



Código TRD: 300

Doctora

ELEONORA BETANCUR GONZÁLEZ

Directora

AGENCIA PRESIDENCIAL DE COOPERACIÓN INTERNACIONAL (APC) COLOMBIA

eleonorabetancur@apccolombia.gov.co

Carrera 10a No 97ª 13. Edificio Bogotá Trade Center Torre A Piso 6.

Ciudad

**ASUNTO: Solicitud para participar como beneficiario de la Operación No Reembolsable Regional
No. RG-T4255**

Estimada Eleonora:

De manera atenta, nos permitimos solicitar a la Agencia Presidencial de Cooperación Internacional de Colombia (APC-Colombia), la gestión para la consecución de una Cooperación Técnica No Reembolsable con el Banco Interamericano de Desarrollo (BID), con código RG-T4255, *Apoyo para cerrar brechas en materia de ciberseguridad en las empresas latinoamericanas*.

El objetivo principal de esta cooperación es apoyar a los países beneficiarios, entre ellos Colombia, en la creación de políticas públicas para sensibilizar a las empresas en ciberseguridad a partir de la identificación de brechas, la exploración de sectores/cadenas, la identificación de problemáticas específicas y el diseño de programas de capacitación a empresas y personas para aumentar la oferta de personas con competencias digitales avanzadas específicamente relevantes en ciberseguridad. El resultado esperado es que las empresas puedan reforzar sus capacidades en ciberseguridad para afrontar los retos de los *clusters* y las Cadenas Globales de Valor.

Con lo mencionado y en línea con el propósito que se lidera desde el Ministerio TIC, de dotar al país de una “*conectividad de 360°*” en la cual se incluyen en acciones que no solo permitan incentivar la productividad del país, sino elevar la confianza y seguridad en el ecosistema digital, de esta forma, se espera generar capacidades de preparación y prevención en la gestión de riesgos de seguridad digital, de manera que permita a los colombianos obtener el mayor aprovechamiento de las ventajas que brinda el estar conectados.

Para este propósito, se ha planteado también, una línea de trabajo orientada a generar una cultura de Seguridad Digital en Colombia, a través de programas concientización, sensibilización, formación y capacitación, dirigidas a ciudadanos, entidades públicas y organizaciones privadas, con el objetivo de lograr un entorno digital seguro, confiable y para todos.



Por lo anterior,

El ejecutor de la operación será el Banco Interamericano de Desarrollo.

Agradecemos la atención prestada y quedamos atentos de su oportuna comunicación con el BID.

Cordialmente,

(FIRMADO DIGITALMENTE)

NOHORA MERCADO CARUSO

Viceministra de Transformación Digital

Ministerio de Tecnologías de la información y las comunicaciones

CC. Kelvin Suero, representante a.i. del Grupo BID en Colombia kelvins@iadb.org

Elaboró: Angela Janeth Cortés Hernández -Asesora Despacho VTD

Revisó: Oscar Eduardo Salazar Rojas – Asesor Despacho VTD -Coordinador COLCERT

REGISTRO DE FIRMAS ELECTRONICAS

232033370

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20230417-155958-e74980-11391752

Creación: 2023-04-17 15:59:58

Estado: Finalizado

Finalización: 2023-04-17 17:24:37



Escanee el código
para verificación

Firma: Viceministra de Transformación Digital

Nohora Mercado Caruso

55250010

nmercado@mintic.gov.co

Viceministra de Transformación Digital

Ministerio de las Tecnologías de la información y comunicaciones

Aprobación: Asesor Despacho VTD -Coordinador COLCERT

OSCAR EDUARDO SALAZAR ROJAS

80054849

osalazar@mintic.gov.co

Funcionario

ASESOR DEL DESPACHO DEL VICEMINISTERIO DE TRANSFORMACIÓN DIGITAL

REPORTE DE TRAZABILIDAD			 Escanee el código para verificación
232033370			
Ministerio de Tecnología de la Información y las Comunicaciones gestionado por: azsign.com.co			
Id Acuerdo: 20230417-155958-e74980-11391752		Creación: 2023-04-17 15:59:58	
Estado:Finalizado		Finalización: 2023-04-17 17:24:37	
TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Aprobación	OSCAR EDUARDO SALAZAR ROJAS osalazar@mintic.gov.co Funcionario ASESOR DEL DESPACHO DEL VICEMINISTERIO D	Aprobado	Env.: 2023-04-17 15:59:59 Lec.: 2023-04-17 16:00:18 Res.: 2023-04-17 16:00:24 IP Res.: 190.71.137.3
Firma	Nohora Mercado Caruso nmercado@mintic.gov.co Viceministra de Transformación Digital Ministerio de las Tecnologías de la info	Aprobado	Env.: 2023-04-17 16:00:24 Lec.: 2023-04-17 17:24:33 Res.: 2023-04-17 17:24:37 IP Res.: 190.145.189.98

19 de abril de 2023
MIDEPLAN-ACI-OF-0053-2023

Señor
Nogui Acosta Jaén
Ministro
Ministerio de Hacienda

Estimado señor:

Reciba un cordial saludo. Por este medio hago referencia a la cooperación técnica regional que está impulsando el Banco Interamericano de Desarrollo (BID), denominada "RG-T4255 Apoyo al cierre de brechas de las empresas en Latinoamérica en ciberseguridad.

Al respecto, mediante oficio MICITT-DM-OF-050-2023, el señor Carlos Enrique Alvarado Briceño, Ministro de Ciencia, Innovación, Tecnología y Telecomunicaciones, nos hace llegar la nota de interés para formar parte de este proyecto regional, el cual busca apoyar a Colombia, Costa Rica, El Salvador 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, que permitan aumentar la oferta de personas con habilidades digitales avanzadas relevantes para la ciberseguridad. El resultado de esta cooperación es que las empresas fortalezcan sus capacidades de ciberseguridad para poder insertarse en clústeres y cadenas globales de valor (CGV).

Este proyecto coadyuva con el cumplimiento del Objetivo de Desarrollo Sostenible (ODS) 8: Promover el crecimiento económico inclusivo y sostenible, el empleo y el trabajo decente para todos; y con el ODS 9: Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación.

El presupuesto del proyecto es regional, por un total de US\$150.000 que estaría aportando, ejecutando y administrando el Banco Interamericano de Desarrollo (BID). Respecto a la contrapartida nacional, la misma será asumida por el MICITT en especie, por un monto aproximado de \$6000.

19 de abril de 2023
MIDEPLAN-ACI-OF-0053-2023
Página 2

El ser un proyecto de importancia nacional, agradezco se indique al BID la No objeción para que Costa Rica, sea parte de este proyecto.

Atentamente,

**SASKIA
RODRIGUEZ
STEICHEN (FIRMA)**

Firmado digitalmente por
SASKIA RODRIGUEZ STEICHEN
(FIRMA)
Fecha: 2023.04.19 10:54:39
-06'00'

Saskia Rodríguez Steichen
Gerente
ÁREA DE COOPERACIÓN INTERNACIONAL

JGU

- C. Sr. Carlos Enrique Alvarado Briceño, ministro de Ciencia, Innovación, Tecnología y Telecomunicaciones.
Sra. Embajadora Adriana Bolaños Arguedas, directora de Cooperación Internacional, MRREE.
Archivo.

Panamá, 20 de abril de 2023
N-SNAC-DINE-2023-378

Su Excelencia
Héctor Alexander
Ministro de Economía y Finanzas
E. S. D.

Respetado Señor Ministro:


Nos dirigimos a usted con el ánimo de solicitar su apoyo para formar parte de la **Cooperación Técnica Regional No Reembolsable** No. RG-T4255 del Banco Interamericano de Desarrollo (BID) para el apoyo al cierre de brechas de las empresas en Latinoamérica en ciberseguridad. Dicha cooperación técnica será por un monto estimado de ciento cincuenta mil balboas (B/. 150,000.00).

Consideramos importante formar parte de esta cooperación técnica porque la Secretaría Nacional de Ciencia, Tecnología e Innovación (SENACYT) tiene como misión convertir a la ciencia y a la tecnología en herramientas para el desarrollo sostenible en Panamá. Esta iniciativa tiene como objetivo apoyar a los países beneficiarios (Colombia, Costa Rica, El Salvador 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).

Por otro lado, solicitamos que el BID ejecute esta cooperación técnica por su experiencia y conocimiento.

Con nuestras consideraciones y aprecio.

Atentamente,



DR. EDUARDO ORTEGA BARRÍA

Secretario Nacional de Ciencia, Tecnología e Innovación

EOB/ADY/pf



(La información suministrada permitirá evaluar la viabilidad de las mismas.)

Fecha:

Nombre de la propuesta:

Apoyo al cierre de brechas de las empresas en Latinoamérica en ciberseguridad

Antecedentes:

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 Cadenas Globales de Valor (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.

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).

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 (Maurdrill, 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. Para el caso de El Salvador, 206.000 empresas fueron víctimas de ataques cibernéticos en 2021.

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 (referencia), 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.

Justificación:

Panamá se encuentra entre las economías con el PIB per cápita más alto de América Latina y el Caribe, lo que corresponde al de una economía de altos ingresos. El país debido a su privilegiada zona geográfica y las grandes inversiones que ha realizado en infraestructura de transporte y logística como el Canal, puertos y aeropuertos que, a su vez están conectadas con zonas económicas especiales han posicionado al país como importante centro logístico (BID, 2018) y facilitador de cadena de suministros para la región y el mundo.

En el 2020 la Pandemia del COVID-19 generó una contracción del PIB del país del 17.9%. Esto debido, entre otras razones, a los cierres y paralizaciones de las economías que, generaron la interrupción del flujo de actividades productivas y de consumo. Muchas empresas se han visto golpeadas por la crisis sanitaria y han surgido fuertes tensiones que pueden limitar su competitividad y su supervivencia (CNC, 2021), el 30% de empresas, ha tenido que cerrar debido a la pandemia (CNC, 2021). Sin embargo, la pandemia ha generado también efectos positivos que ahora deben mantenerse y ampliarse, como es el caso de la digitalización forzada a la que se vieron sometidas las empresas y sociedad, evidenciando beneficios de contar con procesos y canales digitales y barreras existentes para poner en valor estas tecnologías (BID, 2020). El 95% de las empresas panameñas (MIPYMES) consideran que la pandemia aceleró su proceso de transformación digital y el 89% reconoce que la tecnología jugará un papel importante en el modelo de negocio que apliquen una vez superada la pandemia (Microsoft, 2022). Por lo tanto, las empresas han venido incrementando su inversión en tecnología en donde el 31% han realizado las inversiones necesarias en equipos y capacitaciones a sus colaboradores (Microsoft, 2022).

Ciberseguridad. El incremento en la digitalización de las empresas, debido a la pandemia, también ha generado un incremento en la oportunidad para que hackers cometan ataques cibernéticos. Las PYMES tienden a tener un entendimiento limitado de las consecuencias generadas por los ciberataques, lo que explica una baja inversión en sistemas de seguridad digital (OECD, 2020). En Panamá para el 2021 se registraron 3.2 millones de intentos de ciberataques y hasta el primer semestre del 2022, se registraron 163 millones de ataques cibernéticos que no lograron concretarse porque fueron detenidos por los distintos sistemas de seguridad que tienen las empresas. Estas cifras colocan a Panamá en el “top ten” de ataques cibernéticos de la región de Latinoamérica (AIG, 2022). Ante este escenario, es necesario que se fortalezca el conocimiento y capital de las PYMES panameñas para que puedan hacerle frente a esta nueva realidad, tomando en cuenta que, el gobierno reconoce el papel de las PYMES como un elemento fundamental de política para el desarrollo económico del país; y el rol que cumplen estas empresas para una potencial reactivación durante y después de la pandemia (CEPAL, 2021).

Descripción de la propuesta:

La propuesta busca realizar actividades que permita fortalecer las capacidades de políticas públicas que contribuyan a la sensibilización de las empresas en materia de ciberseguridad. Esto se busca lograr mediante un mejor entendimiento de las brechas existentes que evitan que hacen que la situación sea la óptima y el diseño de programas para la formación del personal de las empresas y particulares para fortalecer sus habilidades digitales avanzadas para la ciberseguridad.

Tipo :

☐ Nueva ☐ Continua**Modalidad:**

✓ Asistencia Técnica	Becas/Cursos
Asesorías	Voluntarios
Asesorías	Donación de equipos
Consultorías	✓ Capacitaciones
Talleres/Seminarios/Foros/Reuniones/Misiones	Proyectos Integrales
Intercambio de Expertos	Programas Conjuntos

Entidad solicitante:

Secretaría Nacional de Ciencia, Tecnología e Innovación

Organismo Cooperante:

(BID) Banco Interamericano de Desarrollo

Otra:

Entidad Ejecutora:

Secretaría Nacional de Ciencia, Tecnología e Innovación

Objetivo General:	Apoyar a los países beneficiarios (Colombia, Costa Rica, El Salvador y Panamá) en la creación de políticas públicas para sensibilizar a las empresas en ciberseguridad																																																																																	
Objetivos Específicos:	i) la identificación de brechas; ii) exploración de sectores/cadenas; iii) identificación de problemas específicos; y iv) diseño de programas de formación para empresas y particulares que permitan aumentar la oferta de personas con habilidades digitales avanzadas relevantes para la ciberseguridad.																																																																																	
Duración:	24 meses																																																																																	
Inicio:	1 de junio de 2023																																																																																	
Culminación:	1 de junio de 2025																																																																																	
Sector	<div><div><input checked="" type="checkbox"/> Administración y Servicios Generales <input type="checkbox"/> Agropecuario <input type="checkbox"/> Ambiente <input type="checkbox"/> Educación y Cultura <input checked="" type="checkbox"/> Energía <input type="checkbox"/> Finanzas <input checked="" type="checkbox"/> Industria, Comercio y Turismo <input type="checkbox"/> Justicia</div><div><input type="checkbox"/> Minería <input type="checkbox"/> Protección Ciudadana <input type="checkbox"/> Salud <input checked="" type="checkbox"/> Telecomunicaciones <input type="checkbox"/> Trabajo y Bienestar Social <input type="checkbox"/> Transporte <input checked="" type="checkbox"/> Vivienda</div></div>																																																																																	
Objetivos de Desarrollo Sostenible:	<div><div><input type="checkbox"/> 1. Fin de la Pobreza <input type="checkbox"/> 2. Hambre Cero <input type="checkbox"/> 3. Salud y Bienestar <input type="checkbox"/> 4. Educación de Calidad <input type="checkbox"/> 5. Igualdad de Género <input type="checkbox"/> 6. Agua Limpia y Saneamiento <input type="checkbox"/> 7. Energía Asequible y No Contaminante <input checked="" type="checkbox"/> 8. Trabajo Decente y Crecimiento Económico <input checked="" type="checkbox"/> 9. Industrial, Innovación e Infraestructura</div><div><input checked="" type="checkbox"/> 10. Reducción de las Desigualdades <input type="checkbox"/> 11. Ciudades y Comunidades Sostenibles <input checked="" type="checkbox"/> 12. Producción y Consumo Responsables <input type="checkbox"/> 13. Acción por el Clima <input type="checkbox"/> 14. Vida Submarina <input type="checkbox"/> 15. Vida de Ecosistemas Terrestres <input type="checkbox"/> 16. Paz, Justicia e Instituciones Sólidas <input checked="" type="checkbox"/> 17. Alianzas para Lograr los Objetivos</div></div>																																																																																	
Ubicación Geográfica:	<input checked="" type="checkbox"/> Urbana <input type="checkbox"/> Rural																																																																																	
Actores claves:	SENACYT, INDICATIC AIP, PYMES																																																																																	
Beneficiarios:	PYMES legalmente constituidas en Panamá, emprendedores (personas físicas contribuyentes con facturación legal) y Recurso Humano de la SENACYT e INDICATIC AIP.																																																																																	
Vinculación con el Plan de Gobierno de Panamá (PEG):	A través del Pilar 3: Economía competitiva que genere empleos, en el cual se establece que el modelo de desarrollo del país debe adaptarse a los tiempos actuales para poder generar una prosperidad sostenible, inclusiva y duradera. Para esto, entre otras medidas, establece que se apoyará al sector productivo para incrementar su eficiencia y competitividad y así generar más inversiones, fuentes de empleo y consumo. La PYME es reconocida, en el Plan como motor para el desarrollo económico y generación de empleos, por lo que señala que es necesario impulsar el emprendimiento a través de políticas públicas que promuevan estas iniciativas. En el Pilar 5 Educación, Ciencia, Tecnología y Cultura se reconoce que el país enfrenta grandes desafíos y para hacerle frente, entre otras acciones, está la de consolidar altos niveles de competitividad sostenible basada en la innovación a la cual se podrá llegar con una mayor capacidad de generación, adaptación, difusión y utilización de conocimiento. Por último pero no menos importante está el Pilar 4: Combate a la pobreza y a la desigualdad el cual establece que reducir la pobreza y la desigualdad se hará junto con otras acciones, a través del conocimiento, la ciencia, la tecnología y la innovación.																																																																																	
Vinculación con el Plan Sectorial:	El Plan Estratégico Nacional para el Desarrollo de la Ciencia, Tecnología y la Innovación (2019-2024) está destinado a transformar Panamá en un Estado moderno mediante una gestión eficiente y dinámica, transparente a través de la restauración ética y moral de la gestión gubernamental y de la sociedad. La modernidad no solamente implica mayor desarrollo económico sino también cerrar las brechas sociales que dividen a la sociedad panameña, es decir crear un país justo, y mirando con optimismo el futuro. La Política reconoce que la investigación y la innovación son los principales conductores del crecimiento y la transformación de una economía, de la productividad y la competitividad, de la preservación ambiental y la utilización racional de los recursos naturales, del desarrollo social, la superación de la pobreza y la inequidad, y de la cultura. Son la base sobre la cual opera la economía del conocimiento, y se convierten también en la base sobre la que el gobierno transformará Panamá. En el contexto anterior, el Plan Estratégico Nacional de Ciencia, Tecnología e Innovación (PENCYT) 2019 – 2024 está alineado con las prioridades de gobierno y define las acciones que en el largo y corto plazo deben ser adoptadas en materia de investigación e Innovación para contribuir a lograr la transformación de Panamá.																																																																																	
Resultados esperados:	Apoyo para análisis de capital humano y capacidades de las PYMES. El objetivo es financiar un estudio para analizar: (i) el grado de escasez de habilidades digitales necesarias para proporcionar a las empresas y la infraestructura pública crítica suficiente seguridad cibernética, y (ii) las capacidades de las PYME de los países para hacer frente a los riesgos de ciberseguridad. Generación de habilidades en ciberseguridad para las PYMES. El objetivo es desarrollar un plan de estudios para programas de capacitación específicos de la industria, y un plan de respuesta a incidentes de seguridad. Se financiarán consultorias 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																																																																																	
Indicadores:	Indicadores de Producto: Estudios realizados; Formación de Recurso Humano completada, Diagnósticos completados; Instrumentos e Iniciativas diseñadas, Metodologías elaboradas, Publicaciones realizadas.																																																																																	
Componentes / Productos:	Componente 1. Apoyo para análisis de capital humano y capacidades de las PYMES (US\$50 000). El objetivo es financiar un estudio para analizar: (i) el grado de escasez de habilidades digitales necesarias para proporcionar a las empresas y la infraestructura pública crítica suficiente seguridad cibernética, y (ii) las capacidades de las PYME de los países para hacer frente a los riesgos de ciberseguridad. 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 seguridad. Se financiarán consultorias 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																																																																																	
Cronograma de Actividades:	<table><tr><th>Componente</th><th>Actividad</th><th colspan="3">2023</th><th colspan="9">2024</th></tr><tr><th></th><th></th><th>Octubre</th><th>Noviembre</th><th>Diciembre</th><th>Enero</th><th>Febrero</th><th>Marzo</th><th>Abril</th><th>Mayo</th><th>Junio</th><th>Julio</th><th>agosto</th><th>septiembre</th></tr><tr><td>Componente 1. Apoyo para análisis de capital humano y capacidades de las PYMES pertinente a ciberseguridad</td><td>Consultoria 1: Estudio sobre capital humano y capacidades de las PYME de los países para hacer frente a los riesgos de ciberseguridad</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td>Consultoria 2: Programa de capacitación en ciberseguridad para PYMES</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Componente 2. Generación de habilidades en ciberseguridad para las PYMES</td><td>Consultoria 3: Plan de respuesta a incidentes de seguridad para PYMES</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>												Componente	Actividad	2023			2024											Octubre	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	agosto	septiembre	Componente 1. Apoyo para análisis de capital humano y capacidades de las PYMES pertinente a ciberseguridad	Consultoria 1: Estudio sobre capital humano y capacidades de las PYME de los países para hacer frente a los riesgos de ciberseguridad														Consultoria 2: Programa de capacitación en ciberseguridad para PYMES													Componente 2. Generación de habilidades en ciberseguridad para las PYMES	Consultoria 3: Plan de respuesta a incidentes de seguridad para PYMES												
Componente	Actividad	2023			2024																																																																													
		Octubre	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	agosto	septiembre																																																																					
Componente 1. Apoyo para análisis de capital humano y capacidades de las PYMES pertinente a ciberseguridad	Consultoria 1: Estudio sobre capital humano y capacidades de las PYME de los países para hacer frente a los riesgos de ciberseguridad																																																																																	
	Consultoria 2: Programa de capacitación en ciberseguridad para PYMES																																																																																	
Componente 2. Generación de habilidades en ciberseguridad para las PYMES	Consultoria 3: Plan de respuesta a incidentes de seguridad para PYMES																																																																																	
II. Datos Financieros																																																																																		

¿Ligado a financiamiento público?

☐ Si

☒ No

Ejecución:

☐ Anual ☐ Plurianual

Aporte Externo:

Aporte Local:

0 Efectivo:

Especies:

Nota: es no reembolsable.

Partida presupuestaria:

Presupuesto por Componentes:

Presupuesto Indicativo (en US\$)				
Actividad / Componente	Descripción	BID/Financiamiento por Fondo	Contrapartida Local	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	0,00	50 000
	Programa de capacitación	75 000	0,00	75 000
Componente 2. Generación de habilidades en ciberseguridad para las PYMES	Plan de respuesta a incidentes de seguridad	25 000		25 000
	TOTAL	150 000	0,00	150 000

Administrador de Fondos:

Banco Interamericano de Desarrollo

III. Documentos Anexos

Documentos Anexos:

IV. Datos del Personal Responsable

Entidad beneficiaria: Secretaría Nacional de Ciencia, Tecnología e Innovación

Responsable del Proyecto: Dr. Eduardo Ortega -Barría

Cargo: Secretario Nacional

Dirección: Ciudad del Saber, Clayton, Edif. 205, Panamá, Ciudad de Panamá

Teléfonos: 517-0005

Correo electrónico: eortegabarria@senacyt.gob.pa

Institución Cooperante:

Responsable del Proyecto:

Cargo:

Dirección:

Teléfonos:

Correo electrónico:

Nota: el formulario debe de tener sello y firma del Despacho Superior de la Institución solicitante

Agradecemos igualmente nos remita la versión Excel del documento firmado.

SENACYT

SECRETARÍA NACIONAL DE CIENCIA, TECNOLOGÍA E INNOVACIÓN

PANAMÁ

26 de abril del 2023
MH-DM-OF-0644-2023

Señor
Fernando Quevedo
Representante en Costa Rica
Banco Interamericano de Desarrollo

Asunto: Atención de oficio MIDEPLAN-ACI-OF-0053-2023

Estimado señor:

Me refiero al oficio MIDEPLAN-ACI-OF-0053-2023, suscrito por la Sra. Saskia Rodríguez Steichen, Gerente del Área de Cooperación Internacional del Ministerio de Planificación Nacional y Política Económica (MIDEPLAN), mediante el cual se solicita gestionar ante el Banco Interamericano de Desarrollo (BID) que el país, a través del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), forme parte del proyecto de cooperación técnica regional RG-T4255 "Apoyo al cierre de brechas de las empresas en Latinoamérica en ciberseguridad".

El presupuesto del proyecto es regional por un monto total de USD 150.000, en donde el MICITT aportaría una contrapartida nacional en especie por un monto aproximado de USD 6.000, siendo importante indicar que los compromisos y previsiones de aporte de contrapartida institucional son completa responsabilidad del MICITT en el marco del cumplimiento de las directrices y normativas presupuestarias y el cumplimiento de la regla fiscal.

Este proyecto regional tiene como objetivo apoyar a Colombia, Costa Rica, El Salvador 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, que permitan aumentar la oferta de personas con habilidades digitales avanzadas relevantes para la ciberseguridad.

En el oficio supra citado, el cual se adjunta, se indica que el proyecto coadyuva con el cumplimiento del Objetivo de Desarrollo Sostenible (ODS) 8: Promover el crecimiento económico inclusivo y sostenible, el empleo y el trabajo decente para todos, y con el ODS 9: Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación. Asimismo, se indica que la cooperación será administrada y ejecutada por el BID.

Dado lo anterior, en mi condición de Gobernador ante el Banco comunico el interés para que el país, a través del MICITT, forme parte del proyecto regional citado, y en caso de que el país sea seleccionado para formar parte de la cooperación, ese Ministerio deberá cumplir con lo dispuesto en el Decreto Ejecutivo N°35056-PLAN-RE.

Atentamente,

NOGUI ACOSTA
JAEN (FIRMA)
M.E.E. Nogui Acosta Jaén
Ministro de Hacienda

Firmado digitalmente por
NOGUI ACOSTA JAEN (FIRMA)
Fecha: 2023.04.28 17:54:02
-06'00'

TAR

C: Sr. Carlos Enrique Alvarado Briceño, Ministro de Ciencia, Innovación, Tecnología y Telecomunicaciones.
Sra. Adriana Bolaños Argueta, Directora de Cooperación Internacional, Ministerio de Relaciones Exteriores y Culto.
Sra. Saskia Rodríguez Steichen, Gerente del Área de Cooperación Internacional, MIDEPLAN.

ROSAURA TRIGUEROS ELIZONDO (FIRMA) Firmado digitalmente por ROSAURA TRIGUEROS ELIZONDO (FIRMA) Fecha: 2023.04.26 10:41:57 -06'00'	MELVIN FERNANDO QUIROS ROMERO (FIRMA) Firmado digitalmente por MELVIN FERNANDO QUIROS ROMERO (FIRMA) Fecha: 2023.04.27 00:22:51 -06'00'
VB: Coordinadora del Departamento de Coordinación y Control del Endeudamiento Público Dirección de Crédito Público	VB: Director de Crédito Público