2019

White paper series
Issue 5

— NIST CYBERSECURITY — FRAMEWORK (CSF)

A comprehensive approach to cybersecurity

OAS More rights for more people

aws

— NIST CYBERSECURITY — FRAMEWORK (CSF)

A comprehensive approach to cybersecurity

CREDITS

Luis Almagro

Secretary General
Organization of American States (OAS)

OEA Technical Team

Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Santiago Paz
Fabiana Santellán
Kerry-Ann Barrett
Nathalia Foditsch
Diego Subero
David Moreno
Mariana Cardona
Jaime Fuentes
Miguel Ángel Cañada

AWS Technical Team

Abby Daniell
Michael South
Andres Maz
Melanie Kaplan
Min Hyun

CONTENT

1. Introduction

Given a steady increase in the number of cybersecurity incidents in the US, President Barack Obama, on February 12, 2013, issued Executive Order 13636 [1] entrusting the National Institute of Standards and Technologies (NIST) the development of the Cybersecurity Framework for the protection of critical infrastructures, which is now known as the NIST Cybersecurity Framework (CSF). The US identified 16 critical infrastructure sectors: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems. [18]

The Framework was conceived as a means to identify the applicable safety standards and guidelines in all sectors of critical infrastructure, providing a flexible and repeatable approach, to allow the prioritization of activities. The aim was also to ensure sustainable performance, while remaining profitable for the business.
It is undoubtedly a tool for cybersecurity risk management, which enables technological innovation while adjusting to all types of organizations (regardless of category or size).

The Framework strategy was based on industry-accepted standards in the cybersecurity ecosystem (NIST SP 800-53 Rev.4[2], ISO/IEC 27001:2013[3], COBIT 5[4], CIS CSC[5], among others). They are presented as a simple-approach strategy to cybersecurity governance, to make it possible to easily transfer technical notions to the business objectives and needs. A participatory methodology was used in preparation, where all the interested parties (government, industry, academia) were able to engage and provide improvements.

CSF's main innovation is the setting aside of rigid standards, which was the norm at that time, but it was not the first to advance an initiative for the protection of critical infrastructures. NATO had already developed a series of manuals aimed at the protection of critical infrastructures for national defense, one being the "National Cyber Security Framework Manual" [14]. Far from excluding these documents, NIST's CSF complements and improves them.

The major difference in the CSF with respect to its predecessors is simplicity and flexibility: simplicity in transmiting a technical strategy in terms readily understandable by the business; and flexibility to adapt to any organization. This difference is what has made the industry and the technical community around the world embrace this framework to date. Companies, academia and governments have voluntarily adopted the CSF as part of their cybersecurity strategy. Even leading organizations in preparing standards and regulations, such as ISACA and ISO, have incorporated the CSF. In particular, ISO produced ISO/IEC TR 27103:2018 [6] that provides guidance on how to take advantage of existing standards in a cybersecurity framework, in other words, how to use the CSF.

2. NIST Cybersecurity Framework (CSF)

2.1. History of the CSF

The process of preparing the Framework began in the US with Executive Order No. 13636, published on February 12, 2013. This Order introduced efforts to share information on cybersecurity threats and to build a set of current and successful approaches: a framework to reduce risks to critical infrastructure. Under this Executive Order, NIST took charge of the outlining of the "Cybersecurity Framework."

Some of the development requirements were: to identify the applicable safety standards and guidelines in all critical infrastructure sectors; to provide a priority-based, flexible, repeatable outlook based on performance and profitability; to help identify, evaluate and manage cyber risk; to include guidance on how to measure the performance of Cybersecurity Framework implementation; and to identify areas for improvement that must be addressed through future collaboration with individual sectors and organizations that develop standards.

Creation of the Framework

The Framework was, and continues to be, developed and promoted through continued engagement and input from government, industry and academia stakeholders. To develop the Framework, in the course of a year, NIST used a Request for Information (RFI) and a Request for Comments (RFC), as well as ample dissemination and workshops throughout the US to: **(i)** identify existing cybersecurity standards, guidelines, frameworks and best practices applicable to increase the security of the critical infrastructure sectors and other interested entities; **(ii)** specify high priority gaps which needed new or revised standards; and **(iii)** develop collaborative action plans to address these gaps.

In updating the CSF to version 1.1, which was published in April 2018, NIST continued with its participatory strategy, welcoming experts and industry, as well as governments and non-US companies. For example, participating entities included the government of Israel and Huawei Technologies. [17]

2.2. CSF Structure

The NIST Cybersecurity Framework (CSF) consists of three main components:

- Core
- Implementation Tiers
- Profiles

Framework Core

The Core is a set of desired cybersecurity activities and outcomes, organized into Categories and aligned to Informational References to industry-accepted standards. It is designed to be intuitive and to act as a translation layer to enable communication between multi-disciplinary teams by usin simplistic and non-technical language.

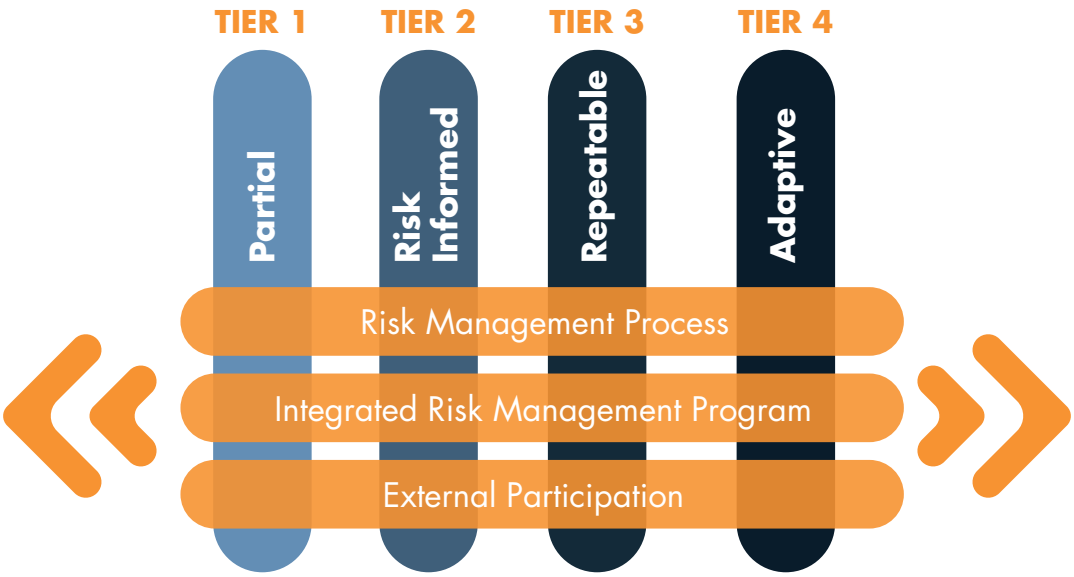
The Core consists of three parts: Functions, Categories and Subcategories. It includes five high-level **functions**: Identify, Protect, Detect, Respond and Recover.

The next level down is the 23 **categories**, which are split across the five Functions. They were designed to cover the breadth of cybersecurity objectives for an organization, without being too detailed, covering issues related to technical aspects, people and processes, with a focus on outcomes.

The **Subcategories** are the deepest levels 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 should achieve those results, it enables risk-based implementations that are customized to the needs of different organizations.

Framework Implementation Tiers

Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework. The Tiers range from Partial (Tier 1) to Adaptive (Level 4) and describe an increasing degree of rigor, and how well integrated cybersecurity risk decisions are into broader risk decisions, and the degree to which organization shares and receives cybersecurity information from external parties.



Although NIST points out that the Tiers do not necessarily represent levels of maturity, in practice they do resemble that. What is important is that organizations should determine the desired Tier (not all controls must be implemented at the highest Tier), making sure that the selected level meets at least the organization's goals, reduces cybersecurity risk to acceptable levels, has an acceptable cost and is feasible to implement.

Framework Profiles

The profiles are the unique alignment of an organization's organizational requirements and objectives, the risk appetite and the resources against the desired outcomes of the Core Framework. Profiles can be used to identify opportunities to improve the cybersecurity posture by comparing a "Current" Profile with a "Target" Profile.

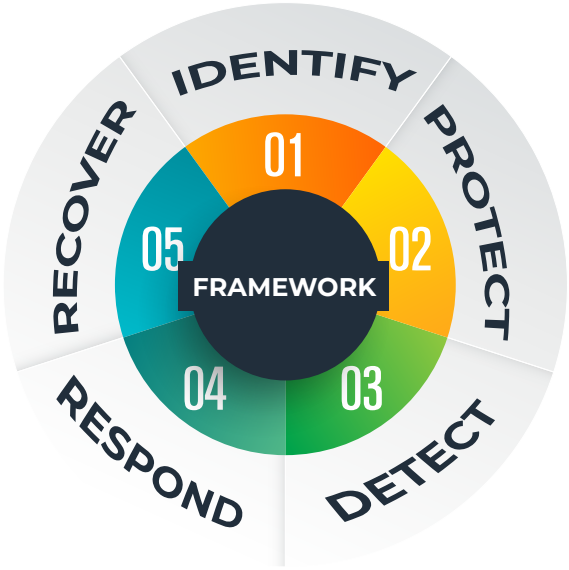
The identification of the current profile allows organizations to conduct an objective review (without involving a formal audit or other technical evaluations) of their cybersecurity program against the CSF and to accurately know what their current security situation is.

Taking into account the organizational risk assessment, compliance requirements and organizational objectives, an objective profile can be created, which, when compared against the current state profile, will inform the leadership strategy and priorities for hiring, training, changes in policies, procedural changes and technology acquisition.

2.3. CSF Functions

The five functions included in the Core Framework are:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover



Functions 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 help organizations to easily express their cybersecurity risk management at a high level and enable risk management decisions.

Identify

The Identity Function assists in developing an organizational understanding to manage the cybersecurity risk of systems, people, assets, data and capabilities. Understanding the business context, the resources that support critical functions and the related cybersecurity risks allows an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Protect

The Protect Function describes the appropriate safeguards to guarantee the delivery of critical infrastructure services. This function supports the ability to limit or contain the impact of a potential cybersecurity event.

Detect

The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event, allowing the timely discovery of the events.

Respond

The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident, developing the capacity to contain the impact of a potential incident.

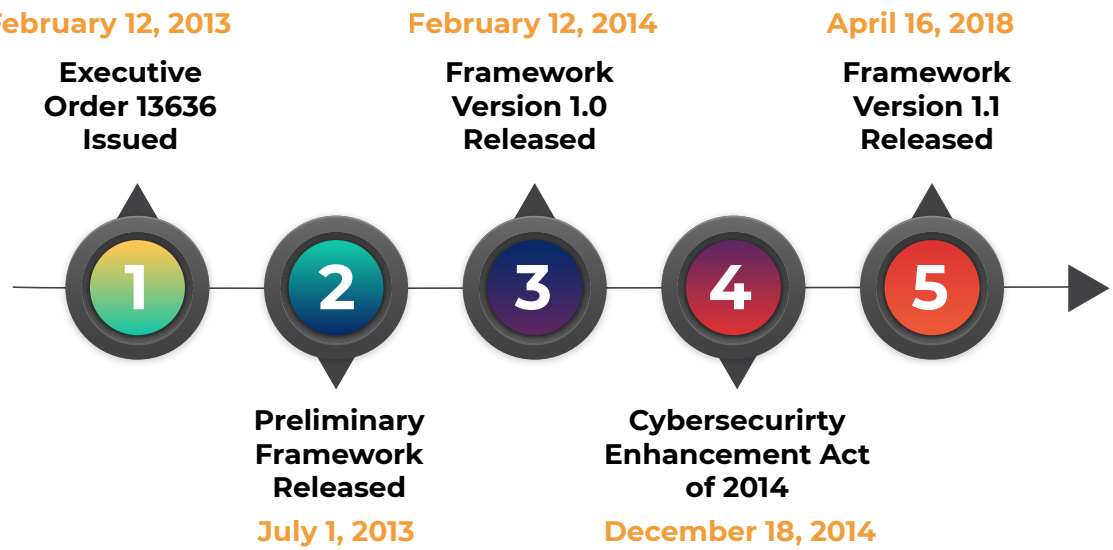
Recover

The Recover Function identifies the appropriate activities to maintain resilience plans and to restore any capability or service that has been impaired due to a cybersecurity incident. This function supports timely recovery of normal operations to reduce the impact of a cybersecurity incident.

2.4. Versions and mechanisms of evolution

The CSF has been developed and promoted through the continuous engagement with, and input from, stakeholders in government, industry and academia. That includes a open public review and comment process, workshops and other means of participation.

The graphic below illustrates the evolution of the NIST Cybersecurity Framework (CSF):



3. How to use the CSF??

The CSF is a tool that enables managing cybersecurity risks, flexibly and in a was that adapts to the reality of any organization, regardless of its size or category.

It is important to highlight that the Framework does not propose new controls or processes, but brings together the controls proposed by the main industry standards, internationally recognized such as NIST SP 800-53, ISO 27001, COBIT 5, among others). It will therefore not replace the organization's established processes and controls, but rather the Framework will continue to use what has already been implemented, and eventually complement it, in order to present a strategy with an executive, outcome-driven focus.

3.1. Strategy to adopt the CSFF

Below are three possible strategies for the use of the CSF, as proposed in the Framework [11], but they are not the only strategies possible.

Basic review of cybersecurity practices

An organization can use the Framework as a key part of its systematic cybersecurity risk management process. It is not designed to replace existing processes, but to determine the gaps in the current approach to cybersecurity risk and then develop a roadmap for improvement. This enables optimization of costs and outcomes.

Creation or improvement of a cybersecurity program

The Framework is designed to complement existing business and cybersecurity operations. It can be taken as a basis for the creation of a new cybersecurity program or as a tool for the improvement of an existing program.

The following 7 steps can guide the creation of a new cybersecurity program or improve an existing one. These steps should be repeated as necessary to continually improve and evaluate cybersecurity:

Step 1: Prioritize and Scope. The organization identifies its business objectives and the high-level priorities. With this information, the scope of the cybersecurity program can be determined: what line of business or processes will be addressed.

Step 2: Orient. The organization identifies the systems and assets related to scope, legal or regulatory requirements, and overall risk approach.

Step 3: Create a Current Profile. The organization conducts an evaluation of the cybersecurity program is done to create a Current Profile. This will indicate which Category and Subcategory outcomes of the Framework Core are currently being achieved. It is essential that this evaluation include People (number of personnel, work roles, skills and training for security professionals and general knowledge of the user), Processes (strategy, policies, procedures, manual vs. automation, communication channels with stakeholders, etc.), and Technology (capabilities, configurations, vulnerabilities, patches, operations and support contracts, etc.).

Step 4: Conduct a Risk Assessment. The organization analyzes the operation environment to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks taking into account the identification of asset vulnerabilities and cybersecurity threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events. Although this step focuses on the identification of cybersecurity risks, it is important that this process be aligned with the organizational risk assessment, as well as the evaluation of business risks so that there is feedback in the evaluations.

Step 5: Create an Target Profile. The Target Profile should focus on the assessment of the Framework Categories and Subcategories that describe the organization's desired cybersecurity results, always bearing in mind the business mission and objectives, as well as requirements related to legal or regulatory compliance. Organizations can also develop their own additional Categories based on business requirements, as well as requirements from external stakeholders, such as sector entities, customers and business partners, not forgetting that the requirements are not only technical or technological, but also associated with staff and training, policies, procedures and other administrative needs.

Step 6: Determine, Analyze and Prioritize Gaps. The Current Profile and the Target Profile are compared to determine the gaps. Next, the organization creates a prioritized action plan to address the gaps (which reflect the mission drivers, costs and benefits, and risks) to achieve the outcomes in the Target Profile. Then, the organization determines the resources needed to address the gaps, which include the funds and the workforce.

Step 7: Implement Action Plan. The organization determines what actions to take to address the gaps, if any, identified in the previous step and then it adjusts current cybersecurity practices to achieve the Target Profile. It is important that the actions include all aspects of the governance of cybersecurity: Personnel (hiring, training, educating, etc.); Technology (current solutions, commercial solutions available, new developments, innovation, etc.) and Processes (policies, processes and procedures adapted to the need and reality of the organization).

Communication of cybersecurity requirements to stakeholders

The Framework can provide a means to express cybersecurity requirements to business partners, customers and suppliers; in particular to the suppliers of services or products linked to the organization's critical infrastructure.

3.2. Main challenges

CSF's greatest challenge is to adapt to different sectors, industries and even countries. It does not use any specific standard to satisfy cybersecurity controls, but abstracts from them by applying a conceptual approach and suggesting a list of multiple possible standards to satisfy the control requirements. It can be used in different areas such as critical infrastructures, government or the private sector.

Clearly, it will depend immensely on the starting point of each organization when implementing the CSF to identify which are the main challenges to be addressed. In general terms, there are some challenges that usually arise in most organizations, they are associated with the commitment by senior management to adopt a cybersecurity strategy, the culture of organizational risk [16] and the lack of qualified professionals to be able to lead these processes [15].

According to the OAS report "Cybersecurity: Are we ready in Latin America and the Caribbean?" [12] published in 2016, aspects related to countries' cybersecurity policy and strategy is one of the points to be reinforced in the entire region of Latin America and the Caribbean. We understand that the adoption of this type of framework can contribute positively in the preparation of the cybersecurity strategies of the governments (in particular, in the protection of their critical infrastructures) and in strengthening the processes of regional collaboration.

4. Case studies

The CSF is recognized by the technical community that considers the best practices in relation to cybersecurity. This framework has been adopted by various countries as part of their cybersecurity strategy; some have even included it in their national legislation. Within the countries that have adopted the CSF are: Bermuda, the United States, Israel, Italy, Japan, the United Kingdom, Switzerland and Uruguay [13].

Below, we present two case studies that ha adopted CSF, using different approaches.

4.1. United Kingdom - An open approach

The United Kingdom's HMG Security Policy Framework - SPF [7] is mandatory for all government departments. To collaborate in the implementation of the aforementioned Framework, a series of guides have been developed to address the different aspects of security. One is the MCSS - Minimum Cyber Security Standard [8].

The Minimum Cybersecurity Standard is a joint development between the government of the United Kingdom and the National Cyber Security Centre (NCSC). It was published in June 2018 and takes into account the CSF.

This standard defines the minimum security measures that the departments of the United Kingdom must implement with respect to the protection of their information, technology and digital services in order to comply with their SPF and National Cyber Security Strategy obligations.

This standard adopts the five CSF functions (Identify, Protect, Detect, Respond and Recover) and, although some of the functions and categories–and the wording of each –have been modified, overall, they are very faithful to the original CSF .

The functions in the MCSS are:

1. **Identify:** Departments must implement appropriate cybersecurity governance processes.
2. Departments will identify and catalog their sensitive information.
3. Departments must identify and catalog the key operational services they provide.
4. The need for users to access sensitive information or key operational services must be understood and managed continuously.

5. **Protect:** Access to sensitive information and key operational services will only be provided to users or systems identified, authenticated and authorized.

6. Systems that handle sensitive information or key operational services must be protected against exploitation of known vulnerabilities.

7. Highly privileged accounts should not be vulnerable to common cyber attacks.

8. **Detect:** Departments must take measures to detect common cyber attacks.

9. **Respond:** Departments must have a defined, planned and proven response to cybersecurity incidents that affect confidential information or key operational services.

10. **Recover:** Departments must have well-defined and proven processes to guarantee continuity of the key operational services in case of failure or compromise.

Like the CSF, the MCSS deliberately leaves open the implementation of the guidelines, since it is understood that trying to define a single cybersecurity approach in different industries, platforms and situations is almost impossible. Instead, companies are encouraged to interpret the standard independently and adapt their own security processes to ensure compliance.

4.2. Uruguay - A guided approach

The main purpose of the Uruguay Cybersecurity Framework (MCU) [9], is to generate confidence in the use of technology, unify all existing resources in cybersecurity, and support the evolution of digital government in Uruguay. It also seeks to promote a comprehensive and multi-sector vision of cybersecurity, committing to the continuous improvement of cybersecurity and contributing to the definition of action plans.

Implementation was based on CSF Core v1.0 (ISO/IEC 27001:2013, ISO 27799:2016 [10], COBIT 5 and NIST 800-53 rev.4). In addition, specialists in cybersecurity, international consultants and academia worked on it. Once the first draft of the MCU was prepared, it was submitted for consideration of Universidad de la Republica, where it was analyzed and recommendations were offered. Then it was submitted for consideration of private consultants of the country and their comments were also collected. Finally, version 1.0 was published in August 2016.

Today it has already been used for the diagnosis and evaluation of all the ministries of the central government, government departments, health institutions and financial institutions.

Adaptation of the CSF to the MCU

Although the MCU integrates the entire Core of the NIST CSF v1.0, it implements only a set of Subcategories, leaving the implementation of the missing subcategories for later stages.

This Framework presents a series of requirements that include good practices on security governance, risk management, access control, security of operations, incident management and business continuity associated with the different NIST CSF Subcategories. It also includes an organizational profile and a maturity model where organizations can define the lines of action to improve their cybersecurity. These requirements have adjustments for organizations of the central administration of Uruguay and for health institutions. At present, work is being carried out on adaptation for financial institutions.

Own requirements

The MCU proposes a set of 65 requirements generated from the ISO/IEC 27001 controls and the Uruguayan regulations in connection with cybersecurity.

Organization Profile

Organizations are separated into three profiles: basic, standard and advanced. The assignment of the profile is given by the perception of technological risk. It is important to clarify that only the advanced profile includes all the subcategories adopted by the MCU.

Prioritization of Subcategories

With the understanding that organizations are not all the same, and that depending on their profile they may have to prioritize the implementation of some Subcategories before others, the MCU prioritizes the approach of the CSF Subcategories with the purpose of facilitating the approach and the drawing up of the action plans.

Maturity Model

This model allows organizations to evaluate their current position and to establish, according to their prioritization, the goal of maturity in each Subcategory. Overall, the Tiers establish:

- **Tier 0:** Cybersecurity-based actions almost or totally non-existent

- **Tier1:** There are some initiatives on cybersecurity. Ad-hoc approaches. High dependence on staff. Reactive attitude to security incidents.

- **Tier 2:** There are certain guidelines for the execution of tasks. There is dependence on the staff. There has been progress in the development of processes and documentation of tasks.

- **Tier 3:** It is characterized by the formalization and documentation of policies and procedures. Governance of cybersecurity. Tracking metrics

- **Tier 4:** The Information Security Manager has a key role in the control and improvement of the SGSI. Internal control is performed. Work on continuous improvement is underway. Cybersecurity is aligned with the objectives and strategies of the organization.

Any public or private organization can use the document as a self-knowledge tool and to improve their security levels. To date, it is not compulsory, although its mandatory nature is foreseen in the short term for some critical sectors.

5. Conclusions

The threats of cybersecurity continue to grow and affect all organizations, regardless of their category or size.

Although the CSF was initially conceived as a tool to evaluate cybersecurity in US Critical Infrastructures, its approach–in relation to the point of view of the standards and technological requirements–has shown that it adapts perfectly to different sectors and countries, and is easily adopted in audit processes.

The CSF can be used to create a new cybersecurity program or as a tool to analyze the gap in existing cybersecurity programs and improve them. It is structured in such a way that it enables a comprehensive approach to the governance of cybersecurity, easily aligning it with business needs.

The CSF Subcategories have been mapped to the controls of the main industry standards, facilitating their consolidation, and providing a flexible and clear approach.

Lastly, the CSF has to be seen as a cybersecurity risk management tool that permits the evaluation of the effectiveness of the controls and their profitability.

The most successful cybersecurity programs are those that are not based simply on the application of technical controls, but which define a strategy, a framework, to address each of the essential functions of cybersecurity: identify the context, protect the systems and assets, detect deviations, respond before incidents and recover business operations. In summary, cybersecurity is a business problem that can only be solved with a holistic vision on the part of People, Processes and Technology.

6. References

[1] Casa Blanca (2013), *Orden ejecutiva 13636:* https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[2] NIST (2013), *NIST 800-53 Rev.4:* https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

[3] ISO (2013), *ISO/IEC 27001:* https://www.iso.org/standard/54534.html

[4] ISACA (2012), *COBIT 5:* http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

[5] CIS (2018), *Critical Security Controls (CSC):* https://www.cisecurity.org/controls/

[6] ISO (2018), *ISO/IEC TR 27103:* https://www.iso.org/standard/72437.html

[7] Gobierno de Reino Unido (2013), *Marco de Políticas de Seguridad de Reino Unido:* https://www.gov.uk/government/collections/government-security

[8] Gobierno de Reino Unido (2018), *Marco de ciberseguridad de Reino Unido:* https://www.gov.uk/government/publications/the-minimum-cyber-security-standard

[9] AGESIC (2018), *Marco de Ciberseguridad de Uruguay:* https://www.agesic.gub.uy/innovaportal/v/5823/1/agesic/marco-de-ciberseguridad-v40.html

[10] ISO (2016), *ISO 27799:* https://www.iso.org/standard/62777.html

[11] NIST (2018), CSF v1.1 *(en español)*: https://www.nist.gov/sites/default/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

[12] OEA (2016), *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?:* https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe

[13] NIST, *Adaptaciones internacionales del CSF:* https://www.nist.gov/cyberframework/international-resources

[14] OTAN (2012), *National Cyber Security Framework Manual:* https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

[15] ISC2 (2017), *2017 Global Information Security Workforce Study - Benchmarking Workforce Capacity and Response to Cyber Risk (LATAM):* https://iamcybersafe.org/wp-content/uploads/2017/06/LATAM-GISWS-Report.pdf

[16] Deloitte (2016), *La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información*: https://www2.deloitte.com/pe/es/pages/risk/articles/la-evolucion-de-la-gestion-de-ciber-riesgos-y-seguridad.html

[17] NIST (2018), RFC - *Cybersecurity Framework Draft Version 1.1:* https://www.nist.gov/cyberframework/rfc-cybersecurity-framework-draft-version-11

[18] Homeland Security, *Sectores de infraestructura crítica:* https://www.dhs.gov/cisa/critical-infrastructure-sectors

7. Sources

NIST, *Sitio web oficial del CSF:*
https://www.nist.gov/cyberframework/

NIST, *Historia y creación del CSF*:
https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework

NIST, *Estructura del CSF*:
https://www.nist.gov/cyberframework/online-learning/components-framework

NIST, *Funciones del CSF*:
https://www.nist.gov/cyberframework/online-learning/five-functions

NIST, *Evolución del CSF*:
https://www.nist.gov/cyberframework/evolution

AWS, *NIST Cybersecurity Framework – Aligning to the NIST CSF in the AWS Cloud*:
https://d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.246c0a886c7d16d2b370c20a04f99511d212613a.pdf

— NIST CYBERSECURITY — FRAMEWORK (CSF)

A comprehensive approach to cybersecurity

2019

White paper series
Issue 5

OAS | More rights for more people

aws

— NIST CYBERSECURITY —
FRAMEWORK (CSF)

A comprehensive approach to cybersecurity