TÉRMINOS DE REFERENCIA PARA LA ADQUISICIÓN DE SOFTWARE GESTIÓN DE IDENTIDADES Y ACCESO CON ENFOQUE EN SEGURIDAD

Consultoría	**Para la gestión de identidades y acceso con enfoque en seguridad**
Proyecto	DTIC
Componente	
Duración del Servicio	5 meses
Tipo de contrato	Adquisición y Configuración de software

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.
Fuentes de Financiamiento: La Secretaría de Integración Económica Centroamericana (SIECA) para su funcionamiento operativo, depende principalmente de las aportaciones que da cada uno de los países miembros, seis países en total, este aporte es anual y por país. La SIECA realiza su presupuesto en base a estos ingresos.
La Secretaría de Integración Económica (SIECA), como parte de su perspectiva contempla el desarrollo de su capital intangible, por lo que uno de sus objetivos estratégicos es garantizar una atención eficiente y con calidad.

2. Justificación y alcance

La SIECA es consciente de las crecientes amenazas cibernéticas y del impacto que la exposición de cuentas privilegiadas puede generar en la organización. Por ello, es fundamental que la SIECA fortalezca su postura de seguridad mediante la adquisición de una solución especializada en la gestión de accesos privilegiados (PAM), que permita proteger las credenciales más sensibles, controlar los accesos a sistemas críticos y supervisar el uso de privilegios en tiempo real. La implementación de (PAM) contribuye al cumplimiento de las mejores prácticas de ciberseguridad y regulaciones vigentes, reduce el riesgo de brechas de seguridad internas y externas, y fomenta una cultura de seguridad continua, protegiendo así los activos más valiosos de la organización.

Alcance

Adquisición de licencias y la implementación de una solución integral para la gestión de accesos privilegiados, incluyendo diseño arquitectónico, instalación, integración con Active Directory y sistemas operativos, así como configuración de políticas de seguridad, alertas y reportes de auditoría. También abarca la capacitación técnica y operativa para administradores y usuarios finales, soporte durante el periodo de garantía, y la entrega de documentación completa. Todo esto se realizará conforme a estándares internacionales de ciberseguridad como ISO 27001, asegurando escalabilidad, seguridad y cumplimiento normativo.

La solución deberá ser implementada y configurada para gestionar el acceso privilegiado a la siguiente infraestructura:

- Contenedores AWS: 7
- Servidores: 147 servidores (61 en AWS y 86 on-premise)

La solución deberá ser compatible e integrable con los siguientes sistemas operativos:

- ✓ Windows Server 2003 (32bits)
- ✓ Windows Server 2008 R2 (64bits)
- ✓ Windows Server 2012 (64bits)
- ✓ Windows Server 2016 (64bits)
- ✓ Windows Server 2019 (64bits)
- ✓ Windows Server 2022 (64bits)
- ✓ Amazon Linux
- ✓ CentOS 4/5/6/ (bits)
- ✓ Other 2.6.x Linux (64bits)
- ✓ Other 3.x or later Linux(64bits)
- ✓ Ubuntu 18
- ✓ Ubuntu 18/FortiGate
- ✓ Ubuntu Linux (64-bit)

3. Objetivo general y específicos de la consultoría

Objetivo General:

Implementar una solución de gestión de accesos privilegiados mediante la adquisición, configuración y puesta en operación de la plataforma, para proteger las credenciales críticas, controlar el acceso a sistemas sensibles y asegurar la trazabilidad de las acciones realizadas por cuentas privilegiadas, en estricto cumplimiento con las políticas de seguridad de la información y los estándares definidos por la Dirección de Tecnologías de la Información y Comunicaciones.

Objetivos Específicos:

a) Implementar la plataforma para gestionar de manera segura las credenciales privilegiadas de los sistemas críticos de la organización.
b) Establecer una bóveda segura de contraseñas y controlar el acceso a las cuentas privilegiadas.
c) Configurar flujos de aprobación para el control de accesos a cuentas privilegiadas y auditar dichos accesos conforme a las políticas de seguridad establecidas.
d) Realizar auditorías periódicas sobre los accesos privilegiados y generar reportes que permitan identificar desviaciones, incumplimientos o riesgos de seguridad.

4. 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, el diseño de arquitectura, 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 de los controles de acceso privilegiado y el cumplimiento de los objetivos de seguridad. Este enfoque garantiza una implementación ordenada, segura y alineada con las mejores prácticas de ciberseguridad.

5. Tabla de especificaciones técnicas

Nota: previo a la entrega de la cotización y firma de contrato se debe asegurar y garantizar la compatibilidad de la solución con la infraestructura tecnológica de la SIECA.

No.	Servicios y Especificaciones Técnicas	Cantidad
1	a) Gestión de credenciales y bóveda segura de contraseñas. b) Control de accesos privilegiados (PAM) con definición granular de roles y permisos. c) Seguridad y monitoreo de sesiones privilegiadas, incluyendo grabación y auditoría. d) Flujos configurables de aprobación para solicitudes de acceso privilegiado. e) Integración con sistemas de identidad: Active Directory, LDAP, AWS AD. f) Integración con bases de datos, dispositivos de red, aplicaciones SaaS y ERP. g) Autenticación multifactor (MFA) para acceso seguro. h) Auditoría completa y monitoreo en tiempo real con generación de reportes.	Ver alcance

	i) Análisis de comportamiento de usuarios privilegiados (UBA) y alertas de actividades sospechosas. j) Cifrado fuerte de datos en reposo y en tránsito. k) Soporte para gestión de parches de seguridad, tanto automáticos como manuales. l) Escalabilidad para soportar el crecimiento y expansión del entorno. m) Compatibilidad multiplataforma: Windows, Linux, Unix y entornos en la nube (on-premise, híbrido, cloud).	

6. **Actividades o tareas para realizar**

- **Diseño de la solución:**
  - ✓ Elaboración del diseño técnico de la arquitectura de la solución.
  - ✓ Definición de roles, perfiles y políticas de acceso.
  - ✓ Planificación de integración con sistemas operativos existentes.
  - ✓ Planificación de la estrategia de gestión de cuentas privilegiadas y credenciales.

- **Adquisición y configuración inicial:**
  - ✓ Instalación y configuración de la plataforma.
  - ✓ Configuración inicial de los módulos requeridos.
  - ✓ Configuración de políticas de acceso, workflows de aprobación y auditoria.
- **Migración y Onboarding**
  - ✓ Importación y registro de cuentas privilegiadas en la solución.
  - ✓ Definición e implementación de ciclos de vida y rotación de contraseñas.
  - ✓ Capacitación inicial a usuarios claves y administradores.
- **Pruebas y validación**
  - ✓ Pruebas de funcionalidad, seguridad y rendimiento de la solución.
  - ✓ Validación de integración con sistemas y cumplimiento de políticas.
  - ✓ Ajustes y correcciones basados en pruebas.
- **Capacitación y transferencia de conocimiento**
  - ✓ Capacitación a equipos de TI y seguridad en operación y administración de la solución.
  - ✓ Entrega de documentación y manuales de usuario.
  - ✓ Entrenamiento en gestión de incidentes y respuesta
- **Puesta en producción y monitoreo**
  - ✓ Migración a ambiente productivo.
  - ✓ Monitoreo inicial de la solución y resolución de incidencias.
  - ✓ Establecimiento de reportes periódicos y mecanismos de auditoría.
- **Soporte y mantenimiento**
  - ✓ Definición de soporte post-implementación.
  - ✓ Actualizaciones y parches de la solución
  - ✓ Revisión periódica de políticas y ajustes a nuevos requerimientos.

7. **Productos y calendario de pagos**

Plan de trabajo de las actividades a desarrollar 5 días después de iniciadas labores, según las prioridades que sean indicadas.

Informes de actividades que incluya anexos que comprueben lo siguiente:

I. **Entregable 1:**
   a. **Informe de diagnóstico y análisis de requerimientos:** Documento que detalle el estado actual, riesgos asociados y requerimientos técnicos y funcionales recogidos, conforme al alcance establecido en este documento.
   b. **Diseño técnico de la solución:** Documento que incluya arquitectura, diagramas de integración, definición de roles y políticas de acceso conforme al alcance establecido en este documento.
   c. Plan de implementación: Cronograma detallado con las fases, actividades, responsables y recursos necesarios conforme al alcance establecido en este documento.

II. **Entregable 2:**
   a. Software y licenciamiento: Entrega de software debidamente licenciado por 3 años que cubra el alcance establecido en este documento.
   b. Configuración y parametrización del sistema: Evidencia documental y técnica de la configuración realizada de la solución (capturas, configuraciones exportadas, manuales) conforme al alcance establecido en este documento.
   c. Cuentas privilegiadas registradas y configuradas: Registro de todas las cuentas privilegiadas gestionadas dentro de la solución (Al menos 5 roles).

III. **Entregable 3:**
   a. Plan de capacitación y material de formación: Agenda, manuales de usuario y administración entregados a los equipos capacitados.
   b. Informe de pruebas y validación: Reporte con resultados de pruebas funcionales, de seguridad y de integración, incluyendo observaciones y correcciones.
   c. Documentación técnica completa: Manuales operativos, manuales de usuario, guías de administración y procedimientos para gestión y mantenimiento.

IV. **Entregable 4:**
   a. Informe de puesta en producción: Documento que certifique la correcta migración a producción y el monitoreo inicial de todos los equipos conforme al alcance establecido en este documento.
   b. Plan de soporte y mantenimiento: bolsón de 150 horas de soporte post-implementación por 3 años conforme a licenciamiento adquirido.

V. **Entregable 5:**
   a. Curso de 40 horas por instructor certificado por el fabricante de la solución con voucher para tomar examen de certificación, para 2 personas, impartido en idioma español.

Calendario de Pagos

Productos	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5
Entregable 1	10%				
Entregable 2		60%			
Entregable 3				10%	
Entregable 4					10%
Entregable 5					10%

Pago tras la entrega del informe final y cierre del proyecto aprobado por el Director de la DTIC.

8. Duración del servicio

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

9. 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.

10. 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.

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

11. Presentación de postulaciones o muestras de interés

Las empresas interesadas en participar deberán enviar:

1. Carta de interés, indicando que acepta los Términos de Referencia.
2. Oferta técnica-económica.
3. Hoja vida de la empresa, detallando su experiencia.
4. Cartas de referencias de (al menos 4) empresas o Instituciones respaldando la experiencia profesional específica en estos equipos y servicios de arrendamiento similares, especialmente de soporte y apoyo técnico.
5. Plan de trabajo y cronograma que describa las etapas y actividades a realizar.
6. Copia simple del testimonio de la escritura constitutiva de la persona jurídica o sociedad, incluyendo las modificaciones (si fuere el caso).
7. Copia simple de la representación legal actualizada de la empresa.
8. Copia simple de la patente de sociedad y de empresa según aplique.
9. Copia simple del RTU de reciente actualización (si aplica).
10. Copia simple del DPI o pasaporte si no fuera guatemalteco, del representante legal de la empresa y que firmará el Contrato.

12. Presentación de las ofertas

Modelo para la presentación de Hojas de Vida

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 Gestión de Identidades y Acceso con enfoque en Seguridad”

13. Plazos de las ofertas

La presentación de las ofertas vía correo electrónico se deberá hacer a más tardar el 02 de noviembre de 2025.

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

14. 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. **Criterios de evaluación**

15. Adjudicación

14.1 Comunicación

La comunicación de la adjudicación de los servicios profesionales ofertados se hará mediante notificación oficial por correo de adquisiciones@sieca.int con asunto Contrato implementación de servidores en infraestructura hibrida

14.2. Requisitos legales

En caso de adjudicación del contrato la empresa deberá presentar los siguientes documentos legales:

14.2.1 Fotocopia autenticada del testimonio de la escritura constitutiva de la persona jurídica o sociedad, incluyendo las modificaciones (si fuere el caso).

14.2.2 Fotocopia autenticada de la patente de sociedad y de empresa según aplique.

14.2.3 Fotocopia autenticada del RTU de reciente actualización (si aplica).

14.2.4. Fotocopia autenticada del DPI del profesional que firmará el Contrato.

14.2.5 Fotocopia autenticada de la representación legal actual de la empresa.

14.2.6 Fotocopia de Estados financieros auditados 2022 y 2023.

Tabla de criterios de evaluación

Matriz de Evaluación		
Criterios de Base	**Cumple**	**No cumple**
Experiencia profesional de más de 10 años en brindar servicios de Ciberseguridad. *Medio de verificación: patente de comercio con giro de negocio requerido*		
Al menos dos profesionales certificados en la solución del producto a implementar. *Medio de verificación: certificado vigente de cada profesional.*		

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 de más de 10 años en brindar servicios de Ciberseguridad. Más de 10 años= 30 puntos 10 años = 20 puntos *Medio de verificación: patente de comercio con giro de negocio requerido*	30	20
Al menos dos profesionales certificados en la solución del producto a implementar. Al menos 2 profesionales certificados = 10 puntos Más de 2 profesionales certificados = 15 puntos *Medio de verificación: certificado vigente de cada profesional.*	15	10
Presentar al menos 3 cartas de recomendaciones de clientes con similar relevancia como la SIECA a las especificaciones técnicas planteadas en la propuesta económica. 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	
Mejor propuesta económica que cumpla con todas las especificaciones técnicas indicadas en este documento. Cumplimiento = 20 puntos *Medio de verificación: Propuesta presentada*	20	
Total	**100**	**40**
Nota 1: Los empresas que no cumplen con los criterios de base no pasan a la evaluación de criterios ponderados. **Nota 2**: En caso de que dos o más empresas obtengan la misma nota, se tomará a la empresa con mayor experiencia como criterio de desempate.		

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.