

## ABSTRACTO DE COOPERACIÓN TÉCNICA

### I. Información Básica del Proyecto

|   |   |
|---|---|
| ▪ País/Región:  | REGIONAL/BID  |
| ▪ 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; LIBEDINSKY, PABLO (IFD/ICS); CABRAL BERENFUS, FLORENCIA ALEJANDRA (IFD/ICS); VILA SAINT-ETIENNE, SARA (LEG/SGO); RIVERA, KATIA (IFD/ICS) |
| ▪ Taxonomía:  | Investigación y Difusión  |
| ▪ Número y nombre de la operación que apoyará la CT:                      | N/A   |
| ▪ Fecha del Abstracto de CT:  | 17 May 2021   |
| ▪ Beneficiario:   | Todos los países prestatarios del Banco.  |
| ▪ Agencia Ejecutora:  | INTER-AMERICAN DEVELOPMENT BANK   |
| ▪ Financiamiento solicitado del BID:                                      | US\$200,000.00  |
| ▪ Contrapartida Local:  | US\$0.00  |
| ▪ Periodo de Desembolso:  | 36 meses  |
| ▪ Tipos de consultores:   | Individuos; Empresas  |
| ▪ Unidad Responsable 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):                             | No  |
| ▪ CT incluida en CPD (s/n):   | No  |
| ▪ 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 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 las mejores prácticas para madurar sus estados específicos de política, gobernanza e iniciativas de ciberseguridad.
- 2.2 El contexto regional es de baja madurez de las capacidades en ciberseguridad de los países de ALC. Según los reportes regionales de madurez publicados por el Banco y la OEA en 2016 y 2020, en puntaje promedio en los indicadores de madurez de los países miembros era 1.74 y 2.03 respectivamente, en una escala de 1 (menor madurez) a 5 (mayor madurez). Junto con la creciente digitalización de los gobiernos y sociedades, en distintos países el cibercrimen suele ser uno de los crímenes de mayor victimización reportada, mientras sus costos pueden llegar a 1% del PIB según estimaciones en países avanzados. En este contexto, el Banco atiende los costos económicos y sociales de este fenómeno enfocando en dos aspectos: Apoyando los países miembros en mejorar sus políticas y capacidades en ciberseguridad; y mitigando riesgos cibernéticos en proyectos de inversión con elementos digitales sensibles. En los últimos años se han dedicado esfuerzos significativos para apoyar ambos aspectos de la ciberseguridad mediante operaciones de préstamo como mediante la generación y difusión de

conocimiento, pero la respuesta sigue siendo menor de las necesidades. Un estudio interno de las operaciones de inversión del Banco ha identificado referencia a ciberseguridad en 18% de las operaciones estudiadas, mientras un total de 64% de las mismas podía ser beneficiado de intervenciones de ciberseguridad. Estos datos muestran la creciente importancia del tema en la agenda operativa del Banco, y el potencial futuro de creciente atención.

### III. Descripción de las Actividades y Resultados

- 3.1 **Componente I: 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.
- 3.2 **Componente II: Componente 2: Intervenciones piloto con gobiernos y sectores de ALC en ciberseguridad.** Se diseñarán intervenciones piloto de apoyo técnico en el ámbito de ciberseguridad, atendiendo necesidades identificadas durante el transcurso del programa mediante el conocimiento generado.

### IV. Presupuesto

Presupuesto Indicativo

| Actividad/Componente   | BID/Financiamiento por Fondo | Financiamiento Total  |
|--|------------------------------|-----------------------|
| Componente 1: Generación de conocimiento en ciberseguridad.                            | US\$150,000.00               | US\$150,000.00        |
| Componente 2: Intervenciones piloto con gobiernos y sectores de ALC en ciberseguridad. | US\$50,000.00                | US\$50,000.00         |
| <b>Total</b>   | <b>US\$200,000.00</b>        | <b>US\$200,000.00</b> |

### V. Agencia Ejecutora y Estructura de Ejecución

- 5.1 Esta CT será ejecutada por el Banco. El equipo del proyecto está dirigido por la División de Innovaciones para Servir al Ciudadano de la Gerencia de Instituciones para el Desarrollo del Banco (IFD/ICS).
- 5.2 Dada la falta de identificación de una institución regional con la experiencia y capacidad legal para ejecutar este proyecto, y 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 a través de la División de Innovación para Servir al Ciudadano (IFD/ICS). 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 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.

### VI. Riesgos Importantes

- 6.1 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.

### VII. Salvaguardias Ambientales

7.1 La clasificación ESG para esta operación es "indefinida".