UNIVERSIDAD DE CHILE
INSTITUTO DE ESTUDIOS INTERNACIONALES
ESCUELA DE GRADUADOS

NIST CYBERSECURITY FRAMEWORK IN SOUTH AMERICA: ARGENTINA, BRAZIL, CHILE, COLOMBIA, AND URUGUAY

Case study submitted to satisfy the requirements for the degree

Master's in International Strategy and Trade Policy

By

Juan Eduardo Catril Opazo

Case study Advisor: Professor Fabiola Wüst Zibetti

Santiago, Chile

2020

SUMMARY

As technology advances at a frenetic pace, interoperability and resilience are critical elements in an increasingly interconnected world, even more so in the new era of telework. The use of technology standards facilitates faster adoption of new products and services by entities and individuals, while also benefitting manufacturers who can prioritize resources. In the technology sector, industry players tend to lead the definition and adoption of new standards, as the winning standard (if multiple alternatives are competing) will see the benefits of being widely adopted. In the case of cybersecurity, due to its complex nature that combines products (hardware) and services (software) the standard setting mechanism is more intricate and cannot be driven by a single player. In 2013, due to the numerous cybersecurity incidents registered in the United States, President Obama issued an executive order tasking the National Institute of Standards and Technology (NIST) with the development of a Cybersecurity Framework, as a collaborative effort by a wide range of industry players and interested parties. Since its inception, and despite the voluntary character of its adherence, the framework has acted as a de facto standard in United States and other countries, it has been adopted by many companies and organizations to measure its maturity in this important area. The aim of this paper is to identify the influence that the framework has had in selected countries in South America.

Keywords of the study: Cybersecurity, Framework, NIST, Critical Infrastructure, Information Systems, Assessment, Core, Tiers, Profiles, Identify, Protect, Detect, Respond, Recover, Risk.

RESUMEN DEL ESTUDIO DE CASO PARA OPTAR AL GRADO DE:

Magíster en Estrategia Internacional y Política Comercial

AUTOR: Juan Eduardo Catril Opazo **PROFESOR GUIA**: Fabiola Wüst Zibetti

NIST CYBERSECURITY FRAMEWORK IN SOUTH AMERICA: ARGENTINA, BRAZIL, CHILE, COLOMBIA, AND URUGUAY

Como la tecnología avanza a un ritmo frenético, la interoperabilidad y estandarización de operaciones en un mundo globalizado deben ser una parte integral de esta desde su creación. El uso de estándares de tecnología permite una adopción más rápida productos y servicios, algo que beneficia a que las empresas pueden priorizar sus recursos, y que también beneficia a los consumidores quienes pueden diferenciar soluciones de una mejor manera. En la industria tecnológica, los principales actores que lideran la definición y adopción de nuevos estándares son precisamente las empresas de tecnología, quienes se benefician al ser los proponentes de nuevos estándares. En el caso de la ciberseguridad, dada la combinación de productos (hardware), servicios (software), y las diversas instancias de intervención humana, los mecanismos de definición de estándares resultan inviables y estos no pueden ser promovidos por un único sector industrial. En 2013, debido a números incidentes de ciberseguridad registrados en los Estados Unidos, el Presidente Barack Obama emitió una orden ejecutiva mandatando al National Institute of Standards and Technology (NIST) –una agencia del gobierno federal de los EE.UU., que promueve la innovación y el uso de tecnología- a desarrollar un Framework de Ciberseguridad, que permitiera mejorar la ciberseguridad de las entidades en los EE.UU. Este fue un esfuerzo colaborativo con una activa participación de la industria y otros stakeholders. Desde entonces, debido a la compleja naturaleza del sector de ciberseguridad, y pese al carácter voluntario del Framework, esta herramienta ha actuado como un estándar de hecho en numerosos países, y se utiliza por diversas entidades para medir su nivel preparación en la materia. El objetivo de este trabajo es identificar la influencia que el framework ha tenido en América del Sur.

Palabras-clave: Ciberseguridad, Framework, NIST, Infraestructura crítica, Sistemas de información, Evaluación, Perfiles, Identificar, Proteger, Detectar, Responder, Recuperar, Riesgo.

Never tell me the odds!

Han Solo

Table of contents

Figures and Tables index

Introduction

Countries have multiple tools to establish public policies: laws that regulate specific industries, dos and don’ts in the way different players must behave in each sector, customs or historic usage that end up becoming customary laws costumes just no name a few. At the domestic level, all these tools and others are used on the policy implementation process. On countries with federal organization –those with provinces or states with their own local government and regulations- the public policy process has unique nuances with policy tools operating at the federal (country-level) and at the state or provincial level. When we analyze how countries can establish policy at the international level, there is yet another level of complexity considering the international agreements and binding compromises that each country can choose to have.

A not so uncommon tool that some countries are able to utilize - under the right circumstances - is technical standards. In most cases, this can be done in new or emerging industries where first movers and trend setters have the advance of defining the way the new industry operates until a standard or other consensus set of rules is established. Evidence shows that, in most cases (and particularly in the technology industry) these standards are defined by the industry players that develop them. A good example is how the Universal Serial Bus, or USB, port came to be: “It was at Intel in Oregon where engineers made it work, at Intel where they drummed up the support of an industry that was eager to make PCs easier to use” (Johnson, 2020). In that same fashion other standards in the tech world have come to life too out of the industry itself: Bluetooth (Triggs, 2018), HDMI (Howard, 2019), and Wi-Fi (Wi-Fi Alliance, 2020) are recognizable examples of standards that started from within the technology industry.

But what happens when an industry or sector it is so complex that industry itself cannot draft or agree to a consensus set of rules to govern itself? That is the type of setup where frameworks come into play. That was the context that the Cybersecurity sector was experiencing prior to 2013, where the NIST Cybersecurity Framework (CSF) was drafted and then released in the United States.

Cybersecurity is a complex subject, it has implications in a wide variety of industries and sectors, from the protection of Critical infrastructure –such a power generation plant- to securing the personal identifiable information that a library might have of its membership (and everything in between). At the same time, there are diverse “elements” that interact within Cybersecurity:

processes that are conducted by humans, hardware, software, physical access to facilities, information, etc. A complex and diverse mix to begin with. Therefore, a Framework makes sense as a tool for this subject. A framework can be understood as “a system of rules, ideas, or beliefs that is used to plan or decide something” (Cambridge University Press, 2020), the “something” being in our case the protection of information systems.

We must understand that a framework is a collection of guidelines and rules. The adoption and adherence to these guidelines and rules is voluntary. The overall goal of this framework is to assess the maturity grade of the cybersecurity of a given entity. It was developed in the United States for U.S. entities, however –and despite being its voluntary nature- it has grown even beyond its national frontiers, getting international traction and different degrees of influence outside the United States.

Considering this scenario, has the NIST Cybersecurity Framework had influence in South America? The hypothesis is that the NIST Cybersecurity Framework can be considered an indirect policy tool, that has had influence outside of the United States, particularly in South America represented by the markets of Argentina, Brazil, Chile, Colombia, and Uruguay.

Purpose of the Study

This work analyzes the NIST Cybersecurity Framework determining its influence in South America.

Given the framework initial intent: to serve as a tool for U.S. entities to assess the maturity of their cybersecurity environments, the phenomena of its adoption outside the U.S. frontiers results interesting since it’s an indirect extension of the influence of U.S. policy makers and market leaders. In this context, we analyze this “model” of indirect policy influence and elaborate on the possibility of replicating its results in other sectors and industries.

The development of this study is organized in four parts. In the first, we examine the bases that substantiate the creation of the NIST Cybersecurity Framework, and its evolution, as well as other technical standards observed in the IT/cybersecurity sector and around the world. In the second part, we examine the NIST Cybersecurity framework, including its scope and characteristics. In the third part, we evaluate the cybersecurity landscape in selected countries in South America:

Argentina, Brazil, Chile, Colombia, and Uruguay, and identify: (a) The regulatory baseline for cybersecurity; (b) Official mentions to the Framework; (c) Changes in cybersecurity legislation. In the fourth part, we determine if the NIST framework has had influence in these markets: by contrasting when the changes took place, identifying if the Framework is being referenced by official sources, and by analyzing the legislation changes specific to cybersecurity.

PART I: Cybersecurity and its importance - Why the framework was needed?

As we already glimpsed, Cybersecurity is a complex subject due to the diverse nature of its different components and areas of application. Therefore, the traditional standard setting and adoption approach that can be done by industry players and stakeholders is simply not doable on this industry. This is where the concept of Framework, understanding it as a voluntary "system of rules, ideas, or beliefs that is used to plan or decide something" (Cambridge University Press, 2020), comes into play.

The NIST Cybersecurity Framework is defined by NIST as a:

> "*voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders*" (National Institute of Standards and Technology, 2020).

This chapter will describe the NIST CSF in detail, the context under it was created, the elements that triggered its development, the involvement of stakeholders in its creation, as well as its scope, evolution, and its status. The goal of this section is to explain in detail what the Framework is, what it does, and how it came to be.

1.1. Cybersecurity in the U.S. prior to the framework

According to Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information" (Cybersecurity and Infrastructure Security Agency, 2019).

Considering that the origin of the Internet can be traced back to the Massachusetts Institute of Technology (MIT), and the Defense Advanced Research Projects Agency (DARPA) -a federal agency part of the U.S. Department of Defense- in the sixties (Leiner, Cerf, & Clark, 1997) it is not surprising that the concept of Cybersecurity and the notion of network security also started in the United States.

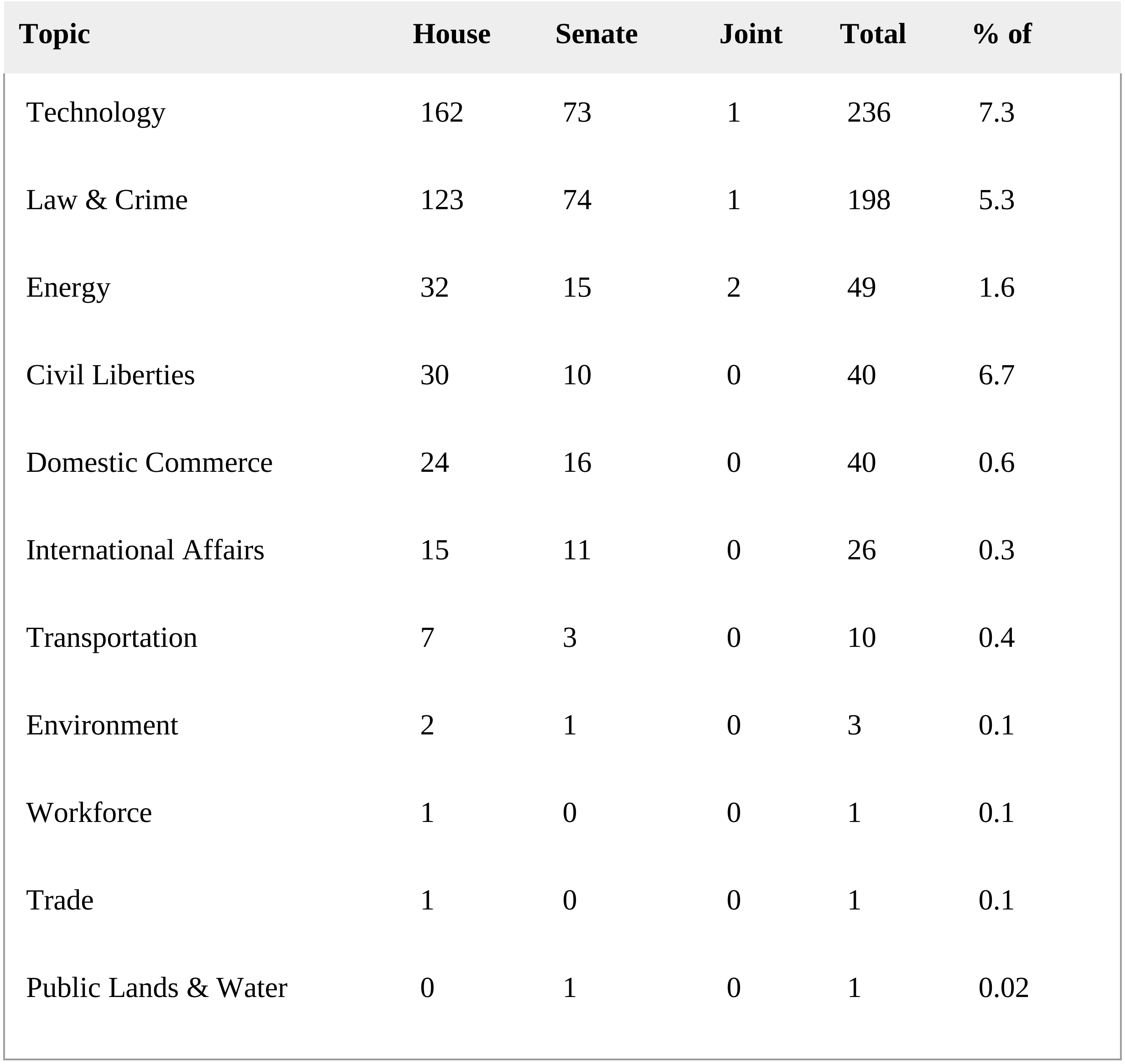
As Jonathan Lewallen describes on his article "Emerging technologies and problem definition uncertainty: The case of cybersecurity" (Lewallen, 2020), new and emerging technologies present multiples challenges for policy makers and governments that try/need to regulate them starting by its definition. As we have mentioned, Cybersecurity it's a particularly trickier subject because it is not a simple type of technology, it involves hardware, software, and human interaction among many other factors. And therefore, its regulation results particularly challenging.

In analyzing how the legislative process has happen in the United States, Lewallen examined mentions of the term cybersecurity in Congressional hearings between 1966 and 2014 (Table 1).

As we can observe, the mere mention of cybersecurity has appeared under a dozen different topics in the legislative process in the U.S., but considering just over a thousand mentions in a span of 48 years, one can anticipate that the discussions (and alleged legislative impact) have been quite diverse.

Table 1: U.S. Congressional hearings that mention cybersecurity, 1966–2014

Topic	**House**	**Senate**	**Joint**	**Total**	**% of**
All Issues	671	368	6	1,044	2.3
Defense	243	136	3	382	5.4



Topic	House	Senate	Joint	Total	% of
Technology	162	73	1	236	7.3
Law & Crime	123	74	1	198	5.3
Energy	32	15	2	49	1.6
Civil Liberties	30	10	0	40	6.7
Domestic Commerce	24	16	0	40	0.6
International Affairs	15	11	0	26	0.3
Transportation	7	3	0	10	0.4
Environment	2	1	0	3	0.1
Workforce	1	0	0	1	0.1
Trade	1	0	0	1	0.1
Public Lands & Water	0	1	0	1	0.02

Source: Policy Agendas Project Congressional Hearings dataset, calculated by Jonathan Lewallen. The last column represents the percentage of all hearings on a given topic during this period that dealt with cybersecurity; for example, the percentage of all civil liberties hearings from 1966 to 2014 that addressed cybersecurity. (Lewallen, 2020)

Lawrence Trautman goes deeper in his analysis of how cybersecurity has been treated by policymakers in the United States, his work "Cybersecurity: What about U.S. policy" explores the evolution of the cybersecurity-related legislative discussion and changes in the United States since the 1960's, and particularly the rapid changes that the sector has experienced over the last decade. Trautman cites that prior to 2014, there was an "absence of any U.S. legislation [on Cybersecurity] since 2002" (Trautman, 2015) alluding to the Cyber Security Research and Development Act, Terrorism Risk Insurance Act, and the Federal Information Security Management Act, all of which were introduced in 2002.

On that same line, the legal overview that Eric Fisher does in "Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Litigation" (Fischer, 2014) goes in the same direction, showing how between the 1960's and the early 2000's only a dozen laws were introduced in the United States, despite the tremendous technological advances of this period: the man going to the moon, the advent of personal computers, internet and its massification, the dotcom bubble, and the beginning of mobile broadband. All these innovations occurred during the same 40 years.

The seemingly lack of regulations reinforces the idea of how challenging it is to regulate technological innovations, and how tricky emerging industries -and particularly Cybersecurity- can be for policy makers and regulators.

1.2. Need for cybersecurity guidance in U.S.

As we have seen, in the United States (and the world) there had been an historic disconnection between the tremendous technological advances of the 1960s-2000s and the regulations and public policy for this sector, despite its increasingly larger footprint and with overlaps with many other non-technological industries.

We saw how even in the U.S., where historically the most prominent Information Technologies (IT) companies have started, the regulation for this sector has been slow. Between the 1960s-2000s, the legislative branch of the government only mentioned cybersecurity just little over a thousand times, and the regulations specific for the sector were just a dozen. One can say that the terrorist attacks of September 11 of 2001 (9/11) were a turning point for the world, particularly in terms of how security (overall) was perceived, enforced, and more proactively engaged.

After 9/11 the world would never the same, and in the 2000's the world started to see a change of style for public policy, at least in the perception of importance of IT regulations, and of the increasing relevance of Cybersecurity as a hidden or underlying backbone of the country’s infrastructure. A glimpse of this change can be exemplified with this dialog of a confirmation hearing in the Senate that took place in 2011.

> “*Senator REED. […] I am old enough to remember when there were three dimensions of conflict—air, land, and sea […] But* **there is a whole new dimension, cyber**. ***I don’t think we know enough yet to be fully prepared****. […] we are just beginning to develop a strategy for a new dimension of warfare that we have never really confronted yet, and your leadership will be critical.*
>
> *Mr. PANETTA. […] I have often said that there is a strong likelihood that* **the next Pearl Harbor that we confront could very well be a cyber-attack that cripples our power systems, our grid, our security systems, our financial systems, and our governmental systems** *This is a real possibility in today’s world […]”* (U.S. Senate Armed Services Committee, 2011)

The dialogue comes from the Confirmation Hearing of Mr. Leon Panetta (then CIA Director) before the U.S. Senate Armed Services Committee on is nomination by President Obama to become the Secretary of Defense, back in June 9, 2011.

It is quite interesting how Senator Reed recognizes that he –and by extension, the Armed Services Committee- have very limited knowledge about Cyber. And even more interesting, the level of urgency that Mr. Panetta pledges by comparing the threats that the Cyber dimension represents with the next Pearl Harbor, perhaps the most recognizable act of war in U.S. soil in modern history. That marked the formal entry of the United States into World War II, triggered the Manhattan Project to develop the atomic bomb, and ended with the bombings of Hiroshima and Nagasaki in 1945. The analogy by Mr. Panetta illustrates the way legislators and policy makers started to change its perception towards Cyber-related issues by 2011. On the transcript of his hearing, Mr. Panetta also mentions that “I have a huge responsibility, if confirmed in this new position, in dealing with the cyber area through the National Security Agency (NSA) and others. My goal would be to work very closely with them and with others to develop not only the capability, but also the law that I think we need to have to determine how we approach this challenge in the future." (U.S. Senate Armed Services Committee, 2011). The need for guidance and regulation here is expressed at the highest and strategic level by the Secretary of Defense.

He talks about the country-level big picture, from the shoes of the Department of Defense (DOD), considering the broad toolbox that the country has allows the U.S. to plan for a broad and complex solution-approach to issues. As for cybersecurity, there are different aspects to it: the role that armed forces play, security and information agencies, energy, and resource agencies, all the way down to "the civilian world" with actors from the civil society such as corporations, universities, and citizens. This distinction is made to understand where the NIST Cybersecurity Framework sits in, and it's into this precisely into this civilian-world category. And while huge, it is just a fraction of the overall scope that Cybersecurity has.

Mr. Panetta's diagnostic was correct, in the sense that the United States needed a holistic approach for Cybersecurity, considering all available agencies, assets, and branches of the government for this task. With the Cybersecurity Act of 2012, which sought the definition of Critical Infrastructure, would have created voluntary standards for protecting key infrastructure, wanted to improve and consolidate existing federal resources for cybersecurity, and even aimed to require to address cybersecurity as a subject with elementary school students; or with the Cybersecurity Information Sharing Act of 2012 who sought to allow private entities to monitor information systems for cybersecurity threats. Mr. Panetta could have had his wishes come true: more resources and a more robust legal environment for Cybersecurity. Unfortunately, those acts failed to pass through the Senate and did not became law. The Financial Times reported on the challenges of creating laws to effectively govern the issue "legislation may be the only route to more transparency but policy makers are finding it hard to strike the right balance between safety and burden" (McCarthy, 2013).

However, a compelling argument of the importance of finding that balance came at the end of 2012 with the cyberattack to Saudi Aramco, a state-owned oil and gas company from Saudi Arabia, and one of the largest oil producers on the world. The attack took place on August 15, 2012, it affected about 30,000 workstations and forced the company to shut down 10 days (Leyden, 2012). This incident helped U.S. Secretary of Defense Leon Panetta to double down on the Pearl Harbor analogy of his confirmation hearing when commenting on the incident "The collective result of these kind of attacks could be a cyber Pearl Harbor […] An attack that would cause physical destruction and the loss of life, an attack that would paralyze and shock the nation and create a new profound sense of vulnerability" (Nakashima, 2012). This narrative would supported by the 2012 cyber-attacks to Bank of America, JPMorgan Chase, Wells Fargo, U.S. Bank, and PNC Bank, considered at the time "biggest cyberattacks in history" (Goldman, 2012).

1.3. Executive Order 13636: birth and development of the Framework

As the Obama administration had faced roadblocks with the legislative branch of the government, the lack of consensus at Congress, the inability to pass cybersecurity laws, and given the increasingly active cyber-warfare momentum, the White House was forced to come up with an alternative to address the issue. Enter the Executive Orders, the American Bar Association defines "An executive order is a signed, written, and published directive from the President of the United States that manages operations of the federal government" (American Bar Association, 2020). They act "like" a legislation, but as they are no proper laws, they escape the scrutiny and scope of the legislative branch. The U.S. Federal Register holds all executive orders, ordered by President and year of issue.

For the purpose of this study, we will discuss Executive Order 13636: Improving Critical Infrastructure Cybersecurity (U.S. Federal Register, 2013).

Among many provisions, this executive order:

- Defines Critical Infrastructure (based on Presidential Policy Directive: Critical Infrastructure Security and Resilience, also of 2013).
- Promotes Cybersecurity policy coordination through the National Security Council.
- Commands the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence to increase the volume, timeliness, and quality of Cybersecurity Information Sharing. And expands the use of private sector experts to reduce and mitigate cyber risks.

Mandates the National Institute of Standards and Technology (NIST) to develop a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. It must incorporate voluntary consensus standards, and industry best practices to the fullest extent possible. The Framework shall be consistent with voluntary international standards. The Executive Order was published on February 19 of 2013, and The National Institute of Standards and Technology (NIST) started working tight away: by February 26, 2013 it had published a notice on the Federal Register for Request for Information (RFI)

> *"NIST is conducting a comprehensive review to develop a framework to reduce cyber risks to critical infrastructure The Framework will consist of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. […] In developing the Cybersecurity Framework, NIST will consult with […] Sector-Specific Agencies and […] owners and operators of critical infrastructure, and other stakeholders including other relevant agencies, independent regulatory agencies, State, local, territorial, and tribal governments. The Framework will be developed through an open public review and comment process that will include workshops and other opportunities to provide input"* (U.S. Federal Register, 2013)

With the information gathered in the first RFI and a series of workshops, a Draft outline - Preliminary Framework was published in July 1, 2013. This was followed by a Message to Senior Executives on the Cybersecurity Framework, a Discussion Draft of the Preliminary Framework, a Draft Illustrative Examples of the Framework, a Discussion Draft of the Illustrate Examples. This initial work to develop a preliminary version culminated with the publishing of the Preliminary Cybersecurity Framework, followed by a Request for Comments on the Preliminary Cybersecurity Framework request on the Federal Register in October of the same year (National Institute of Standards and Technology, 2013).

As for what exactly the Framework really is, NIST defines it as:

> "*The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal*

> *and external organizational stakeholders*" (National Institute of Standards and Technology, 2020)

Following its preliminary definition, the Framework went on a progressive incremental revision process in its first year of development. What is remarkable about this initial process, is the involvement of different stakeholders, and the collaborative approach that industry, policy makers and interested parties were able to generate in a really comprised span of time.

For example, as NIST notes on the description of the Draft-outline publication of July 1st:

> *"The primary audiences for the document and intended users of the Framework are critical infrastructure owners and operators and their partners. However, it is expected that many organizations facing cybersecurity challenges may benefit from adopting the Framework. The Framework is being designed to be relevant for organizations of nearly every size and composition. It is also expected that many organizations that already are productively and successfully using appropriate cybersecurity standards, guidelines, and practices – including those who contributed suggestions for inclusion in this document – will continue to benefit by using those tools"* (National Institute of Standards and Technology, 2018)

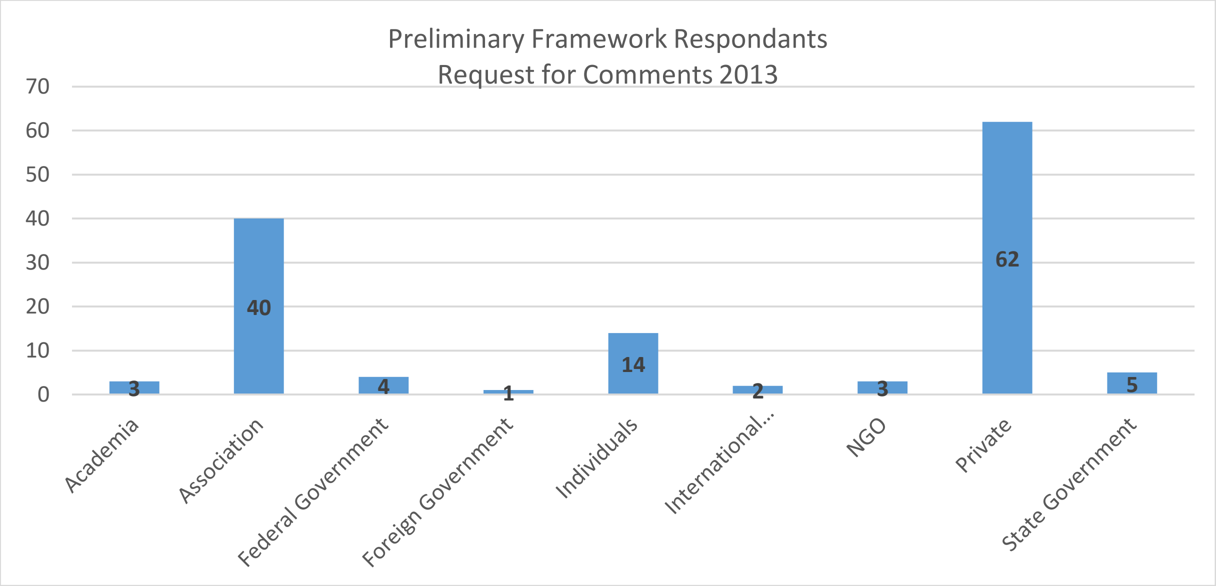
The relevance from this extract is the statement of the framework being designed to be relevant for entities of any size and composition –something that likely help in its international adoption-, and that it also builds up on the use/adoption of existing standards –another factor that will likely facilitate its adoption-.

The Request for Comments (RFC) on the Preliminary Cybersecurity Framework what went out in October of 2013 and that lasted for two months ended up getting comments from over 130 entities from the U.S. and the world who provided feedback for the Preliminary Framework.

This instance received comments by the International Telecommunication Union (ITU) which is the United Nations specialized agency for information and communication technologies. U.S. associations representing many of its U.S. and international members such as Computing Technology Industry Association (CompTIA), Telecommunications Industry Association (TIA) and the Information Technology Industry Council (ITI), and the U.S. Chamber of Commerce, among many others participated. Other U.S. firms also participated directly with comments, including Honeywell, IBM, Intel, Microsoft, and Symantec, along with Universities, members of the Academia and even private citizens.

On the initial development of the Preliminary Framework (2013), the respondents were analyzed (counting only one comment/part submitted). The aggregated results are as follow:

Figure 1: Preliminary Framework Respondents Request for Comments 2013



Personal compilation, based on data from "Initial Analysis of RFI (2013) - Preliminary Cybersecurity Framework" (National Institute of Standards and Technology, 2014)

This stage was heavily influenced by the Private sector, and Associations –with private sector members-, however it is quite positive to see that nearly every possible actor was represented and submitted comments.

We have also mentioned that one of the unique characteristics of the Framework is its voluntary basis for adoption, and to be consistent with voluntary international standards. Even Section 7 of Executive Order commands it directly: "The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order" (U.S. Federal Register, 2013).

The Framework responded to that commandment by relying on the respondents of the RFI, workshops, and RFC. In these instances, participants suggested different best practices, regulations, and standards already in use or recommended by themselves.

As NIST notes on the Preliminary Framework Compendium:

> "*The Framework's core also includes the compendium of informative references, existing standards, guidelines, and practices to assist with specific implementation. The compendium of informative references that included standards, guidelines and best practices is provided as an initial data set to map specifics to sub-categories, categories, and functions. The Framework's compendium points to many standards – including performance and process-based standards. These are intended to be illustrative and to assist organizations in identifying and selecting standards for their own use and for use to map into the core Framework. The compendium also offers practices and guidelines, including practical implementation guides*" (National Institute of Standards and Technology, 2018)

The Preliminary Framework Compendium is a spreadsheet that contains 448 specific regulations, standards, guidelines, best practices, and other suggestions already in use by the respondents. If we analyze these responses, we can notice how the references to Standards already in use, are by far, the most cited resource by respondents:

Table 2: Resources cited by respondents of RFC

Type of Resource	Instances	% of total
Standard	278	62%
Guidelines	52	12%
Other resources	22	5%
Best Practices	18	4%
Federal Regulation	16	4%
Framework	13	3%
Technical Report	11	2%
Report- Gov	10	2%

Maturity Model	8	2%
Specification	7	2%
Executive Order	5	1%
State Law	4	1%
Regulation	4	1%
Grand Total	448	

Personal compilation based on data from Preliminary Framework Compendium (National Institute of Standards and Technology, 2018)

Table 3: Scope of recommended resources by respondents of RFC

Type	Instances	% of total
General	202	45%
Sector-Specific	246	55%
Grand Total	448	

Personal compilation based on data from Preliminary Framework Compendium (National Institute of Standards and Technology, 2018)

If we analyze the type of resource, we can notice that Sector-specific resources slightly dominate the total of recommendations.

As some sample resources to get a broad idea of what was suggested by respondents, we observed that NIST received over 450 items in the RFI process and workshops (National Institute of Standards and Technology, 2019)

The development process receives 278 responses just on Standards

Table 4: Sample of suggested Standards

Organization	Title	Type	Source	Description
NIST	FIPS 140	Standard	https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdfhttp://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf	SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES
ISO/IEC	IEC 9899	Standard	http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=57853http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=57853	ISO/IEC 9899:2011 Information technology -- Programming languages -- C
IEEE	IEEE 1686	Standard	https://standards.ieee.org/standard/1686-2013.htmlhttp://Standards.ieee.org/develop/project/1686.html	P1686 - IEEE Draft Standard for Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
ISO	ISO 11568	Standard	https://www.iso.org/standard/34937.html	Banking -- Key management (retail)

Table 5: Sample of suggested Guidelines

Organization	Title	Type	Source	Description
ISO	ISO 19011	Guidelines	https://www.iso.org/standard/50675.html	Guidelines for auditing management systems
NIST	NIST SP 800-153	Guidelines	http://csrc.nist.gov/publications/PubsSPs.html	Guidelines for Securing Wireless Local Area Networks
ANSI	X9/ TG9	Guidelines	http://webstore.ansi.org/RecordDetail.aspx?sku=X9+TG-9%3A1995#.UcRk4fbwLq4	Abstract Syntax Notation and Encoding Rules for Financial Industry Standards

Table 6: Sample of suggested Best Practices

Organization	Title	Type	Source	Description
MAAWG	Best Practices to Address Online Mobile Threats	Best Practices	http://www.maawg.org/sites/maawg/files/news/M3AAWG_LAP_Best_Practices_to_Address_Online_and_Mobile_Threats_0.pdf	Best Practice prepared by international group of mobile experts from industry and government. It summarizes best practice recommendations to address new and more sophisticated online and mobile threats.
ISO	ISO 21188	Best Practices	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35707	Public key infrastructure for financial services Practices and Policy Framework

NIST	NISTIR 7622	Best Practices	http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf	NIST IR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems

To review a sample of how the comments were submitted by respondents, one can see the comments by CTIA- the Wireless Association. NIST has also made public:

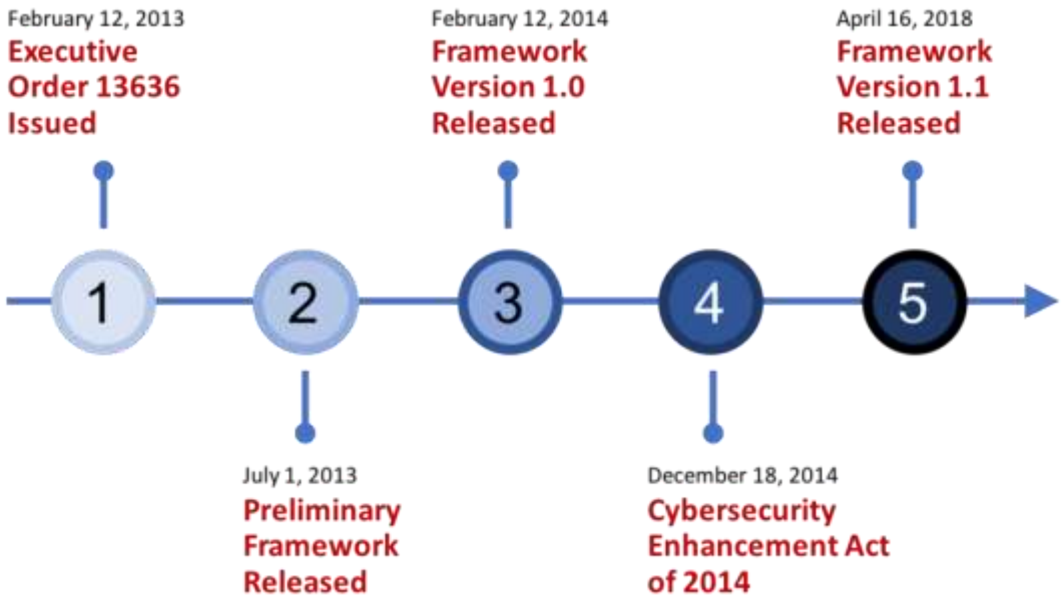
- The Initial Analysis of the Request for Information (RFI) responses.
- The Comments Received in Response to the Request for Comments (RFC) responses.
- The Analysis of Cybersecurity Framework RFI Responses
- A Development Overview of the Cybersecurity Framework

After the draft and preliminary versions of the Framework were completed, along with the RFI, RFC and 5 Cybersecurity Framework Workshops were completed, the Framework 1.0 was published on February 12, 2014. It gathered the yearlong collaborative work among stakeholders and regulators.

Later in 2017, version 1.0 was revised following a similar process:

- Publishing a Draft of the Cybersecurity Framework v1.1, followed by a Request for comments
- Industry workshops, and the publication of a 2nd Draft
- And finally, publishing the Framework 1.1 on April 16, 2018

Figure 2: Development milestones for the NIST CSF


February 12, 2013
Executive Order 13636 Issued
February 12, 2014
Framework Version 1.0 Released
April 16, 2018
Framework Version 1.1 Released
1
2
3
4
5
July 1, 2013
Preliminary Framework Released
December 18, 2014
Cybersecurity Enhancement Act of 2014

(National Institute of Standards and Technology, 2019)

Notably, along with the publication of the Framework update 1.1, came the roadmap for the Framework's future development process. This includes the participation of third parties, such as the British Standards Institute, and the Information Systems Audit and Control Association (ISACA) who at the time were developing "*confidence mechanism programs*" to help organizations assess its individual performance of the framework.

While the NIST CSF was a novel approach to cybersecurity back in 2013. Today there are several alternatives, and a variety of cybersecurity frameworks and standards are available to achieve different goals, these can be commonly classified as:

- Program Frameworks: ISO 27001, and NIST CSF
- Risk Frameworks: ISO 27005, and NIST 800-39
- Control Frameworks: CIS Controls (CSC), and NIST 800-53

However, specialized publications such as TechRepublic, PreyProject, IT Governance, and CyberExperts recognize the NIST Cybersecurity Framework among the top and most widely used alternatives that entities have available.

The framework also has been formally exposed to multilateral policy discussions as part of Asia-Pacific Economic Cooperation's (APEC) Sub-Committee on Standards and Conformance (SCSC), and the work that the International Trade Administration, part of the U.S. Department of Commerce, has conducted with the projects Facilitating Trade through Adherence to Globally-Recognized Cybersecurity Standards and Best Practices (2019), and APEC Workshop on Approaches for Communicating Cybersecurity Practices to Stakeholders (2020). In these instances, the Department of Commerce has been able to share the experience of the United States with the NIST Cybersecurity Framework, with important policy influencers around the world.

The United States, through the U.S. Department of Commerce, has found a "recipe" for success in the way the NIST CSF was developed and continues to be updated. This formula appears to continue expanding, now with other technology areas such as Distributed Ledger Technologies (DLT) and Blockchains and also Internet of Things (IoT), only time will tell if this was successful, but –so far- it seems to be going in the same direction as the CSF, and that worked just fine. IoT will be huge, with estimations calculating the *"IoT total spending of nearly $1.4 trillion by 2021"* (Crowell & Moring, 2019).

In this section, we described the historical context that triggered the creation of the NIST CSF, why it was needed, and how it was developed by the cooperation between the U.S. Government and many other public and private stakeholders. The Framework has not remained static and continues to evolve. In the next chapter we will take a deep dive into the structure of the Framework, examining its functions, profiles and implementation tiers.

PART II: The NIST Framework: How it works?

This part of the study examines the NIST Cybersecurity Framework, particularly its components: its core, tiers, and different profiles.

Figure 3: NIST Cybersecurity Framework

CORE
TIERS
CYBERSECURITY
FRAMEWORK
PROFILE

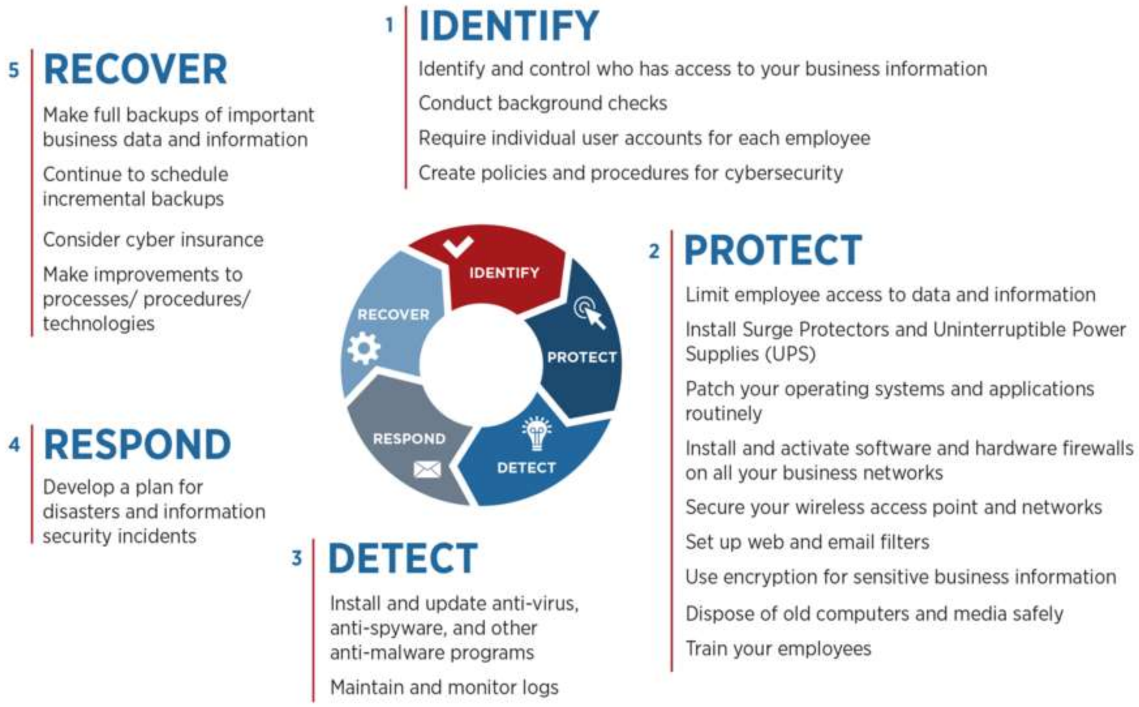
(National Institute of Standards and Technology, 2020)

2.1. NIST Framework Core Functions

The **Core of the Framework** consists of Cybersecurity activities and informative references, organized around particular outcomes. The 5 functions – presented in the image below - are considered the core of the Framework: Identify, protect, detect, respond, and recover. According to NIST:

> *"The Functions are the highest level of abstraction included in the Framework. They act as the backbone of the Framework Core that all other elements are organized around.*
>
> *These five Functions were selected because they represent the five primary pillars for a successful and holistic cybersecurity program. They aid organizations in easily expressing their management of cybersecurity risk at a high level and enabling risk management decisions"* (National Institute of Standards and Technology, 2018)

Figure 4: NIST CSF Functions


1 IDENTIFY
Identify and control who has access to your business information
Conduct background checks
Require individual user accounts for each employee
Create policies and procedures for cybersecurity
2 PROTECT
Limit employee access to data and information
Install Surge Protectors and Uninterruptible Power Supplies (UPS)
Patch your operating systems and applications routinely
Install and activate software and hardware firewalls on all your business networks
Secure your wireless access point and networks
Set up web and email filters
Use encryption for sensitive business information
Dispose of old computers and media safely
Train your employees
3 DETECT
Install and update anti-virus, anti-spyware, and other anti-malware programs
Maintain and monitor logs
4 RESPOND
Develop a plan for disasters and information security incidents
5 RECOVER
Make full backups of important business data and information
Continue to schedule incremental backups
Consider cyber insurance
Make improvements to processes/ procedures/ technologies
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

(National Institute of Standards and Technology, 2018)

These Five functions are at the very center of the Framework, in what NIST defines as the Framework Core. The core, starting by each of the functions defines 23 different “Categories” of activities and outcomes. It allows entities to think in cybersecurity terms but in a non-technical way, moving from business-oriented type of questions, towards other more task-oriented (and more technical in nature) at the end of the process. The core covers topics across cyber, physical, and personnel.

In this context, **Identify** seeks to trigger the questioning and evaluation within the organization. The question that an entity will have ask itself is “What processes and assets need protection?” at the same time, if we drilled down on the categories under the function Identify, we will find a simple division of the functional aspects of an organization. Categories under this function are:

- Asset Management
- Business Environment

- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management

The function of **Protect** aims to map out the safeguards that are available within the organization. The question that an entity will have ask itself is “What safeguards are available?”. Categories under this function are:

- Identity Management and Access Control
- Awareness and Training
- Data Security
- Information Protection Processes & Procedures
- Maintenance
- Protective Technology

The function of **Detect** aims to unveil the activities and processes that entities must monitor to detect threats and incidents. The question that an entity will have ask itself is “What techniques can identify incidents?”. Categories under this function are:

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

The function of **Respond** seeks identify resources and assets for the organization to respond, mitigate or improve in the event of an incident or a breach. The question that an entity will have ask itself is “What techniques can contain impacts of incidents?”. Categories under this function are:

- Response Planning

- Communications
- Analysis
- Mitigation
- Improvements

The function of **Recover** aims to map out the resources the organization must have to recover after a breach or incident has happened. The question that an entity will have ask itself is "What techniques can restore capabilities?". Categories under this function are:

- Recovery Planning
- Improvements
- Communications

Also, within each of the categories we will find **Subcategories**, which NIST defines as

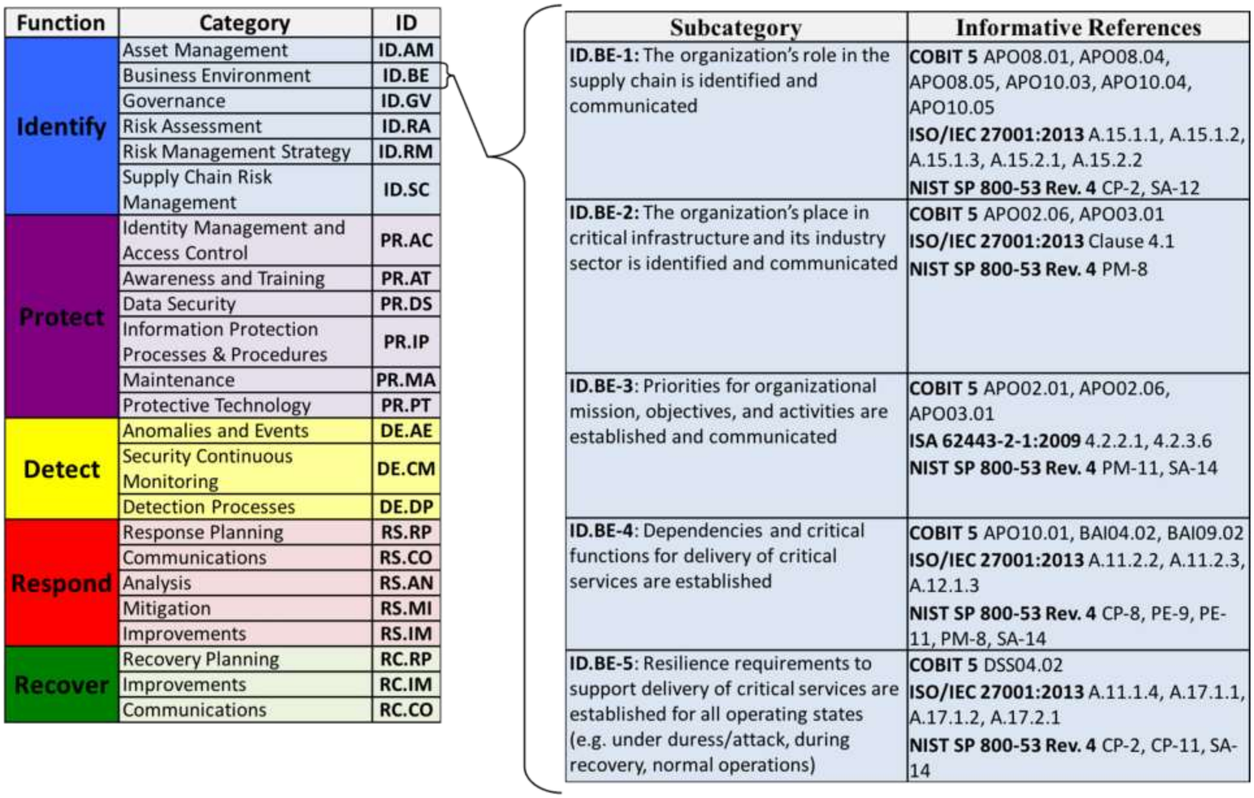
> *"The deepest level of abstraction in the Core. There are 108 Subcategories, which are outcome-driven statements that provide considerations for creating or improving a cybersecurity program. Because the Framework is outcome driven and does not mandate how an organization must achieve those outcomes, it enables risk-based implementations that are customized to the organization's needs"* (National Institute of Standards and Technology, 2020)

Is at the Subcategory level where we can see the direct link between the Framework and industry recognized standards. The rationale (or processes) behind it is that: an entity goes through each of the **Functions** (5), and then review each of the **Categories** (23), and –when needed- will go and examine specific **Subcategories** according to its needs. These subcategories will reference specific resources/standards/best-practices that entities may use to address each of the topics.

The process that entities should follow, goes like this:

FUNCTION ➤ Category ➤ Subcategory ➤ Standard/Resources

Figure 5: NIST CSF Categories, Subcategories, and Informative References



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

(National Institute of Standards and Technology, 2020)

The overall Framework Core consist of:

- 5 Functions
  - 23 Categories
    - 108 Subcategories
      - Informative References

As for the Informative References, NIST mentions:

> *"Through the early Requests for Information (RFIs) and Framework Workshops, NIST considered a large compendium of standards, guidance, and publications consisting of over 450 items. Ultimately, six of these were selected to become informative references included in the Framework Core due to being broad*

> *references which were widely recognized, and had a large adoption rate"* (National Institute of Standards and Technology, 2019)

This is the current list of informative resources that NIST recommends as part of the Framework:

Table 7: Table 4: Scope of recommended resources by respondents of RFC

Informative Reference	Link
NIST SP 800-53 Rev. 4	nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-
ISO/IEC 27001:2013	iso.org/standard/54534.html
COBIT 5	isaca.org/cobit/pages/default.aspx
CIS CSC	cisecurity.org/controls/
ISA 62443-2-1:2009	isa.org/templates/one-
ISA 62443-3-3:2013	isa.org/templates/one-

Informative References Included in the Framework Core (National Institute of Standards and Technology, 2019)

NIST provides an example of how entities work with these references:

> *"A healthcare organization who organizes their existing controls around NIST 800-53 and is seeking to become ISO compliant may choose to use the ISO/IEC 27001 and the NIST 800-53 mappings included in the Framework Core along with the mapping for HITRUST from the larger Informative References catalog that applies specifically to healthcare organizations"* (National Institute of Standards and Technology, 2019)

In this case, the healthcare organization is working with NIST 800-53, a standard for **Security and Privacy Controls for Federal Information Systems and Organizations** and also with ISO/IEC 27001:2013, a standard for **Information technology, Security techniques, Information security management systems**.

2.2. Profile and Implementation Tiers

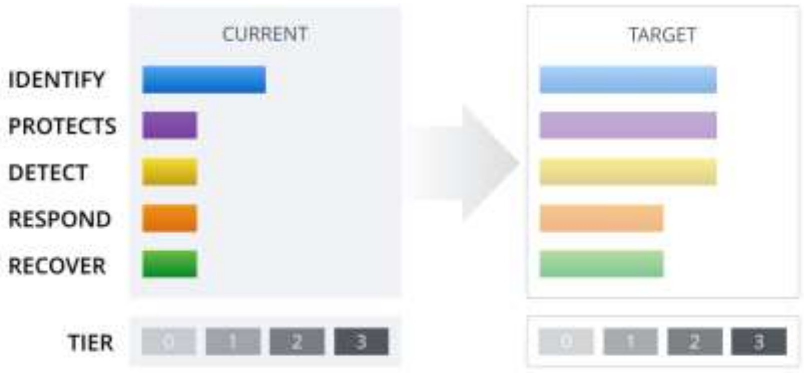
The component of the Framework that allows organizations to "align industry standards and best practices to the Framework Core in a particular implementation scenario" is the **Profile** (National Institute of Standards and Technology, 2020)

According to NIST, a Framework Profile

> "*Is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs*" (National Institute of Standards and Technology, 2018)

Having created a baseline benchmark by mapping out the Core of the framework, and after completing an Implementation Tier assessment, an entity can determine where it stands in terms of cybersecurity. And from there, define its goals to where it wants to be in the future.

Figure 6: NIST CSF Functions, Tiers and Targets



(Chang-Gu, 2015)

The Tiers provide an organization views on cybersecurity risk:

> "*Provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Ranging from Partial (Tier 1) to Adaptive (Tier 4), Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices*" (National Institute of Standards and Technology, 2018)

The TIERS are the level of importance that an entity gives to a given process, from 1 to 4, they are classified as followed:

Tier 1: Partial

Tier 2: Risk Informed

Tier 3: Repeatable

Tier 4: Adaptive

These are not necessarily maturity levels. Its main purpose is to describe:

> "*an increasing degree of rigor and sophistication in cybersecurity risk management processes, how well integrated cyber risk decisions are into broader risk decisions, and the degree to which the organization shares and receives cybersecurity info from external parties*" (National Institute of Standards and Technology, 2020)

In the implementation of the tier, the entity must analyze its own:

- Risk Management Process
- Integrated Risk and Management Program
- External Participation

To determine its current implementation tier, for each of the functions (and categories).

Table 8: Comparison of Implementation Tiers

	Tier 1: Partial	Tier 2: Risk Informed	Tier 3: Repeatable	Tier 4: Adaptive
Risk Management Process	Not formalized Ad-hoc risk Reactive	Formalized (but limited) Prioritizing of Cyber activities by objectives	Formalized and wide Practices tied to Risk mgmt. assessments and can adapt	Adapts formalized cyber practices. Continuous improvement. Adapts to change
Integrated Risk Management Program	Limited awareness Irregular risk management No internal information sharing	Awareness of Cybersecurity risk Occasional cyber-risk assessment Informal information sharing	Org. wide approach to Cyber Risk informed policies Formal information sharing	Org. wide approach to Cyber well understood. Budget for risk mitigation. Cyber-culture at org.
External Participation	Doesn't understand ecosystem Doesn't collaborate No external information sharing	Understands role on ecosystem Collaborates with others May share information	Understands larger role Acts formally on risk and collaborates. Shares information	Acts on role + community Internal & external info sharing. Communication with clients

Personal summary, based on NIST Cybersecurity Framework (National Institute of Standards and Technology, 2020)

All in all, the structure of the Framework allows entities to map out its own resources, it encourages organizations to think in order to identify the different functions and responsibilities to prevent breaches and to react and respond when these happen. And the Implementation Tiers allow organizations to be able to measure their state of maturity while planning a road ahead to continue improving. This *simple* yet attainable self-examination has turned the NIST CSF into a very popular entry level assessment for organizations seeking to establish a baseline for the understanding of their own cybersecurity maturity, and a clear path for improvement.

2.3 Traction of the Framework

Its easy and free access, voluntary adoption, and down to earth approachability has made the NIST CSF a recognizable resource that its used globally. The popularity and impact of the Framework can be illustrated by its translations and documented adoption around the world. It has translated and/or adapted to many languages and by different countries:

- Arabic Translation
- Bulgarian Translation
- Japanese Translation
- Polish Translation
- Portuguese Translation
- Spanish Translation
- Israel’s Cyber Defense Methodology (based on the CSF)
- Italy's National Framework for Cyber Security (based on the CSF)
- Ontario Cyber Security Framework
- Scotland's Public Sector Action Plan 2017-2018
- Uruguay's Cybersecurity Framework v4.0

(National Institute of Standards and Technology, 2020)

Also, we can track down mentions and references by official government sources from around the world. In this sense, it is possible to grasp its popularity at the governmental level, but due to its voluntary adoption it is much tricker to track and document its influence with private entities and corporations. While entities can interact with NIST and share supportive quotes or lessons learned as part of their implementation process, for the most part it is difficult to track down private adoption and adherence to the Framework. At the same time, because of the voluntary character of the mapped processes, “compliance” with the Framework is not “certifiable” by NIST itself.

However, there are private entities that offer cybersecurity assessments based on the NIST framework, such as Tenable, ComplianceForge, Netsurion, and others. An aspect that can facilitate this process, is the concordance of the NIST CSF and standards such as the ISO 27001, in fact some companies offer the combined mapping for both bodies.

NIST also has a repository of Success Stories, with the testimonies of different entities not just from the U.S. For example, Saudi Aramco, the oil company that suffered a big cybernetic attack in 2012 (something that helped fast track the discussion on cybersecurity policy in the U.S.) tells one of those success stories.

While as a voluntary standard, the NIST framework cannot be certified by NIST or other entities, some private parties have developed process to audit and certify compliance with the Framework, and particularly its international spin off, the ISO/IEC TR 27103:2018.

Companies such as Tenable advertise its services as "Tenable Security Center Continuous View *provides automation and continuous monitoring capabilities that allow for the efficient and effective adoption of the NIST Cybersecurity"* (Tenable, 2020). Other service providers, such as Amazon Web Services offer its cloud environment as aligned with the NIST CSF and emphasizes its native adoption of the framework's recommendations as a basic feature for its services.

In this chapter we have analyzed the NIST CSF, its ability to map out resources, assign responsibilities, and overall assess risk and inform of the different maturity levels that organizations can have when it comes to cybersecurity. Also, we have seen how the influence of the Framework has gone beyond the United States with the different translations and adaptations of the model into a variety of languages and different implementation solutions. The framework has been put at the disposal of whoever needs to use it, its simplicity and ease of implementation has turned the tool into a popular Cyber/IT risk assessment tool, that has even created a niche industry that certifies and facilitates compliance with the Framework or its parts.

In the following section, we will review the region of South America and how it has evolved in technology and cybersecurity terms in recent years, trying to identify if there is a link between the establishment and development of the NIST CSF and the changes in the region.

PART III: Cybersecurity in South America.

The technology world is driven by innovation. A straight forward angle to unveil innovation is to check patent filling requests, according to the World Intellectual Property Organization (WIPO), the world's leading countries in patent fillings for Computer technology and Digital communications are the U.S., China, the Republic of Korea, and Japan (World Intellectual Property Organization, 2019). And while companies filling those patents might have interesting strategies for patent applications, and not necessarily come from the countries where the patent request is filled, one thing is clear: South America is nowhere to be found in those rankings. And makes the region a de facto policy follower in terms of policy for technologies, including cybersecurity.

This chapter will describe the state of the art of some technologies that are closed connected with the cybersecurity, including Information and Communications Technologies (ICT), Digital Economy and eGovernment in South America. We will also explore how the region is doing in Cybersecurity analyzing the Incidents in the region, and Key Elements for policy analysis, such as the definition of Critical Infrastructure, the existence of: a National Cybersecurity Strategy, a Framework for Cybersecurity, an Agency dedicated to Cybersecurity and a Taskforce Response Team, and whether there is a clear definition of Critical Infrastructure.

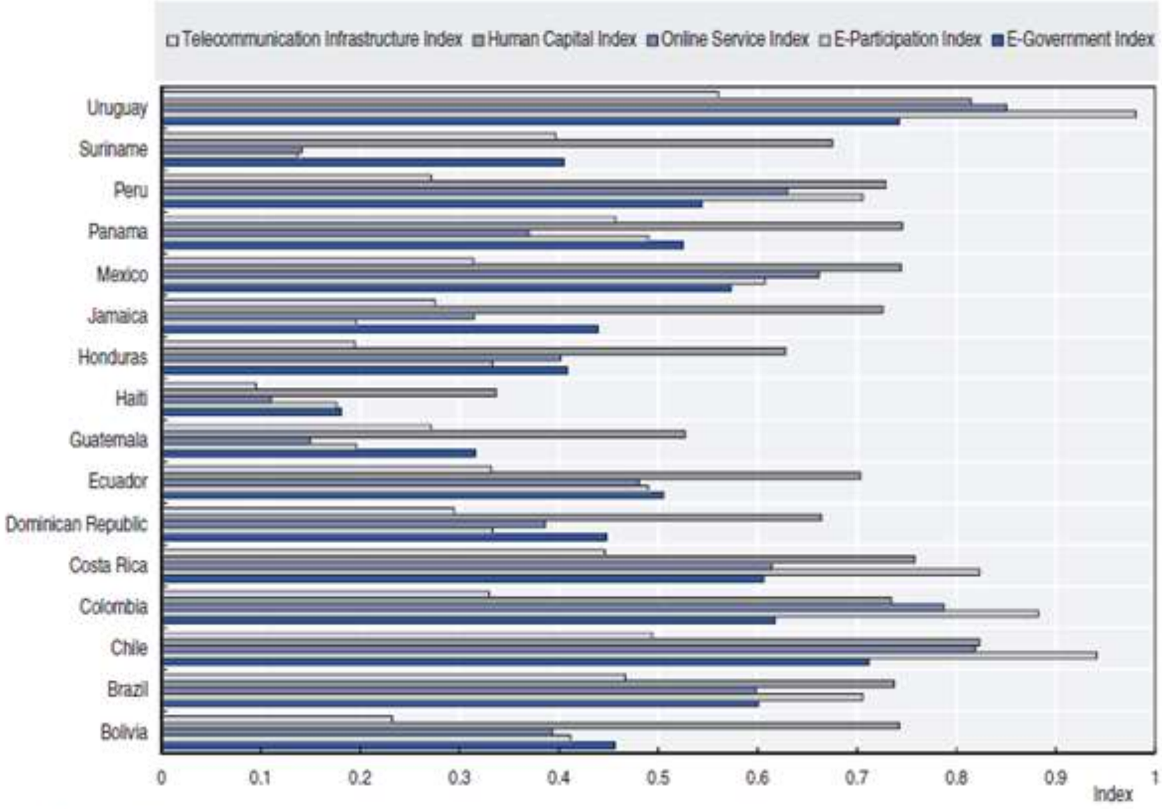
As trying to analyze the entire region would be too demanding, we will narrow down the scope of analysis to the most prominent markets, the ones more likely to have policy innovations relevant to cybersecurity.

3.1 WHO's who in South America

When studying South America, one fact that rapidly becomes evident is the diversity in terms of development. For example, if we analyze the Electronic Government Index of the United Nations, we can already notice the tremendous differences that can be found on all the elements that the index captures:

- Telecommunication Infrastructure Index
- Human Capital Index
- Online Service Index
- E-Participation Index
- E-Government Index

Figure 7: United Nations E-Government Index (2014)



Source: UN (2014), United Nations E-Government Survey 2014, https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2014.

StatLink http://dx.doi.org/10.1787/888933354510

(Inter-American Development Bank & Organisation for Economic Co-operation and Development, 2016)

Uruguay and Haiti are two completely opposite realities. And their priorities –and policies- would be to no surprise, quite different. The same applies to the broader sample of countries.

In the region, the access to the Internet is another useful comparison data point. To evaluate this, we will use the publication "State of broadband in Latin America and the Caribbean, 2017" published by the United Nations Economic Commission for Latin America and the Caribbean (CEPAL).

Figure 8: Households with internet and Penetration of fixed and mobile broadband

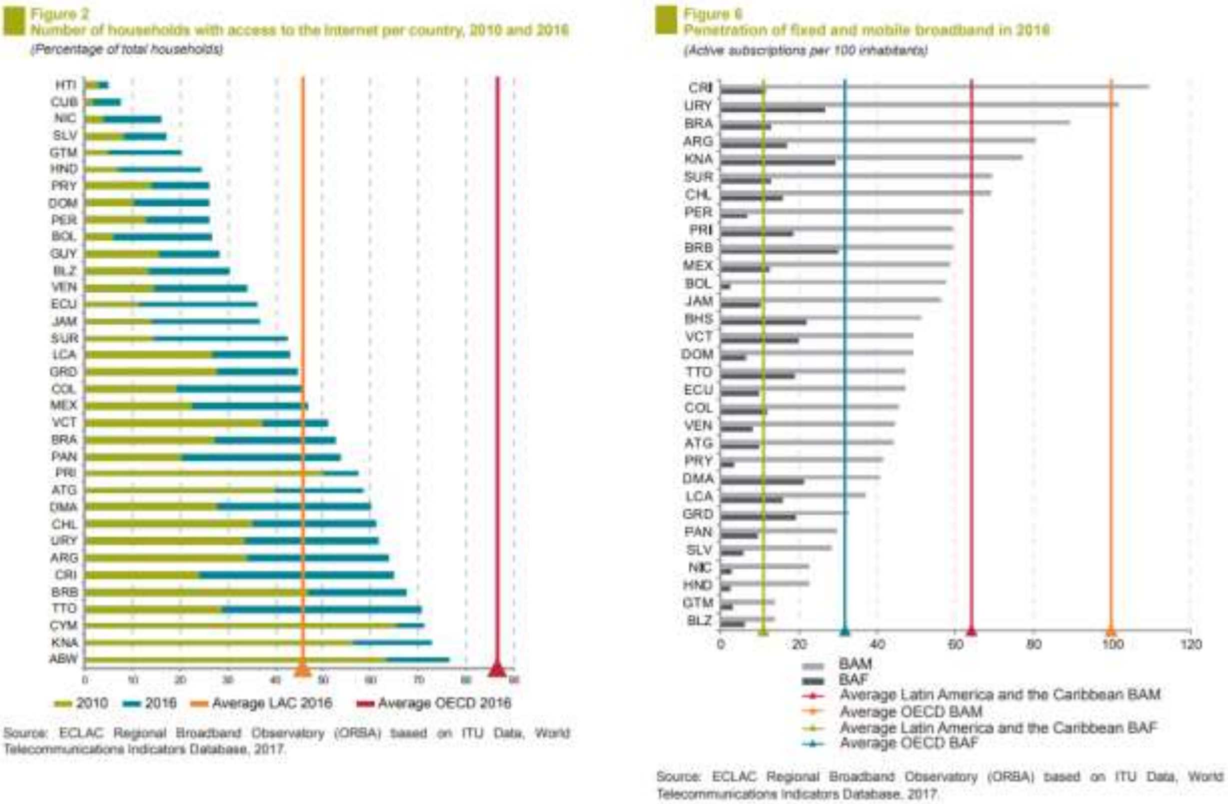


Figure 2
Number of households with access to the Internet per country, 2010 and 2016
(Percentage of total households)

Source: ECLAC Regional Broadband Observatory (ORBA) based on ITU Data, World Telecommunications Indicators Database, 2017.

Figure 6
Penetration of fixed and mobile broadband in 2016
(Active subscriptions per 100 inhabitants)

Source: ECLAC Regional Broadband Observatory (ORBA) based on ITU Data, World Telecommunications Indicators Database, 2017.

(Economic Commission for Latin America and the Caribbean, 2017)

In this case, when analyzing internet penetration and broadband, we continue to see a huge gap between Haiti and Uruguay or Costa Rica. Reinforcing the idea of a fragmented region, particularly on infrastructure for telecommunications.

Based on this and trying to get a sounded and representative set of countries from South America, with a high percentage of internet use, access to broadband, and digital government initiatives, we will narrow down the countries for this analysis to **Argentina, Brazil, Chile, Colombia, and Uruguay.**

Information on cybersecurity incidents it is difficult to track, mainly because the entities that have suffered attacks don't want to publicize such events for fear it will impact its reputation negatively. From the evidence and data that is available in public outlets, most of the information available for this is related to Financial Institutions.

According to the State of Cybersecurity in the Banking Sector in Latin America and the Caribbean report, in Latin America "At least 9 out of 10 banking entities suffered cyber incidents during the last year (2018), and 37% of the banks in the region were victims of successful attacks" (Organization of American States, 2018).

The incident that has received the most press coverage in the selected markets of this study, was the register in May of 2018, when Banco de Chile, one of Chile's biggest banks, was the target of a SWIFT-related cyber-attack and lost over $10 million USD (Reuters, 2018)

In order to get a regional sense of the attacks on the region, we will use rely on information by Carnegie's Cyber Policy Initiative, which uses data from Cyber Threat Intelligence unit of BAE Systems (Carnegie Endowment for International Peace & BAE Systems, 2020). According to this platform, the 2010's decade looked like this in South America, particularly in Argentina, Brazil, Chile, Colombia and Uruguay:

Table 9: Publicly available reported incidents

Year	**Argentina**	**Brazil**	**Chile**	**Colombia**	**Uruguay**
2010	n/a	n/a	n/a	n/a	n/a
2011	n/a	n/a	n/a	n/a	n/a
2012	n/a	Brazil Banks DDoS Attacks Brazilian Payments System Attack	n/a	Operation High Roller	n/a
2013	n/a	n/a	n/a	n/a	n/a
2014	n/a	n/a	n/a	n/a	n/a
2015	n/a	n/a	n/a	n/a	n/a
2016	n/a	n/a	n/a	n/a	n/a
2017	n/a	n/a	n/a	n/a	n/a
2018	n/a	Brazilian Mobile	Banco de Chile	n/a	n/a
2019	n/a	Banco Pan Data Breach	Chile ATM Attack Silence Group Targets	n/a	n/a
2020	DeathStalker	Vizom Banking	Banco Estado		
Incidents	**1**	**5**	**4**	**1**	

Personal compilation, based on data from Timeline of Cyber Incidents Involving Financial Institutions (Carnegie Endowment for International Peace & BAE Systems, 2020)

Some notable exceptions to this list are the Panama Papers leaks of 2016, and the attack to the Peruvian Banco de la Nación in 2018, but both attacks occurred outside the borders of the selected countries for this study, even though some institutions might have been impacted by the leaks of 2016, but no actual financial information was lost in the selected countries.

As we can see, 11 cybersecurity incidents have been public over the last decade in Argentina, Brazil, Chile, and Colombia. In comparison, the region seems to be a relatively peaceful region, during the same period Eastern Europe had 9 incidents, Western Europe 19 incidents, and the U.S. registered 31 incidents. However, if we consider that these are just the number of publicly recognized incidents, the substance of the numbers can be questioned. According to a study by Accenture, "The average number of breaches per company has more than tripled over the past five years, from 40 in 2012 to 125 in 2017" (Accenture, 2018). The study also mentions that "nearly 60% of financial services companies 'total security cost is spent on containment and detection of cyber breaches" (Accenture, 2018). If we were to make an estimation of "actual breaches" by factoring the number of attacks provided by Accenture, we have a radically different picture:

Table 10: Estimation of actual annual breaches by country (Financial Institutions)

Country	Number of Banks	Accenture's estimation per financial institution	Estimated number of annual breaches
Argentina	12	x 125	1,500
Brazil	20		2,500
Chile	26		3,250
Colombia	11		1,375
Uruguay	23		2,875

Personal compilation, based on data from Timeline of Cyber Incidents Involving Financial Institutions (Accenture, 2018) *and List of Banks all the banks in the World by Country*

As we mentioned, this is the count of publicly disclosed incidents, so the actual number is expected to be higher, since the analysis of Carnegie's only considers the major incidents, and not all incidents are reported. Compiling data from different sources could compromise the reporting standardization, so therefore better to stick with one comparable source for all markets.

3.2 Key Elements of Cybersecurity analysis

For this section, we will work based on the information by the report "Cybersecurity Are We Ready in Latin America and the Caribbean?" (Inter American Development Bank & Organization of American States, 2016). This publication establishes a type of ranking to measure the maturity of each market, and its stability among other factors in a comparable way that facilitates our analysis. Also, we have cited the criteria for analysis covered on prior tables.

To compare the selected markets, we try will identify the following concepts in their respective legislations.

- **National Security Strategy** (NSS): "key framework for a country to meet the basic needs and security concerns of citizens, and address external and internal threats to the country" (DCAF-ISSAT, 2020)

- **National Cybersecurity strategy**: same as NSS, but specific to Cybersecurity

- **Government Agency dedicated to Cybersecurity**: the country has it Yes/No.

- **Cybersecurity Taskforce**: that exists to monitor and respond on cybersecurity incidents. Yes/No.

In the following table we will review if the countries have the key elements of cybersecurity. If the resource is present, it will be linked.

Table 11: Presence of Key Elements of Cybersecurity on selected markets

	Argentina	Brazil	Chile	Colombia	Uruguay
National Security	Yes	Yes	Yes	Yes	Yes
National Cybersecurity	Yes	Yes	Yes	Yes	Yes
Cybersecurity Framework	No	No	No	No	Yes, based on NIST
Government Agency dedicated to Cybersecurity	Yes, "Dirección Nacional de Ciberseguridad"	Yes, "Centro de Defensa Cibernética"	Yes, "Sistema Nacional de Ciberseguridad"	Yes, "Centro Cibernetico Policial"	Yes, "AGESIC (Agencia de Gobierno Electrónico y Sociedad de la Información)"
Cybersecurity Taskforce	Yes, MINSEG-CSIRT	Yes, CERT.br Brazilian National Computer Emergency Response Team	Yes, CSIRT Computer Security Incident Response Team	Yes, Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT	Yes, Centro de Respuesta a Incidentes de Ciberseguridad (CERT)

Personal compilation based on official sources on each market. References directly linked.

Other Key Elements of this analysis are the existence of a Critical Infrastructure definition, and by specific guidelines or recommendations by government agencies on the Telecommunications and Financial Services sectors, which are the most likely to produce recommendation because of the industries that they regulate.

Table 12: Definition of Critical Infrastructure on selected markets

Country	Definition	Legislation/Resource that includes it	Page or reference	Date Established
Argentina	Yes	Resolución 580/2011: Programa Nacional de Infraestructura Critica (Jefatura de Gabinete de Ministros)	First section	July, 2011
Brazil	Yes	Política Nacional de Segurança de Infraestruturas Críticas (Presidência da República)	Art. 1	November, 2018
Chile	Yes	Norma Técnica sobre Fundamentos de Ciberseguridad para Telecomunicaciones (Diario Oficial)	Page 4	Augusto, 2020
Colombia	Yes	Agenda Estratégica de Innovación: Ciberseguridad (Ministerio de Tecnologías de la Información y las Comunicaciones)	Page 14	March, 2014
Uruguay	Yes	Decreto 65/020: Sistema Nacional de emergencias (Consejo de Ministros)	Art. 2	March, 2020

Personal compilation based on official sources on each market. References directly linked.

Table 13: Official Mentions to the NIST Cybersecurity Framework

Country	Definition	Legislation/Resource that includes it	Page or reference	Date Established
Argentina	Yes	Decálogo Tecnológico ONTI (Oficina Nacional de Tecnologías de Información)	Recursos	November, 2018
Brazil	Yes	Aprova a Estratégia Nacional de Segurança Cibernética (Diário Oficial)	Parte I	February, 2020

Chile	Yes	Programa de Formación para la Seguridad de la Información y la Ciberseguridad (CORFO)	Módulo 1	September, 2018
Colombia	Yes	Revisión del marco regulatorio para la gestión de riesgos de seguridad digital (Comisión de Regulación de Comunicaciones)	Evaluación de Estándares y Mejores Prácticas de Seguridad Digital (p57)	November, 2017
Uruguay	Yes	Marco de Ciberseguridad (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento)	1st paragraph	March, 2020

Personal compilation based on official sources on each market. References directly linked.

Table 14: References to NIST CSF in Cybersecurity, Telecom and/or Financial Services regulations

Country	Definition	Legislation/Resource that includes it	Page or reference	Date Established
Argentina	Yes	Glosario de Ciberseguridad (Banco Central de la República Argentina)	Función "Detectar"	November, 2018
Brazil	Yes	Fórum Infraestruturas do Mercado Financeiro (Banco Central do Brasil)	Page 18	December, 2018
Chile	Yes	Concursos 5G, Norma técnica Ciberseguridad y Puerta Digital Asia Sudamérica (Subtel)	Objetivos norma técnica de ciberseguridad	July, 2020
		Evaluación del Grado de Madurez de los Procesos de Ciberseguridad (Banco Central)	Antecedentes técnicos	July, 2020
		Avances tecnológicos y desarrollo del Mercado de Capitales de Chile (Comisión para el Mercado Financiero)	Proyecto de Ley de Ciberseguridad para el sector Financiero	October, 2018

Colombia	Yes	Smart Grids Colombia Vision 2030 (Unidad de Planeación Minero-Energética)	Page 17	April, 2016
Uruguay	Yes	Cuenta Pública Presidencial (Presidencia de la República)	Page 176	February, 2019

Personal compilation based on official sources on each market. References directly linked.

3.3 Cybersecurity Sophistication index

In order to compare these markets in a structured way we will establish a index model by combining the elements from Tables 11 to 14 and assigning "points" to each of the sections, each criterion has its respective point matrix and its designed to measure and compare the Policy sophistication of each of the markets in regards to cybersecurity:

Table 15: Country Cybersecurity Sophistication index

Criteria	**COUNTRY**	Date	Points
1. National Security Strategy	YES: **0.2 points** - NO: 0 points		
2. National Cybersecurity Strategy	YES - date before Dec. 2013: 0.2 point, **after 2014: 0.5 points**. NO: 0 points		
3. Cybersecurity Framework	YES: **1.5 points** - NO: 0 points		
4. Government Agency dedicated to Cybersecurity	YES - date before Dec. 2013: 0.1 point, **after 2014: 0.5 points**. NO: 0 points		
5. Cybersecurity Taskforce	YES: **0.3 points** - NO: 0 points		
6. Definition of Critical Infrastructure	YES - date before Dec. 2013: 0.5 point, **after 2014: 1 point**. NO: 0 points		
7. Official Mentions to the NIST CSF	YES: **1.5 points** - NO: 0 points		
8. Other sectoral Cyber regulation referencing NIST CSF	YES: **0.5 points** - NO: 0 points		
		Points	

Personal compilation based on official sources on each market. References directly linked.

In total 6 points are the maximum that can be obtained in this classification.

We can categorize the results as:

a. 0 to 1.9 points = NIST CSF has LOW influence in the market
b. 2.0 – 3.9 points = MID influence
c. 4.0 – 6.0 points = HIGH influence

While there are multiple elements that can influence policy decisions, the scorecard has been designed attributing more points to the elements that are more closely related with the creation of the Framework, such as specific references to a country having a Cybersecurity Framework (a concept that didn't exist prior to the NIST CSF), and official mentions to the NIST CSF. While the definition of Critical Infrastructure could have been established prior to the creation of the Framework, the data suggest that the majority of these definitions were established after the United States served as an example to other countries by establishing its own definition.

The rationale behind this structure assumes the availability of the framework makes it an influential factor in the policy definition of each country. By defining the index using the criterion that we already had defined as key elements for cybersecurity, we will be able to compare the different policy realities of the selected markets.

The index is inspired by the work of Anthoula, K., & Alexandros, H. in the adaptation of the Balance Scorecard methodology -typically used to measure business and operational performance in private entities- for the adapted evaluation of a local authority organization (Kladogeni & Alexandros, 2011)

In the next section, by using the *Country Cybersecurity Sophistication index* we evaluate each one of the countries using this methodology. The main goal is to provide an explanation to market changes related to regulatory aspects for cybersecurity, critical infrastructure, and framework adoption among others.

PART IV: Country analysis

In this section, we will analyze each of the markets by using the *Country Cybersecurity Sophistication index* of Table 15, that in turn combines the information of Tables 11 to 14, allowing a comparison between the markets, we will be seeking for references to National Security Strategy, National Cybersecurity Strategy, Cybersecurity Framework, Government Agency dedicated to Cybersecurity, Cybersecurity Taskforce, Definition of Critical Infrastructure, Official Mentions to the NIST CSF, and Other sectoral Cyber regulation referencing NIST CSF.

4.1 Argentina

Table 16: Cybersecurity Sophistication index - Argentina

Criteria	Detail	Date	Points
1. National Security Strategy	Libro Blanco de la Defensa - República Argentina	1998	0.2
2. National Cybersecurity Strategy	Estrategia Nacional de Ciberseguridad de la República Argentina	2019	0.5
3. Cybersecurity Framework	No	-	0.0
4. Government Agency dedicated to Cybersecurity	Dirección Nacional de Ciberseguridad	2019	0.5
5. Cybersecurity Taskforce	MINSEG-CSIRT	2017	0.3
6. Definition of Critical Infrastructure	Resolución 580/2011: Programa Nacional de Infraestructura Critica	2011	1.0
7. Official Mentions to the NIST CSF	Decálogo Tecnológico ONTI	2018	1.5
8. Other sectoral Cyber regulation referencing NIST CSF	Banco Central de la República Argentina – Glosario de Ciberseguridad	2018	0.5
		Points	**4.5**

In Argentina, the regulatory baseline indicates that the country is an early adopter. Argentina established its **Computer Security Incident Response Team** (CSIRT) back in 1994. This unit operated since 2011 under the Programa Nacional de Protección de Infraestructuras Criticas de Información y Ciberseguridad (Jefatura de Gabinete de Ministros, 2011)

In terms of **Definitions for Critical Infrastructure,** Cabinet Resolution 580/2011 (Jefatura de Gabinete de Ministros, 2011) published on 2011 defined Critical Infrastructure. The Presidential Decree 898/2016 (Administración Pública Nacional, 2016) published on 2016 modernizes the missions of Argentinian government agencies, and reorganizes the Subsecretaría de Tecnología y Ciberseguridad (Vice ministry of IT and Cybersecurity).

In relation to the **NIST CSF - Mentions and references**, Argentina has not currently adopted the NIST Cybersecurity Framework, however private institutions utilize the Framework as a reference to measure and compare the maturity of cybersecurity assessments.

Based on this information, Argentina scores 4.5 points (out of 6) in our index.

While Argentina has possessed a National Security Strategy since 1998, and a Definition of Critical Infrastructure since 2011 (meaning prior to 2013 when the NIST CSF was started), the changes in the rest of the analized elements took place after 2013, and those changes can be attributable to the Framework. The highest individual contributor to Argentina’s score is the official mention to the NIST CSF in 2018 by the Argentinian National Office of Information Technologies.

4.2 Brazil

Table 17: Cybersecurity Sophistication index - Brazil

Criteria	Detail	Date	Points
1. National Security Strategy	Estratégia Nacional de Defesa: Paz e Segurança para o Brasil	2012	0.2
2. National Cybersecurity Strategy	Aprova a Estratégia Nacional de Segurança Cibernética	2020	0.5
3. Cybersecurity Framework	No	-	0.0
4. Government Agency dedicated to Cybersecurity	Centro de Defesa Cibernética	2012	0.1
5. Cybersecurity Taskforce	CERT.br Brazilian National Computer Emergency Response Team	2003	0.3
6. Definition of Critical Infrastructure	Política Nacional de Segurança de Infraestruturas Críticas	2018	1.0
7. Official Mentions to the NIST CSF	Aprova a Estratégia Nacional de Segurança Cibernética	2020	1.5
8. Other sectoral Cyber regulation referencing NIST CSF	Fórum Infraestruturas do Mercado Financeiro	2018	0.5
		Points	**4.1**

The country can be considered as a reactive market, since up until 2014 –where attacks targeted events organized in Brazil (Israel, 2014)- the country had not taken a proactive approach towards cybersecurity. While a law from 2010 had created a Reference Guide for Security and Critical Infrastructure, not much had been implemented up until the attacks in 2010.

The specific definition of the Cybersecurity Sector as strategic for the National Security Strategy of Brazil was done in 2012 (Silva, 2019). And while the definition of Critical infrastructure in

Brazil can be traced back to 2008 (Iure, 2017), it was only in 2015 where Brazil's National Telecommunications Agency (Anatel) issued official guidelines for its inspection, and now the country is actively reviewing its cyber implications.

There is no official adoption of the NIST Framework, the CSF has been translated into Brazilian Portuguese. Cabinet level dialogue between the Brazilian Government and the U.S. Department of Commerce has happened.

Brazil's score of 4.1 points out of 6 can be mainly explained by its early definitions for National Security Strategy and the establishment of their Cybersecurity Taskforce prior to 2013. However, of the momentum of the Portuguese translation of the CSF continues Brazil could take the regional lead.

4.3 Chile

Table 18: Cybersecurity Sophistication index - Chile

Criteria	Detail	Date	Points
1. National Security Strategy	La Estrategia Nacional de Seguridad y Defensa	2012	0.2
2. National Cybersecurity Strategy	National Cybersecurity Policy	2017	0.5
3. Cybersecurity Framework	No	-	0.0
4. Government Agency dedicated to Cybersecurity	Sistema Nacional de Ciberseguridad	2018	0.5
5. Cybersecurity Taskforce	CSIRT Computer Security Incident Response Team	2015	0.3
6. Definition of Critical Infrastructure	Sector specific - Norma Técnica sobre Fundamentos de Ciberseguridad para Telecomunicaciones	2020	1.0
7. Official Mentions to the NIST CSF	Programa de Formación para la Seguridad de la Información y la Ciberseguridad	2019	1.5
8. Other sectoral Cyber regulation referencing NIST CSF	Programa de Formación para la Seguridad de la Información y la Ciberseguridad	2020	0.5
		Points	**4.5**

With cyber-related regulation that dates back from 2004, Chile initially struggled a bit in addressing the challenges of cybersecurity. Initially the governmental agencies responsible for incidents where the specific divisions within the Chilean Armed Forces, but since the mid 2000 things have changed.

As for definitions for Cubersecurity, in 2017 the National Policy for Cybersecurity (Gobierno de Chile, 2017) was published. Essentially, a roadmap to continue delegating responsibilities and providing resources to the new actionable actors. This policy criticized for its lack of resources and proper agency adjustments. The new entity did not have its own budget, making it a bit ineffective.

It took a huge social crisis, riots, and a high level of threat for the country to properly assess the importance of Critical Infrastructure. In 2020 a sector specific definition was stablished for the Telecom sector.

While Chile has not adopted the NIST CSF, there are several Chilean agencies reference it, including CORFO, Subtel, the Central Bank, and the Chilean Financial Markets Commission, who inspired its Cybersecurity regulation on the 5 functions of the CSF.

Chile's score of 4.5 points out of 6 offers paints a good influencial picture for the CSF. Just the lack of a Cybersecurity Framework leaves it behing Uruguay. Despite its low comparatively to Uruguay, Chile seems to be as invested into the Framework as Uruguay.

4.4 Colombia

Table 19: Cybersecurity Sophistication index - Colombia

Criteria	Detail	Date	Points
1. National Security Strategy	Política de Defensa y Seguridad	2019	0.2
2. National Cybersecurity Strategy	Policy Guidelines on Cybersecurity and Cyber defense	2011	0.2
3. Cybersecurity Framework	No	-	0.0
4. Government Agency dedicated to Cybersecurity	Centro Cibernetico Policial	2001	0.1
5. Cybersecurity Taskforce	Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT	2013	0.3
6. Definition of Critical Infrastructure	Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia	2017	1.0
7. Official Mentions to the NIST CSF	Agenda Estratégica de Innovación: Ciberseguridad	2014	1.5
8. Other sectoral Cyber regulation referencing NIST CSF	Revisión del marco regulatorio para la gestión de riesgos de seguridad digital	2017	0.5
		Points	**3.8**

Colombia seems to have a style and approach somehow similar to Chile, since most of the regulatory changes for cybersecurity have been recent. Back in 2014, a technical mission from the Organization of American States helped Colombia to kick start its Cybersecurity regulation sector. As for industry definitions, only in 2016 we could find specific references to Critical Infrastructure and measurements to protect it. Starting in 2017, there is a National Plan of Protection and Defense of Cyber Critical Infrastructure.

The definition of this plan promotes not only the leadership of armed forced institutions, but also seeks to generate Public private partnerships to facilitate synergies.

Colombia has not officially adopted the NIST CSF as a national policy, nor has adapt it, whoever several private entities –not just in the financial services sector- are using it. The Colombian private sector and academia understand the importance of having a base plane field to understand each institution's status and levels of maturity towards cybersecurity.

However, considering our comparison index, Colombia has the lowest score of all markes with 3.8 points out of 6, due to the National Cybersecurity Strategy having been established prior to the NIST CSF, back in 2011, and by the lack of Cybersecurity Framework in place.

4.5 Uruguay

Table 20: Cybersecurity Sophistication index - Uruguay

Criteria	Detail	Date	Points
1. National Security Strategy	Política de Defensa Nacional	2014	0.2
2. National Cybersecurity Strategy	Política de Seguridad de la Información	2014	0.5
3. Cybersecurity Framework	Marco de Ciberseguridad (Basado en NIST CSF)	2018	1.5
4. Government Agency dedicated to Cybersecurity	AGESIC	2005	0.1
5. Cybersecurity Taskforce	Centro de Respuesta a Incidentes de Ciberseguridad (CERT)	2014	0.3
6. Definition of Critical Infrastructure	Decreto 65/020: Sistema Nacional de emergencias	2020	1.0
7. Official Mentions to the NIST CSF	Marco de Ciberseguridad (Basado en NIST CSF)	2018	1.5
8. Other sectoral Cyber regulation referencing NIST CSF	Cuenta Pública Presidencial	2019	0.5
		Points	**5.6**

Of all the countries in South America that we have analyzed, Uruguay is the best example of influence by the Framework, the country is featured as an international success case by NIST itself and independent players. Uruguay certainly is the most aggressive country in terms of the framework´s adoption.

In terms of cybersecurity regulation, Uruguay can be considered as an early adopter, back in 2009 the Government of Uruguay –using a Presidential Decree, similar to the U.S.'s executive orders- required all government agencies to come up with specific cybersecurity policies.

While there isn't a specific definition for cybersecurity, Uruguay's efforts are under the umbrella of the country's Digital Agenda, that date back from 2006, and that have continue to be developed in 2 up to 5 year intervals. As part of these agendas, Uruguay's main goals are: to develop inclusive digital skills for its citizens, to create and develop a digital economy and innovation sectors for the country, and to offer trust, security, and reliability in the use of digital technologies.

Following its early adopter trend, and by closely working with the U.S., Uruguay adapted the NIST Cybersecurity Framework v1.1 in 2016.

The country has been able to continue enhancing its already predominant position within the region –despite its relatively small size-, and in 2019 secured an $8 million USD loan by the Inter-American Development Bank to "*support the strengthening of Uruguay's capacity to protect its digital space*" (Inter-American Development Bank, 2019)

We have seen how Uruguay has the greatest integration with the NIST CSF, having adapt it locally and even translated it into Spanish. In addition to Uruguay´s success case in adapting the framework, there is a white paper published by The Organization of American States (OAS) and Amazon Web Services (AWS), where the United Kingdom and Uruguay are featured as success stories in the implementation of the framework (Organization of American States & AWS, 2019)

4.6 NIST CSF South American Resources

In addition to the country specific analysis, there are several other resources available, from public and private entities in the region and around the world. Here is a small sample of what's easily available for the region:

Table 21: NIST CSF South American references

Country	Sector	Document	Entity
Brazil	International Organization	Cybersecurity Capacity Review: Federative Republic of Brazil	Organization of American States
Brazil	Professional Services	Como o NIST Privacy Framework pode melhorar o gerenciamento de riscos	EY
Brazil	International Organization	NIST Cybersecurity Framework	Organization of American States & AWS
Chile	Financial Services	Fundamentos básicos de ciberseguridad	Asociación Administradores de Fondos Mutuos
Chile	Telecom	Entel CyberSecure	ENTEL
Chile	Information Technologies	Ciberseguridad	Sonda
United States	International Organization	State of Cybersecurity in the Banking Sector in Latin America and the Caribbean	Organization of American States
United States	Cloud Services	NIST Cybersecurity Framework: Aligning to the NIST CSF in the AWS Cloud	AWS
United States	Information Technologies	The Cybersecurity Framework in Action: An Intel Use Case	Intel

The bottom-line here is, the market is aware of the NIST CSF, and it embraces its influence. As well as the public sector parties, and particularly specialized agencies that have prominent roles in Cybersecurity.

This section has established a primarily close relationship between the different changes in the studied markets, and the apparition of the NIST CSF. While some of the the key cybersecurity aspects that we analized were established prior to 2013, the vast majority of the 8 criteria took place after 2013 in all the markets.

The fact that Uruguay is considered a success story by NIST, and that this has been documented with the support of the Organization of American States and Amazon demonstrates how intrincated the intergovernmental cooperation can be. The added literature and resources tied to NIST that are available in South America are also another testament to the collaboration between the region and U.S. policy makers.

While South America can be considered a region that's politically volatile, these policy changes have stayed and continue moving forward regardless of the government ideologies running each country. This appears to demonstrate that when it comes for cybersecurity political differences can be left behind.

Conclusions

In this work we described in detail the context, development, and evolution of the NIST Cybersecurity Framework (CSF). At the beginning we saw the tremendous impact that the Cybersecurity sector can have for a country, as big as to be compared with "**the next Pearl Harbor**" in the United States.

Cybersecurity is a complex subject, as a mix of processes, software, hardware, and human being interactions. And because of this complexity, it needs to be addressed at multiple levels. The cyber-response forces, the new cyber rules of engagement, this whole new perception that the cyber domain is another arena where countries need to be able to protect using all the elements of the national power… all of that at the most strategic and executive levels. But at the same time, another dimension of cybersecurity are the normal and down to earth considerations that entities and individuals must have to properly conduct our daily routines. The fact that financial institutions must spend 2/3s of their security budgets goes to cyber-detection activities, and the huge attack estimations that the industry must face, tell a compelling story about the benefits of preparing institutions in advance, rather than having to face the consequences of being attacked.

The Framework doesn't solve all problems. It's just a voluntary set of standards, best practices, and guidance for entities to "address the problem" and correct course from that diagnostic. And that contribution might initially sound irrelevant, but as we have experienced over and over, even a couple of times in the middle of the pandemic, even the smallest advances can make a huge difference. Perhaps the recent attack to Banco Estado in Chile would have played differently, should the bank had had an assessment process to begging with. Or maybe we would not be wondering if the Government Databases with the passwords of millions of Chileans were compromised, should the data handlers have decided to Identify gaps or stress points across their infrastructure.

Certainly, a lot could have done differently. But if one of the biggest companies in the world, such as Saudi Aramco can learn from its mistakes to recover, and Build Back Better, there is no excuse for other entities to do the same, or at least to try.

The question that we have had at the center of this project has been: **What has been the influence of the NIST Cybersecurity framework in cybersecurity policies in South America?**

On this last section we will bring it all together and try to answer this question.

The initial hypothesis that South America operates as a follower region, and therefore CAN be influenced is what we have tried to unveil. We searched for:

- Changes in regulation for Cybersecurity sector pre and post framework in selected markets in South America.
- Mentions and references to the framework on official documents by government institutions in the selected countries in South America.
- Hidden references, when elements of the frameworks (or parts of it) are mentioned o referenced in official documents, but without mentioning NIST.

What we were able to find:

For criteria number 7. Official Mentions to the NIST CSF, and 8. Other sectoral Cyber regulation referencing NIST CSF, **ALL the countries have references in official sources**. Of all the criteria defined in the analysis, the most point-dominant factors were: Having a Cybersecurity Framework, which would award 1.5 points, and as a close second criteria 7 and 8 (together) would also award 1.5 points (out of the 6 maximum points in total).

With this exercise, we tried to capture the influence of the Framework, by being referenced in official documents of government agencies.

Table 22: Aggregated compounded points

Country	Compounded total points
Argentina	4.5
Brazil	4.1
Chile	4.5
Colombia	3.8
Uruguay	5.6

Personal compilation, based on data from Tables 16-20

As we defined that the maximum total points to obtain were 6, which implied a market where the NIST CSF had been tremendously influential, and 0 points would imply no influence at all.

With that characterization, we can say that the Framework has mostly has a HIGH impact in the region, since all the country have a total point value of 4.0 or more, the only exception being Colombia.

The Framework´s has demonstrated to have a positive influence in the region and the whole world, which is impressive considering its voluntary character.

The Framework can be considered an influential indirect policy tool for the U.S., since it has helped the United States define what it considers positive industry defined standards and recommendations for its users.

It is considered as a de facto standard by many, and the fact that it was collaboratively conceived, with industry and a wide range of stakeholders helps it to fulfill its goal: to be adopted and used by organization of any size, in any industry. After all its mission is straightforward: to help organizations address the (cyber) situation in which they currently stand, to visualize a better tomorrow, and to define a roadmap so they can get there in time. The first step in solving any problem is recognizing there is one, the Framework helps to do that. And with that diagnostic we can start to move forward if we want, the good news that: yes, we can (move forward).

References

Accenture. (2018). *Cost of Cyber Crime: Financial Services*. Retrieved from Accenture: https://newsroom.accenture.com/news/cybercrime-costs-financial-services-sector-more-than-any-other-industry-with-breach-rate-tripling-over-past-five-years-according-to-report-from-accenture-and-ponemon-institute.htm#:~:text=Among%20the%20key%20findings%20

Administración Pública Nacional. (2016). *Decreto 898/2016 - Modificación. Decreto N° 357/2002*. Retrieved from InfoLEG: Ministerio de Justicia y Derechos Humanos: http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/263831/norma.htm

American Bar Association. (2020). *What Is an Executive Order?* Retrieved from American Bar Association: https://www.americanbar.org/groups/public_education/publications/teaching-legal-docs/what-is-an-executive-order-/

Cambridge University Press. (2020). *Framework*. Retrieved from Cambridge Dictionary: https://dictionary.cambridge.org/us/dictionary/english/framework

Cambridge University Press. (2020). *Voluntary*. Retrieved from Cambridge Dictionary: https://dictionary.cambridge.org/us/dictionary/english/voluntary?q=VOLUNTARY

Carnegie Endowment for International Peace & BAE Systems. (2020). *Timeline of Cyber Incidents Involving Financial Institutions*. Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide

Chang-Gu, A. (2015, March 5). *NIST Cybersecurity Framework vs. NIST Special Publication 800-53*. Retrieved from Praetorian: https://www.praetorian.com/blog/nist-cybersecurity-framework-vs-nist-special-publication-800-53?edition=2019

Considine, M. (1994). *Public policy : a critical approacH.* Melbourne: Macmillan Education Australia.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 13-21.

Crowell & Moring. (2019). *APEC Taking Lead on IoT Standards and Cybersecurity*. Retrieved from Crowell Moring: https://www.crowell.com/NewsEvents/AlertsNewsletters/all/APEC-Taking-Lead-on-IoT-Standards-and-Cybersecurity#footnotes

Cybersecurity and Infrastructure Security Agency. (2019, November). *What is Cybersecurity?* Retrieved from Cybersecurity and Infrastructure Security Agency (CISA): https://www.us-cert.gov/ncas/tips/ST04-001

DCAF-ISSAT. (2020). *National Security Strategies: Towards a New Generation*. Retrieved from DCAF-ISSAT: https://issat.dcaf.ch/Learn/SSR-in-Practice/Thematics-in-Practice/National-Security-Strategies

Economic Commission for Latin America and the Caribbean. (2017). *State of broadband in Latin America and the Caribbean.* Retrieved from https://repositorio.cepal.org/bitstream/handle/11362/43670/1/S1800532_en.pdf

Fischer, E. (2014). *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation.* Washington, D.C.: Congressional Research Service. Retrieved from https://crsreports.congress.gov/product/pdf/R/R42114

Gobierno de Chile. (2017). *Política Nacional de Ciberseguridad 2017-2022.* Retrieved from Ciberseguridad: https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

Goldman, D. (2012). *Major banks hit with biggest cyberattacks in history*. Retrieved from CNN Business: https://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html

Howard, D. (2019, January). *The history of HDMI*. Retrieved from Sensory Technologies: https://sensorytechnologies.com/2019/01/15/the-history-of-hdmi/

Inter American Development Bank & Organization of American States. (2016, Mar). *Cybersecurity: Are We Ready in Latin America and the Caribbean?* Retrieved from Publications: Inter American Development Bank: https://publications.iadb.org/publications/english/document/Cybersecurity-Are-We-Ready-in-Latin-America-and-the-Caribbean.pdf

Inter-American Development Bank & Organisation for Economic Co-operation and Development. (2016). *Broadband Policies for Latin America and the Caribbean A Digital Economy Toolkit.* Retrieved from Inter-American Development Bank: Publications: https://publications.iadb.org/publications/english/document/Broadband-Policies-for-Latin-America-and-the-Caribbean-A-Digital-Economy-Toolkit.pdf

Inter-American Development Bank. (2019). *IDB approves Uruguay's first cybersecurity credit in its history*. Retrieved from Inter-American Development Bank: News: https://www.iadb.org/en/news/idb-approves-uruguays-first-cybersecurity-credit-its-history

Israel, E. (2014). *Hackers target Brazil's World Cup for cyber attacks*. Retrieved from Reuters: https://www.reuters.com/article/us-worldcup-brazil-hackers-idUSBREA1P1DE20140226

Iure, P. (2017). Política Nacional de Defensa e Protecão da Infraestrutura Energética Crítica no Brasil. *Austral Brazilian Journal of Strategy & International Relations*, 173.

Jefatura de Gabinete de Ministros. (2011). *Resolución 580/2011 - Créase el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Objetivos.* Retrieved from InfoLEG: Ministerio de Justicia y Derechos Humanos: http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm

Johnson, J. (2020, September). *The unlikely origins of USB, the port that changed everything*. Retrieved from FastCompany: https://www.fastcompany.com/3060705/an-oral-history-of-the-usb

Kladogeni, A., & Alexandros, H. (2011). Designing a balanced scorecard for the evaluation of a local authority organization. *European Research Studies Journal*, 65-80. doi:https://www.um.edu.mt/library/oar/handle/123456789/31464

Leiner, B. M., Cerf, V. G., & Clark, D. D. (1997, February). *The Past and Future History of the Internet*. Retrieved from ACM Digital Library: https://dl.acm.org/doi/pdf/10.1145/253671.253741?casa_token=3fNX6gMJ17UAAAAA%3AiAW1JSc44ofB9ITq5B8WxZj1UCJAql01II0rkx33-fXZBYq7CeJ5qGOVEgh0aEf1WeiHznd8SCecEw

Lewallen, J. (2020, July). *Emerging technologies and problem definition uncertainty: The case of cybersecurity*. Retrieved from Wiley Online Library: https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12341?casa_token=iE64Mdim3dsAAAAA%3AIp4zpLv6eQL_9X2xmPkmZpUkiES_e5X3fOMzoG9AH9zJFqC9PU_2uKIr_L4JLr6MQebu6tDBb6eYDLwr

Leyden, J. (2012). *Hack on Saudi Aramco hit 30,000 workstations, oil firm admits*. Retrieved from The Register: https://www.theregister.com/2012/08/29/saudi_aramco_malware_attack_analysis/

McCarthy, B. (2013). Secrecy hampers battle for cyber security. *Financial Times*. London, United Kingdom. Retrieved from https://www.ft.com/content/5adfe5cc-c938-11e2-9d2a-00144feab7de

Merriam-Webster, Inc. (2020). *Adherence*. Retrieved from Merriam-Webster Dictionary: https://www.merriam-webster.com/dictionary/adherence

Merriam-Webster, Inc. (2020). *Adopt*. Retrieved from Merriam-Webster Dictionary: https://www.merriam-webster.com/dictionary/adopting

Merriam-Webster, Incorporated. (2020). *Resilience*. Retrieved from Merriam-Webster Dictionary: https://www.merriam-webster.com/dictionary/resilience

Nakashima, E. (2012, October). *Cyberattack on Mideast energy firms was biggest yet, Panetta says*. Retrieved from The Washington Post: https://www.washingtonpost.com/world/national-security/cyberattack-on-mideast-energy-firms-was-biggest-yet-panetta-says/2012/10/11/fe41a114-13db-11e2-bf18-a8a596df4bee_story.html

National Institute of Standards and Technology. (2013, October). *Request for Comments on the Preliminary Cybersecurity Framework.* Retrieved from U.S. Federal Register: https://www.federalregister.gov/documents/2013/10/29/2013-25566/request-for-comments-on-the-preliminary-cybersecurity-framework

National Institute of Standards and Technology. (2014). *Initial Analysis of RFI (2013)*. Retrieved from Cybersecurity Framework: https://www.nist.gov/cyberframework/initial-analysis-rfi-2013

National Institute of Standards and Technology. (2018). *Cybersecurity Framework Archived Documents*. Retrieved from Cybersecurity Framework: https://www.nist.gov/cyberframework/evolution/archived-documents

National Institute of Standards and Technology. (2018, April 16). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.* Retrieved from Cybersecurity Framework: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology. (2018). *MEP Centers Aid Manufacturers on Cybersecurity*. Retrieved from NIST: https://www.nist.gov/news-events/news/2018/05/mep-centers-aid-manufacturers-cybersecurity

National Institute of Standards and Technology. (2018). *The Five Functions*. Retrieved from Cybersecurity Framework: https://www.nist.gov/cyberframework/online-learning/five-functions

National Institute of Standards and Technology. (2019, April 2). *Evolution of the Framework*. Retrieved from Cybersecurity Framework: https://www.nist.gov/cyberframework/evolution

National Institute of Standards and Technology. (2019). *Informative References: What are they, and how are they used?* Retrieved from Cybersecurity Framework: https://www.nist.gov/cyberframework/online-learning/informative-references

National Institute of Standards and Technology. (2020). *An Introduction to the Components of the Framework*. Retrieved from Cybersecurity Framework: https://www.nist.gov/cyberframework/online-learning/components-framework

National Institute of Standards and Technology. (2020). *International Resources*. Retrieved from Cybersecurity Framework: https://www.nist.gov/cyberframework/international-resources

National Institute of Standards and Technology. (2020, September). *New to Framework*. Retrieved from NIST: https://www.nist.gov/cyberframework/new-framework

National Institute of Standards and Technology. (2020). *New to Framework*. Retrieved from Cybersecurity Framework: https://www.nist.gov/cyberframework/new-framework

Organisation for Economic Co-operation and Development (OECD). (2020). *Policy Framework on Sound Public Governance*. Retrieved from OECD.org: https://www.oecd.org/governance/policy-framework-on-sound-public-governance/

Organization of American States & AWS. (2019). *Ciberseguridad Marco NIST: Un abordaje integral de la Ciberseguridad.* Retrieved from Organization of American States: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Organization of American States. (2018). *State of Cybersecurity in the Banking Sector in Latin America and the Caribbean.* Retrieved from Organization of American States: http://www.oas.org/es/sms/cicte/sectorbancarioeng.pdf

Oxford University Press. (2020). *Definition of effect*. Retrieved from Lexico: https://www.lexico.com/definition/effect

Oxford University Press. (2020). *Definition of influence*. Retrieved from Lexico: https://www.lexico.com/definition/influence

Reuters. (2018, June 11). *Bank of Chile trading down after hackers rob millions in cyberattack*. Retrieved from Reuters: https://www.reuters.com/article/us-chile-banks-cyberattack-idUSKBN1J72FC

Silva, M. (2019). *Cyber security : a case study of Brazil*. Retrieved from Semantic Scholar: https://www.semanticscholar.org/paper/Cyber-security-%3A-a-case-study-of-Brazil-Silva/7ed7e758652675fdc5d6c9a9f94859bd1f9ee15b?p2df

Tenable. (2020). *NIST Cybersecurity Framework (CSF)*. Retrieved from Tenable: https://www.tenable.com/solution-briefs/nist-cybersecurity-framework-csf

The Law Dictionary. (2020). *Policy Framework*. Retrieved from The Law Dictionary: https://thelawdictionary.org/policy-framework/

Trautman, L. J. (2015). Cybersecurity: What about US policy. *University of Illinois Journal of Law, Technology & Policy*, 341. Retrieved from http://illinoisjltp.com/journal/wp-content/uploads/2015/12/Trautman.pdf

Triggs, R. (2018, March). *A quick history of Bluetooth*. Retrieved from Android Authority: https://www.androidauthority.com/history-bluetooth-explained-846345/

U.S. Federal Register. (2013, February). *Federal Register / Vol. 78, No. 38.* Retrieved from Federal Register: https://www.nist.gov/system/files/documents/itl/csd/fr_noticerfi_framework_cybersecurity_2-26-13.pdf

U.S. Federal Register. (2013). *Improving Critical Infrastructure Cybersecurity.* Retrieved from Federal Register: https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

U.S. Senate Armed Services Committee. (2011). *Nominations Before the Senate Armed Services Committee First Session, 112th Congress.* Washington, D.C.: Committee on Armed Services . Retrieved from https://www.govinfo.gov/content/pkg/CHRG-112shrg74537/pdf/CHRG-112shrg74537.pdf

Wi-Fi Alliance. (2020, September). *History*. Retrieved from Wi-Fi Alliance: https://www.wi-fi.org/who-we-are/history

World Intellectual Property Organization. (2019). *WIPO IP Facts and Figures 2019.* Retrieved from WIPO: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_943_2019.pdf

ANNEX 1 – Definitions

ADHERENCE: “*steady or faithful attachment*” (Merriam-Webster, Inc., 2020)

ADOPT: “*to take up and practice or use*” (Merriam-Webster, Inc., 2020)

CYBERSECURITY: “*Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights*" (Craigen, Diakun-Thibault, & Purse, 2014)

INFLUENCE: “*The capacity to have an effect on the character, development, or behavior of someone or something*” (Oxford University Press, 2020)

EFFECT: “The extent to which something succeeds or is operative” (Oxford University Press, 2020)

FRAMEWORK: “*a system of rules, ideas, or beliefs that is used to plan or decide something*” (Cambridge University Press, 2020)

POLICY FRAMEWORK: “*The set of guidelines, as well as long term goals which are taken into account when policies are being made*” (The Law Dictionary, 2020). Also, according to the OECD a policy framework “*builds on lessons learned and on practice-based evidence of what works, what does not and why*” (Organisation for Economic Co-operation and Development (OECD), 2020)

PUBLIC POLICY: “*a public policy is an action which employs governmental authority to commit resources in support of a preferred value*” (Considine, 1994)

RESILIENCE: “*ability to recover from or adjust easily to misfortune or change*” (Merriam-Webster, Incorporated, 2020)

VOLUNTARY: “*done, made, or given willingly, without being forced or paid to do it*” (Cambridge University Press, 2020)