Considerations for the Design and Implementation of a

CYBERSECURITY PROMOTION FUND

OAS

More rights
for more people

Considerations for the Design and Implementation of a

CYBERSECURITY PROMOTION FUND

Prepared and published by the Cybersecurity Program of the Inter-American Committee against Terrorism (cybersecurity@oas.org).

The contents expressed in this document are presented exclusively for informational purposes and do not represent the official opinion or position of the Organization of American States, its General Secretariat or its Member States.

CREDITS

Luis Almagro
Secretary General
Organization of American States (OAS)

OAS Technical Team

Arthur Weintraub

Alison August Treppel

Kerry-Ann Barrett

Gabriela Montes de Oca Fehr

Sofía Hunter

Laura Nathalie Hernández Rivera

Pablo Viollier

CONTENT

01 PREFACE

In recent decades, great strides have been made in providing connectivity in the region. In 2017, the mobile revolution and the implementation of public policies designed to promote universal telecommunication access provided nearly 438 million Latin Americans with Internet access, or about 55% of the region's population[1].

Over time, the Internet has ceased t o be just a place for browsing; it has become a medium for daily interaction among millions of individuals. We use the Internet today to communicate, get organized, and debate, but also to educate ourselves, promote governmental efficiency and transparency, and do business.

At the same time, as the dependence of individuals, governments, and companies on the services offered in cyberspace mounts, so too does the risk in its use. This risk can take the form of service interruptions, scams, cybercrime, and theft of personal data and credentials.

For its part, worldwide, the digitization process, as a result of the global SARS-CoV-2 (COVID-19) pandemic, has accelerated, deepened, and brought to the fore the social and economic consequences of the digital divide. The pandemic has found all Latin American countries in a similar situation in terms of cybersecurity: ill-prepared owing to a lack of capacities and resources, and an inadequate institutional framework. Given the ongoing growth of connectivity and dependence of governments, companies, and individuals on cyberspace, cybersecurity has become a necessity and a priority on the agenda of the different countries of the region.

However, these advances in connectivity have not necessarily been accompanied by public policies and joint and coordinated efforts among the different societal actors to ensure the integrity of infrastructure, IT systems, and interactions that take place in cyberspace. In short, the region has grown in connectivity, but not placed enough emphasis on promoting cybersecurity at all levels.

In this sense, setting up a cybersecurity solution can be a great challenge, it is also an opportunity to improve the industry. As an example from the private sector, in the Americas, the Organization of American States, Cisco and the Citi Foundation have created the Cybersecurity Innovation Fund to support and spread business initiatives in Latin America and the Caribbean and create the necessary workforce to fill cybersecurity related jobs in the region. Through this Innovation Fund, financial support and access to a network of professionals in the field, are offered to projects winners of a long selection process based on the originality, sustainability, impact and scalability of the proposals.

[1] Statista (2019)

In this regard, the public sector also has to consider sustainable sourcing for addressing cybersecurity concerns. The reason why national cybersecurity promotion funds (hereinafter, cybersecurity funds) are needed is to provide the means to address the minimization of risks, improve the recovery capacities of stakeholders, and mitigate the damage of potential Cyber incidents. This paper explores the need for a funding mechanism with these characteristics and provides some possible options for consideration.

02 INTRODUCTION

In order to evaluate the feasibility of taking as a model the telecommunication development fund (TDF), explained below, for the funding of cybersecurity funds in Latin America, this paper contains a comparative study of the TDFs of Chile, Brazil, Colombia, and Costa Rica that assesses the feasibility of adopting a similar model for funding initiatives to promote cybersecurity in the region. Specifically, the paper examines the existing governance, formation, fund collection, and criteria analysis mechanisms for resource allocation of the TDFs of these countries.

Based on the analysis of the characteristics, regulatory frameworks, and manner of operation of the aforesaid TDFs, a conceptual framework was developed for the design of public policies that could generate a mechanism for stable, sustainable, and equitable funding of cross-cutting cybersecurity initiatives for Latin America. Lastly, the paper proposes a set of relevant recommendations and adjustments to be taken into account in creating national funds for the promotion and funding of national cybersecurity strategies and initiatives, which should be evaluated based on each country's specific context.

03 CYBERSECURITY FUNDS

Unlike other economic areas, cyberspace is an ecosystem where not only governments and companies participate, but also other actors, such as the technical community, the academic community, civil society, and users. The digital ecosystem's different participants have specific and complementary roles. This means that an opportunity exists for mechanisms promoting the creation of joint initiatives to generate synergies and positive externalities. Thus far, each actor in this ecosystem has had responsibility for funding its own cybersecurity initiatives, although on occasion they have also been funded through specific projects of international organizations such as the Organization of American States (OAS), the World Bank, the International Telecommunication Union (ITU), and the Inter-American Development Bank (IDB). However, there are no stable, transparent, and accessible mechanisms for funding cross-cutting cybersecurity initiatives in the region.

At the same time, as mentioned above, as the dependence of individuals, governments and companies on the services offered in cyberspace mounts, so too does the risk in its use. This risk can take the form of service interruptions, scams, cybercrime, and the theft of personal data and credentials.

These aspects provide justification for the creation of an efficient, multisectoral, and sustainable mechanism for funding initiatives to promote cybersecurity in the region. By such means, the region will be able to prevent a widening gap between the growth of internet access and cyberspace security conditions through a robust, participatory, multisectoral, and multidisciplinary policy.

04 TELECOMMUNICATION DEVELOPMENT FUNDS (TDFS)

Telecommunication development funds (TDFs) or universal service funds (USFs) are a supply subsidy model that has been implemented in different countries of the world and the region to promote and expand telecommunication service coverage. The main form of regulatory intervention in the region was a subsidy for the provision of telephony and internet services, especially through infrastructure deployment and network operation. TDFs, through different funding models generally administered by each country's telecommunication regulatory agency, subsidize telecommunication companies in expanding service delivery and coverage to areas not economically profitable.

TDFs in the region have served as a relatively stable and successful mechanism for the collection, administration, and allocation of resources for funding projects that promote the expansion of telecommunication service coverage in the region, especially services not viable using market criteria.

In order to establish a framework for comparison of the characteristics of the TDFs, the paper analyzes six relevant aspects in the four countries studied:

01 **Goal:** To analyze the rationale and motivation of each country's regulator in implementing and funding the TDF. The four countries studied have a common goal: to increase telecommunication service coverage. However, programs such as those in Brazil and Costa Rica have secondary goals, such as fostering technological innovation, reducing the digital divide, and/or promoting job creation.

02 **Legal framework:** The paper examines in depth the legal basis of each TDF, which in all cases includes an enabling law. In Colombia and Costa Rica, the TDFs are also guided by periodic telecommunication development plans.

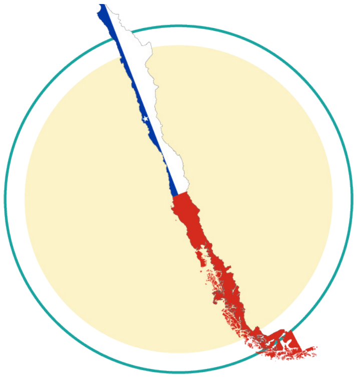
03 **Governance and administration:** Special attention was paid to the different programs' governance and participation schemes, especially to ministries or public entities that participate in decision-making, and to the possibility of participation and influence by civil society, industry, and the academic sector. In general, little room was found for multisectoral participation, Chile being the exception.

04 **Initiatives to be funded:** Considerable latitude was found in the variety of initiatives that could be funded by the different TDFs. Chile's approach focuses more on projects designed to expand telecommunication service coverage, while the other TDFs allow initiatives to be funded in the areas of research and innovation, education, and e-government, among others.

05 **Funding sources:** The paper also explores the programs' different funding sources, which are usually mixed. In general, there are three models: those whose main source is the national budget (Chile), those that impose some type of special rate or tax on telecommunication companies (Brazil), and those with a mixed system that combines the two (Colombia and Costa Rica). In all cases, these revenues are supplemented by other sources, such as donations, remuneration, fines collected, credits, and local government contributions.

06 **Resource allocation criteria:** Also compared are the criteria established in each TDF's regulations for selecting projects that merit funding. It was noted that the different countries allow their regulators different levels of discretion in deciding resource allocation criteria. Chile's law establishes six criteria that must be taken into consideration, while Colombia, Brazil, and Costa Rica allow greater discretion in the competition's terms and conditions prepared.

Lastly, the paper presents a comparison based on the available statistics on the number of projects funded and the amounts involved in each country studied.



CHILE

A total of 14 projects funded: 12 for allocations of funds, and two for radio spectrum allocations in exchange for remuneration from the companies.

Total amount allocated: US$147,667

COLÔMBIA

21 projects funded.

Amount allocated: US$210,135,152

BRAZIL

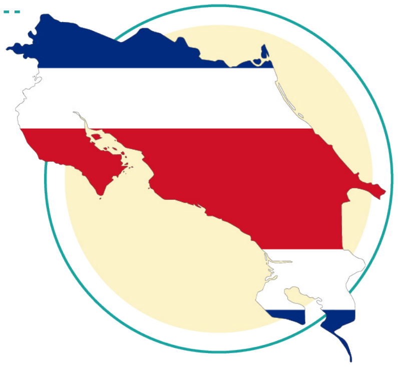
18 projects of different types, for a **total of US$133,889,347**

COSTA RICA

FONATEL funds six programs: Connected Communities, Connected Homes, Connected Public Centers, Connected Public Spaces, Solidarity Broadband, and Connected Citizen.

Budget execution as of 2018: US$44,278,899.39 (representing 90%).

Total budget execution as of December 31, 2018: US$81,284,304.44



05 TDFS AS A MODEL FOR FUNDING CYBERSECURITY INITIATIVES

Fundamentals

The relative success of TDFs in Latin America is due, in part, to the fact that they were created in response to a real societal need: to extend telecommunication coverage to economically unviable areas. Two aspects of the TDFs that should be considered for inclusion in a model for the cybersecurity fund, were identified:

01 **Network effects:** A cybersecurity fund may be understood as a way of generating a network effect[2] different from that of TDFs. If the TDF's goal is to increase telecommunication services coverage, a cybersecurity fund would make it possible to fund cybersecurity initiatives not now profitable for market reasons, and would create a more secure and resilient digital ecosystem. In other words, by increasing the confidence of individuals and organizations in cyberspace, it is possible to increase the universe of people willing to use digital media for social and economic activities and their interactions with the government[3]. This not only makes it possible to increase the number of commercial interactions that take place in cyberspace, but can also serve as an incentive to promote the digital transformation of different productive sectors of the region.

02 **Resource distribution mechanism:** The fund would operate as a form of direct transfer of resources from members of the cybersecurity ecosystem that have sufficient resources to finance their cybersecurity initiatives to those that do not.

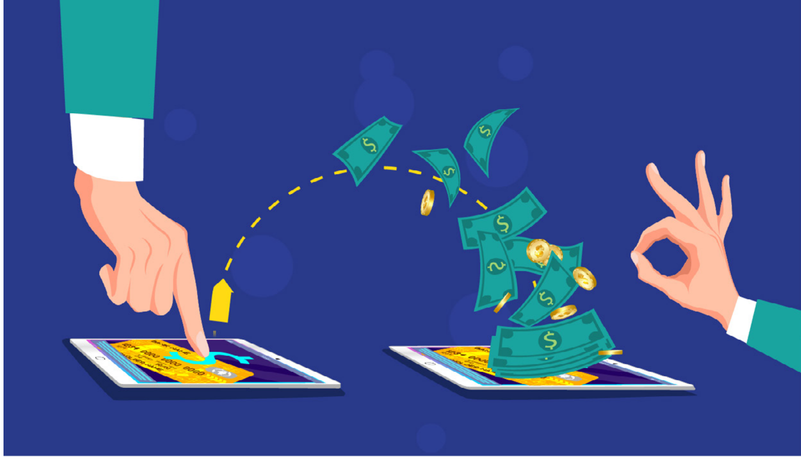
This redistributive effect can be achieved in two ways. The first, through a specific tax intended to ensure that members of the industry absorb the negative externalities of their economic activity. This alternative has been used, for example, in environmental regulation to ensure that the mining industry absorbs pollution costs that otherwise would have to be borne by society as a whole.

[2] Network effect is defined as the increase in the value of the network for each user due to the increase in the number of other users (Neuchterlein and Weiser, 2005: 352).

[3] Thus, for example, a survey conducted in 2017 by the National Telecommunications and Information Administration of the United States showed that 33% of American households did not engage in e-commerce activities due to computer security and privacy concerns (NTIA, 2017).

The second can be achieved indirectly through direct State funding of the fund through general taxes, provided the country has a progressive, non-regressive tax system.

The TDFs of Brazil and Colombia may be considered the most efficient models for achieving the network effect, and, as for resource distribution mechanisms, desirable for the creation of a cybersecurity fund.



Necessary adaptations of the TDF model for cybersecurity initiatives

Governance scheme

The governance model of the telecommunications funds of the four countries studied, in general, is based on the coordination and assignment of competencies at the inter-ministerial level, in accordance with the provisions of the corresponding internal laws and regulations. A multisectoral governance scheme that allow for the inclusion and consideration of different key cybersecurity sectors is a strategic and operational approach for three reasons:

- It allows for multidisciplinary feedback of experience, which promotes evidence-based decision-making.
- It produces a mutual control mechanism.
- It facilitates more efficient resource execution by creating the conditions for greater oversight of resources, projects, and decisions.

Characterization of the initiatives to be funded

In creating cybersecurity funds, a major challenge will be to describe specifically the projects or initiatives to be funded. However, it is adviced to adopt a broad framework of competition-based projects. Thus, rather than analyzing resource allocation criteria, consideration could be given to creating a fund with sub-competitions, under categories or aspects such as:

1. Infrastructure
2. Technological solutions
3. Vulnerability diagnostic assessment
4. Training
5. Awareness Training campaigns

In order to promote cooperation between the different digital ecosystem participants, the possibility might be explored of prioritizing initiatives designed to address any issues established as priorities through dialogue among different actors. Mechanisms could also be established to promote collaboration among sectors or actors, assigning higher scores in competitions to projects composed of diverse participants (e.g., a joint research project between civil society and companies).

Forms of funding

The selection of a specific funding mechanism is heavily contingent upon the theoretical framework justifying its creation, and this may directly impact the political legitimacy and viability of implementing a fund with these characteristics. Below is a brief description of possible mechanisms for financing this public policy:

Specific rate or tax:

This is the financing mechanism most used in the TDFs in Latin America, and in the case studies of Colombia and Brazil in this paper. Once a specific rate or tax is established, permanence over time would be established until the law that enacted it is modified, resulting in economic and legal certainty to the funding of the policy. However, unlike TDFs (where the number of companies naturally subject to these taxes is limited and defined), a multiplicity of actors coexist in the cybersecurity ecosystem, with no uniform criterion as to which should bear this specific tax burden, and their respective proportions. If this form of financing is chosen, it would be fundamental–albeit a challenge–to design an objective, transparent and rigorously founded criterion to decide which sectors of the technology industry would be subject to this special fee and which would not.

Redistributive Tax:

Through this mechanism, the fund is funded through general national revenues. To some extent, it makes sense that, if cybersecurity becomes a cross-cutting need for society, it is up to society as a whole to fund those cybersecurity initiatives that are not profitable according to market criteria. However, this is only feasible if the country's tax system is effectively redistributive. Moreover, the availability of economic resources is contingent upon the political debate and the annual governmental budget allocation.

Supplementary income:

Although the two options analyzed above are presented as the main options for financing the existence of a cybersecurity fund, there are complementary financing sources that deserve to be explored. Some alternatives in the telecommunications area explored by the countries studied include:

- Spectrum license income for the funding of universal services.
- Income from fines.
- Remuneration (the industry's commitment to carry out public investment or deliver free of charge a service to a given rural area for a given period of time, in exchange for a spectrum allocation license).
- There are also other options, such as tax benefit schemes, public-private partnerships for specific projects, and cross-subsidy schemes.

Resource allocation criteria

An element key to the institutional legitimacy of a cybersecurity fund is to ensure that the relevant resource allocation criteria are transparent and objective, that allocations are open to all ecosystem participants, and that the impact of the funded projects can be measured.

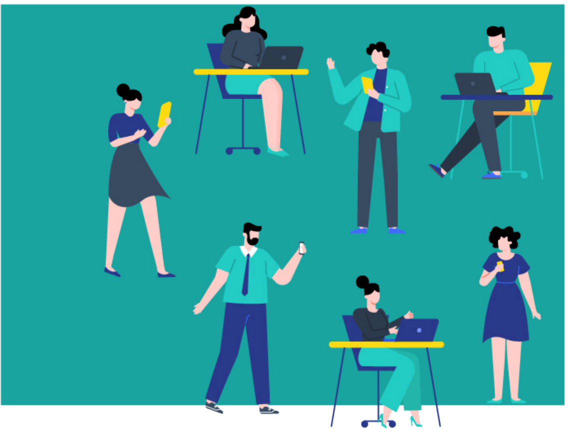
Unlike initiatives in telecommunications, a cybersecurity fund would fund a wide array of initiatives whose impacts may be extremely difficult to measure using exclusively quantitative criteria. Therefore, qualitative impact evaluation methodologies may be helpful when estimating the impact of projects funded. However, at the regulatory level, the challenge remains as to how to include these impact criteria in the competition's terms and conditions, so that the allocation criteria are transparent, objective, and not arbitrary, especially when initiatives of a diverse nature compete.

Lastly, it is also recommended that project proposals undergo a technical-economic evaluation before they are submitted for the competition. To the extent possible, this evaluation should study the technical feasibility of projects, and estimate their costs and potential benefits, as mentioned above, taking into account a wide range of impact indicators, both quantitative and qualitative.

06 CONCLUSIONS

The experience in the operation of the TDFs may serve as reference in designing cybersecurity funds. In this way, a mechanism can be designed aimed at strengthening cybersecurity conditions, together with policies aimed at bridging the gap in internet access.

The TDFs of Chile, Costa Rica, Brazil, and Colombia provide valuable experience for the design of funding mechanisms for cybersecurity initiatives, both those aspects of the TDF that merit assimilation or reproduction, and those needing to be adapted or modified according to the specificities of a cybersecurity challenge.



This paper analyzes the form of operation, resource use efficiency, heterogeneity in the types of initiatives funded, democratization of participation and decision-making, and the achievement of results with positive impact for the country and the multiple stakeholders comprising or intervening in cyberspace.

The TDFs studied in this paper have several elements that should be incorporated in the design and operation of an effective, efficient, participatory, and sustainable cybersecurity fund. However, it will always be necessary to consider cybersecurity's different challenges and specificities and make the adjustments relevant to the local context where a cybersecurity fund with these characteristics is to be created.

07 RECOMMENDATIONS

Identify the conceptual basis justifying the cybersecurity fund, and its funding mechanism.

Adopt the multisectoral governance model for the deliberations and decision-making from a multidisciplinary and participatory perspective.

Promote the funding of diverse and heterogeneous projects by creating competition subcategories that describe in detail, objectively and transparently, the types of initiative to be funded.

Initially, use public funds as a funding mechanism for initiatives, so as to inject resources into public policy.

Adopt qualitative methodologies that make it possible to evaluate the impact of training initiatives, awareness campaigns, and other initiatives for the drafting of resource allocation and objective evaluation criteria for the initiatives.

Identify the funding needs of the different actors in the region's cybersecurity ecosystem, with an emphasis on actors who are members of or represent vulnerable groups.

Map the options currently available to actors of the region's cybersecurity ecosystem when they are seeking funding for their cybersecurity projects.

Develop a qualitative methodology for evaluating the impact of the cybersecurity measures implemented, using objective and transparent mechanisms.

08 REFERENCES

Álvarez, Daniel y Vera, Francisco (2017) Ciberseguridad y derechos humanos en América Latina. En Hacia una Internet libre de censura II: Perspectivas en América Latina; compilado por Agustina Del Campo . - 1a ed . - Ciudad Autónoma de Buenos Aires: Universidad de Palermo - UP.

Statista (2019) Internet usage in Latin America - Statistics & Facts. Disponible en: https://www.statista.com/topics/2432/internet-usage-i

Sturzenneger, Federico y Tommasi, Mariano (1998) The political economy of economic reforms. Boston: MIT Press.

Nuechterlein, Jonathan y Weiser, Philip (2005) Digital Crossroads: American Telecommunications Policy in the Internet Age. The MIT Press. ISBN: 978-0262640664.

NTIA (2017) Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds. Available at: https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds

Brazil

Decree No. 3.737, January 30, 2001 http://www.planalto.gov.br/ccivil_03/decreto/2001/D3737.htm

Decree No. 8.943, December 27, 2016. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8943.htm

Act No. 10.052, November 28, 2000 http://www.planalto.gov.br/ccivil_03/LEIS/L10052.htm

Chile

Act 20.522. Available at: https://www.leychile.cl/Navegar?idNorma=1027475&buscar=20522

Act 18.168. Available at: https://www.leychile.cl/Navegar?idNorma=29591

Regulation of the Telecommunications Development Fund, contained in Supreme Decree No. 353, of 2001, of the Ministry of Transport and Telecommunications. Available at: https://www.leychile.cl/Navegar?idNorma=193117

Report on the Telecommunications Development Fund 2017. Subtel. Available at: https://www.subtel.gob.cl/quienes-somos/divisiones-2/fondo-de-desarrollo-de-las-telecomunicaciones/memoria-fdt/

Colombia

Decree 129, of January 26, 1976 http://www.suin-juriscol.gov.co/viewDocument.asp?id=1028789

Decree 1,078, of May 26, 2015 https://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

Decree 1,414, August 25, 2017 https://www.mintic.gov.co/portal/604/articles-57805_documento.pdf

Evaluation of the Programs of the Vive Digital para la Gente Plan, Financed with Resources from the Information and Communication Technologies Fund (FONTIC) (National Planning Directorate) https://colaboracion.dnp.gov.co/CDT/Prensa/EstudioFONTIC.pdf

Management Report 2018 (MINTIC) https://www.mintic.gov.co/portal/604/articles-1785_informe_gestion_plan_accion_fontic_mintic_2018_v20190131.pdf

Act 1,341, of July 30, 2009 https://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

Act 1,887, of April 23, 2018 http://es.presidencia.gov.co/normativa/normativa/LEY%201887%20DEL%2023%20DE%20ABRIL%20DE%202018.pdf

Act 1753, of June 9, 2015 https://colaboracion.dnp.gov.co/CDT/Normograma/Ley%201753%20de%202015.pdf

2019 Action Plan (MINTIC) https://www.mintic.gov.co/portal/604/articles-1785_plan_accion_2019_20190131.pdf

Vive Digital Plan 2010-2014 https://www.mintic.gov.co/portal/vivedigital/612/articles-1510_recurso_1.pdf

Vive Digital Plan 2014-2018 https://www.mintic.gov.co/portal/604/articles-5193_recurso_2.pdf

Costa Rica

Costa Rica. Ministry of Science, Technology, and Telecommunications (MICITT). National Cybersecurity Strategy Costa Rica 2017. San José, C. R.: MICITT, 2017.

Costa Rica. Ministry of Science, Technology, and Telecommunications (MICITT). Digital Transformation Strategy towards Bicentennial Costa Rica 4.0, 2018-2022. Available at: https://www.micit.go.cr/documentos/micitt_estrategia_transformacion_digitaldel_bicentenario.pdf

Costa Rica. Ministry of Science, Technology, and Telecommunications (2015). National Plan for the Development of Telecommunications 2015-2021. Costa Rica: A Connected Society. Available at: http://www.siteal.iipe.unesco.org/sites/default/files/sit_accion_files/siteal_costa_rica_5039.pdf

General Telecommunications Act No. 8642. Available at: https://www.palermo.edu/cele/pdf/Regulaciones/CostaRica8642eyGraldeTelecomunicaciones(2008).pdf

Act for the Strengthening and Modernization of Public Entities of the Telecommunications Sector, No. 8660/08. Available at: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=63786&nValor3=91177&strTipM=TC

Considerations for the Design and Implementation of a

CYBERSECURITY PROMOTION FUND

OAS | More rights for more people