

TC ABSTRACT

I. Basic Project Data

▪ Country/Region:	REGIONAL/IDB
▪ TC Name:	Strengthening of Cybersecurity in Latin America and the Caribbean
▪ TC Number:	RG-T3024
▪ Team Leader/Members:	PORRUA VIGON, MIGUEL ANGEL (IFD/ICS) Team Leader; BOUSKELA, MAURICIO SIMON (CSD/HUD); MAHFOUZ, GIOVANNA L. (IDB); MUENTE KUNIGAMI, ARTURO (IFD/ICS); ROS, LUIZ; HENNIG, BETINA TIRELLI (LEG/LEG); CABRAL BERENFUS, FLORENCIA ALEJANDRA (IFD/ICS); KAGELMACHER, DARIO GUILLERMO (IFD/ICS)
▪ Taxonomy:	Research and Dissemination
▪ Number and name of operation supported by the TC:	N/A
▪ Date of TC Abstract:	11 Apr 2017
▪ Beneficiary:	Países miembros del BID
▪ Executing Agency:	INTER-AMERICAN DEVELOPMENT BANK
▪ IDB funding requested:	\$ 500,000.00
▪ Local counterpart funding:	\$ 0.00
▪ Disbursement period:	30 months
▪ Types of consultants:	Individuals; Firms
▪ Prepared by Unit:	Innovation in Citizen Services Division
▪ Unit of Disbursement Responsibility:	Institutions for Development
▪ TC included in Country Strategy (y/n):	No
▪ TC included in CPD (y/n):	No
▪ Alignment to the Update to the Institutional Strategy 2010-2020:	Institutional capacity and rule of law

II. Objective and Justification

- 2.1 The objective of this project is to improve security in the cyberspace in Latin America and the Caribbean, by making use of the knowledge and experience of those countries most advanced in this domain.
- 2.2 Más del 50 por ciento de la población de América Latina y el Caribe tiene acceso a Internet, cerca de 350 millones de ciudadanos. Esta importante población de Internet crece a un ritmo del 12% anual, el más rápido en el mundo. Además, las TIC se han convertido en la base del funcionamiento eficiente de varias áreas clave de la economía de estos países, y sin las políticas de seguridad cibernética apropiadas esta fuente de actividad económica puede ser anulada por los delitos informáticos.
- 2.3 Un reciente informe del Centro de Estudios Estratégicos e Internacionales estima que la ciberdelincuencia cuesta anualmente un 0.5 por ciento del PIB mundial, alrededor de US\$500 billones. De acuerdo a cifras del Informe Ciberseguridad 2016, recientemente publicado por el BID y la OEA, el 80 por ciento de los países de ALC no cuentan con una estrategia nacional de seguridad cibernética, ni un plan para proteger su infraestructura crítica nacional. Al ser consultados respecto a su percepción del grado de preparación para gestionar y responder a incidentes en el ciberespacio, sólo 2 de los 32 países parte del estudio respondieron que estaban "preparados".

- 2.4 Adicionalmente, ALC enfrenta una carencia estructural de capital humano en el área TIC. Si bien AL produce 123,000 ingenieros por año, necesitaría incrementar este número en aproximadamente 40 por ciento anual para poder responder a las necesidades de capital humano que derivan del desarrollo económico actual. Esto implica también que la mayoría los países no cuenta con los recursos humanos calificados necesarios para hacer frente a estas amenazas que crecen en número y sofisticación. Un estudio realizado por Trend Micro en 20 países de ALC concluye que con el fin de proteger a los países de ALC en contra de los ataques cibernéticos es necesario incrementar los presupuestos, construir las capacidades necesarias y compartir más información.
- 2.5 España es considerado como uno de los países líderes en ciberseguridad a nivel global. De acuerdo a cifras para el 2014 del ONTSI, España cuenta con 533 empresas especializadas en este subsector, las cuales dan empleo a 5.808 personas y durante ese año facturaron casi 600 millones de euros. España cuenta también con una moderna Estrategia Nacional de Seguridad Cibernética (2013) que establece objetivos y líneas específicas de acción, compatibilizando estos esfuerzos con el Plan de Seguridad Nacional y una sólida arquitectura institucional, en la que destaca el Instituto Nacional de Ciberseguridad (INCIBE). Dado el reconocimiento de España en esta materia y la cercanía cultural y lingüística de este país a América Latina, el trabajo de intercambio de experiencias y conocimiento que el Banco viene apoyando se verá enormemente potenciado.
- 2.6 Durante los últimos dos años, el Banco ha contribuido a los esfuerzos de los países de ALC por mejorar su seguridad cibernética, documentando el estado de la misma a través del Informe sobre Ciberseguridad 2016, así como mediante la organización del taller regional de responsables de políticas de ciberseguridad, en colaboración con la OEA. Fruto de este trabajo inicial han surgido demandas de apoyo técnico y financiero en ciberseguridad que han generado componentes específicos sobre el tema en algunas operaciones. El conocimiento y la red desarrollados a partir de este trabajo serán de gran valor para la implementación exitosa de esta cooperación técnica.

III. Description of Activities and Outputs

- 3.1 Componente 1. Definición de la oferta y la demanda de conocimiento en ciberseguridad, con el fin de cubrir los gaps de conocimiento de los gobiernos de ALC y contribuir al diseño de políticas e iniciativas de Ciberseguridad en ALC, a partir de:
- 3.2 Realización de un estudio acerca de las debilidades de conocimiento que impiden el avance de las políticas de ciberseguridad en ALC. Mediante la combinación de encuestas en línea con entrevistas presenciales, se llevará a cabo una investigación que permita identificar las carencias de conocimiento y las necesidades de apoyo técnico para cada uno de los países de la región. Realización de una misión de identificación de la oferta española de conocimiento en ciberseguridad. La misión estará integrada por los responsables de ciberseguridad de 8 países de la región (2 por cada subregión de trabajo del BID, con el fin analizar la experiencia española en ciberseguridad y elaborar un documento acerca de la oferta de conocimiento que pueda ser compartido con el resto de países de ALC.
- 3.3 Componente 2. Formación de Recursos Humanos en Seguridad Cibernética para apoyar a la construcción de una base de recursos humanos altamente cualificada, a partir de:
- 3.4 Elaboración de un programa base de formación en ciberseguridad que pueda ser utilizado por escuelas nacionales de administración pública, institutos técnicos o centros académicos de ALC. Taller de presentación del programa de formación en ciberseguridad a instituciones de formación de la región, al que se invitará al sector privado a que se sume al esfuerzo.

Entrenamiento en la gestión de un ataque cibernético a partir de un ejercicio de simulación a realizar en las instalaciones del INCIBE.

- 3.5 Componente 3. Asistencia Técnica en Seguridad Cibernética para apoyar el avance de la ciberseguridad en la región.
- 3.6 Realización de consultorías para el diseño e implementación de proyectos concretos en el ámbito de seguridad cibernética, bajo alguna de las cinco dimensiones antes mencionadas a cuatro países de la ALC, uno de cada región operativa del Banco. Entre los proyectos se priorizarán los que apoyen la implantación de programas de formación en ciberseguridad en la región.
- 3.7 **Component I: Definición de la oferta y la demanda de conocimiento en ciberseguridad.** Cubrir los gaps de conocimiento de los gobiernos de ALC y contribuir al diseño de políticas e iniciativas de Ciberseguridad en ALC
- 3.8 **Component II: Formación de Recursos Humanos en Seguridad Cibernética .** Apoyar a la construcción de una base de recursos humanos altamente calificada
- 3.9 **Component III: Asistencia Técnica en Seguridad Cibernética .** Apoyar el avance de la ciberseguridad en la región

IV. Budget

Indicative Budget

Activity/Component	IDB/Fund Funding	Counterpart Funding	Total Funding
Definición de la oferta y la demanda de conocimiento en ciberseguridad	\$ 85,000.00	\$ 0.00	\$ 85,000.00
Formación de Recursos Humanos en Seguridad Cibernética	\$ 215,000.00	\$ 0.00	\$ 215,000.00
Asistencia Técnica en Seguridad Cibernética	\$ 200,000.00	\$ 0.00	\$ 200,000.00

V. Executing Agency and Execution Structure

- 5.1 Dado 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 varios esfuerzos para apoyar la seguridad cibernética en la región acumulando con ello una valiosa experiencia, este proyecto será ejecutado directamente por el Banco a través de la División de Capacidad Institucional del Estado (IFD/ICS).
- 5.2 Contemplando que el Banco ha lanzado recientemente sus esfuerzos para apoyar la seguridad cibernética en LAC es importante que el conocimiento generado a partir de la ejecución de este proyecto sea vigilado 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. Project Risks and Issues

- 6.1 En algunos países, la debilidad institucional y la fragmentación plantea un desafío para la estabilidad de las iniciativas de seguridad cibernética, incluyendo la retención de los recursos humanos. Este riesgo será mitigado mediante la colocación de un

énfasis en la prestación de asesoramiento en la definición de la arquitectura institucional adecuado para administrar un programa de seguridad cibernética estable.

VII. Environmental and Social Classification

7.1 The ESG classification for this operation is "undefined".