IDB
Inter-American Development Bank

Cyber Security Strategy Review for Paraguay

August 2018

CYGOV
Intelligent Cyber Security

CyGov for IDB: Gal Shmueli, Nir Peleg
gshmueli@cygov.co, npeleg@cygov.co

Document Administration

Lead Assessors: Gal Shmueli, Nir Peleg

Approved By: Yair Solow

Version	Date	Notes
1	29/06/2018	Drafting
2	12/07/2018	Editing - Goldie
3	19/07/2018	Approved by Cygov
4	30/07/2018	Approved by IDB
5	01/08/2018	Delivered
6	03/10/2018	Corrections from PY
7	16/10/2018	Corrections after presentations in Paraguay
8	10/11/2018	Added new Organizational chart

Table Of Content

Document Administration 2

Acknowledgements 7

Executive summary 8

Required Budget 11

Cert-PY – Human Resources Budget 12

SOC-PY – Human Resources Budget 12

Overview 13

Document Methodology 13

Terminology and Definitions 14

Acronyms 14

Current Status – National Level Organizations and Strategy 15

Organizations and Sectors 15

Organizations: 15

Regulators per Sector: 15

Stakeholders: 16

Paraguay Cyber Threats/Risks Landscape 16

Major Threats 16

Threat Actors 17

Threat Vectors 17

Incidents 17

Regulations and Legal 17

Regulations 17

Legal 18

National Level Cyber Strategy 19

1. The public Sector – The Government Domain.. 20

2. The Private Sector – Focus on Critical Infrastructure 20

3. Capacity Building.. 20

National Relevant Projects 21

SOC-Py (potential).. 21

CERT-Py 22

SII 22

ISP (gov) 23

Government Cloud (gov-cloud) 24

Identified Gaps 25

1. Budget 25

2. Roles and Responsibilities 25

3. Critical Infrastructure Definitions 26

4. Critical Mass of People 26

Operational Level – CERT-Py and SOC-Py 26

Capacity Building... 26

5. Minimum Baseline Standards and Guidelines (government sector)............ 27

6. Regulation 27

7. Legal.. 28

8. Information Sharing and Partnership with the Private Sector 28

9. Ability to Execute Defined Cyber Strategy... 28

10. Government Infrastructure... 29

Recommended Principles.. 30

Phased Approach 30

Strong Start 30

Shared Responsibility between Government Offices 30

Goals and Measurements 31

Roles, Responsibilities, Authority and Definitions 31

Recommendations – National Strategy and Implementation 32

Strategic 32

National Cyber Security Strategy 32

Find a Cyber Security Champion within the government structure 32

Appoint a National Cyber Security Manager at the relevant position 32

Perform Capacity Building - Start with the Human Capital 33

Establish the SOC-Py Project 33

Prioritize and Approve National Cyber Security Strategy Action Items 33

Plan and Monitor Implementation of the National Cyber Security Strategy Prioritized Goals 35

Provide Budget for the National Cyber Security Strategy 36

Complete required Cyber Security Definitions 36

Conduct Annual National Cyber Security Review 36

Perform Gap Analysis on the Cybercrime Justice Process 36

Perform Gap Analysis with respect to the Budapest Convention 37

Consider Cyber as an Opportunity 37

Roles and Responsibilities 37

Define Responsibility and Authority for the Relevant Cyber Security Body 37

Appoint a Government CIO 38

Separate Roles of Plan, Operate and Control in SENATICS 38

Legal ... 39

Adjust Appropriate Law for the New Cyber Security Body ... 39

Regulation ... 39

Approve a Cyber Regulator for the Energy Sector ... 39

Consider to Appoint a Regulator for the Energy Sector ... 39

Standards and Guidelines ... 39

Define Set of Cyber Standards, Guidelines and Security Framework ... 39

Operative ... 40

Train the Trainer’s Program ... 40

Centralized DNS and DNS Filtering ... 40

Centralized Services ... 41

Perform Annual Cyber “War Game” for the National Level ... 41

Recommendations – Prioritized and Staged ... 42

Total Cost and Resources ... 44

Appendixes: ... 45

Meetings List ... 45

Law of SENATICS ... 45

National Cyber Strategy Program Document ... 47

Critical Assets and Systems List ... 47

SENATICS Organigram – August 2018 ... 50

SENATICS Organigram – November 2018 ... 51

Types of Computer Network Operations ... 52

Acknowledgements

CyGov, on behalf of the IDB (the Inter-American Development Bank), would like to acknowledge and thank SENATICS for their full cooperation and utmost attention provided to us during the consultation process.

Specifically, we would like to thank Ms. Gabriela Ratti for her assistance in coordinating our visit to Paraguay for and providing us with highly valuable insights.

Additionally, we would like to thank other members of SENATICS, Mr. Robert Insfran and Mr. Herman Mereles for their involvement during the week we spent in Paraguay. We would also like to thank the staff of SENATICS that was very helpful in making our visit as convenient as possible.

Executive summary

The following two reports are based on research of Paraguay that we conducted prior to our arrival, our conclusions from valued meetings - organized by our SENTICS hosts - with several stakeholders, and our vast experience in strategic cyber policy, program building, and implementation of those programs and projects.

We have met with a highly motivated team and stakeholders seeking for a more cyber-secured Paraguay. Although the paper addresses many existing gaps, we wish to stress that we have observed many positive factors in terms of people and processes, but those are given less expression in this work for understandable reasons (the goal of this paper is to *improve* the current state).

Although we will focus on the most important recommendations in the executive summary, we highly recommend that the report be read in its entirety as it includes many additional detailed recommendations. One may also prioritize the recommendations differently from the way we have prioritized them, and therefore it would behoove him to read the entire report and come to his own conclusions.

We would like to stress that since cyber buildup takes time ("Rome was not built in one day") and since the recommendations are considering the budget situation in Paraguay the above recommendations are considered to be "Phase I" of a more strategic effort to protect Paraguay from cyber threats. "Phase II" of this strategic effort may include sectorial SOCs for critical infrastructure, more sophisticated plans for capacity buildings involving the ministry of education, deeper protection for government assets and so on.

From a strategic point of view, we would like to stress the following recommendations:

Leadership Support

Cyber strategy is such an important issue that the role of leadership is critical. Strong support from leadership will help progress the implementation process and solve issues that will undoubtedly arise between the different government offices and between the public and private sector. The leadership role is also to ensure that the necessary resources are available to perform and sustain the cyber program.

Capacity Building

Cyber security is mostly based on people (with technology and processes following closely). This means that building a professional workforce is critical for the success of the program. We have placed the capacity building recommendations only second to the need of leadership support.

Staged Implementation

The remaining recommendations are prioritized according to our expert opinion. We highly recommend that the implementation be done in a staged manner. It is better to have small but successfully completed objectives than to set high level goals that are never achieved. Careful implementation of the recommendations must ensure that each recommendation be broken into smaller, achievable and measurable goals.

From operational point of view:

CERT-Py

We recommend to stabilize the CERT-Py team to be able to carry out incident response activities on already occurring cyber breaches. The recommended size of team is 6 people which means a perpetual annual budget of $90K.

SOC-Py Project

We recommend proceeding with implementing the SOC-Py project with the resources we have recommended. The SOC-Py can be implemented in parallel to the implementation of our strategic recommendations. As the SOC-Py is more of a technological implementation, it requires different skills and can progress faster. It also sets a better stage for some of the strategic recommendations. Our estimation of the project cost and resources is $2M for a period of 3 years, with a perpetual annual budget of $160K.

Required Budget

No	Topic	2019 ($,000)	Perpetual ($,000)
1	CERT-Py – Human Resources	60 + 30 (Training)	60 + 30 (Training)
2	SOC-Py – Technological Project	667	667 for 2 years
3	SOC-Py – Human Resources	110 + 50 (Training)	110 + 50 (Training)
4	Training Center - Human Resources	15.6	15.6
5	Training Center - Budget		
6	Capacity Building – Human Resources	15.6	15.6
7	Capacity Building - Budget		
8	Budget for the National Cyber Security Strategy		
	Total:		

⇒ **Empty budget lines should be filled during the strategic process conducted according to the recommendations in this report.**

Cert-PY – Human Resources Budget

- Phase I Recommendation (Minimum):
    - Budget:
        - 6 people, $60K (Annual)
        - Training budget $30K (Annual, $5K per person)
    - 2 x Tier 3, 4 x Tier 1
    - Outcome:
        - One incident response team 24x7
        - Infrastructure, capacity building
- Phase II: To be defined in 1-2 years.

SOC-PY – Human Resources Budget

- Phase I:
    - Budget: 6 people, $57.2K (Annual)
    - Training budget $30K (Annual, $5K per person)
    - 1 x Manager, 2 x Tier 2, 3 x Tier 1
    - Outcome: 8x5 operating SOC (8 hours, 5 days a week)
- Phase II:
    - Budget: 11 people, $110K (Annual)
    - Training budget $50K (Annual, $5K per person)
    - 1 x Manager, 2 x Tier 3, 2 x Tier 2, 6 x Tier 1
    - Outcome: 24x7 operating SOC

Overview

Document Methodology

The methodology used to create this action plan is based on a practical approach which considers the different strengths and constraints which are unique to the Paraguay cyber ecosystem.

We have separated the project report into two main documents:

1. **Cyber Security Strategy Review for Paraguay (this document)**

   The first document elaborates on our understanding of the Paraguay government system with respect to cyber security. Our recommendations are divided into two levels: (1) Strategic Recommendations – these recommendations require attention and decision making from Paraguayan leadership and involves consideration of strategy, budget, structure, legal, legislative activities and so on; (2) Operative – these recommendations are aimed more on the execution, yet still they require attention and resources in order to be actualized.

   Although the document is high level, and strategic by nature, we have included practical, detailed recommendations whenever possible, to provide actionable steps to ensure achievable results.

2. **The SOC-Py Project for Paraguay**

   The second document is a detailed paper on the implementation plan and considerations for the SOC-Py project, including budget and resource estimations.

Terminology and Definitions

Acronyms

SENATICS	Secretary for Information and Communication Technologies
ISP	Internet Service Provider
IAAS	Infrastructure as a Service
PAAS	Platform as a Service
SOC	Security Operations Center
IOC	Initial Operational Capability
CERT	Cyber Emergency Response Team
CI	Critical Infrastructure
CIRT	Cyber Incident Response Team

Current Status – National Level Organizations and Strategy

Organizations and Sectors

We've identified the following organizations in Paraguay that are relevant to the National cyber security landscape and stakeholders:

Organizations:

1. Top leadership organizations - The Presidential administration, relevant for national priority, budget allocation, legislation and crisis national management.
2. Responsible Ministries - The Ministry of Communication and Information (current).
3. Operational organization relevant to cyber security - SENATICS, responsible for operating the CERT-Py and serves as the point of contact for the government cyber security. Additionally, SENATICS manages the government IT central services such as the government cloud and the data interchange highway project (IIS).
4. Police: Responsible for cybercrime investigations and for implementing the Budapest Convention.
5. Justice Ministry: Responsible for the prosecution of cyber criminals.

Regulators per Sector:

1. Communication Service Providers - CONATEL
2. Private Banks - Central Paraguay Bank
3. Energy/Electricity Regulator – none

4. Privacy Regulator - none.

Stakeholders:

1. ISPs - Most of the ISPs managing the main communications infrastructure are private while one ISP ('COPACO') is a government-owned company.
2. The Energy sector - Comprised of electricity companies that generate and distribute electricity. Some examples of large companies are ITAIPU (producer of electricity for Brazil and Paraguay) and ANDE (transmitter & distributer of electricity).
3. The Banking Sector – There are 16 private banks and one public, Private Bank Association.

There are other relevant organizations aside from those listed above, however, we have focused on those that are most important and relevant to national cyber security posture, gap analysis and remediation implementation.

Paraguay Cyber Threats/Risks Landscape

The threats and risks mentioned in this section are not in place of a deep and thorough assessment that must be done (and updated annually) by the team responsible for the strategic issues of cyber security for Paraguay. Nevertheless, the items discussed here are a result of our findings from the different meetings we have taken and the research conducted on the IT landscape of Paraguay. The importance of setting a reference threat is to ensure that all relevant stakeholders are aligned on the issues, and to keep focus on the problem we are aiming to solve.

Major Threats

1. Cybercrime
2. Global cyber threats
3. Regional threats imposed by the reliance on infrastructure from Brazil and Argentina (for example, telecom and electricity).

Threat Actors

Identifying the threat actors did not fall under the scope of this work, and no attempt has been made to identify the threat actors.

Threat Vectors

Two main threat vectors:

1. **Internet threats** - Due to the high connectivity of the networks, the sensitive data being transferred, and the government services offered such as ISP, web hosting, email hosting, banking etc., the exposure to threats (such as cybercrime and cyber terror risks) is similar to most connected organizations.
2. **Insider threat** – Corporate data breaches and leaks caused by malicious users or employees, resulting in the loss of credentials. Both a deliberate attack, such as phishing or theft, and a careless action from an employee, such as inviting malware into the system by opening a bad link or unknowingly bringing an infected device to work, present a major insider threat.

Incidents

There are several known incidents of threats against the Paraguayan government networks and systems, and we can assume that there must be many “unknown” incidents as well. This situation will continue unless the “cost of doing cybercrime” will be raised and good deterrence and effective cyber security measures will be implemented.

Regulations and Legal

Regulations

There are several sectors that are most relevant to cyber security and therefore must be regulated:

Financial Sector – Central Bank of Paraguay

The Central Bank of Paraguay is the official regulator for the banking sector. Additionally, there exists an informal group of private banks that is sharing information regarding fraud and security incidents.

Energy – None!

The energy companies are self-regulated, as no formal regulator for the energy sector exists.

Some of the energy companies are conforming with Brazilian regulation (Brazilian-Paraguayan companies).

Telecom – CONATEL

CONATEL is the formal regulator of the telecom sector. In addition to its role as a regulator, it is also responsible for approving operational licenses for the mobile and internet operators.

Government IT – SENATICS

SENATICS has many formal roles and holds a mandate to define some policies but it is not an actual regulator. Even so, SENATICS is not using its current authority to its full capacity to promote or enforce the use of IT and cyber security policies in the government offices.

We've chosen the above sectors because they are the most fundamental sectors that cyber relies on: **Finance, Energy, Telecommunications, and Government**. These are also the fundamental pillars of many state processes. Together, these sectors construct the critical services of normal state operation, and are highly dependent on networks and digital systems, thereby proving their importance.

Legal

The legal posture of Paraguay in regard to cyber security is influenced by the following factors:

Paraguay has signed and joined the "Budapest Convention" for fighting cybercrime, necessitating the implementation of a few derivatives in the Paraguayan system to ensure compliance with the requirements of the Convention. See also Cybercrime policies/strategies[1] for a legal perspective of the Budapest Convention for Paraguay.

The Paraguayan prosecution and justice systems are not mature enough to deal with cybercrime. From our observation, the current level of professional capacity is insufficient in the areas of evidence collection, digital evidence, forensics investigation, and cybercrime prosecution.

Based on our observations, **there exists an informal relationship between SENATICS and the police and the justice system regarding cybercrime**. In order to have a working, efficient judicial process, there must be formal relationship between the relevant stakeholders with respect to their roles, responsibilities and authority.

National Level Cyber Strategy[2]

The National level cyber strategy was conceived on April 24, 2017 and appears in the National cyber strategy Program document[3]. Since its approval, there have been no meetings, nor any steps taken, regarding practical implementation of the national cyber security strategy.

The national cyber security strategy is comprehensive enough for Paraguay, and there is an urgent need for high-level government leadership to push for its implementation with all relevant stakeholders.

Under the approved **National Cyber Strategy**, we've identified an important opportunity with the establishment of a **National Cyber Security Committee**.

[1] https://www.coe.int/sl/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/paraguay/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=print&_101_INSTANCE_hFPA5fbKjyCJ_languageId=sl_SI

[2] We did not go into municipal level

[3] https://www.presidencia.gov.py/archivos/documentos/DECRETO7052_5cq17n8g.pdf

This committee will play a major role in supporting and monitoring the implementation of the national cyber security program by removing and resolving obstacles, while allocating and prioritize adequate relevant resources. This committee can be a source of authority for SENATICS and can serve as the national board of cyber in an effort to help progress Paraguay's cyber security plans and projects.

We've identified three main areas of focus for the national cyber capacity building plan:

1. The public Sector – The Government Domain

Protection of the government digital assets, networks and government digital services. The top priority should be on investing in more security personnel.

2. The Private Sector – Focus on Critical Infrastructure

Protection of the critical assets of the private sector, mainly defined as national critical infrastructure such as **energy, water**, **banking, financial services, and telecommunications**. The main organizations and stakeholders for these private sectors should be identified, and a cyber security guidance document should be created using a risk-oriented cyber security approach to set the minimum baseline of cyber security regulation for that sector.

Additionally, the National CERT and SOC should work closely with these organizations, cooperating on cyber threat mitigations, best practices, information sharing and incident response.

3. Capacity Building

As mentioned above, there is a substantial gap in the cyber security personnel in SENATICS and in the relevant government offices. In order to address this issue, capacity building activities must be PLANNED and EXECUTED as part of the annual work plan of the Cyber Security Committee.

Capacity building is mainly about people, education and professional training programs. A collaboration of the government with the private sector and the academia is highly recommended.

National Relevant Projects

SOC-Py (potential)

As a major part of the framework in Paraguay Cybersecurity Strategy, the National Secretariat of Information Technology and Communication (SENATICS), is aiming to launch its project of a Cybersecurity Operations Center Paraguay (SOC-Py). The **SOC-Py** is considered an important pillar and a commitment for implementing the National Cybersecurity roadmap.

The SOC Project has the following main objectives:

1. **Managed Detection and Response** - The SOC-Py will offer managed security services focused on detection, situation awareness and response **for the government administrations,** based on the dedicated SOC-MDR model. The following services will be planned: security monitoring, threat and vulnerability management, operating security systems and sensors, incident response (mainly remotely).
2. **Enhance CERT-Py capacities and services** - The SOC-Py will work closely and support the CERT-Py to empower its security services and to **create security synergy** between the **public and private sector**. The concept of the SOC with the CERT is to create a critical mass of personnel, knowledge, and security operations under the same roof as the national center for cyber security.
3. A **Cyber hub of Knowledge and Training - A Training center** for professionals. Offering courses and hands-on experience from real-life incidents and threats, along with events analysis, the hub will create and maintain a knowledge base for the lessons learned from past events and the

changes to current standards, policies and procedures. The training center will then train professionals according to those updated materials.

We've addressed the SOC-Py project in a dedicated paper of the submitted work.

CERT-Py

CERT-Py is an established group and is the organization responsible for investigating cyber incidents that were detected or reported to the SOC-Py.

Currently, from our observation and in our expert opinion, the CERT-Py team is understaffed, and is unable to effectively mitigate the cyber challenge at a national level.

SII

Based on the Estonian model, the SII project creates a "data bus" between various government offices, enabling the use of existing government data between the different offices, making government processes much more efficient.

Although this infrastructure is very important from a functional point of view, it exposes the critical data and systems to cyber risk. Some of the identified cyber risks during our review were: (1) lateral movement between government systems using the "data bus"; (2) local copies of databases, limiting the ability to prevent data leakage and data leakage investigation.

We highly recommend that the implementation of the SII project be accompanied by a "red team" who will perform a cyber security review of the architecture and implementation, as well as a pen-testing activity and report.

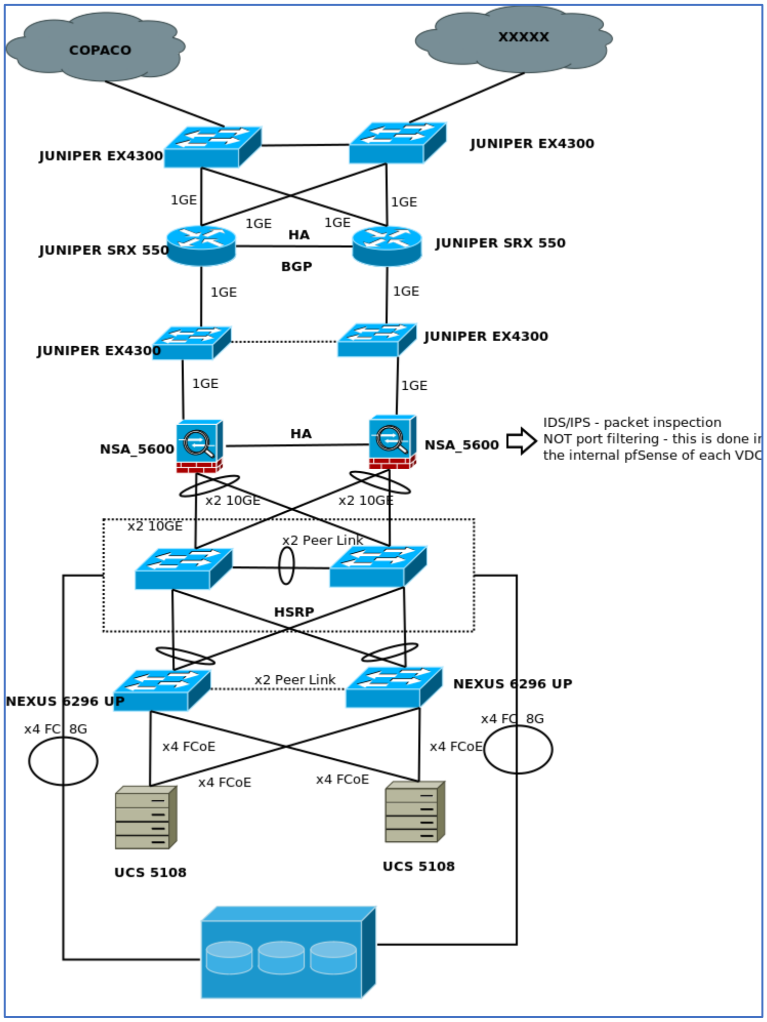
ISP (gov)

The government ISP ('COPACO') is an Internet Service Provider that supplies connection services to the different government offices. COPACO is responsible for some services (like DNS) and may be potentially relevant for the cyber security of the government sector. For example, they employ a RadWare firewall service that also protects from DDoS attacks.

The gov-ISP budget is globally set and is paid by an annual budget from the central government.

There is a presidential guideline that requires all government offices to use the gov-ISP. This is a good first step, as it can set the groundwork for performing cyber security visibility, monitoring activities and setting policies using the ISP. This guideline demonstrates the importance and the presidential administration's prioritization of the issue, along with the high-level management support necessary to ensure implementation.

Government Cloud (gov-cloud)



The government cloud is a central project providing cloud-like virtual services. The services are focused on IAAS and PAAS cloud models. The gov-cloud infrastructure is based on COTS (Common Off the Shelf) equipment and software with support.

Government offices using the gov-cloud are not paying for the use, and many of them use the gov-cloud as a central or redundant VDC (virtual data center) and for WEB hosting services.

There is no presidential order or any other regulation directing the use of the gov-cloud.

Identified Gaps

1. Budget

Budget allocation for cyber security activities should be well planned and must be sustainable in order to reflect a long-term priority of the government. The budget enables the building of a sustainable operational process with qualified personnel and continuous improvement.

We didn’t identify any specific criteria for budget allocation of cyber security activities in the SENATICS budget.

There is no apparent alignment between the national cybersecurity plan and the budget to implement its roadmap.

Additionally, the government administrations are not participating in the IT costs or the cyber security costs for central IT or security services, and all of their IT and security needs are being funded by SENATICS’ budget.

2. Roles and Responsibilities

It is our observation that roles and responsibilities are not clearly defined, from the strategic level to the formal level, and down to the operational level.

There is no **central authority or entity that is responsible for the national level cyber security strategy, implementation and capacity building.**

SENATICS’ formal role in cyber security relates **only to responsibilities in the governmental domain**, and even in that capacity, it holds no clear authority for publishing directives for minimum standard implementation.

There is no government body appointed as responsible for data privacy of sensitive information.

3. Critical Infrastructure Definitions

There is no clear definition of national critical infrastructure and assets. In Paraguay, there are certain sectors which include government entities as well as private companies that operate and maintain critical assets with vulnerabilities to cyber threats. There is a need to analyze and identify the CI (critical infrastructure) from a risk and national impact analysis perspective. Organizations that operate and maintain critical assets must be accompanied by cyber security regulation, government cooperation, periodic assessment reports etc.

4. Critical Mass of People

Critical mass is the minimum number of people needed in order for an initiative to be effective or achieved at all. The currently available number of people for the CERT and the SOC is much beneath the required critical mass, resulting in less effective operations.

The current work force is comprised of two (2) individuals, including one manager, who are occupied with multiple tasks including strategic planning, IT operations, cyber operations, infrastructure building, workforce training, assisting law enforcement, working with relevant sectors and more. The lack of qualified personnel results in a non-effective workforce, where each person is forced to handle both operational duties and capacity building, along with many administrative duties.

Operational Level – CERT-Py and SOC-Py

Understaffed and unable to perform the relevant activities.

Capacity Building

Understaffed and unable to perform activities relevant to the national level.

Insufficient consistent training activities.

No personnel certification program.

Insufficient incentives for the professional staff to earn professional certifications.

5. Minimum Baseline Standards and Guidelines (government sector)

There is no set of defined standards or even guidelines for the government sector. This lack makes it difficult to establish a **“baseline of defense”** which is critical and very effective. The must be a baseline that can be **measured for compliance** in each administration, thus giving good situational awareness and creating a common language. This effort will also help to promote and perform cyber security monitoring activity as each network will have common baseline and structures.

No defined framework is used or regulated (or even recommended) for the government institutions. There is a work in progress about this topic in SENATICS.

6. Regulation

The use of the regulatory authority (wherever available) is very limited to unused. For example, CONATEL is not utilizing its regulatory authority to enforce any kind of cyber security requirements from the ISPs. In fact, CONATEL could enforce cyber security requirements also in its capacity of issuing operating licenses and could be requiring each ISP to comply with certain standards of cyber security. But CONATEL doesn’t require or enforce any such standards under either of its roles.

Some sectors, like the energy sector, don’t have a regulatory body. Although this is a clear problem, there is no quick resolution as it requires changes in legislation.

Some of the organizations that we met emphasized the importance of a regulator or a policy enforcement body. The absence of the legal requirements for compliance creates an obstacle when trying to receive money to be allocated to handle cyber security issues.

7. Legal

There is no regulator, laws or regulations surrounding data privacy which is critical when organizations are handling sensitive data.

There is a need for the basic training and/or workshops about cybercrime for judges and prosecutors.

The law enforcement is focused mainly on the "what" (has happened) and the "who" (did it), where the cyber security perspective is different and requires additional questions to be asked such as: How it was done?, could it have been PREVENTED? Could it have been IDENTIFIED earlier? Should it concern other SECTORs?

8. Information Sharing and Partnership with the Private Sector

There is no established program for information sharing with the private sector.

There are some initiatives by the private sector (specifically banking) for information sharing among themselves regarding security and fraud incidents.

There is great NEED stated by the various stakeholders (energy, financial, telecom etc.) to have a secure mechanism for trusted information sharing regarding cyber threats, incidents, and best practices.

9. Ability to Execute Defined Cyber Strategy

The current defined national cyber security strategy is comprehensive and expands to many important domains. In a limited resources environment, there is a critical need to prioritize the most important steps that are practical in their potential to implement. A focused implementation plan will lead to successful results, enabling the continued success at implementing the rest.

In the cyber security environment, the threat actors and the threats change rapidly over time. It is not enough to have a defined cyber security strategy, it is also important to have a mechanism in place for reviewing the present situation and adjusting the cyber strategy accordingly.

It is also important to have effective government mechanisms to perform the plan. These mechanisms need to be monitored and managed as well.

10.Government Infrastructure

There is no formal policy used for the government IT infrastructure except that the internet connection should be through the government ISP.

There is no formal cyber security and IT policies.

Each office is responsible for its individual IT hardware, software and applications.

There is minimal use of Domain Controllers (DC) for access management and monitoring, a problem from a managed security perspective.

Offices are not paying for the use of the government infrastructure (ISP, cloud), making it difficult to maintain the quality without proper budget.

Recommended Principles

Phased Approach

Regardless of the cyber security strategy chosen and its long-term goals, it will clearly demand extensive resources and executive attention. We believe that creating a realistic, sustainable action plan calls for a phased approach in which the various required actions shall be executed gradually over time. This enables the right prioritization as well as enabling real and measurable progress while focusing on the most pressing issues.

The stage of the phased approach should be planned with minimal requirements that fit the resources at hand and with clear measurements for success. This approach enables progressing in “small” and measurable steps, performing closed cycles of lessons learned and improving the ability to accomplish the next phases in a more efficient manner.

Strong Start

The National Cyber Strategy must become a prominent plan in Paraguay, and SENATICS must fulfill its role as the coordinator of the cyber security activities and the professional authority. From our experience, this can only be achieved if SENATICS commences its operations with strong political support and an appropriate budget, both of which will contribute to cultivating a prestigious image which will ensure the attraction and ability to recruit talented professionals.

Shared Responsibility between Government Offices

Cyber security is not a standalone activity. It is a highly complex problem that requires the support and help from all participating stakeholders. Therefore, it cannot be considered as the sole responsibility of SENATICS. Each of the government ministries must be gradually held responsible for its own cyber security posture.

SENATICS's role is to guide each of the ministries to achieve its goal of enhanced cyber security readiness while maintaining overall accountability.

Goals and Measurements

Each phase of the action plan requires clearly defined goals. For each goal, the definition of clear KPIs (Key Performance Indicators) is critical in order to measure progress and ensure goals are achieved.

Roles, Responsibilities, Authority and Definitions

We believe that it is crucial to make refined and accurate definitions for the cyber terminology (e.g. what is a cyber breach).

It is essential to define the roles and responsibilities for the different aspects of the cyber strategy while giving authority to the relevant stakeholders.

Recommendations – National Strategy and Implementation

Strategic

National Cyber Security Strategy

Find a Cyber Security Champion within the government structure

The most important issue when considering a cyber security plan is to find a powerful Champion that can lead the cyber security plan and strategy as a government plan. The cyber security topic is very complex, not only from the technology and required resources but also from the required involvement of many different government offices. This calls for a person – champion – that has enough influence to perform this duty and be able to reconcile or influence the government administration.

In the long-term, Paraguay needs to consider an establishment of a national cyber security authority that will be responsible for these topics, from strategy to operational implementation and capacity building.

Appoint a National Cyber Security Manager at the relevant position

After finding the champion, Paraguay will need to appoint a **National Cyber Security Manager** that will be responsible for the day to day execution of the Cyber Security Plan.

The National Cyber Security Manager will also be heading the **National Cyber Security Committee,** which will be built from the different stakeholders from the public sector, as well as select members from the private sector. This is the steering committee responsible for planning, executing and monitoring the different cyber security activities.

Perform Capacity Building - Start with the Human Capital

Capacity building is the most crucial task when you want to build a sustainable cyber security strategy for any country. This is also true for Paraguay. As mentioned before in this work, the cyber security strategy is built from People, Processes and Technology. The one thing that a country relies on and cannot be accomplished by budget or more work is professional People. A plan must be defined to develop people's skills and experiences as a long-term effort, alongside a recruitment plan. The capacity building plan should be monitored from the strategic level and be given the most attention and resources.

Establish the SOC-Py Project

The establishment of the SOC-Py project is essential to creating the operational cyber security capacity in the government, developing skills and knowledge that will potentially influence many other partners in the government as well as in the private sector. We highly recommend allocating the adequate resources (people and budget) and igniting the project as recommended in our detailed document.

Prioritize and Approve National Cyber Security Strategy Action Items

This work is based on Plan Nacional de Ciberseguridad – Ejes, Objetivos y Acciones (Autoguardado).xlsx

The following table is an example of prioritization effort we have conducted with the SENATICS team. The priorities given from the complete list can be approved or changed, but the decision process itself, evaluating priority levels and making decisions, is a crucial part. The decision on a small, yet achievable set of goals is important for making progress while getting a feeling of "things are done". We will name the approved objectives from now on as the National Cyber Security Strategy Prioritized Goals.

Ejes	Objetivos	Líneas de Acción	Remarks
1. Awareness and Culture	1.a. Public awareness campaigns are recognized and promoted by the general public, and knowledge and safe behavior in cyberspace are improved.	1.a.2 Develop thematic campaigns of public awareness among diverse demographic groups in Paraguay in partnership with the private sector, civil society and academia.	
3. Protection of Critical Infrastructures	3.a. Critical Paraguayan infrastructure is resilient to cyber threats and guarantees the stability of essential services.	3.a.1 Create a database of all critical infrastructure (public and private) with critical information systems.	
4. Ability to respond to cyber incidents	4.c. The unit responsible for the incident response has an infrastructure and the appropriate tools to conduct their respective tasks in a timely and efficient manner.	4.c.1 Strengthen the technical resources and infrastructure of the CERT-PY to better coordinate at the national level with all stakeholders.	
5. Ability to Investigate and Prosecute Cybercrime	5.a. The agents responsible for the investigation of computer crimes are trained and possess the necessary	5.a.1 Develop and implement a training program for law enforcement in cybercrime, including testing	

Ejes	Objetivos	Líneas de Acción	Remarks
	knowledge to conduct their work.	and digital forensic analysis.	
6.b. The governmental cybersecurity efforts are coordinated with each responsible agent aware of their role and role regarding cybersecurity.	6.b.1 Establish by regulation a National Cybersecurity System, which includes a National Coordinator and a National Cybersecurity Commission. When the need arises, Thematic Working Groups will be set up where representatives from different sectors (public, private, academic and civil society) will be invited.		This is also referenced in our recommendations Appoint a National Cyber Security Manager at the relevant position

Plan and Monitor Implementation of the National Cyber Security Strategy Prioritized Goals

Similar to any other project, a more detailed plan of the approved goals must be made. The level of detail must be sufficient for determining the necessary budget and resources needed to achieve the goals, as well as for allowing the performance of high level monitoring of the plan's progress.

Provide Budget for the National Cyber Security Strategy

There are two levels of budgets that must be approved. The above-mentioned budget is for the approved annual plan of the National Cyber Strategy. The second budget is a higher-level planning budget, looking at the National Cyber Security effort as a multi-year plan and providing it with a sustainable budget. The existence of such a budget enables a long-term, multi-year planning effort that is crucial for a complex issue such as the National Cyber Security.

Complete required Cyber Security Definitions

On the strategic as well as the operational level, many definitions of roles, responsibilities, processes and events are missing. An effort should be conducted to create the necessary definitions, enabling the clear implementation of processes, boundary lines between organizations and so on.

Conduct Annual National Cyber Security Review

There should be an annual presentation of the National Cyber Security Posture of Paraguay, managed by the highest levels of the Paraguayan Government. The content of this event should include issues such as defined "Threat Reference" and accompanying intelligence updates, a National Cyber Security Plan progress update, the National Cyber Security Plan for the upcoming year, major incidents and lessons learned, and major challenges.

Perform Gap Analysis on the Cybercrime Justice Process

The readiness of the justice system for the evolvement of the cyber security and cybercrime threat is unclear. As the justice system holds an integral part in the prosecuting of cyber criminals and bringing them to justice, we recommend **performing a gap analysis on the justice process** including digital investigation, digital evidence gathering, attribution, prosecution, relevant laws and cyber expertise made available to the judges.

Perform Gap Analysis with respect to the Budapest Convention

Another identified gap is the implementation of necessary controls that result from the signature of the Budapest Convention for fighting cybercrime. We want to emphasize that this is a good opportunity for Paraguay to progress on its own fight against cybercrime.

We recommend performing a gap analysis on the requirements of the Budapest Convention for fighting cybercrime and the Paraguayan system in order to identify and prioritize implementation phases to ensure compliance with the Convention requirements.

Consider Cyber as an Opportunity

We have become accustomed to thinking about cyber security from a threat perspective, yet it would be prudent to consider cyber and IT as an opportunity for progress. The reliance on computers and data technologies creates an opportunity to offer better services to the people, along with allowing organizations to implement technologies with relatively low costs of investment. We were shown the innovation program (named "#{innovandopy}") and the digital Paraguay project which are great examples of how the approach of leveraging technology can drive big success.

Roles and Responsibilities

Define Responsibility and Authority for the Relevant Cyber Security Body

A clear and formal definition of roles, responsibilities and authority must be made in accordance with the National Cyber Security Plan.

Formal definitions are critical to ensure a clear understanding of the responsibilities of people and organizations, in order to eliminate overlapping positions and also to ensure that no issues falling between the cracks.

The definitions of roles, responsibilities and authority can be broken down to a level that includes system/project life cycle. This could include: set policies, requirements definition, make/buy decisions, development, maintenance, support and so on.

Appoint a Government CIO

A Government CIO role is missing from the current structure of the Paraguayan government, a role that is responsible for setting the ground rules of doing IT operations in the different offices. As the IT operations are decentralized, a common professional ground must be set, including mandatory standards, policies, and guidelines to be used across government offices.

Once this function is achieved, the work on cyber security becomes much easier as the processes, technology and network topology are all in accordance with the required standards, although there is still much work to be done.

Separate Roles of Plan, Operate and Control in SENATICS

As the current team in SENATICS is very small, the work is being done with “all hands-on deck”. As more people are recruited, we recommend separating the different roles of planning from operations. We also recommend that the team will only be responsible for cyber security issues and not daily IT activities.

Legal

Adjust Appropriate Law for the New Cyber Security Body

Current laws must be checked to see that they encompass the needs of the new Cyber Security Body (or SENATICS with their revised role).

See also: Perform Gap Analysis on the Cybercrime Justice Process

Regulation

Approve a Cyber Regulator for the Energy Sector

A cyber security regulator is crucial for the energy sector in order to set the mandatory standards for all energy companies, to be a point of contact (POC) in the case of a suspected cyber threat, and to be a point of knowledge transfer between energy companies and other related sectors.

Consider to Appoint a Regulator for the Energy Sector

In a broader scale, there is no regulator for the energy (not only for cyber) Paraguay should consider whether it would be wise to create a government regulator for this sector.

Standards and Guidelines

Define Set of Cyber Standards, Guidelines and Security Framework

As mentioned in Appoint a Government CIO, as there needs to be someone defining mandatory standards, policies and so on, with cyber security, there MUST exist a person with the ability to set the mandatory standards, policies, procedures and guidelines to be used across the public sector.

Another important activity is to select the security framework that will be used in the public sector, such as NIST or ISO. The process of implementation of the framework in the public sector will require attention and resources in order to customize the framework to better fit the Paraguayan system.

Operative

Train the Trainer's Program

Once the training center at the SOC-Py (see SOC-Py (potential)) is established, we recommend considering a "train the trainers" program. This kind of program enables a much more scalable growth of cyber security professionals. It uses the strength of the SOC and CERT personnel to engage in training people that will be responsible for training other individuals. This kind of program has proven itself in many different countries. Still, it requires close attention to good and qualitative implementation.

Centralized DNS and DNS Filtering

We believe that a "quick kill" for improving the cyber security status (Prevention) while providing more information for the SOC (Detection) could be the use of DNS Filtering solution. This solution can be implemented quite easily from the technical perspective. It does require that government offices configure their primary DNS to the government DNS, which will enable the DNS filtering function (probably to be hosted at COPACO).

Quoting from an explanation about DNS filtering from the web: "DNS filtering is designed to combat malware, spam, child pornography and other dangerous sites on the web. In those cases, the DNS server filters the request and blocks it rather than return an IP address. It is also useful for organizations that want to protect internal assets by blocking known malicious sites. This function is normally conducted at the router level by blocking IP addresses or filtering ports. For those without the luxury of high-end routers, DNS filtering is great alternative."

Centralized Services

We strongly recommend to continue the effort already started with using centralized services such as Government cloud, Government ISP and so on.

The centralized services are a great platform to perform much more effective and efficient cyber security, for example, installing a common WAF to be used to protect different clients (such as the above-mentioned DNS filtering or the mentioned Imperva WAF) and the ability to place monitoring sensors to enhance the centralized SOC monitoring capabilities, giving better visibility and protection.

We encourage Paraguay to continue the centralization effort, saving cost at the different government offices, providing better service, and promoting more professional work. This effort can be combined with the role of the Government CIO to establish guidelines for the government offices.

On the professional level, we encourage the switch to more centralized services such as email and web.

Perform Annual Cyber "War Game" for the National Level

Once a national cyber security plan is established, it is recommended to conduct an annual "cyber war game". The "cyber war game" is a great tool to check cyber readiness in different areas. It identifies gaps in processes, procedures, and guidelines, promotes interactions between different offices or organizations, and practices cyber crisis situations. Cyber ware games usually also help top level managers to become better prepared for a cyber event and helps to sharpen the interaction with the professional people involved.

Recommendations – Prioritized and Staged

1. Find a Cyber Security Champion within the government structure
2. Appoint a National Cyber Security Manager at the relevant position
3. Perform Capacity Building - start with the human capital
4. Establish the SOC-Py Project
5. Allocate long-term budget for the National Cyber Security Strategy
6. Prioritize, approve, plan implementation and monitor progress of the National Cyber Security action items
7. Define responsibility and authority for the relevant cyber security body
8. Define selection criteria and the resulting list of Critical Infrastructure (CI) at the national level – using risk-oriented criteria. Then, build a roadmap for the cyber security of the CI (Regulation, information sharing, incident response, annual risk assessments etc.)
9. Separate roles of plan, operation from capacity building in SENATICS
10. Define set of Cyber Baseline Standards and Guidelines
11. Conduct Annual National Cyber Security Review by the National Cyber security committee
12. Perform gap analysis with respect to the Budapest Convention and the derivatives on the Paraguay government
13. Perform gap analysis on the cybercrime justice process (from gathering evidence to prosecution)
14. Adjust appropriate law for the new Cyber Security Body, enabling it to perform its defined work
15. Although not actionable: Consider Cyber as an Opportunity

We highly recommend that the implementation of the SII project will include a “red team” to perform a cyber security review of the architecture and implementation, along with a pen-testing activity and report.

Total Cost and Resources

SOC-Py Project:

Budget of $2M for a period of 3 years.

Perpetual Annual budget of $160K (SOC-Py operation).

Communication costs:

Annual budget for dedicated links from institutions to SOC center (according to Gov. ISP agreements).

CERT-Py:

Recommendation to set minimum number of personnel to 6 people in order to be able to perform.

Perpetual Annual budget of $90K which establishes a team to deal with cyber incidents and another team that can work on infrastructure and tools OR handle second incident.

Training Center:

Recommendation to appoint Personnel - 1 people.

Capacity Building:

Recommendation to appoint Personnel - 1 people to be responsible on planning and operational activities.

Professional resource growth

Recommendation to have 10% annual growth for at least 5 years.

Other resources (legal, regulatory, …) as needed by plan

Appendixes:

Meetings List

19/06 12:00 – 12:30: Meeting with Minister David Ocampos

Minister David Ocampos

20/06 09:00 - 12:00: Meeting with the financial sector - Central Bank of Paraguay (BCP), ASOBAN

BCP: Marcelo Galván

ASOBAN: Ricardo Rolón

20/06 13:00 - 15:00: Meeting with two Data Center and Internet Service Providers, TIGO (private) and COPACO (governmental)

COPACO: Carlos González

21/06 09:00 - 12:00: Meeting with the energy sector (critical infrastructure) - ITAIPU (main electricity producer) and ANDE (electricity distribution)

ANDE: Luis Ribeiro, Fernando Gonález, Gustavo Quiroga, Christian Ruiz, Carlos Alfonso, Jose Duarte

ITAIPU: Alberto Weingarthofer, Segundo Bogarin, Ramón Edgar Pedrozo

21/06 13:00 - 15:00: Meeting with the Telecom regulator, CONATEL

CONATEL: Cesar Martínez

Law of SENATICS

https://www.senatics.gov.py/application/files/2414/5200/6345/ley_4989_senatics.pdf (Spanish)

Responsibilities of SENATICS:

a) Orient, prioritize and direct the implementation and maintenance of IT in the government.

b) Promote and give directives for optimization of procedures and processes of government entities of the Executive Power.

c) Promote studies and investigation in the field of IT …

d) Improve the cooperation between the public and private sector in IT field

e) Coordinate the actions between different government entities regarding e-government.

f) Design, monitor and follow up public policies adopted by government entities in the field of e-government; control, monitor and supervise the processes, programs and policies in e-gov.

g) Implement and manage the technological infrastructure of public networks and data centers of the Executive Power.

h) Establish and manage policies for the protection of personal and government information and cultivate knowledge of information security industry, for which a security organization system must be established; propose a security policy at the national level and establish a plan of information protection integration.

i) Promote studies and evaluate software for efficiency and usefulness … taking as reference open source software.

j) Promote the development of common and integrated physical infrastructure, technological platforms, networks and systems which allow the interactive management.

k) Improve and harmonize the existing IT resources.

l) Develop suitable human resources for the implementation of IT programs and projects.

m) Monitor public policies of e-government in entities of the executive power.

n) Implement plans to introduce IT in the educational system.

o) Promote initiatives to improve the knowledge of IT in communities.

p) Define the best technologies and specifications of IT equipment, programs, and connectivity and carry out the buying process for IT equipment for the schools designated by the Education Ministry.
q) Implement (by themselves or by third parties) operations, maintenance and help desk unit, that should be efficient and relevant for the IT equipment and connectivity that is hired.
r) Advise and participate in the formulation of national policies related to the use of technologies in education.
s) Promote initiatives and develop projects to improve the knowledge of IT in the education community.
t) Monitor the public procurement system related to IT acquisition in order to ensure property, efficiency and low cost.
u) Advise and provide support to technical consultants from government entities and the Directorate of Public Procurement regarding technology.

Exceptions: government institutions that have a duty of reservation in the information to third parties (i.e.: banks, BCP, BNF and maybe others)

Functions of the Direction of Policies, Standards and Infrastructure:

…

h) Define and promote the National Cybersecurity Plan

…

National Cyber Strategy Program Document

Plan Nacional de Ciberseguridad - Ejes, Objetivos y Acciones (Autoguardado).xlsx

Critical Assets and Systems List

During our visit, we have built with SENATICS personnel a list of critical systems and databases. This list is not to be considered complete without further work. However, from the list it appears that there are many national systems and databases that need to be protected. This list will serve as input for the Critical Infrastructure prioritization process, as well as for regulations, policy and guidelines to help protect those important assets.

BCP (Central Bank of Paraguay)

Payment System of Paraguay - national transaction gateway

Treasury

National Payment System - government (Assignment of State Budgets, supplier payments, salaries, etc.)

SET Sub-secretaria de Estado de Tributacion (Taxes)

Tax Systems

DGEEC

Database of Paraguayan Citizenship (Statistics and Census)

Ministry of Health

Database of Medical Records

Ambulance Management System

Telemedicine System

Blood Bank Database System

Power of attorney

Collection System of Judicial Fees

Judicial Database

Judicial Records

Identification Department of the National Police

Identity Card Registration System

Passport Registration System

Police System

Citizen Biometric Registry System

Civil registration

Database of births, living, dead, marriages, etc.

Ministry of Industry and Commerce

System of Payment of Export and Import Taxes

Single Window of Exportation (MIC Ministry of Industry and Commerce)

Business Registration System

ANDE National Electricity Administration

Billing Database and System

Controller of the Electrical Distribution Network

National Bank of Paraguay BNF

ATM Network

Online Banking

Customer Account State Database

Migrations

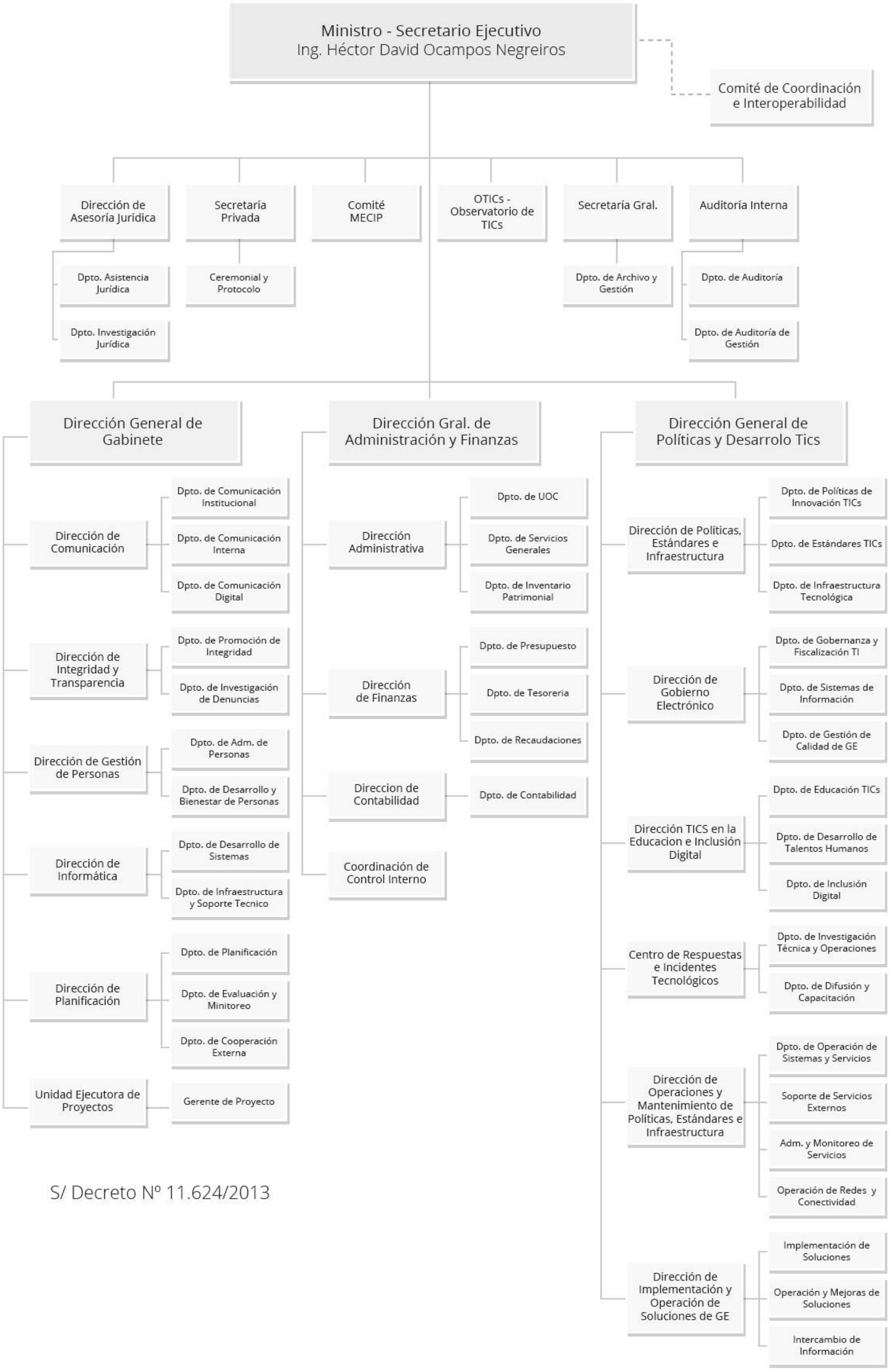
Input / output database

Searchable Database

Acraiz - MIC

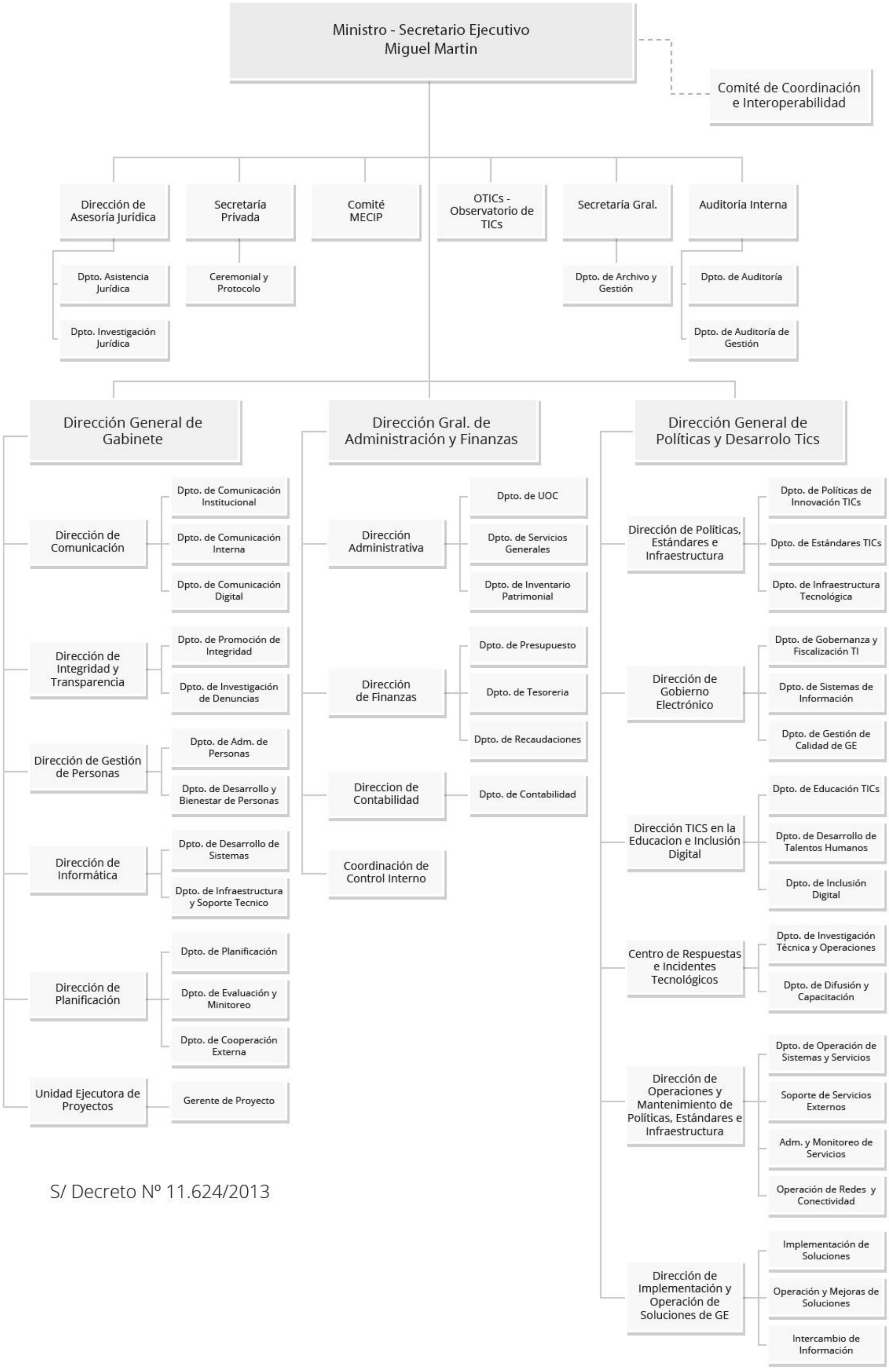
PKI de firma digital

SENATICS Organigram – August 2018


Ministro - Secretario Ejecutivo
Ing. Héctor David Ocampos Negreiros
Comité de Coordinación e Interoperabilidad
Dirección de Asesoría Jurídica
Secretaría Privada
Comité MECIP
OTICs - Observatorio de TICs
Secretaría Gral.
Auditoria Interna
Dpto. Asistencia Jurídica
Dpto. Investigación Jurídica
Ceremonial y Protocolo
Dpto. de Archivo y Gestión
Dpto. de Auditoría
Dpto. de Auditoría de Gestión
Dirección General de Gabinete
Dirección de Comunicación
Dpto. de Comunicación Institucional
Dpto. de Comunicación Interna
Dpto. de Comunicación Digital
Dirección de Integridad y Transparencia
Dpto. de Promoción de Integridad
Dpto. de Investigación de Denuncias
Dirección de Gestión de Personas
Dpto. de Adm. de Personas
Dpto. de Desarrollo y Bienestar de Personas
Dirección de Informática
Dpto. de Desarrollo de Sistemas
Dpto. de Infraestructura y Soporte Tecnico
Dirección de Planificación
Dpto. de Planificación
Dpto. de Evaluación y Minitoreo
Dpto. de Cooperación Externa
Unidad Ejecutora de Proyectos
Gerente de Proyecto
Dirección Gral. de Administración y Finanzas
Dirección Administrativa
Dpto. de UOC
Dpto. de Servicios Generales
Dpto. de Inventario Patrimonial
Dirección de Finanzas
Dpto. de Presupuesto
Dpto. de Tesoreria
Dpto. de Recaudaciones
Direccion de Contabilidad
Dpto. de Contabilidad
Coordinación de Control Interno
Dirección General de Políticas y Desarrolo Tics
Dirección de Políticas, Estándares e Infraestructura
Dpto. de Políticas de Innovación TICs
Dpto. de Estándares TICs
Dpto. de Infraestructura Tecnológica
Dirección de Gobierno Electrónico
Dpto. de Gobernanza y Fiscalización TI
Dpto. de Sistemas de Información
Dpto. de Gestión de Calidad de GE
Dirección TICS en la Educacion e Inclusión Digital
Dpto. de Educación TICs
Dpto. de Desarrollo de Talentos Humanos
Dpto. de Inclusión Digital
Centro de Respuestas e Incidentes Tecnológicos
Dpto. de Investigación Técnica y Operaciones
Dpto. de Difusión y Capacitación
Dirección de Operaciones y Mantenimiento de Políticas, Estándares e Infraestructura
Dpto. de Operación de Sistemas y Servicios
Soporte de Servicios Externos
Adm. y Monitoreo de Servicios
Operación de Redes y Conectividad
Dirección de Implementación y Operación de Soluciones de GE
Implementación de Soluciones
Operación y Mejoras de Soluciones
Intercambio de Información

S/ Decreto Nº 11.624/2013

SENATICS Organigram – November 2018


Ministro - Secretario Ejecutivo
Miguel Martin
Comité de Coordinación e Interoperabilidad
Dirección de Asesoría Jurídica
Secretaría Privada
Comité MECIP
OTICs - Observatorio de TICs
Secretaría Gral.
Auditoría Interna
Dpto. Asistencia Jurídica
Dpto. Investigación Jurídica
Ceremonial y Protocolo
Dpto. de Archivo y Gestión
Dpto. de Auditoría
Dpto. de Auditoría de Gestión
Dirección General de Gabinete
Dirección Gral. de Administración y Finanzas
Dirección General de Políticas y Desarrolo Tics
Dirección de Comunicación
Dpto. de Comunicación Institucional
Dpto. de Comunicación Interna
Dpto. de Comunicación Digital
Dirección de Integridad y Transparencia
Dpto. de Promoción de Integridad
Dpto. de Investigación de Denuncias
Dirección de Gestión de Personas
Dpto. de Adm. de Personas
Dpto. de Desarrollo y Bienestar de Personas
Dirección de Informática
Dpto. de Desarrollo de Sistemas
Dpto. de Infraestructura y Soporte Tecnico
Dirección de Planificación
Dpto. de Planificación
Dpto. de Evaluación y Minitoreo
Dpto. de Cooperación Externa
Unidad Ejecutora de Proyectos
Gerente de Proyecto
Dirección Administrativa
Dpto. de UOC
Dpto. de Servicios Generales
Dpto. de Inventario Patrimonial
Dirección de Finanzas
Dpto. de Presupuesto
Dpto. de Tesoreria
Dpto. de Recaudaciones
Direccion de Contabilidad
Dpto. de Contabilidad
Coordinación de Control Interno
Dirección de Politicas, Estándares e Infraestructura
Dpto. de Políticas de Innovación TICs
Dpto. de Estándares TICs
Dpto. de Infraestructura Tecnológica
Dirección de Gobierno Electrónico
Dpto. de Gobernanza y Fiscalización TI
Dpto. de Sistemas de Información
Dpto. de Gestión de Calidad de GE
Dirección TICS en la Educacion e Inclusión Digital
Dpto. de Educación TICs
Dpto. de Desarrollo de Talentos Humanos
Dpto. de Inclusión Digital
Centro de Respuestas e Incidentes Tecnológicos
Dpto. de Investigación Técnica y Operaciones
Dpto. de Difusión y Capacitación
Dirección de Operaciones y Mantenimiento de Políticas, Estándares e Infraestructura
Dpto. de Operación de Sistemas y Servicios
Soporte de Servicios Externos
Adm. y Monitoreo de Servicios
Operación de Redes y Conectividad
Dirección de Implementación y Operación de Soluciones de GE
Implementación de Soluciones
Operación y Mejoras de Soluciones
Intercambio de Información

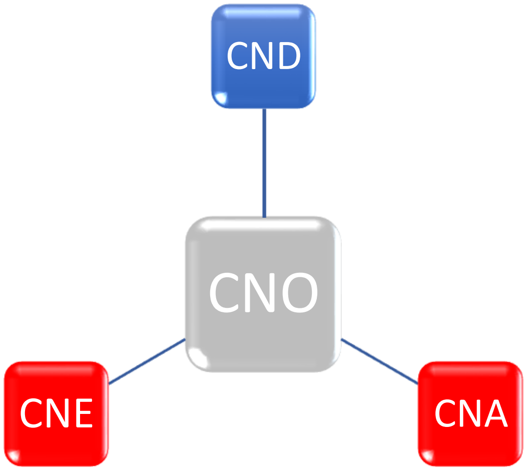
S/ Decreto Nº 11.624/2013

Types of Computer Network Operations

Computer Network Operations (CNO) is a broad term that has both military and civilian application.

According to Joint Pub 3-13, CNO consists of computer network attack (CNA), computer network defense (CND) and computer network exploitation (CNE):

- Computer Network Defense (CND): Includes actions taken via computer networks to protect, monitor, analyze, detect and respond to network attacks, intrusions, disruptions or other unauthorized actions that would compromise or cripple defense information systems and networks.
- Computer Network Exploitation (CNE): Includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks.
- Computer Network Attack (CNA): Includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves.



CNE and CNA are mostly considered to be relevant to security agencies (e.g. army) since they involve special law and approval by the department of defense and government. Also, on the philosophical level those organizations are accustomed to think about the "enemy" and this kind of activities expand the capabilities that these organizations can operate.

On the other hand, CND, deals with the defense of systems from potential malicious actors. The systems that need to be defended are mostly located in the "civilian space". You can look at different levels of systems that need defending in the civilian space:

1. CI – Critical Infrastructure is defined as the systems, networks and assets that are so essential that their continued operation is required to ensure the security of a given nation, its economy, and the public's health and/or safety. Such systems could be financial operations, electricity, telecommunications and so on.
2. Government infrastructure – the systems, networks and assets that are being used by the government to perform it's task or communicate with the people.
3. Private sector infrastructure - the systems, networks and assets that are being used by the private sector (e.g. factories, plants, services) that are not considered CI.
4. Citizens – the computers, mobile phones or any other of computer based systems that are being used by the public.

Usually you will not find the security services operating to defend the above mentioned systems therefore calling for a civilian agency to perform this tasks.

The tasks may include:

1. Awareness campaigns
2. Capacity building
3. Regulations, standards and policies
4. Active defense
5. Information sharing
6. Public shareable guidance
7. Gap analysis and risk assessment
8. International relations and international treaties
9. Cooperation with academia

Cooparation between CND and CNE is recommended especialy in terms of defining the “reference threat” on which the annual planning and strategic program is based on. With the “reference threat” it is easier to perform the strategic planning. Thus, the “reference threat” can be monitored for major changes calling for changing the annual strategic plan.

Another shared issue between all of the CNO disciplines is the need for “capacity building”. Cyber security with all of its disciplines requires very talented, professional and experienced people. This usually means that the country needs a strategic plan for “capacity building”. The result of this plan, which are educated people, will be divided between the different positions in the relevant places (civilian or army).