Documento de Cooperación Técnica

I. Información Básica de la CT

▪ País/Región:	Regional
▪ Nombre de la CT:	Fortalecimiento de la Ciberseguridad en América Latina y el Caribe
▪ Número de CT:	RG-T3024
▪ Jefe de Equipo/Miembros:	Miguel Porrúa, Jefe de Equipo (IFD/ICS); Mauricio Bouskela (CSD/HUD); Arturo Muente, Florencia Cabral, Giovanna Mahfouz (IFD/ICS); Luiz Ros (PCY/DEI); y Betina Hennig (LEG/SGO)
▪ Indicar si es: Apoyo Operativo, Apoyo al Cliente, o Investigación y Difusión	Investigación y difusión
▪ Fecha de Autorización del Abstracto de CT:	28 de setiembre de 2017
▪ Beneficiario:	Países miembros del BID en América Latina y el Caribe[1]
▪ Agencia Ejecutora y nombre de contacto	Banco Interamericano de Desarrollo, a través de IFD/ICS
▪ Donantes que proveerán financiamiento:	Fondo General de Cooperación de España (FGE)
▪ Financiamiento Solicitado del BID:	US$500,000
▪ Contrapartida Local:	N/A
▪ Periodo de Desembolso:	24 meses
▪ Fecha de Inicio requerido:	Marzo 2018
▪ Tipos de consultores:	Firma Consultora y Consultores individuales
▪ Unidad de Preparación:	IFD/ICS
▪ Unidad Responsable de Desembolso:	IFD/IFD
▪ CT incluida en la Estrategia de País:	No
▪ CT incluída en CPD:	No
▪ Alineación a la Actualización de la Estrategia Institucional 2010-2020:	Instituciones para el crecimiento y el bienestar social[2]

II. Objetivos y Justificación de la CT

2.1 Más del 50% de la población de América Latina y el Caribe (ALC) tiene acceso a Internet, cerca de 350 millones de ciudadanos. Esta importante población de Internet crece a un ritmo del 12 por ciento anual, el más rápido de cualquier región en el

[1] Previo a la realización de cualquier actividad en un país beneficiario, se obtendrá la nota de no-objeción correspondiente de parte del órgano enlace con el Banco.

[2] La Estrategia Sectorial sobre las Instituciones para el Crecimiento y el Bienestar Social identifica el mejoramiento de la innovación y la productividad como áreas prioritarias donde el Banco puede ayudar a la región a superar los desafíos que obstaculizan el crecimiento y el bienestar social. Con este fin, el BID apoya el fortalecimiento de las instituciones, y ha reconocido específicamente la necesidad de mejorar las políticas y la acción gubernamental en el sector de las tecnologías de la información y la comunicación (TIC) (5.1 de la Estrategia Sectorial previamente referida). También se ha identificado como un área prioritaria que contribuye a los objetivos del noveno aumento de capital del Banco, GCI-9.

mundo. Los dispositivos se están conectando incluso a mayor ritmo que las personas a internet, más de 8 billones de "cosas" estarán conectadas a internet a finales de 2017[3]. Además, las TIC se han convertido en la base del funcionamiento eficiente de áreas clave de la economía de estos países, por lo que, sin las políticas de seguridad cibernética adecuadas, estos sectores corren el riesgo de verse desestabilizados por ataques cibernéticos.

2.2 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$500 billones de US$. De acuerdo a cifras del *Informe Ciberseguridad 2016: ¿Estamos preparados en América Latina y el Caribe?*[4], 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 incluidos en el estudio respondieron que estaban "preparados".

2.3 Adicionalmente, ALC enfrenta una carencia estructural de capital humano en el área TIC. Si bien América Latina (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.[5] Esto implica también que la mayoría de 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 contra los ataques cibernéticos es necesario incrementar los presupuestos, construir las capacidades necesarias y compartir más información.[6] El reporte *Global Information Security Workforce Study* (GISWS)[7], publicado por el *Center for Cybersafety and Education* a principios de 2017, estima que para 2022 Latinoamérica enfrentará una carencia de 185.000 profesionales de ciberseguridad para cubrir la creciente demanda. Asimismo, un 67% de los profesionales del área de ciberseguridad encuestados expresaron que actualmente no hay suficientes trabajadores en sus departamentos, y 35% atribuyó esta carencia a la dificultad de encontrar personal calificado en el área.

2.4 Estos datos demuestran claramente que la necesidad de capacidad profesional en ciberseguridad en Latinoamérica se agravará en los próximos años. Sin embargo, la oferta de programas universitarios de formación es muy escasa en la región. Universidades en Argentina, Colombia, México y Panamá[8] ya han instaurado programas de maestría en ciberseguridad, y diversos institutos de la región ofrecen certificaciones en áreas técnicas concretas tales como protección de bases de datos y *ethical hacking,* siguiendo planes de estudio y evaluación estándar en la industria.

---

3 https://www.gartner.com/newsroom/id/3598917.

4 Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? BID y OEA. Marzo 2016. https://publications.iadb.org/handle/11319/7449?locale-attribute=es&.

5 Katz, Raul. El Ecosistema y la Economía Digital en América Latina. 2015. 125-128.

6 Report on Cybersecurity and Critical Infrastructure in the Americas. Trend Micro y OEA. 2015. https://www.sites.oas.org/cyber/Certs_Web/OAS-Trend%20Micro%20Report%20on%20Cybersecurity%20and%20CIP%20in%20the%20Americas.pdf

7 https://iamcybersafe.org/wp-content/uploads/2017/06/LATAM-GISWS-Report.pdf.

8 Programas de educación en ciberseguridad a nivel de maestría que existen en Latinoamérica son ofrecidos por la Universidad de Buenos Aires (Argentina), Universidad de los Andes (Colombia), Universidad LaSalle (México), y Universidad Tecnológica de Panamá.

No obstante, sólo se ha encontrado oferta en 4 de 32 países y las cifras demuestran que la actual oferta educativa no alcanza a cubrir la necesidad regional de entrenamiento en ciberseguridad.

2.5 Durante los últimos cuatro 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 anual de talleres regionales de responsables de políticas de ciberseguridad, en colaboración con la OEA. En el pasado año, se han llevado a cabo capacitaciones internacionales a funcionarios de 10 países representando a las diferentes regiones de operación del Banco en LAC, con el fin de explorar las experiencias de los países más avanzados en la materia. Durante estas visitas, se ofreció exposición a las mejores prácticas en organización gubernamental, desarrollo de estrategias nacionales y de legislación relevante para combatir el cibercrimen, así como entrenamiento de funcionarios púbicos en la prevención y gestión de ataques cibernéticos.

2.6 España es considerado como uno de los países líderes en ciberseguridad a nivel global. De acuerdo a cifras para el 2014 del ONTSI (Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información), 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.[9] 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 destacan el Instituto Nacional de Ciberseguridad (INCIBE) y el Centro Criptológico Nacional. Con el fin de aprovechar la experiencia de España en la temática, el Banco ha facilitado la participación de 97 funcionarios públicos de Latinoamérica y el Caribe del curso "Cybersecurity Summer Boot Camp 2017"[10], organizado por el INCIBE en León, España, donde se ofreció capacitación especializada a través de 440 horas de talleres y 21 seminarios magistrales distribuidos a lo largo de dos semanas. 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.

2.7 Producto de esta exposición a la oferta de conocimiento internacional, el Banco ha recibido solicitudes de asesoría técnica y apoyo financiero en áreas específicas tales como desarrollo de estrategias nacionales, establecimiento de Centros de Operaciones de Ciberseguridad (SOC), centros regionales de capacitación, y protección de datos biométricos, por parte de 5 países de la región (Bahamas, Ecuador, República Dominicana, Paraguay y Uruguay). En otros casos, dichas solicitudes han generado componentes específicos en operaciones de préstamo[11]. A medida que el Banco continúa estimulando el desarrollo de estructuras y capacidades

---

9 Caracterización del subsector y el mercado de la ciberseguridad. ONTSI, Ministerio de Industria, Energía y Turismo, y el Instituto Nacional de Ciberseguridad (INCIBE). http://www.ontsi.red.es/ontsi/sites/default/files/ndp_caracterizacion_del_subsector_y_el_mercado_de_la_ciberseguridad_2015.pdf.

10 https://www.incibe.es/en/summer-bootcamp.

11 Programa Panamá En Línea: PN-L1114 (3683/OC-PN); Proyecto de Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y las Empresas a Nivel Nacional: PE-L1222 (4399/OC-PE).

en las instituciones públicas en materia de ciberseguridad, se espera que la demanda de talento en esta área continúe incrementándose. El conocimiento y las relaciones desarrolladas a partir de este trabajo serán de gran valor para la implementación exitosa de esta cooperación técnica.

2.8 El **objetivo** de este proyecto es mejorar la seguridad del ciberespacio en ALC aprovechando el conocimiento y la experiencia de países avanzados, especialmente España, en este sector.

III. Descripción de las actividades/componentes y presupuesto

3.1 Esta operación consistirá en tres componentes: (i) definición de la oferta y la demanda de conocimiento en ciberseguridad; (ii) formación de recursos humanos, y (iii) asistencia técnica.

3.2 **Componente 1. Definición de la oferta y la demanda de conocimiento en seguridad cibernética (US$76.600).** Este componente estará orientado a 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 las siguientes actividades:

1.1 Realizar 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. Entre otros aspectos, el estudio identificará los perfiles profesionales más demandados en el área de ciberseguridad y la oferta formativa necesaria para cubrir el déficit de profesionales en los próximos 5 años.

1.2 Realizar una misión de análisis de la oferta española de conocimiento en ciberseguridad. La misión tiene como propósito conocer la experiencia española en ciberseguridad y estará integrada por los responsables de ciberseguridad de 8 países de la región[12] (2 por cada región de trabajo del BID)..

1.3 Elaborar un documento acerca de la oferta de formación y conocimiento existente en España que pueda ser compartido con el resto de países de ALC. El documento presentará la oferta formativa de grado y posgrado en el sector académico español, así como actividades formativas relevantes ofrecidas por instituciones privadas. El documento incorporará un capítulo sobre publicaciones y metodologías de uso frecuente en España que puedan tener valor para los países de ALC.

3.3 **Componente 2. Formación de recursos humanos en seguridad cibernética (US$231.400).** Este componente apoyará la construcción de una base de recursos humanos altamente cualificada, a partir de las siguientes actividades:

2.1 **Elaborar un programa de formación en ciberseguridad** que pueda ser utilizado por instituciones académicas de ALC. Este programa estará basado tanto en la experiencia española como en las más reconocidas experiencias de América

[12] Los siguientes países han sido inicialmente identificados como potenciales receptores de apoyo dado el interés manifestado por los mismos: Paraguay, Brasil, Ecuador, Perú, Panamá, República Dominicana, Bahamas y Jamaica.

Latina, el Caribe y otros países que constituyan una referencia valiosa. Además de la estructura y los contenidos, incluirá una guía metodológica para su implantación en la currícula formativa de instituciones académicas de ALC.

2.2 **Realizar un taller de presentación del programa de formación en ciberseguridad** a instituciones de formación de la región, involucrando representantes del sector privado. Previo a la ejecución del taller, se contactará a empresas de diferentes sectores y países con el fin de que proveen input acerca de los perfiles profesionales necesarios y de que ayuden a dimensionar la demanda de los mismos. El taller reunirá también a los decanos de ingeniería de 50 instituciones académicas de la región[13], a quienes se invitará asimismo a que compartan sus experiencias formativas en ciberseguridad.

2.3 **Llevar a cabo un curso de capacitación en ciberseguridad** a ser impartido por el INCIBE en España. Entre otros aspectos, el curso incluirá entrenamiento en la gestión de ataques cibernéticos a partir de ejercicios de simulación que utilizarán tecnologías avanzadas de formación en el tema.[14]

2.4 **Realizar una competencia de *hackers*[15]** entre equipos de ALC y España que permita identificar potenciales profesionales de la ciberseguridad y generar una red de colaboración con la comunidad de *white hat hackers*[16]. Cada país interesado en tomar parte de la competencia será representado por un equipo.

3.4 **Componente 3. Asistencia técnica en seguridad cibernética (US$160.000).** Este componente apoyará el avance de la ciberseguridad en la región a través de las siguientes actividades:

3.1 **Realizar consultorías para el diseño e implementación de proyectos** concretos en el ámbito de seguridad cibernética, bajo alguna de las cinco dimensiones establecidas por el modelo de madurez de la capacidad de seguridad cibernética desarrollado por el *Global Cyber Security Capacity Centre* (Universidad de Oxford): política, sociedad, educación, legislación y tecnología. Cuatro países serán beneficiados de acuerdo a las necesidades identificadas, 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.

---

13 Para seleccionar las instituciones académicas participantes, se realizará un llamado a interés en el cuál se solicitará información acerca de sus actividades actuales de formación en el área TIC y sus planes futuros de incluir formación en ciberseguridad, con el fin de identificar aquellas con mayor capacidad para implementar un programa de formación en ciberseguridad.

14 Se seleccionará participantes para este curso con base en nominaciones directas de oficiales responsables del área de ciberseguridad en los gobiernos de la región. Los participantes seleccionados deberán estar en condición de aplicar el conocimiento a sus responsabilidades diarias y comprometerse a permanecer en su trabajo al menos un año.

15 El proyecto financiará los gastos logísticos, organizativos y los premios de la competencia.

16 Los *white hat hackers* son especialistas en seguridad cibernética que realizan pruebas de seguridad en sistemas informáticos con el fin de informar acerca de potenciales vulnerabilidades, antes de que estas sean explotadas por quienes realizan *hacking* para delinquir.

3.5 **Resultados esperados:** A continuación de detallas los resultados esperados:

- 8 instituciones académicas en ALC ofrecen estudios de postgrado en ciberseguridad;
- 1 estudio publicado sobre las debilidades de conocimiento en ciberseguridad en ALC;
- 8 responsables de ciberseguridad de países de la región informados acerca de la oferta de conocimiento de España;
- 1 documento informativo de la oferta española de formación y conocimiento en ciberseguridad elaborado;
- 1 programa de formación en ciberseguridad en base a experiencias avanzadas internacionales elaborado y difundido a 50 instituciones académicas de ALC;
- 32 funcionarios responsables de ciberseguridad capacitados;
- 1 comunidad de *white hat hackers* creada en ALC;
- 4 proyectos de apoyo técnico en diferentes países de ALC diseñados e implementados. Para mayor detalle sobre estos resultados y sus indicadores ver detalle en enlace.

IV. Presupuesto indicativo. El total de la CT es de US$500,000, que provendrán del Fondo General de Cooperación de España (FGE). En el cuadro de presupuesto indicativo a continuación, se distribuye de la siguiente manera:

Presupuesto indicativo (US$)

Actividad	Año 1	Año 2	Total US$
Componente 1. Definición de la oferta y la demanda de conocimiento en seguridad cibernética	76,600		76,600
Componente 2. Formación de recursos humanos en seguridad cibernética	88,000	143,400	231,400
Componente 3. Asistencia técnica en seguridad cibernética	80,000	80,000	160,000
Gestión y monitoreo del proyecto			32,000
Total			US$500,000

Para mayor detalle sobre Presupuesto ver enlace.

V. Agencia Ejecutora y estructura de ejecución

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). 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.

5.2 El Banco contratará los servicios de firma consultora y/o consultores individuales de conformidad con las políticas y procedimientos de adquisiciones vigentes en el Banco. Para la contratación de firmas consultoras se aplicarán las políticas de selección de consultores (GN-2765-1) y las guías operativas (OP-1155-4), para las contrataciones de consultores individuales las normas de recursos humanos (AM-650) y para los gastos relacionados a servicios distintos de consultoría, las políticas de adquisiciones corporativas (GN-2303-20).

VI. Riesgos importantes

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. Excepciones a las políticas del Banco

7.1 Ninguna.

VIII. Salvaguardias Ambientales

8.1 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:

ANEXO I: Matriz de Resultados
ANEXO II: Términos de Referencia
ANEXO III: Plan de Adquisiciones

FORTALECIMIENTO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE

RG-T3024

CERTIFICACIÓN

Por la presente certifico que esta operación fue aprobada para financiamiento por el **Fondo General de Cooperación de España (FGE)**, de conformidad con la comunicación de fecha 28 de septiembre de 2017 subscrita por Kai Hertz (ORP/GCM). Igualmente, certifico que existen recursos en el mencionado fondo, hasta la suma de **US$500.000** para financiar las actividades descritas y presupuestadas en este documento. La reserva de recursos representada por esta certificación es válida por un periodo de cuatro (4) meses calendario contados a partir de la fecha de elegibilidad del proyecto para financiamiento. Si el proyecto no fuese aprobado por el BID dentro de ese plazo, los fondos reservados se considerarán liberados de compromiso, requiriéndose la firma de una nueva certificación para que se renueve la reserva anterior. El compromiso y desembolso de los recursos correspondientes a esta certificación sólo debe ser efectuado por el Banco en dólares estadounidenses. Esta misma moneda será utilizada para estipular la remuneración y pagos a consultores, a excepción de los pagos a consultores locales que trabajen en su propio país, quienes recibirán su remuneración y pagos contratados en la moneda de ese país. No se podrá destinar ningún recurso del Fondo para cubrir sumas superiores al monto certificado para la implementación de esta operación. Montos superiores al certificado pueden originarse de compromisos estipulados en contratos que sean denominados en una moneda diferente a la moneda del Fondo, lo cual puede resultar en diferencias cambiarias de conversión de monedas sobre las cuales el Fondo no asume riesgo alguno.

Original Firmado — 01/09/18

Sonia M. Rivera — Fecha
Jefe
Unidad de Gestión de Donaciones y Cofinanciamiento
ORP/GCM

APROBADO: Original Firmado — 01/09/18

Carlos Santiso — Fecha
Jefe de División
División de Capacidad Institucional del Estado
IFD/ICS