

Documento de Cooperación Técnica

I. Información Básica de la CT

▪ País/Región:	REGIONAL
▪ Nombre de la CT:	Generación de Conocimiento y Apoyo a Gobiernos en LAC en Ciberseguridad
▪ Número de CT:	RG-T3877
▪ Jefe de Equipo/Miembros:	Nowersztern, Ariel (IFD/ICS) Líder del Equipo; Paz Gonzalez, Santiago (IFD/ICS) Jefe Alternativo del Equipo de Proyecto; Cabral Berenfus, Florencia Alejandra (IFD/ICS); Libedinsky, Pablo (IFD/ICS); Pareja Glass, Alejandro (IFD/ICS); Rivera, Katia (IFD/ICS); Vasquez Rossi, Maria Ines (IFD/ICS); Vila Saint-Etienne, Sara (LEG/SGO); Wilks, Jason Malcolm (IFD/ICS)
▪ Taxonomía:	Investigación y Difusión
▪ Operación a la que la CT apoyará:	N/A
▪ Fecha de Autorización del Abstracto de CT:	17 May 2021.
▪ Beneficiario:	Regional
▪ Agencia Ejecutora y nombre de contacto:	Inter-American Development Bank
▪ Donantes que proveerán financiamiento:	Programa Estratégico para el Desarrollo de Instituciones(INS)
▪ Financiamiento solicitado del BID:	US\$200,000.00
▪ Contrapartida Local, si hay:	US\$0
▪ Periodo de Desembolso (incluye periodo de ejecución):	30 meses
▪ Fecha de inicio requerido:	Octubre 2021.
▪ Tipos de consultores:	Firmas y Consultores Individuales.
▪ Unidad de Preparación:	IFD/ICS-División de Innovación para Servir al Ciudadano
▪ Unidad Responsable de Desembolso:	IFD/ICS-División de Innovación para Servir al Ciudadano
▪ CT incluida en la Estrategia de País (s/n):	N/A
▪ CT incluida en CPD (s/n):	N/A
▪ Alineación a la Actualización de la Estrategia Institucional 2010-2020:	Productividad e innovación; Capacidad institucional y estado de derecho

II. Objetivos y Justificación de la CT

- 2.1 Las Tecnologías de la Información y la Comunicación (TIC) se han convertido en la base del funcionamiento eficiente de muchas áreas clave en los países de América Latina y el Caribe (ALC), desde el acceso a los servicios públicos hasta la generación y suministro de energía, distribución de agua e infraestructura de transporte, sólo por mencionar algunas áreas críticas. El ciberespacio, o el espacio en línea de las redes informáticas e Internet, se convirtió en un medio esencial en el que las personas, las empresas, los gobiernos y las máquinas se comunican entre sí y realizan transacciones. Este nuevo ecosistema también viene de la mano de nuevos tipos de riesgos, como el robo financiero cibernético, la interrupción de servicios, el robo de información, los ataques terroristas y espionaje cibernéticos. Estas amenazas sólo han aumentado en los últimos años. Un reciente informe de *McAfee* sobre el impacto económico de la ciberdelincuencia estimó que esta le cuesta a la economía mundial

alrededor de 600.000 millones de dólares anuales, o el 0,8% del PIB mundial¹. Los proveedores de servicios de Internet detectan 80 mil millones de escaneos maliciosos cada día, y las incidencias de ciberdelito crecen día a día. Muchas de estas amenazas cibernéticas se basan en buscar dispositivos y redes vulnerables en *internet*, lo que afecta particularmente al creciente número de usuarios en países en desarrollo con débiles medidas de seguridad en línea, quienes se ven constantemente expuestos a posibles ataques. Un informe de seguridad de 2017 de *Eset Latin America* demostró que el número de casos de *ransomware* en la región creció un 131% con respecto al año anterior². Según un informe de 2015 de la OEA y *Trend Micro*, los sectores más atacados en el ciberespacio fueron el gobierno, con el 51% de todos los ataques a organizaciones, y el sector energético, con el 47%. El estudio también mostró un aumento del 43% en los ataques a infraestructura crítica con respecto al año anterior, que se percibieron como cada vez más sofisticados³. Por otra parte, el Centro de Estudios Estratégicos e Internacionales (CSIS) registró que los ataques cibernéticos significativos a entidades gubernamentales se duplicaron entre 2018 y 2020⁴.

- 2.2 El creciente uso de las TIC en ALC es un catalizador del progreso económico y social; sin embargo, introduce riesgos de ciberseguridad inherentes que deben gestionarse de forma continua; de lo contrario, la seguridad ciudadana y la confianza del público en las TIC, incluida la fe del consumidor en las transacciones en línea y el acceso a los servicios públicos digitales pueden verse afectadas negativamente. En 2020, el informe “Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe”⁵ fue desarrollado y publicado por el BID en colaboración con la OEA, como actualización a los datos obtenidos en su primera edición en 2016. Este informe analizó el estado de preparación de 32 países de la región, con base en los indicadores de capacidad en ciberseguridad según el Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM) de la Universidad de Oxford. Este reporte constituye el primer estudio significativo del nivel de preparación de la región para enfrentar la creciente frecuencia y sofisticación de las amenazas cibernéticas y sus actores. Según las conclusiones del informe, la región se encuentra en general en un estado incipiente en términos de políticas y marcos nacionales de ciberseguridad. Dado que más de la mitad de los países de la región carecen de una estrategia nacional de seguridad cibernética, la ausencia de una visión clara de la seguridad cibernética a nivel nacional dificulta la participación de los países en el debate internacional sobre el ciberespacio, y en la formulación de normas internacionales. Además, los formuladores de políticas de la región en general carecen de una comprensión holística de la ciberseguridad, lo que puede llevar a una grave desconexión entre las políticas, los marcos legales y los problemas tecnológicos actuales. A pesar del estado incipiente notado en 2020 (analizando datos levantados en 2018 y 2019), el mismo representa un incremento del puntaje de madurez de todos los países estudiados por un promedio del 17%. Una medición actualizada y detallada del desarrollo realizado en los últimos años y de las deficiencias restantes alimentará la definición de estrategias concretas y viables para abordar las brechas significativas restantes.

¹ [The Economic Impact of Cybercrime—No Slowing Down, McAfee.](#)

² [ESET Security Report Latin America 2017.](#)

³ [Report on Cybersecurity and Critical Infrastructure in the Americas.](#)

⁴ [CSIS Significant Cyber Incidents Report.](#)

⁵ [Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe.](#)

- 2.3 Este proyecto pretende avanzar y profundizar los esfuerzos de los últimos años por generar conciencia y capacidad en ciberseguridad en el sector público, que se han enfocado en áreas como el diseño de Centros de Operaciones de Seguridad (SOC), la actualización y alineación de marcos normativos, estudios de madurez y mejores prácticas, acceso a conocimientos especializados, e intercambios de conocimiento regionales. También busca dar continuidad a estos esfuerzos, promover y reforzar los resultados alcanzados en los últimos años a través de la ejecución de los proyectos ATN/CF-15598-RG, “Mejora de la capacidad de los recursos humanos en ciberseguridad”, iniciado en 2016, y ATN/FG-16633-RG, “Fortalecimiento de la Ciberseguridad en América Latina y el Caribe”, iniciado en 2017. Algunas lecciones aprendidas de su ejecución incluyen la importante brecha en el nivel de preparación en ciberseguridad de los países de la región, según demostraron estudios de madurez llevados a cabo en el marco de estos proyectos, así como el interés creciente de los clientes en reforzar su ciberseguridad, manifestado a través de su amplio interés en el material generado y en el apoyo del Banco para cerrar estas brechas.
- 2.4 Como resultado de estos esfuerzos, el Banco ha visto un aumento significativo en la demanda de los países miembros del BID de apoyo técnico y operativo en ciberseguridad. Se espera que esta demanda continúe creciendo en los próximos años, como resultado de la mayor conciencia de los países sobre la importancia de proteger su ciberespacio, a nivel nacional y sectorial. El presente proyecto pretende dar respuesta a tales demandas y profundizar el apoyo brindado a los países en esta temática.
- 2.5 El **objetivo** de esta CT es generar conocimiento sobre el estado de las políticas nacionales y sectoriales de ciberseguridad en ALC y su aplicación en la práctica, así como realizar intervenciones piloto atendiendo brechas relevadas. Los organismos rectores nacionales y sectoriales de ciberseguridad de ALC accederán a las mejores prácticas para madurar sus estados específicos de política, gobernanza e iniciativas de ciberseguridad.
- 2.6 **Alineación Estratégica.** Esta propuesta está alineada con la Actualización de la Estrategia Institucional 2020-2023 (AB-3190-2), y se alinea estratégicamente con los desafíos de desarrollo de: (i) Productividad e Innovación, ya que promoverá la adopción de tecnología y la innovación en la región, a través del fortalecimiento de la seguridad en su ciberespacio, en contexto del esfuerzo transversal del fortalecimiento de la Capacidad Institucional; y (ii) Capacidad Institucional y Estado de Derecho, ya que contribuirá a fortalecer los instrumentos tecnológicos y de gestión y elevar los niveles de eficiencia y efectividad del sector público para la entrega de servicios, priorizando los temas de ciberseguridad. Asimismo, la CT se encuentra alineada con los resultados esperados del Programa Estratégico para el Desarrollo de Instituciones Financiado con Capital Ordinario (GN-2819-1), en particular con la prioridad de aprovechar las oportunidades de la economía digital, mediante el fortalecimiento de las capacidades en áreas que incluyen el desarrollo, uso y adopción de tecnologías digitales por parte de los gobiernos, las empresas y los ciudadanos. Finalmente, este proyecto se alinea con el Marco de Resultados Corporativos 2020-2023 (GN-2727-12), a través del eje de respaldo a la capacidad institucional y el Estado de derecho. Finalmente, este programa está alineado con el área prioritaria de Economía Digital de la “Visión 2025: Reinvertir en las Américas: Una década de oportunidades” del Banco, pues los datos y capacidades que se generen ayudarán a lograr una recuperación económica sostenible e incluyente, a promover más y mejores empleos

en un área de enorme potencial económico y creciente demanda de profesionales y servicios como es la ciberseguridad.

III. Descripción de las actividades/componentes y presupuesto

- 3.1 **Componente 1: Generación de conocimiento en ciberseguridad.** Este componente estará orientado a cubrir las brechas de conocimiento sobre el estado de la ciberseguridad en ALC, a fin de contribuir al diseño de políticas e iniciativas para su fortalecimiento. Para alcanzar este objetivo, se llevarán adelante las siguientes actividades:
- 3.1.1 **Generación de estudios regionales y sectoriales.** Se desarrollarán estudios, análisis, recomendaciones, casos de estudio, mejores prácticas, herramientas de evaluación y/o metodologías, a fin de capturar el nivel de desarrollo y fortalecer el conocimiento en ciberseguridad de todos los países de la región⁶. Estos productos incluirán estudios de madurez en ciberseguridad nacional, que evalúen aspectos clave como políticas, legislación, tecnologías, educación y concientización social. Los estudios sectoriales se enfocarán en diversas áreas que podrán incluir salud, educación, seguridad ciudadana, transporte, energía, finanzas, e innovación, entre otros. Esta actividad incluirá la recolección y validación de datos, así como la edición, traducción, diseño y publicación de los productos.
- 3.1.2 **Elaboración de observatorios de ciberseguridad.** Esta actividad incluirá la generación y facilitación de compendios de los datos y conclusiones obtenidos a través del desarrollo de productos de conocimiento en el marco de la agenda de ciberseguridad. Esta actividad incluirá la actualización y mantenimiento de un Observatorio Regional de madurez en ciberseguridad de carácter público, el cual reflejará el estado de madurez en ciberseguridad de todos los países beneficiarios del Banco.
- 3.1.3 **Campañas de difusión y promoción.** Mediante esta actividad, se financiará el diseño e implementación de material y campañas de difusión y promoción de los productos de conocimiento desarrollados durante la ejecución de las actividades de esta CT y otros proyectos en el marco de la agenda de ciberseguridad. Esta actividad incluirá la disseminación de los productos y resultados de esta CT a través de sitios *web*, medios sociales, eventos, blogs y otros canales de comunicación (tales como el blog Gobernarte y página web del Clúster de Datos y Gobierno Digital⁷ de IFD/ICS), a fin de darlos a conocer en los países beneficiarios.
- 3.1.4 **Consultorías para la gestión de los productos de conocimiento.** Se financiarán consultorías para la gestión de las actividades asociadas al desarrollo y difusión de los productos de conocimiento en ciberseguridad. Estas consultorías contribuirán a la generación, revisión, publicación y actualización de los productos, desarrollo de documentación y materiales relevantes, y coordinación de

⁶ Se prevé adjudicar la consultoría para la actualización de los datos regionales de madurez en ciberseguridad a la Organización de los Estados Americanos (OEA), organización con la que se ha colaborado en la elaboración de las previas ediciones este estudio (2016 y 2020).

⁷ <https://www.iadb.org/en/reform-modernization-state/data-and-digital-government-cluster>

actividades relacionadas, tales como procesos de publicación, difusión y organización de reuniones y talleres, entre otras.

3.2 Componente 2: Intervenciones piloto con gobiernos y sectores de ALC en ciberseguridad.

3.2.1 **Consultorías para el diseño e implementación de proyectos de apoyo técnico.** Se diseñarán intervenciones piloto de apoyo técnico en el ámbito de ciberseguridad, atendiendo necesidades identificadas durante el transcurso del programa mediante el conocimiento generado. Estos proyectos incluirán la contratación de consultores individuales para ofrecer servicios de diagnóstico, orientación técnica y recomendaciones a los clientes. También se ofrecerán consultorías de firmas para servicios técnicos, tales como apoyo en la respuesta a incidentes cibernéticos, campañas de detección de vulnerabilidades, *ethical hacking*, mediciones, recomendaciones, y otras actividades orientadas a fortalecer la ciberseguridad de sus activos⁸. Estas actividades se definirán en consonancia con las necesidades regionales y considerarán los niveles de madurez y vulnerabilidad de los beneficiarios a los riesgos de seguridad cibernética, así como el potencial de impacto y desarrollo futuro. Las intervenciones específicas se autorizarán por cartas de no objeción emitidas por sus beneficiarios inmediatos.

3.3 **Presupuesto indicativo.** El presupuesto total de la CT es de US\$200,000, cuya fuente será el Programa Estratégico para el Desarrollo de Instituciones (INS), y que se distribuirá de la siguiente manera:

Presupuesto Indicativo

(En US\$)

Actividad / Componente	BID/INS	Financiamiento Total
Componente 1: Generación de conocimiento en ciberseguridad	150.000	150.000
Componente 2: Intervenciones piloto con gobiernos y sectores de ALC en ciberseguridad.	50.000	50.000
Total US\$	200.000	200.000

IV. Agencia Ejecutora y estructura de ejecución

4.1 Considerando que el Banco ha emprendido múltiples esfuerzos para apoyar la seguridad cibernética en la región, y acumulado con ello una valiosa experiencia, este proyecto será ejecutado directamente por el Banco (de acuerdo con lo establecido en la sección 1.1 del Anexo II de la OP-619-4) a través de la División de Innovación para Servir al Ciudadano (IFD/ICS). El jefe de proyecto será responsable de la gestión y monitoreo de las actividades, presupuesto y contrataciones que se realicen en el marco de esta CT. Se asegurará también la coordinación con las Oficinas de Países que involucren las actividades de la CT. Es importante que el conocimiento generado a partir de la ejecución de este proyecto sea gestionado de cerca por los especialistas, y que tanto ellos como las autoridades de ciberseguridad de los países prestatarios

⁸ Se prevé la identificación de firmas consultoras idóneas para llevar adelante cada instancia de apoyo, las cuales deberán poseer experiencia directamente relevante a la naturaleza específica de dichas intervenciones.

del Banco se beneficien del mismo. Esto facilitará no sólo el diseño de las iniciativas futuras, sino también la identificación de socios potenciales, tanto entre los organismos multilaterales y las agencias nacionales especializadas como entre las numerosas empresas TIC con las que el Banco tiene relación de trabajo ejecutora están involucradas en el proyecto, también se deberá proporcionar información sobre su existencia y representación legal. Asimismo, en el contexto de la ejecución de las actividades, el equipo de proyecto mantendrá la debida coordinación con las Representaciones de los países involucrados.

- 4.2 Está prevista la contratación de consultores individuales, firmas consultoras y otros servicios de acuerdo con las políticas y procedimientos actuales de adquisición del Banco. Específicamente, la Sección AM-650 del Manual Administrativo “Fuerza Laboral Complementaria” se aplicará en el caso de consultores individuales, la Política para la Selección y Contratación de Empresas de Consultoría para Trabajo Operativo ejecutado por el Banco (GN-2765-4) y su Operativo Directrices (OP-1155-4) para contratar servicios de consultoría de naturaleza intelectual y la Política de Adquisiciones Corporativas (GN-2303-28) para otros servicios. Todos los productos de conocimiento derivados de esta Cooperación Técnica serán propiedad intelectual del Banco. Los beneficiarios de los componentes y actividades de este proyecto serán seleccionados para incluir los múltiples sectores que el Banco está apoyando en la región, una variedad de países que conforman los diferentes Departamentos de Países, y diferentes instituciones del sector público en la región, con la intención de maximizar equitativamente el impacto de las intervenciones. Asimismo, al momento de definir las instituciones beneficiarias, se tomará en consideración su nivel de madurez, de manera de favorecer a aquellas en estado de desarrollo más incipiente, así como el potencial de impacto significativo, efectivo y eficiente, en relación también a las sinergias que existan con otras operaciones del Banco y otros tipos de asistencia técnica.

V. Riesgos importantes

- 5.1 En algunos países, la debilidad institucional y la fragmentación plantean un desafío para la estabilidad de las iniciativas de seguridad cibernética, incluyendo la retención de los recursos humanos. Este riesgo será mitigado mediante un énfasis en la prestación de asesoramiento en la definición de la arquitectura institucional adecuada para administrar un programa de seguridad cibernética estable. Esta medida servirá también para mitigar el riesgo a la sostenibilidad de las iniciativas derivada de los cambios en el escenario político de los países de la región. Asimismo, estos esfuerzos se verán sustentados por la relación existente que el equipo de ejecución del proyecto ha desarrollado y fortalecido en los últimos años con diferentes organismos gubernamentales de la región, a los cuales se ha prestado diferentes formas de apoyo, y en particular con sus autoridades responsables de la gestión de su ciberseguridad. En este sentido, se proyecta que las actividades de esta CT impulsen y soporten el diseño de políticas públicas adecuadas en el área de ciberseguridad en la región; por ejemplo, a través del conocimiento generado en el marco del Componente 1, trabajo que dará continuidad a los resultados alcanzados con la publicación de los reportes regionales de madurez en ciberseguridad publicados en 2016 y 2020, antes descritos. Adicionalmente, se buscará incrementar la sostenibilidad, efectividad y eficiencia de estas intervenciones a través de las alianzas con otros actores y posibles sinergias con la creciente cartera de operaciones del Banco con componentes o actividades relacionadas al fortalecimiento de la ciberseguridad en la región.

- 5.2 Por otro lado, se reconoce que, a pesar de los avances que ha visto la región en los últimos meses, la crisis del COVID-19 podría afectar la implementación de las actividades de la CT; por ejemplo, en el proceso de recopilación de datos para la generación de los productos de conocimiento enmarcados en este proyecto. Como medida de mitigación, se enfatizará el uso de herramientas digitales para este tipo de actividades, y se aprovecharán las oportunidades de implementar el apoyo técnico a los clientes de manera remota. Debido a la naturaleza digital de las actividades del proyecto, se espera que estos mecanismos no representen dificultades mayores en su ejecución.

VI. Excepciones a las políticas del Banco

- 6.1 No hay excepciones a la política del Banco.

VII. Salvaguardias Ambientales

- 7.1 Dadas las características del proyecto no se esperan riesgos ambientales ni sociales negativos, por lo que la clasificación de esta operación de acuerdo a la Política de Medio Ambiente y Cumplimiento de Salvaguardias (OP-703) es “C” (Ver clasificación de ESG). The Safeguard Policy Filter ([SPF](#)) y The Safeguard Screening Form ([SSF](#)).

Anexos Requeridos:

[Matriz de Resultados - RG-T3877](#)

[Términos de Referencia - RG-T3877](#)

[Plan de Adquisiciones - RG-T3877](#)