PRACTICAL GUIDE FOR CSIRTs

Volume 2, 2023

A Sustainable Business Model

OAS More rights for more people

CSIRTAmericas Network

START

SMALL AND GROW

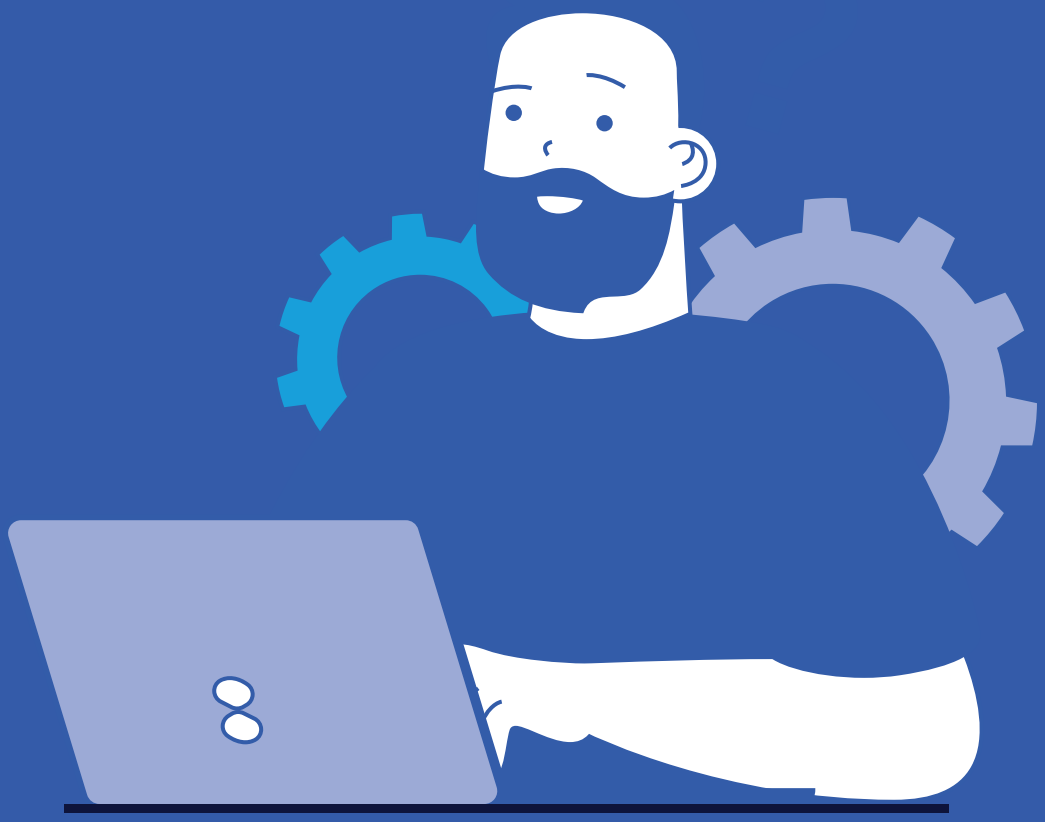
”

PRACTICAL GUIDE FOR CSIRTs

Volume 2, 2023

A Sustainable Business Model

Table of Contents



0. HOW TO USE THIS GUIDE

This guide is based on the previous document, Best Practices for Establishing a National CSIRT[1], developed by the Organization of American States (OAS) in 2016, which covers topics on planning and implementing a Computer Security Incident Response Team (CSIRT), including its organization, human resources, training, and infrastructure aspects, among others. This second edition is intended to build upon the previous and serve as a directional guide for project leaders, decision makers, and anyone interested in creating, developing, modernizing, or sustaining a strategically focused CSIRT.

The guide is limited to CSIRTs in the public sphere, with a special focus on Latin America and the Caribbean, and is based on more than 15 years' experience, paired with the OAS's knowledge on the topic, as well as real statistical data obtained from the CSIRTAmericas Network[2] of the Inter-American Committee Against Terrorism of the Organization of American States (CICTE/OAS, for their acronyms in Spanish). Additionally, it takes advice and experiences from regional and international facilitators who were interviewed and cited for purely educational purposes in the preparation of this document.

This guide presents general recommendations, so it is important to understand that when evaluating best practices, it is essential to contextualize the space, time, and resources available to each situation. Each country has a different political structure, culture, geographical landscape, and legal framework. As such, this guide is not meant to serve as a static template, but rather as a resource adaptable to local conditions, as necessary.

[1] Best Practices for Establishing a National CSIRT, the Organization of American States, 2016. https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

[2] CSIRTAmericas is the network of governmental Computer Security Incident Response Teams (CSIRTs) from OAS Member States. More information: https://csirtamericas.org/

1. WHY IS A CSIRT NEEDED?

Just a few years ago, certain events – a region experiencing fuel shortages; a government agency having its information exposed; or a citizen facing online identity theft – could have been considered isolated and unrelated events. Today, given information systems' exponential progression, connectivity, complexity in hybrid technology, data sharing, and expanding business ecosystems, we know that there is a possible common factor on the scene: "cybersecurity incidents," the origin of the above and many other scenarios.

It is essential and necessary, then, for an organization to have the capability to detect, contain, mitigate, and thus, recover the provision of its services as soon as possible – or, in other words, to be capable to both prevent and respond to a cybersecurity incident.

We live in a digitized world where so-called critical infrastructures – distribution chains, transportation, communications, and essential services, such as electricity and water, to name a few – coexist in cyberspace and, therefore, require adequate protections. Therefore, we can say that cybersecurity vivisects and challenges all areas of our life, allowing for proper function and operations of governments, companies, and citizens.

As mentioned above, in an adverse scenario, it is necessary for each organization to prevent and respond to a cybersecurity incident. However, the reality is that many times, an organization does not have sufficient knowledge or experience to do so; thus, a Computer Security Incident Response Team (CSIRT) can mark the difference in launching a coordinated and efficient response to an attack, while helping mitigate its consequences.

In simple words, a CSIRT **provides cybersecurity services to prevent, detect, mitigate, and respond to cyber incidents in a defined community.** A CSIRT has an organizational structure that extends to established processes and a catalog of technological tools, in addition to a budget, mandates, a service catalog, specialized personnel, a network of contacts, a communications plan, and a legal framework that empowers it to act, among many other elements that create a baseline for managing cyber incidents within a defined community and develop methods for supporting said community to the greatest extent possible.

Both public organizations and private companies, as well as military entities, academia, and other organizations considered critical infrastructures face cyber incidents and yet, in many cases, have not established formal procedures to respond to incidents. Others lack clear guidance on how to address an incident. With this in mind, it is important to ask: Is a **CSIRT really necessary?**

That is a common question faced by decision-makers responsible for developing national policies, guidelines, and strategies, as well as by budget managers, project managers, industry leaders, private companies, law enforcement, and academia. Typically, the answer is neither linear nor simple, due to a lack of clarity regarding what a CSIRT can or should do; however, a country or sector with a CSIRT may:

- **Respond to an incident** based on standardized procedures and better response preparation.

- **Coordinate support** with technical collaborators from other national or international institutions, to resolve an incident.

• **Have a broader picture of current risks** in their sector or country.

• **Anticipate the onset of an incident,** based on threat intelligence strategies and early warning systems.

• **Alert a served community** regarding Indicators of Compromise (IoC), Indicators of Attack (IoA), or other vulnerabilities identified at either the national or international level.

• **Develop and coordinate cyber incident response operations** that require action from other areas or organizations, for training and preparation purposes.

• **Support citizen culture and education** regarding cybersecurity issues.

• **Serve as a benchmark for building** sectoral or national cybersecurity strategies.

• **Detect and promote cybersecurity talent** in the educational sector, communities, or a country.

• **Establish strategies** that align prevention, detection, and response capabilities to manage, mitigate, and overcome cyberattacks.

• **Promote development of a national-level cybersecurity ecosystem,** via the creation and consumption of services provided to and from the public, private, and academic sectors.

• **Serve as a coordinating entity for countrywide national cybersecurity,** based on a legal framework that respects human rights.

Given the importance of a CSIRT and its scope, in this guide we will present – based on testimonials from cybersecurity specialists who have worked in CSIRTs throughout Latin America and the Caribbean – best practices for creating, operating, and sustaining a Computer Security Incident Response Team.

2. WHAT IS THE DIFFERENCE BETWEEN A *nCSIRT* AND A SECTORAL CSIRT?

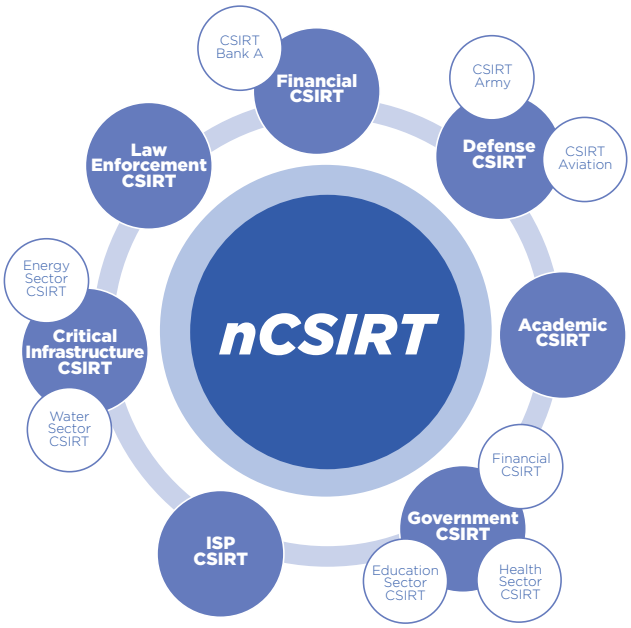
In Latin America and the Caribbean, today, we're witnessing an increase in CSIRTs in the military, government, health, and banking fields, among others. Importantly, although there are similarities, there are also differences between a ***nCSIRT* and a sectoral CSIRT.**

A *nCSIRT* acts as a single international and national point for coordinating a response to cyber incidents that affect a country. Its scope of competence extends to centralizing the situational analysis, establishing routine coordination actions, and, in crisis circumstances (for example, electoral or sporting events, social conflicts, or regional summits), providing technical recommendations, promoting cybersecurity legislative initiatives within a country, and creating and promoting a cybersecurity community and culture, as well as coordinating the response to cyber incidents under other circumstances – for example, with other sectoral CSIRTs and/or international organizations – as well as developing their cyber capabilities.

For its part, a sectoral CSIRT provides assistance in solving cyber incidents within specific communities, often via specialized technologies that require specific treatment. For example, the military sector often makes use of technologies classified as flight path systems or command controls for vessels that require a certain level of expertise in response to an incident. This situation is different when talking about a CSIRT belonging to a private sector company, as this unites organizations from the retail or financial sector, for example, where not only their technologies but also their interests are completely different. As mentioned in Chapter 0, for the purposes of this guide, we will focus on public-sector CSIRTs.

As shown in the image below (Image 1), a best practice in an ecosystem where both a *nCSIRT* and multiple sectoral CSIRTs coexist, is one in which there is a collaborative environment of continuous coordination and information exchange; this allows a national CSIRT access to a real and updated panorama on cybersecurity threats facing a country across its sectors, thus creating a national approach to cybersecurity, which then becomes part of Digital Governance. However, for this ideal scenario to occur, it is first necessary to establish the key elements compiled and described in this guide.

Image 1
Example of a Collaborative Structure for *nCSIRTs* and Sectoral CSIRTs



Source: Organization of American States, 2023.

3. OVERVIEW OF CSIRTs IN LATIN AMERICA AND THE CARIBBEAN

3.1 Where Are National CSIRTs Institutionally Located?

Given the increase in cyber incidents of national relevance in Latin American and Caribbean countries, as well as the need for governments to react to them, a CSIRT's role has been relevant since 2003 and has, thus, created the necessary conditions to develop and allocate the budgets necessary to create CSIRTs throughout the region; over time, this led to establishing not only national but also sectoral CSIRTs.

In some cases, CSIRTs were created through a National Cybersecurity Strategy and in others, through bills of law, a government ministry, a presidentially issued decree, or public policy. Regardless of their origin, the emergence of *Computer Security Incident Response Teams* has empowered the region to address cyber incidents.

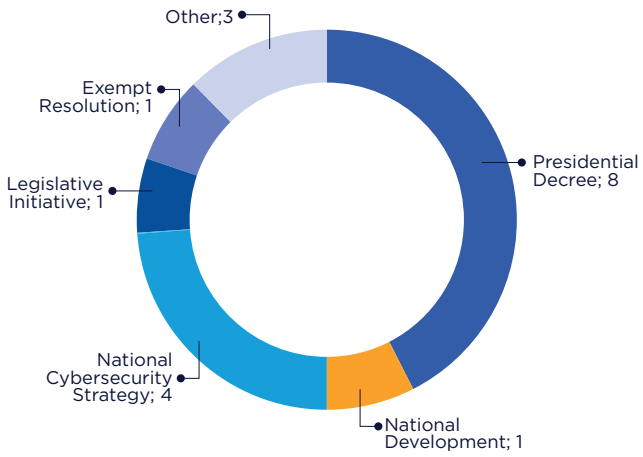
Creating a CSIRT requires a formalization process that typically depends on a mandate derived via government request. In Latin America and the Caribbean, mandates have been issued through, among others:

- Presidential Decree
- National Development Plan
- National Cybersecurity Strategy
- Legislative Initiative
- Exempt Resolution
- Ministerial Agreement

Chart 1 shows the regulatory procedure by which government CSIRTs – specifically, those in the OAS region and that are part of the *CSIRTAmericas Network*[3], – were constituted. Table 1 demonstrates that there is no defined standard for their location within government; it all depends on the country, mandate, economy, legal organizational structure, and political-sociocultural context in which a CSIRT operates.

Chart 1

Regulatory Procedure by Which a National CSIRT Was Created within the CSIRTAmericas Network



Source: Information from the CSIRTAmericas Network of the Organization of American States (OAS), 2023.

[3] CSIRTAmericas is a network of governmental Computer Security Incident Response Teams (CSIRTs) from OAS Member States. More information: https://csirtamericas.org/

Table 1

Institutional location of CSIRTs in the region
(Information based on official responses to a survey conducted by CSIRTAmericas Network)

COUNTRY	CSIRT	OFFICIAL NAME	ASSIGNED TO
Argentina	CERT.ar	National Information Technology Emergency Response Team - CERT.ar	Head of the Cabinet of Ministers (Office of the Presidency/State or Local Government)
Argentina	BA-CSIRT	Cybersecurity Center for the Autonomous City of Buenos Aires	State or Local Government
Barbados	CIRT-BB	CIRT-BB	Ministry of Industry, Innovation, Science and Technology
Bolivia	CSIRT-Bolivia	IT Incident Management Center (CGII, for its acronym in Spanish)	Ministry of the Presidency
Brazil	CTIR Gov	Computer Security and Incident Response Team (CTIR Gov)	Presidential Cabinet
Chile	CSIRT-CL	Chilean Information Security Incident Response Team	Ministry of the Interior and Public Security
Colombia	ColCERT	Colombian Cyber Emergency Response Group - ColCERT	Ministry of Information and Communication Technologies
Colombia	CSIRT-CCOCI	CSIRT - Joint Cyber Command	Ministry of National Defense (FF.AA.)
Costa Rica	CSIRT-CR	CSIRT-CR	Ministry of Science and Technology
United States of America	US-CERT	Cybersecurity and Infrastructure Security Agency (CISA)	Department of Homeland Security
Guatemala	CRIC-GT	Cyber Incident Response Center (CRIC) of the Guatemalan Army	Ministry of Defense (FFAA)
Guyana	CSIRT.GY	CSIRT.GY	Prime Minister's Office – National Data Management Authority

Table 1

Institutional location of CSIRTs in the region
(Information based on official responses to a survey conducted by CSIRTAmericas Network)

Jamaica	Ja-CIRT	Jamaica Cyber Incident Response Team (Ja-CSIRT)	Ministry of Science, Energy and Technology
Mexico	CSIRT-SEMAR-MX	CSIRT-SEMAR-MX	Ministry of Defense (FFAA)
Mexico	CSIRT-SEDENA-MX	CSIRT-SEDENA-MX	Ministry of Defense (FFAA)
Paraguay	CERT-PY	CERT-PY	Ministry of Information and Communication Technologies (MITIC)
Peru	CSRIT-MGP	CSIRT – Peruvian Navy	Ministry of Defense (FFAA)
Dominican Republic	CSIRT-RD	National Cyber Incident Response Team (CSIRT-RD)	Ministry of the Presidency
Dominican Republic	CSIRT-Defense	Cyber Incident Defense Response Team (CSIRT-Defense)	Ministry of Defense (FFAA)
Suriname	SurCSIRT	SurCSIRT	National Security Agency
Trinidad & Tobago	TTCSIRT	Trinidad and Tobago Cyber Security Incident Response Team	National Security Agency
Uruguay	DCSIRT-UY	DCISRT-UY	Ministry of Defense (FFAA)
Uruguay	CERTuy	National Information Security Incident Response Center	AGESIC / Presidency of the Republic

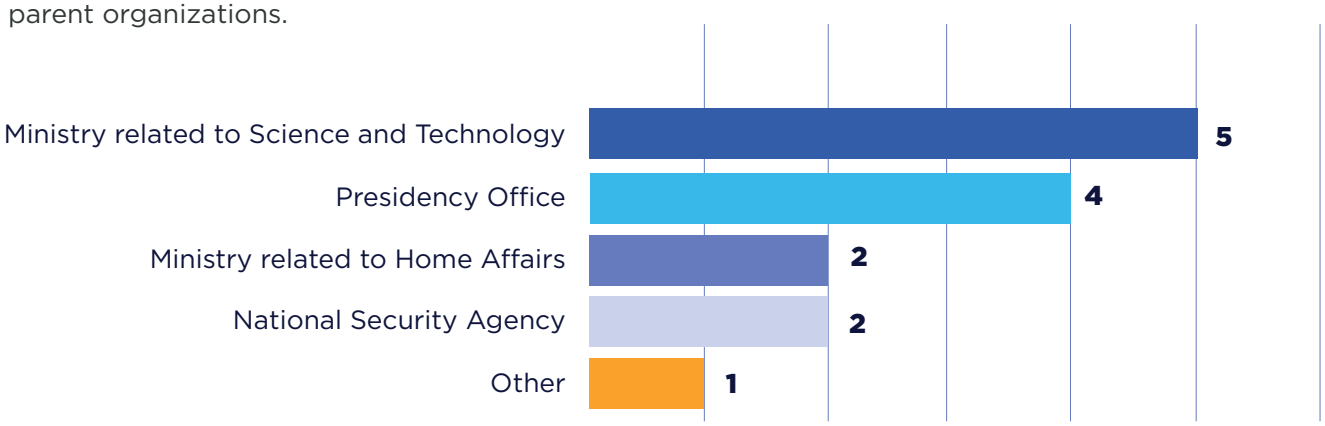
Source: Information based on official responses to a survey conducted by CSIRTAmericas Network of the Organization of American States (OAS), 2023.

| Complete information about CSIRTs members of CSIRTAmericas Network: https://csirtamericas.org/en/member_teams

When the topic of creating a national CSIRT is raised, the question arises: **Where should it be located within the governmental framework?** In Latin America and the Caribbean, ministries related to Science and Technology, the Interior, and Defense, as well as agencies or departments attached to the presidency, among the other possibilities detailed in Chart 2, predominate as parent organizations.

Chart 2

Government Institution to Which a National CSIRT is Attached in the CSIRTAmericas Network



Source: Information from the CSIRTAmericas Network of the Organization of American States (OAS), 2023.

To select a governing body and define where (within which institution) said national CSIRT will be located, it is advisable to pose the following questions:

- Does the organization inspire confidence among the sector's organizations?
- Is the organization capable of coordinating, serving, and accessing all sector organizations?
- Does the organization have financial footing solid enough to maintain and strengthen CSIRT operations?

To answer these questions, an important consideration is that a CSIRT's **primary characteristic and ability must inspire trust in the organizations that serve a particular community;** the institutions it serves should not be afraid to report an incident or request support, especially in times of crisis, since a CSIRT is an organization that primarily provides support, recommendations, and mentoring, but does not impose sanctions, judgement, or regulations.

> We carried out an evaluation prior to creating the CSIRT and concluded that they had to find a place where there was sufficient trust to provide these services. Ultimately, we decided on the Office of the Presidency

Dominican Republic
CSIRT-RD, national CSIRT

Two other characteristics that are important to consider are that **the sector in which the CSIRT is located must understand the importance of prioritizing information protections, in addition to having sufficient capacity to support and coordinate with any member of the served community.** In other words, a CSIRT must be able to immediately meet with and respond via multisector coordination and, additionally, must have solid financial resources to support daily operations, personnel training, and the creation and maintenance of services. It must also maintain a fund for emergencies or circumstantial crises that occur within the served community and have highest-level political support to be able to manage incidents at the national level.

Some experts also state that when choosing the CSIRT's location, it is important to consider the organization's required **autonomy and independence** in conducting its work. Both of these characteristics are rooted in trust, proper prioritization of information protections, and the ability to work hand-in-hand with members of the served community, knowing that they have one common goal: incident resolution.

Additionally, when defining a national CSIRT's location within a government ministry, entity, or secretariat, it is recommended to consider how the CSIRT could leverage any necessary internal services available – those such as human resources, finances, infrastructure, etc. – to build its structure.

Finally, it is important to have support from the host government ministry, entity, or secretariat, to empower the CSIRT to operate **flexibly and expeditiously** – both necessary elements in facing current challenges – while sustaining and growing over time.

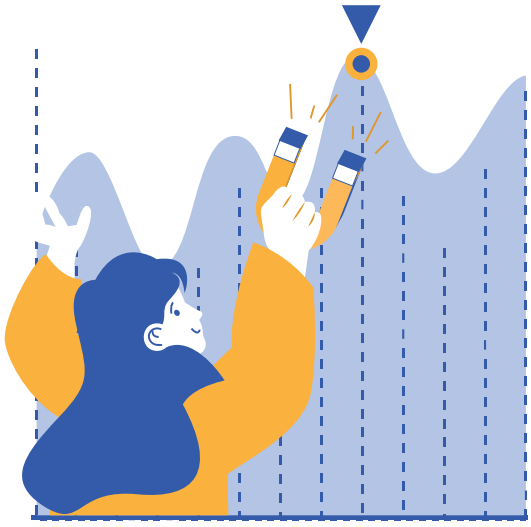
3.2 Ensuring the Continuity of CSIRTs in Latin America and the Caribbean

To achieve continuity, as well as a CSIRT's strength and sustainability over time, it is important to weigh the factors that impact effective cyber incident management; these include human talent, developing trust, establishing processes, and obtaining the necessary budgets, which will not only be used for human resources, infrastructure, training, and offices for normal operations, but also for any necessary improvement projects.

Many of the region's specialists who were interviewed in the preparation of this document agree **that starting small is an important contributing factor in a CSIRT's success: Build from a simple plan, based on specific actions or services, and carry out periodic evaluations that make progress possible. If necessary, propose changes.**

Proposing change implies a transformation process that can be achieved by strategically identifying and analyzing what the community requires in terms of services, the number and characteristics of human resources involved in the operation, and the technology necessary to cover the services offered. This requires **active listening** by the CSIRT and putting the "client" at the center of the operation. Among the initial basic services and tools, it is recommended to offer the following: a ticketing system[4], an email server, a telephone line, a webpage, and at least one additional service, such as the issuance of alert bulletins. It is not advisable to launch a service simply because other CSIRTs offer it or because of an out-of-context recommendation, since each community is different. Therefore, a strategic evaluation is necessary on the value

"START SMALL AND GROW"



[4] Automatic case registration system for the correct monitoring and prioritization of community requests.

that each service contributes to the community and its specific needs. Small but high-impact actions are recommended to strengthen the CSIRT's work through achievement.

Regarding human talent, it is advisable to launch with the minimum staff necessary to operate the aforementioned services. According to ENISA, the average number of staff who comprise a small team is three to seven[5]; however, this number will depend on the services defined above. It is not uncommon, at the start, to hire *junior* personnel and/or those with little or no experience in cybersecurity; however, this means that much of the CSIRT's foundational work is not built on solid ground. Although this can improve over time, it is more expensive when compared to doing it up front. A good recommendation in this regard would be to hire staff with sufficient experience, or to contract consulting services.

With the defined personnel, limited services, and established necessary processes, it will be possible to manage any expectations that are established with decision-makers and the served community at the start of CSIRT operations. Addressing these recommendations will also allow for organic growth and respond to any incidents that arise.

Just as the start of CSIRT operations is generally carried out based on a series of limited basic services, a mature CSIRT may respond to notifications from institutions affected by cyber incidents, thus deploying personnel to attend an information leak-related incident onsite, monitor and analyze cyber threat patterns, train community organizations, carry out laboratory tests on new services to mitigate Distributed Denial of Service (DoS) attacks, update rules for a *Web Application Firewall (WAF)*[6], analyze *logs*, participate in committees to develop and update cybersecurity strategies, coordinate work groups to protect against events of national scope, carry out *hardening*[7] on servers, and many other processes found in the FIRST service catalog[8], which is based on the following five areas:

- Information Security Incident Management
- Vulnerability Management
- Situational Awareness
- Knowledge Transfer
- Information Security Event Management

A CSIRT should not only focus on responding to cyber incidents when an institution requires it but should also play a fundamental role in coordinating cybersecurity for events with a social and economic impact within a country; this is why they must develop trust beyond existing decrees and agreements. **It is through trust and value creation that a CSIRT can act on the side of the affected party and work with them, not against them.**

[5] ENISA, December 2020. How to set up CSIRT and SOC, Good Practice Guide. https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc
[6] Web Application Firewall: Web Application Firewall
[7] Hardening: Consists of the process of reducing vulnerabilities in applications or systems.
[8] FIRST: Forum of Incident Response and Security Teams. https://www.first.org/

> “Regulations state that CERTuy has the power to intervene in computer security incidents; however, thanks to the trust they have built, their participation never had to be forced – quite the opposite”
>
> **Uruguay**
> **CERTuy, national CERT**

Latin America and the Caribbean CSIRTs have had a leading role in coordinating events and initiatives related to cybersecurity and that have required them to include new services. Some of those events or initiatives are:

- Election Days
- National and Regional Sports Games
- Intersectoral Exercises
- Preparation of National Cybersecurity Strategies
- Situations involving Escalation of Social Conflicts
- Regional or National Summits
- Content coordination with university chairs and programs

Developing CSIRTs and their continuity in the region has led to incorporating services that would normally be provided by a *Security Operations Center (SOC)*. This can be of great value to the community, but it will be important to review the mandate that determines whether this is a service that can be provided by the CSIRT. Annex 1 describes the characteristics and differences between a CSIRT, a CERT, and a SOC, but in general, the mandate that gives rise to the CSIRT will also define its scope of operation.

3.3 The Challenge: Unpredictable Scenarios, Human Resources, Budget, and Technology

One of the great challenges and opportunities that a CSIRT must face is an **unpredictable, everyday scenario** that can include: waves of cyber-attacks, the appearance of new patterns, new and more sophisticated cybercrime groups, and political tensions or electoral cycles, which push a CSIRT's capabilities to their limit regarding attention, response, and incident management. In the region, this rhythm of cyber phenomena has produced a series of challenges that begin with limitations to the budgets assigned for daily operations, a change of direction due to variable political contexts, and delays in acquiring cybersecurity tools, as well as risks to continuity in the provision of services (both established and new) to the community.

Likewise, the risks to continuity have two aspects: The first is **high personnel turnover,** whose cause is rooted in the knowledge acquired by the CSIRT, as well as interest from the private sector in obtaining trained resources to confront their own cybersecurity challenges.

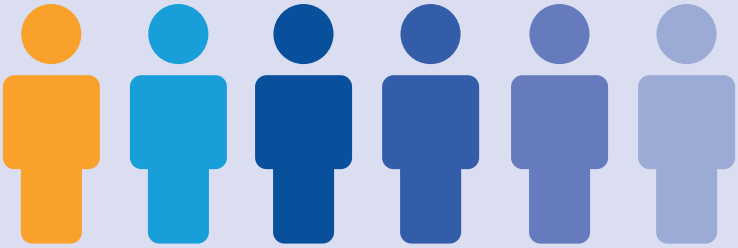
To understand the panorama in terms of personnel – currently, the average number of people working in a government CSIRT in Latin America and the Caribbean is 6, of which 74% are men and 26% are women. This distribution varies in terms of leadership positions, as shown in Chart 3.[9]

> "After 18 or 24 months of working in a CSIRT, a person becomes a very attractive candidate for the private initiative. To avoid high team turnover, it is important to keep people motivated, trained, and committed to the mission"
>
> **Dominican Republic**
> **CSIRT-RD, national CSIRT**

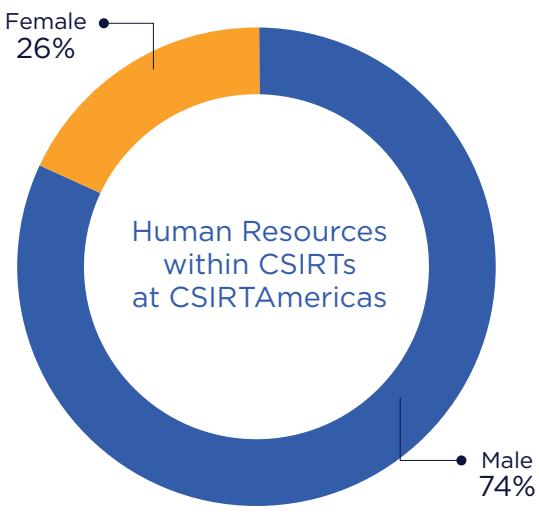
[9] Source: CSIRTAmericas Network, Organizations of American States, 2023

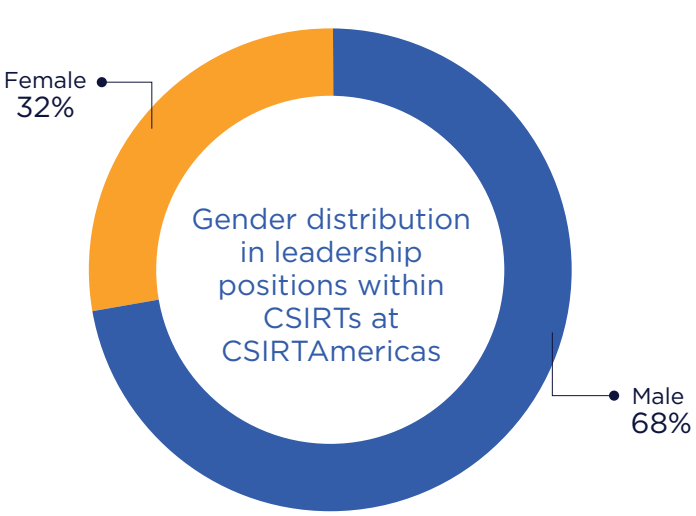
Chart 3

Human Resources and CSIRTs in the CSIRTAmericas Network



6 Members per CSIRT
On average





Source: CSIRTAmericas Network, Organizations of American States, 2023.

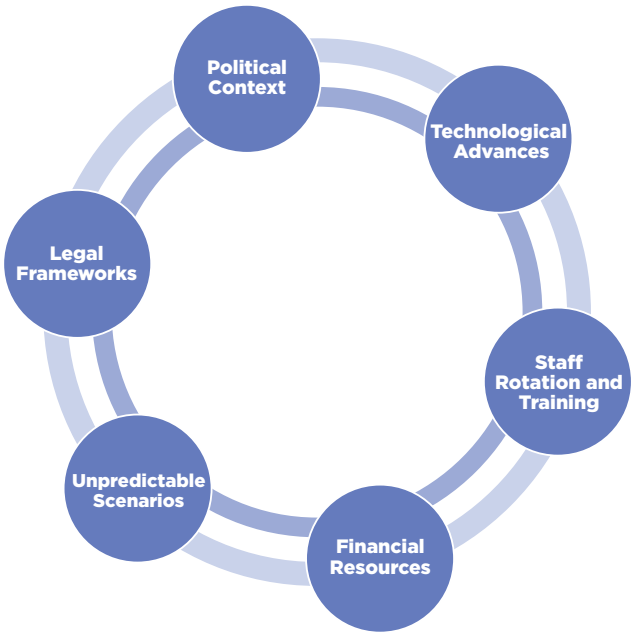
The second aspect is related to **budget:** Throughout the region, in some cases, CSIRTs are created without assigned fixed budgets. Teams are formed based on personnel loaned from other areas of the institution or from external entities. Salary profiles are not compatible with the CSIRT budget. There are governmental changes, delayed purchasing processes, extraordinary activities, technology migration, and technological debt phenomena that end up considerably eroding a CSIRT's sustainable operations. In this sense, it is essential to establish an assigned, flexible budget that includes acquiring new tools and licenses, their renewal and updating, consulting services on solution migration, special days for staff rotation, training, and expanding services, among others. Annex B demonstrates a budget that contains important considerations and can serve as a reference point in preparing an initial budget.

Regarding **technology,** CSIRTs have a great advantage in the use and implementation of free software solutions that are developed and shared by cybersecurity communities around the world. However, it is important to consider that the organization's technological architecture must be implemented strategically with an adequate mix between free software and software acquired for specific purposes. In this sense, it is important to consider that, due to the changing nature of the technologies associated with operations and attention to incidents, it is essential to adapt to this reality by evaluating new solutions, updates, and frequent adjustments to the technologies associated with these services. This and other aspects will be addressed in the next section, with specific recommendations for CSIRT maintenance.

As can be seen, there are several challenges and daily activities that comprise the essence of a CSIRT, from political aspects to the most technical challenges. These challenges affect a CSIRT to different degrees and levels, and they all coexist in a manner interconnected by the CSIRT life cycle, as represented in the diagram below.

Chart 4

Continuity Challenges for government CSIRTs



To face continuity challenges, it is useful to think of a CSIRT as a business model that must be profitable in terms of creating value for a specific served community. Additionally, some CSIRTs in the region consider the following actions as strategic:

- Recruit staff with soft skills, rather than technical ones; that is, people with critical thinking, analytical, risk-oriented, or strategic mindsets, as it is more difficult to develop soft skills than it is to teach techniques.

- Do not centralize responsibilities into a single resource.

- Inspire commitment and a sense of belonging.

- Make agreements with private companies to train personnel working in the CSIRT.

- Establish internship agreements with universities that offer degrees associated with cybersecurity.

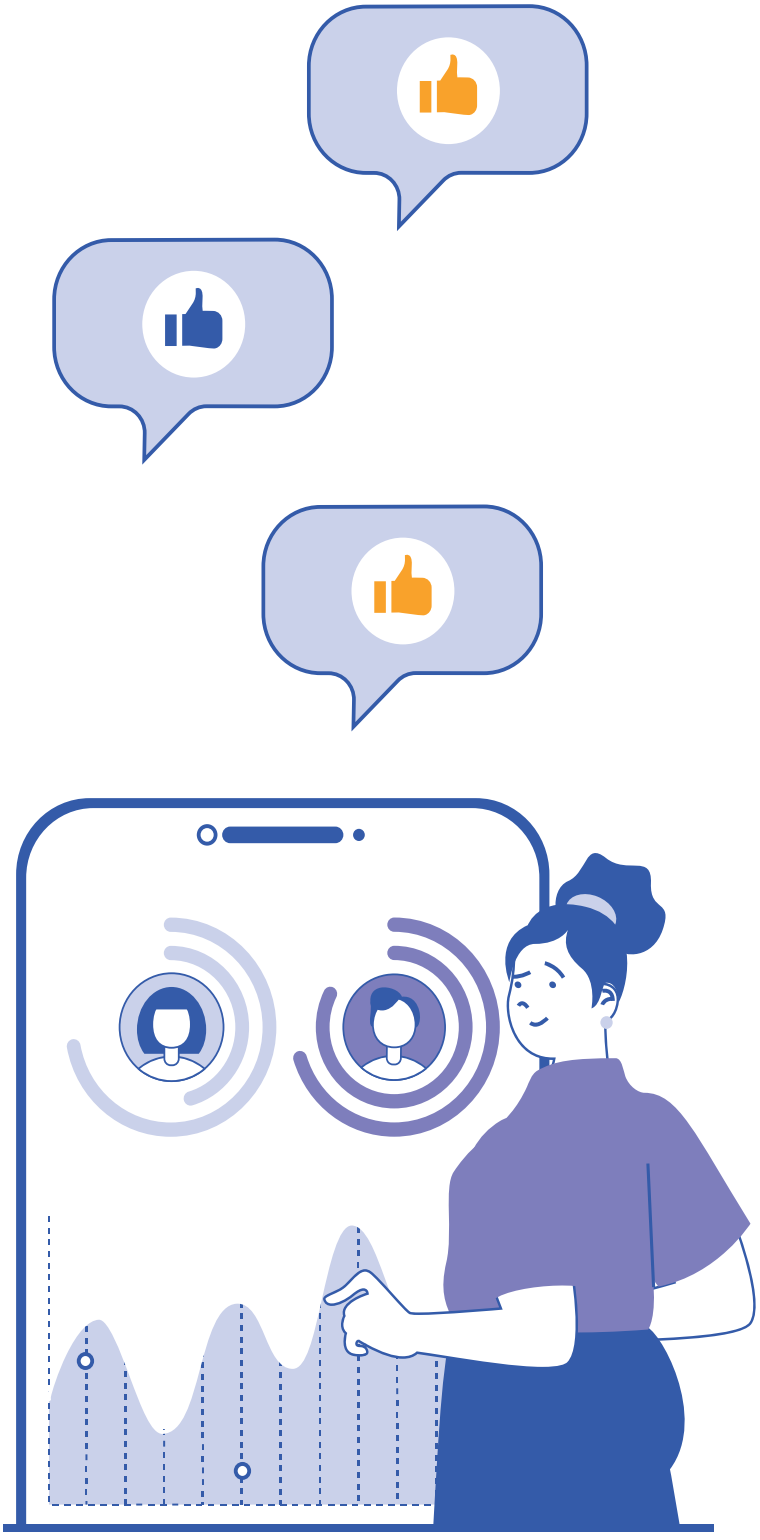
- Implement special projects, such as creating new services supported by funds from international organizations.

- Seek national funds dedicated to technology and cybersecurity projects.

- Develop programs, competitions, and activities that strive to get to know emerging talent, with the purpose of future recruitment.

- Sign international agreements that allow for education and two-way training for response team personnel, as well as being able to share valuable information regarding threats.

- Create strategic alliances with national industry, academia, and civil society, in order to develop sectored strategies with the capacity for deployment and dissemination.



> At first, the National CERT of Colombia - colCERT and the CSIRT of the Colombian Military Forces - CCOCI were attached to the Ministry of National Defense and were comprised of military and civilian personnel who were trained through international agreements. Subsequently, an internal knowledge management plan was developed that allowed for strengthening the capabilities of entity officials

Colombia
colCERT, national CSIRT

> With the understanding that the best formula to achieve results is based in information plus the power to act, the CSIRT held events at universities to recruit students who were in their final semesters and had the flexibility to work and finish their theses. It was even proposed that they do their thesis on something relevant to the CSIRT

Chile
CSIRT-CL, national CSIRT

> In the first phase of the CSIRT, students were recruited, offering advantages such as remote work as a differentiator between other jobs

Argentina
CERT.ar, national CSIRT

4. A CSIRT AS **BUSINESS MODEL**

As stated, cyber incident management goes far beyond a technical procedure. The region has many successful cases in creating CSIRTs, but there are also cases where the CSIRT lives only on paper and does not see the light of day.

Therefore, **before creating a CSIRT, it is important to plan and design it with a long-term vision and a plan for sustained growth.** This vision will make it possible to identify the key elements to meet CSIRT objectives, as well **as to develop clear and measurable indicators that, when met, demonstrate CSIRT effectiveness and justify its existence.**

In other words, a best practice when creating a CSIRT is to structure it as a business model adjusted to changing opportunities and limitations, while keeping in mind that it will not necessarily create monetary profitability but will act as a differentiator by helping build more efficient systems, inspiring greater citizen confidence, and minimizing serious impacts in the event of cyber incidents. That is why this guide addresses creating a CSIRT based on a business model and using a CANVAS model.

This section has been inspired by the guide, *"Getting Started with a National CSIRT"*[10], which presents a CSIRT business model (Global Forum on Cyber Expertise, GFCE. Mayo, 2021).

4.1 Defining the CANVAS Model

A business model is a tool that allows for modulating, describing, and defining the way in which an organization orchestrates elements and activities to achieve its objectives – in other words, a method of creating and delivering the value for which said organization was conceived.

The CANVAS model (Osterwalder-Pigneur, 2010) is a graphic method of representing a business model. This methodology is useful for project leaders, managers, and directors to clearly explain the value and necessity of a CSIRT in each or its relevant contexts, to all relevant parties.

Below is a CANVAS that represents a generic business model for a national CSIRT; this model can be adapted to various needs, including those of a sectoral CSIRT.

[10] Getting Started with a national CSIRT. Cybersecurity Capacity Building – Global Forum on Cyber Expertise (GCFE), 2021. https://cybilportal.org/wp-content/uploads/2021/06/TNO-2021-Getting_started_with_a_national_CSIRT_FINAL.pdf

Chart 5

CANVAS Template
for a CSIRT

The CANVAS typically has a specific order in which it must be created, as well as read, so it is presented in that order. In this case, to launch an operational and strategic business model, the most important thing is to define the served community. At the end of this chapter, we will see how this dovetails with the CANVAS model.

4.1.1 Customer Segment. Who Does the CSIRT Serve?

This CANVAS element describes the served community, which represents a fundamental element when launching the plan to create or update a CSIRT. This defines the groups, organizations, and/or entities to which CSIRT services will be offered.

In the case of a national CSIRT, this community is formed first by public state entities, since one of its primary functions is to support them in identifying, preventing, and mitigating cyber incidents. Among these entities are included the executive and judicial powers, electoral institutions, and the Armed Forces, which must be considered as segments to serve and for whom needs related to the value proposition will be covered. But it is also necessary to consider public and private organizations that could be identified as critical elements of infrastructure.

A sectoral CSIRT would have a smaller community than that of a national CSIRT. For example, a country's Military Forces could form a sectoral CSIRT that coordinates with and provides cyber incident management services to its various components (Air Force, National Army, etc.).

Types of sectoral CSIRTs, which vary according to the served community:

- Critical infrastructures. Public and private organizations that manage physical or virtual systems considered vital to the country, because their incapacitation or destruction would have a debilitating effect on national economic security, health, national public safety, or any combination of the above.

- Internet Service Providers (ISP) or *Internet Exchange Points* (IXP). Organizations in charge of Internet connectivity.

- Military or Armed Forces

- The Financial Sector (can be coordinated through associations)

- Health Services

- Retail Businesses or Specific Sectors

- Academics and Education (universities or educational institutions)

- Local or Provincial Governments

- Civil Society

- Private Initiative Sectors

4.1.2 Value Proposition. What Needs Does the CSIRT Meet?

This element forms the model's backbone, as it defines the proposal to solve a problem or fulfil the defined community's needs.

The ability to identify a compromised production server in time, collect logs to analyze traces of a malware attack, recover an online service, defend a critical asset from a denial-of-service attack, receive training on cybersecurity issues, detect exposed credentials, or respond to a leak of sensitive information, are some of the possible needs that may present in a CSIRT served community.

In this sense, the community expects an ecosystem that connects various processes, tools, people, and services that support them in the resolution of cyber incidents.

Therefore, the CSIRT's main value proposition to its served community is to "identify, prevent, respond, and mitigate cyber incidents. Likewise, the CSIRT will offer a series of services that add value by *"assisting and advising the served community"* on cybersecurity issues. This proposal must be aligned with the specific mandate, mission, and vision that the CSIRT has defined.

4.1.3 Channels. How to Make Contact and Deliver Services?

This block defines how CSIRT services will be delivered to the served community. This topic is fundamental, since the CSIRT is an organization that falls under the dynamic of permanent contact with different organizations inside and outside its served community. CSIRT channels should always be available and easily accessible to the community.

These channels represent bridges that enable community outreach regarding use of CSIRT services and, therefore, establish a network of trust between the community and the CSIRT.

It is important to maintain a balance between automating response channels and direct interaction with CSIRT members. This is always well received by the community, as it helps strengthen the bonds of trust with the people who interact with each other while managing an incident.

Do not forget that proper promotion on social networks and other forums, such as specialized cybersecurity conferences, allow for positioning, referencing, and providing visibility on the CSIRT's work. These service channels must be friendly and segmented, per the community's needs.

When a CSIRT communicates with the general population on social networks or via conferences, they should try to use simple language and minimize excessive technicalities.

A strategy adopted by CSIRTs in cases of circumstantial crises or those with major media coverage is to use a single point of communication via a status page that allows for reporting, updating, and maintaining information on past actions and case history, without compromising incident management confidentiality. This allows for control over the distortion of false information, helps manage community expectations, and supports information traceability, while guaranteeing transparency and keeping informed all parties involved in a case.

It is important to define and publish the RFC 2350 document (Expectations Regarding Response to Computer Security Incidents), which will inform the served community on topics regarding the response team's policies and procedures, collaboration in managing incidents, the relationship between the CSIRT and its counterparts, CSIRT services, and other information relevant to the entity.

Some channel options to consider are as follows:

- Website
- *Ticketing* System
- Distribution List/Email
- Telephone
- Alert Notification System
- Conferences and Events
- Social Media
- *Status Pages*
- Information Exchange Platforms (for example, MISP[11])
- Messaging and Communication Groups on Platforms such as WhatsApp, Signal, or Telegram

[11] MISP: Malware Information Sharing Platform.

4.1.4 Relations. What Type of Relationship Will You Maintain with The Served Community?

This relationship is derived from that agreed in the CSIRT mandate. Therefore, the legal mandate for the CSIRT will be essential to adjusting the value proposition.

Among the primary ways to attract the served community and build bonds that result in relationships of trust are the following:

- Assistance and Incident Support
- Consulting
- Training Sessions/Events
- Contact Network

> "Workshops were held directly with the served community to listen to their ideas, interests, and doubts. This made it possible to better define the services that the community really required"
>
> **Chile**
> **CSIRT-CL,**
> **national CSIRT**

4.1.5 Sources of Income. How to Secure Operational Funding?

A source of income is a crucial issue for the sustainability and growth of a Cyber Incident Response Team. Many national CSIRTs do not monetize their services to the community, so gaining financial attention becomes a creative task.

Usually, one organization hosts a CSIRT and that organization, through a public budget, guarantees support for CSIRT general operations and the employees who work in therein. However, to expand or create new services, according to the served community's daily demand, human and financial resources are required for their execution. Many times, these services fall outside the scope of the fixed budgets assigned by the organization that hosts the CSIRT.

In this sense, apart from the public budget, there are some alternatives to seek financing. They are listed below:

- **Funding from International Organizations:**
  - »Support in creating new services
  - »Training and education
  - »Obtaining resources for ongoing support
- **Project Consulting (if allowed):**
  - »Provide specific paid services
- **Private Sector Initiatives:**
  - »Support in educating the community
  - »Laboratory development

»Pro-bono services
»Donating tools
»Invitation to forums and events

•Initiatives with Civil Associations:
»Training for free software tools for its creators
»Promoting and/or invitations to community events

•Initiatives with Universities and Educational Centers:
»Training
»Internship programs
»Support with researchers on complex cases

•Armed Forces and Law Enforcement Sector:
»Training
»Support programs through commissioned personnel

These alternatives have been offered throughout in the region; however, it is important to identify those organizations or groups that are available in each country, outside of those listed in this document.

4.1.6 Key Activities. What Activities Does a CSIRT Require to Fulfill Its Value Proposition?

This section defines the activities necessary to materialize the value proposition. This block constitutes the catalog of service offerings; that is, each CSIRT will review the needs it wishes to cover and the scope of the same (defined in its value proposition) and, derived from this, will offer specific services. According to the FIRST framework of services[12], we consider:

•Information Security Incident Management

•Vulnerability Management

•Situational Awareness

•Knowledge Transfer

•Information Security Event Management

As mentioned in the previous chapter: "Start Small and Grow" – In its early years, a CSIRT should not and cannot operate or offer all the services found within this framework; doing so (or trying to do so) is one of the main causes of a CSIRT's unsustainability, as each listed service implies operating costs and human resources that often cannot be paid for by public budgets assigned to a newly created CSIRT.

[12] FIRST CSIRT Services Framework version 2.1. FIRST, 2019. https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0_bugfix1.pdf

Therefore, **a best practice is to begin with essential services – those with high impact and reach – for a served community.** As explained previously, one is the cyber incident management service, which acts as the heart of the CSIRT. On the other hand, a service that is easy to operate and understand is a community alert system via communication on reports and recommendations regarding situations that either may be or are affecting the technological resources of a serviced organization. In this same order, creating awareness campaigns and organizing training sessions are other ways to bring the CSIRT closer to the community and create bonds of trust at the start of operations.

Selecting how these services will be delivered is as important as the services themselves. It is important to have shift and on-call structures (special shifts to respond to any eventuality) to cover and maintain an adequate level of service, 24 hours a day, 7 days a week. Offering a defective service, or one for which you do not have sufficient capacity, will inspire a loss of confidence that would harm the CSIRT.

As mentioned above, one aspect that is interesting to highlight is that both the description and especially the scope of services must be very well defined. You must know which aspects are covered and which are not, since an incorrect definition in this scope can create a false sense of security.

When we talk about value, there are different ways to offer this through services, one of which is to provide alerts on existing vulnerabilities or indicators of compromise (IOC). Another service of value could be to provide training to the served community on how to make use of the information that is constantly being sent; this can emerge as a result of an analysis on the served community's maturity.

An idea shared by specialists from the region (CSIRT-CL in Chile and TT-CSIRT in Trinidad and Tobago) is to focus on creating the trust necessary to exchange training or alerts that are not normally publicly accessible, to thus position the CSIRT brand. At the same time, the recommendation is to make agreements with companies from different sectors to distribute their contents. This action has made it possible to create first-hand reports and build value for those who received the information. In the end, it allowed the companies themselves to directly report incidents via the *ticketing* system.

4.1.7 Key Resources. What Resources are Needed to Develop the Value Proposition?

This block lists those resources that are considered fundamental for the CSIRT to produce, deliver, and manage their services and other fundamental activities. Proposed resources are those that are essential to carrying out the services described in the previous block:

•**Organizational Resources.** They group everything necessary for the CSIRT to operate a physical location, with furniture, telephone lines, servers, official transportation, general services, special facilities (*war room*[13]), meeting rooms, organizational charts, processes, and the procedures described.

•**Actionable Information.** This is the information that can be used without carrying out additional major processing to communicate or validate said information. In this sense, according to the European Union Agency for Cybersecurity (ENISA)[14], This type of information must present the levels of relevance, timeliness, precision, completeness, and digestibility that help the CSIRT to take action to identify, prevent, respond, and mitigate cyber incidents. These can be, for example, cyber intelligence feeds[15], threat intelligence, indicators of compromise, indicators of attack, and even information obtained directly from the community.

> "Threat intelligence is not just about implementing tools for feed ingestion. Tools are nothing more than applications and a couple of lines of code. It is a philosophy, a methodology, a preventive tool, and response operation based on the consumption, processing, and analysis of data"
>
> **Dominican Republic**
> **CSIRT-RD, National CSIRT**

Indicators of Commitment	•IP addresses, domain names, URLs •Hashes or integrity values, registry entries linked to malicious code •File names and locations
Alerts	•Vulnerabilities •Updates •Exploits[16] •Behavior Patterns •International Alerts

[13] War room: A space to gather the Incident Response Team decision makers to allow for better team coordination. Sometimes referred to as Situation Rooms, Control Rooms, or a Command Center.
[14] European Union Agency for Cybersecurity (ENISA), 2023. https://www.enisa.europa.eu/
[15] Content that can be exported to other sites also known as data streams.
[16] Exploit: Software program or code that exploits a vulnerability in an application or computer system.

•**Tools.** These bring together the necessary technologies required to support the value proposition, channels, and relationships with organizations in the served community. An example is a ticket system through which requests and reports can be addressed. Also, the entire set of tools aimed at the prevention, detection, and resolution of cyber incidents, as well as those via telephone and email services. CSIRTs can choose to maintain a balance between open-source and proprietary solutions to support their services, while taking into account the budgets (in many cases annual) that each of them requires to stay updated.

•**Human Resources.** These constitute the most important resource of this block. Without talent, there is no provision of services, and even less building bonds of trust. Therefore, it is the most valuable resource within a team. The profiles needed to form a team are varied. In the GFCE[17], FIRST[18], and ENISA[19] reports, you can find the appropriate profiles to form a CSIRT.

Even though technical roles are essential within a team, cybersecurity communications specialists are becoming more relevant by the day. The increase in cyber incidents, as well as their direct impact on essential citizen services, demand timely information that citizens can digest and understand. Attacks that affect banking systems, identification entities, and health services quickly become crises that demand centralized, timely information adapted to each type of community. In addition, these profiles could support the technical team in spreading the word and inspiring understanding of the benefits a CSIRT offers.

[17] Getting Started with a national CSIRT. Cybersecurity Capacity Building – Global Forum on Cyber Expertise (GCFE), 2021. https://cybilportal.org/wp-content/uploads/2021/06/TNO-2021-Getting_started_with_a_national_CSIRT_FINAL.pdf
[18] CSIRT Roles and Competences (Addendum). FIRST, 2023. https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Roles_and_Competencies_v_0.9.0.pdf
[19] How to set up CSIRT and SOC. ENISA, 2020. https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

4.1.8 Key Partners. Who are the Key Partners or Suppliers?

This answer encompasses the partners, vendors, or entities that either play a strategic role or contribute significantly to making a CSIRT function properly. Some of a national CSIRT's key providers or partners are:

•**Internet Service Providers (ISPs).** They can provide support via information and, in some cases, in response to certain cyber incidents. A clear example is in containing Distributed Denial of Service attacks, in which a relationship of trust between an ISP and the CSIRT allows for the immediate execution of blocking and containment actions. Another common example is in carrying out cyber hygiene operations on infected Internet of Things devices under the segment of an ISP. This is a clear relationship that allows for generating bidirectional value.

•**Law Enforcement.** CSIRTs and law enforcement must have fluid and permanent communication, due to the close relationship between cyber incidents and cybercrime cases that foster a common ground for collaboration and constant information exchange between these organizations. A CSIRT can keep law enforcement agencies updated on the latest techniques and patterns of compromised email accounts of interest or access to administrative panels of virtual infrastructures exposed on the Internet, which could perhaps facilitate resolution of a cybercrime case that law enforcement agencies are currently working to solve, for example. A collaborative initiative between a national CSIRT and military forces could involve carrying out joint simulation exercises to measure the cyber incident response capabilities of a country or region.

•**Legislative Power.** This is a potential CSIRT client and, at the same time, a benchmark for the promoting legislative aspects related to cybersecurity. For example, a national CSIRT can provide indicators on the number of compromised government systems that could encourage legislative bodies to strengthen and monitor highly critical systems, including the adoption of two-factor authentication mechanisms, limitations to administrative accounts, etc.

•**Justice Department.** Some attention to cyber incidents may require intervention from the judiciary. In these cases, CSIRTs could act as active collaborators in judicial processes that require testimony from an expert in cybersecurity.

•**International Organizations.** International organizations play a key role in CSIRT operations. The relationship could occur in several ways, including:

»Regional Coordination.
International organizations can support coordination on cyber incidents that require regional support or international contacts. An example of regional reference is the CSIRTAmericas Network, a hemispheric network of Computer Security Incident Response Team (CSIRTs) of the member states of the Organization of American States (OAS); this network acts as the main promoter of the CICTE/OAS Cybersecurity Program, in strengthening its ability to respond to cyber incidents throughout the OAS region and also serves as a platform for 24/7 information exchange on cyber threats,

provides technical assistance programs, and offers professional development opportunities to its members.

»Project Funds.
CSIRTs can elevate high-impact new service creation projects, training programs, or awareness programs to international organizations, in order to explore funding options.

»Training and Events.
CSIRT members can benefit from training and cybersecurity events organized by international organizations that allow training team specialists and make visible a CSIRT's initiatives.

•**Universities and Institutions of Higher Education.** The relationship with universities is strategic, because a common problem that CSIRTs face is the scarcity of resources with adequate profiles and that have the basic training required to carry out activities within a CSIRT. Relationships can be established with a university to allow for a classroom education for students who could eventually be invited to form part of the CSIRT workforce; this can happen through programs such as *Creating a Professional Path in Cybersecurity*, an initiative promoted by the OAS with the support of the *CITI Foundation*, and which seeks to train and inspire talented young people to consolidate a regional workforce. This program includes a component that directly links universities and other higher education institutions with CSIRTs, thus providing opportunities for students from the region to create solutions for CSIRT members of the CSIRTAmericas network.

The academic sector can also collaborate with a national CSIRT in preparing and delivering training programs of interest to the served community, as well as collaborating on investigations of highly complex cyber incidents.

•Private Cybersecurity Companies. Private companies interact with a CSIRT in several ways. The most common are through:

•Providing equipment, licenses, or technological solutions that support services provided by the CSIRT.

•Establishing agreements and mechanisms for reporting alerts or cyber incidents detected by private companies that affect the community served by a CSIRT.

•Organizing training and capacity building programs in cybersecurity and that are of interest to the served community.

•Outsource the hiring of human talent, if necessary.

It is important to remember that in the case of National CSIRTs, there must be a legal framework that enables this action, such as having a Memorandum of Understanding (MoU).

•**Civil Associations.** Civil organizations promote and influence the creation of a cybersecurity culture in a region or sector. Both a CSIRT and civil associations can work closely on projects including:

»Organizing and promoting cybersecurity training of interest to the served community.

»Exploring the creation of *bug bounty*[20] programs to report vulnerabilities associated with organizations in the served community.

[20] Program that allows "ethical hackers" to access the technical security of a technological platform (web or mobile) to discover flaws or vulnerabilities in exchange for remuneration depending on the severity of what is found.

»Facilitate locating experts specialized in cybersecurity issues and who could support the resolution of a cyber incident case.

»Participating in simulation exercises organized by the CSIRT.

•**Other CSIRT.** The nature of a CSIRT is to provide technical assistance and carry out multisectoral coordination actions. That is why it is important to strengthen collaborative agreements and information exchange with other CSIRTs, at both the national and international levels. Collaboration may benefit from mutual assistance in cases of cyber incidents, support through expertise, exchange of actionable information, integration of solutions to detect and mitigate cyber incidents, and exchange of experiences and good practices.

4.1.9 Cost Structure. What Expenses Should a CSIRT Consider?

This block helps us define the expenses and investments necessary to operate a CSIRT. It is worth mentioning that, if at any point the team decides to grow into offering new services, or if it expands its value proposition, it will be necessary to rethink the CANVAS before reviewing the cost structure, which can be segregated into different categories such as fixed costs and variable costs. Some associated costs are:

•**CapEX (Capital Expenditures).** Investment in material resources, such as an office and its equipment, as well as the purchase of servers and other investments in non-current asset capital should be considered. This must extend to both new investments necessary to grow services, as well as those expenses required for updating or improving equipment and offices.

•**Opex (Operating Costs).** Consider the following options:

»Technological infrastructure.
Se mencionó en el bloque de recursos clave la importancia de este punto que soporta la operación y la prestación de servicios del CSIRT.

»Cyber Threat Intelligence Licensing (CTI).
Licenses to obtain feeds (data flows) are key to operating a CSIRT, since they provide real and actionable information on possible threats

to technological infrastructures in the served community. Specifically, they may contain information regarding critical infrastructures exposed to the internet, compromised emails, exposed credentials and leaks of sensitive information, among others. Taking the previous example as a reference, the information shared through the *CSIRTAmericas Network* allows member CSIRTs to identify threats that could affect an organization's security, critical infrastructures, and the citizens of their country, which is the first step to prepare and defend against attacks. In other words, by obtaining (free of charge) large volumes of cyber intelligence data, a CSIRT can directly identify, manage, and notify government institutions affected by a cyber-attack, which thus directly strengthens its Event Security Management Service Information.

»Human and Administrative Resources.
This item can consume a high percentage of operating expenses, both in salaries and in the constant training of personnel. Operating expenses for after-hours work schemes, transportation, lodging, and other recurring expenses must also be included. It cannot be overlooked that, in all cases, ongoing training for human resources cannot be obtained only through donations or invitations.

»Membership in International Security Forums.
These are associated costs whose purpose is so that CSIRT representatives may have access to a series of resources, such as technical assistance and team training plans.

4.2 How to Efficiently Communicate the CSIRT Business Model?

Efficiently and correctly communicating a CANVAS is as important as its own definition and the design of its components. For this reason, the CANVAS has a defined structure for how it should be read and that recommends a storytelling technique to explain and transmit the model in an attractive way; that is, telling the story through the perspective of the served community, its problems, and its needs. This can be done as follows:

1. The served community is the protagonist of the story. You should talk about the challenges you face and the tasks you must carry out, emphasizing those aspects where the CSIRT will be relevant.

2. Subsequently, the story must explain how the CSIRT creates value for this community and then describe its services, emphasizing how each service responds to a specific community need. As part of the story, also tell what resources and activities will support CSIRT enhancement.

As mentioned at the beginning of this paper, this methodology serves project leaders, managers, and directors in their mission to explain, in a simple and intimate way, the necessary value of a CSIRT to all relevant parties.

5. KEYS TO AN EFFICIENT CSIRT

This section attempts to present, in a simple and concrete way, the experiences and advice of the authors of this document, as well as the specialists interviewed according to specific categories. It does not intend to express any technical considerations for CSIRT functioning and operations.

Mandate

•It is important to conform to the functions and guidelines outlined in the official CSIRT mandate. As a CSIRT becomes known for their work, they are often consulted on support situations outside their mandate. The CSIRT must channel these requests to the proper corresponding agency.

•It will be important to manage expectations from senior management and the served community at the start of CSIRT operations. Having a CSIRT does not mean that cyber incidents will disappear the day after the organization goes live, but rather implies that they will undergo a formal management process.

•Define the regulations to which the CSIRT must comply. Document procedures, processes, and responsibilities.

Human Resources

•In the case of a small *pool* of specialists, it is recommended to assign several roles within the CSIRT and to rotate their positions throughout the various departments.

•It is necessary to interact with universities to specify initiatives to attract human talent and structure training programs.

•Flexible labor policies should be implemented to help mitigate staff turnover.

•It is important to take advantage of training programs offered by international organizations, on the condition that those who attend a training session return to the CSIRT to document and share their knowledge.

•It is required to train staff in handling communications in public or press settings.

•It is important to document these processes to minimize the learning curve among the new members of the group.

THE LEARNING CURVE WHEN ONBOARDING NEW HUMAN TALENT CAN BE LONG; DOCUMENTING PROCEDURES HELPS INCREASE OPERATIONAL EFFICIENCY.

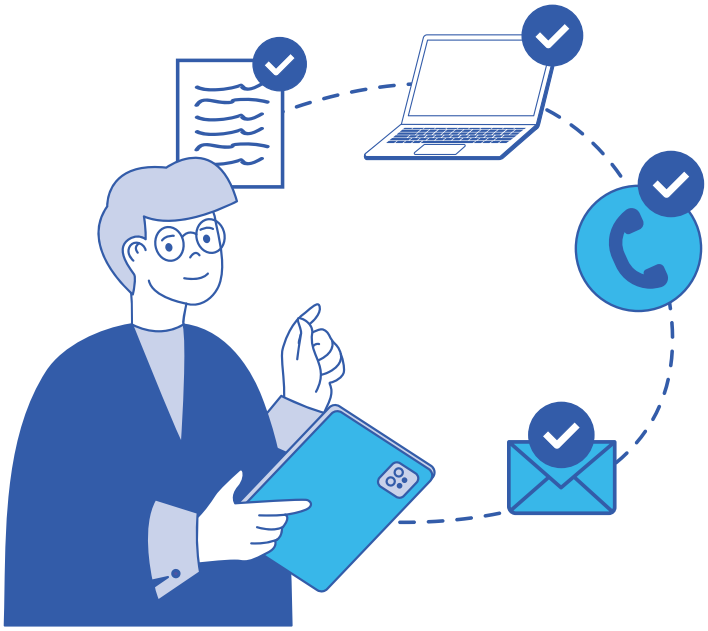
Services

•Start with a CSIRT's core service – cyber incident management – and then, add services that have broad, community-wide benefits and are simple to operate.

•When designing and offering a new service to the community, it is necessary to first think about its possible utility to the community. Services should be kept simple and avoid creating a high additional burden on community users.

•To implement a CSIRT's essential technological tools (webpage, distribution list, ticket management tool, email, telephone line), they can rely on open-source technologies that would help prioritize and guide costs, as well as strengthen the services they offer; the choice between open-source or self-developed tools will depend on budget, needs, and available team resources.

•When launching a new service, it is important to always consider that each CSIRT is different and must prioritize those services that create the greatest value for their own served community, which will depend on demand, national context, legal authorization, and the organization's level of maturity, among other factors.



I CREATE ADDED VALUE FOR THOSE WHO NOTIFY ME OF AN INCIDENT, WHEN I DEPLOY TECHNICAL CHANNELS, COMMUNICATIONS, LEGAL ADVICE, AND A PREVENTION STRATEGY. WITH THIS, THE CSIRT NOT ONLY RESPONDS, BUT ALSO ACCOMPANIES.

Community

•A common mistake is in measuring the number of tickets that are received and handled, thus creating the perception that more people in the community know about the CSIRT; having more tickets does not mean that the job is being done better.

•The community needs to recognize this work and really see the value of the services that the CSIRT provides. This is accomplished by making the community aware of the tasks and services that have either supported or helped community members.

•The value of the CSIRT must be properly communicated; having visibility and good communication builds trust and allows for community outreach. Therefore, the community must be involved in what the CSIRT does.

•Bear in mind that many times, a CSIRT can create great impact through simple services (news, alerts, bulletins, and prevention campaigns).

AMONG THE KEY FACTORS FOR SUSTAINED CSIRT SUCCESS IN THE COMMUNITY, ARE INTEGRATION (FOR EXAMPLE, SHARING INDICATORS OF COMMITMENT) AND TRUST, BOTH TO REPORT AND TO BE AWARE OF WHAT CAN BE DISSEMINATED.

Budget

•Scenarios should always be considered in which something urgent or not contemplated is then required.

•Make decision makers understand that the budget can change over time, to offer more and greater services to the community.

•From time to time, in addition to reviewing the budget, it is necessary to check the way in which tools are being used to identify possible changes in products and thus, make said budget more efficient.

THE MAIN RISK TO A CSIRT IS IN MAKING OPERATIONS SUSTAINABLE, MAINLY DUE TO ECONOMIC RESOURCES, WHICH IS WHY IT IS RECOMMENDED TO NOT BEGIN WITH A LARGE INVESTMENT OR BECOME DEPENDENT ON LICENSING OR PLATFORMS THAT NECESSARILY REQUIRE RENEWAL OR HEAVY INVESTMENT.

Political Support

•Deliver results that are measurable and demonstrate how the CSIRT provides value to the community.

•Make decisions based on data, reports, dashboards, and relevant information.

•Trust in the community will empower decision makers with more tools to maintain CSIRT continuity.

•Partnering with international organizations has benefits such as increasing CSIRT functionality and services, without the need for additional investment.

Communication

•The CSIRT must be capable of articulating, negotiating, and defining different issues related to its mission with organizations; this requires involving decision makers in the business model presented to achieve visible successes for the CSIRT.

•Establish an area, a person in charge, and a communication or press plan to issue incident notifications to either the media or the general public.

•Define communication channels and strategies according to representatives. For example, when communicating with the public, language must be simple and intimate, while when speaking with a technical public, the language must be precise, reliable, and actionable.

6. THE CSIRT OF THE **FUTURE**

The CSIRT of a decade or two ago was a team that revolved in a purely technical niche. Cyber incidents, for the most part, were dealt with based on reports from an affected organization. Currently, the diversity of platforms and the explosive increase in services exposed or connected to the Internet, and that are part of society's daily life, has required CSIRTs to transition from a technical approach to a comprehensive approach aligned with a country's social, economic, technological, and environmental objectives.

THAT IS WHY CSIRTS THROUGHOUT THE REGION MUST BUILD COMMUNITY SERVICES ALIGNED WITH THE PUBLIC POLICIES IN A SPECIFIC COUNTRY OR A SECTOR. IN THIS SENSE, THE CSIRT OF THE NEXT FEW YEARS COULD:

1. Be the national coordinator on a platform to exchange indicators of commitment between your community and other sectoral CSIRTs.

2. Identify the end user as the central axis in designing and developing services.

3. Ensure that users have an understanding (depending on their context) of the impact and benefit of a CSIRT's work.

4. Have a data-driven approach in operations or decision making, based on interpretation and analysis. It is imperative that a CSIRT feeds on actionable information in each of the services it offers to the community. A CSIRT with actionable and timely information will have the ability to increase its response capacity and resilience.

5. Get involved as an active collaborator in the creation, and execute and update national cybersecurity, Governance and Digital Transformation strategies, and public policies that benefit the entire ecosystem. A CSIRT collects and centralizes information on attack patterns, most affected sectors, and institutional response capacity, which is vital for prioritizing guidelines at the national or sectoral levels.

6. Develop incident response capabilities at the national level, including all sectors.

7. Guide the processes and procedures to create agile methodologies that allow for improving response times in the attention of cyber incidents.

8. Develop flexible alliances with partner organizations to, for example, create mechanisms to share cyber threat intelligence and achieve response actions with Internet Service Providers (ISPs), regulators, and/or government authorities.

9. Get involved in creating services that allow for identifying risks before their development and application. Early engagement creates more and better benefits for the CSIRT and the community it serves.

10. Seek job alternatives for specialists to avoid staff turnover, to strengthen sustainability in CSIRT operations.

11. Take advantage of the exponential moment that exists in terms of new technology and new models, to react to incidents.

12. Develop communication skills not only internally and toward decision makers, but also toward the community as a way to build trust.

13. Act as leaders in the sector, achieving results-based recognition.

14. Build and manage robust processes that can be audited.

7. CONCLUSIONS

CSIRTs face challenges that vary according to different circumstances in given times and spaces, but they all have a single goal in common: ensure the safety of their served community. That is why there are tips, recommendations, and best practices that work across the board and are described in this document.

The business model approach can enable creation of a CSIRT, from its inception, in a sustainable and efficient manner. For this, it is essential to clearly define where it will be located and what services will provide the best value for its served community. However, the possibility of stopping, reviewing, and rethinking activities, services, or ways in which an already established CSIRT operates should always be kept in mind.

The fundamental axis that must always be present is trust, which is a key resource in ensuring CSIRT operations and allowing both the sustainability and the necessary development based on 10 points that serve as the foundations for the CSIRT of the future.

It is important to remember that we are within democratic frameworks of action, so CSIRTs must act in accordance with regulations and remember to act within the context of human rights.

Finally, it is essential to highlight that the CSIRTs are part of an ecosystem at the country level, and coexist with other institutions that have different capabilities, so having a clear scope and plan of action for each is essential to enable different actions and to support one other.

Table 2

10 Foundations for creating a CSIRT

1 ORIGIN AND STRUCTURE	2 NEED	3 SERVED COMMUNITY	4 HUMAN RESOURCES	5 BUSINESS MODEL
A CSIRT provides cybersecurity services to prevent, detect, mitigate, and respond to cyber incidents in a defined community. It has an organizational structure with established processes and a catalog of technological tools, as well as a budget, mandates, catalog of services, specialized personnel, network of contacts, and communications plan.	Both public organizations and private companies, military entities, academia, and other organizations that are considered critical infrastructures face cyber incidents and, in many cases, do not have formal procedures to respond to an incident and, in others, lack clear guidance in how to deal with an incident. Given this scenario, a CSIRT is necessary.	The served community are the groups, organizations, or entities to which CSIRT services will be offered. Defining these is essential when starting to plan or create a CSIRT, or when updating it. Among the main ways to attract the served community and create bonds that result in relationships of trust are assistance and support on incidents, consulting, formations, contact and networks.	Some strategic actions are: Recruit staff with soft skills, rather than technical ones; that is, people with critical thinking, analytical, risk-oriented, or strategic mindsets, as it is more difficult to develop soft skills than it is to teach techniques. Do not centralize responsibilities into a single resource. Make agreements with private companies to train personnel working in the CSIRT.	Before forming a CSIRT, it is important to plan and design it with a long-term vision and a plan for sustained growth. This vision will make it possible to identify the key elements to meet CSIRT objectives, as well as to develop clear and measurable indicators that, when met, demonstrate CSIRT effectiveness and justify its existence. It is important to keep in mind that it will not necessarily create monetary profitability but will act as a differentiator by helping build more efficient systems, inspire greater citizen confidence, and minimize serious impact in the event of cyber incidents.
6 ACTIVITIES	**7 FINANCING**	**8 KEY RESOURCES**	**9 VALUE ELEMENTS**	**10 COMMUNICATE**
"Think big, start small, and grow from there." In its early years, a CSIRT should not and cannot operate or offer many services, since doing so (or trying to do so) is one of the main causes of a CSIRT's unsustainability, as each listed service implies operating costs and human resources while faced with limited public budgets. It can start with fundamental services – those of high impact and reach – to the served community, such as providing alerts on existing vulnerabilities, indicators of compromise (IOC), or publication of best practices guides.	Many national CSIRTs do not monetize the provision of their services to the community, so gaining financial attention becomes a creative task. Usually, one organization hosts a CSIRT and that organization, through a public budget, guarantees support for CSIRT general operations and the employees who work in therein. However, to expand or create new services, there are alternatives to financing, including funding from international organizations, project consulting (if allowed), and private sector initiatives, among others.	These are the indispensable resources for the CSIRT to produce, deliver, and manage services and other essential activities. The essentials are: organizational resources; actionable information (this refers to information that can be used without carrying out additional processing to communicate or validate the information must present the relevance, timeliness, precision, completeness, and digestibility that help the CSIRT to take action to identify, prevent, respond, and mitigate cyber incidents; tools to support the value proposition or services, channels and relationships with organizations in the served community; and human resources.	The primary value proposition that a CSIRT makes to its served community is to identify, prevent, respond to, and mitigate cyber incidents. To this end, the CSIRT will offer a series of services that will add value by assisting and advising the served community on cybersecurity issues. These services must be aligned with the held mandate, mission, and vision and also be designed according to the served community.	A story must be told to explain and transmit the model in an attractive way; that is, telling the story through the perspective of the served community, its problems, and its needs. The served community is the protagonist of the story. You should talk about the challenges you face and the tasks you must carry out, emphasizing those aspects where the CSIRT will be relevant. Subsequently, the story must explain how the CSIRT creates value for this community and then describe its services, emphasizing how each service responds to a specific community need. As part of the story, also tell what resources and activities will support the enhancement of the CSIRT.

8. CREDITS

Luis Almagro
Secretary General of the Organization of American States

OAS Technical Team
Luis Fernando Lima Oliveira
Alison August Treppel
Kerry-Ann Barrett
Diego Subero
Sofía Hunter
Volker Esteves

Editors
Andrés Velázquez - MaTTica
Laura Jácome - MaTTica

Expert Contributors
Angus Smith
Carlos Landeros
Carlos Leonardo
Gabriela Ratti
José Callero
Katherina Canales
Lia Molinari
Roberto Lemaître
Samuel Maroon
Wilson Prieto

Design and Layout
María Paula Lozano

Acknowledgments to

Canada

DEPARTMENT OF STATE · UNITED STATES OF AMERICA

9. ANNEXES

9.1 ANNEX A: Differences between CSIRT, CERT and SOC

CSIRT – Computer Security Incident Response Team

A CSIRT, according to the European Union Agency for Cybersecurity (ENISA),[21] is a generic name given to a team that provides a set of both preventive and reactive services that include information sharing, awareness, cyber incident management (core or main services), monitoring, vulnerability management, and cybersecurity knowledge. However, this definition can be adapted at the moment in which a CSIRT is provided a government location, as well as according to its size and the specific services that it will provide.

CERT – Computer Emergency Response Team

CSIRT is also defined by the CERT/CC of Carnegie Mellon University[22] as the service organization responsible for receiving, reviewing, and responding to cyber incident reports and activities; the services they provide are for a defined group of organizations: a company, government, a region or country, or a network of researchers. CERT is, therefore, a registered trademark since 1997.

SOC – Security Operations Center

SOC is normally a group of people within an organization that have processes and technology that allow for security monitoring from a technical perspective. When we see this from the perspective of comparison with a CSIRT, a SOC could be a service that a CSIRT provides to help prevent, detect, and analyze possible cyber incidents or, based on the information it has, to respond to a cybersecurity incident.

9.2 ANNEX B: Considerations in budget creation

Overhead Costs
Staff
Wages
Unofficial Costs
Incentive Programs
Information systems
Equipment (HW)
Licenses
Maintenance, Support, and Improvement
Communications
Training
National
International
Other Training
General Expenses
Rental Expenses
Conditioning and Maintenance
Furniture and Office
General Inputs
External Services
Consulting, Specialized Support
Memberships, Certifications, Taxes
Communications, Promotion and Events
Service Outsourcing
Other Expenses
Insurance, Special Operations

[21] CSIRT Capabilities. How to assess maturity? Guidelines for national and governmental CSIRTs. ENISA, 2015. https://www.enisa.europa.eu/publications/csirt-capabilities/@@download/fullReport

[22] CSIRT Frequently Asked Questions - FAQ. Software Engineering Institute. Carnegie Mellon University, 2017. https://resources.sei.cmu.edu/asset_files/WhitePaper/2017_019_001_485654.pdf

START

SMALL AND GROW

PRACTICAL GUIDE FOR CSIRTs

Volume 2, 2023

A Sustainable Business Model

OAS More rights for more people

CSIRTAmericas Network