cigre Chile

CYBER SECURITY MASTER PLAN

for electricity sector

2021 - 2023

1 INDEX

Elaboration and Production: CIGRE Chilean commission
Editor: Working Group (WG) Cybersecurity in Electrical Systems
CIGRE CHILE

Coordinator and leader of WG Cybersecurity:
Engineer Eduardo Morales Cabellos - CIGRE Partner and
representative in CIGRE Mundial Study Committee (SC D2)
Information Systems and Telecommunication

General Production Coordinator / Manuel Silva P.
Correction / Luz Marina Fuenzalida Gutierrez
Design and layout / Paulina Ventura Peillard
Translation / Claudia Fajardo R.
Digital printing /
First Edition / September 2020 / September 2020
Any total or partial reproduction must clearly cite the CIGRE
Chilean commission. www.cigre.cl Printed in Chile

@ 2020, CIGRE Chile
A partial or total reproduction of this technical document is
forbidden. All rights reserved.

OPENING STATEMENTS 1

The CIGRE Chilean commission has been closely observing what has been happening around the world for some time about the potential threats and cyberattacks that the electricity system infrastructures could suffer. In addition, there is an increase in standards and policies that have been carried out in the country regarding guidelines and recommendations for both public and private institutions that have their information systems connected to their internal / external networks and the internet, and the risk which entails not taking control, visibility and mitigation measures against cyber security incidents. In this scenario and together with the absence today of a Critical Infrastructures Law (II.CC.)

-which rules and regulates the areas of protection thereof- it is proposed to form a working group in August 2018, in order to generate a discussion and analysis on the security standards, systems and architectures present in the electricity grids in Chile. The foregoing under the prism of studying the main international regulations and best practices in industrial cybersecurity, considering at the same time a view of cyber-risks to determine their greater or lesser robustness and resilience against cyber attacks. All this would make it possible to develop proposals for cybersecurity in the electricity sector.

The present work is the effort of about 40 engineers, technicians and experts who for more than a year met periodically to analyze the cybersecurity gaps in the sector, quantify the degree of cybersecurity maturity (based on international regulations) and propose a Cybersecurity Master Plan for the electricity sector with concrete short, medium and long-term measures, which allows to support the government and companies in the sector in conducting the management of cybersecurity of critical infrastructures in a strategic, collaborative and proactive way.

Gabriel Olguín P.
President
CIGRE Chile

Gabriel Olguín Parada
President CIGRE Chile

1 OPENING STATEMENTS

In August 2018 we started as CIGRE Chile the cybersecurity working group for the electricity sector with a very clear and ambitious objective, to contribute with analysis and reflections to generate a plan with concrete measures to address cybersecurity in the electricity sector from the perspective of risk management and cyber resilience. All this after a year of having published in 2017 the National Cybersecurity Policy by the Government of Chile, where the energy sector appears as one of the main critical information infrastructures that must be protected against potential cyber attacks.

Eduardo Morales Cabello
Member CIGRE and leader of the GW Technical Cybersecurity CIGRE Chile representative

Representative at CIGRE Mundial Study Committee (SC D2) Information Systems and Telecommunication

The working group made up of nearly 40 specialist engineers from both the public and private sectors met periodically to advance the analysis in question. With great pride I must emphasize that I feel privileged to have led a team of this professional quality. Thanks to the contribution and vision of each of them, we have been able to arrive at a document with a consensual technical view that presents a Cybersecurity Master Plan 2021-2023 that proposes a route to address the protection of electrical infrastructure in cyberspace, but which It can also serve as a guide for critical infrastructure in other sectors of the country. This document sets out seven long-term strategic objectives, aimed at addressing the challenges as the electricity sector and also as a country for the protection of critical infrastructures facing cyberspace threats, incorporating concrete measures for both public and private sector institutions. Additionally, a report on the analysis of cybersecurity gaps in the electricity sector in Chile is attached, which complements and provides the necessary support to reach the Master Plan. For this work we employ agile methodologies, organizing ourselves into work cells where we address cybersecurity gaps in the legal, technical regulation and organizational governance areas. We firmly believe that an exhaustive analysis of the current situation of the electricity sector with respect to cybersecurity allowed us to arrive more quickly and concretely at the recommendations and specific measures regarding the subject.

The great challenge we face once this work is completed will be how to implement and monitor these measures and strategic guidelines over time. Without a doubt, it is essential to have the collaboration of all the actors in the electricity sector, so that they cooperate, as mentioned in our National Cybersecurity Policy, in the construction of an open, free and safe cyberspace for all Chileans.

Eduardo Morales Cabello
Member CIGRE and leader of the GW Technical Cybersecurity CIGRE Chile representative

Representative at CIGRE Mundial Study Committee (SC D2) Information Systems and Telecommunication

INTRODUCTION 2

The mass use of information and communication technologies (ICT) generates multiple benefits in the work of citizens, such as the use of increasingly automated systems that provide greater facilities and access and the delivery of services that allow people a better standard and quality of life. Although this digitization of things contributes to the development of the country, it also entails risks that can affect public safety, the essential rights of people, and Chile's foreign security. These risks can come from multiple sources and can manifest themselves through activities such as espionage, sabotage, fraud or cyberattacks carried out by other countries, by organized groups or by individuals. These scenarios lead us to have a greater awareness of what it means to protect not only information, as we have conceptually assumed for years, but also those infrastructures whose continuous and controlled operation is critical for communities, and which could eventually be subject to cyber attacks in view of the effect or reaction that this may produce.

Critical Infrastructure (II.CC) is defined as the facilities, systems or part of these that are essential for the maintenance of basic social functions, and whose disturbance or destruction would seriously affect health, physical integrity, security and safety. social and economic welfare of the population 1. In fact, to speak of critical infrastructure is to speak of a strategic and security issue of national defense, both in physical environments and in cyberspace. At the Latin American level, the issue of critical infrastructure is pending, as revealed in the report "Protection of critical infrastructure in Latin America and the Caribbean 2018" 2, launched by the Organization of American States (OAS) and Microsoft. Nearly 500 owners and operators of critical infrastructure were surveyed and it was found that 57% do not have a dedicated budget for cybersecurity measures. This reveals that the legislation is weak and that there is still a lack of awareness in Latin American countries to work on a national policy of critical infrastructures that allows this issue to be given the relevance it deserves.

In Chile, the National Cybersecurity Policy3 already mentions the importance of protecting the so- called Critical Information Infrastructures (ICI) from the perspective of their protection in cyberspace, defining the following sectors as critical: energy, telecommunications, water, health , financial services, public safety, transportation, public administration, civil protection and defense.

Without a doubt, this is progress, but an even greater effort is required to be able to generate a II.CC. policy. and a law that supports the bases of protection both in the physical and in cyberspace. In our country, a high percentage of our II.CC. is in private hands,

who must adapt to the incorporation of defined criteria, standards and good practices in cybersecurity matters in a coordinated manner with the interests of a II.CC. policy. long term.

That is why a solid base of information must be built, starting with the strategic sector plans that allow identifying which are the critical assets that must be protected and

http://www.cigre.cl/wp-content/uploads/2018/08/CARLOS-LANDEROS.pdf
https://www.oas.org/es/sms/cicte/cipreport.pdf
https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

2 INTRODUCTION

what are their specific threats and vulnerabilities, to later determine the eventual impacts. All this in order to measure maturity levels and monitor compliance with protection measures.

Clearly, there are basic solutions that are recommended for the protection of critical infrastructure, such as ensuring a clear division of responsibilities at the organizational level; a holistic approach (that addresses technical, social, economic, organizational, law enforcement and security policy, among others); development of references (frameworks, guides, procedures); training in physical and digital security for the personnel operating II.CC .; create sectoral incident response teams (CSIRT); management of providers in the field of information security (third parties) e; knowledge exchange at the national (private-public) and international level (collaboration agreements), among other solutions.

For the owners of critical infrastructure, awareness finally becomes a duty that is connected with their institutional mission and that allows them to strengthen national security and the sustainability of the service they provide to all the country's inhabitants. As long as there is no critical infrastructure law, there will be no way to force homeowners to raise security standards and society risks vulnerabilities in the provision of basic services ranging from human error due to negligence, terrorist attacks and cyber attacks that they could affect a significant part of the population.

Therefore, it is everyone's duty to take action on this matter in such a way as to equal ourselves to the most developed countries that, through a legal framework and well-defined guidelines for owners of critical infrastructure, oblige us to protect the services that are provided. they are providing for a higher good that is "to ensure the economic and social stability of the countries." It is there where the publication of this master plan and the cybersecurity gap analysis report is aimed.

INTRODUCTION 2

This work responds to the following vision and commitment:

View

- To provide the Chilean electricity sector with strategic guidelines and recommendations to become, in the medium and long term, a critical cyber-resilient infrastructure in the face of new threats and vulnerabilities in a digital world.

Commitment

- In a limited period of time, deliver the recommendations on cybersecurity for the electricity sector at the governmental and business levels to contribute to a future law on critical infrastructure in cyberspace.

3 STRATEGIC CYBERSECURITY MAGNITUDE

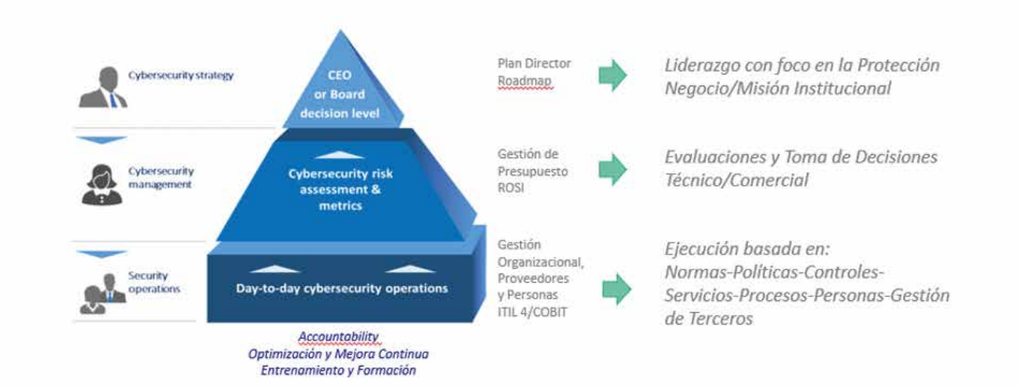
Although cybersecurity, currently defined as the protection of information systems in cyberspace, has a technical component based on regulations, frameworks and good practices that deals with day-to-day operational and tactical actions, it tends to stop side the most strategic and management component.

For cybersecurity experts, a strategic vision of management and organizational leadership is essential to obtain effective and resilient protection against cyberattacks to critical infrastructures. Without a strategic cybersecurity planning, a tough road is predicted for whoever is in charge of this matter within the organization since they will have to manage risks and business continuity, attending only to critical day-to-day events or tactical actions of medium-term, lacking a longer-term vision to measure security maturity levels and anticipate cyberattacks with defensive and offensive security measures combined with cyber intelligence.

Strategic cybersecurity raises in a simple way the main points to emphasize from the strategic, tactical and operational aspects, based on the basis that strategic cybersecurity requires a leader with technical and management skills that allow defining and carrying out a master plan that sets the path in terms of maturity levels in cybersecurity and that ensures that the organization achieves greater degrees of cyber-resilience and risk management.

A comprehensive and 360 ° approach is required as a methodology to carry out a sector cybersecurity master plan with concrete measures in the short, medium and long term. On the other hand, it is seen that the strategic level is the one who must leverage all the guidelines of this master plan and make the corresponding organizational downgrade. A master plan of this type is aimed at the decision makers of the organization.

Finally, the strategic cybersecurity approach guarantees companies and organizations an efficient and secure digital transformation, aligned with the business or institutional commitment.



Source: WG Ciberseguridad Chile adaptation of https://www.brookings.edu/blog/africa-in-focus/2018/06/04/cybersecurity-in-africa-securing-businesses-with-a-local-approach-with -global-standards /

ENVIRONMENT AND CYBERSECURITY GAPS IN THE ELECTRICITY SECTOR ANALYSI 4

The work carried out by the cybersecurity technical team of CIGRE Chile is based mainly on an analysis of the environment and cybersecurity gaps that allowed us to know the reality of cybersecurity in the country's electricity sector and whose most relevant aspects are listed below:

- Current regulations in the electricity sector do not explicitly contemplate cybersecurity in its practical requirements, nor does it mention information security incidents as a well-defined risk element.

- The institutional framework in the electricity sector exists and the responsibilities of each institution in terms of cybersecurity in regulatory activities must be clearly and explicitly established, which can be recommendations, good practices, definition of criteria, awareness-raising activities and management of incidents of cybersecurity.

- There is partial adherence to some international regulations such as NIST, NERC CIP and ISO 27,000, among others, but it is still necessary to add these standards to the existing regulation and, above all, to add some stricter ones in terms of critical infrastructure for the protection of security of information and data such as IEC 62443, ISO27019, ISO 27005, 27014, 27017 (Controls in the Cloud), ISO 22301, Law 19.628 and GDPR, among others.

- iSOC4 models and in-depth security architectures are recently becoming known for the visibility, protection and comprehensive monitoring of electrical networks, in favor of supply security and service continuity.

- The organizational structure based on silos is maintained and a senior manager is required in each company, a CISO (Chief Information Security Officer).

- New technologies to face new and advanced threats such as Sandboxing, UBA (User Behavior Analytics), Anti-malware, EDR (Endpoint Detection and Response) and Cyber Intelligence tools, Attack Simulators (cyber exercises), Malware Analysis and Forensic Analysis platforms , they are scarce in the sector even especially for OT Networks.

- Planning and coordination of cybersecurity exercises in the sector is required, where the TSO (Transmission System Operator), coordinated companies of the system (companies in the sector) participate and with the observance of the market regulatory authority and the supervisory authority, in view of evaluating impacts, lessons learned, good practices or challenges to face.

- Convergent IT / OT architectures integrated in a secure way, which allow the visibility and protection of both the IT and OT networks, are only just beginning to be seen in technological projects.

- Greater investment in training and education of engineers in the field, as well as in training and awareness tools.

- Large-scale electrical projects must begin to contemplate embedded cybersecurity from their design.

A greater number of findings and more specific gaps can be found in the Cybersecurity Gap Analysis Report in the Electricity Sector in Chile, which is the base document that accompanies this work.

https://www.smart-energy.com/wp-content/uploads/2014/02/EPRI-Planning-ISOC-report.pdf

5 RECOMMENDED CYBERSECURITY LAYER STRUCTURE FOR THE ELECTRICITY SECTOR

Currently, the electricity sector is governed by organizations at three levels (strategic, tactical and operational) that play a fundamental role in the realization of the plans and policies of the electricity sector.

Organizational Layers of the Electricity Sector in Chile

Source: WG Cibersecurity CIGRE Chile "Being able to distinguish and know the role of the main organizational institutions of the electricity sector in Chile in each of the layers allows us to better understand and define the role that each of the institutions will play in terms of cybersecurity." According to this well-structured level of organization and with defined functional layers, we can deduce that, in terms of cybersecurity, each layer also has functions that must be developed at each level. Here are some recommendations:

Strategic Laye

- Set technical and quality standards under the prism of cybersecurity and privacy, essential for the operation and operation of energy facilities.

- Future updates to the legal regulations and technical regulations should consider adding the component of cybersecurity and protection of personal data.

Tactical Layer

- Improvement of regulations and control systems in cybersecurity.

- Create cybersecurity awareness plans for the education of companies in the sector, employees and users.

Operational Layer

- Implement cybersecurity requirements in the coordination of the operation of the facilities of the National Electric System (SEN).
- Preserve the security of the service in the electrical system not only in the physical plane, but also supervise in the cyberspace of its competence in coordination with the facilities of the coordinated agents, making use of visibility tools, cyber intelligence, risk management and incidents and layers of cybersecurity protection in the elements and / or actors that make up the system.

"Only joint and coordinated work between all layers will allow cybersecurity to be tackled in a comprehensive manner for the protection and cyber-resilience of the SEN, whose operation is based today not only on a physical plane, but also on a virtual one."

CYBERATTACKS TO SCADA SYSTEMS IN THE ELECTRICITY SECTOR 6

The control systems that are used in the world for the monitoring and operation of electrical systems have also become a target of cyber attackers, due to the large amount of sensitive information they handle and the direct relationship they have with the security of supply in the country. Specialists agree that the big data that the energy industry has has become a critical asset, therefore, it is becoming part of cybersecurity strategies in several countries, especially in those with greater technological development in generation, transmission and electrical distribution.

Some time ago, worldwide, threats and cyberattacks to electrical systems have been observed with great attention. An emblematic case study that should be analyzed in Chile is the cyberattacks on the electricity grid systems that occurred in December 2015 and December 2016 in western Ukraine, operated by private electricity transmission and distribution companies.

In the first cyberattack in 2015, several electrical substations were affected, leaving nearly 700,000 residents without power for about 7 hours. Experts indicate that this cyberattack used the KillDisk malware whose variant included additional functionalities that allowed the BlackEnergy backdoor Trojan not only to erase files from the system to avoid any possibility of rebooting, but also carried specific codes to sabotage industrial systems.

Industroyer, the first modular and highly customizable malware that could adapt to any critical infrastructure (such as electricity, water and gas supplies), is responsible for Ukraine going dark again in December 2016, a kind of cyber weapon that does not It was seen from Stuxnet.

Industroyer is a particularly dangerous threat since it is capable of controlling the breakers of an electrical substation directly. To do so, it uses globally implemented industrial communication protocols (standards IEC 60870-5-101, IEC 60870-5-104, IEC 61850 and OLE for Process Control Data Access, OPC DA).

The latest information collected on cyberattacks on electrical systems worldwide reveals that they are on the rise, highlighting the cyberattack on the Northwest Territories Power Corporation (NTPC), an electricity generator and distribution company in Canada, which suffered a ransomware attack. However, NTPC is not the only organization facing incidents of breach or ransomware as several other entities worldwide in the energy sector have faced such incidents. These are listed below

- In June 2020, the car manufacturer Honda and a division of the Italian power company Enel are the new victims of the SNAKE ransomware that attacked their financial and customer service services.

- In April 2020, the multinational energy giant Energias de Portugal (EDP) received the Ragnar Locker ransomware through which hackers stole 10 TB of confidential company files and also asked for 1580 BTC (US $ 10.9M) in ransom.

- In March 2020, the European Network of Transmission System Operators for Electricity (ENTSO- E) was the target of a cyber intrusion incident, although no further details about the incident were released.

https://cyware.com/news/cyberattack-on-ntpc-further-exposes-the-cybersecurity-risks-of-energy-sector-6896de5e

6 CYBERATTACKS TO SCADA SYSTEMS IN THE ELECTRICITY SECTOR

• In February 2020, the Reading Municipal Light Department (RMLD) in Massachusetts, United States, was targeted by cybercriminals who tried to ask for money by encrypting data in the station's computer system.

• In January 2020, an Iranian hacker campaign targeting the European energy sector was observed, in which attackers attempted to steal confidential information using the PupyRAT malware.

"All this reveals that adequate risk management with a comprehensive vision will allow us to periodically review the different vulnerabilities and threats present in SCADA systems. It is also important to recognize that nothing can prevent a cyber attack on electrical installations, but if we can reduce the impact of the criticality of cybersecurity incidents with adequate preparation, it will be possible to mitigate and respond quickly to any cyber attack ".

COVID-19

Finally, it should be said that the effects of the covid-19 pandemic have also left an impact at the cybersecurity level, as shown by the latest Deloitte report6 that indicates that cybercriminals around the world are taking advantage of this crisis. An increase in phishing, malspams, and ransomware attacks has been observed, targeting not only businesses, but also end users (remote workers) downloading covid-19-related applications.

Without a doubt, the pandemic will change our lives forever, emerging new work styles, new cybersecurity problems, and new health policies, among others. The fight against covid-19 will be a joint effort and organizations will obviously need to rethink their cyber risk management, as well as their business continuity plans.

https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html

ORIGINAL CAUSE OF ATTACKS ON CRITICAL INFRASTRUCTURES 7

At a global level, if we analyze the myriad of attacks on both the physical and virtual infrastructure associated with cyberspace, at least three main reasons for the root cause are observed: money, power and subversion, important to understand as they will shed light on future laws that have to be enacted or modified in the country:

1) Money: mainly associated with delinquency and organized crime that today sees in cyberspace the opportunity to commit crimes without leaving obvious traces since it is more difficult to investigate and trace the crime. The associated computer crimes are generally electronic fraud, violation of intellectual property, misuse of credit or debit cards, etc.

According to the manufacturer Symantec in its latest Norton Cyber Security Insights Report 2017, Global Results 7, during that year, 172,000 million dollars were stolen in cyber attacks and more than 978 million people in the world lost money the previous year (2016), on average around 142 dollars per person, due to organized cybercrime. 20% of the victims used the same password between multiple accounts and at least 58% of the victims shared their passwords with others.

In Chilean legislation there is a law dating from 1993 that sanctions cyber crimes through 4 articles. However, according to the Budapest Convention 8, which is the first international treaty that seeks to tackle cybercrime and internet crime, to which Chile acceded in April 2017, it is required to modify the current law. In none of the 4 articles is explicitly mentioned (according to Claudio Magliona, 2018) "computer fraud, as a malicious figure, in which profit-making is required as a subjective element, and as an objective element, obtaining through manipulation computerization of an undue transfer of any patrimonial asset to the detriment of a third party ".

2) Power: mainly associated with states (the PandaLabs Annual Report 20179, mentions as a clear example the attack on companies with offices in Ukraine through Petya / Goldeneye, with a clearly political motive where the Ukrainian government itself openly accused the Russian government of being behind it) or factual powers (according to the Dictionary of the Royal Spanish Academy, the factual power is "that which is exercised in society outside the legal institutions, by virtue of the capacity for pressure or authority that is possessed; eg, the bank, the Church, the press, etc. ")10, who are currently trying to control and manage.

information for their own benefit. The crimes associated with this type of root cause can be computer sabotage, industrial espionage or malicious intervention of SCADA control systems, among others.

This should be a precedent to be considered in a future law for the protection of critical infrastructures since they could be affected both by cyber espionage or computer sabotage on the part of factual groups, as well as by cyber attacks by enemy countries that affect national sovereignty. The National Chilean Cyber Defense Policy11 It expressly makes clear in its Article 1, point 3.2, the recourse of the use of force in legitimate defense in cyberspace:

https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf
https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
https://www.pandasecurity.com/spain/mediacenter/src/uploads/2017/11/Informe_Anual_PandaLabs_2017.pdf
http://www.revistas.unam.mx/index.php/rmcpys/article/viewFile/42190/38336

7 ORIGINAL CAUSE OF ATTACKS ON CRITICAL INFRASTRUCTURES

"The Cyber Defense Policy is part of the National Defense Policy, and is an integral part of its objectives and principles, especially in relation to:

- Defense operations in cyberspace constitute a specific dimension of the contemporary spectrum of the use of defense capabilities.

- The planning, conduction and execution of operations in cyberspace will strictly adhere to the respect of Public International Law, with special consideration to International Human Rights Law and International Humanitarian Law. Therefore, Chile will refrain from resorting to the threat of use or the use of force in a way that contravenes International Law and may use force in legitimate defense in cyberspace, in accordance with the provisions of Article 51 of the United Nations Charter ".

3) Subversion: mainly associated with terrorist groups or anti-system political activists who resort to cyberterrorism or hacktivism to pressure governments and cause fear in the population to impose their ideologies and destabilize the political or economic system of a country.

According to the U.S. Federal Bureau of Investigation, cyberterrorism is 12 "Any premeditated and politically motivated attack against information, computer systems, computer programs and data that results in violence against non-combatant targets by sub-national groups or clandestine agents."

Some examples of cyberterrorism are:

• Website break-in to create public nuisance or inconvenience, or to stop traffic to web pages that post content that hackers disagree with.

• International cyberterrorists access and disable or modify the signals that control military technology.

• Cyber-attacks that target critical infrastructure systems, for example to disable a water treatment plant, cause a regional power outage, or they disrupt an oil pipeline or oil refinery. This type of cyberattack could hit major cities, cause a public health crisis, endanger the safety of millions of people, and lead to mass panic and deaths.

The term hacktivism was coined in 1996 by the Cult of the Dead Cow (cDc) group, an international organization of hackers and other protesters dedicated to human rights. Rather than launch cyberattacks, hacktivism used its programming skills to develop software tools to support freedom of expression and privacy. They criticized the use of DoS (Denial of Service) attacks and web alterations as unethical to freedom of speech13.

Both cyberterrorism and hacktivism are or could be present with greater force in the near future in our country.

http://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf
https://www.military.com/defensetech/2011/09/12/cyber-terrorism-now-at-the-top-of-the-list-of-security-concerns

https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism

MEASUREMENT OF THE MATURITY LEVEL IN CYBERSECURITY 8

Measuring maturity levels in cybersecurity is vital to ensure an optimal master plan that provides a roadmap for any organi zation. In accordance with the foregoing and having detected its importance in the Chilean electricity sector, the CIGRE working group decided to seek a measurement methodology.

Thus, it was decided to use the Cybersecurity Capacity Maturity Model of the Electricity Subsector (ES-C2M2) Version 1.114 developed by the United States Department of Energy (DOE) in collaboration with the Department of Homeland Security (DHS), the sector private and public sector experts.

The C2M2 program is an American public-private initiative that was established as a result of the administration's efforts to enhance the cybersecurity capabilities of the electricity subsector and understand the cybersecurity status of the network. The C2M2 helps organizations, regardless of size, type or industry, to evaluate, prioritize and improve their own cybersecurity capabilities. The model focuses on the implementation and management of cybersecurity practices associated with the operation and use of information technology and operational assets and their environments. The goal is to support the continuous development and measurement of cybersecurity capabilities within any organization by:

• Strengthening the cybersecurity capacities of organizations.

• Allow organizations to assess their cybersecurity capabilities effectively and consistently.

• Sharing knowledge, best practices, and relevant references between organizations as a means to enhance cybersecurity capabilities.

• Allow organizations to prioritize actions and investments to improve cybersecurity.

• Support the adoption of the National Institute of Standards and Technology (NIST) Cyber Security Framework.

The ES-C2M2 is designed to be used as a self-assessment methodology and has a toolkit for an organization to measure and improve its cybersecurity program.

https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

8 MEASUREMENT OF THE MATURITY LEVEL IN CYBERSECURITY

This methodology was used to measure the Chilean electricity sector in the following domains:

For each domain, the level of maturity in cybersecurity was measured on a scale of 0 to 3, according to the characteristic indicated by the methodology:

circular maturity indicator incorporates in the center the total number of manageable activities proposed by the ES- C2M2 methodology and that must be met to achieve the MILX of the specific domain. In the following figure, the number of activities that are fulfilled at 100% (full) is reflected in dark green, in light green the number of activities that are fulfilled at 75% (broadly), in red the number of activities that are met at 50% (partially) and in brown the number of activities that are not met 0% (non- compliance).

Level	Characteristics
MIL0	• Practices are not performed
MIL1	• Initial practices are performed but may be ad hoc
MIL2	*Institutionalization characteristics:* • Practices are documented • Stakeholders are identified and involved • Adequate resources are provided to support the process • Standards or guidelines are used to guide practice implementation *Approach characteristic:* • Practices are more complete or advanced than at MIL1
MIL3	*Institutionalization characteristics:* • Activities are guided by policy (or other directives) and governance • Policies include compliance requirements for specified standards or guidelines • Activities are periodically reviewed for conformance to policy • Responsibility and authority for practices are assigned to personnel • Personnel performing the practice have adequate skills and knowledge *Approach characteristic:* • Practices are more complete or advanced than at MIL2

**MIL: Maturity Indicator Level*

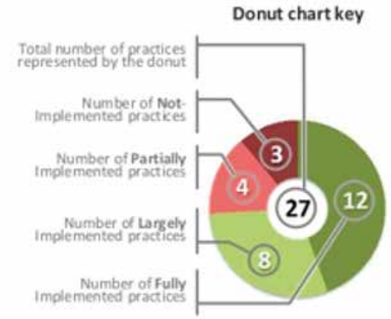
Fuente: ES-C2M2, https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

Each cybersecurity domain requires a list of C2M2 practices. In this way, to achieve MIL2 status it is required to have implemented all the practices of MIL1 and MIL2 levels and so on up to MIL3.

In this way, for each domain and each level of maturity we will have a measurement of the knowledge achieved and the horizon of gaps in order to complete each level. This

In the end, a dashboard was obtained of the level of maturity in cybersecurity of each organization that accessed this self-assessment and through a statistical analysis using the average and in some cases the mode, according to the criteria applied for each practice, a sample of the most representative level of maturity in cybersecurity in the Chilean electricity sector.

MEASUREMENT OF THE MATURITY LEVEL IN CYBERSECURITY 8



Fuente: ES-C2M2 https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

Of a total of around 40 companies that were summoned to this measurement between March and August 2019, only 5 organizations from the public and private world (equivalent to 12.5% of all companies), decided to deliver their results. It should be noted that the low participation exposes the fact that cybersecurity is not necessarily an action that is permanently monitored. Thus, in the future, it is essential to strengthen collaboration and greater awareness among the sector's actors in this matter.

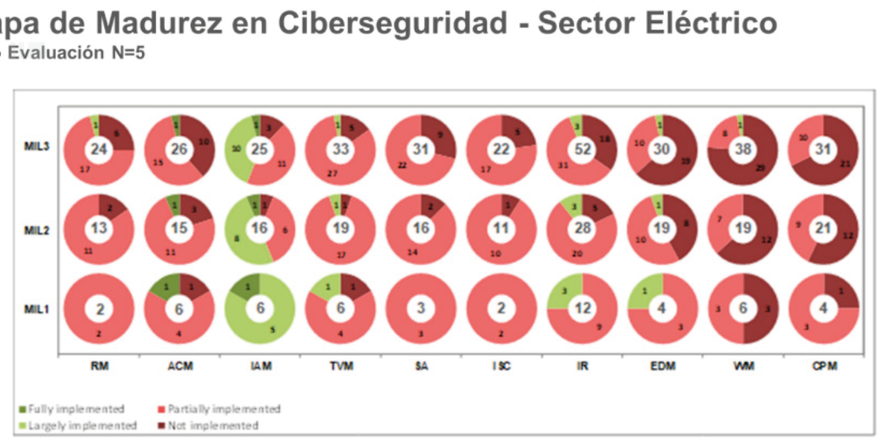
"Although the sector continuously incorporates technologies and updates its systems, not having a measurement pattern or standard that rescue the realities, or the effective level with which cybersecurity is incorporated as part of the companies' processes were part of the observed reasons for low participation.

It is relevant to highlight the difficulties in this self-assessment process, either due to the lack of documentation that evidences compliance with the activities identified by the self- assessment tool, the asymmetry in company sizes in some cases, the availability or not of specialized professionals that will facilitate this measurement and the lack of systems that demonstrate the treatment or attention to cybersecurity matters over a conventional IT treatment, among others. On the other hand, if the sample is representative or not of the maturity of the electricity sector in terms of cybersecurity, due to the low participation of companies in the self-assessments, we believe that the representativeness of the maturity indicator is indeed questionable. Notwithstanding this, we highlight that it is the first cybersecurity maturity indicator that is measured in the Chilean electricity sector and that allows to have a base to work from there to increase capacities and awareness in cybersecurity ".

8 MEASUREMENT OF THE MATURITY LEVEL IN CYBERSECURITY

Finally, and considering the sample obtained in the self-assessments, a first maturity map of the cybersecurity capabilities of the electricity sector was generated, presented below:

RM: Risk Management
ACM: Asset, Change, and Configuration Management IAM: Identity and Access Management
TVM: Threat and Vulnerability Management
SA: Situational Awareness ISC: Information Sharing and Communications



RM: Risk Management	ISC: Information Sharing and Communications
ACM: Asset, Change, and Configuration Management	IR: Event and Incident Response, Continuity of Operations
IAM: Identity and Access Management	EDM: Supply Chain and External Dependencies Management
TVM: Threat and Vulnerability Management	WM: Workforce Management
SA: Situational Awareness	CPM: Cybersecurity Program Management

Fuente: WG Ciberseguridad CIGRE Chile de Toolkit ES-C2M2

MEASUREMENT OF THE MATURITY LEVEL IN CYBERSECURITY 8

IR: Event and Incident Response, Continuity of Operations EDM: Supply Chain and External Dependencies Management WM: Workforce Management
CPM: Cybersecurity Program Management

The dashboard shows the vast majority of domains in red, indicating partial compliance (50%) of the manageable activities required for each level of maturity in each domain. The IAM domain (Access and Identity Management) stands out with the best maturity index due to the fact that historically the electricity sector has complied with the technical regulations in a rigorous way with regard to the physical security of the facilities, through a rigorous access and identity control. There are 4 critical domains for which the level of maturity is much lower than expected: SA (Situational Awareness), EDM (Third Party Management, External Dependencies and Supply Chain), WM (Employee and Workforce Management) and CPM (Management of a Cybersecurity Program).
The rest of the domains -RM (Risk Management), ACM (Asset, Change and Configuration Management), IR (Continuity of Operations, Events and Incident Response), ISC (Communications and Information Sharing) and TVM (Management of Threats and Vulnerabilities) - contributes most to the average maturity indicator of this study and the mode.

This leads us to obtain the following average cybersecurity maturity indicator for the electricity sector in Chile:

Fuente:WG Ciberseguridad CIGRE Chile

An average indicator of 0.7 and a mode of 1 reveal that for the vast majority of domains basic cybersecurity practices are adopted, but in an ad hoc manner, showing that they depend a lot on the expertise of the people in charge rather than on the procedures. and documentation evidencing said practices.

This quantitative measurement reveals a low maturity in cybersecurity for the Chilean electricity sector that requires not only a clear and specific master plan, but also monitoring and governance. In this way, in the short and medium term this sector will be able to rapidly raise its maturity levels.

MASTER PLAN: STRATEGIC CYBERSECURITY GUIDELINES

The CIGRE working group defined 7 specific strategic guidelines for the electricity sector that are supported by the guidelines established in the National Cybersecurity Policy:

	Lineamientos Estratégicos en Ciberseguridad para el Sector Eléctrico (2021-2023)	Concepto Clave
1.-	El sector eléctrico contará con una infraestructura ciber-resiliente ante amenazas y vulnerabilidades, preparada para resistir y recuperarse ante incidentes de ciberseguridad, bajo el enfoque de la gestión de riesgos.	Ciber-resiliencia
2.-	Desarrollar una cultura de ciberseguridad con el fin de generar conciencia en cada organización, mediante buenas prácticas, capacitación en áreas críticas y campañas periódicas de responsabilidad en el manejo de las tecnologías digitales, sea tanto en tecnologías de información (TI) como en tecnologías de operación (TO).	Cultura de Ciberseguridad
3.-	Conformar un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT) sectorial que permita alertar y apoyar la respuesta ante ciberataques, así como también coordinar con otros CSIRT públicos y privados para afrontar los ataques de manera coordinada.	CSIRT Sectorial
4.-	Establecer relaciones de cooperación en ciberseguridad entre todos los actores del mercado eléctrico y formar alianzas internacionales con entidades eléctricas expertas en el área.	Alianzas de Cooperación
5.-	Planificar y participar en ciberejercicios nacionales, internacionales y multisectoriales que permitan evaluar la ciber-resiliencia de la infraestructura de la información.	Ciberejercicios
6.-	Medir periódicamente los avances y la evolución de la madurez de la ciberseguridad a través de un plan de trabajo con base normativa y manejo de la privacidad, para alcanzar los niveles más altos de protección de los activos críticos de la información y de datos personales.	Medición de Madurez
7.-	Fomentar el desarrollo e innovación en ciberseguridad industrial tanto en la academia como en la industria eléctrica para alcanzar los lineamientos estratégicos definidos.	I+D+i

CYBERSECURITY ARRANGEMENTS FOR THE ELECTRICITY SECTOR 2021-2023

These arrangements are part of the Cybersecurity Master Plan for the electricity sector that leverage each of the proposed strategic guidelines for their implementation in the short term (CP) between 6 months and 12 months, medium term (MP) between 13 months and 24 months and long term (LP) between 25 months and 36 months. Additionally, the institutions responsible and collaborating in the fulfillment of the arrangements and their follow-up are suggested as a recommendation.

Ciber-Resiliencia	Medidas Propuestas	Responsables/Colaboradores Propuestos	Horizonte
1	Implementar un listado de requerimientos mínimos en ciberseguridad exigibles en contratos para proveedores de servicio.	Coordinador / SEC	CP
2	Conformación de un comité de expertos en ciberseguridad del sector eléctrico que permita concretar las medidas de corto, mediano y largo plazo del Plan Director.	Ministerio de Energía / CNE / SEC / Coordinador / Empresas Eléctricas A.G. / CIGRE	CP
3	Revisión, ampliación y fiscalización de las 13 medidas urgentes de ciberseguridad impuestas por el Coordinador para los Coordinados.	SEC / Coordinador / Coordinados	CP
4	Solicitud a la CNE de la Revisión de la Norma Técnica y definición de requerimientos mínimos de ciberseguridad a cumplir.	Coordinador / CIGRE / Coordinados / Empresas Eléctricas A.G. / Otros	MP
5	Definir distintos escenarios de crisis ante ataques cibernéticos que requieran de ciber-resiliencia para la continuidad del servicio del sector eléctrico.	Ministerio del Interior / Coordinador / SEC / CNE / Ministerio de Energía / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros	MP
6	Desarrollar programas de *pentesting* o *ethical hacking* para el equipamiento eléctrico (medidores inteligentes, plc, sensores, etc.) ante ciberataques.	Coordinador / Universidades-Institutos / Coordinados	MP
7	Elaborar y confeccionar un reporte tipo de incidentes de seguridad que permita tener la información adecuada en caso de registrarse en la empresa afectada un ciberataque.	SEC / Coordinador / Ministerio del Interior / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros)	MP
8	Establecer la institucionalidad con roles definidos y gobernanza en materia de incidentes de seguridad en caso de un ciberataque.	Ministerio de Energía / CNE / SEC / Coordinador	MP
9	Definir las instituciones públicas y privadas del sector que por su grado de criticidad de activos deben poseer un equipo de respuesta ante incidentes de seguridad (CSIRT) y un *Security Operation Center* (SOC).	Ministerio del Interior / Ministerio de Energía / CNE / Coordinador / SEC / Empresas Eléctricas A.G. / Ministerio del Interior	LP

Cultura de Ciberseguridad	Medidas Propuestas	Responsables/Colaboradores Propuestos	Horizonte
10	Programación anual de seminarios, congresos, charlas de ciberseguridad industrial, entre otros, para el sector eléctrico.	CIGRE / Ministerio de Energía / Empresas Eléctricas A.G. / Universidades-Institutos	CP
11	Diseñar planes periódicos de concienciación en ciberseguridad para todos los empleados de instituciones públicas y privadas del sector.	SEC / Coordinador / Coordinados	MP
12	Definir cursos de perfeccionamiento en ciberseguridad para los encargados de seguridad de la información en ambientes TI/TO para instituciones públicas y privadas del sector.	Ministerio de Energía / Coordinador / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros	MP
13	Diseñar e implementar una campaña de ciberseguridad industrial de carácter masivo para empleados y empresas del sector, y fomentar la ejecución de programas de difusión y guías de buenas prácticas en acciones de sensibilización.	Ministerio de Energía / Coordinador / SEC / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros	MP
14	Conformar una mesa intersectorial para fomentar la importancia de la protección de infraestructuras críticas. Creación de un Centro Nacional de II.CC.	Ministerio del Interior / Ministerio de Energía	MP
15	Acercamiento con universidades, institutos y centros de capacitación que permitan aumentar el conocimiento (cursos, diplomados, carreras) en ciberseguridad industrial para la creación de capital humano en el sector.	Coordinador / Ministerio de Energía / Universidades-Institutos	LP
16	Definir un mes para la protección de infraestructuras críticas que permita crear concienciación.	Ministerio del Interior / Ministerio de Energía	LP
17	Creación de un grupo de trabajo y alianzas con centros nacionales e internacionales de análisis de *malware*/forense para la compartición de información relevante ante ciberamenazas en el sector eléctrico.	SEC / Ministerio de Energía / Coordinador / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros	LP

CSIRT Sectorial	Medidas Propuestas	Responsables/Colaboradores Propuestos	Horizonte
18	Diseño y desarrollo de capacidades técnicas para un CSIRT Eléctrico.	Coordinador / Coordinados	CP
19	Acuerdo de colaboración con el CSIRT de Gobierno para establecer apoyo para la creación del CSIRT Eléctrico.	Coordinador / Ministerio del Interior / Ministerio de Energía	CP
20	Desarrollo de un RFI (Request for information) que permita a empresas de ciberseguridad nacionales e internacionales presentar posibles soluciones, dimensionamiento y presupuesto para proyectar a futuro el CSIRT sectorial.	Coordinador	MP
21	Definir, documentar e implantar un proceso para la gestión de los incidentes de seguridad en el sector eléctrico.	Coordinador / Ministerio de Energía / CNE / SEC / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros	MP
22	Generar una base de conocimiento de incidentes de seguridad del sector, procedimientos y prácticas a aplicar para el monitoreo, detección y respuesta de incidentes.	Coordinador / SEC / Ministerio de Energía / CNE	MP
23	Definir un canal de comunicación oficial del sector eléctrico, para compartir información referente a los incidentes y amenazas de ciberseguridad.	SEC / Coordinador / Ministerio de Energía	MP
24	Liberación y adjudicación de RFP (Request for Proposal) de implementación del CSIRT Eléctrico.	Coordinador / Ministerio de Energía / CNE	MP

Alianzas de Cooperación	Medidas Propuestas	Responsables/Colaboradores Propuestos	Horizonte
25	Alianza con el CSIRT de Gobierno	Ministerio de Energía / Coordinador / SEC	CP
26	Creación de alianzas con entidades de prestigio en ciberseguridad industrial, nacionales e internacionales, para compartir experiencias respecto a estándares y buenas prácticas en esta materia.	Coordinador / SEC / Coordinados / Universidades-Institutos	MP
27	Establecer alianzas multisectoriales (banca, defensa, Gobierno) que permita compartir mejores prácticas en seguridad de la información y protección de datos críticos.	Coordinador / SEC / Universidades-Institutos	MP
28	Alianzas con universidades, institutos y centros de formación para la creación de capital humano en pregrado/postgrado a formar parte de los CSIRT y SOC para el sector eléctrico.	Ministerio de Energía / SEC / Coordinador / Universidades-Institutos	MP
29	Alianzas con CSIRT nacionales o internacionales para la compartición y colaboración ante amenazas e incidentes de seguridad relacionados con el sector eléctrico.	Coordinador /SEC / Ministerio del Interior / Ministerio de Energía	LP

Ciberejercicios	Medidas Propuestas	Responsables/Colaboradores Propuestos	Horizonte
30	Diseñar un Plan de Ciberejercicios basado en experiencias internacionales para el sector eléctrico.	Coordinador / SEC / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros	CP
31	Acercamiento y acuerdo con universidades e institutos para programar en un mediano y largo plazo ciberejercicios que unan los talentos del mundo académico y privado.	Coordinador / Ministerio de Energía / Coordinados / Universidades-Institutos	MP
32	Realizar ejercicios de simulación de crisis y ciberejercicios al menos una vez al año, con la participación de las principales empresas eléctricas, Coordinador, Gobierno y entidades internacionales.	Coordinador / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros / SEC / Ministerio de Energía / CNE	LP
33	Crear un centro de entrenamiento con plataformas y simuladores especializados con el fin de estandarizar los conocimientos y experiencias de los directores de los CSIRT de ciberseguridad del sector.	Coordinador / Ministerio del Interior / Coordinados	LP

Medición de Madurez	Medidas Propuestas	Responsables/Colaboradores Propuestos	Horizonte
34	Desarrollar una encuesta periódica para las empresas coordinadas que permita medir las brechas en ciberseguridad y en protección de datos críticos.	SEC	CP
35	Establecer un estándar anual de medición de madurez en ciberseguridad por dominios y protección de datos en el sector eléctrico, con el fin de conocer el nivel y los *gaps* y alcanzar niveles de madurez superiores en el sector.	SEC / Ministerio de Energía / Coordinador	MP
36	Actualizar la normativa técnica que permita exigir a las empresas reguladas la medición anual de las brechas de ciberseguridad y sus mejoras.	CNE / Ministerio de Energía / SEC / Coordinados / Agrupaciones o Asociaciones Gremiales / CIGRE / Otros	MP
37	Crear un Plan de Concienciación en Ciberseguridad Industrial para el sector eléctrico para empleados y proveedores (terceros) que permita prevenir delitos informáticos.	Coordinador / SEC / Coordinados / Ministerio de Energía / Agrupaciones o Asociaciones Gremiales / Otros	MP
38	Creación de una base de datos con los responsables de ciberseguridad de las empresas eléctricas que permita un canal de comunicación en caso de incidentes de seguridad críticos.	SEC / Coordinador	LP
39	Añadir un capítulo de ciberseguridad a la preparación y gestión de contratos en licitaciones públicas y privadas del sector eléctrico.	CNE / Ministerio de Energía / Coordinador / SEC	LP
40	Creación de un grupo de trabajo que permita dar continuidad y seguimiento a la medición de los niveles de madurez dentro de un marco normativo y de obligaciones para las infraestructuras críticas del sector eléctrico.	Coordinador / SEC / CIGRE / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros	LP

10 CYBERSECURITY ARRANGEMENTS FOR THE ELECTRICITY SECTOR 2021-2023

I+D+i	Medidas Propuestas	Responsables/Colaboradores Propuestos	Horizonte
41	Estudio, investigación y análisis de *malwares* de ataques cibernéticos a nivel internacional que permita sacar lecciones aprendidas en arquitecturas, procesos, concienciación, gestión y respuestas ante incidentes frente a ataques en el sector eléctrico.	Coordinador / Coordinados / Universidades-Institutos	CP
42	Elaborar programas o proyectos de inversión público-privado para el desarrollo de tecnología y *software* que permita el monitoreo, ciberinteligencia, *big* data e inteligencia artificial aplicada a la ciberseguridad del sector.	Ministerio de Energía / CORFO / ANID /Coordinador / Coordinados	MP
43	Promover iniciativas académicas, como memorias o concursos estudiantiles, donde se ofrezca como premio el financiamiento de proyectos que apoyen a la ciberseguridad y la protección de datos del sector.	Coordinador / SEC / Universidades-Institutos / CIGRE	MP
44	Desarrollo de una herramienta de visibilidad con un *dashboard* estratégico del sector en materia de incidentes de ciberseguridad para el CSIRT Eléctrico.	Coordinador / SEC / Ministerio de Energía / Coordinados	LP
45	Acercamiento y acuerdos con empresas fabricantes nacionales e internacionales en ciberseguridad industrial para fomentar la inversión en la industria como polo de desarrollo económico y capital humano.	Ministerio de Energía / Ministerio de Economía	LP

CONCLUSIONS 11

The information contained in this document represents the work of a group of specialists gathered at a CIGRE Chile work table who decided to analyze cybersecurity threats and risks given the relevance that this issue represents in the electricity sector. The main conclusions are presented below:

- Given the Analysis of Cybersecurity Gaps in the Electricity Sector, it is required as a priority to place the accent on cybersecurity at the legal, technical regulatory and institutional governance level that explicitly allows companies in the sector to start investing and increasing budgets in technology, processes and people regarding the protection of assets and critical cyber assets against possible cyber attacks.

- Given the current electrical infrastructure and its progressive digital transformation, concrete measures are required to help develop a cyber-resilient infrastructure aimed at risk management and business continuity, in such a way that impacts are minimized and mitigated quickly risk risks from cyberspace threats.

- Knowing that the weakest link in the information security chain are people, it is necessary to develop a cybersecurity culture in the electricity sector at the level of employees, executives, stakeholders and suppliers (third parties) that contributes proactively to take care of the critical information of the infrastructure through awareness campaigns, awareness programs and training courses on industrial cybersecurity.

- Worldwide, cyber attacks on critical infrastructures have been on the rise, it is necessary to start a plan to have an Electric CSIRT in the medium term for the management and response to security incidents, allowing connection with other CSIRTs of Government, banking and defense for rapid cooperation and information sharing that minimizes the impact of any sabotage, fraud or information theft at the country level.

- National and international collaborative alliances are essential to increase the knowledge base. In this context, the current treaties that have been signed on cybersecurity with different countries and the relationship with experts from research centers, manufacturing companies and universities, among others, are essential to learn about the latest advances in industrial cybersecurity.

- Cyber exercises are an effective and practical measure to prepare the electrical infrastructure for cyberattacks since they allow simulating and creating risk situations in the event of an attack through communication and control networks and seeing how prepared the systems are and what they would be. improvements that should be made. Cyber exercises carried out on a regular basis represent a good practice to contribute to cyber-resilience and risk management and business continuity over time.

- It is extremely important to measure the level of maturity in cybersecurity both in the electricity sector and in the main companies and organizations that comprise it. It is proposed to do this practice annually so that the electricity sector transitions from lower levels of cybersecurity to an advanced level in a period of 3 years. The proposed Master Plan proposes concrete measures in the short, medium and long term, assuming

11 CONCLUSIONS

that gradualism will help to achieve the desired maturity objective in this matter.

- Since industrial cybersecurity is a recent field of study and development in the country, it is proposed to approach universities, institutes and manufacturing companies, among others, to promote research, development and innovation and careers and diplomas that allow solving the national cybersecurity problems in the electricity sector, through access to investment funds that contribute to the development of a powerful economic pole over time by increasing human capital and new jobs.

- Finally, it should be said that this work by the Cybersecurity Group of CIGRE Chile has the hope and desire to continue contributing to this issue at the national level in a future Policy or Law of Critical Infrastructures, of great relevance for the country, and we hope That the guidelines, measures, recommendations and conclusions set out in this study can be very useful for the electricity sector and also for other industrial sectors of equal criticality, in such a way as to prioritize actions and investments that are in this line.

ANNEX A: SUMMARY OF MODEL ES-C2M2 12

"The ES-C2M2 Model used and applied in the United States electricity sector is detailed below, which allowed us to carry out a sample of the level of maturity in cybersecurity of the electricity sector in Chile. As a CIGRE Chile working group we give special thanks to the DOE (Department of Energy) of the USA for having agreed to our request to use and send the self-assessment toolkit and the guides for its use of its version 1.1 ".

The electricity subsector cybersecurity capacity maturity model (ES-C2M2) can help electricity companies and organizations evaluate and make improvements to their cybersecurity programs.

The ES-C2M2 is part of the DOE's (US Department of Energy) Cybersecurity Capability Maturity Model (C2M2) Program and was developed to address the unique characteristics of the electricity subsector. The program supports the ongoing development and measurement of cybersecurity capabilities in the electricity subsector and can be used to:

- Strengthen cybersecurity capabilities in the electricity sector.
- Enable utilities to effectively and consistently evaluate and compare cybersecurity capabilities.

- Share knowledge, best practices and relevant references within the sector as a means to improve cybersecurity capabilities.

- Allow public services to prioritize actions and investments to improve cybersecurity.

The ES-C2M2 is designed to be used with a self-assessment methodology and a toolkit (available upon request) for an organization to measure and improve its cybersecurity program. A self- assessment using the toolkit can be completed in one day, but this same kit could be adapted for a more rigorous assessment effort. Additionally, the model can inform the development of a new cybersecurity program.

The ES-C2M2 provides descriptive guidance rather than prescriptive and industry focused. The content of the model is presented at a high level of abstraction so that it can be interpreted by subsector organizations of various types, structures and sizes. The massive use of the model is expected to support the benchmarking of the subsector's cybersecurity capabilities. These attributes also make the ES-C2M2 an easily scalable tool for implementation in the subsector of the Cybersecurity Framework (framework) of the National Institute of Standards and Technology (NIST). The model emerges from a combination of existing cybersecurity standards, frameworks, programs and initiatives and provides flexible guidance to help organizations develop and enhance their cybersecurity capabilities. As a result, model practices tend to be at a high level of abstraction and can be interpreted for organizations of various structures and sizes. The model is organized in 10 domains. Each domain is a logical grouping of cybersecurity practices. The practices within a domain are grouped by objectives.

12 ANNEX A: SUMMARY OF MODEL ES-C2M2

Within each objective, the practices are ordered by a Maturity Indicator Level (MIL) indicator.

Each of the 10 model domains contains a structured set of cybersecurity practices. Each set of practices represents the activities that an organization can perform to establish and mature a certain domain capability. For example, the Risk Management domain is a group of practices that an organization can perform to establish and mature cybersecurity risk management capacity. For each domain, the model provides a statement of purpose, which is a high-level summary of the domain's intent, followed by introductory notes that give context to the domain and introduce its practices.

Fuente: ES-C2M2, https://www.energy.gov/sites

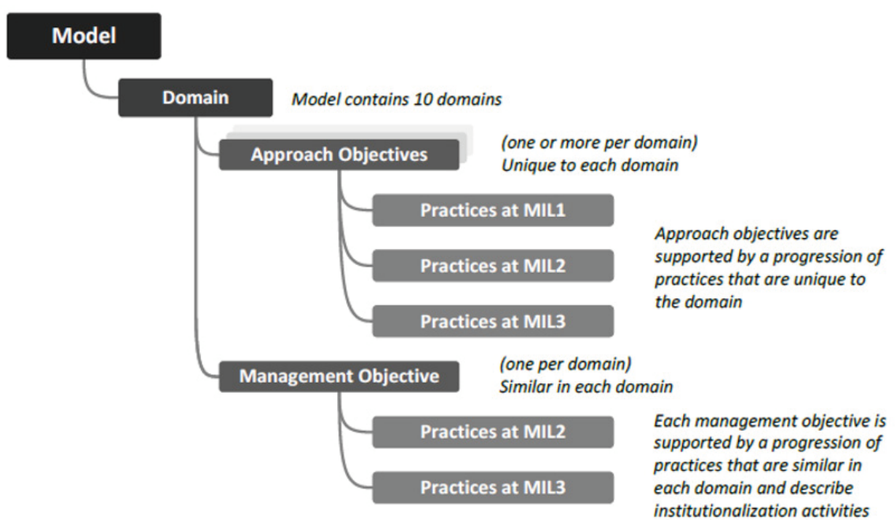


Figure 4: Model and Domain Elements

/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

Below is a brief description of the 10 domains in the order they appear in the model.

Risk management

Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, including business units, subsidiaries, related interconnected infrastructure, and stakeholders.

Asset, change and configuration management

Manage the organization's IT and OT assets, including hardware and software, in proportion to the risk to critical infrastructure and the organization's goals.

Identity and access management

Create and manage identities for agencies that can be granted logical or physical access to organization assets. Control access to the organization's assets according to the risk to critical infrastructure and the organization's objectives.

Threat and vulnerability management

Establish and maintain plans, procedures and technologies to detect, identify, analyze, manage and respond to cybersecurity threats and vulnerabilities, proportional to the risk to the organization's infrastructure (example: critical, IT, operational) and organizational objectives .

Situational awareness

Establish and maintain activities and technologies to collect, analyze, alarm, present and use operational and cybersecurity information, including status information and summaries of the other domains of the model to form a common operational image.

Exchange of information and communications

Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and increase operational resilience, commensurate with the threat to critical infrastructure and the organization's objectives.

Response to events and incidents, continuity of operations

Establish and maintain plans, procedures and technologies to detect, analyze and respond to cybersecurity events and protect operations during a cybersecurity event, consistent with the risk to critical infrastructure and organizational objectives.

Supply chain and external dependency management

Establish and maintain controls to manage cybersecurity risks associated with services and assets that depend on external entities, commensurate with the risk to critical infrastructure and the organization's objectives.

Staff Administration

Establish and maintain plans, procedures, technologies and controls to create a culture of cybersecurity and to guarantee the

suitability and continuous competencies of the personnel, in accordance with the risk to the critical infrastructure and the organizational objectives.

Cybersecurity program management

Establish and maintain a business cybersecurity program that promises governance, strategic planning, and supports the organization's cybersecurity activities in a way that aligns cybersecurity objectives with the organization's strategic objectives and risk to critical infrastructure.

The model defines four levels of indicators of maturity, MIL0 to MIL3, which are applied independently to each domain of the model. MILs define a dual progression of maturity (focus and institutionalization) that are explained in the following sections.

There are four aspects of MILs that are important to understanding and applying the model:

1. The maturity indicator levels are applied independently to each domain. As a result, an organization using the model may be operating with different MIL ratings for different domains. For example, an organization could be operating on MIL1 in one domain, MIL2 in another domain, and MIL3 in a third domain.

2. MILs are cumulative within each domain. To earn a MIL in a given domain, an organization must complete all practices at that level and its previous levels. For example, an organization must perform all domain practices on MIL1 and MIL2 to achieve a MIL2 on the domain. Similarly, the organization would have to perform all practices on MIL1, MIL2, and MIL3 to achieve a MIL3.
3. Establishing a target MIL for each domain is an effective strategy to use the model to guide cybersecurity program improvement. Organizations should familiarize themselves with the practices in the model before determining the target MIL. Gap analysis activities and improvement efforts should focus on meeting those target levels.

4. Both practice performance and achieving a MIL should be aligned with the organization's business objectives and cybersecurity strategy. Striving for the highest MIL across all domains may not be optimal. Companies must weigh the costs of achieving a specific MIL against the potential benefits. However, the model was developed so that all companies, regardless of size, can achieve MIL1 across all domains.

Table 1: Example of Approach Progression in the Cyber Program Management Domain

MIL0		
MIL1	a.	The organization has a cybersecurity program strategy
MIL2	b.	The cybersecurity program strategy defines objectives for the organization's cybersecurity activities
	c.	The cybersecurity program strategy and priorities are documented and aligned with the organization's strategic objectives and risk to critical infrastructure
	d.	The cybersecurity program strategy defines the organization's approach to provide program oversight and governance for cybersecurity activities
	e.	The cybersecurity program strategy defines the structure and organization of the cybersecurity program
	f.	The cybersecurity program strategy is approved by senior management
MIL3	g.	The cybersecurity program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile (TVM-1d)

Fuente: ES-C2M2, https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

The management practices for each MIL are described below:

Maturity Indicator Level 0 (MIL0)
The model does not contain practices for MIL0. Performance in MIL0 simply means that MIL1 in a given domain has not been achieved.

Maturity Indicator Level 1 (MIL1)
In each domain, MIL1 contains a set of initial practices. To achieve a MIL1, these initial activities can be done on an ad hoc basis, but they must be done. If an organization starts out without the ability to manage cybersecurity, it should initially focus on implementing MIL1 practices.

MIL1 is characterized by a unique management practice:

1. Initial practices are done, but can be ad hoc. In the context of this model, ad hoc (that is, an ad hoc practice) refers to performing a practice that relies heavily on the initiative and expertise of an individual or team (team leadership), without much organizational guidance to through a verbal or written plan, policy or training. The quality of the outcome can vary significantly depending on who is doing the practice, when it is done, the context of the problem being addressed, the methods, tools and techniques used, and the priority given to a particular instance of the practice. With experienced and talented staff, high-quality results can be achieved even if practices are ad hoc. However, in this MIL, the lessons learned are generally not captured at the organizational level, making the approaches and results difficult to replicate or improve across the organization.

Maturity Indicator Level 2 (MIL2)
Four management practices are present in MIL2, which represent an initial level of institutionalization of activities within a domain:

1. Internships are documented and performed according to a plan. The focus here should be on planning to ensure that practices are intentionally designed (or selected) to serve the organization.

2. The stakeholders of the practice are identified and involved in its performance. This could include stakeholders within the function, the entire organization, or outside the organization, depending on how the organization implemented the practice.

3. Adequate resources are provided in the form of people, funding and tools to ensure that internships can be carried out as planned. The performance of this practice can be evaluated by determining if the desired practices have not been implemented due to limited resources. If all desired practices have been implemented as intended by the organization, then appropriate resources have been provided.

4. The organization identified some standards and / or guidelines to inform the implementation of practices in the domain. These may simply be the reference sources that the organization consulted when developing the plan for conducting the internships.

In general, the practices in MIL2 are more complete than in MIL1 and are not performed irregularly or are not ad hoc in their implementation. As a result, the performance of the practices in the organization is more stable and will be maintained over time.

Maturity Indicator Level 3 (MIL3)
In MIL3, the activities in a domain have been institutionalized and managed. Five management practices support this progression:

1. Activities are guided by policy (or other organizational guidelines) and gover-

ANNEX A: SUMMARY OF MODEL ES-C2M2

nance. Managed activities in a domain receive guidance from the organization in the form of organizational direction, such as policy and governance. Policies are an extension of the planning activities that exist in MIL2.

2. Policies include requirements for compliance with specific standards and / or guidelines.

3. Activities are periodically reviewed to ensure they are consistent with the policy.

4. The responsibility and authority to perform the practices are assigned to the staff.

5. Assigned personnel have appropriate domain-specific skills and knowledge to perform their tasks.

In MIL3, practices in a domain are further stabilized and guided by high-level organizational guidelines, such as politics. As a result, the organization must have additional confidence in its ability to maintain practice performance over time and throughout the institution. The ES-C2M2 is intended to be used by an organization to assess its cybersecurity capabilities on a consistent basis, to communicate its capability levels in meaningful terms, and to inform the prioritization of its cybersecurity investments.

Figure 6 summarizes the recommended approach to using the model. An organization performs an assessment against the model, uses that assessment to identify gaps in a given capacity, prioritizes those gaps, and develops plans to address them. As plans are implemented, business objectives change, and the risk environment evolves, the process repeats itself.

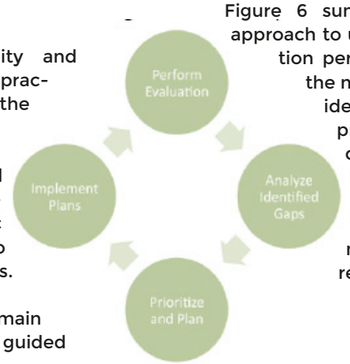


Figure 6: Recommended Approach for Using the Model

Fuente: ES-C2M2, https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

Table 4: Recommended Process for Using Evaluation Results

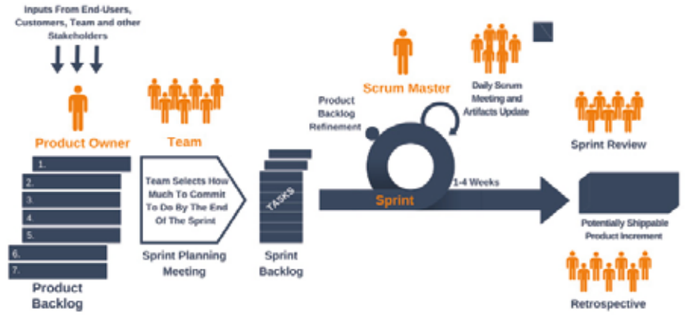
	Inputs	Activities	Outputs
Perform Evaluation	1. ES-C2M2 Self Evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	1. Conduct ES-C2M2 Self Evaluation Workshop with appropriate attendees	ES-C2M2 Self Evaluation Report
Analyze Identified Gaps	1. ES-C2M2 Self-Evaluation Report 2. Organizational objectives 3. Impact to critical infrastructure	1. Analyze gaps in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention	List of gaps and potential consequences
Prioritize and Plan	1. List of gaps and potential consequences 2. Organizational constraints	1. Identify actions to address gaps 2. Cost-benefit analysis (CBA) on actions 3. Prioritize actions (CBA and consequences) 4. Plan to implement prioritize actions	Prioritized implementation plan
Implement Plans	1. Prioritized implementation plan	1. Track progress to plan 2. Reevaluate periodically or in response to major change	Project tracking data

Fuente: ES-C2M2, https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

ANNEX B: CIGRE CHILE CYBERSECURITY WORKING GROUP

The collaborative work was carried out in face-to-face mode according to the planning inspired by the Agile Methodology, distributing the work in three cells, legal, technical regulations and Government (technology-processes-people). These groups aimed to generate progress deliverables in three previously defined sprints in order to obtain the final document of recommendations and master plan.

Within the methodology, the invitation of specialists from the electricity, government or other sectors that would provide a broader vision was considered. In this way, the meetings with Senator Kenneth Pugh and Mario Farren from the Ministry of the Interior stand out, adding value to the analysis and quality of the final document.



- Scrum Muster: CIGRE Chile Cybersecurity WG Leader
- Product Owner: Leaders of each cell
- Team: Experts and dedans

Source: Agile Methodology: Revolutionizing Project Management, https://medium.-com/@rromanss23/ agile-methedology-revolutionizing-project-management-91636775191d

13 ANNEX B: CIGRE CHILE CYBERSECURITY WORKING GROUP

The following is a list made up of the participants of the periodic sessions, either as specialists or observers, of the CIGRE Chile Cybersecurity Working Group, who are thanked for their important contribution with ideas, observations, comments and objections, among others, for this analysis and research process on cybersecurity in the electricity sector.

Eduardo Morales Cabello (Specialist - Leader WG Cybersecurity)) ENTEL S.A.

Alejandra Caro Troncoso (Specialist - Legal Cell Leader) EDF
Fernando Muñoz A. (Specialist - Technical Regulations Cell Leader) Saesa
Constanza Levicán Torres (Specialist - Government Cell Leader) Suncast

EXPERTS:

Jerson Reyes Sánchez (CNE)
Alvaro Acoria González (CEN)
Roxana Varela Otárola (SEC)
Oscar Álamos Guzmán (Ministerio de Energía)
Javiera Ketterer (Empresas Eléctricas AG.)
Mireya Isabel Pérez Martínez (Fluor Chile)
Christians Espinoza Roga (EEPA)
Fabián Serradell Díaz (Integración Sistemas S.A.)
Frandimar Belisario (Celeo Redes Chile)
Nicolás Ramos Giannini (Celeo Redes Chile)
Giovanni Guzmán (Saesa)
Daniel Soto Alquinta (CGE Naturgy)
Maria Cristina Sanhueza Bustamante (ENEL)
Miguel Torres N. (Transelec)
Natalio Schonhaut B. (IACEL SpA)
Paola Cortés Auger (Eléctrica Puntilla)
Rodrigo Moyano Colipe (Renea Chile SPA)
Gustavo Masman Paredes (Latin America Power S.A.)

DEDANS:

Andrés Jauregui Cabrera (SEC)
Francisco Balcázar González (SEC)
Hans Rother Salazar (ENEL)
Héctor Ubal Leyton (ENEL)
Rodrigo Apablaza (ENEL)
Rodrigo Velásquez Salazar (ENEL)
Filippo Gentili (ENEL)
Doris Herrera Ferrada (Chilquinta)
Cristián Muñoz Catalán (ABB)
Daniel Andrade Mancilla (ABB)
Mauricio Moran Concha (Colbún)
Sebastián Celis Cáceres (Colbún)
Jaime Berrios Maturana (Comulsa)
Víctor Ballivián (IEC Chile)
Guillermo Parada Milanese (Cornelec)
Oscar Guarda Ríos (TEN S.A.)
Roberto Díaz M. (Prosus Corp)
Yerko Pincheira Sánchez (Prosus SPA)
Ali Lobo Uzcategui (IM3)
Carlos Jaureche (Security Advisor Chile)
Gonzalo Fuentes Rojas (Underfire S.A.)

Chile

CYBER SECURITY MASTER PLAN

for electricity sector

2021 - 2023