

Documento de Cooperación Técnica

I. Información Básica de la CT

▪ País/Región:	REGIONAL
▪ Nombre de la CT:	Apoyo al cierre de brechas de las empresas en Latinoamérica en ciberseguridad
▪ Número de CT:	RG-T4255
▪ Jefe de Equipo/Miembros:	Solis Ahumada, Galileo Humberto (IFD/CTI) Líder del Equipo; Torrico Duran, Blanca Paola (IFD/CTI) Jefe Alterno del Equipo de Proyecto; Cathles, Alison Regan (IFD/CTI); Daniela Acevedo (LEG/SGO); Genesis Morales (IFD/CTI); María Alejandra Galeano (IFD/CTI); Nowersztern, Ariel (IFD/ICS); Vargas Cuevas, Fernando Esteban (IFD/CTI)
▪ Taxonomía:	Apoyo al Cliente
▪ Operación a la que la CT apoyará:	.
▪ Fecha de Autorización del Abstracto de CT:	No aplica
▪ Beneficiario:	Colombia, Costa Rica y Panamá
▪ Agencia Ejecutora y nombre de contacto:	Inter-American Development Bank
▪ Donantes que proveerán financiamiento:	OC SDP Ventanilla 2 - Instituciones(W2C)
▪ Financiamiento solicitado del BID:	US\$150,000.00
▪ Contrapartida Local, si hay:	US\$0
▪ Periodo de Desembolso (incluye periodo de ejecución):	24 meses
▪ Fecha de inicio requerido:	1 de junio 2023
▪ Tipos de consultores:	Firmas y consultores individuales
▪ Unidad de Preparación:	IFD/CTI-División de Competitividad, Tecnología e Innovación
▪ Unidad Responsable de Desembolso:	IFD/CTI-División de Competitividad, Tecnología e Innovación
▪ CT incluida en la Estrategia de País (s/n):	Si
▪ 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 Cooperación Técnica (CT) no reembolsable es apoyar a los países beneficiarios (Colombia, Costa Rica y Panamá) en la creación de políticas públicas para sensibilizar a las empresas en ciberseguridad a partir de la identificación de brechas, exploración de sectores/cadenas, identificación de problemas específicos, y diseño de programas de formación para empresas y particulares que permitan aumentar la oferta de personas con habilidades digitales avanzadas relevantes para la ciberseguridad. El resultado esperado es que las empresas fortalezcan sus capacidades de ciberseguridad para poder insertarse en clústeres y cadenas globales de valor (CGV).
- 2.2 Debido a la pandemia, las economías de la región sufrieron cierres y paralizaciones, interrumpiendo el flujo de actividades productivas y de consumo lo que se tradujo en contracciones en la oferta y la demanda. Esta sucesión de fricciones afectó la relación entre empresas y consumidores e interrumpió las CGV al suspender las transacciones

entre proveedores, productores y servicios relacionados. Las empresas se vieron obligadas a responder en múltiples frentes simultáneamente: mientras trabajaban para proteger la seguridad de sus empleados, también necesitaban salvaguardar su viabilidad operativa, cada vez bajo un estrés más significativo debido a un gran impacto en las CGV.

- 2.3 Las consecuencias de la interrupción de la CGV se han hecho evidentes por la pandemia y otros eventos globales, como la guerra en Ucrania, incluidos los atacantes cibernéticos. En efecto, los proveedores externos de una empresa pueden poner en riesgo toda la cadena de suministro. Gartner [informa](#) que en 2019 solo el 21% de los líderes de la cadena de suministro creen que su red de proveedores es "altamente resistente" a los ataques cibernéticos. Asimismo, de acuerdo a [una encuesta realizada por el grupo NCC](#) en 2022 a cerca de 1.400 tomadores de decisiones de seguridad cibernética en 12 economías avanzadas, encontró que solo el 32% estaba "muy seguro" de poder responder de manera rápida y efectiva a un ataque a la cadena de suministro. Las empresas en una cadena de suministro son tan fuertes como su eslabón más débil, pero pueden mejorar esta situación asegurándose de que cada eslabón (empresa) a lo largo de su cadena de suministro esté protegido contra amenazas cibernéticas (McAlmont, 2022).
- 2.4 Lo anterior también aplica al sector público, donde los países necesitan mejor equipamiento para combatir la creciente sofisticación de los atacantes cibernéticos. Por ejemplo, en abril de 2022, el gobierno de Costa Rica confirmó haber sido víctima del *ransomware* Conti, el cual afectó, en su mayoría, al Ministerio de Hacienda y a entidades como la Costarricense y la Caja Costarricense del Seguro Social. Debido a esta situación, el gobierno se vio obligado a deshabilitar varios servicios informáticos y a declarar Estado de Emergencia Nacional ([Maundrill, 2022](#)). Por su parte, de acuerdo con [IBM Security X-Force Threat Intelligence Index 2023](#), Colombia es el segundo país de la región que más ciberataques se reportaron en 2022, detrás de Brasil. Entre enero y octubre de 2022, se reportaron más de 50.000 denuncias por ciberataques en Colombia, según cifras del Centro Cibernético de la Policía Nacional. Además, más de 30 empresas informaron que fueron objeto de hackeos, entre ellas EPS Sanitas que administra la salud a más de cinco millones de colombianos. El último informe semestral del panorama global de amenazas de [FortiGuard Labs](#) resalta que Panamá recibió 1.400 millones de intentos de ciberataques en 2022.
- 2.5 A esto se suma la escasez de talento vinculado a ciberseguridad. El Informe Global de Brecha de Habilidades en Ciberseguridad de 2023 encontró que se necesitan aproximadamente 3,14 millones de profesionales para cubrir la demanda de fuerza laboral global en ciberseguridad. El informe indica que muchos equipos de ciberseguridad no tienen suficiente personal mientras trabajan tratando de mantenerse al día con miles de alertas de amenazas diarias e intentando administrar soluciones diversas para proteger adecuadamente los dispositivos y datos de su organización. Así, la brecha de habilidades es una de las principales preocupaciones del sector privado donde el 94% de las juntas en compañías de América Latina y el Caribe aboga por contratar más personal de seguridad de TI, lo que enfatiza la demanda de talento en ciberseguridad.
- 2.6 Los ataques cibernéticos se dirigen cada vez más a las pequeñas y medianas empresas (PYMES), normalmente los eslabones más débiles de una cadena, lo cual puede ser devastador desde el punto de vista financiero ([OCDE, 2021](#)). En efecto, cerca del 70% de las pymes de la región afirman haber experimentado recientemente problemas de ciberseguridad ([OCDE, 2021](#)). por lo que resulta fundamental

comprender mejor los riesgos y las posibles estrategias y buenas prácticas para que las PYMES operen de manera más segura.

- 2.7 La CT es consistente con la actualización de la Estrategia Institucional (UIS) 2020-2023 (AB-3190-2) en cuanto al ámbito prioritario de Productividad e Innovación y con el área transversal de Capacidad Institucional y Estado de Derecho al apoyar el fortalecimiento institucional para ofrecer sensibilización y asistencia técnica a las empresas y programas para desarrollar el talento digital en el ámbito de la ciberseguridad. En esa línea, la CT contribuye a los indicadores de: (i) Instituciones y Estado de Derecho; y (ii) Productividad e Innovación del Marco de Resultados Corporativo (CRF) 2020-2023 (GN-2727-12), al apoyar a las instituciones encargadas de fomentar la productividad del sector privado a diseñar mejores políticas públicas para en el ámbito de la ciberseguridad. En cuanto a las Estrategias del Grupo BID con los Países: (i) Colombia (GN-2972) está en línea con el objetivo de estimular la innovación y el desarrollo empresarial, y reducir la brecha digital de la economía; (ii) Costa Rica (GN-2977) el proyecto contribuye a la mejora del clima de negocios con base en la Agenda Digital del país; y (iii) Panamá (GN-3055) la CT está alineada con los objetivos de promover la transformación digital de la administración pública y mejorar los niveles de adopción digital. También está alineada con el Área prioritaria 3 de “Instituciones eficaces, eficientes y transparentes” del Programa Estratégico para el Desarrollo Financiado con Capital Ordinario (W2C) (GN-2819-14) al apoyar el fortalecimiento de las entidades públicas vinculadas con el proyecto y las capacidades en ciberseguridad del sector privado.
- 2.8 La CT también complementa los esfuerzos del Banco en apoyar a las empresas y gobiernos con capacidades en temas de ciberseguridad. Específicamente en Panamá la operación Panamá Digital (PN-L1171) apoya al gobierno en crear un entorno conductivo a la ciberseguridad de las personas y empresas en el país, incluso la concientización y la formación de talento. En temas de disseminación de conocimiento, la [publicación](#) “Recomendaciones de ciberseguridad y reducción de riesgos cibernéticos para pequeñas empresas: mejores prácticas en ciberseguridad” y el [MOOC sobre Ciberseguridad](#) orientado a gerentes y administradores de micro, pequeñas y medianas empresas (MiPyMEs), interesados en proveer a sus organizaciones de un nivel básico de protección, que ayude a reducir los riesgos cibernéticos a los que se exponen a diario.

III. Descripción de las actividades/componentes y presupuesto

- 3.1 **Componente 1. Apoyo para análisis de capital humano y capacidades de las PYMES pertinentes a ciberseguridad (US\$50.000).** El objetivo es financiar una consultoría para llevar adelante un estudio que analice: (i) el grado de escasez de habilidades digitales necesarias para proporcionar a las empresas y la infraestructura pública crítica suficiente para contar con seguridad cibernética; y (ii) las capacidades de las PYME de los países para hacer frente a los riesgos de ciberseguridad. El resultado del estudio será la base para la ejecución del plan de estudios contemplado en el Componente 2
- 3.2 **Componente 2. Generación de habilidades en ciberseguridad para las PYMES (US\$100.000).** El objetivo es desarrollar un plan de estudios para programas de capacitación específicos de la industria, y un plan de respuesta a incidentes de

seguridad¹. Se financiarán consultorías para llevar a cabo al menos un programa de capacitación y el desarrollo de una herramienta específica del sector. El resultado esperado es contar con PYMES, otras empresas que forman parte de clústeres, y personas capacitadas para manejar las amenazas de ciberseguridad

- 3.3 Si bien los criterios de selección de los beneficiarios de ambos componentes serán acordados con las contrapartes técnicas de la CT (ministerios), se priorizarán a empresas que pertenezcan a sectores productivos estratégicos para cada país, con al menos dos años de constitución formal, y que cuenten con al menos un empleado experto en informática.
- 3.4 El costo total del proyecto financiado por el Banco será de US\$150.000 corresponden a la Ventanilla 2, Área prioritaria 3: Instituciones eficaces, eficientes y transparentes (W2C) del Programa Estratégico para el Desarrollo financiado con Capital Ordinario (OC SDP). La siguiente tabla presenta un desglose del presupuesto por componentes y actividades.

Presupuesto Indicativo (en US\$)

Actividad / Componente	Descripción	BID/ Financiamiento por Fondo	Financiamiento Total
Componente 1. Apoyo para análisis de capital humano y capacidades de las PYMES pertinente a ciberseguridad	Estudio sobre capital humano y capacidades	50.000	50.000
Componente 2. Generación de habilidades en ciberseguridad para las PYMES	Programa de capacitación	75.000	75.000
	Plan de respuesta a incidentes de seguridad	25.000	25.000
TOTAL		150.000	150.000

- 3.5 El especialista responsable de la ejecución de esta CT es el líder del proyecto, quien contará con el apoyo técnico y operativo de los miembros del equipo del proyecto, en el análisis de documentos de carácter técnico que la CT producirá, así como en la definición de términos de referencia para contrataciones de consultores externos. No se requerirá el financiamiento de sistemas de monitoreo de la ejecución, ni informes externos de evaluación más allá de las actividades propias del equipo.

IV. Agencia Ejecutora y estructura de ejecución

- 4.1 De acuerdo con los criterios establecidos en el Anexo II de los Procedimientos para el Procesamiento de Operaciones de Cooperación Técnica (OP-619-4), y a solicitud de los países beneficiarios (Anexo I), el ejecutor de la CT será el Banco a través de la División de Competitividad, Tecnología e Innovación. Lo anterior, debido a su vasta experiencia en la implementación de proyectos con los temas relacionados a esta CT, y por limitaciones de carácter administrativo respecto a la plena aplicación de las

¹ El plan de respuesta podrá incluir recomendaciones sobre mantenimiento de los equipos informáticos, licencias y accesos a servicios de pago en línea, entre otros.

políticas de adquisiciones del Banco. En tal sentido, el Banco será responsable por las adquisiciones y supervisión de los productos de este proyecto. Es importante mencionar que, la supervisión involucra coordinar los esfuerzos en conjunto con los equipos de otras divisiones del Banco, BID *Invest* y las Oficinas de País, según corresponda. La ejecución por el Banco tiene el beneficio adicional de aprovechar lecciones aprendidas y recolectar el resultado de diferentes experiencias para diseminar conocimiento a la región².

- 4.2 Las actividades a ejecutar bajo esta operación se han incluido en el Plan de Adquisiciones (Anexo IV) y serán ejecutadas de acuerdo con los métodos de adquisiciones establecidos del Banco en el Anexo II de la OP-619-4, a saber: (i) Contratación de consultores individuales, según lo establecido en las normas AM 650; (ii) Contratación de firmas consultoras para servicios de naturaleza intelectual según la GN-2765-4 y sus guías operativas asociadas (OP-1155-4); y (iii) Contratación de servicios logísticos y otros servicios distintos a consultoría, de acuerdo a la política GN-2303-28. Todos los productos de conocimiento derivados de esta Cooperación Técnica serán propiedad intelectual del Banco. La ejecución de la CT está prevista por 24 meses donde la unidad responsable de desembolso es la oficina del Banco en Costa Rica.

V. Riesgos importantes

- 5.1 El principal riesgo al que se enfrenta esta CT es la posible falta de coordinación interinstitucional y resistencia al cambio de las instituciones públicas y privadas involucradas, el cual se mitigará a partir de la creación de instancias de colaboración y acciones de capacitación y sensibilización, las cuales forman parte del proyecto.

VI. Excepciones a las políticas del Banco

- 6.1 No se prevén excepciones a las políticas del Banco.

VII. Salvaguardias Ambientales

- 7.1 Esta CT no financiará estudios de factibilidad o prefactibilidad de proyectos de inversión con estudios ambientales y sociales asociados; por lo tanto, está excluida del alcance del Marco de Política Ambiental y Social (MPAS) del Banco.

Anexos Requeridos:

[Solicitud del Cliente - RG-T4255](#)

[Matriz de Resultados - RG-T4255](#)

[Términos de Referencia - RG-T4255](#)

[Plan de Adquisiciones - RG-T4255](#)

- [Checklist de Género y Diversidad](#)

² No se financiarán actividades de CT en ninguno de los países beneficiarios hasta que se reciba la correspondiente carta de no objeción.