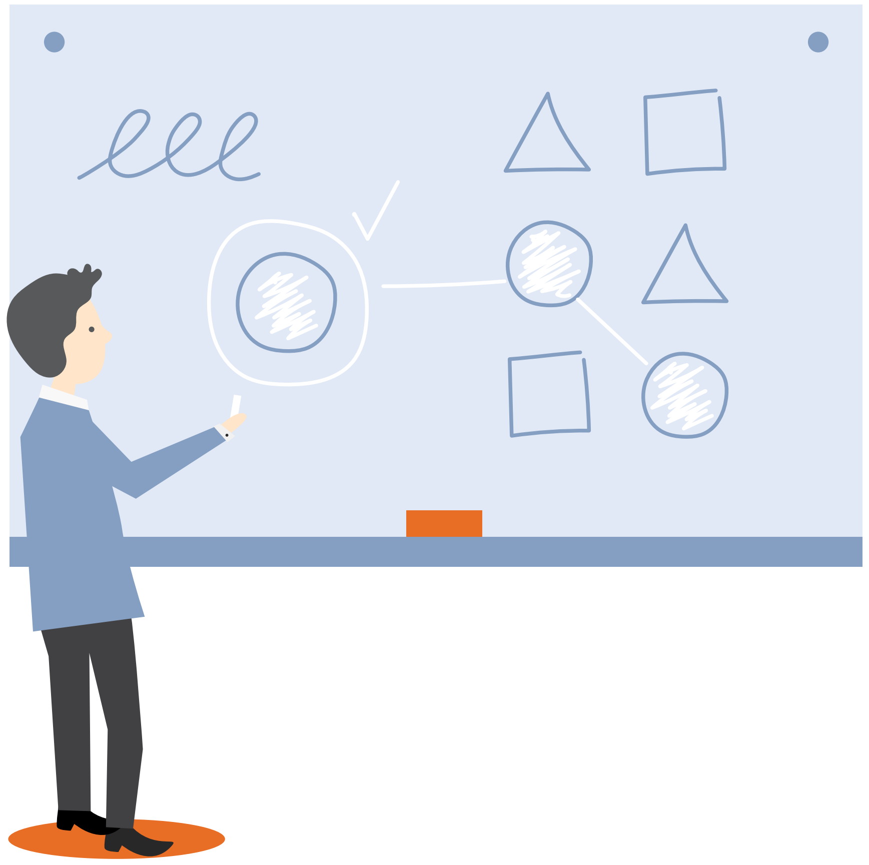
B Establishment

After identifying stakeholders, the project team should generate the necessary documentation to establish the National CSIRT.

In this section, a document of establishment of the National CSIRT will be created, which will define its Mission and Vision; Institutional Framework; and Legal Framework

Input	Tools	Output
- Project Team - Document of stakeholders	- Moderated working tables - Expert Consultation	- Document of Establishment - Mission and Vision - Institutional Framework - Legal Framework

Document of Establishment



To create a CSIRT it is necessary to define the framework that will guide and govern how the team will operate. Among other things, the establishment document or framework will cover: [7]

- The nature and goals of the CSIRT
- Target community (government, private sector, or both)

A National CSIRT must clearly identify its **mission and vision**. These two aspects will not only guide those who work on the team, but will also serve as a guide and reference to anyone who receives its services or collaborates with it. In short, mission and purpose are the reasons why the CSIRT exists.

A CSIRT's **institutional framework** will establish its configuration. A CSIRT can be constituted as an independent enterprise to provide services in the private context; as a unit within a public or private organization to deliver internal or external services; or it may be an organization unto itself that does not report to any particular group or body. This guide will focus on an organizational structure for a National CSIRT.

Finally, a **legal framework** will likely be necessary to protect the CSIRT and its operations, considering that a response team with national-level responsibilities will deal with many sensitive issues, possibly with implications on national security, the macro economy, or public safety. This guide will present and analyze the pros and cons of several types of legal frameworks for a National CSIRT.

Mission and purpose

The mission explains why an organization exists. It must detail, both to internal and external actors, what the organization does and for whom and what values drive it[8]. Normally, the mission does not include "how" it achieves its mission, since this can vary over time. The mission must be specific and clearly defined, since it should not change over time. Verbs are usually used in the infinitive and in the present. In the context of a National CSIRT, the purpose of the organization must be concrete, explicit and use clear terms.[9]

WHAT

In describing **what** the team does, it is customary to use terms such as coordinate, promote regulation, lead efforts, protect, prevent, or articulate activities like incident response, cyber security, information systems or assets, etc.

WHOM

In describing for **whom** activities are performed, terms often used are country, state, government, sector, or others.

VALUES

Regarding the **values** that drive the mission, the motive must be clearly stated, for example by using terms like: development, wellbeing, safety, or risk management. Values such as security, trust or responsibility, among others can also be invoked.

Here are examples of some mission statements from CSIRTs around the Americas.

National Cyber Security and Communications Integration Center Mission | NCCIC, USA

To reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the Nation's critical information technology and communications networks. To execute its mission effectively, the NCCIC will focus on three core strategic priorities and associated operational objectives. The NCCIC will implement this strategy by expanding and attaining the capabilities, products, and services required to meet each of its strategic priorities over the next five years. Many of these activities will be coordinated, developed, and executed collaboratively with the NCCIC's operational partners to the benefit of the entire community of cyber and communications stakeholders.

It can be noted that each of the missions clearly states the CSIRT's main objective and whom it will serve. Later, this mission statement will be used as reference to express the scope of the National CSIRT in detail.

ColCERT Mission | Colombia

The Colombian Cyber Emergency Response Group, colCERT, has as its main responsibility coordination of National Cyber Security and National Cyber Defense, which will be framed within the Mission Process of Security and Defense Management of the Ministry of Defense. Its main purpose will be to coordinate the necessary actions for the protection of critical infrastructure of the Colombian state against cyber emergencies that threaten or compromise national security and defense.

VenCERT Mission | Venezuela

The mission assigned to VenCERT, which is to contribute to the general objective of the National Information Security System, is detailed in the following points:

- Prevention, detection and management of incidents affecting State Information Systems and entities that manage the Critical Infrastructures of the Nation.
- Main national point of coordination of other incident management centers in the country and abroad.
- Provide advice, support and training on security issues to heads of ICT in government agencies or entities managing National Critical Infrastructure.
- Coordination of public and private initiatives on ICT security in the State, carried out through R&D projects, training and awareness raising, development of standards, policies or guidelines, both for the benefit of the community (State and national CI operators) and for the improvement of services provided within VenCERT

VenCERT stands, therefore, as the Venezuelan government CERT, whose main objective is the prevention, detection and management of incidents generated in information systems throughout the National Public Administration and Public Sectors in charge of the management of Critical Infrastructure in the nation.

CERTuy Mission | Uruguay

Protect critical information assets of the State and promote awareness in information security in order to prevent and respond to security incidents.

Vision

The vision provides long-term direction of where the organization will move and how it expects to be viewed by outsiders, whether they are customers, peers, or sponsors. It speaks to the organization's reputation and its aims for the future. The vision sets out the long-term path the organization will take and serves to guide strategic decisions.[10] Bill Gates set forth one of the most famous ICT visions of all time, characterized by its clarity, brevity, and ambition: "A personal computer on every desk."

Vision is closely associated with the culture of each country, and the CSIRT may embody certain traits like a country's reputation, efficiency, reliability, efficacy, accountability and innovation. However, vision is important not only for external actors but also for actual operations of a CSIRT or organization, since it will shape the values of the organization[11]. The vision of an organization should not change over time.

These are examples of Visions of some of the National CSIRTs in the region.

VenCERT Vision | Venezuela

VenCERT services protect and guarantee the defense and security of the Nation and the absolute vigilance of the general interests of the Republic, the preservation of the public peace and the proper enforcement of law throughout the country, according to the powers established in the Constitution of the Bolivarian Republic of Venezuela for the National Government.

CERTuy Vision | Uruguay

To be a reliable computer security incident response center and a reference at national and regional levels.

NCCIC | USA Vision

The NCCIC Vision is a secure and resilient cyber and communications infrastructure that supports homeland security, a vibrant economy, and the health and safety of the American people. In striving to achieve this vision, the NCCIC will:

- Focus on proactively coordinating the prevention and mitigation of those cyber and telecommunications threats that pose the greatest risk to the Nation.
- Pursue "whole-of-nation" operational integration by boarding and deepening engagement with its partners to manage threats, vulnerabilities, and incidents.
- Break down the technological and institutional barriers that impede collaborative information exchange, situational awareness, and understanding of threats and their impact.
- Maintain a sustained readiness to respond immediately and effectively to all cyber and telecommunications incidents of national security.
- Serve stakeholders as a national center of excellence and expertise for cyber and telecommunications security issues.

Suggested methodology for defining Mission and Vision

Since the mission and vision define the CSIRT's outlook in the medium and long term, it is important that these portions of the CSIRT plan have the buy-in of as many, if not all, of the stakeholders identified in the previous chapter. In this sense, it is helpful to form a working group composed of a plurality of stakeholders to determine these two critical components of a CSIRT plan. Delegates to the working group should be designated by their senior management to ensure that final products have the authority and official approval of participating institutions. At the same time, the number of representatives making up the drafting team should be small enough that progress is efficient and only those with the highest interest and influence in the project participate.

Once an appropriate list of stakeholders is identified, several working groups should be established to work independently on the mission and vision. With one person serving as moderator, a variety of questions will help attendees throughout the discussion.

Similar to drafting the mission, for creating the vision, the moderators can pose questions to guide delegates.

After gathering the opinions of the participants, the moderator will help with the wording to finalize clear and concise statements. Once this step is complete, the results should be circulated to the wider stakeholder group. It is also important to document the process and ensure that minutes are taken at all meetings clearly stating how the activities were conducted and who participated in them.

Once completed, the mission and vision will be used throughout the lifecycle of the national CSIRT.

Delegates to the working group should be designated by their senior management to ensure that final products have the authority and official approval of participating institutions.

- How do you expect clients/ the community will view a National CSIRT?
- What values do you expect it to inspire?
- Will it help improve the quality of life of people? Why or why not? How?
- How will the National CSIRT adapt to changes in technology and management?
- How will it be able to stand out in its environment?

- What do you understand to be the main purpose of a National CSIRT?
- What needs would be covered?
- Who should it serve?
- What kind of services shall it offer?
- What considerations would restrict its operations?
- What goals or success factors must be considered for the National CSIRT?

Institutional Framework

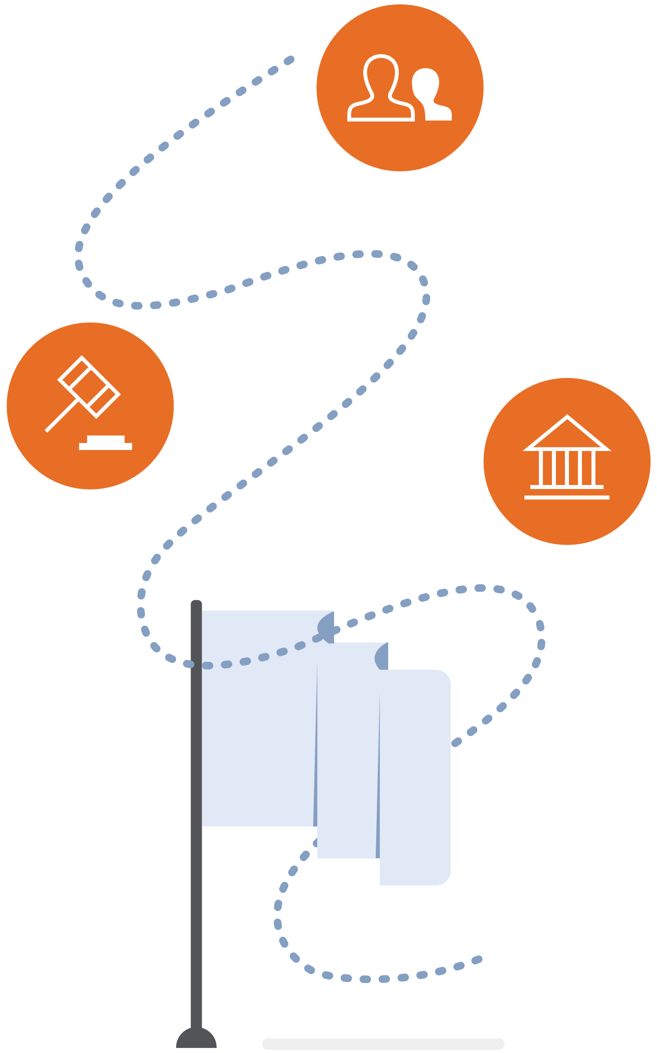
The institutional framework of the National CSIRT is key to its establishment and function throughout its lifecycle. As stated above, National CSIRTs may be set up in different ways, but they will have traits in common. It is important that the country adopt a CSIRT structure that fits the its legal, political, and cultural realities.

A National CSIRT's institutional framework will set guidelines for the following considerations:

- Responsibilities
- Authority
- Interaction with stakeholders
- Financial resources
- Human Resources
- Infrastructure
- Resilience

A National CSIRT with a coordinating role must be located in an office or body that has contact and influence with a range of stakeholders. Otherwise, it will be difficult to execute and communicate the response team's work. As with most things described in this guide, the CSIRT's location will depend on the structure of its government. In Latin America, CSIRTs are housed in a variety of institutions. In Brazil, Panama, and Uruguay, for example, the teams are in executive bodies under the Presidency. In Colombia and Peru, the Ministries of Defense and Security handle national incident response. Still, in other countries like Paraguay, the CSIRT operates from the Ministry of Technology. The fact that a team is part of government should in no way preclude it from information sharing and strategizing with the private sector and other actors. In fact, many CSIRTs form steering committees or boards comprised of select stakeholders that debate and discuss key decisions facing the response team. While some CSIRTs accept decisions of their committees as binding, others use them simply as a forum for debate and collaboration, with the final decision ultimately residing with the team.

An aspect often overlooked when establishing a CSIRT is funding. It seems obvious, but a national incident response team without a steady source of funding will not be able to function beyond the short term. For this reason, while securing seed or startup funding is pivotal, the project team must also make projections of how much money will be needed to finance the team after initial costs are met to sustain it.[12]



Methodology for creating the institutional framework

Once stakeholders, mission, and vision are established, the project team must identify where the National CSIRT will be established. The team must be located in an institution that:

- Has the ability to establish or influence ICT-security related policies at the national level
- Resides close enough to the highest levels of government that it can enlist its support when needed
- Is able to secure funding
- Has appropriate jurisdiction and autonomy when needed

Due to the cross-cutting nature of issues with which a CSIRT works, a multidisciplinary group shall be formed to determine where the CSIRT shall sit. It should be composed of experts in:

- Computer Security and Incident Response
- Public Policy in Technology and Telecommunications
- National Security and Defense
- Public Law
- Legal Framework

The project team must recommend:

- Whether the CSIRT will be an independent organization, whose sole purpose is to be a National CSIRT, or a division within another organization
- Whether the CSIRT will be solely a state organization or include private-sector, academia and/or civil society participation
- If there is third-party involvement, exactly how it will take place and what the associated business model will be
- How the organization's funding structure will look and how it will be secured.
- How the coordination/steering committee will be formed and what powers it will have

As with other processes, discussions should be annotated so as to promote transparency and increase stakeholder buy-in. The final recommendations agreed upon by this working group, together with the mission and vision, will be unified into a single document, which will then be reviewed by legal experts to establish its implementation.

Due to the cross-cutting nature of issues with which a CSIRT works, a multidisciplinary group shall be formed to determine where the CSIRT shall sit

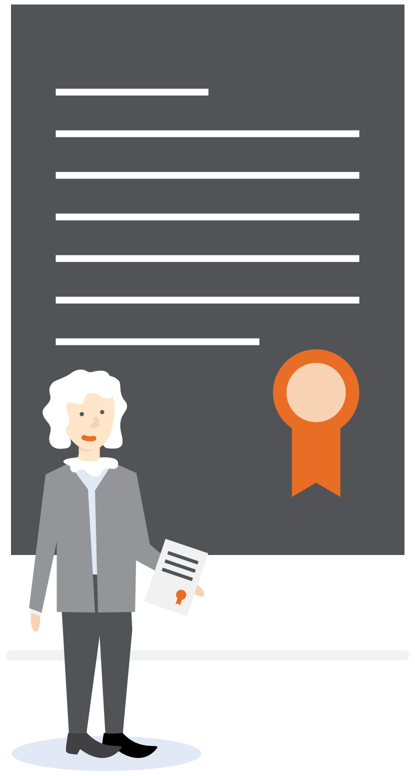
Legal Framework

Finally, it is extremely important to define the legal authority under which the National CSIRT will be established. This must conform to the legal standards of the country concerned, and it must ensure implementation. If not adopted correctly, a faulty legal framework can lead to lawsuits or complications in responding to cyber incidents. This is why it is so important that mission, vision, and the institutional framework are assessed by legal experts, either from government or academia or both, specifically to answer the following questions.

- Is the CSIRT acceptable from a legal standpoint? Does it contradict any laws, or allow for any loopholes whose exploitation may have a negative effect on the response team and its duties?
- What instrument will be used for the institutional framework? Legislation, decrees, or resolutions?
- Can the CSIRT employ any legal measures to guarantee funding?
- How will human resources be contracted?

The conclusions of the legal analysis should appear as an appendix or addendum to the CSIRT's document of establishment.

The following are examples of different legal frameworks that institutionalize CSIRTs in the region:



CSIRT | Panama

Executive Decree No. 709 of September 26, 2011

ColCERT | Colombia

CONPES Document 3701

CERTuy | Uruguay

Law 18.719 year 2008. Executive Decree 451, year 2009

ICIC CERT | Argentina

Resolution Chief of the Cabinet of Ministers 580/2011

C Scope

Once the CSIRT’s mission, vision and institutional and legal frameworks are established, it is important to define its scope, specifically by determining what services will be provided and to whom.

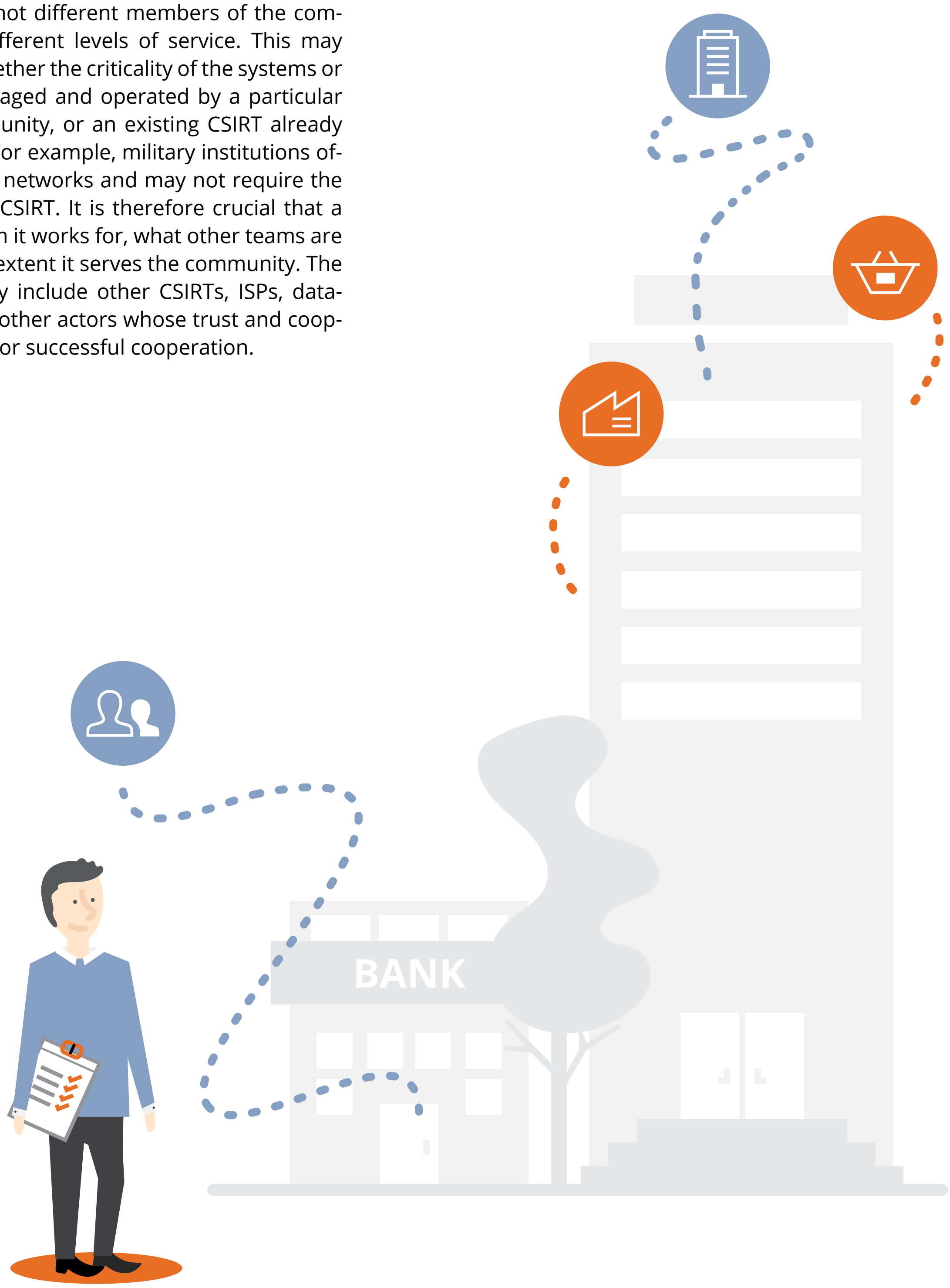
The scope will be determined by the needs of human resources, technical training, infrastructure, tools and budget.

Input	Tools	Output
- Statement of establishment - Mission - Vision	- Analysis of service requirements - Expert Consultations - Resource Analysis	- Target Community - Definition of Services

Target Community

The CSIRT target community is the group of persons or entities that will receive services from the team; in other words, they are the clients.

The CSIRT must clearly define what its target audience is, including whether or not different members of the community will receive different levels of service. This may vary depending on whether the criticality of the systems or infrastructures is managed and operated by a particular member of the community, or an existing CSIRT already serves a given entity. For example, military institutions often oversee their own networks and may not require the services of a national CSIRT. It is therefore crucial that a CSIRT determine whom it works for, what other teams are involved, and to what extent it serves the community. The target community may include other CSIRTs, ISPs, datacenter operators, and other actors whose trust and cooperation will be crucial for successful cooperation.



Authority Models with the Target Community

Authority models are the types of powers a CSIRT can exercise. Several authority models connect the CSIRT with its community. These models define the CSIRT powers and obligations when facing an incident occurring in its community.

There are four popular types of authority that a CSIRT can hold over its community:[13]

Full Authority

The CSIRT has authority to carry out all necessary actions relating to the management of an incident, and community members are required to implement the measures proposed by the CSIRT or, at most, allow members of the CSIRT to implement them.

Shared Authority

The decision regarding an incident is made jointly between members of the affected community and the CSIRT. The CSIRT supports the actors involved in an incident and collaborates with equipment and expertise.

Null Authority

The CSIRT has no authority over decisions regarding incidents. It provides advice, information and experience, but decisions are taken by those affected.

Indirect Authority

The CSIRT has no authority over the community, however it can exert indirect pressure on it-- for example, through regulators or other organizations with which the CSIRT has established bonds of trust.

Services

The services of a CSIRT are strongly related to its mission, target community and the knowledge, skills, and abilities of the human resources at its disposal.

These services can be provided entirely by CSIRT staff, with the assistance of stakeholders, or through other actors with whom the CSIRT has agreements, such as software or hardware companies. In each case the CSIRT should evaluate the best way to offer the service in a given situation, depending on resource availability and specialization.

In each case the CSIRT should evaluate the best way to offer the service in a given situation, depending on resource availability and specialization

The services provided by the CSIRT are usually grouped into three types: Reactive Services, Proactive Services and Value-added Services. [14]

Proactive Services

→ **Monitoring and alert services**

- External Monitoring
- Internal Monitoring
- Development of security tools
- Security alerts and Reports

→ **R&D Services**

- Security Audits
- Vulnerability scanning
- Malicious artifact scanning
- Technology Monitoring
- Artifact analysis
- Forensic analysis

Reactive Services

→ **Incident management**

- Post mortem analysis
- On-site assistance

→ **Vulnerability response**

→ **Malicious artifact response**

Value-added Services

→ **Training and education**

→ **Awareness raising**

→ **Risk Analysis and business continuity**

→ **Support to security undertakings**

Reactive Services

Reactive services are the most important services provided by a CSIRT. In essence, “reactive services” respond to cyber security incidents occurring within the CSIRT’s community or within its own infrastructure. A response can be launched based either on a request for assistance or from monitoring and sensor networks maintained by the team. The principle types of reactive services are incident management, vulnerability response, and artifact response.

Incident management

Incident management service consists of several phases: notification and receipt of an incident, classification or triage, response, analysis and resolution. The CSIRT must first determine the type, potential impact, and severity of an incident, followed closely by designating a response team to devise a plan of action that will restore services or systems to normal operation or otherwise mitigate the impact of a cyber-security event. In certain cases, this will necessitate that CSIRT personnel visit the site of the security event.

Many actors are typically involved in cyber-incident response, including ISPs, other CSIRTs, technology providers, law enforcement agencies, international actors, legal teams, press departments, and different areas of an affected organization. The CSIRT coordinates response activities and communications of the various stakeholders to optimize efforts and reduce incident resolution times. To accomplish this, the CSIRT should know the requirements and procedures of each of the stakeholders in order to positively manage interaction between them.

Vulnerability response

This comprises a variety of vulnerability management processes, including patching, implementation of countermeasures, and other mitigation strategies. As new patches become available for detected vulnerabilities, the CSIRT must notify all stakeholders and distribute patches or describe techniques for implementing countermeasures while coordinating and confirming that adequate measures are taken.

Response to malicious artifacts

A malicious artifact is a file or object in a system that is involved in an attack on a network or system, or used to evade security controls or measures. Managing malicious artifacts requires removing them from an affected system or informing stakeholders of how to do the same.

Proactive Services

These services aim to improve the infrastructure and security processes of the target community to prevent security incidents or reduce their impact when they occur. The main types of proactive services are performing monitoring, distributing alerts, and offering research and development services.

Monitoring and alert services

1 First Level

One of the most basic services offered by a CSIRT, monitoring and alerting involve the implementation of systems that detect security events, perform event and incident correlation, produce automated reports, and scan for vulnerabilities within the target community. To perform these functions, the CSIRT can either develop its own in-house solutions or employ third party commercial or open source tools and sensors. Information produced by monitoring and alert initiatives will inform strategic decision making and improve incident response processes.

2 Second Level

A more developed CSIRT will offer more advanced monitoring and alert services. These track target community infrastructure and systems in much more depth, but generally provide similar types of alerts and incident correlation as first level monitoring and alerts. More closely monitoring client systems allows for earlier detection of security events, vulnerabilities, or malicious artifacts. To perform this kind of in-depth monitoring, system interconnection or installation of safety sensors in community infrastructure is generally needed.

As a coordinator and collaborator, the CSIRT generates knowledge of the systems, processes, and infrastructure of the target community. Accordingly, the response team can develop strategies, specific tools, and plug-ins from existing systems to analyze, monitor and protect the particular infrastructure of the community it serves.

Research and Development

1 First Level

These services allow the CSIRT and its community to stay abreast of developments in the field of information security and incident response. Specifically, it will allow them to stay up to date on alerts, evolving threats, emerging attack vectors, best practices and new norms in services and device maintenance and operation, defense strategies, and a host of other topics.

2 Second Level

As a CSIRT matures, it will develop more robust R&D capabilities. With the information it gathers and generates, the CSIRT can carry out security audits and assessments on its own systems or those of the target community. This may include application or infrastructure analysis, review of security policies, vulnerability scanning, penetration testing, and compliance with market standards or norms.

As technology evolves, threats and vulnerabilities change. The CSIRT must be able to detect emerging threats or vulnerabilities inherent to new technologies and distribute information relevant to them that can improve security levels.

3 Third Level

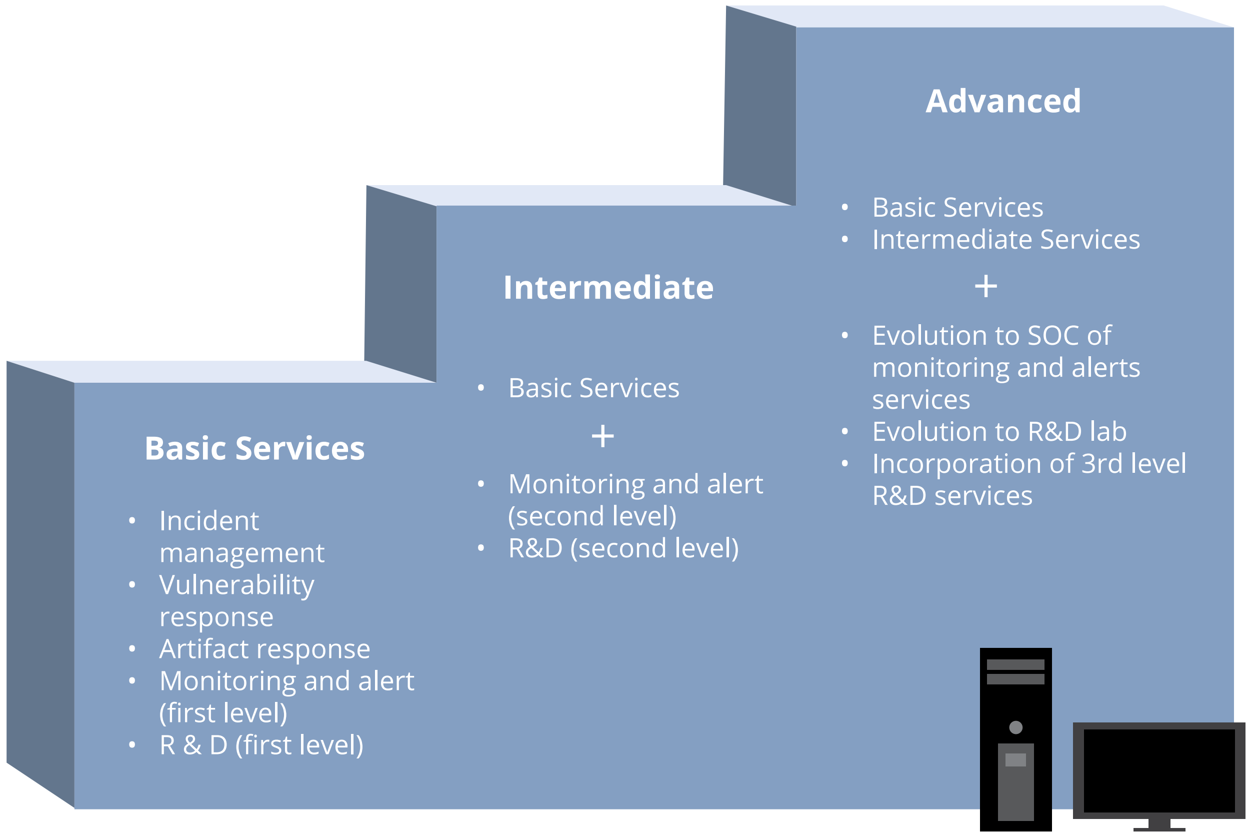
The most advanced CSIRTs will continue to develop R&D capabilities, for example, malicious code analysis, so as to be able to determine the nature, behavior and purpose of a specific artifact.

Value Added Services

These services complement monitoring and alert warnings issued by the CSIRT. In general, value added services consist of security training courses and events, awareness-raising initiatives, skills analysis, and security labs. By conducting these types of events, the CSIRT also builds trust within the community, and creates awareness of the response team's purpose and function, allowing it to operate more effectively. One of the most important aspects of efficient training activities is to identify the information gaps and needs of the target community. Much of this will be gleaned through the normal, day-to-day activity of the CSIRT and interaction with its clients. In delivering value added services, the CSIRT can partner with academic institutions or invite clients to share their experience and knowledge related to a security case study.

Evolution of CSIRT Services

The services offered by a CSIRT will depend on its size, infrastructure and resources, and the abilities of its team members. They can be broadly broken down into basic, intermediate, and advanced, and likely will grow as a team matures over time.



Basic Services

- Incident management
- Vulnerability response
- Artifact response
- Monitoring and alert (first level)
- R & D (first level)

Intermediate

- Basic Services

+

- Monitoring and alert (second level)
- R&D (second level)

Advanced

- Basic Services
- Intermediate Services

+

- Evolution to SOC of monitoring and alerts services
- Evolution to R&D lab
- Incorporation of 3rd level R&D services

D Organization and HR

To put the institutional framework into practice and to perform the services required by the target community, the CSIRT needs a defined organizational structure, including detailed roles and responsibilities of its personnel.

Input	Tools	Output
- Mission - Vision - Target Community - Services	Analysis of CSIRT structures Available material resources	Organizational chart HR

Organizational Structures

There are four main CSIRT structures[15,16]:

Localized Security Team

This is the least formal CSIRT structure. The theory behind the simple "security team" is that security events are resolved by existing staff in organizations. Security team members are not necessarily specialists in incident response or information security; they can be system administrators or database managers or have specialized knowledge in the various components or products involved in IT systems like firewalls and routers, among others. In most cases, the security team will not have all the expertise and experience necessary to perform robust security operations. For example, it may resolve an incident but not determine its cause, leaving the organization open to further exploitation. The nature of a "security team" usually precludes the implementation of best practices, research and development, monitoring, and security alert activities. Continued improvement in an organization's information security posture with a security team is not likely.

Centralized Incident Response Team

In this structure there is a single team responsible for the management and response of security incidents across a number of locations that belong to one larger organization. This model would be appropriate, for example, in an enterprise. This structure is appropriate for organizations whose IT infrastructure is not dispersed geographically.

In these structures, there is a defined response team and dedicated staff trained in managing information security and responding to security incidents. These teams interact with specialists on products or services.

Distributed Incident Response Teams

Large organizations with geographically-distributed IT infrastructures or several distinct business units often adopt distributed incident response structures. These are made up of a comprehensive response center divided into several teams, one of which coordinates the activities of the others. Incident response duties are divided according to each team's knowledge area, depending on the geographical location where incidents occur, or depending on the affected target community sector.

The role of the coordinating team is essential to ensure effective and standardized of response procedures, to maintain statistics of incidents, increase synergy, and promote collaborative work through the sharing of best practices and lessons learned, and how to properly allocate security resources.

Another vital function of the coordinating team is to facilitate interaction and cooperation between the teams.

Coordinating Team

This model is similar to the model of distributed response teams, but at the level of response centers. The difference is that the response center coordinator does not necessarily need to intervene in other coordinated teams' efforts.

This type of model arises from the response centers' need to interact coordinatively to achieve a common goal, or generate synergy between centers of similar sectors or regions, corporations, or agencies of a same government.

Its main function is to coordinate interaction and response effectiveness through coordination of efforts and collaboration, providing analysis of incidents and vulnerabilities, newsletters, statistics and documentation of best practices, among others.

It is important to note that in order to define the CSIRT model to be implemented, it is essential to analyze the services they want to offer. Certain CSIRT models are not suitable for the provision of some of the above-mentioned services, particularly services that require permanent resources. For example, it is not suitable to implement monitoring services with Security Team models.

It is important to define the type of CSIRT model to be implemented, since this will have a direct implication on the size of the organization.

Organization Size

The organizational structure of a CSIRT, like any organization, depends on precisely what it will do and how it aims to accomplish its goals. Some of the questions the CSIRT Project Manager needs to answer that will help determine how the team will be organized are:

- What services do I want to offer and at what times?
- How big is the target community?
- What is the geographical distribution of my target community?

Where the CSIRT is housed will similarly play a part in determining how it will be structured. It also bears mentioning that its organizational model, along with the services offered, is subject to change over time.

Roles and Responsibilities

To define a CSIRT's organizational structure, one must have a clear idea of the various roles and responsibilities within a response team.[17]

MANAGEMENT

- Strategic management of the team/ response center
- Supervises the entire team
- Interviews and hires new team members
- Attends meetings of the security advisory council

MIDDLE MANAGEMENT

- Supports leadership
- Leads the team in day-to-day activities
- Assigns duties and tasks
- Manages codes
- Authorizes information access permits

EVENT CLASSIFIER

- Provides initial incident response assistance
- Classifies and prioritizes the information received from a case

TRIAGE MANAGER

- Classifies and prioritizes events
- Assigns cases to technical staff

INCIDENT HANDLER

- Analyzes incidents, monitoring, recording and response
- Coordinates incident response
- Collaborates with other response groups or technicians to solve an incident

ANALYST / RESEARCHER

- Conducts specific research
- Develops technical material for internal use or training
- Performs monitoring tasks
- Develops tools

COMMUNICATIONS MANAGER

- Develops and publishes CSIRT documents
- Maintains the CSIRT website and social media profile

NETWORK ADMINISTRATOR

- Manages and maintains the CSIRT networks, IDS and ISP
- Assists in responding to incidents when networking expertise is needed

SYSTEMS ADMINISTRATOR

- Manages and maintains CSIRT systems
- Assists in responding to incidents when systems expertise is needed
- Manages access to information

ASSISTANT

- Assists staff in performing their assigned tasks as directed

REPRESENTATIVE

- Represents the CSIRT at events
- If instructed, the representative can train other actors

SPEAKER

- Authorized communication channel with the press

RECORDS CUSTODIAN

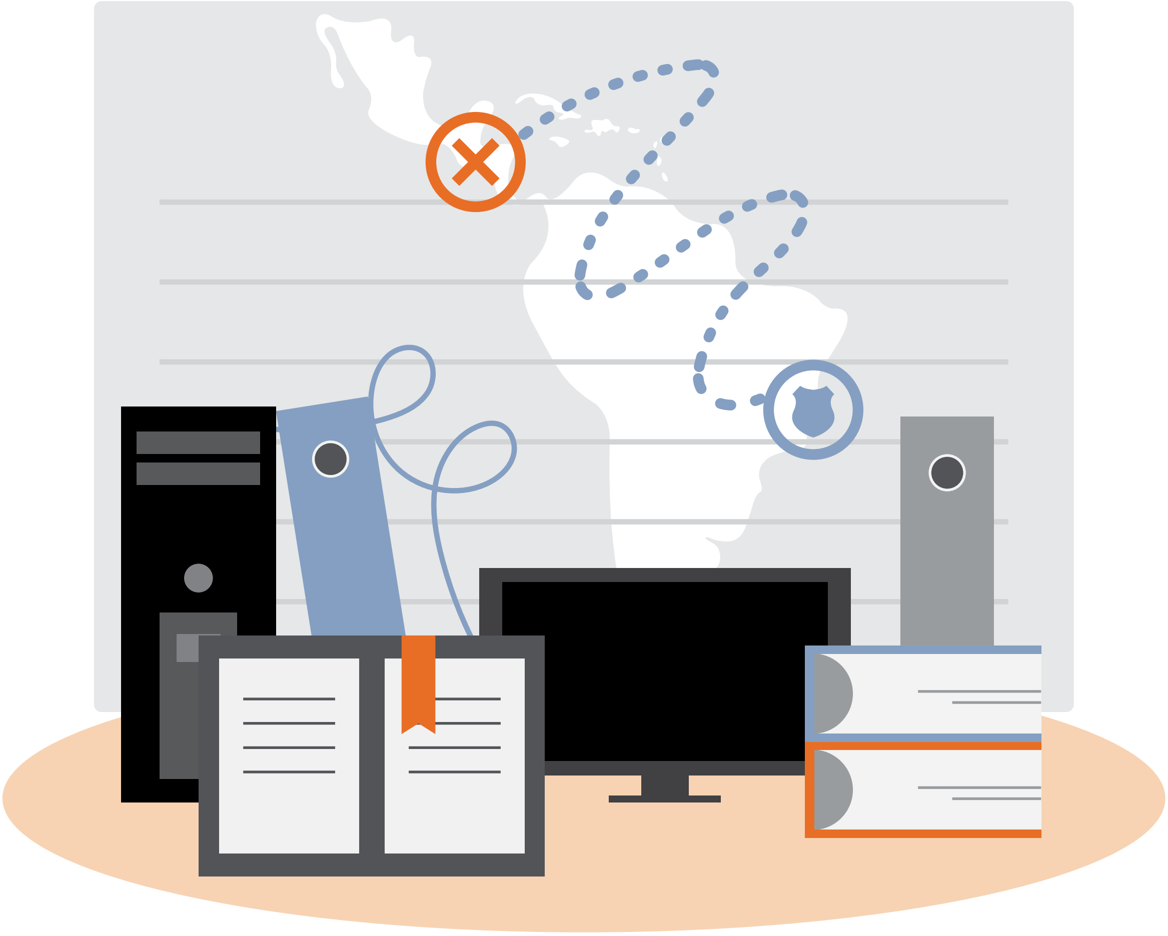
- Access to secure information repositories

These roles will be distributed among different people and work areas. In most all CSIRTs, people will be in charge of multiple roles at once. In this case, it is essential that there is a policy and practice of separation of duties.

Here is how these roles are assigned to different CSIRT areas.

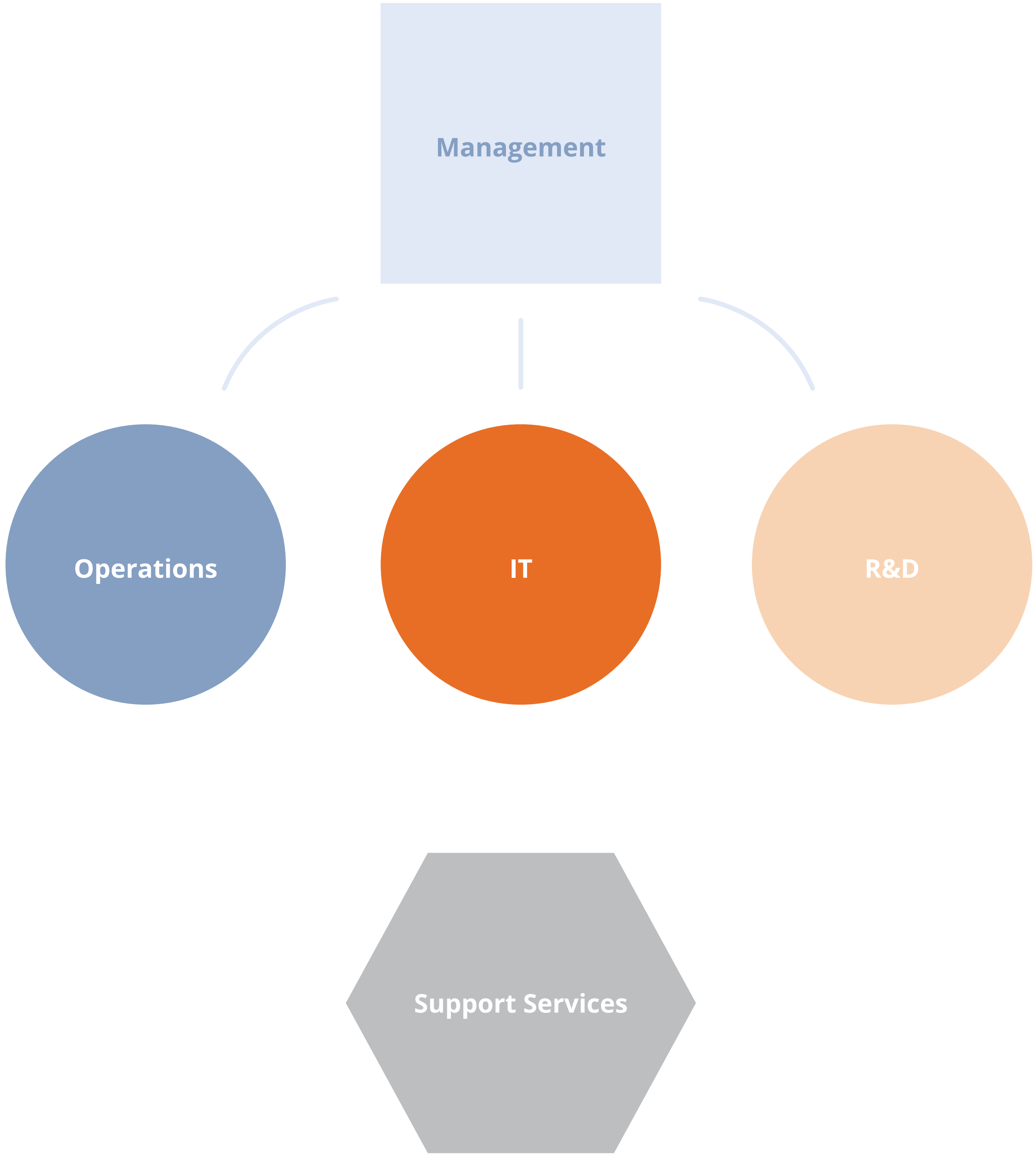
Organizational Structure

As mentioned above, the initial services recommended for a National CSIRT are incident management, vulnerability management, system monitoring, alert publishing and training.



The following diagram illustrates the minimal initial structure recommended for a National CSIRT, which can grow over time as needed. Several CSIRTs in the Americas, like those from Panama, Paraguay and Uruguay, began with organizational structures similar to this and have shown significant growth.

Support Services:
Marketing. Communications.
Legal Support. Press Management.
Administration & Finance



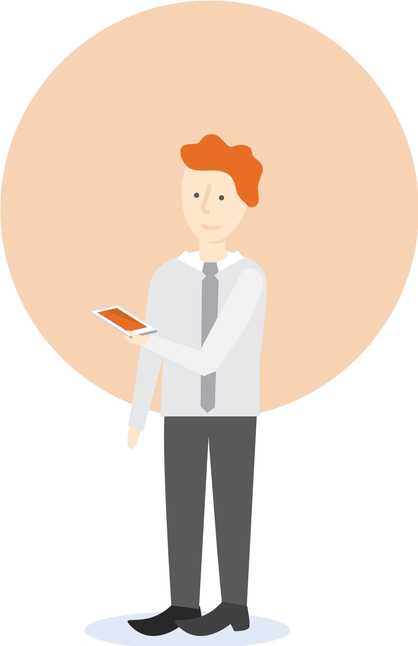
Under this model, each area is responsible for the following tasks:

Management

- Strategic management
- Monitoring of activities
- External linkage: other CSIRTs, organizations and advisory board
- Budget management
- Media/public liaison

CSIRT Management primarily sets the course for the organization and conducts strategic planning. It also establishes co-operation agreements with other organizations and liaises with the CSIRT Steering Committee. The CSIRT director also acts as spokesperson to the press.

Operations



- Incident Management
- Monitoring

The **Operations** area is the critical part of the CSIRT. This is where incident management, monitoring, and incident analysis is performed. It may take some time for the operations area to begin receiving large numbers of incidents as word spreads of the CSIRTs existence and the services it offers to constituents.

IT

- Management of IT infrastructure
- Operations Support
- Support to R&D

The **IT Section** implements and manages all proprietary systems that control and administer the CSIRT's email, webpage, file server, ticket management system, monitoring system, network and firewalls. Like the R&D department, the IT section will be busy from the outset deploying and adjusting the CSIRT's architecture.

Research and development

- Technological Observatory
- Statistical analysis of incidents and trends
- Development of systems and tools
- Training
- Special Research
- Support to Operations

Research and Development is the area of the CSIRT that will implement the teams secondary functions such as the development of tools, carrying out trainings, and otherwise researching new cyber security trends and threats. R&D will be busy from the inception of the CSIRT since it will be in charge of the bulk of planning, training, and development of any necessary in-house solutions. This area will work closely with the IT area.

Support Services

- Marketing/communications
- Legal Support
- Press Management
- Administration and Finance

Support Services that oversee press management, legal considerations, and administration and finance are essential to the functioning of any CSIRT. These activities must be accounted for in a National CSIRT, although they can be subcontracted or provided externally.

As the response team matures, it will likely create new areas and functions. Among possible new areas are:

Laboratory

This area, which can fall under management or R&D, will conduct forensic activities and/or malware analysis and provide research services to other areas.

Security Operations Center

If the service roadmap indicates having a security operations center, a SOC area can be created, which can depend directly on management or operations.

Information Security Management Systems

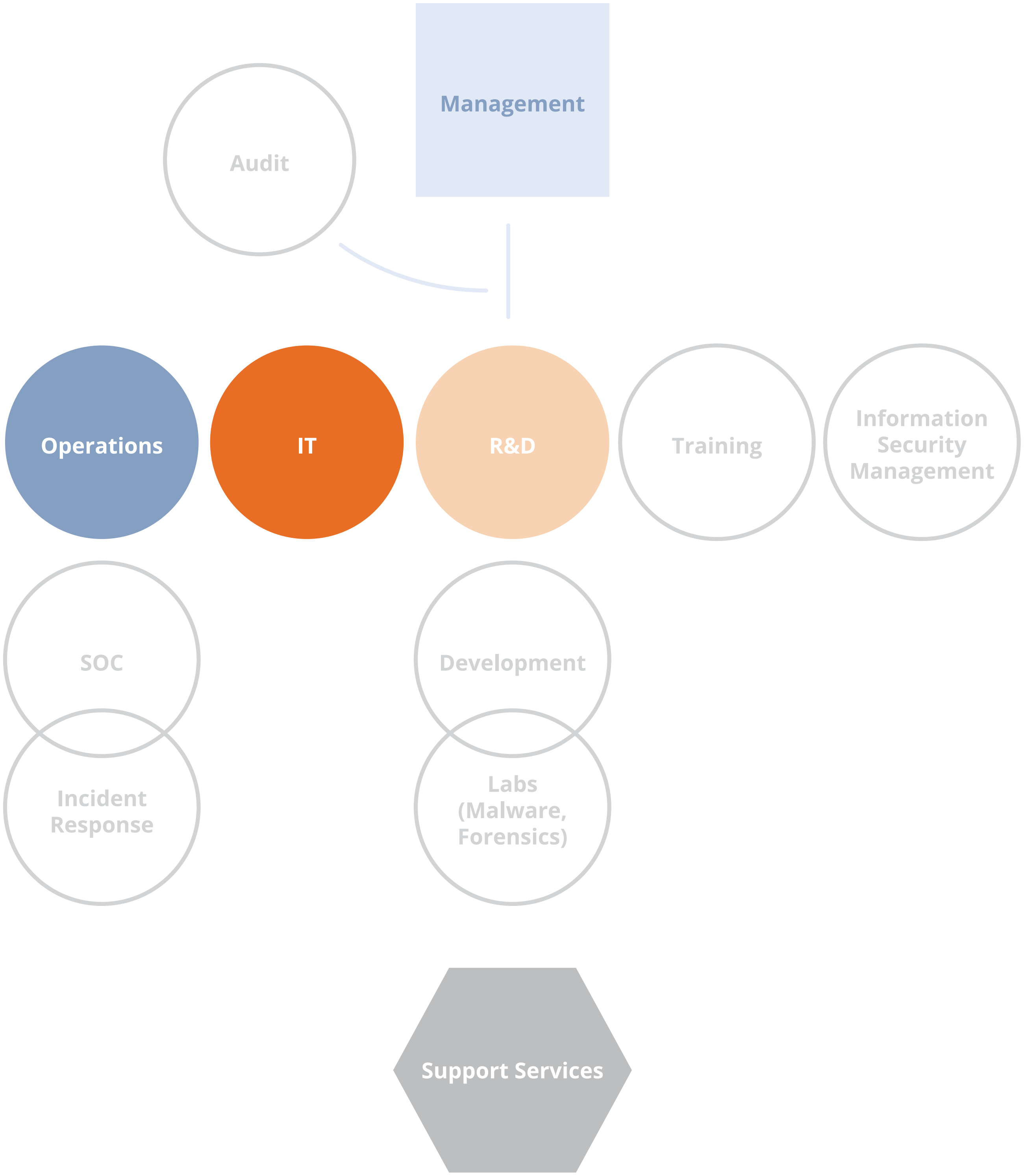
If the aim is to establish support services for the implementation of ISMS, a specific area may be established for that.

Training

If the CSIRT and its target community have sufficient requests for training, a dedicated training department can be established.

As the team size grows, it may eventually have to incorporate an auditing department to verify whether policies and procedures at the CSIRT are followed in accordance with the level desired by the target community.

With additional services, the CSIRT’s flowchart would be:



Size and Quantity of Resources

Once the desired structure is defined, the CSIRT Project Manager will recruit and hire personnel with the skills required by the functions to be carried out. Regardless of what position they are hired for, personnel should have a breadth of skills so as to avoid single points of failure within the CSIRT.[19] Moreover, CSIRT staff will not be expected to devote 100% of their time to any singular activity, especially in the time immediately following its launch. In certain cases, successful teams may begin with three people, for example one director, one IT manager and one leader to cover multiple roles, including operations and R&D, that also supports the IT manager. In the first phase of CSIRT development, (implementation), IT support takes priority. Incident-response capacity will grow as the CSIRT increases its staff size, secures funding and becomes fully operational. This will be particularly true in the operations department.

Regardless of what position they are hired for, personnel should have a breadth of skills so as to avoid single points of failure within the CSIRT

The table shown below provides an example of how a CSIRT with a staff size of 10 may distribute its roles and functions. Information was acquired through consultations with CSIRTs from the region, that, while varying in circumstances and experiences, all serve as models for success.

Notes

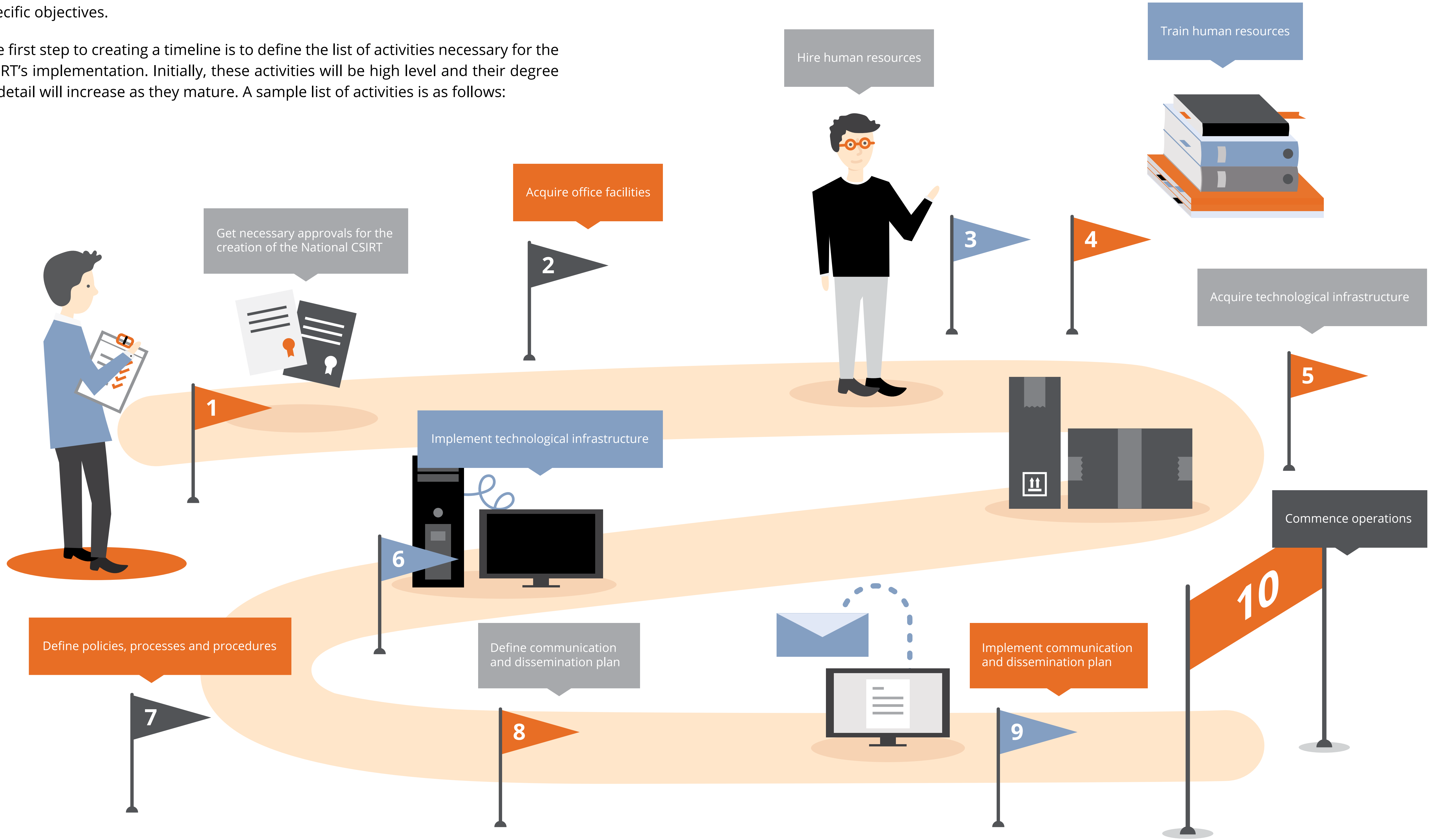
- This table is based on experiences acquired through consultation with some CSIRTs in the region (no CSIRT is structured exactly the same; each CSIRT is different based on its particular needs and/or functions).
- Some positions may be assumed by the same person.

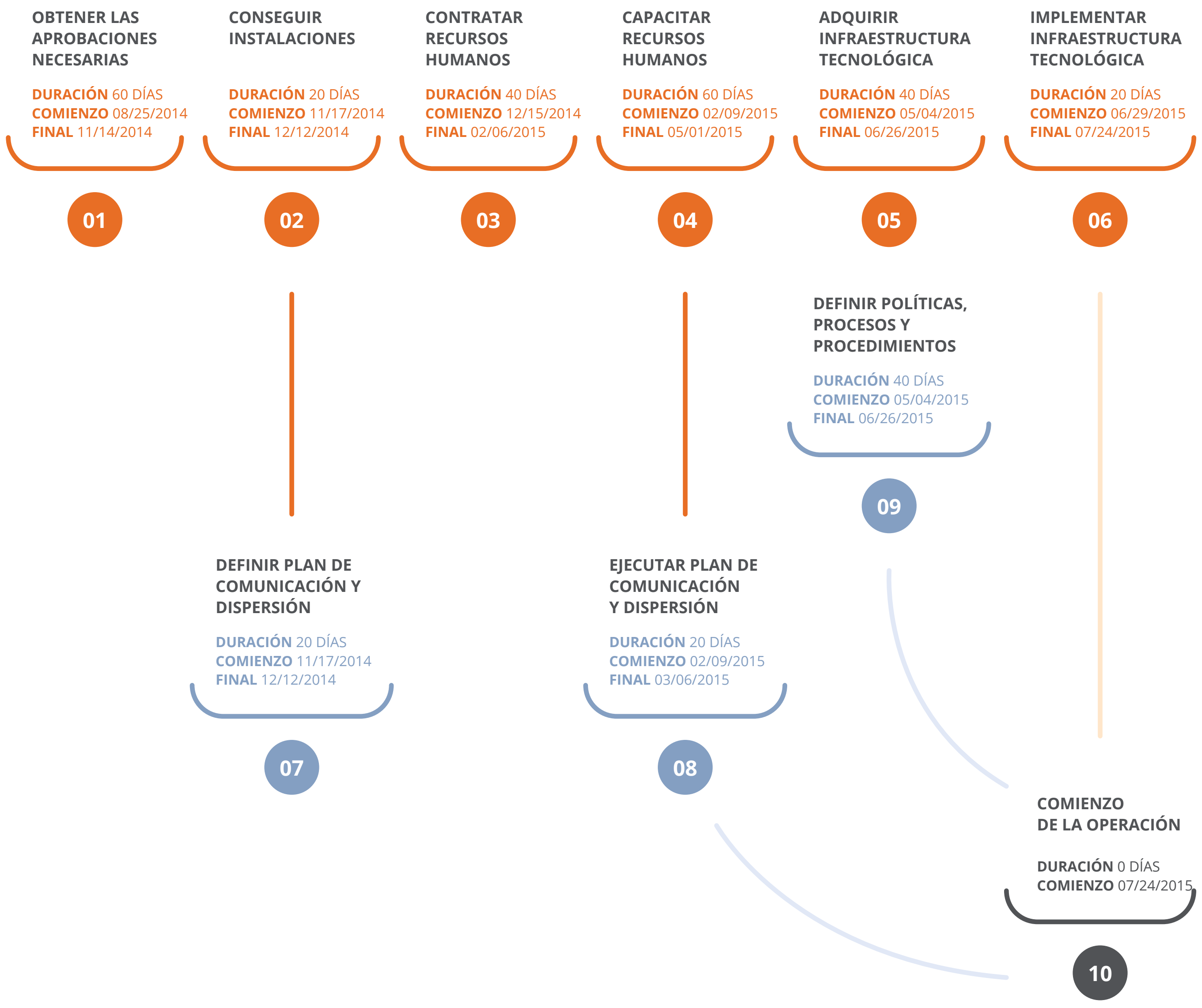
CSIRT Departments	Personnel	
	1st Phase | Implementation 9 (6 employees + 3 support staff)	**2nd Phase | Operation** 15 (12 employees + 3 support staff)
Management 	**1** Director/Coordinator	**1** Director **1** Coordinator
IT Support 	**1** Leader **2** Technical Specialists	**1** Leader **2** Technical Specialists (Network Administrator, Systems Administrator)
Research and Development 	**1** Leader **1** Technical Specialists	**1** Leader **2** Security specialists (Analyst/Researcher, Records Custodian)
Operations 	**1** Leader **1** Technical Specialists	**1** Leader **3** Incident specialists (classification, triage, handling)
Support Services*1 	**1** Lawyer (Legal support) **1** Reporter (communications) **1** Financial analyst	**1** Lawyer (Legal support) **1** Reporter (communications) **1** Financial analyst

Timeline

The implementation period of a CSIRT must be guided by a defined timeline and specific objectives.

The first step to creating a timeline is to define the list of activities necessary for the CSIRT's implementation. Initially, these activities will be high level and their degree of detail will increase as they mature. A sample list of activities is as follows:


1
Get necessary approvals for the creation of the National CSIRT
2
Acquire office facilities
3
Hire human resources
4
Train human resources
5
Acquire technological infrastructure
6
Implement technological infrastructure
7
Define policies, processes and procedures
8
Define communication and dissemination plan
9
Implement communication and dissemination plan
10
Commence operations



Once a list of activities is completed, they must be organized sequentially, taking into account the dependencies among them. One of the most convenient ways to map out and plan a project, including dependencies, is to construct a diagram using the Precedence Diagramming Method (PDM).

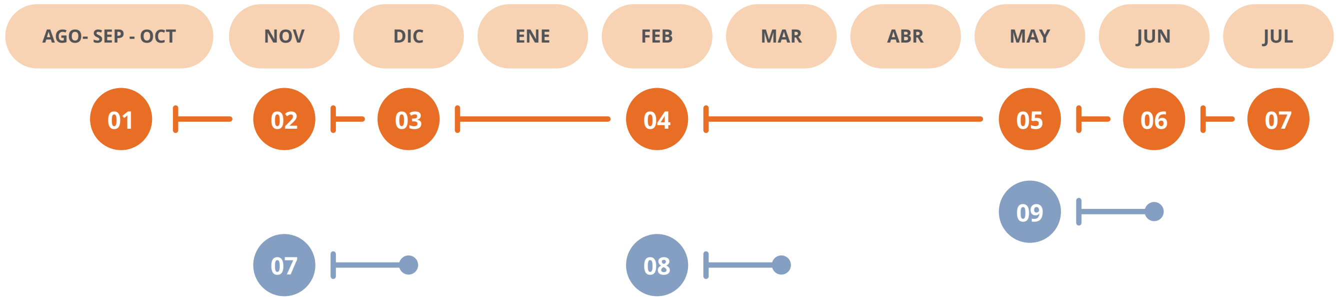
The Precedence Diagramming Method (PDM) uses nodes and arrows. Each node represents an activity that is connected with another via arrows representing dependencies. In PDM there are four types of relationships of activities:

- **Final to Start:** The start of a successor activity depends on the end of the predecessor.
- **Final to Final:** the completion of a successor activity depends on the end of the predecessor activity.
- **Start to Start:** The start of the successor activity depends upon the initiation of the predecessor activity.
- **Start to Finish:** The completion of the successor activity depends upon the initiation of the predecessor activity.

During this stage of planning, the Project Team should examine parallelizing activities to reduce the time needed for implementation.

An example of a precedence diagram with the activities listed above could be mapped as above.

	NOMBRE	DURACIÓN	COMIENZO	FINAL	PREDECESORES
01	OBTENER LAS APROBACIONES NECESARIAS	60 DÍAS	08/25/14	11/14/14	
02	CONSEGUIR INSTALACIONES	20 DÍAS	11/17/14	12/12/14	01
03	CONTRATAR RECURSOS HUMANOS	40 DÍAS	12/15/14	02/06/15	02
04	CAPACITAR RECURSOS HUMANOS	60 DÍAS	02/09/15	05/01/15 v	03
05	ADQUIRIR INFRAESTRUCTURA TECNOLÓGICA	40 DÍAS	05/04/15	06/26/15	04
06	IMPLEMENTAR INFRAESTRUCTURA TECNOLÓGICA	20 DÍAS	06/29/15	07/24/15	05
07	DEFINIR PLAN DE COMUNICACIÓN Y DISPERSIÓN	40 DÍAS	05/05/15	06/26/15	04
08	EJECUTAR PLAN DE COMUNICACIÓN Y DISPERSIÓN	20 DÍAS	11/17/14	12/12/14	01
09	DEFINIR POLÍTICAS, PROCESOS Y PROCEDIMIENTOS	20 DÍAS	02/09/15	03/06/15	03
10	COMIENZO DE LA OPERACIÓN	0 DÍAS	07/24/15		06 - 07 - 09



Finally, once the PDM is ready, the timeline must be established. This requires estimating the duration of each of the activities, which depend on the resources available to execute them. There may be important external factors to consider in determining the timeline, as well, including political deadlines, licensing processes, dates of training courses taught, resource allocation, etc.

There are various ways to estimate the duration of activities needed for CSIRT implementation. Three are shown below:

- **Expert Judgment:** With background information the project team may consult experts in the field, who can perform the estimation based on their experience. This technique is simple and effective.
- **Estimation by analogy:** This technique looks at historical information of other projects that have had similar activities and uses historical values of durations.
- **Estimation of three values:** The aforementioned techniques are used, but in this case three values are taken for estimation: one pessimistic, one optimistic and one most likely. This technique is widely used when it is difficult to find historical information with similar properties.[20]

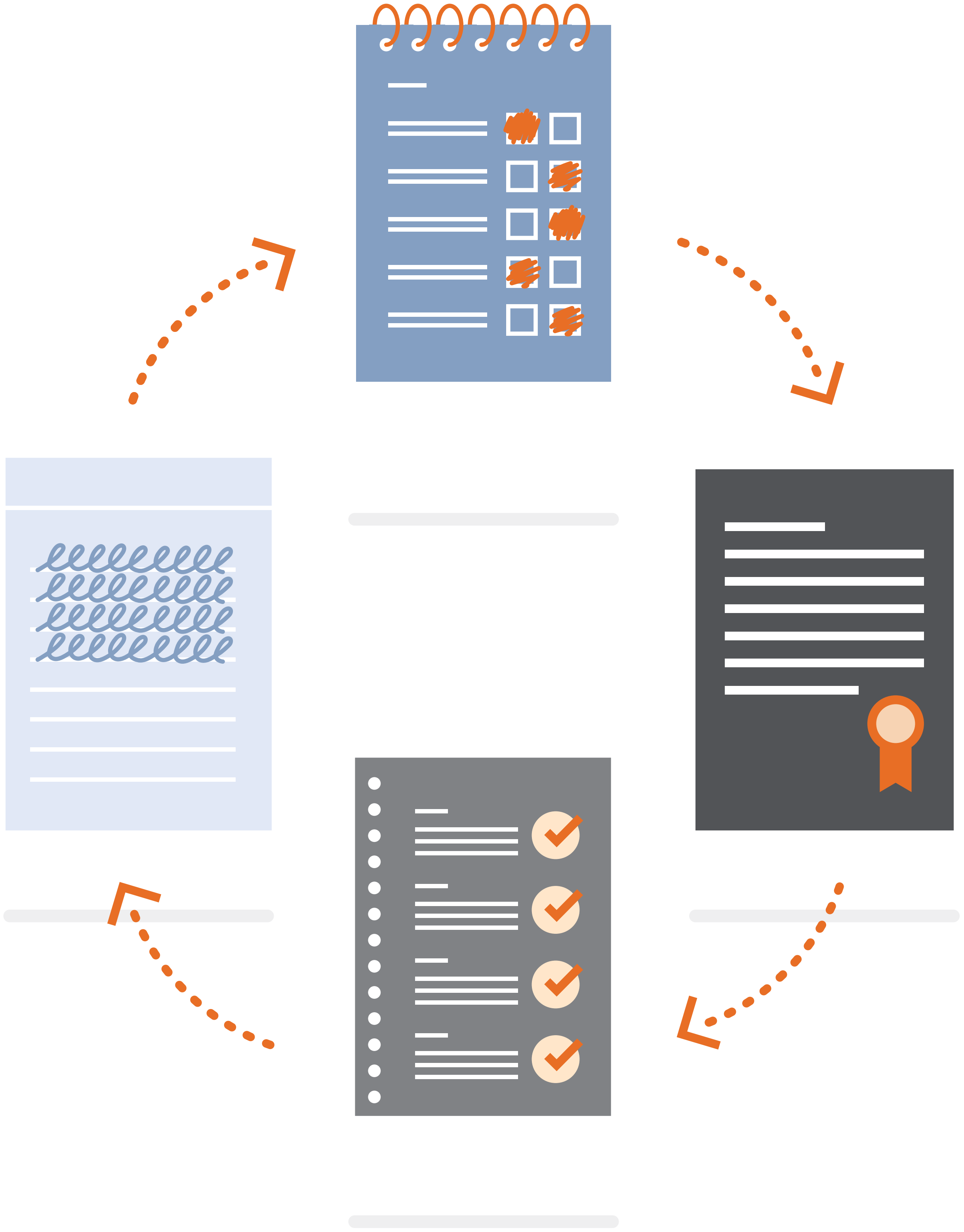
Finally, the timeline diagram is set. A sample Gantt chart is shown above.

Conclusion of Preliminary Planning

Upon completing the planning stage, there should be a number of finalized documents related to the establishment of a National CSIRT, including:

- Stakeholder Identification Document
- Stakeholder Management Plan
- Document of Establishment of the National CSIRT
- Mission and Vision
- Institutional Framework
- Legal framework
- Minutes of meetings
- Lists of participants to the different activities
- Emails exchanged with experts
- Definition of target community
- List of Services to be provided
- Organizational Structure
- Human Resources needed
- Timeline for implementation

These documents will serve as a reference and guide to the rest of the project; some will be signed, formal documents, while others only supporting documents.



2 IMPLEMENTATION

A Human Resource Selection

This section details the knowledge, experience, and abilities necessary for potential employees of a CSIRT. Hiring qualified candidates is undoubtedly one of the most difficult parts of the CSIRT establishment process, and may be especially challenging in Latin America and the Caribbean, or any other place where highly trained computer security technicians may be in short supply. Nevertheless, this section can be used as a reference when evaluating candidate profiles during the recruitment process.

Profiles are listed for positions in each of the main areas within the CSIRT: Management, R&D, IT and Operations.

Management

For managers, leadership skills, qualities, and experience. Of course, a candidate may not always fit a job profile perfectly; however, he or she may be the best option available out of the pool of applicants for a given position.

TRAINING

Required

- University degree in IT
- Concentration in cyber security

Desired

- Graduate studies in management (MBA, MMoT or similar)
- Cyber Security certifications (CISSP, CISM, CISA or similar)

EXPERIENCE

Required

- Over ten years' experience in technical positions in IT or Cyber Security
- More than three years' experience in IT management

Desired

- Experience in cyber security incident response highly desirable
- Experience in similar positions

Operations

For positions in Operations, persons who fit the profile will be efficient, organized and dynamic and will be able to adapt to high-pressure environments.

TRAINING

Required

- University Degree in IT
- Concentration in cyber security

Desired

- Specialized courses and experience in cyber security incident response
- Specialized courses in computer forensics or other area of cyber security and information assurance
- Cyber security certifications (CISSP, CISM, CISA or similar)

EXPERIENCE

Required

- More than five years' experience in technical positions in IT or cyber security

Desired

- Experience in operations and cyber security incident response
- Experience in agile management methodologies
- Experience in systems administration, support and work in organizations using ITIL

R&D

The profile of R&D is focused on systems development and analysis. R&D specialists must be detail oriented and organized while also possessing programming and scripting skills.

TRAINING

Required

- University Degree in IT
- Knowledge of systems development, familiarity with at least three programming languages (Python, BashShell, PHP, C++, Java, etc.)

Desired

- Specialized courses in cyber security and cyber security incident response
- Specialized courses in computer forensics
- Cyber Security certifications (CISSP, CISM, CISA or similar)

EXPERIENCE

Required

- More than five years' experience in technical positions in IT, project development, and cyber security

Desired

- Research and development experience
- Experience in agile management methodologies
- Experience working with PKI and cryptography systems

IT

All technicians at the CSIRT will have IT experience and knowledge. What differentiates the specialist in charge of IT is that they will be the system administrator and must possess knowledge of cryptography.

TRAINING

Required

- University degree or IT advanced student

Desired

- Specialized courses in cyber security and cyber security incident response
- Management courses based on ITIL

EXPERIENCE

Required

- More than three years' experience in technical positions in IT or system administrator

Desired

- Experience in organizations using ITIL
- Experience in agile management methodologies
- Experience working with cryptographic systems (PKI, PGP)

B Training Requirements

This section describes the suggested training for each of the members of the National CSIRT staff. Bear in mind that the courses listed here can be replaced or complemented by other similar trainings that cover comparable topics. While the courses listed below do not include those offered by manufacturers, they are often some of the best but can be quite expensive.

Additionally, there are university undergraduate and graduate specializations available, depending on the country or region.

General Cyber Security

The (ISC)² (International Information Systems Security Certification Consortium) and ISACA (Information Systems Audit and Control Association) organizations offer some of the most respected and comprehensive cyber security certifications available, particularly the CISSP, CISM, and CISA titles. Training for these certifications can be found on their respective websites:

- → ISACA
- → (ISC)²

The CERT Coordination Center (CERT-CC) at Carnegie Mellon University also has excellent cyber security courses including Information Security for Technical Staff, many of which are available through its online learning platform.

Training in Cyber Security Incident Response

The authoritative institutions for cyber security incident response are Carnegie Mellon University (CMU) and the SANS Institute.

CMU offers both basic and advanced cyber incident handling courses. Links to these courses are found below:

- → Fundamentals of Incident Handling
- → Advanced Incident Handling

The SANS Institute offers certification in incident response and a multitude of other courses related to information security, including those that cover hacking techniques, exploitation, and incident handling:

- → Incident response
- → Hacker Tools, Techniques, Exploits and Incident Handling

Forensics and malware analysis courses

CMU and SANS are world leaders in courses on forensics and malware analysis as well:

- → CMU
  Advanced Forensic Response and Analysis
- → CMU
  Malware Analysis Apprenticeship
- → SANS
  Advanced Computer Forensics and Incident Response, FOR 508
- → SANS
  Advanced Network Forensics and Analysis, FOR 572
- → SANS
  Reverse-Engineering Malware: Malware Analysis Tools and Techniques, FOR610

C IT Facilities and Infrastructure

This section describes the basic facilities the CSIRT must maintain, including IT infrastructure, network architecture and diagrams. It is one of the many ways a CSIRT could structure its hardware.

As a general rule, CSIRT facilities, their data networks and telecommunications will be designed with great care to not only protect sensitive information collected but also protect the CSIRT Staff. This means that information should be stored and managed by the CSIRT itself, as opposed to having it outsourced or stored off site or out of country.

CSIRT Facilities

Owing to the sensitivity of the information with which it works, a CSIRT and its employees must be secured much in the same way an organization protects a datacenter. This means that a CSIRT cannot be in an open cubicle environment. Rather, it should have its own office space separated by walls and doors, thereby reducing the possibility of sensitive information being seen or heard. Access to CSIRT facilities should be restricted in order to prevent unauthorized access to resources and information. The building or the area where the main CSIRT facilities are located must have 24-hour surveillance to minimize the risk of improper access to facilities.

Servers, communications equipment, logic safety devices and data repositories can stay in a datacenter or in the CSIRT facilities, but in all cases the physical and logical access to equipment shall be governed by strict access control that will ensure information access policies are upheld. In addition to securing electronic information, the CSIRT shall maintain a safe or deposit box to store sensitive non-digital information, tokens, hard disks and servers, among others.

Access to CSIRT facilities should be restricted in order to prevent unauthorized access to resources and information.

The following diagram gives an example of a blueprint for a CSIRT. The example should serve as a guideline for setting up a CSIRT facility; however, countries may adapt the model to fit their needs and logistical realities.

General considerations

→ **Means of outfitting the space**

- Air conditioning and False-floors (primarily for the Data Center)
- Detection systems and fire extinguishers in the common rooms and Data Center
- Redundant systems (Uninterrupted Power Supply (UPS) source, air conditioner, etc.)
- Locked, stationery cabinets

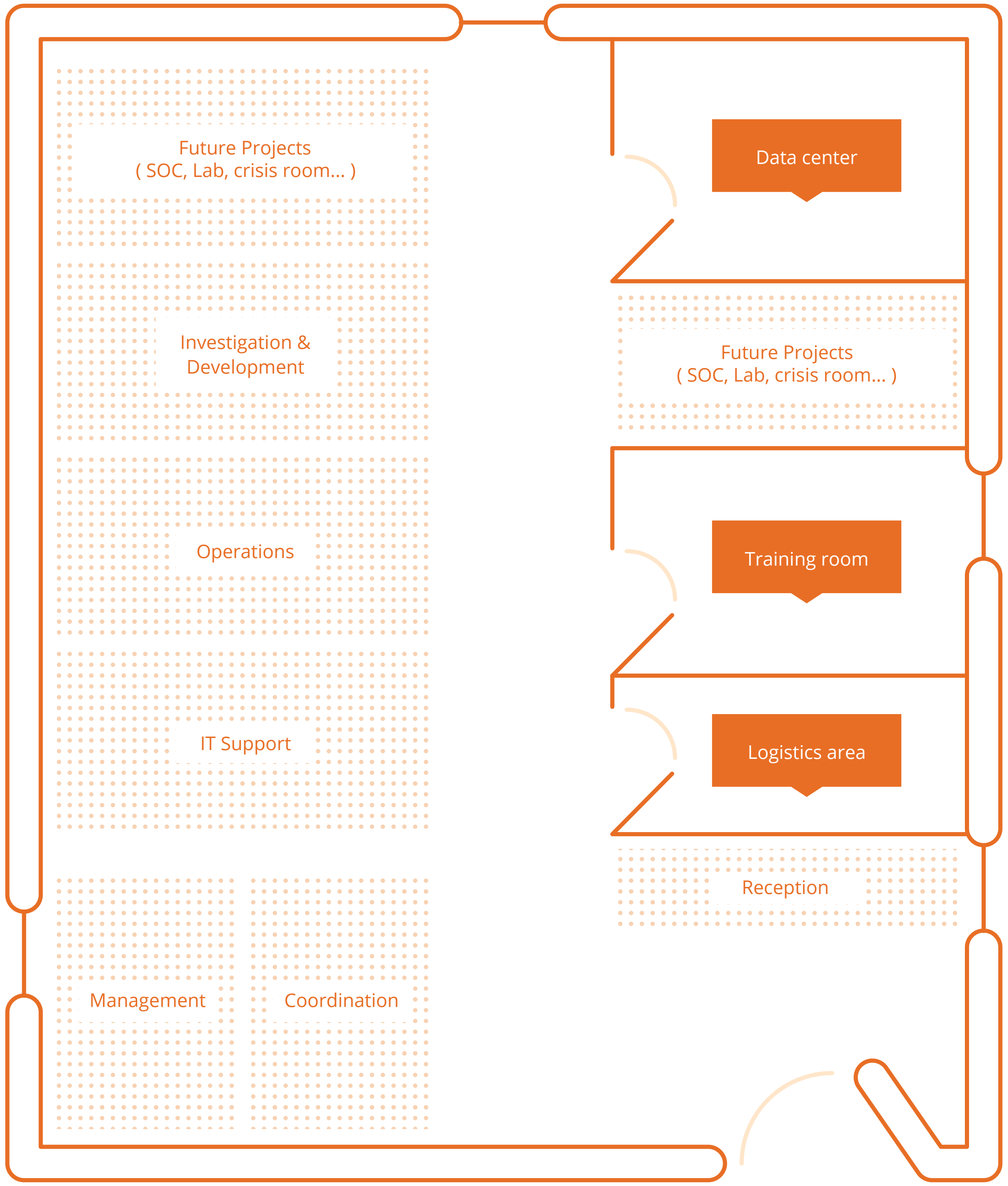
→ **Methods of restricting physical access & awareness to the zones**

- Controlled access to:
  - the building (doors and windows)
  - the floor
  - the common zones (Operations, IT support, R&D, etc.)
  - the Data Center
  - the Logistics area
  - the future projects (lab, monitoring room)

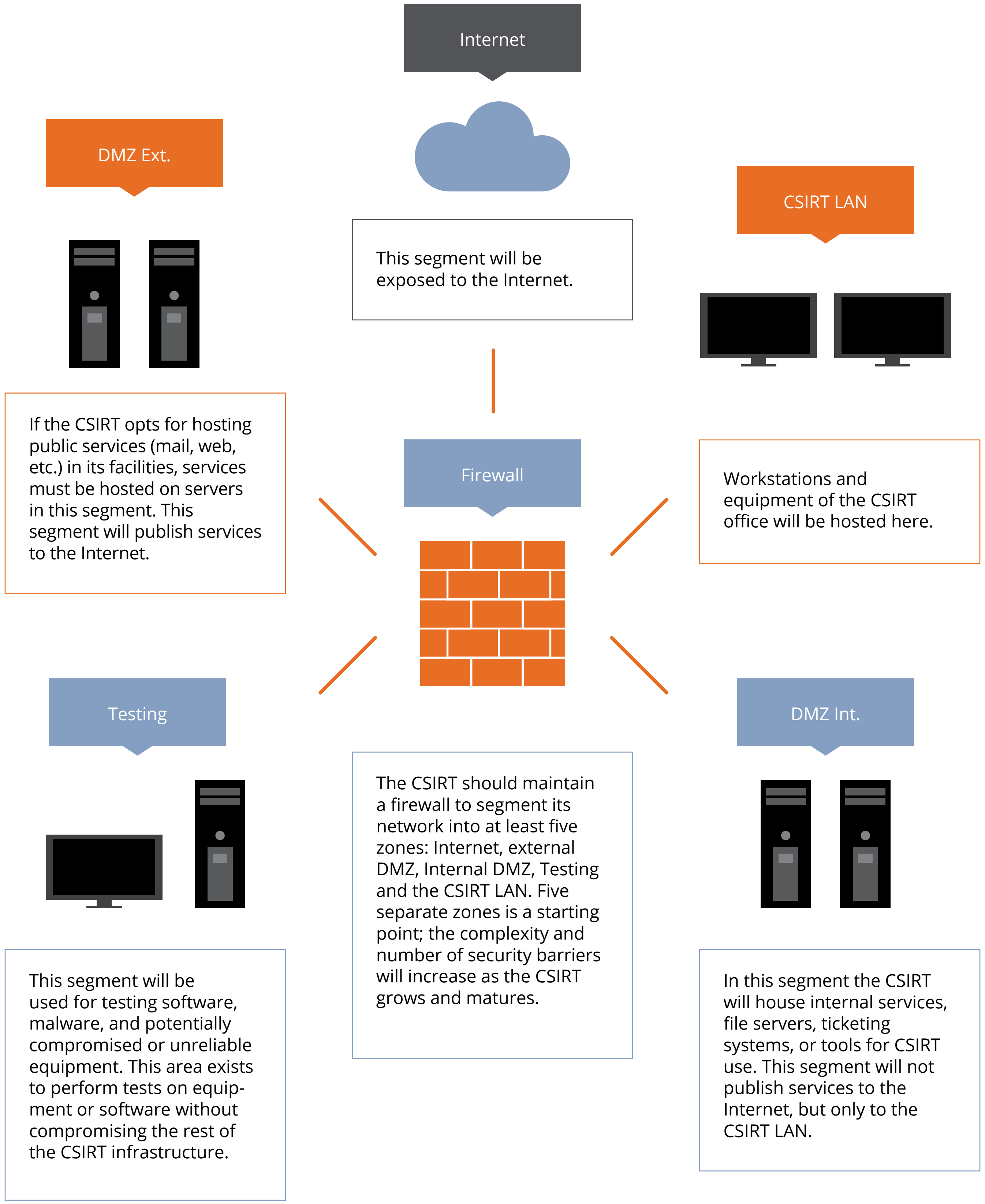
→ **Restricted visits (providers, etc.), accompanied all the time in all CSIRTs areas.**

→ **Vigilance through CCTV**

Basic Floor Plan



CSIRT Network Basic Design



This segment will be exposed to the Internet.

If the CSIRT opts for hosting public services (mail, web, etc.) in its facilities, services must be hosted on servers in this segment. This segment will publish services to the Internet.

Workstations and equipment of the CSIRT office will be hosted here.

This segment will be used for testing software, malware, and potentially compromised or unreliable equipment. This area exists to perform tests on equipment or software without compromising the rest of the CSIRT infrastructure.

The CSIRT should maintain a firewall to segment its network into at least five zones: Internet, external DMZ, Internal DMZ, Testing and the CSIRT LAN. Five separate zones is a starting point; the complexity and number of security barriers will increase as the CSIRT grows and matures.

In this segment the CSIRT will house internal services, file servers, ticketing systems, or tools for CSIRT use. This segment will not publish services to the Internet, but only to the CSIRT LAN.

Suggested Basic Equipment

Computers and servers

CSIRT software systems include the following:

Institutional Web Server

This server contains the institutional site where all public, non-sensitive information on CSIRT issues, including alerts, newsletters, contacts and incident reporting forms are located.

Institutional Mail Server

This server is in charge of communications via CSIRT email and stores the CSIRT e-mailboxes.

Intranet Server

The purpose of this server is to facilitate information exchange between CSIRT staff. It stores data relevant to the team and procedures, incident response techniques, best practices, operation manuals, incident documentation and other information of interest.

File Server

This server is used to store the team's digital files, which should stay online and be published within the CSIRT facilities.

Server backups

This server is tasked with backing up information from all CERT systems and workstations. Offsite vault backups are generated from this computer.

DNS Server

This server is responsible for name resolution of CSIRT infrastructure.

Monitoring Server

Active monitoring of systems is implemented on this CSIRT server, including: monitoring of government portals, CSIRT proprietary monitoring and active vulnerability detection systems. It is recommended that monitoring consoles be visible for all CSIRT staff.

Hub and events correlation

The role of this server is to concentrate all CSIRT systems audit trails, implemented monitoring systems and sensor network deployed by it. This server performs event correlation and alerting.

Log system and incident tracking

This is perhaps the most important of the CSIRT's servers and is committed to keeping records and tracking CSIRT incidents. It records reports of incidents received, communications flowing into and out of the CSIRT related to incident response, and is used to check the status of the technicians involved in an incident response. It also serves as a source of knowledge to the team. Each email sent to the incidents@cert.xx box as well as the completed forms on the CSIRT website will automatically generate a ticket in the management system. The triage manager will use this system to assign incident handlers to a particular ticket and close incidents at the appropriate time.

Computers

CSIRT staff must have laptops that are used exclusively for work functions.

Telephones

The CSIRT has direct access to telephone services, fixed line, IP telephony and mobile phones that allow it to make local and international calls as required to operate.

Fax

It is recommended that the CSIRT have an exclusive-use FAX machine within the CSIRT facilities in order to prevent any fax with sensitive information from being seen by unauthorized personnel.

Shredder

The CSIRT must have a shredder that allows it to destroy sensitive printed and CD information. This shredder can be shared with other members of the organization outside of the CSIRT, but the destruction of materials should be performed by the CSIRT staff, or as indicated in the information destruction policy.

Portable logical storage

During incident response, it is often necessary to use external drives or flash drives to store information. The CSIRT should have at least four 2TB external drives and five 32GB flash drives.

D Operational polices and procedures

CSIRT policies are central to its operation. They are guidelines to be followed by its staff in performing operations and reflect the guidelines of the CSIRT sponsors, govern the operation and activities of the response center, and ensure the confidentiality, availability and integrity of the CSIRT information and resources, as well as the quality of its services.

The policies of a CSIRT, in addition to serving as a guide for its employees and target community, are useful resources for members of the target community, since they detail when a CSIRT provides what type of services and how it maintains and protects the information it manages.

FIRST, the largest international forum of CSIRTs in the world, has the following minimum mandatory policies for a CSIRT that wishes to become a member of the community.

Mandatory Minimum Policies

Information Classification Policy

This policy defines how the CSIRT classifies information and differentiates between secret, sensitive, confidential and public information.

Information Protection Policy

This policy defines how to protect information according to its assigned.

Information Retention Policy

This policy defines how long the CSIRT should keep records or other information in its possession.

Information Destruction Policy

This policy defines how the CSIRT destroys information, records, media, devices, etc. to ensure that information is protected when its life cycle or the media containing it comes to an end.

Information Disclosure Policy

This policy should specify how and when the CSIRT may share or distribute information internally or externally.

Policy on Access to Information

This policy establishes who can access CSIRT information, taking into account CSIRT staff, members of the target community, or personnel from the CSIRT's parent organization (if it has one).

Appropriate Use of CSIRT Systems Policy

This policy defines the acceptable use of CSIRT equipment and resources, specifically how, when and for what facilities and equipment can be used.

Definition of Security Incidents and Events Policy

This policy outlines the criteria that determine the definition of a security event or incident and the classification of each by type and severity.

Incident Management Policy

This policy should define how incident management occurs, including the type of incidents the CSIRT will answer, acceptable response times, procedures to be applied, etc.

Cooperation Policy

This policy defines what other entities the CSIRT will cooperate with and how it will do so, particularly other incident response teams.

Other Policies

In addition to the minimum policies required for a CSIRT, there may be others in order to improve the quality of services and the operation of the Center:

- Internet Use Policy
- Incident Reporting Policy
- CSIRT Communication Policy
- Training and Education Policy
- Personal Computer Security Policy
- Computer Network Security Policy
- Email Use policy
- Mobile Device Use Policy
- Telecommunications Equipment Security Policy
- Backup Policy
- Segregation of Roles Policy
- Change Management Policy
- Password Policy

The annexes contain more policy examples.

3 CLOSURE

Formal Closure occurs when all the information generated in the CSIRT establishment process, including its completeness, is analyzed and verified. After the closure process is complete, the National CSIRT will be formally established.

Upon closing the establishment process, the CSIRT Project Manager will have:

- A list of stakeholders
- Statements of establishment of the CSIRT (Mission, Vision, services, etc.)
- Legal documents for the creation of CSIRT
- Physical facilities, leases, etc.
- Hired and trained human resources
- Operations Manual with policies and procedures
- Technological infrastructure and respective support contracts

In addition, other documents are drafted during the establishment phase, including definition of scope, timeline and budget. The project team should be convened for a debriefing session to discuss lessons learned and where the process might be improved upon.

Finally, with all the information generated, it is essential to make a closing report containing:

- The overall objective of the project
- Activities performed
- Performance of the project (scope, timeline, budget)
- Lessons learned
- Future Recommendations

This report will be attached to the project documentation and it will give formal closure to the project.

Formal Completion of Activities

During planning, the Project Team establishes clear steps to be completed during project implementation. Each of these has a clear indicator of completion, such as "Trained Human Resources." To record the activity as formally completed, the project team must verify that all necessary staff received the training and then collect appropriate documentation. Similarly, all contracts and service agreements must be verified and have legal approval and necessary documentation.

Finally, the closing report should be approved by the project sponsor in order to complete the implementation phase of the CSIRT.

ANNEXES

Sample Acceptable Use Policy

OBJECTIVE

The purpose of this policy is to establish acceptable and unacceptable uses of the electronic devices and network resources that belong to CSIRT-XX. It has been drafted to conform with established legal, and ethical norms, and relies on trust, integrity, and transparency of the activities of the CSIRT.

CSIRT-XX operates computing devices, networks and other information systems in order to carry out its mandates, objectives and initiatives. All such devices must be managed responsibly to maintain the confidentiality, integrity and availability of information assets that CSIRT-XX has in its possession or works with.

This policy requires users of the devices and network resources to accept and comply with the policies defined, so as to protect CSIRT-XX, its personnel, its operations, and its partners, from damage and lawsuits.

SCOPE

All employees, contractors, consultants, interns and others who work directly or indirectly in CSIRT-XX, including all personnel affiliated with third parties, must comply with this policy. This policy applies to information assets that are owned or leased by CSIRT-XX, or to devices that connect to CSIRT-XX's network or that are hosted on a site belonging to CSIRT-XX.

In extenuating circumstances, exceptions may be approved by CSIRT-XX management that would contravene this policy. Any exceptions must be formally approved in writing and include a justification and evaluation of possible risks of such an exception.

STATEMENT OF POLICY

General Requirements

As an employee of CSIRT-XX, you are responsible for exercising good judgment regarding the appropriate use of CSIRT-XX resources in accordance with the policies and procedures established by the CSIRT-XX. CSIRT-XX resources may not be used for illegal purposes or that are in violation of CSIRT-XX's Ethics Policy.

System Accounts

You are responsible for the security of the data, accounts and systems under your control. Keep secure passwords and do not share your account information or password with anyone, including other staff members, relatives or friends. Facilitating access to another person, whether intentionally or due to failure to ensure access is a violation of this policy. You must maintain a level of user and system passwords according to the Password Policies.

You must ensure, through legal or technological means, that the information with which you work remains under the control and management of CSIRT-XX at all times. Storage, access, or use of confidential information in environments or applications run by a third party or not directly operated or controlled by CSIRT-XX is prohibited. This includes devices that are maintained by third parties with which there is no contractual agreement in place. This specifically prohibits the use of an email account that has not been provided by the CSIRTxx to exchange information owned by the CSIRTxx.

Computer assets

You are responsible for ensuring the protection of the assets you were assigned by CSIRT-XX. This includes the use of computer lock cables and any other security devices. Laptops that are left overnight at the CSIRT-XX should be placed in a locked drawer or a cabinet. Any theft or loss of equipment must be reported to CSIRT-XX management immediately.

All personal workstations and devices must be secured with a password protected screen saver, and you must lock the screen or log out when the workstation or device is unattended. Moreover, the the autolock function should be activated as set in the workstation setup procedure. Any devices you connect to the CSIRT-XX network must meet the Minimum Access Policy.

Internet and Electronic Communications Use

You are responsible for the security and proper use of network resources and tools under your control. It is strictly prohibited to use resources in such a manner that they:

- Cause a security breach or violation in one or more CSIRT-XX network resources;
- Cause a service interruption to one or more CSIRT-XX network resources;
- Violate the provisions of copyright law;
- Violate established security policies of local laws;
- Support any illegal activity, including by transmitting or aiding in the transmission of material that violates policies that protect confidential or proprietary information; and
- Misrepresent, obfuscate, delete or replace a user identity in any electronic communication in order to mislead the recipient about who the sender is.

Finally, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the views of CSIRT-XX to the public.

APPLICATION

An employee found in violation of this policy or any other CSIRT-XX policies is subject to disciplinary action, possibly including termination of employment. A violation of this policy by a temporary employee, contractor or supplier may result in termination of the contract or assignment with CSIRT-XX.

Disclosure Policy

OBJECTIVE

Define how and what information can be disclosed to whom and under what circumstances, including stakeholders, partner CSIRTs, other government bodies, or even other members of CSIRT-XX. The way information is shared will be done according to its level of classification.

SCOPE

All information held or generated by CSIRT-XX.

STATEMENT OF POLICY

Public Information

Disclosure of public information is authorized, though it must be disseminated through channels established and managed by the communications or public affairs unit of CSIRT-XX, and done in accordance with that unit's procedures.

Classified Information

Classified information may only be disclosed when authorized by the Director of CSIRT-XX or his or her designee. In all cases, a non-disclosure agreement shall be signed which holds that any recipient of classified information be duly notified of the classification of the information they are receiving.

Classified Information for Community Use

Information that is classified but still approved for dissemination within the community is a special kind of information. All considerations previously mentioned still apply, except that disclosure to certain members of the target community will be authorized by the Director of CSIRT-XX.

Confidential information

CSIRT-XX and its personnel will not disclose confidential information. If for operational reasons it becomes necessary to share confidential information with third parties, you shall seek the consent of the owner of the information, who may authorize disclosure or not. If the owner authorizes it, the recipient shall be required to sign a non-disclosure agreement either provided by the owner of the information or the CSIRT.

Secret information

Under no circumstances will CSIRT-XX disclose secret information by law.

Incomplete/Unfinished Information

Information that is in a state of preparation that does not contain sensitive information may be disclosed individually following the guidelines defined for this purpose.

INTERNAL DISCLOSURE

Within the CSIRT-XX team there shall be no limitations on information disclosure and sharing, unless made at the express request of the Director in regards to a specific action. As part of daily operational requirements, the CSIRT-XX will disclose certain information to the members of the organization. Any disclosure should take into account established procedures according to classification of information in question; disclosure of sensitive information must be authorized by the Director of CSIRT-XX or his or her designee.

LEGAL ASPECTS

CSIRT-XX will comply with all national legislation or organizational policy in responding to all third party requests for information. Such requests for information should be made through CSIRT-XX's legal department of advisor.

ORDERING INFORMATION

Incident Response Groups

Cooperation and information sharing with other incident response groups is vital to the operation and survival of CSIRT-XX and the greater national and international community of computer security incident response teams. As much information as possible will be shared with other response groups, in accordance with this policy, evaluating each case individually and with the permission of the Director of CSIRT-XX or his or her designee.

Press

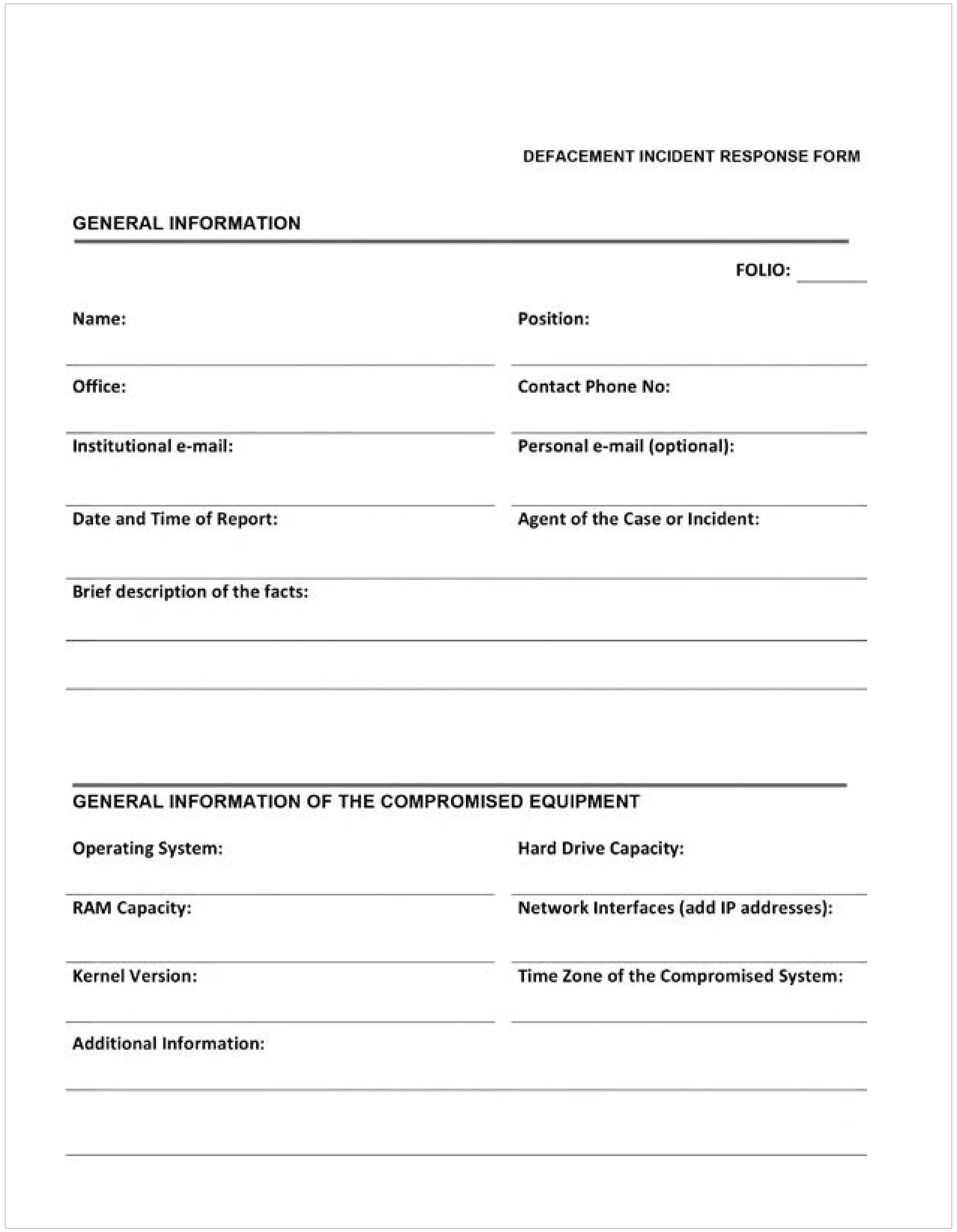
Communication and liaison with the press will be coordinated and performed solely by the designated spokesperson of CSIRT-XX, with prior approval of the Director of CSIRT-XX or his or her designee. When contacted by any representative of the press, all members of CSIRT-XX will refer requests to the spokesperson, indicating that they are not authorized to disclose information and will not disclose any information under any circumstances regardless of the classification of the information involved.

MEDIA RELEASE OF SENSITIVE INFORMATION

When necessary, sensitive information shall be disclosed in such a way so as to prevent access to it by an unauthorized third party.

Incident Response Forms

1 Defacement Incident Response Form



DEFACEMENT INCIDENT RESPONSE FORM

GENERAL INFORMATION

FOLIO: ______

Name:

Position:

Office:

Contact Phone No:

Institutional e-mail:

Personal e-mail (optional):

Date and Time of Report:

Agent of the Case or Incident:

Brief description of the facts:

GENERAL INFORMATION OF THE COMPROMISED EQUIPMENT

Operating System:

Hard Drive Capacity:

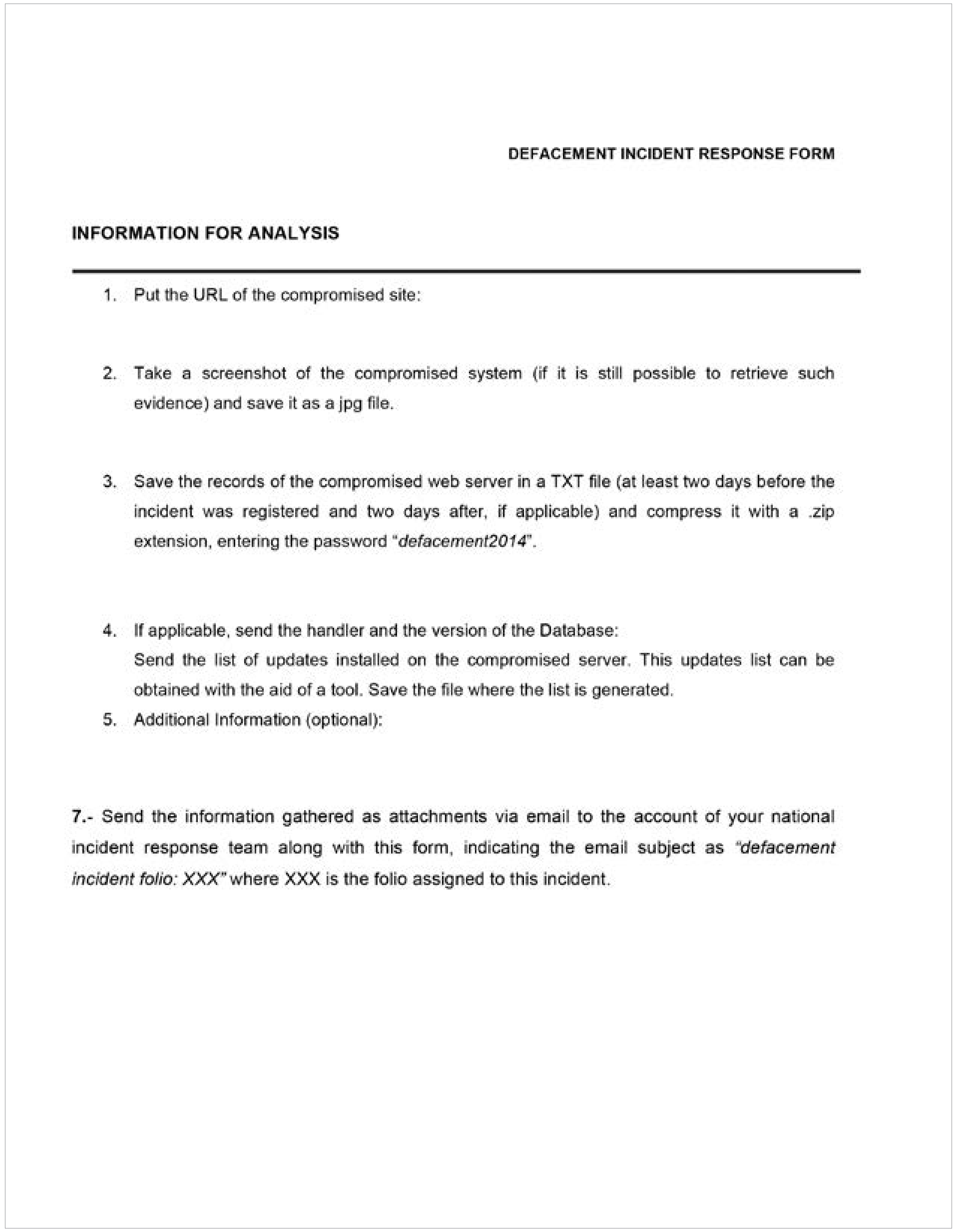
RAM Capacity:

Network Interfaces (add IP addresses):

Kernel Version:

Time Zone of the Compromised System:

Additional Information:



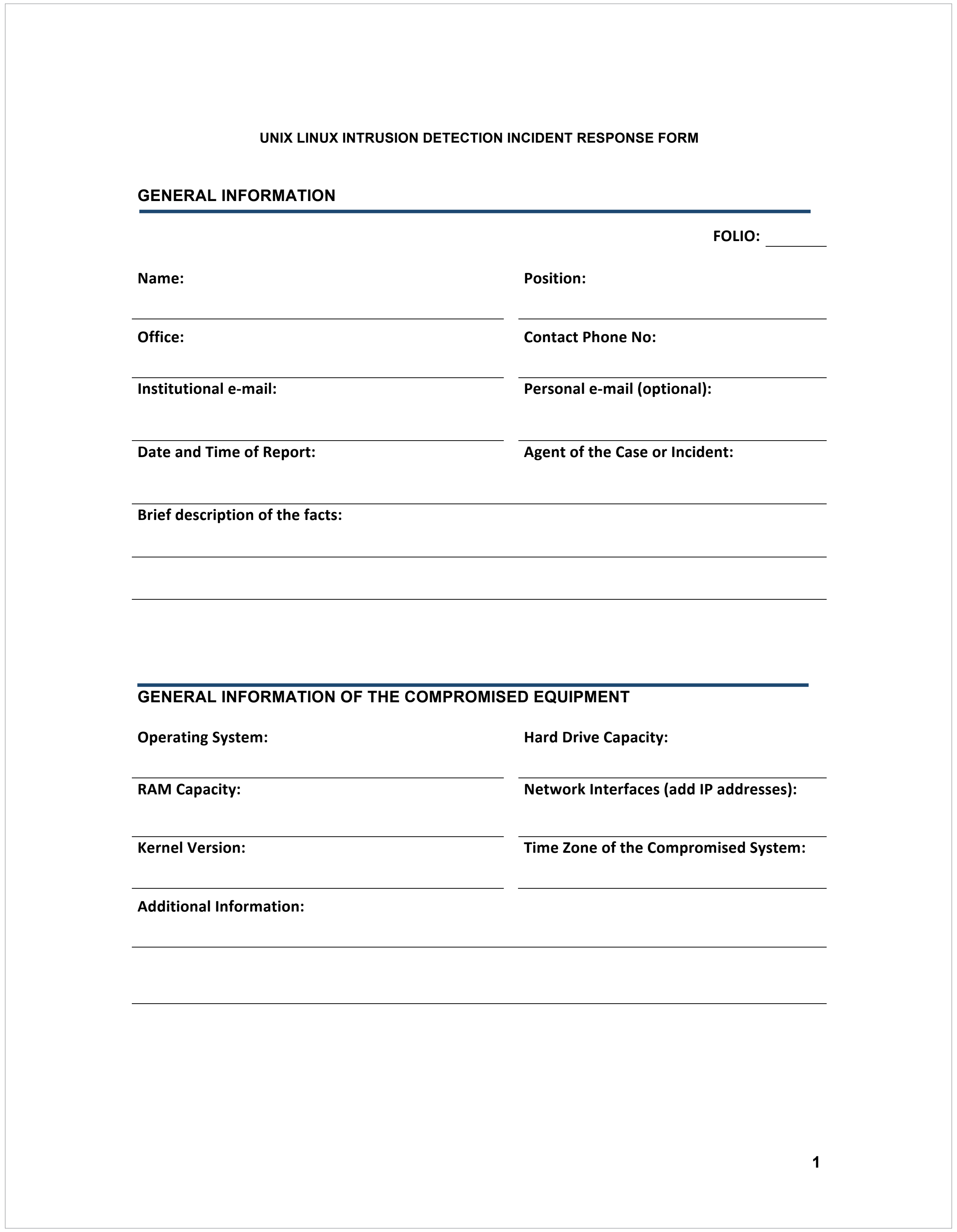
DEFACEMENT INCIDENT RESPONSE FORM

INFORMATION FOR ANALYSIS

1. Put the URL of the compromised site:
2. Take a screenshot of the compromised system (if it is still possible to retrieve such evidence) and save it as a jpg file.
3. Save the records of the compromised web server in a TXT file (at least two days before the incident was registered and two days after, if applicable) and compress it with a .zip extension, entering the password "*defacement2014*".
4. If applicable, send the handler and the version of the Database:
   Send the list of updates installed on the compromised server. This updates list can be obtained with the aid of a tool. Save the file where the list is generated.
5. Additional Information (optional):

7.- Send the information gathered as attachments via email to the account of your national incident response team along with this form, indicating the email subject as *"defacement incident folio: XXX"* where XXX is the folio assigned to this incident.

2 Unit Linux Intrusion Detection Incident Response Form



UNIX LINUX INTRUSION DETECTION INCIDENT RESPONSE FORM

GENERAL INFORMATION

FOLIO: ______

Name:

Position:

Office:

Contact Phone No:

Institutional e-mail:

Personal e-mail (optional):

Date and Time of Report:

Agent of the Case or Incident:

Brief description of the facts:

GENERAL INFORMATION OF THE COMPROMISED EQUIPMENT

Operating System:

Hard Drive Capacity:

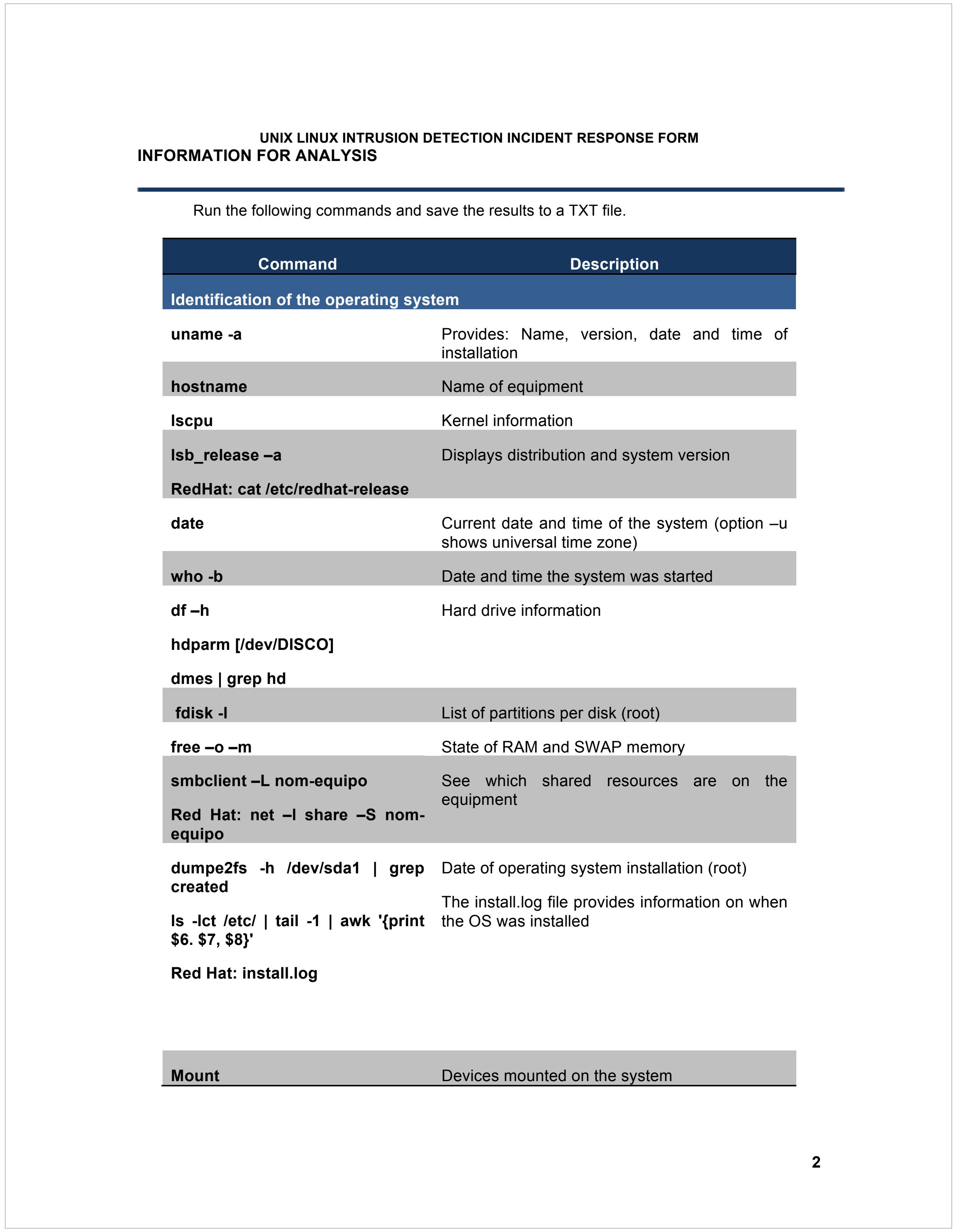
RAM Capacity:

Network Interfaces (add IP addresses):

Kernel Version:

Time Zone of the Compromised System:

Additional Information:

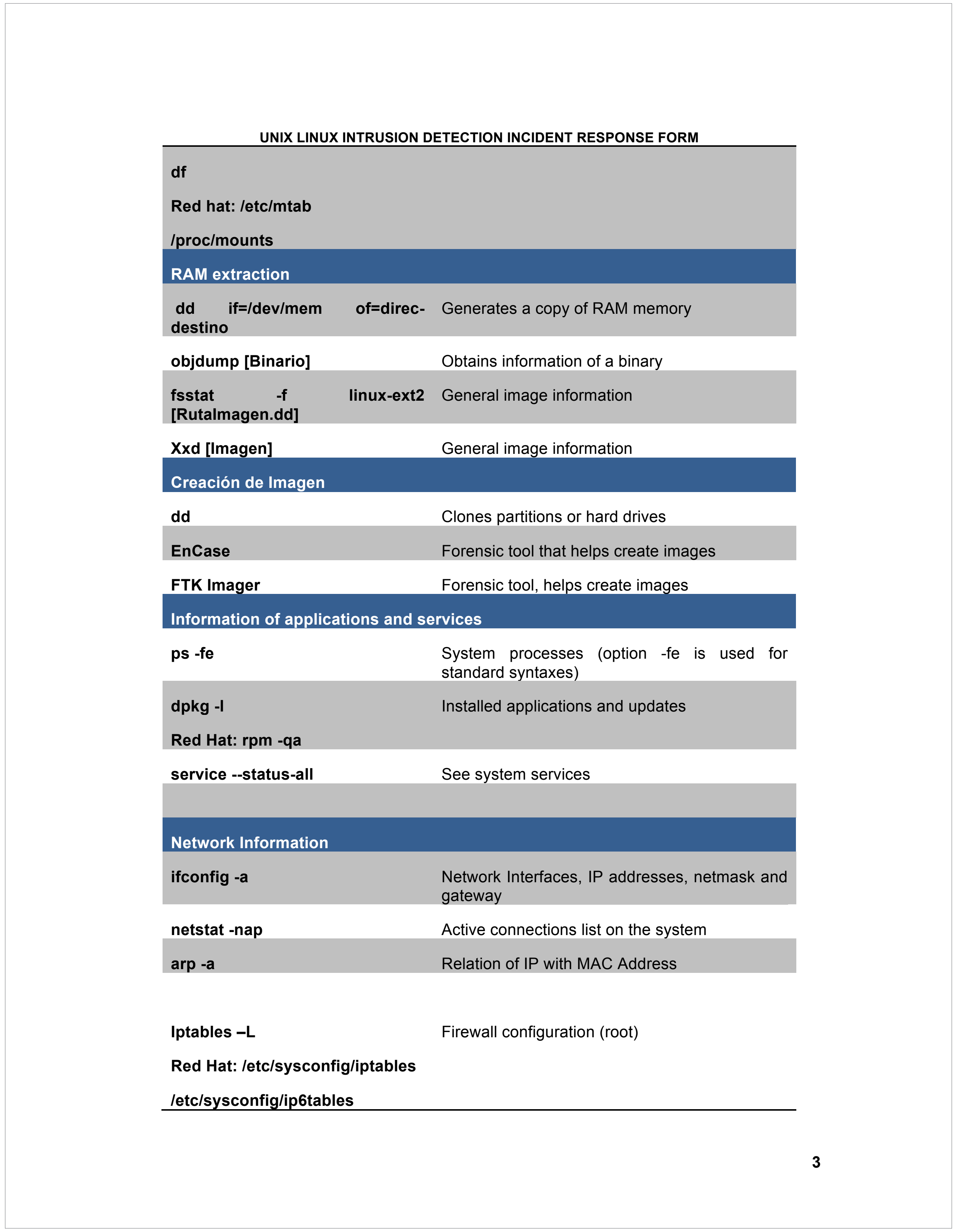


UNIX LINUX INTRUSION DETECTION INCIDENT RESPONSE FORM

INFORMATION FOR ANALYSIS

Run the following commands and save the results to a TXT file.

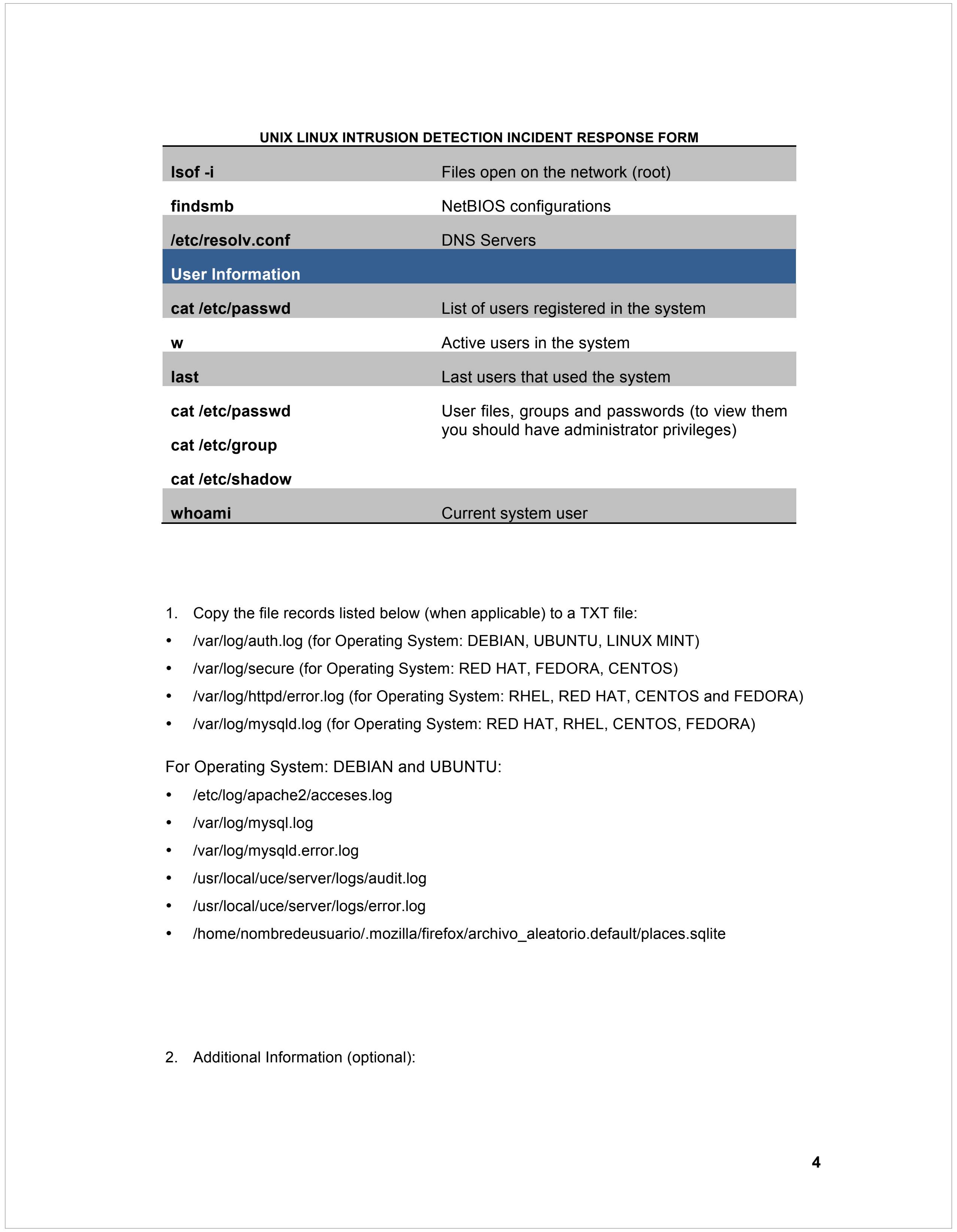
Command	Description
Identification of the operating system	
uname -a	Provides: Name, version, date and time of installation
hostname	Name of equipment
lscpu	Kernel information
lsb_release –a **RedHat: cat /etc/redhat-release**	Displays distribution and system version
date	Current date and time of the system (option –u shows universal time zone)
who -b	Date and time the system was started
df –h **hdparm [/dev/DISCO]** **dmes | grep hd**	Hard drive information
fdisk -l	List of partitions per disk (root)
free –o –m	State of RAM and SWAP memory
smbclient –L nom-equipo **Red Hat: net –l share –S nom-equipo**	See which shared resources are on the equipment
dumpe2fs -h /dev/sda1 | grep created **ls -lct /etc/ | tail -1 | awk '{print $6. $7, $8}'** **Red Hat: install.log**	Date of operating system installation (root) The install.log file provides information on when the OS was installed
Mount	Devices mounted on the system



UNIX LINUX INTRUSION DETECTION INCIDENT RESPONSE FORM

df **Red hat: /etc/mtab** **/proc/mounts**	
RAM extraction	
dd if=/dev/mem of=direc-destino	Generates a copy of RAM memory
objdump [Binario]	Obtains information of a binary
fsstat -f linux-ext2 [RutaImagen.dd]	General image information
Xxd [Imagen]	General image information
Creación de Imagen	
dd	Clones partitions or hard drives
EnCase	Forensic tool that helps create images
FTK Imager	Forensic tool, helps create images
Information of applications and services	
ps -fe	System processes (option -fe is used for standard syntaxes)
dpkg -l **Red Hat: rpm -qa**	Installed applications and updates
service --status-all	See system services
Network Information	
ifconfig -a	Network Interfaces, IP addresses, netmask and gateway
netstat -nap	Active connections list on the system
arp -a	Relation of IP with MAC Address
Iptables –L **Red Hat: /etc/sysconfig/iptables** **/etc/sysconfig/ip6tables**	Firewall configuration (root)

3



UNIX LINUX INTRUSION DETECTION INCIDENT RESPONSE FORM

lsof -i	Files open on the network (root)
findsmb	NetBIOS configurations
/etc/resolv.conf	DNS Servers
User Information	
cat /etc/passwd	List of users registered in the system
w	Active users in the system
last	Last users that used the system
cat /etc/passwd **cat /etc/group** **cat /etc/shadow**	User files, groups and passwords (to view them you should have administrator privileges)
whoami	Current system user

1. Copy the file records listed below (when applicable) to a TXT file:

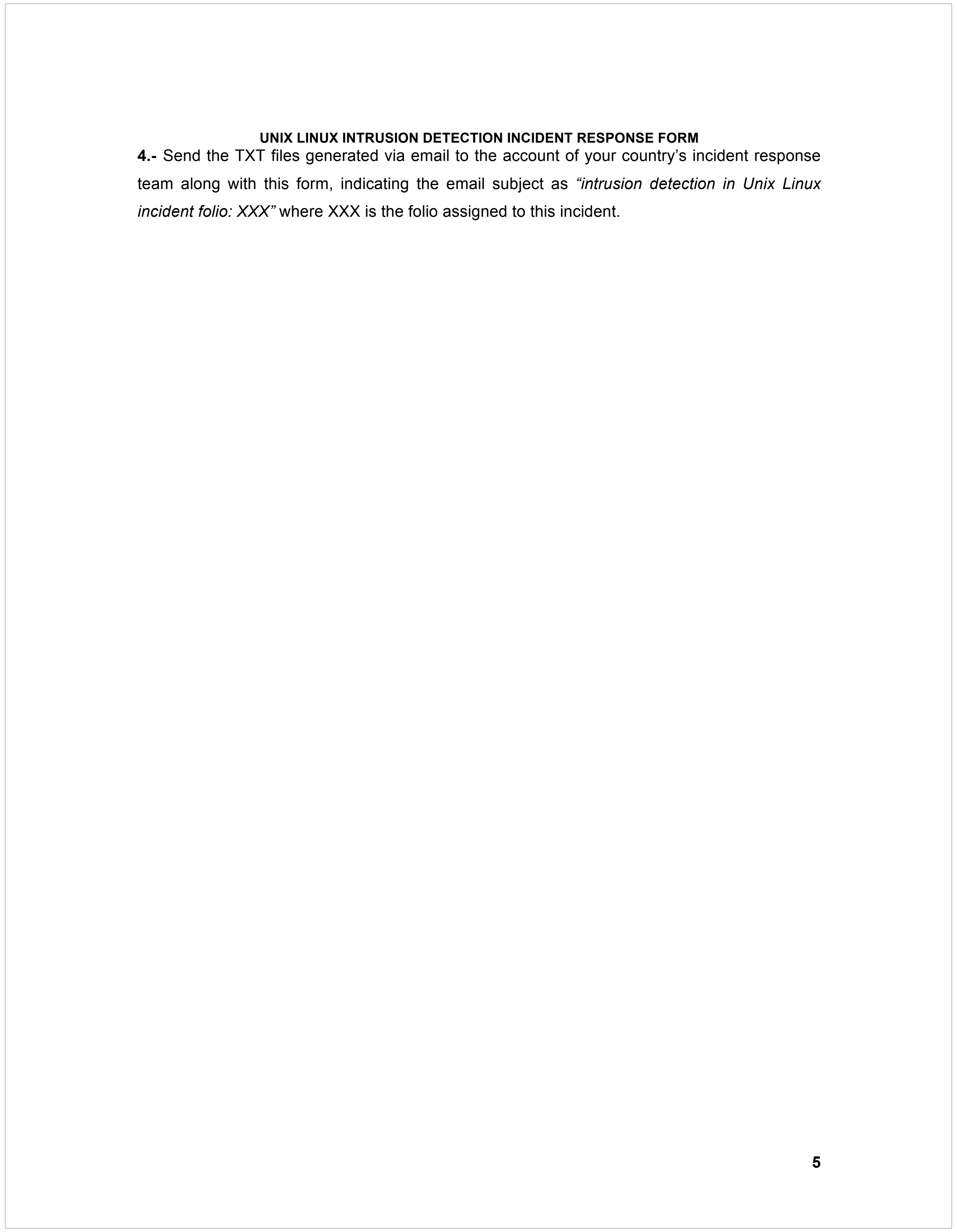
- /var/log/auth.log (for Operating System: DEBIAN, UBUNTU, LINUX MINT)
- /var/log/secure (for Operating System: RED HAT, FEDORA, CENTOS)
- /var/log/httpd/error.log (for Operating System: RHEL, RED HAT, CENTOS and FEDORA)
- /var/log/mysqld.log (for Operating System: RED HAT, RHEL, CENTOS, FEDORA)

For Operating System: DEBIAN and UBUNTU:

- /etc/log/apache2/acceses.log
- /var/log/mysql.log
- /var/log/mysqld.error.log
- /usr/local/uce/server/logs/audit.log
- /usr/local/uce/server/logs/error.log
- /home/nombredeusuario/.mozilla/firefox/archivo_aleatorio.default/places.sqlite

2. Additional Information (optional):

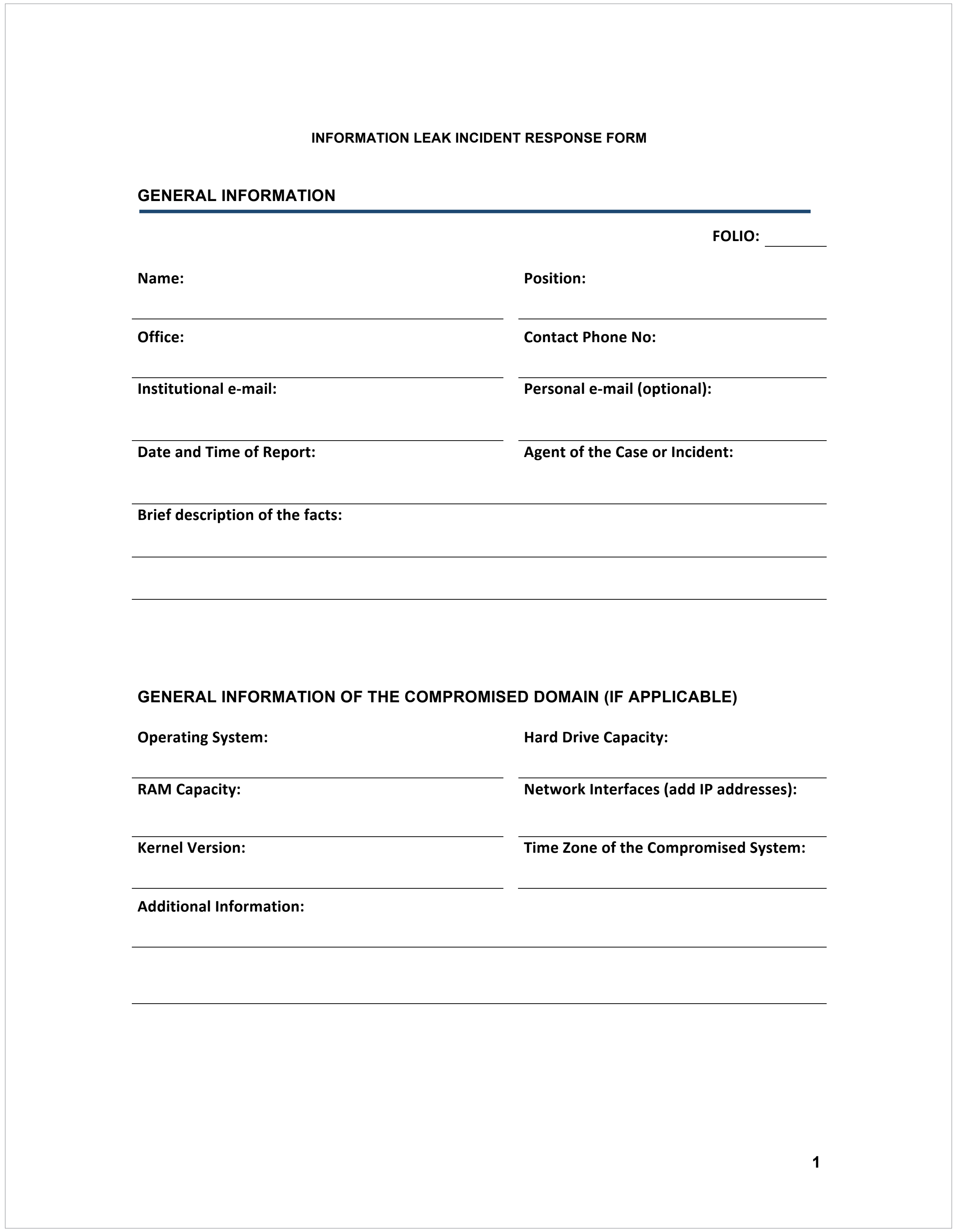
4



UNIX LINUX INTRUSION DETECTION INCIDENT RESPONSE FORM

4.- Send the TXT files generated via email to the account of your country's incident response team along with this form, indicating the email subject as *"intrusion detection in Unix Linux incident folio: XXX"* where XXX is the folio assigned to this incident.

3 Information Leak Incident Response Form



INFORMATION LEAK INCIDENT RESPONSE FORM

GENERAL INFORMATION

FOLIO: ______

Name:

Position:

Office:

Contact Phone No:

Institutional e-mail:

Personal e-mail (optional):

Date and Time of Report:

Agent of the Case or Incident:

Brief description of the facts:

GENERAL INFORMATION OF THE COMPROMISED DOMAIN (IF APPLICABLE)

Operating System:

Hard Drive Capacity:

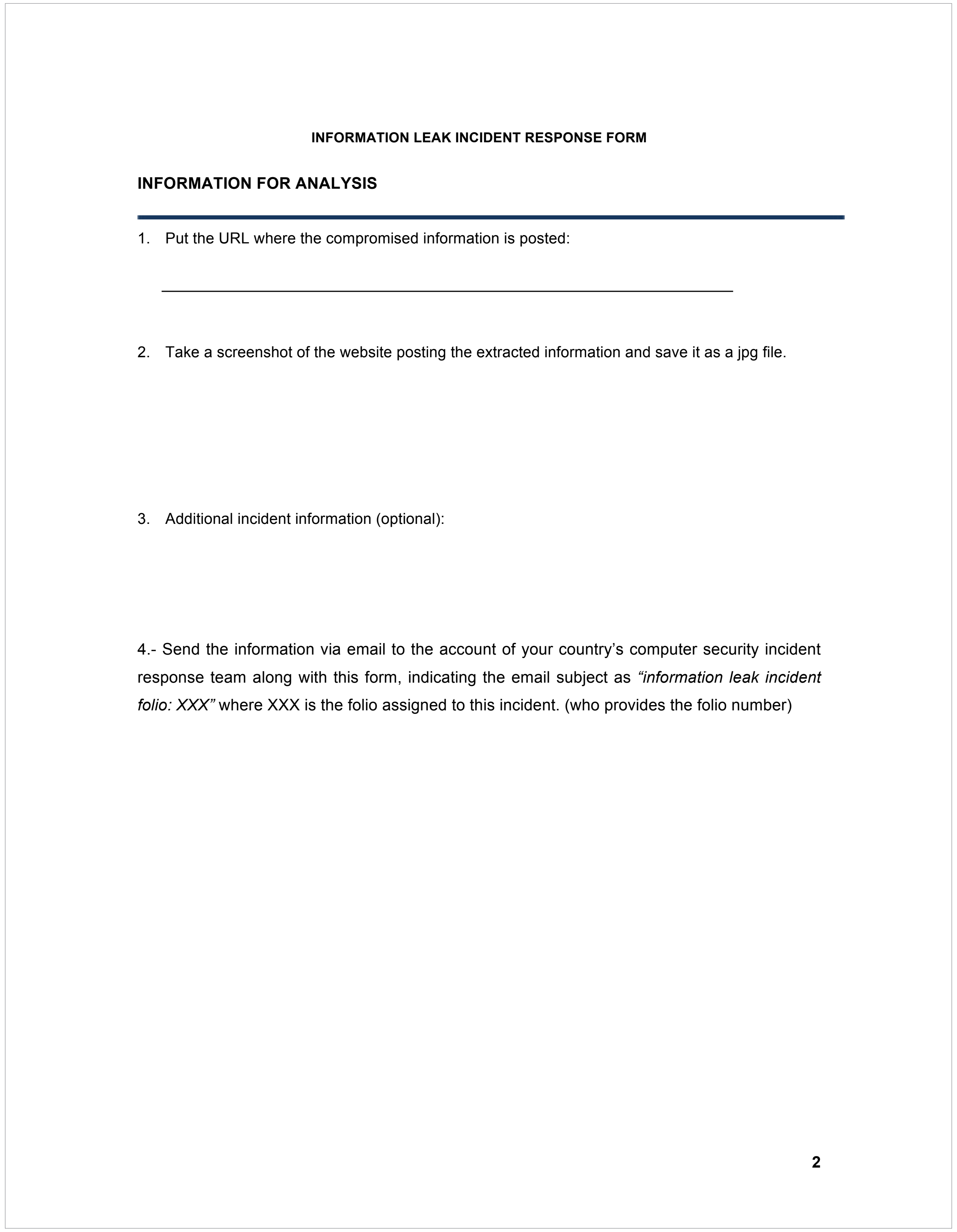
RAM Capacity:

Network Interfaces (add IP addresses):

Kernel Version:

Time Zone of the Compromised System:

Additional Information:



INFORMATION LEAK INCIDENT RESPONSE FORM

INFORMATION FOR ANALYSIS

1. Put the URL where the compromised information is posted:

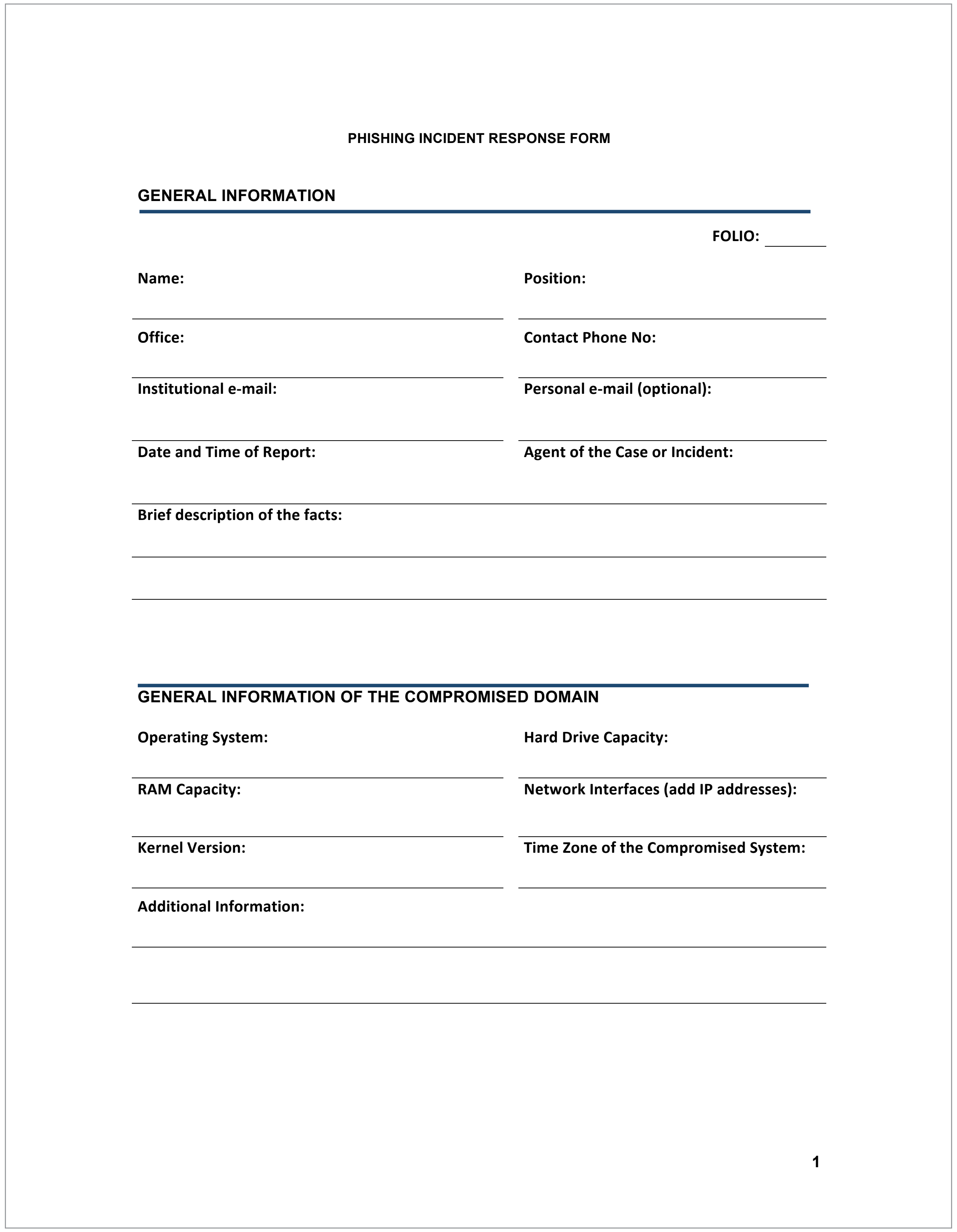
   ____

2. Take a screenshot of the website posting the extracted information and save it as a jpg file.

3. Additional incident information (optional):

4.- Send the information via email to the account of your country's computer security incident response team along with this form, indicating the email subject as *"information leak incident folio: XXX"* where XXX is the folio assigned to this incident. (who provides the folio number)

4 Phishing Incident Response Form



PHISHING INCIDENT RESPONSE FORM

GENERAL INFORMATION

FOLIO: ________

Name:	**Position:**
Office:	**Contact Phone No:**
Institutional e-mail:	**Personal e-mail (optional):**
Date and Time of Report:	**Agent of the Case or Incident:**

Brief description of the facts:

____

____

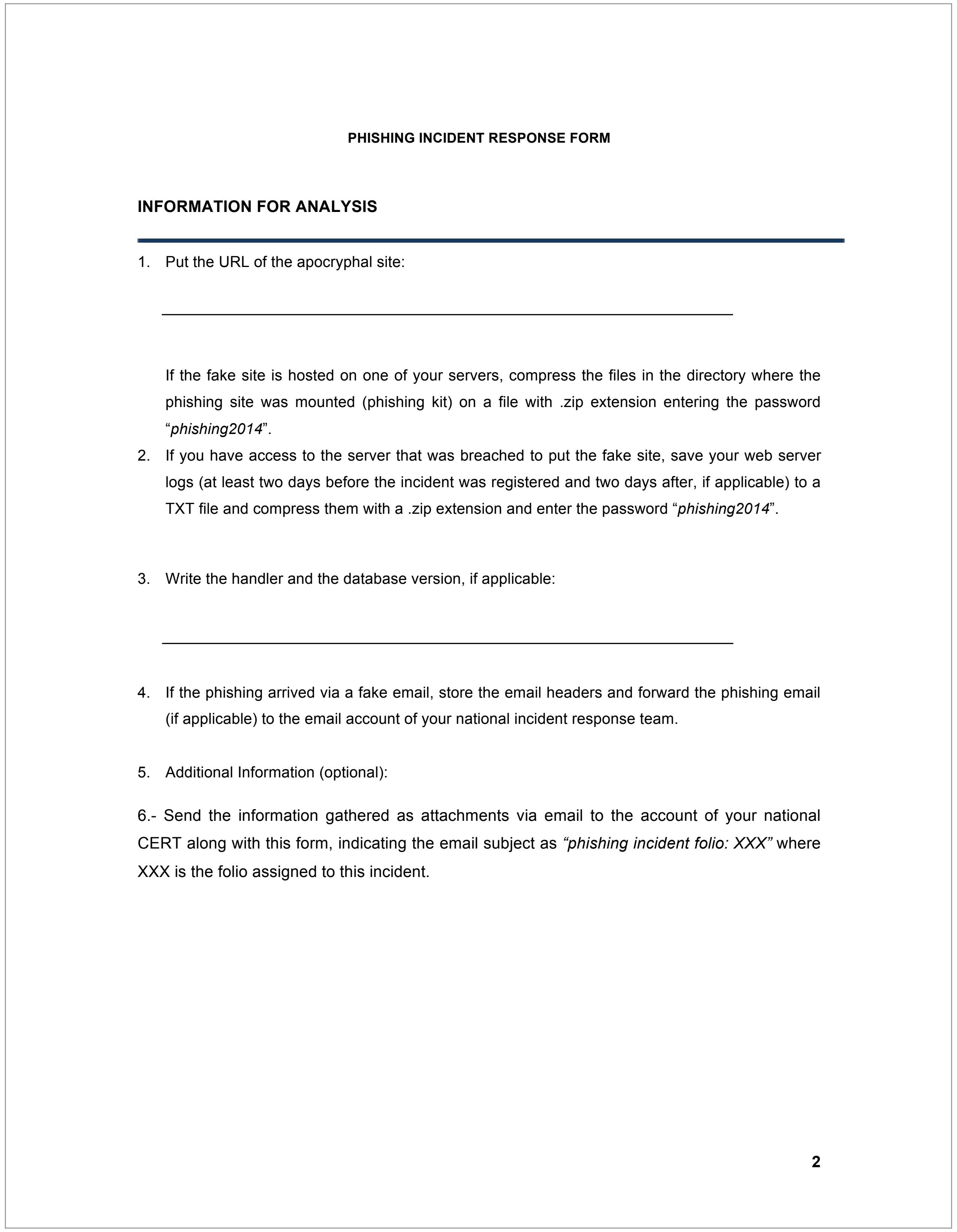
GENERAL INFORMATION OF THE COMPROMISED DOMAIN

Operating System:	**Hard Drive Capacity:**
RAM Capacity:	**Network Interfaces (add IP addresses):**
Kernel Version:	**Time Zone of the Compromised System:**

Additional Information:

____

____



PHISHING INCIDENT RESPONSE FORM

INFORMATION FOR ANALYSIS

1. Put the URL of the apocryphal site:

____

If the fake site is hosted on one of your servers, compress the files in the directory where the phishing site was mounted (phishing kit) on a file with .zip extension entering the password "*phishing2014*".

2. If you have access to the server that was breached to put the fake site, save your web server logs (at least two days before the incident was registered and two days after, if applicable) to a TXT file and compress them with a .zip extension and enter the password "*phishing2014*".

3. Write the handler and the database version, if applicable:

____

4. If the phishing arrived via a fake email, store the email headers and forward the phishing email (if applicable) to the email account of your national incident response team.

5. Additional Information (optional):

6.- Send the information gathered as attachments via email to the account of your national CERT along with this form, indicating the email subject as *"phishing incident folio: XXX"* where XXX is the folio assigned to this incident.

2

References

1. Centro Criptológico Nacional: Guía de Creación de un CERT/CSIRT (CCN-STIC-810): España, 2011

2. CERT Program at the Software Engineering Institute: FIRST Site Visit Requirements and Assessment: Estados Unidos, Carnegie Mellon University, 2013

3. CERT Program at the Software Engineering Institute CMU: Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability: Estados Unidos, Carnegie Mellon, 2011

4. CERT/CC: CMU Creating and Managing CSIRTs: Estados Unidos, Carnegie Mellon, 2004.

5. Charles W. L. HILL y Gareth R. JONES: Administración estratégica. Un enfoque integrado. Santa Fé de Bogotá: McGraw – Hill Interamericana S.A, 1996

6. ENISA: Good Practice Guide for Incident Management: Unión Europea, ENISA, 2010.

7. ENISA: Baseline Capabilities of National/Governmental CERTs: Unión Europea, ENISA, 2012

8. Georgia Killcrece et al: Organizational Models for Computer Security Incident Response Teams (CSIRTs. Estados Unidos, Carnegie Mellon, 2003

9. Jack Fleitman: Negocios Exitosos: México, Interamericana McGraw Hill, 2000

10. Moira J. West-Brown, et al: Handbook for Computer Security Incident Response Team: Estados Unidos, Carnegie Mellon, 2003.

11. Orión Aramayo: Manual de Plaificación Estratégia: Chile, Ude chile, 2009

12. Ruben Aquino Luna et al: Manual de gestión de incidentes de seguridad informática. AMPARO y LACNIC.

End Notes

1. Guide to Creating a CERT/CSIRT (CCN-STIC-810) of the National Cryptologic Centre, Spain

2. Guide to Good Practice in Incident Management (2010) http://www.enisa.europa.eu/act/cert/support/incident-management/files/good-practice-guide-for-incident-management

3. Baseline Capabilities of National/Governmental CERTs: European Union, ENISA, 2012

4. Guide to Creating a CERT/CSIRT (CCN-STIC-810) of the National Cryptologic Centre of Spain

5. CERT Program at the Software Engineering Institute CMU: Best Practices for National Cyber Security

6. John M. Bryson, in his article "Stakeholder Identification and Analysis Techniques

7. Handbook for Computer Security Incident Response Team Carnegie Mellon University

8. Administración estratégica. Un enfoque integrado. Santa Fé de Bogotá: McGraw – Hill Interamericana S.A.

9. Handbook for Computer Security Incident Response Team: Estados Unidos, Carnegie Mellon, 2003.

10. Negocios Exitosos: México, Interamericana McGraw Hill, 2000

11. Orión Aramayo, Manual de Planificación Estratégia, U de chile

12. Handbook for Computer Security Incident Response Team: Estados Unidos, Carnegie Mellon, 2003.

13. Add footnote to the national cryptologic center in spain

14. Handbook for Computer Security Incident Response Team: Estados Unidos, Carnegie Mellon, 2003

15. Organizational Models for Computer Security Incident Response Teams (CSIRTs. USA, Carnegie Mellon, 2003

16. Manual de gestión de incidentes de seguridad informática. AMPARO y LACNIC

17. Manual de gestión de incidentes de seguridad informática. AMPARO y LACNIC

18. http://www.enisa.europa.eu/activities/cert/support/guide2/internal-management/structure

19. CMU Creating and Managing CSIRTs: USA, Carnegie Mellon, 2004.

20. PMBOK project management institute

Secretary General
Luis Almagro Lemes

Assistant Secretary General
Nestor Mendez

BEST PRACTICES
FOR ESTABLISHING A NATIONAL CSIRT

Executive Secretary of the Inter-American Committee against Terrorism
Alfred Schandlbauer

Developed by
Ignacio Lagomarsino
Santiago Paz

Project Coordination
Diego Subero
Belisario Contreras

Editors
Pablo Martinez
Kerry-Ann Barrett
Robert Fain
Barbara Marchiori
Geraldine Vivanco

Contributors
Brian Dito
Yezyd Donoso
Luis Fuentes
Gonzalo Garcia-Belenguer
José María Gómez de la Torre
Catalina Lillo
Raul Millan
Emmanuelle Pelletier
Francisco Javier Villa

U.S. Department of Homeland Security
Mexico Federal Police

Organization of
American States

More rights for more people