Términos de Referencia
Asistencia Técnica de Corto Plazo de Empresa de Tecnología con experiencia en ciberseguridad para
"Fortalecer el Plan de Contingencia Regional en materia de Ciberseguridad"

1. Antecedentes

El proyecto de Apoyo al Diseño e Implementación de la PDCC se ejecutó desde marzo 2018 hasta diciembre de 2022. El primer trimestre de 2019 se suscribió el Acuerdo de Adopción del Modelo de la PDCC, el cual incluye 67 procesos institucionales que involucran a las 71 funcionalidades de la PDCC los cuales pueden ser unificadas y/o anidadas. El proyecto de la PDCC finalizó con la plataforma desarrollada de conformidad al modelo acordado (71 funcionalidades).

Basado en lo anterior, para asegurar la adecuada utilización de la plataforma se planteó un conjunto de actividades para el Fortalecimiento y Ampliación de la Plataforma Digital de Comercio Centroamericana (PDCC2.0) para la Facilitación del Comercio, dirigidas en forma general a lo siguiente:

- Consolidar la adopción y uso de la PDCC desarrollada, para alcanzar el compromiso de cada país al 100% en su implementación.
- Escalar la capacidad de la PDCC incorporando módulos de automatización y trazabilidad relacionados con el Arancel Informatizado Centroamericano, el comercio extrarregional con otros socios comerciales y comercio multimodal.
- Fortalecer la gestión de seguridad informática y de servicios tecnológicos de las instituciones nacionales involucradas en la PDCC.
- Socializar, divulgar y fortalecer las competencias de los agentes económicos y otros socios internacionales en la utilización efectiva de las funcionalidades de la PDCC y el SGIRR.
- Avanzar en esquemas de interoperabilidad con otras plataformas informáticas regionales de comercio administradas por la SIECA.

2. Descripción General del Proyecto de Fortalecimiento y Ampliación de la PDCC (PDCC2.0) para la Facilitación de Comercio

El proyecto de la PDCC2.0 es apoyado por la Unión Europea y se ejecuta en forma directa con la SIECA y a través de dos componentes: b) Acuerdo de subvención directa "Fortalecimiento de la Plataforma Digital de Comercio para la facilitación del comercio (PDCC II)" ND1CI LA/2022/436-197 – Componente SIECA.

Objetivo General/Impacto, es Fortalecer la Integración Económica Regional Centroamericana y maximizar los beneficios del Acuerdo de Asociación (AACUE), mediante el uso de instrumentos digitales de interoperabilidad de procesos y de los sistemas nacionales y regionales, incluyendo la consolidación de la PDCC y el SGIRR.

Objetivo de la Cooperación Técnica No Reembolsable ATN/ER-19855-RG-T4217 – Componente BID: Fortalecer la integración económica regional en Centroamérica, mediante el uso de instrumentos digitales de interoperabilidad entre sistemas nacionales y regionales centrados en consolidar la implementación y uso de la PDCC. Los objetivos específicos son: (i) fortalecer las funcionalidades de la PDCC, su interoperabilidad y el uso de la plataforma como un sistema regional

consolidado de servicios y/o procesos conexos al comercio intra y extrarregional; y (ii) implementar desarrollos conexos para ampliar capacidades de la PDCC.

Objetivo del Acuerdo de subvención directa ND1CI LA/2022/436-197 – Componente SIECA: Facilitar y fortalecer el intercambio comercial en CA mediante el uso de la PDCC y el SGIRR. Asimismo, la seguridad de la información y capacidades técnicas en las instituciones nacionales; con dos resultados esperados establecidos.

Temporalidad de ejecución: El proyecto tiene una temporalidad de 36 meses (3 años)

3. Justificación y contexto de la contratación

El Organismo Ejecutor (OE) del proyecto, tanto del Componente BID CT ATN/ER-19855-RG y Componente de Subvención SIECA/UE, es la Secretaría de Integración Económica Centroamericana (SIECA) que, debido a la complejidad y magnitud del proyecto, dentro de la estructura interna del OE para una eficiente ejecución del Proyecto se requiere la contratación de Técnicos Informático para el fortalecimiento de la PDCC.

La contratación responde a los compromisos establecidos en el marco lógico del proyecto de subvención (Gestión Directa), el cual establece en el Objetivo Específico 1 (OE1), indicador 1: Un Plan de Contingencia regional en materia de ciberseguridad fortalecido con apoyo de los países interesados.

En el marco del proyecto PDCC 1 Fase, el 17 de agosto de 2022 se desarrolló el Taller Centroamericano sobre seguridad de Información en Aduanas y Pasos de Frontera en Guatemala, con la participación de autoridades de Aduanas y agencias conexas de comercio exterior de la región, como parte de una iniciativa conjunta entre la Secretaría de Integración Económica Centroamericana (SIECA) y el Banco Interamericano de Desarrollo (BID). El Taller tuvo como objetivo sensibilizar y dimensionar los desafíos que Centroamérica enfrenta en materia de seguridad de la información para la gestión del comercio intra y extrarregional. En particular, se buscó iniciar la identificación de brechas nacionales y/o regionales que deban atenderse para fortalecer la ciberseguridad aduanera a través de una combinación adecuada de creación de capacidades, herramientas tecnológicas y protocolos en el contexto de buenas prácticas internacionales.

Durante el Taller se acordó que este tema podría ser incorporado en la Agenda del Comité Aduanero Centroamericano con la idea de crear una Mesa Técnica de ciberseguridad de la información que avance en la elaboración de la hoja de ruta con la asistencia técnica de la SIECA y, eventualmente, del BID.

Con el lanzamiento de la PDCC el pasado 28 de noviembre del 2023 se determinó la necesidad de ampliar la ciberseguridad de la plataforma por medio del fortalecimiento de los mecanismos incluidos en un plan de ciberseguridad, mediante la contratación de una consultoría “Fortalecer el Plan de Contingencia Regional en materia de Ciberseguridad”, asistencia técnica que tendrá como línea base los temas abordados y acuerdos establecidos en dicho taller.

La PDCC 2.0 que fortalece las operaciones de la PDCC por medio de la conectividad de otras plataformas preparando el intercambio de información con sistemas nacionales expondrá más información de estas operaciones principalmente en materia de comercio relacionadas con agencias de aduana de los países centroamericanos por lo que es importante fortalecer los planes de

contingencia y ciberseguridad no solo de las instituciones, sino que apliquen a la infraestructura y operaciones de la PDCC.

Asimismo, de acuerdo al análisis de vulnerabilidad realizado a la PDCC, en su fase 1 por SECPRO, existen oportunidades para fortalecer la seguridad de la PDCC atendiendo las sugerencias de mejoras y adecuaciones de la infraestructura como la creación de planes que apoyen a la continuidad de las operaciones en situaciones de -ciberseguridad y con esto garantizar la disponibilidad de todo el sistema en cuanto a los aspectos de seguridad perimetral de la Nube donde se tiene instalada la infraestructura. A su vez, la confidencialidad e integridad y disponibilidad de la información, en el escenario que se combinen con otros vectores de ataques que involucren interacción directa con usuarios legítimos del sistema y plataformas regionales que interactúan con la PDCC.

4. Objetivos de la Asistencia Técnicas

Objetivo general

Fortalecer el Plan de Contingencia Regional en materia de ciberseguridad en coordinación con los países, desarrollado por los grupos técnicos normativo e informático de aduanas.

Objetivos específicos

a. El Plan de Contingencia Regional Centroamericano actual y los resultados del taller de ciberseguridad realizado el 22 de agosto de 2022, analizado
b. Las brechas y oportunidades por país, identificadas.
c. El Plan de Contingencia Regional Centroamericano fortalecido, por medio de la adición de acciones para atender situaciones relacionadas a la seguridad de la información regional, basado en los siguientes ejes:
    i. Fomentar una cultura de ciberseguridad.
    ii. Desarrollar las capacidades de los funcionarios de informática de las instituciones involucradas.
    iii. Definir Infraestructuras críticas.
    iv. Definir Estándares técnicos y de desarrollo utilizando las mejores prácticas de la industria.
d. Las acciones a implementar para robustecer y garantizar las transmisiones electrónicas, de la PDCC con relación a las DUCA-T y DUCA-F y de los sistemas informáticos involucrados en estas operaciones que transfieren datos a través del bus regional de interoperabilidad, en materia de seguridad de la información, identificadas.
e. Los lineamientos que permitan a los países y la SIECA, contar con un marco para atención de incidencias relacionadas con el tema de ciberseguridad, establecidos y aplicable a la PDCC
f. La metodología de creación del CSIRT (Computer Security Incident Response Team – Equipo de Respuesta a Incidentes de Seguridad Informática) regional recomendada.

5. Alcance de la Asistencia Técnica:

El Alcance de la Asistencia Técnica requerida es fortalecer el Plan de Contingencia Regional en materia de ciberseguridad en coordinación con los países en las instituciones de Aduanas debido a que son las instituciones que procesan la información de comercio y documentación de soporte dentro del proceso a nivel regional, tomando como línea base, el Plan Regional de contingencia actual, los resultados del Taller Centroamericano sobre seguridad de Información en Aduanas y

Pasos de Frontera en Guatemala realizado el 17 de agosto de 2022 y el análisis de vulnerabilidad realizado a la PDCC.

6. Actividades de la Asistencia Técnica:

A continuación, se presentan las actividades establecidas de acuerdo con lo que se estima necesario para cumplir con el objetivo. Inicialmente deberán presentar un plan de trabajo con cronograma a los 15 días después de la firma del contrato, el cual no genera pago de honorarios.

Se presentan las actividades por medio de un cronograma indicativo en el cual se presenta el tiempo previsto para cada actividad dentro de la consultoría, esto con el fin de orientar la presentación de la propuesta técnica.

ACTIVIDADES GENERALES	MES 1.	MES 2.	MES 3.	MES 4.	MES 5.
Levantamiento de información sobre la infraestructura de ciberseguridad de cada país.	X				
Revisión de la documentación actual. En caso de que no esté alineada con ninguna normativa específica, se debe definir la normativa adecuada como ISO 27001, NIST, entre otras y alinear la documentación y procesos con los requisitos de la normativa seleccionada.	X				
Entrevistas a autoridades sobre incidentes de ciberseguridad pasados y mecanismos actuales		X			
Identificación y documentación de activos informáticos críticos y escenarios de vulnerabilidad		X			
Análisis y elaboración del Informe de Brechas			X		
Diseño del procedimiento de actuación ante incidentes de ciberseguridad			X		
Diseño del modelo de establecimiento y operación del CSIRT regional			X		
Elaboración del análisis de costos de las actividades de ciberseguridad propuestas				X	
Elaboración de recomendaciones para prevención de ataques y continuidad del negocio				X	
Desarrollo del Plan de Continuidad de Negocio y Recuperación ante Incidentes					X
Redacción del informe final de la consultoría					X

ACTIVIDADES GENERALES	MES 1.	MES 2.	MES 3.	MES 4.	MES 5.
Preparación y realización de la presentación del informe final a autoridades					X

7. Productos esperados y cronograma de pagos

Producto o entregable	Descripción
Plan de contingencias regional actualizado	En este plan se debe incluir el informe actual de la región y el plan de contingencia sobre los temas de ciberseguridad y se debe contemplar una sección o anexo sobre la atención ante los eventos de ciberseguridad.
Documento que defina el Procedimiento que describa la forma de establecer un CSIRT y la manera de actuar por parte de una o varias autoridades nacionales o la SIECA, ante un incidente de ciberseguridad donde se vea vulnerado o comprometido el funcionamiento de los sistemas informáticos. Informe de análisis de brecha para alcanzar la propuesta de mejora en continuidad de negocio.	Presentar un protocolo de los pasos a seguir en caso se materialice algún riesgo identificado en los activos informáticos que incluya la gobernanza del CSIRT a nivel regional. El informe de brechas debe contener costos, actividades y normativa.
Documento que defina el Procedimiento de prevención de ciberataques basado en las mejores prácticas internacionales de la industria a nivel de seguridad informática que ayude a evitar incidentes de infraestructura informática de los servicios de autoridades nacionales y de la SIECA. Informe final de la consultoría.	El procedimiento de prevención y mitigación de ciberataques, aprobado por los directores de aduanas y las recomendaciones normativas que impliquen los procedimientos.

Es obligación de la empresa presentar los productos de óptima calidad conforme a los parámetros de calidad establecidos en el medio. El trabajo deberá contar con el contenido y la cantidad de información necesaria para lograr una óptima comprensión y calidad de los objetivos establecidos.

8. Tipo de contrato, temporalidad y forma de pago

Empresa de tecnología de la información que provea lo solicitado en la sección de productos esperados en un período de 5 meses. Posterior a la firma del contrato.

Los pagos se realizarán por transferencia bancaria y posterior a la entrega de factura original **a nombre de SIECA/PDCC-2.0 número de NIT: 636007-6 e** informe mensual de actividades debidamente aprobado por el Director de Tecnologías de la Información y Comunicación. Todos los productos/entregable indicado en el numeral 6. deberán estar revisados y aprobados técnicamente por el Director de Tecnologías de la Información y Comunicación y la gestión de pago será gestionada a través de la Dirección de Cooperación y Proyectos.

La fuente de financiamiento corresponde a recursos financieros de Subvención directa de la Unión Europea (UE) convenio No ND1CI LA/2022/436-197. Los pagos se realizarán en dólares norteamericanos, por medio de transferencia bancaria a través de la SIECA**,** contra presentación de factura original expresada en dólares o en quetzales (tipo de cambio oficial del día proporcionado por la SIECA)**.** El profesional contratado deberá contar con una cuenta en dólares y asumirá los costos financieros de transferencia internacional, si fuera el caso. El pago de impuestos, costos financieros y administrativos en que se incurran por cualquier concepto durante la consultoría contratada, son responsabilidad de cada consultor(a).

La empresa contratada y su régimen sea ***general,*** se le extenderá una constancia de exención de IVA, caso contrario, la empresa deberá asumir los impuestos que apliquen de acuerdo con el régimen en que se encuentre inscrito (aplicable para empresas guatemaltecas).

9. Sede y coordinación de la contratación

La empresa por contratar deberá proporcionar sus servicios de forma remota.

Todas las actividades por desarrollar dentro de la contratación deberán ser coordinadas y notificadas a la Dirección de Tecnologías de las Información y Comunicación.

10. Perfil de la empresa a contratar

- ✓ Experiencia individual e indivisible de la empresa comprobable de al menos 10 años en el mercado en implementación de infraestructura tecnológica.
- ✓ Experiencia individual e indivisible de la empresa comprobable de al menos 5 años en ciberseguridad.

11. Perfil del personal clave:

- Formación académica: (presentar atestados correspondientes)

✓ Al menos 2 Ingeniero/Licenciatura en Sistemas de Información y Ciencias de la Computación o carreras afines (Ingeniería/Licenciatura Telecomunicaciones, Electrónica, otros).

✓ Al menos 2 profesionales que cuenten con 2 de las siguientes Certificaciones

- Certified System Auditor CRISC
- Certified System Auditor CISA
- Certified System Auditor CISM

- Certified Information Systems Security Professional CISSP
- Lead Cybersecurity Proffesional Certificate LCSPC

12. Forma de Postulación

Enviar la siguiente documentación al correo electrónico adquisiciones@sieca.int asunto "**Fortalecer el Plan de Contingencia Regional en materia de Ciberseguridad**" más tardar el 15 de diciembre de 2025 a las 24 horas:

- Carta de expresión de interés, que explique en detalle la información sobre: experiencia profesional, formación académica de los profesionales clave, conocimientos y habilidades adquiridas relevantes para la consultoría y que acepta los requisitos definidos en estos Términos de Referencia (máximo 1 página).
- Hoja de vida de la empresa
- Representación legal.
- Copia Documento de identificación del representante legal.
- Copia Documento de registro tributario.
- Copia Patente de comercio y sociedad.
- Copia de escritura constitutiva.

13. consultas y aclaraciones

Para comunicación de consultas y aclaraciones sobre los términos de referencia y el proceso correspondiente de selección, se podrán comunicar al correo adquisiciones@sieca.int antes del de noviembre del 2025.

14. Criterios de evaluación

CRITERIOS DE BASE DE CUMPLIMIENTO		
CITERIO	**CUMPLE**	**NO CUMPLE**
Experiencia individual e indivisible de la empresa comprobable de al menos 10 años en el mercado en implementación de infraestructura tecnológica *(patente o registro comercial de la empresa)*	X	
Experiencia individual e indivisible de la empresa comprobable de al menos 5 años en ciberseguridad. *(medio de verificación: cartas de recomendación que demuestren que la empresa ha estado trabajando en los últimos 5 años en ciberseguridad)*	X	
Al menos 2 profesionales que cuenten con 2 de las siguientes Certificaciones • Certified System Auditor CRISC • Certified System Auditor CISA • Certified System Auditor CISM	X	

• Certified Information Systems Security Professional CISSP • Lead Cybersecurity Proffesional Certificate LCSPC *(medio de verificación: certificaciones vigentes)*		
CRITERIOS DE CALIFICACIÓN		
CRITERIO	**MÁXIMO**	**MÍNIMO**
Experiencia individual e indivisible de la empresa comprobable de al menos 10 años en el mercado en implementación de infraestructura tecnológica. 10 años = 20 puntos Mas de 10 años = 25 puntos *(patente o registro comercial de la empresa)*	25	20
Experiencia individual e indivisible de la empresa comprobable de al menos 5 años en ciberseguridad. 5 años = 15 puntos Mas de 5 años = 20 puntos *(medio de verificación: proyectos desarrollados por la empresa en los últimos 5 años)*	20	15
Al menos 2 profesionales que cuenten con 2 de las siguientes Certificaciones • Certified System Auditor CRISC • Certified System Auditor CISA • Certified System Auditor CISM • Certified Information Systems Security Professional CISSP • Lead Cybersecurity Proffesional Certificate LCSPC 2 profesionales certificados = 20 puntos Mas de 2 profesionales = 30 puntos *(medio de verificación: certificaciones vigentes)*	30	20
Oferta de cumplimiento con todos los productos y actividades solicitadas en este documento Cumple = 10 puntos	10	0
Mejor propuesta económica presentada conforme a lo requerido en este documento.	15	0
TOTAL	100	60
Nota 1: Las empresas que no cumplen con los criterios de base (cumple o no cumple) no pasan a la evaluación de criterios ponderados.		
Nota 2: En caso de empate en dos o más empresas, se considerará a la empresa con mayor experiencia como criterio para desempatar.		

La SIECA, como órgano técnico administrativo del Proceso de Integración Económica Centroamericana, promueve y favorece el desarrollo y contratación de nacionales de los países miembros del Subsistema de Integración Económica Centroamericana (Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá). Para ello la contratación de nacionales del Subsistema de Integración Económica Centroamericana se atenderá a la capacidad, idoneidad y disponibilidad en igualdad de condiciones para todos los países miembros, conforme las posibilidades y necesidades de la SIECA. En casos debidamente calificados o justificados, podrán participar personas de otras nacionalidades en los procesos de contratación de la SIECA.