I. Información Básica de la CT

▪ País/Región:	REGIONAL
▪ Nombre de la CT:	Ciberseguridad y Transformación Digital en el Sector de Energía
▪ Número de CT:	RG-T4687
▪ Jefe de Equipo/Miembros:	Irigoyen, Jose Luis (INE/ENE) Líder del Equipo; Alarcon, Arturo (INE/ENE) Jefe Alterno del Equipo de Proyecto; Riobo Patino, Jairo Alexander (INE/TSP); Martha Carvalho (INE/ENE); Urquijo, Lee (TTD/TTR); Echevarria Barbero, Carlos Jose (INE/ENE); Gomez, Jose Ramon (INE/ENE); Baldivieso, Hector (INE/ENE); Paredes, Juan Roberto (INE/ENE); Moleres Regalado, Estefania (INE/ENE); Mayorga Acosta Nayeli (INE/ENE); Rubio Fernandez, Eva (TTD/TTR); Jacome Montenegro, Carlos Alberto (INE/ENE); Correa Poseiro, Cecilia (INE/ENE); Paz Gonzalez, Santiago (IFD/ICS); Goncalves Dos Santos, Carolina (LEG/SGO)
▪ Taxonomía:	Apoyo al Cliente
▪ Operación a la que la CT apoyará:	.
▪ Fecha de Autorización del Abstracto de CT:	5 Feb 2025.
▪ Beneficiarios:	Centrais Elétricas de Santa Catarina (CELESC) de Brasil, Empresa Nacional de Energía Eléctrica (ENEE) de Honduras y Secretaria Nacional de Energía (SNE) de Panamá
▪ Agencia Ejecutora y nombre de contacto:	Inter-American Development Bank
▪ Donantes que proveerán financiamiento:	Fondo General de Cooperación de España(FGE)
▪ Financiamiento solicitado del BID:	US$500,000.00
▪ Contrapartida Local, si hay:	US$0
▪ Periodo de Desembolso (incluye periodo de ejecución):	36 meses
▪ Fecha de inicio requerido:	01/08/2025
▪ Tipos de consultores:	Individual; Firmas
▪ Unidad de Preparación:	INE/ENE-Energía
▪ Unidad Responsable de Desembolso:	INE/ENE-Energía
▪ CT incluida en la Estrategia de País (s/n):	S
▪ CT incluida en CPD (s/n):	N
▪ Alineación con la Estrategia Institucional 2024-2030:	Infraestructura sostenible, resiliente e inclusiva

II. Objetivos y Justificación de la CT

2.1 América Latina y el Caribe (ALC) enfrentan el doble desafío de garantizar el acceso universal, en 2023 la tasa de electrificación en ALC era de 97%[1] a electricidad de calidad y, al mismo tiempo, erradicar la pobreza energética[2]. En este contexto, la transformación digital surge como una herramienta poderosa para modernizar la infraestructura, mejorar la eficiencia operativa y fortalecer la relación entre los

[1] Hub de Energia, BID

[2] El quintil 1 (más vulnerable) tiene en promedio 9 veces menos acceso a la electricidad que el de mayores ingresos, llegando a casi duplicarse esta brecha en la población rural. La población indígena y afrodescendiente sin acceso a electricidad representa más de un tercio del total. En promedio, el 15,5% de la población que no tiene acceso a la energía reside en viviendas precarias. CEPAL, 2024

consumidores y el sistema eléctrico. La digitalización implica no solo la adopción de nuevas tecnologías, sino también la capacitación de una fuerza laboral altamente calificada y la creación de marcos que promuevan la participación activa de los usuarios en nuevos modelos de negocio y servicios energéticos. Sin embargo, el ritmo de avance digital en la región es desigual. Persisten barreras importantes como la falta de estándares comunes, la resistencia institucional a la innovación, la distribución asimétrica de costos y beneficios, y la escasez de habilidades digitales en el sector energético. A estos desafíos se suma uno transversal y urgente: la ciberseguridad.

2.2 La digitalización, cuando no está acompañada de una estrategia sólida de ciberseguridad, puede aumentar significativamente la exposición del sistema energético a riesgos externos. La creciente automatización, el uso de datos en tiempo real y la integración de tecnologías operativas (TO) con sistemas de información (TI) amplían la superficie de ataque. Esta realidad es particularmente crítica en un sector que constituye infraestructura esencial para el funcionamiento económico y social de los países.

2.3 Los ciberataques a sistemas eléctricos pueden generar consecuencias graves, desde interrupciones en el suministro hasta el robo de datos sensibles y fallas en cascada en otras infraestructuras. En América Latina, se estima que la mitad de la cadena de suministro eléctrico está expuesta a ciberamenazas[3], y los costos económicos derivados de estos ataques pueden alcanzar hasta el 6% del PIB en casos que afectan infraestructura crítica4. Entre los factores que agravan esta vulnerabilidad están el uso de redes comunes de operación e información, la falta de control sobre accesos remotos y la inexistencia de protocolos estandarizados de protección.

2.4 Frente a este escenario, la ciberseguridad no puede ser tratada como un componente secundario. Requiere un enfoque sistémico que combine capacitación técnica, incorporación de tecnologías de protección avanzadas y fortalecimiento institucional. Para mitigar riesgos, es fundamental: (i) identificar y corregir vulnerabilidades, (ii) implementar monitoreo continuo, y (iii) fortalecer la cultura de seguridad dentro de las organizaciones. Esto implica invertir en monitoreo continuo, identificación proactiva de vulnerabilidades, desarrollo de marcos regulatorios claros y fortalecimiento de la cultura organizacional de seguridad. También es fundamental contar con equipos multidisciplinarios capaces de integrar conocimientos de ingeniería eléctrica, tecnologías de la información y gestión de riesgos.

2.5 En respuesta a estos desafíos, algunos países han creado organismos especializados. En Estados Unidos, por ejemplo, se estableció la Oficina de Seguridad Cibernética, Energética y de Respuesta ante Emergencias luego de un intento de hackeo en 2017 dirigido a múltiples empresas eléctricas. Infraestructuras de gran escala, como centrales hidroeléctricas y nucleares, son objetivos particularmente vulnerables a este tipo de amenazas, lo que refuerza la urgencia de una respuesta estructurada y coordinada en la región.

2.6 Afortunadamente, ya existen experiencias concretas en la región que demuestran cómo avanzar de forma segura en la transformación digital. El Complejo Hidroeléctrico Salto Grande entre Argentina y Uruguay, por ejemplo, ha integrado soluciones digitales con una visión clara de protección cibernética desde el inicio. Por su parte, el proyecto Itaipú Binacional (Brasil-Paraguay) implementa desde 2003 un

[3] Estado de preparación en ciberseguridad del sector eléctrico en América Latina
[4] Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe

sistema de control centralizado que permite la operación sincronizada a través de interfaces externas, con arquitectura diseñada para integración progresiva en la nube. Estas experiencias muestran que, a medida que se modernizan los sistemas de automatización y se amplía la conectividad, también se vuelve indispensable una estrategia de defensa cibernética integrada desde la concepción de los proyectos.

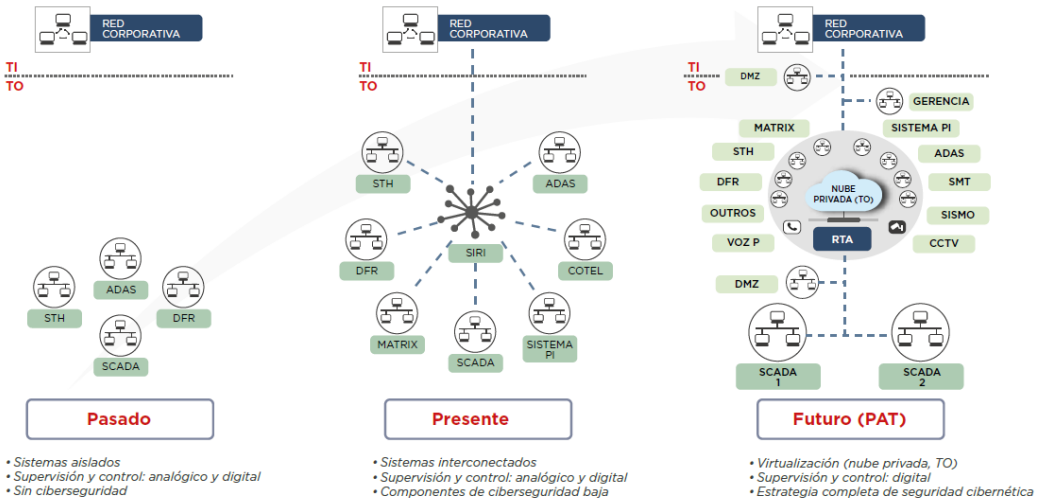

Fig. 1. Evolución del sistema de monitoreo binacional de Itaipú[5][6] .

2.7 La figura ilustra el esquema progresivo de digitalización implementado en la central hidroeléctrica de Itaipú Binacional, destacando la integración gradual de tecnologías operativas (TO), sistemas de automatización y plataformas de monitoreo. Se observa cómo estas tecnologías se interconectan y sincronizan para permitir la visualización y el control en tiempo real del desempeño energético a través de una interfaz externa (IE). El diagrama también muestra la arquitectura diseñada para soportar, en etapas futuras, el almacenamiento y análisis de datos en la nube.

2.8 La literatura técnica respalda la efectividad de invertir en ciberseguridad. Estudios recientes muestran que esquemas de protección con técnicas de aprendizaje automático pueden reducir significativamente el riesgo operativo[7][8][9]. Por ejemplo, mecanismos de acción correctiva capaces de desconectar componentes vulnerables han demostrado reducir en hasta 40% los costos adicionales asociados a ataques cibernéticos.

---

[5] **TI:** Tecnología de la Información. Sistemas corporativos e administrativos, como servidores, bases de datos, redes internas y plataformas de gestión empresarial.
TO: Tecnología Operativa. Sistemas que permiten operar, controlar y monitorear procesos industriales en tiempo real, como SCADA, PLCs y sensores.
IE: Interfaz Externa. Punto de acceso que permite a usuarios externos visualizar o interactuar con los sistemas operativos de forma segura.
DMZ: Demilitarized Zone. Zona intermedia de seguridad entre la red interna y externa, que permite el acceso controlado a ciertos servicios sin comprometer los sistemas críticos.
SCADA: Supervisory Control and Data Acquisition. Sistema de supervisión y adquisición de datos para el monitoreo y control de procesos industriales.
PLC: Programmable Logic Controller. Dispositivo de control industrial que ejecuta instrucciones programadas basadas en entradas del entorno operativo.
ERP: Enterprise Resource Planning. Plataforma integrada de gestión empresarial para procesos como finanzas, logística y recursos humanos.
HMI: Human-Machine Interface. Interfaz que permite la interacción entre los operadores humanos y los sistemas de control.
RTU: Remote Terminal Unit. Unidad remota utilizada para recopilar datos y ejecutar comandos en sistemas SCADA.
IoT: Internet of Things. Dispositivos interconectados que recopilan e intercambian datos a través de internet, como medidores inteligentes y sensores.
NOC: Network Operations Center. Centro encargado de supervisar el funcionamiento de las redes de comunicación y sistemas interconectados.
SOC: Security Operations Center. Centro especializado en la vigilancia, detección y respuesta ante incidentes de ciberseguridad.

[6] Estado de preparación en ciberseguridad del sector eléctrico en América Latina

[7] On the Cybersecurity of Traffic Signal Control System With Connected Vehicles

[8] A Region-based Framework for Cyberattacks Leading to Undervoltage in Smart Distribution Systems

[9] A remedial action framework against cyberattacks targeting energy hubs integrated with distributed energy resources

2.9 En ALC, el tema aún es incipiente y requiere una acción decidida. Por eso, el Banco ha establecido como prioridad estratégica el apoyo a la transformación digital del sector energía, con un foco especial en ciberseguridad. La presente CT busca justamente apoyar el diseño, dimensionamiento e implementación de acciones concretas de digitalización segura, que puedan ser incorporadas en operaciones de inversión en energía en los países de la región.

2.10 **Solicitud**. Ante este diagnóstico, los países Brasil, Honduras y Panamá solicitaron la CT al BID para intervenir en los problemas descritos, con el objetivo de aumentar la capacidad en ciberseguridad y promover la transformación digital en el sector energético.

2.11 **Objetivo**. El principal objetivo de esta CT es contribuir a incrementar la capacidad del sector de energía de la región para avanzar en su transformación digital. Los objetivos específicos son: (i) incrementar la capacidad en ciberseguridad mediante el uso de herramienta de autoevaluación de ciberseguridad, el uso de auditorías de ciberseguridad, brindar capacitación en ciberseguridad a gerentes, reguladores, técnicos y operadores; (ii) incrementar el uso eficiente de herramientas digitales en el sector; y (iii) abrir oportunidades de intercambio de experiencias y conocimiento internacionales mediante visitas.

2.12 **Complementariedad**. El BID ha financiado varios proyectos que abordan la digitalización y la ciberseguridad en el sector energético. Esta CT amplía, refuerza y da sostenibilidad al trabajo realizado en el proyecto RG-T4513, que financió el desarrollo y el mejoramiento de las capacidades de ciberseguridad a través de autoevaluaciones, auditorías y entrenamientos dirigidos. Además, implementó herramientas digitales basadas en inteligencia artificial para enfrentar los desafíos en el sector energético, asegurando una infraestructura más segura y eficiente. La Cooperación Técnica RG-T4687 amplía, refuerza y da sostenibilidad a los avances logrados en la operación RG-T4513 a través de la aplicación de las herramientas desarrolladas en otros países.

2.13 **Alineación Estratégica**. La TC está alineada con la Estrategia Institucional Transformando para lograr un mayor impacto y escala (CA-631), en el área de enfoque operativo de Infraestructura Sostenible, Resiliente e Inclusiva con Énfasis en la Integración Regional. El Grupo BID se ha comprometido a incrementar la capacidad en ciberseguridad del sector eléctrico. La CT también si alinea con el área transversal Capacidad institucional, Estado de Derecho y Seguridad ciudadana, una vez que brinda capacitación en ciberseguridad a gerentes, reguladores, técnicos y operadores, así como a fomentar la infraestructura digital y los servicios innovadores basados en tecnología. Además, la CT está alineada con el Marco de Resultados Corporativos 2024–2030 (GN-3195-8) al mejorar la capacidad institucional de los gobiernos y entidades sectoriales. Esta CT es coherente con el Marco Sectorial de Energía (GN-2830-8), al contribuir a: (i) el desarrollo sostenible del sector; (ii) la diversificación de la matriz energética; y (iii) el fortalecimiento de la capacidad para formular y ejecutar políticas energéticas. Entre otras actividades, la CT financiará capacitaciones en ciberseguridad en Brasil, Honduras y Panamá. La CT está alineada con las Estrategias País de Brasil 2024–2027 (GN-3243-3), con el Pilar 2: transformación digital para la productividad y la inclusión, al apoyar el desarrollo de infraestructura digital y servicios públicos innovadores. También con la Estrategia País de Honduras 2019–2024 (GN-2944), con el eje estratégico de fortalecimiento institucional y digitalización, al impulsar la modernización de la infraestructura crítica y la digitalización de servicios públicos para mejorar la eficiencia y resiliencia del

Estado. Y por último, la CT está alineada con la Estrategia País de Panamá 2025-2029 (GN-3289), con el Pilar 1 al apoyar la transformación digital como herramienta transversal para mejorar la eficiencia en la provisión de servicios básicos.

III. Descripción de las actividades/componentes y presupuesto

3.1 **Componente I (US$300.000):** Ciberseguridad. El objetivo de este componente es desarrollar capacidades en materia de ciberseguridad mediante las siguientes actividades:

a. Fomentar el uso de la herramienta de autoevaluación de ciberseguridad proporcionando el apoyo técnico necesario para que se complete la autoevaluación. La herramienta fue diseñada en conjunto con IFD/ICS-Ciberseguridad. Es un cuestionario de opción múltiple que genera dinámicamente un score de cumplimiento por cada función y un set de recomendaciones específicas. Les sirve a las instituciones para ver cómo están en el tema y también como base para armar un plan de acción y un presupuesto que el BID luego pueda apoyar con CT o préstamo.

b. Facilitar el uso de las auditorías y proporcionar el apoyo necesario a los ministerios de la región para llevarlas a cabo. El objetivo de las auditorias es contratar a una empresa experta en riesgos de ciberseguridad para evaluar la situación de ciberseguridad de la organización, y medir la brecha existente con las mejores prácticas de la industria. La mejor práctica internacional es realizar esta auditoría cada 2 años.

c. Continuar los cursos de capacitación en ciberseguridad, dictados por Tecnalia (empresa española), con un énfasis en la capacitación de mujeres del sector. El objetivo es dotar a los participantes de los conocimientos fundamentales y necesarios para poder reforzar e implementar estrategias de defensa ante posibles ciberataques y ser conscientes de las amenazas actuales y futuras a las que se enfrenta el sector. Ofrecemos 2 modalidades: curso de 10 horas para gestores, orientado a gerentes, directivos y reguladores (puestos de decisión), y curso de 40 horas para técnicos, para puestos de supervisión, mantenimiento y configuración de smart grids) con parte teórica y parte práctica.

3.2 **Componente II (US$140.000):** Herramientas Digitales. El objetivo de este componente es acelerar y apoyar a los gobiernos a desarrollar y promover el uso de herramientas digitales en el sector eléctrico en la región, incluyendo las empresas públicas del sector; por ejemplo, “Energiza2”[10] y “SunscanIDB”[11]. Mediante las siguientes actividades:

[10] Energiza2 es una iniciativa del BID, cuyo objetivo principal es reducir las pérdidas no técnicas de energía eléctrica mediante el uso de ciencia de datos y aprendizaje automático. Este proyecto busca fortalecer las capacidades técnicas de los equipos de empresas de transmisión para identificar fraudes o consumos anómalos en la red eléctrica. Para ello, se desarrolló una solución basada en Python que utiliza bibliotecas como Pandas, técnicas de ingeniería de variables y modelos predictivos.

[11] SunScanIDB es una herramienta digital de código abierto desarrollada por el BID para estimar el potencial de generación de energía solar en techos urbanos y rurales. Utiliza modelos de aprendizaje profundo como UNET y SAM, junto con imágenes satelitales de alta resolución, para: (i) detectar y delinear contornos de techos; (ii) calcular la radiación solar disponible en cada ubicación; y (iii) estimar la capacidad anual de generación solar mediante modelos estadísticos personalizables

a. Fomentar el desarrollo de nuevas herramientas de fácil replicabilidad e implementación en la región además de las herramientas existentes “Energiza2” y “SunscanIDB”.

b. Apoyo para la aplicación de las herramientas existentes en nuevos países.

3.3 **Componente III (US$60.000):** Intercambio de Conocimiento y Diseminación. El objetivo de este componente será crear una mayor vinculación y dar mayor diseminación del conocimiento técnico y practico generado. Se financiarán las siguientes actividades:

a. Visita de aprendizaje de ministerios de energía de los países participantes de la CT a España con el fin de compartir mejores prácticas y lecciones aprendidas en temas de regulación e implementación de medidas de ciberseguridad en infraestructura crítica;

b. Diseminación de los resultados obtenidos por los productos de esta CT mediante una publicación.

3.4 **Resultados Esperados.** El valor agregado de esta cooperación técnica se centrará en: (i) la realización de autoevaluaciones de ciberseguridad y la elaboración de planes de acción; (ii) la ejecución de auditorías de ciberseguridad en instituciones clave del sector; (iii) la oferta de cursos de capacitación en ciberseguridad para fortalecer capacidades institucionales; (iv) la implementación de herramientas digitales innovadoras, incluyendo soluciones basadas en inteligencia artificial; (v) la organización de un *study tour* para funcionarios de ministerios de energía de América Latina y el Caribe (ALC) a España, con el objetivo de conocer buenas prácticas y experiencias exitosas en transformación digital del sector energético; y (vi) la diseminación de resultados mediante una publicación.

3.5 **Beneficiarios.** Los beneficiarios de esta CT son las siguientes instituciones: Centrais Elétricas de Santa Catarina (CELESC) de Brasil, Empresa Nacional de Energía Eléctrica (ENEE) de Honduras y Secretaria Nacional de Energía (SNE) de Panamá.

Presupuesto Indicativo

3.6 **Presupuesto**. Fondo General de Cooperación de España, FGE, prevé comprometer a este proyecto US$500.000.

3.7

Actividad / Componente	Descripción	BID/Financiamiento por Fondo	Financiamiento Total
1	Autoevaluación de ciberseguridad y plan de acción	$60.000	$60.000
	Auditorías de ciberseguridad	$180.000	$180.000
	Cursos de ciberseguridad	$60.000	$60.000
2	Herramientas Digitales	$140.000	$140.000
3	Study tour de ministerios de energía ALC a España	$40.000	$40.000
	Diseminación de resultados	$20.000	$20.000
	Total	$500.000	$500.000

3.8 **Monitoreo, Presentación de Informes y Supervisión**. La supervisión de la CT estará a cargo del Banco Interamericano de Desarrollo (BID) a través de su División de Energía (INE/ENE). Se coordinará con las contrapartes para designar puntos focales específicos encargados de acompañar el desarrollo de esta CT. El progreso de esta CT será monitoreado con base en sus resultados esperados, definidos en la matriz de resultados. Esta matriz también establece los indicadores y el cronograma previsto. El equipo será responsable de monitorear la evolución de estos indicadores y reportar su avance físico y financiero por producto y componente. La información requerida se registrará en Convergencia. Los informes anuales que se presenten describirán el avance hacia la finalización de cada uno de los componentes de la CT a lo largo de su duración, indicando el grado de cumplimiento de los indicadores de productos y el avance respecto a la matriz de resultados registrada en el Plan de Adquisiciones actualizado. Asimismo, se proporcionará información relevante para identificar áreas que requieran mejoras y lecciones aprendidas. Se espera que estos resultados sean complementarios a otros esfuerzos realizados por el Banco, no solo en el sector energético, sino también en infraestructura y otros sectores.

3.9 **Evaluación**. El equipo del proyecto será responsable de la preparación y envío, al Donante, de los informes del proyecto, de conformidad con lo estipulado en el Acuerdo de Administración.

IV. Agencia Ejecutora y estructura de ejecución

4.1 **El Organismo Ejecutor** será el Banco Interamericano de Desarrollo (BID), a solicitud de los beneficiarios, y de acuerdo con las directrices y requisitos establecidos en la Política de Cooperación Técnica (GN-2470-2) y en los Procedimientos para la tramitación de operaciones de cooperación técnica y asuntos conexos (OP-619-4), a través de la División de Energía (INE/ENE).

4.2 **Capacidad Institucional.** Esta CT es de carácter regional, y el Banco cuenta con una amplia experiencia y capacidad para convocar y coordinar a los distintos actores de los países involucrados, lo cual es fundamental para el éxito del proyecto. El BID ha liderado múltiples iniciativas regionales en ciberseguridad y transformación digital, incluyendo la ejecución de la CT RG-T4513, que sentó las bases técnicas y metodológicas que ahora se amplían con esta operación. El Banco ha desarrollado herramientas, como metodologías de autoevaluación y plataformas digitales, y ha establecido alianzas estratégicas con actores clave del ecosistema digital y energético, lo que le permite brindar acompañamiento técnico efectivo durante toda la ejecución de la CT incluyendo también la capacitación en ciberseguridad.

4.3 **Adquisiciones.** Todas las adquisiciones a ejecutarse bajo esta Cooperación Técnica han sido incluidas en el Plan de Adquisiciones (Anexo IV) y se contrataran de conformidad con las políticas y regulaciones aplicables del Banco de la siguiente manera: (a) Contratación de consultores individuales, según lo establecido en la norma sobre Fuerza Laboral Complementaria (AM-650) y (b) Contratación de servicios prestados por firmas consultoras de acuerdo con la Política de Adquisiciones Institucionales (GN-2303-33) y sus Directrices.

4.4 **Periodo de Ejecución y Desembolso**. Los fondos de esta operación se destinarán a la contratación de servicios de consultoría. Está previsto que estas actividades se completen dentro de los 36 meses posteriores a la aprobación de la CT

V. Riesgos importantes

5.1 No se anticipan riesgos mayores para esta CT.

5.2 **Propiedad Intelectual.** En el marco de esta cooperación técnica, se desarrollarán herramientas digitales cuyo licenciamiento garantizará la plena titularidad de los derechos de propiedad intelectual del BID, conforme a lo establecido en la política AM-331. Para ello, las consultorías transferirán todos los derechos necesarios para modificar, adaptar, personalizar, usar, mantener y redistribuir el sistema desarrollado. Esta transferencia incluye el acceso irrestricto al código fuente y a todos los artefactos técnicos asociados (documentación, librerías, esquemas de base de datos, entre otros), permitiendo al BID realizar mejoras continuas, desarrollar nuevas funcionalidades y asegurar la sostenibilidad del sistema en el tiempo. El código fuente de sistema desarrollados con esta CT, debidamente probados y validados en cuanto al cumplimiento de requerimientos funcionales, de escalabilidad y de manejo eficiente de datos, será almacenado en el repositorio de código proporcionado por el BID. Las consultorías se comprometen a garantizar que todas las entregas se realicen libres de derechos de terceros, y que el software no infringe patentes, licencias restrictivas ni otras disposiciones legales vigentes. Además, se establecerán mecanismos de verificación y control de calidad del código, así como buenas prácticas de documentación técnica, para facilitar su adopción futura por parte del Banco u otros actores autorizados. Estos lineamientos aseguran que los productos derivados de esta cooperación técnica sean plenamente reutilizables y sostenibles, consolidando su valor como bien público regional.

VI. Excepciones a las políticas del Banco

6.1 No se identifican excepciones a las políticas del Banco.

VII. Aspectos Ambientales y Sociales

7.1 Esta Cooperación Técnica no está destinada a financiar estudios de prefactibilidad o factibilidad de proyectos de inversión específicos o estudios ambientales y sociales asociados a ellos; por lo tanto, esta TC no tiene requisitos aplicables del Marco de Política Ambiental y Social (ESPF, por sus siglas en inglés) del Banco.

Anexos Requeridos:

Solicitud del Cliente_2427.pdf

Matriz de Resultados_86817.pdf

Términos de Referencia_89288.pdf

Plan de Adquisiciones_14204.pdf