TÉRMINOS DE REFERENCIA SOFTWARE PARA AUTENTICACIÓN MULTIFACTOR

Consultoría	Adquisición de Software y Servicio para Autenticación Multifactor del Proyecto ECOTRADE
Proyecto	NDICI LA/2024/460-208 "Integración Económica para un Comercio Sostenible en Centroamérica (ECOTRADE)
Componente	COMPONENTE 1. Estrategia Centroamericana de Facilitación de Comercio (ECFCC-2023), aprovechamiento del Acuerdo de Asociación (AACUE) y Plan Maestro Regional de Movilidad y Logística 2035 (PMRML 2035)en la Región Centroamericana.
Resultado ECOTRADE	R2 - Fortalecida la integración económica regional para el aprovechamiento del Acuerdo de Asociación y la promoción del comercio regional centroamericano
Subactividad	A.2.11.3 Fortalecimiento de capacidades de ciberseguridad en la nube por medio de la certificación Cloud security professional y la implementación de herramienta de ciberseguridad y confidencialidad de la información
Duración del Servicio	5 meses
Tipo de contrato	Adquisición de software y servicios de configuración

1. Antecedentes

La Secretaría de Integración Económica Centroamericana (SIECA,) es el órgano técnico y administrativo del proceso de Integración Económica Centroamericana, tiene personalidad jurídica de derecho internacional y funciona como enlace de las acciones de las otras Secretarías del Subsistema Económico, definido todo ello en el Artículo 28 del Protocolo de Tegucigalpa.

Dentro del nuevo ciclo de cooperación de la Unión Europea, la SIECA implementa el proyecto regional "Integración Económica para un Comercio Sostenible en Centroamérica (ECOTRADE)" durante el período 2024-2028, en coordinación con los Estados Parte de la integración económica centroamericana. El objetivo general del proyecto es fortalecer la competitividad de la región centroamericana y maximizar los beneficios del Acuerdo de Asociación entre Centroamérica y la Unión Europea, reduciendo las barreras comerciales y promoviendo la facilitación del comercio, la mejora significativa de la movilidad y logística de las mercancías y las personas y aumentando las oportunidades de comercio e inversión en la región.

Los objetivos específicos del proyecto son impulsar la implementación de la Estrategia Centroamericana de Facilitación del Comercio 2023, el Acuerdo de Asociación entre Centroamérica y la Unión Europea y el Plan Maestro Regional de Movilidad y Logística 2035 promoviendo la

cooperación regional, la armonización de políticas y regulaciones comerciales, el fortalecimiento de las capacidades institucionales de los actores privado y público para fortalecer la competitividad de la región y fortalecer la consolidación del proceso de Integración Profunda entre El Salvador, Guatemala y Honduras, por medio de la coordinación y armonización de medidas y políticas de facilitación del comercio, de conectividad y logística, de digitalización y de sostenibilidad en los puestos fronterizos.

2. Área que realiza el requerimiento

Dirección de Tecnología de la Información y Comunicaciones (DTIC)

3. Objeto de la contratación

Objetivo General

Implementar una solución de Autenticación Multifactor (MFA) para reforzar la seguridad en el acceso a cuentas críticas como como Microsoft 365, FortiClient VPN, AWS, Sistemas nativos y otros sistemas. Esto permitirá mitigar riesgos de accesos no autorizados, garantizar la integridad de la información y asegurar el cumplimiento de las políticas de seguridad establecidas. Además, fortalecerá la protección ante amenazas externas, especialmente en entornos de trabajo remoto o híbrido, sin afectar la experiencia del usuario ni la continuidad operativa.

Objetivos Específicos

i. Fortalecer los mecanismos de control de acceso mediante la implementación de una solución de autenticación multifactor que minimice los riesgos asociados al uso exclusivo de contraseñas.
ii. Garantizar la protección de los accesos a sistemas críticos institucionales (locales y en la nube), mediante la verificación de identidad en múltiples factores de autenticación, especialmente en accesos remotos, administrativos y privilegiados.
iii. Integrar la solución MFA con la infraestructura tecnológica actual sin afectar la continuidad operativa de los servicios.
iv. Reducir la superficie de ataque ante amenazas como robo de credenciales, phishing o fuerza bruta, mediante políticas adaptadas a los niveles de riesgo y tipo de usuarios.

4. Justificación y alcance de la consultoría

La organización reconoce la necesidad de fortalecer la seguridad en el acceso a plataformas críticas como Microsoft 365, FortiClient VPN, AWS, Sistemas nativos y otros. La implementación de Autenticación Multifactor (MFA) permitirá mitigar riesgos asociados al uso exclusivo de contraseñas, reduciendo la posibilidad de accesos no autorizados y suplantación de identidad. Esta medida se alinea con las mejores prácticas de ciberseguridad y los requerimientos normativos vigentes, garantizando la protección de la información sin afectar la operatividad. Su adopción será gestionada conforme a las políticas internas de seguridad de la información.

Alcance

i. Licenciamiento del software, incluyendo los módulos necesarios para la autenticación, multifactor (MFA) en todas las plataformas ("como Microsoft 365, FortiClient VPN, AWS, Sistemas nativos y otros sistemas), con soporte para métodos de autenticación como tokens de hardware, aplicaciones de autenticación.
ii. Diseño de arquitectura de la solución, acorde a la infraestructura actual de la SIECA, considerando la integración con sistemas existentes como Active Directory (AD), como Microsoft 365, FortiClient VPN, AWS, Sistemas nativos y otros sistemas.
iii. Capacitación técnica para administradores de la plataforma, incluyendo la gestión de usuarios, configuración de políticas de acceso basada en riesgos, generación de logs de auditoría y mantenimiento de la solución MFA.
iv. Capacitación operativa para usuarios finales que interactúen con la solución, cubriendo el proceso de registro de dispositivos, uso de MFA en los distintos accesos, recuperación de cuentas y resolución de problemas comunes relacionados con la autenticación.
v. Asistencia en la resolución de incidentes relacionados con la herramienta, incluyendo soporte ante posibles bloqueos de acceso, problemas con los métodos de autenticación y fallos técnicos en usuarios administradores.
vi. Manual de usuarios administradores y usuarios finales, que complete procedimientos detallados para la gestión de la solución MFA, desde la configuración inicial hasta el manejo de problemas de acceso.

5. Metodología

Para la implementación de la solución, se propone una metodología estructurada y supervisada directamente por la Dirección de Tecnologías de la Información y Comunicaciones. El equipo de servicios profesionales será responsable de realizar el levantamiento de requerimientos, la instalación, configuración, integración y validación de la solución, conforme a las políticas de seguridad establecidas por la organización.

Cada fase del proyecto será documentada y validada en conjunto con los responsables designados, asegurando la trazabilidad de las actividades, la correcta configuración para el cifrado seguro y el cumplimiento de los objetivos de seguridad. Este enfoque garantiza una implementación ordenada, segura y alineada con las mejores prácticas de ciberseguridad.

6. Tabla de especificaciones técnicas

No.	Servicios y Especificaciones Técnicas	Cantidad
1	Adquirir licencias por 3 años con las características siguientes: ✓ MFA (opciones flexibles que incluyen FIDO2 y Verified Duo Push) ✓ Autenticación sin contraseña (Usando FIDO2 o Duo Mobile) ✓ Inicio de sesión único ✓ Verificación de puntos finales de confianza. ✓ Autenticación adaptiva, que permita crear políticas de accesos personalizadas basadas en factores contextuales como rol, aplicación, ubicación geográfica, red y estado del dispositivo. ✓ Integraciones de aplicaciones ilimitadas ✓ Compatibilidad con cuentas Microsoft 365, FortiClient VPN, AWS, Servicios de Google y Azure AD. ✓ API REST para integraciones personalizadas a) SDKs y plugins para apps web propias	170

7. Actividades o tareas a realizar

Durante la implementación, la entidad proveedora del servicio deberá desarrollar las actividades siguientes:

- **Planeación**: se realizara la planeación de las actividades a realizar para integrar la solución en la infraestructura tecnológica de la SIECA.
- **Instalación y configuración:** Instalar y configurar los componentes necesarios del sistema, garantizando su correcta integración y funcionamiento cuando los usuarios interactúan con las diferentes aplicaciones como office 365, gestor de documentos, AWS, herramientas de monitoreo, entre otros.
- **Validación y pruebas:** Realizar pruebas exhaustivas para verificar que la herramienta cumpla con los requisitos y funcione correctamente en computadoras, servidores y dispositivos móviles.
- **Capacitación:** Proporcionar formación a los usuarios finales y al personal técnico para asegurar un uso adecuado y eficiente del sistema.
- **Soporte y mantenimiento posterior a la implementación**: Ofrecer soporte para asegurar la operatividad y actualización de la herramienta posterior a su implementación.

8. Productos y calendario de pagos

a. Plan de trabajo de las actividades a desarrollar 5 días después de iniciadas labores, según las prioridades que sean indicadas.
b. Informes de actividades que incluya anexos que comprueben lo siguiente:

i. Instalación del software MFA con licencia por 3 años en la infraestructura de la SIECA.
ii. Documento de evidencia de Autenticación en Office 365 para todos los usuarios de la SIECA, Software de gestión administrativa en equipos FortiNet, AWS, VPN, herramientas XDR, NDR, Cisco Umbrella, Wordpress, herramientas de monitoreo y aplicaciones propias como DOFIE, SIVAS, Portal de Mesa de ayuda regional, adquisición de tokens.
iii. Documentación de configuración de la solución.

c. Transferencia de conocimientos de al menos 8 horas para 4 personas con instructor personalizado sobre la solución del MFA.
d. Curso en línea de 40 horas de ITIL Foundation Versión 4 para 2 personas con voucher para examen certificación, impartido por instructor oficial.

Calendario de Pagos

Producto/Mes	**1**	**2**	**3**	**4**	**5**
Instalación del software MFA con licencia por 3 años en la infraestructura de la SIECA.	15%				
Documento de evidencia de Autenticación en Office 365 para todos los usuarios de la SIECA, Software de gestión administrativa en equipos FortiNet, AWS, VPN, herramientas XDR, NDR, Cisco Umbrella, Wordpress, herramientas de monitoreo. Aplicaciones propias como DOFIE, SIVAS, Portal de Mesa de ayuda regional, adquisición de tokens.				55%	
Documentación de configuración de la solución.				10%	
Transferencia de conocimientos de al menos 8 horas para 4 personas con instructor personalizado sobre la solución del MFA.					10%
Curso en línea de 40 horas de ITIL Foundation Versión 4 para 2 personas con voucher para examen certificación, impartido por instructor oficial.					10%

9. Duración del servicio

El tiempo requerido es de cinco (5) meses contados a partir de la firma del contrato.

10. Tipo de Contrato, temporalidad y forma de Pago

La contratación se realiza a través de contrato de “Contrato por Servicios”, elaborado por la Dirección Jurídica de la SIECA por un monto cerrado, en el cual se especifica las actividades, productos esperados, precio, forma de pago y la duración de la contratación.

El servicio se prestará bajo la coordinación y supervisión de la Dirección de Tecnologías de la Información y Comunicación-DTIC de la SIECA.

Los pagos se realizarán por transferencia bancaria y posterior a la entrega de factura original a nombre de SIECA/ECOTRADE número de NIT: 636007-6 e informe mensual de actividades debidamente, de conformidad al numeral anterior, 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.

El pago se realizará 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 del consultor.

El proveedor del producto y su régimen sea general, se le extenderá una constancia de exención de IVA, caso contrario, el proveedor deberá asumir los impuestos que apliquen de acuerdo con el régimen en que se encuentre inscrito (aplicable para consultores guatemaltecos).

El contrato no genera una relación laboral con la SIECA, por lo que no genera pasivo laboral.

11. Sede y coordinación de la contratación

La implementación, del servicio se realizará en la oficina de la SIECA 4ª. Avenida 10-25, Zona 14 Ciudad de Guatemala o de forma remota, plazo no mayor a 1 día posterior a la recepción de la orden de compra y el servicio no puede durar más de 5 meses.

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

12. Presentación de postulaciones o muestras de interés

Las empresas interesadas en participar deberán enviar:

i. Carta de interés, indicando que acepta los Términos de Referencia.
ii. Oferta técnica-económica.
iii. Hoja vida de la empresa, detallando su experiencia.
iv. Cartas de referencias de (al menos 3) empresas o Instituciones respaldando la experiencia profesional específica en estos equipos y servicios de arrendamiento similares, especialmente de soporte y apoyo técnico.
v. Plan de trabajo y cronograma que describa las etapas y actividades a realizar.
vi. Copia simple del testimonio de la escritura constitutiva de la persona jurídica o sociedad, incluyendo las modificaciones (si fuere el caso).
vii. Copia simple de la representación legal actualizada de la empresa.

viii. Copia simple de la patente de sociedad y de empresa según aplique.
ix. Copia simple del RTU de reciente actualización (si aplica).
x. Copia simple del DPI o pasaporte si no fuera guatemalteco, del representante legal de la empresa y que firmará el Contrato.

13. Presentación de las ofertas

Para la presentación de las ofertas deberá dirigirse por medio de un correo electrónico en un único documento en formato PDF de la Oferta técnica-económica, indicando claramente la "Propuesta".

La propuesta Técnica y Económica incluyendo toda la documentación requerida puede remitirse vía electrónica al correo adquisiciones@sieca.int, indicando en el asunto: "Adquisición de Software y Servicio para Autenticación Multifactor"

14. Plazos de las ofertas

La presentación de las ofertas vía correo electrónico se deberá hacer a más tardar el 20 de agosto de 2025 a las 23:59 horas.

Las ofertas tendrán validez de 45 días luego de la fecha límite de presentación.

Tabla de criterios de evaluación

Matriz de Evaluación		
Criterios de Base	**Cumple**	**No cumple**
Experiencia profesional de al menos 10 años en brindar servicios de Ciberseguridad. *Medio de verificación: patente de comercio con giro de negocio requerido*		
Mínimo 2 profesional con alguna de las siguientes Certificación: CISSP, CISM, CISA, CDPSE, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor. *Medio de verificación: Certificaciones vigentes.*		
Presentar al menos 3 cartas de recomendaciones de clientes con similar relevancia como la SIECA a las especificaciones técnicas planteadas en la propuesta económica. *Medio de verificación: Cartas de recomendación, membretadas y firmadas por clientes.*		
Criterios Ponderados	**Máximo**	**Mínimo**
Experiencia profesional demostrada de diez o más años en servicios de Ciberseguridad e integración de proyectos similares Al menos 10 años = 20 puntos Más de 10 años= 30 puntos	30	20

Medio de verificación: patente de comercio con giro de negocio requerido y atestados profesionales		
La empresa debe contar entre su equipo profesional con un mínimo de 2 profesionales con alguna de las siguientes Certificación: CISSP, CISM, CISA, CDPSE, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor. Más de 2 profesionales = 15 puntos Al menos 2 profesionales = 10 puntos *Medio de verificación: Certificaciones vigentes.*	15	10
La empresa debe presentar un mínimo de 3 cartas de recomendaciones de clientes de empresas corporativas, instituciones internacionales y/o organismos regionales en servicios similares al objetivo de la presente adquisición. Más de 3 cartas = 15 puntos Al menos 3 cartas = 10 puntos *Medio de verificación: Cartas de recomendación, membretadas y firmadas por clientes.*	15	10
Cumplimiento con todas las especificaciones técnicas indicadas en este documento. Cumplimiento = 20 puntos *Medio de verificación: Propuesta presentada*	20	0
Mejor propuesta económica que cumpla con todas las especificaciones técnicas indicadas en este documento. Cumplimiento = 20 puntos *Medio de verificación: Propuesta presentada*	20	0
Total	**100**	**40**

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.