Consideraciones para el diseño e implementación de un fondo de promoción DE LA CIBERSEGURIDAD

OEA | Más derechos para más gente

Consideraciones para el diseño e implementación de un fondo de promoción DE LA CIBERSEGURIDAD

Preparado y publicado por el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (cybersecurity@oas.org).

CRÉDITOS

Luis Almagro
Secretario General
Organización de los Estados Americanos (OEA)

Equipo Técnico de la OEA

Arthur Weintraub

Alison August Treppel

Kerry-Ann Barrett

Gabriela Montes de Oca Fehr

Sofía Hunter

Laura Nathalie Hernández Rivera

Pablo Viollier

ÍNDICE

01 PRESENTACIÓN

En las últimas décadas, la región ha avanzado a pasos agigantados en materia de conectividad. La revolución móvil y la implementación de políticas públicas que aspiran a promover el acceso universal en materia de telecomunicaciones ha permitido que, para el año 2017, cerca de 438 millones de latinoamericanos hayan logrado tener acceso a Internet, lo que equivale a cerca del 55% de la población de la región[1].

Con el tiempo, internet ha dejado de ser sólo un lugar para buscar y se ha transformado en un medio para la interacción cotidiana de millones de individuos. Hoy usamos internet para comunicarnos, organizarnos y debatir, así como para educarnos, promover la eficiencia y transparencia de los Gobiernos y hacer negocios.

Al mismo tiempo, a medida que aumenta la dependencia de los individuos, Gobiernos y empresas de los servicios ofrecidos en el ciberespacio aumenta el riesgo en su utilización. Este riesgo puede tomar la forma de interrupciones en el servicio, estafas o delitos informáticos y el robo de datos y credenciales personales.

Por su parte, la pandemia global producida por el SARS-CoV-2 (Covid-19) ha tenido la consecuencia de acelerar y profundizar el proceso de digitalización a nivel mundial, así como de evidenciar las consecuencias sociales y económicas de la brecha digital. La pandemia nos encontró a todos los países de América Latina en una situación similar en materia de ciberseguridad: poco preparados debido a la falta de capacidades, recursos y una institucionalidad poco adecuada. De esa forma, ante el sostenido aumento de la conectividad y la dependencia de Gobiernos, empresas e individuos en el ciberespacio, la ciberseguridad se ha transformado en una necesidad y una prioridad en la agenda de los distintos países de la región.

Sin embargo, los avances en materia de conectividad no han estado acompañados necesariamente por políticas públicas ni por el esfuerzo coordinado entre los distintos actores de la sociedad para asegurar la integridad de la infraestructura, los sistemas informáticos y las interacciones que tienen lugar en el ciberespacio. En definitiva, la región ha crecido en conectividad, pero no ha puesto el énfasis necesario en promover la ciberseguridad en todos sus niveles.

En este sentido, la creación de una solución de ciberseguridad puede ser un gran desafío, como es también una oportunidad para mejorar la industria. Como ejemplo del sector privado, en América, la Organización de Estados Americanos, Cisco y la Fundación Citi han creado el Fondo de Innovación en Ciberseguridad para apoyar y difundir iniciativas empresariales en América Latina y el Caribe y crear la fuerza laboral necesaria para cubrir puestos de trabajo relacionados con la ciberseguridad en la región. A través de este Fondo de Innovación, apoyo financiero y acceso a una red de profesionales en la materia son ofrecidos a los proyectos ganadores de un largo proceso de selección basado en la originalidad, sostenibilidad, impacto y escalabilidad de las propuestas.

[1] Statista (2019)

En este sentido, el sector público también debe considerar el abastecimiento sostenible para abordar los problemas de ciberseguridad. La razón por la que se necesitan fondos nacionales de promoción de la ciberseguridad (en adelante, fondos de ciberseguridad) es proporcionar los medios para abordar la minimización de los riesgos, mejorar las capacidades de recuperación de actores clave, y mitigar los daños de posibles incidentes cibernéticos. Este documento explora la necesidad de un mecanismo de financiación con estas características y ofrece algunas posibles opciones para su consideración.

02 INTRODUCCIÓN

El presente informe se propone evaluar y desarrollar un marco conceptual para la formulación de políticas públicas que permitan generar un mecanismo de financiamiento estable, sostenible y equitativo para iniciativas transversales en materia de ciberseguridad para América Latina. En particular, se propone la creación de fondos nacionales para la promoción de la ciberseguridad (en adelante, fondos de ciberseguridad), tomando como experiencia a emular el funcionamiento que han tenido distintos fondos de desarrollo de las telecomunicaciones (en adelante, FDT) en la región a partir de los años noventa.

Con la finalidad de evaluar la factibilidad de emular la forma de funcionamiento de los Fondos de Desarrollo de las Telecomunicaciones (FDT), los cuales se explican más adelante, para que sirvan como modelo para la asignación de financiamiento de iniciativas que promuevan la ciberseguridad en América Latina, este documento contiene un estudio comparativo entre los FDT de Chile, Brasil, Colombia y Costa Rica en el que se evalúa la factibilidad de la adopción de un modelo similar para la asignación de financiamiento de iniciativas que tengan como fin la promoción de la ciberseguridad en la región. Específicamente, el documento analiza los mecanismos de gobernanza, integración, recaudación de fondos y análisis de criterios para la asignación de los recursos presentes en los FDT de estos países.

A partir del análisis de las características, los marcos normativos y la forma de funcionamiento de los mencionados FDT se construyó un marco conceptual para el diseño de políticas públicas que permitan generar un mecanismo para el financiamiento estable, sostenible y equitativo de iniciativas transversales en materia de ciberseguridad para América Latina. Finalmente, el documento propone una serie de recomendaciones y adecuaciones pertinentes que deberán considerarse en la creación de fondos nacionales para la promoción y el financiamiento de estrategias nacionales e iniciativas de ciberseguridad las cuales deberán ser evaluadas de acuerdo con el contexto particular de cada país.

03 FONDOS DE CIBERSEGURIDAD

A diferencia de otras áreas económicas, el ciberespacio es un ecosistema en donde no sólo participan Gobiernos y empresas, sino también otros actores, como la comunidad técnica, los círculos académicos, la sociedad civil y los usuarios. Los distintos participantes del ecosistema digital cumplen roles específicos y complementarios. Ello significa que existe la oportunidad para que los mecanismos que tiendan a la creación de iniciativas conjuntas generen sinergias y externalidades positivas en su funcionamiento. Hasta el momento, a cada actor de este ecosistema le ha correspondido financiar sus propias iniciativas de ciberseguridad, aunque en algunas ocasiones también hayan sido financiadas por proyectos específicos de organismos internacionales como la OEA, el Banco Mundial, la Unión Internacional de Telecomunicaciones (UIT) y el Banco Interamericano de Desarrollo (BID). No obstante, no existen mecanismos estables, transparentes y accesibles que busquen financiar iniciativas transversales de ciberseguridad en la región.

Al mismo tiempo, como se mencionó anteriormente, a medida que aumenta la dependencia de los individuos, Gobiernos y empresas de los servicios ofrecidos en el ciberespacio, aumenta el riesgo en su utilización. Este riesgo puede tomar la forma de interrupciones en el servicio, estafas o delitos informáticos y robo de datos personales y credenciales.

Son estos los aspectos que justifican la creación de un mecanismo eficiente, multisectorial y sostenido en el tiempo para financiar iniciativas de promoción de la ciberseguridad en la región. De esta forma, la región podrá evitar la expansión de la brecha entre el crecimiento en el nivel de acceso a internet y las condiciones de seguridad del ciberespacio a través de una política robusta, participativa, multisectorial y multidisciplinaria.

04 LOS FONDOS DE DESARROLLO DE LAS TELECOMUNICACIONES (FDT)

Los fondos de desarrollo de las telecomunicaciones (FDT) o fondos de servicio universal (FSU) son un modelo de subsidio a la oferta que se implementó en distintos países del mundo y la región con el objetivo de promover y extender la cobertura de los servicios de telecomunicaciones. La principal forma de intervención normativa en el área tomó la forma de subsidio a la prestación de servicios de telefonía e internet, en particular a través del despliegue de infraestructura y la operación de redes. A través de distintos modelos de financiamiento, generalmente administrados por la agencia reguladora de las telecomunicaciones de cada país, los FDT buscan subsidiar a las empresas de telecomunicaciones a fin de extender la prestación y cobertura de servicios a las áreas que no resultan económicamente rentables.

Los FDT en la región han servido como un mecanismo relativamente estable y exitoso para la recaudación, administración y asignación de recursos que permiten financiar proyectos que promueven el aumento de la cobertura de los servicios de telecomunicaciones en la región, en particular aquellos que no son viables de acuerdo con criterios de mercado.

A fin de establecer un marco común para comparar las características de los FDT, el documento analiza seis aspectos importantes en los cuatro países objeto de estudio:

01 **Objetivo:** analizar el fundamento y la motivación del organismo regulador de cada país al implementar y financiar el FDT. Los cuatro países estudiados comparten un objetivo común: aumentar la cobertura de los servicios de telecomunicaciones. Sin embargo, algunos programas, como los de Brasil y Costa Rica, incluyen objetivos secundarios, tales como fomentar la innovación tecnológica, reducir la brecha digital y promover la generación de empleos.

02 **Marco jurídico:** el documento analiza en profundidad el fundamento jurídico de cada uno de los FDT, los cuales, en todos los casos, están basados en una ley habilitante. Además, en Colombia y Costa Rica los FDT están guiados por planes de desarrollo periódicos en materia de telecomunicaciones.

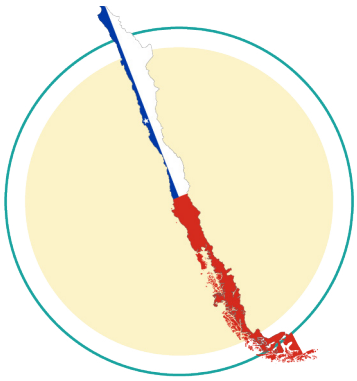
03 **Gobernanza y administración: se prestó especial atención a los esquemas de gobernanza y participación de los distintos programas, en** especial a los ministerios u organismos públicos participan en la toma de decisiones y a la posibilidad de participación e incidencia de la sociedad civil, industria y el sector académico. En general, se observó poco espacio para la participación multisectorial, siendo Chile la excepción.

04 **Iniciativas a financiar: r**especto al espectro de iniciativas susceptibles de ser financiadas por los distintos FDT, se constató un importante nivel de flexibilidad. Chile tiene un enfoque más centrado en aquellos proyectos que buscan aumentar la cobertura de los servicios de telecomunicaciones, mientras que los otros FDT permiten financiar iniciativas en materia de investigación e innovación, educación y Gobierno digital, entre otras.

05 **Fuentes de financiamiento:** el documento también analiza las distintas fuentes de financiamiento de los programas, los cuales suelen ser mixtos. Sin embargo, en general, se dividen en tres modelos: aquellos cuya principal fuente proviene del presupuesto nacional (Chile), aquellos que establecen algún tipo de tasa o impuesto especial a las empresas de telecomunicaciones (Brasil) y aquellos que tienen un sistema mixto, que utiliza una combinación de ambos (Colombia y Costa Rica). Estos ingresos se complementan en todos los casos con otras fuentes, tales como donaciones, contraprestaciones, cobro de multas, créditos y aportes de Gobiernos locales.

06 **Criterios para la asignación de recursos:** del mismo modo, se comparan los criterios establecidos en la regulación de cada FDT para determinar los proyectos que merecen ser financiados. Se observa que los distintos países entregan distintos niveles de discrecionalidad a sus organismos reguladores para decidir los criterios utilizados en la asignación de recursos. Por ejemplo, Chile tiene seis criterios establecidos por ley que deben ser tomados en consideración, mientras que Colombia, Brasil y Costa Rica cuentan con mayor discrecionalidad para elaborar las bases de la licitación de proyectos.

Por último, el documento realiza una comparación en base a las estadísticas disponibles con respecto al número de proyectos financiados y a los montos involucrados en cada país estudiado.



CHILE

14 proyectos financiados en total: 12 de asignación de fondos y 2 asignaciones de espectro radioeléctrico a cambio de contraprestaciones por parte de las empresas.

Monto total asignado asciende a US$147.667

COLOMBIA

21 proyectos financiados.

Monto asignado asciende a los US$210.135.152

BRASIL

18 proyectos de distinta naturaleza que corresponden **a un total de US$133.889.347**

COSTA RICA

FONATEL financia 6 programas: Comunidades Conectadas, Hogares Conectados, Centros Públicos Conectados, Espacios Públicos Conectados, Banda Ancha Solidaria y Ciudadanos Conectados.

Ejecución presupuestaria al 2018: US$44.278.899,39 (representa un 90%).

Total de ejecución presupuestaria hasta el 31 de diciembre de 2018: US$81.284.304,44

05 LOS FDT COMO MODELO A SEGUIR PARA EL FINANCIAMIENTO DE INICIATIVAS DE CIBERSEGURIDAD

Fundamentos

El relativo éxito de los FDT en América Latina se debe, en parte, al hecho de que su creación respondió a una necesidad social real: extender la cobertura de las telecomunicaciones a áreas económicamente inviables. Dos aspectos que sirven de fundamento para considerarlos como modelo para la creación de fondos de promoción de iniciativas de ciberseguridad, fueron identificados:

01 **Efectos de red:** un fondo de promoción de la ciberseguridad podría entenderse como una forma de generar un efecto de red[2] en un sentido distinto a los FDT. Si el objetivo de los FDT es aumentar la cobertura de los servicios de telecomunicaciones, un fondo de ciberseguridad permitiría financiar iniciativas que hoy no resultan rentables por razones de mercado y generaría un ecosistema digital más seguro y resiliente. En otras palabras, al aumentar la confianza de los individuos y las organizaciones en el ciberespacio se logra aumentar el universo de personas dispuestas a utilizar los medios digitales para actividades sociales, económicas y sus interacciones con el Gobierno[3]. Esto no sólo permite expandir las interacciones comerciales que se realizan a través del ciberespacio, sino que puede servir como un incentivo para promover la transformación digital de los distintos sectores productivos de la región.

02 **Mecanismo para la distribución de recursos:** el fondo operaría como un mecanismo de transferencia directa de recursos desde los miembros del ecosistema de ciberseguridad que cuentan con suficientes recursos para financiar sus iniciativas de ciberseguridad hacia aquellos que no cuentan con dichos recursos.

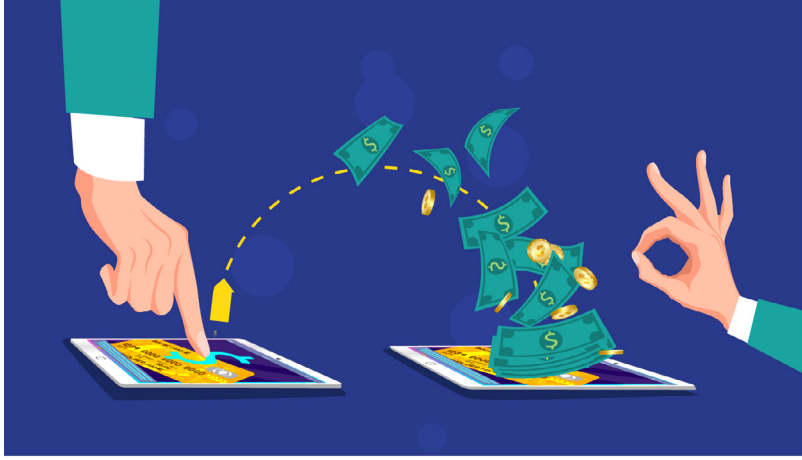
Este efecto redistributivo puede concretarse de dos formas. La primera, a través de un impuesto específico destinado a que los miembros de la industria internalicen las externalidades negativas de su actividad económica. Esta alternativa ha sido utilizada, por ejemplo, por la regulación medioambiental, con el objetivo de que la industria minera internalice los costos de la contaminación que, de otra forma, debe costear la sociedad en su conjunto.

[2] El efecto de red se define como el aumento del valor de la red para cada usuario debido al aumento del número de otros usuarios. (Nuechterlein y Weiser, 2005:352)

[3] Por ejemplo, una encuesta realizada el año 2017 por la *National Telecommunications and Information Administration* de Estados Unidos mostró que un 33% de los hogares estadounidense se abstuvo de realizar actividades de comercio electrónico a raíz de preocupaciones relacionadas con seguridad informática y privacidad (NTIA, 2017).

La segunda se materializa, de forma indirecta, a través de un financiamiento directo del Estado al fondo a través de impuestos generales, siempre y cuando el país cuente con un sistema impositivo progresivo y no regresivo.

Los FDT de Brasil y Colombia pueden considerarse los modelos más eficientes para lograr el efecto red y respecto de los mecanismos adoptados para la distribución de recursos, deseables para la creación de un fondo de promoción de la ciberseguridad.

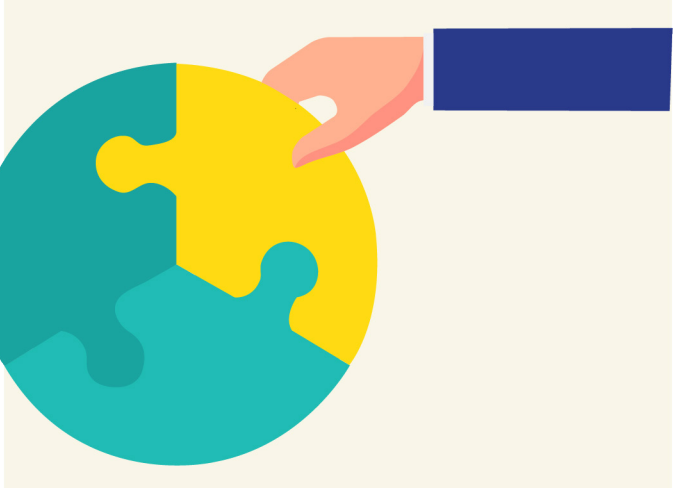


Adecuaciones necesarias del modelo de FDT para iniciativas de ciberseguridad

Esquema de gobernanza

El modelo de gobernanza de los fondos de telecomunicaciones de los cuatro países estudiados, en general, se basa en la coordinación y asignación de competencias a nivel interministerial, de acuerdo con lo establecido en las correspondientes leyes y reglamentos internos. Generar un esquema de gobernanza multisectorial que permita incluir y considerar a distintos sectores clave en materia de ciberseguridad es un enfoque estratégico y operacional por tres razones:

- Permite una retroalimentación multidisciplinaria de experiencia que promueve la toma de decisiones basadas en evidencias.
- Genera un mecanismo de control mutuo.
- Permite una ejecución más eficiente de los recursos al generar las condiciones para una mayor fiscalización sobre los recursos, proyectos y decisiones.



Caracterización de las iniciativas que se financian

Un desafío significativo para la creación de fondos de promoción de la ciberseguridad será describir específicamente los proyectos o iniciativas que serán financiadas. Sin embargo, se sugiere la adopción de un marco amplio de proyectos concursables. Por lo tanto, en lugar de analizar criterios para la entrega de recursos, podría considerarse la creación de un fondo con sub-concursos, bajo categorías o aspectos tales como:

1. Infraestructura
2. Soluciones tecnológicas
3. Diagnóstico de vulnerabilidad
4. Capacitación
5. Campañas de concientización

A fin de promover la cooperación entre los distintos participantes del ecosistema digital es posible explorar la posibilidad de priorizar las iniciativas que apunten a abordar temáticas que hayan sido establecidas como prioritarias a través del diálogo entre distintos actores. Además, podrían establecerse mecanismos de promoción de la colaboración entre los sectores o actores, asignando mayor puntaje en los concursos a proyectos que estén compuestos por una diversidad de participantes (por ejemplo: un proyecto de investigación conjunto entre sociedad civil y empresas).

Forma de financiamiento

La elección de un mecanismo específico de financiamiento está fuertemente determinada por el marco teórico de justificación para la creación del mismo, lo que puede repercutir directamente en la legitimidad y viabilidad política de implementar un fondo con estas características. A continuación, se describen brevemente los posibles mecanismos de financiación de esta política pública:

Tasa o impuesto específico:

Este sistema de recaudación es el más utilizado en los TDF de América Latina, y en los casos de estudio de Colombia y Brasil en este documento. Una vez establecida una tasa o impuesto específico, se establecería la permanencia en el tiempo hasta que se modifique la ley que lo promulgó, resultando en certeza económica y jurídica al financiamiento de la política. Sin embargo, a diferencia de los FDT (donde existe un número acotado y definido de empresas que son naturalmente objeto de estos impuestos), en el ecosistema de la ciberseguridad conviven una multiplicidad de actores sin existir un criterio uniforme respecto de quiénes y en qué proporción deberían asumir esta carga tributaria específica. Si se opta por esta forma de financiación, sería fundamental -aunque sea un desafío- diseñar un criterio objetivo, transparente y rigurosamente fundamentado para decidir qué sectores de la industria tecnológica estarían sujetos a esta tasa especial y cuáles no.

Impuesto redistributivo:

A través de este mecanismo, el fondo se financia a través de los ingresos generales de la nación. Hasta cierto punto tiene sentido que, si la ciberseguridad se transforma en una necesidad transversal para la sociedad, le corresponda a la sociedad, en su conjunto, financiar aquellas iniciativas de ciberseguridad que no sean rentables de acuerdo con criterios de mercado. Sin embargo, esto sólo resulta viable si el sistema tributario del país es efectivamente redistributivo. Además, la disponibilidad de recursos económicos está condicionada al debate político contingente y a la asignación de presupuesto anual por parte de los Gobiernos.

Ingresos complementarios:

Aunque las dos opciones analizadas anteriormente se presentan como las principales para financiar la existencia de un fondo de ciberseguridad, existen fuentes de financiación complementarias que merecen ser exploradas. Algunas alternativas exploradas por los países estudiados en materia de telecomunicaciones incluyen:

- Ingresos por licencias de espectro para financiar los servicios universales.
- Ingresos procedentes de multas.
- Contraprestaciones (el compromiso de la industria de realizar por su cuenta una inversión pública o la entrega de un servicio gratuito a cierta área rural por un determinado período de tiempo, a cambio de la asignación de una licencia de espectro también).
- Asimismo, existen otras alternativas tales como esquemas de beneficios tributarios, alianzas público-privadas para proyectos específicos y esquemas de subvenciones cruzadas.

Criterios para la asignación de recursos

Uno de los elementos centrales para dotar de legitimidad institucional a la creación de un fondo de ciberseguridad es que los criterios pertinentes para dirimir la asignación de recursos sean transparentes, objetivos y abiertos a todos los participantes del ecosistema y que el impacto de los proyectos financiados sea medible.

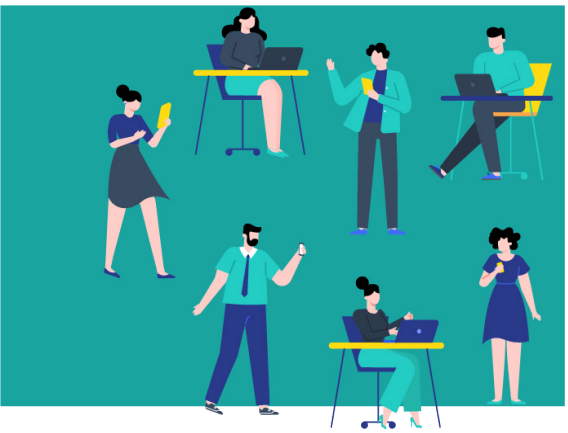
A diferencia de las iniciativas de telecomunicaciones, un fondo de ciberseguridad se encargaría de financiar iniciativas de naturaleza muy variada y cuyo impacto puede resultar sumamente difícil de medir a través de criterios exclusivamente cuantitativos. Para ello, recurrir a metodologías cualitativas de evaluación de impacto puede resultar útil para estimar los efectos de los proyectos financiados. Sin embargo, a nivel regulatorio se mantiene el desafío de establecer estos criterios de impacto en las bases de los concursos públicos, de forma tal que los criterios de asignación resulten transparentes, objetivos y no arbitrarios, especialmente cuando compiten iniciativas de naturaleza diversa.

Por último, también resulta recomendable que los proyectos sean sometidos a una evaluación técnico-económica previa al momento de presentarse al concurso público. En lo posible, esta evaluación debería estudiar de factibilidad técnica de los proyectos, estimar sus costos y sus posibles beneficios, teniendo en consideración, como mencionamos anteriormente, una amplia gama de indicadores de impacto, tanto cuantitativos como cualitativos.

06 CONCLUSIONES

La experiencia en el funcionamiento de los fondos de desarrollo de las telecomunicaciones (FDT) puede servir como referencia para diseñar un fondo de promoción de iniciativas de ciberseguridad. Por lo tanto, es posible diseñar un mecanismo que busque fortalecer las condiciones de seguridad en el ciberespacio, acompañado por políticas orientadas a disminuir la brecha del acceso a internet.

Los FDT de Chile, Costa Rica, Brasil y Colombia ofrecen una experiencia valiosa para la creación de mecanismos de financiamiento de iniciativas de ciberseguridad tanto en los aspectos de los FDT que merecen ser asimilados o reproducidos, como en aquellos que requieren ser adaptados o modificados conforme a las particularidades que plantean un desafío en la ciberseguridad.



Este documento analiza conjuntamente la forma de funcionamiento, la eficiencia en el uso de recursos, la heterogeneidad en los tipos de iniciativas financiadas, la democratización de la participación y toma de decisiones y la obtención de resultados de impacto positivo para el país y las múltiples partes interesadas que conforman o intervienen en el ciberespacio. En este sentido, los FDT estudiados en este documento poseen varios elementos que deben incorporarse en el diseño y la forma de funcionamiento de un fondo de promoción de iniciativas de ciberseguridad cuyo funcionamiento sea efectivo, eficiente, participativo y sostenido a través del tiempo. Sin embargo, siempre será necesario considerar los diversos desafíos y particularidades inherentes a la ciberseguridad y realizar las adecuaciones pertinentes para el contexto local en el que se pretenda crear un fondo de promoción con esas características.

07 RECOMENDACIONES

- **Identificar** el fundamento conceptual que justifique la creación de un fondo de promoción de iniciativas de ciberseguridad y su mecanismo de financiamiento.
- **Adoptar** el modelo de gobernanza multisectorial para la deliberación y toma de decisiones desde una perspectiva multidisciplinaria y participativa.
- **Promover** el financiamiento de proyectos de naturaleza variada y heterogénea mediante la creación de subcategorías de concursos que describan de forma detallada, objetiva y transparente el tipo de iniciativas a financiar.
- **Utilizar** inicialmente fondos públicos como mecanismo de financiamiento de iniciativas para inyectar recursos a la política pública.
- **Adoptar** metodologías cualitativas que permitan evaluar el impacto de iniciativas de capacitación, campañas de concientización y otras iniciativas para la redacción de criterios de asignación de recursos y evaluación objetiva de las iniciativas.
- **Identificar** las necesidades de financiamiento de los distintos actores del ecosistema de la ciberseguridad de la región, con un énfasis en aquellos actores que pertenecen o representan a grupos vulnerables.
- **Mapear** las alternativas disponibles actualmente para los actores del ecosistema de la ciberseguridad en la región en el momento de buscar financiamiento para sus proyectos en esta materia.
- **Construir** una metodología cualitativa para evaluar el impacto de la implementación de medidas de ciberseguridad a través de mecanismos objetivos y transparentes.

08 REFERENCIAS

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

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. Disponible en: https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds

Legislación, reglamentos y documentos públicos

Brasil

Decreto nº 3.737, de 30 de enero de 2001 http://www.planalto.gov.br/ccivil_03/decreto/2001/D3737.htm

Decreto nº 8.943, de 27 de diciembre de 2016. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8943.htm

Ley nº 10.052, de 28 de noviembre de 2000. http://www.planalto.gov.br/ccivil_03/LEIS/L10052.htm

Chile

Ley 20.522. Disponible en: https://www.leychile.cl/Navegar?idNorma=1027475&buscar=20522

Ley 18.168. Disponible en: https://www.leychile.cl/Navegar?idNorma=29591

Reglamento del Fondo de Desarrollo de las Telecomunicaciones contenido en el Decreto Supremo No 353 de 2001 del Ministerio de Transporte y Telecomunicaciones. Disponible en: https://www.leychile.cl/Navegar?idNorma=193117

Memoria Fondo de Desarrollo de las Telecomunicaciones 2017. Subtel. Disponible en: https://www.subtel.gob.cl/quienes-somos/divisiones-2/fondo-de-desarrollo-de-las-telecomunicaciones/memoria-fdt/

Colombia

Decreto 129 de 26 de enero de 1976 http://www.suin-juriscol.gov.co/viewDocument.asp?id=1028789

Decreto 1078 de 26 de mayo de 2015 https://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

Decreto 1414 de 25 de agosto de 2017 https://www.mintic.gov.co/portal/604/articles-57805_documento.pdf

Evaluación de los Programas del Plan Vive Digital para la Gente, Financiados con Recursos del Fondo de Tecnologías de la Información y Comunicaciones (FONTIC) (Dirección Nacional de Planeación) https://colaboracion.dnp.gov.co/CDT/Prensa/EstudioFONTIC.pdf

Informe de Gestión Año 2018 (MINTIC) https://www.mintic.gov.co/portal/604/articles-1785_informe_gestion_plan_accion_fontic_mintic_2018_v20190131.pdf

Ley 1341 de 30 de julio de 2009 https://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

Ley 1887 de 23 de abril de 2018 http://es.presidencia.gov.co/normativa/normativa/LEY%201887%20DEL%2023%20DE%20ABRIL%20DE%202018.pdf

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

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

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

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

Costa Rica

Costa Rica. Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). Estrategia Nacional de Ciberseguridad Costa Rica 2017. – San José, C. R.: MICITT, 2017.

Costa Rica. Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0, 2018-2022. Disponible en: https://www.micit.go.cr/documentos/micitt_estrategia_transformacion_digitaldel_bicentenario.pdf

Costa Rica. Ministerio de Ciencia, Tecnología y Telecomunicaciones (2015). Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021. Costa Rica: Una Sociedad Conectada. Disponible en: http://www.siteal.iipe.unesco.org/sites/default/files/sit_accion_files/siteal_costa_rica_5039.pdf

Ley General de Telecomunicaciones Nro. 8642. Disponible en: https://www.palermo.edu/cele/pdf/Regulaciones/CostaRica8642eyGraldeTelecomunicaciones(2008).pdf

Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones, Nº 8660/08. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=63786&nValor3=91177&strTipM=TC

Consideraciones para el diseño e implementación de un fondo de promoción DE LA CIBERSEGURIDAD

OEA | Más derechos para más gente