Documento de Cooperación Técnica

I. Información Básica de la CT

▪ País/Región:	GUATEMALA
▪ Nombre de la CT:	Respuesta a ciberataques y mejora de la ciberseguridad en el Ministerio de Finanzas Públicas de Guatemala
▪ Número de CT:	GU-T1359
▪ Jefe de Equipo/Miembros:	Nowersztern, Ariel (IFD/ICS) Líder del Equipo; Barragan Crespo, Enrique Ignacio (LEG/SGO); Grayeb Bayata, Claudia (CID/CME); Larrazabal, Luis Bernal (CID/CGU); Martinez, Ynty Koyllor (IFD/ICS); Schaeffer Cabrera, Maria Jose (IFD/ICS); Bordese Maria Paula (IFD/ICS); Rivera Arteaga, Cesar Augusto (IFD/ICS); Restrepo Restrepo Andres De Jesus (CID/CGU); Calderon Ramirez, Ana Cristina (IFD/FMM); Paz Gonzalez, Santiago (IFD/ICS)
▪ Taxonomía:	Apoyo al Cliente
▪ Operación a la que la CT apoyará:	No Aplica
▪ Fecha de Autorización del Abstracto de CT:	6 Feb 2024
▪ Beneficiario:	Ministerio de Finanzas Públicas de Guatemala
▪ 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$400,000.00
▪ Contrapartida Local, si hay:	US$0
▪ Periodo de Desembolso (incluye periodo de ejecución):	36 meses
▪ Fecha de inicio requerido:	Octubre de 2024
▪ Tipos de consultores:	Consultores Individuales y Firmas
▪ Unidad de Preparación:	IFD/ICS-División de Innovación para Servir al Ciudadano
▪ Unidad Responsable de Desembolso:	CID/CGU-Representación Guatemala
▪ 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 2024-2030:	Capacidad institucional y estado de derecho

II. Objetivos y Justificación de la CT

2.1 **Objetivo**. Esta Cooperación Técnica (CT) tiene como objetivo asistir al Ministerio de Finanzas Públicas (MINFIN) de Guatemala en la respuesta a ciberataques y en el fortalecimiento de su ciberseguridad[1]. Los objetivos específicos de esta CT son proporcionar asistencia técnica al MINFIN en: (i) la respuesta técnica y el análisis de ciberataques recientes, incluyendo la identificación de evidencia potencial, su adquisición, análisis forense, producción y presentación de informes; y (ii) el fortalecimiento de la ciberseguridad del MINFIN a través de servicios y herramientas

[1] Según la Unión Internacional de Telecomunicaciones (UIT), la ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardias de seguridad, directrices, enfoques de gestión de riesgos, acciones, formación, mejores prácticas, garantías y tecnologías que pueden utilizarse para proteger el entorno cibernético y los activos de las organizaciones y los usuarios.

profesionales para analizar la postura actual de ciberseguridad, actualizar las políticas de ciberseguridad, proteger y monitorear los sistemas, detectar, responder y recuperarse de incidentes cibernéticos.

2.2 **Justificación**. El creciente uso de las Tecnologías de la Información y las Comunicaciones (TIC) en América Latina y el Caribe (ALC) es un catalizador para el progreso económico y social; sin embargo, introduce riesgos inherentes a la ciberseguridad que deben ser gestionados de forma continua, ya que de lo contrario la seguridad ciudadana y la confianza pública en las TIC, incluyendo la confianza de los consumidores en las transacciones en línea y el acceso a los servicios públicos digitales, pueden verse afectados negativamente. Así pues, reforzar la ciberseguridad es esencial para salvaguardar los derechos de los ciudadanos en la esfera digital, como la privacidad y la propiedad, para promover la confianza de los ciudadanos en las tecnologías digitales y para apoyar el crecimiento económico a través de una transformación digital segura. Los ciudadanos deben tener la seguridad de que los sistemas digitales que utilizan para sus actividades personales o profesionales, así como aquellos en los que se involucran sus datos personales, cuentan con las medidas de seguridad adecuadas para garantizar la integridad, confidencialidad y disponibilidad de su información y de los servicios de los que dependen.

2.3 En este contexto, estar preparados y saber a qué atenernos es fundamental. El Banco Interamericano de Desarrollo (BID) lleva a cabo evaluaciones para captar la evolución de las capacidades de sus Estados miembros para defenderse de las crecientes amenazas en el ciberespacio. El Reporte Regional de Madurez en Ciberseguridad 2020: "Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe", desarrollado en colaboración con la Organización de Estados Americanos (OEA), mostró que los países se encontraban en diferentes etapas de desarrollo en su preparación para hacer frente a los desafíos de ciberseguridad, pero en general todavía tenían un amplio margen de mejora. En el caso de Guatemala, su madurez en políticas públicas de ciberseguridad a lo largo de 53 indicadores fue valorada en menos de 2.0 sobre 5.0 puntos, en promedio. Específicamente, Guatemala ha aprobado una Estrategia Nacional de Ciberseguridad en 2018; sin embargo, sus objetivos y plan de acción aún no se han realizado en su totalidad. En 2019, Guatemala aprobó una Ley de Ciberdelincuencia. Guatemala no cuenta con una agencia de ciberseguridad a nivel nacional ni con un plan de protección de infraestructuras críticas. En este contexto, el gobierno tiene una capacidad limitada para prevenir, detectar y responder a los ciberataques.

2.4 Estas vulnerabilidades de ciberseguridad subyacentes dan lugar ocasionalmente a ataques de ciberseguridad de gran repercusión. A finales de noviembre de 2023, el MINFIN anunció que había sufrido un ciberataque que afectó la disponibilidad de parte de su información y sistemas. Algunos de los principales sistemas de información del MINFIN incluyen SICOIN (Sistema de Contabilidad Integrada), utilizado para gestionar los pagos y cuentas del gobierno, GuateCompras, utilizado para gestionar las compras del gobierno, y Guatenominas, utilizado para gestionar los salarios del gobierno. Como es de esperarse, la menor disponibilidad de estos sistemas afectó el cumplimiento ordenado de los procesos financieros del gobierno y la confianza en su estabilidad continua.

2.5 El problema específico atendido por este programa es apoyar la acción continua del MINFIN para controlar el riesgo cibernético a sus datos, sistemas y procesos de negocio. Los eventos de noviembre 2023, así como incidentes cibernéticos sufridos por otros gobiernos de LAC e internacionalmente, muestran que el MINFIN no es

exento al potencial de daño a sistemas, datos y procesos gubernamentales en caso de un incidente cibernético. Un análisis reciente de las capacidades de ciberseguridad del MINFIN realizado por el BID identifica un número de recomendaciones de mejora, clasificando las recomendaciones por su nivel de riesgo, complejidad y costo de implementación, así como en una de 17 áreas profesionales de actuación. Siguiendo metodologías internacionales de ciberseguridad, ese análisis identifica factores determinantes del nivel de ciberseguridad del MINFIN en esas áreas de actuación según su potencial de mejora, y estima el nivel consolidado de riesgo organizacional. Cada factor determinante cuenta con recomendaciones específicas para implementación, según mejores prácticas profesionales, para mejorar las capacidades de control de riesgos digitales. Los hallazgos y recomendaciones de ese análisis informan la preparación y ejecución de este programa de cooperación técnica.

2.6 El BID ha respondido a los desafíos de ciberseguridad en ALC con una serie de esfuerzos de desarrollo de capacidades, incluyendo operaciones de préstamo y asistencia técnica específica. Guatemala se ha beneficiado de actividades regionales de desarrollo de capacidades como el estudio regional de madurez en ciberseguridad del BID-OEA, el curso de Liderazgo Nacional en Ciberseguridad del BID, eventos regionales y subregionales y cursos de estudio sobre cibercrimen y ciberseguridad para investigadores, aduanas, prisiones, entre otros.

2.7 El BID se encuentra en una posición única para apoyar el desarrollo de capacidades en ciberseguridad del MINFIN, dados nuestros proyectos de inversión y asistencia técnica en curso, y un historial comprobado en lo que respecta al aprovechamiento del apoyo técnico de los países más avanzados en ciberseguridad en todo el mundo. Por ejemplo, el gobierno de Israel ha apoyado la capacidad en ciberseguridad a lo largo de toda América Latina desde 2016 y actualmente participa ofreciendo acceso a los profesionales de ciberseguridad de la región a la capacitación, el conocimiento, la experiencia y las mejores prácticas más avanzadas a nivel mundial (RG-T2788, RG-T4010). El ámbito de Japón, Corea y España también augura lecciones significativas y apoyo técnico en capacidad estatal y coproducción de ciberseguridad (TT-T1137, SU-T1158, RG-T4172, RG-T3024 y RG-T3741). Las lecciones aprendidas de proyectos anteriores incluyen la importancia del protagonismo del beneficiario mediante su equipo TIC y la importancia de especificaciones exactas y acordadas para los contratos. En caso del MINFIN su equipo TIC es altamente comprometido a la ejecución del proyecto y se acordaron procesos para asegurar la calidad de las especificaciones para el cumplimiento de los productos esperados en la implementación de esta cooperación técnica.

2.8 **Alineación estratégica.** La CT es consistente con la Estrategia Institucional del Grupo BID: Transformación para una Mayor Escala e Impacto (CA-631) y se alinea con el objetivo de impulsar el crecimiento regional sostenible al promover la inversión en infraestructura digital sostenible. La CT también se alinea con las siguientes áreas de enfoque operativo: Capacidad institucional, Estado de derecho y seguridad, contribuyendo a la transformación digital del sector público; e Infraestructura sostenible, resiliente e inclusiva, fomentando la mejora en la infraestructura digital fortaleciendo las capacidades del Ministerio de finanzas Públicas. Asimismo, se alinea al área prioritaria de “Instituciones eficaces, eficientes y transparentes” (W2C) del Programa Estratégico para el Desarrollo Financiado con Capital Ordinario (GN 2819 14) y a la Estrategia de País.

III. Descripción de las actividades/componentes y presupuesto

La CT cuenta con dos componentes:

3.1 **Componente 1: Respuesta y Análisis de Ciberataques (USD 300,000).** Este componente apoyará la respuesta técnica, análisis e investigación de ciberataques ocurridos recientemente, incluyendo: (i) la identificación de evidencia potencial, su adquisición, análisis forense, producción y presentación de informes; (ii) análisis de los sistemas del MINFIN para determinar los datos técnicos de estos incidentes, vulnerabilidades potenciales de ciberseguridad involucradas, impactos potenciales a la confidencialidad, integridad y disponibilidad de los sistemas; y (iii) recomendar pasos inmediatos de mejora basados en los hallazgos, apoyando la recuperación completa del MINFIN, la prevención de recurrencias futuras y su preparación.

3.2 En este componente se estarán ejecutando 2 consultorías realizadas por empresas e individuales, las cuales apoyarán el MINFIN realizando actividades como la identificación y reportaje de evidencia potencial, análisis de datos técnicos de incidentes y de vulnerabilidades potenciales de ciberseguridad, así como el apoyo a la remediación, endurecimiento de sistemas y la mejora de la preparación ante posibles futuros incidentes, para reducir y mitigar impactos potenciales a la confidencialidad, integridad y disponibilidad de los datos y los sistemas.

3.3 **Componente 2: Fortalecimiento de la Ciberseguridad del MINFIN (USD 100,000).** Este componente proporcionará servicios profesionales y herramientas para analizar la situación actual del MINFIN en materia de ciberseguridad, ofrecer diagnósticos detallados, recomendaciones, políticas actualizadas de ciberseguridad, planes de corrección y acción y apoyo continuo para mejorar las capacidades preventivas del MINFIN, incluidas la protección y supervisión de los sistemas, así como también para reforzar sus capacidades profesionales del personal a través de actividades como capacitaciones especializadas, elaboración de manuales técnicos, y reforzar las capacidades de detección, respuesta y recuperación en caso de incidentes cibernéticos.

3.4 En este componente se estarán financiando 2 consultorías, realizadas por empresas e individuales, las cuales apoyarán la implementación y adaptación de estándares avanzados de ciberseguridad así como la de implementación de medidas de protección, monitoreo, detección, y gestión de incidentes cibernéticos.

3.5 El costo total requerido de la CT es de USD 400.000,00 a ser financiado por la Ventanilla 2, Área prioritaria 3: Instituciones eficaces, eficientes y transparentes (W2C) del Programa Estratégico para el Desarrollo Financiado con Capital Ordinario (OC-SDP) de acuerdo con el siguiente presupuesto.

Presupuesto Indicativo (US$)

Actividad / Componente	Descripción	BID/Financiamiento por Fondo	Contrapartida Local	Financiamiento Total
Respuesta y análisis de ciberataques	Apoyará la respuesta técnica, análisis e investigación de ciberataques ocurridos en MINFIN	**300,000**	**0**	**300,000**
Refuerzo de la ciberseguridad del MINFIN	Proporcionará servicios profesionales y herramientas para analizar y reforzar la	**100,000**	**0**	**100,000**

	situación actual del MINFIN en materia de ciberseguridad			
Total		**400,000**	**0**	**400,000**

3.6 En la ejecución de esta cooperación técnica, tanto los beneficiarios directos como los finales son el Ministerio de Finanzas Públicas, ya que se fortalecerán los sistemas de ciberseguridad y las capacidades del personal para evitar ataques cibernéticos y disminuir los riesgos informáticos, mejorando la preparación frente a futuros incidentes que pudieran afectar sus sistemas.

3.7 **Resultados esperados**. Con respecto a los resultados de esta CT, se espera que el MINFIN fortalezca su capacidad para prevenir, detectar, responder y recuperar futuros incidentes cibernéticos, así minimizando los riesgos digitales y protegiendo sus sistemas, datos y procesos de negocio. Para ese fin, se espera implementar 4 o más medidas avanzadas de ciberseguridad, incluyendo la adaptación de reglamentos y procesos internos, la aplicación de tecnologías y la capacitación del personal correspondiente.

3.8 **Monitoreo**. La CT será supervisada por la División de Innovación para Servir al Ciudadano (IFD/ICS). El equipo de proyecto será responsable de la supervisión, monitoreo y evaluación de la CT. El equipo de proyecto elaborará los informes anuales de progreso de los indicadores de la CT. La Unidad Responsable para los Desembolsos (UDR) estará en la Representación del Banco en Guatemala. La supervisión se hará de forma continua, revisando productos de consultoría intermedios y finales, y mediante al menos dos reuniones anuales con las áreas de gobierno nacional o jurisdiccionales para revisar el desarrollo de las diferentes consultorías.

IV. Agencia Ejecutora y estructura de ejecución

4.1 **Organismo Ejecutor**. A solicitud del Gobierno de Guatemala, este proyecto será ejecutado directamente por el Banco, a través de la División de Innovación para Servir al Ciudadano (IFD/ICS), en coordinación con la oficina de país de Guatemala y la División de Gestión Fiscal (IFD/FMM). Asimismo, FMM es un socio y aliado estratégico en esta cooperación, dado que trabaja directamente con el Ministerio de Hacienda, apoyándole en la modernización de procesos, plataformas y transformación. El rol de FMM en la ejecución del proyecto incluirá el asesoramiento técnico en la implementación de nuevas tecnologías y procesos de modernización. Se coordinarán reuniones periódicas con FMM para asegurar que los insumos en temas de ciberseguridad sean tenidos en cuenta y priorizados. Además, FMM participará en la capacitación del personal del Ministerio de Hacienda en nuevas plataformas y herramientas tecnológicas, y colaborará en el monitoreo y evaluación de los avances del proyecto, asegurando que se cumplan los objetivos de transparencia, seguimiento y confianza en los datos. Estas actividades específicas garantizarán una coordinación efectiva con FMM, priorizando la ciberseguridad como un elemento clave para un mejor manejo de los recursos públicos, lo cual es fundamental para una gestión fiscal eficiente. El MINFIN solicita que el BID ejecute esta asistencia técnica por medio de sus especialistas en ciberseguridad. La ejecución por el BID se justifica por dos razones de acuerdo al numeral 2.2 Anexo II de OP-619-4: (a) Por motivo de los desafíos que tienen las entidades de gobierno de

Guatemala para ejecutar cooperaciones técnicas, todas las CTs que benefician al gobierno son ejecutadas por el Banco; y (b) El conocimiento especializado en ciertos aspectos de ciberseguridad requeridos para la ejecución existe en el BID, mientras el equipo informático del MINFIN va a ser reforzado en esos aspectos. IFD/ICS tiene una amplia y reciente experiencia en la prestación de asistencia técnica en ciberseguridad al sector público en ALC, incluyendo el fortalecimiento de las capacidades de ciberseguridad en las organizaciones, y en la respuesta a incidentes, por lo que está mejor equipada para gestionar esta operación y asegurar la coordinación necesaria. La CT se implementará a lo largo de 36 meses.

4.2 Como organismo ejecutor de la CT, el Banco será responsable de: (i) identificar los estudios y trabajos técnicos necesarios para la realización de la CT; (ii) seleccionar y contratar consultores para brindar los servicios necesarios; (iii) supervisar los servicios de consultoría a los que el beneficiario brinda insumos técnicos; y (iv) gestionar la ejecución y prestación de servicios de consultoría.

4.3 **Adquisiciones**. Las actividades por ejecutar en el marco de esta operación se incluirán en el Plan de Adquisiciones y serán ejecutadas de acuerdo con los métodos de adquisiciones establecidos por el Banco. Específicamente, los Lineamientos para Empleados de la Fuerza Laboral Complementaria con Financiamiento Externo (AM-650), la Política de Adquisiciones Institucionales (GN-2303-33) y sus directrices asociadas para la contratación de firmas consultoras para servicios de naturaleza intelectual y la contratación de servicios logísticos y otros servicios distintos a consultoría.

V. Riesgos importantes

5.1 El principal riesgo está relacionado con la magnitud desconocida y variable de los servicios profesionales necesarios para alcanzar los objetivos del proyecto, los cuales dependerán de los resultados. Para mitigar este riesgo, se adoptaría un modelo de contratación por fases modulares en el que los paquetes de trabajo se definirían y aprobarían gradualmente. También existe el riesgo de obtener pleno acceso a la información y los sistemas pertinentes para llevar a cabo el análisis y su posterior corrección. Para mitigarlo, el proyecto colaborará estrechamente con las contrapartes gubernamentales de nivel directivo y técnico para proporcionar esta asistencia.

VI. Excepciones a las políticas del Banco

6.1 Esta operación no prevé ninguna excepción a la política 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 CT no tiene requisitos aplicables del Marco de Política Ambiental y Social (MPAS) del Banco.

Anexos Requeridos:

Solicitud del Cliente_24479.pdf

Matriz de Resultados_96492.pdf

Términos de Referencia_11361.pdf

Plan de Adquisiciones_76827.pdf