



Crédito Agrícola de Habilitación CAH

Proyecto 1005229.
Fortalecimiento Institucional del CAH

SOLICITUD DE COTIZACIÓN (SDC)
1005229 Fortalecimiento Institucional del CAH

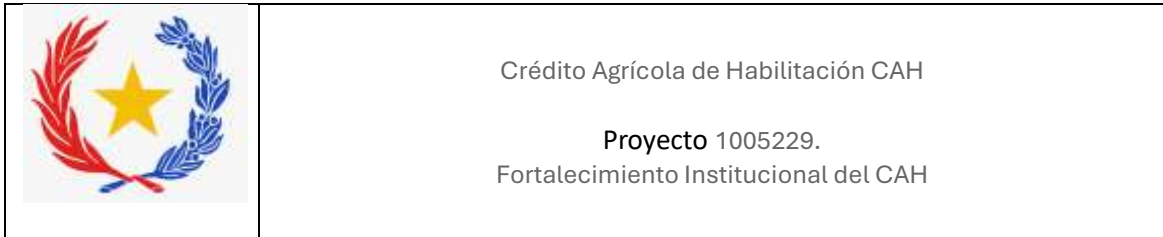
Para: Señores de (Nombre de la empresa) (Dirección de la empresa) (Ciudad)	Referencia (Número y Nombre del Proceso) (Favor indicar en comunicaciones sucesivas)
Atención: Señor Director	Fecha: (Día, Mes, Año)
Tel: (Número)	Tel: (Número)
Fax: (Número)	Fax: (Número)

El **Crédito Agrícola de Habilitación (CAH)** en su carácter de Asociado en la Implementación del Proyecto **1005229 Fortalecimiento Institucional del CAH** (en adelante, indistintamente, el CAH o el Proyecto) invita a su empresa a cotizar los servicios que se resumen a continuación:

Item N°	Breve descripción	Cantidad
1	SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) – (MESES)	6
Validez mínima de la oferta:	30 días <input type="checkbox"/> 45 días <input type="checkbox"/> 60 días <input checked="" type="checkbox"/>	
Términos de adquisición:	Plaza <input checked="" type="checkbox"/> CIP Asunción <input type="checkbox"/> Otro <input type="checkbox"/>	
Lugar para presentación de ofertas:	Crédito Agrícola de Habilitación Gerencia de Área de Planificación Unidad Ejecutora de Proyecto 1005229 Dirección: Carios 362 c/ William Richardson Asunción	
Plazo para presentación de ofertas:	22/05/2026 15:00 Hs.	

Quedamos a la espera de su cotización.

Atentamente,



Sección 1 - CONDICIONES DE LA SOLICITUD DE COTIZACIÓN (SDC)

El Proyecto **1005229** tiene el agrado de invitar a su empresa a presentar una cotización para la adquisición de los servicios motivo de la presente solicitud.

Este llamado está siendo llevado a cabo en el marco de las disposiciones establecidas en el “Acuerdo entre el Gobierno de Paraguay y el Programa de las Naciones Unidas para el Desarrollo” firmado el 12 de diciembre de 1985. Los procedimientos para adquisición de los servicios objeto de este llamado serán los que el Gobierno de Paraguay y el Programa de las Naciones Unidas para el Desarrollo (PNUD) han acordado en el respectivo Documento del Proyecto y en la Guía de Pautas y Procedimientos para la Implementación Nacional de Proyectos por parte de los Gobiernos a través del PNUD.

1. La oferta a ser presentada deberá incluir los documentos indicados a continuación:
 - a) Carta de Presentación firmada por un representante legal de la empresa oferente.
 - b) Formulario de Oferta y Formulario de Especificaciones Mínimas Requeridas debidamente completado y firmado por un representante legal de la empresa
 - c) Garantía de Mantenimiento de Oferta. El Oferente garantizará el mantenimiento de su oferta mediante Póliza de Seguro equivalente al 2% del monto total de su oferta. La póliza deberá ser emitida por un banco legalmente establecido y ejecutable en Paraguay. El documento deberá ser emitido a nombre del Crédito Agrícola de Habilitación (CAH) y deberá estar vigente por un periodo mínimo igual al de la validez de la oferta. La garantía será devuelta al Proveedor una vez firmado el contrato con el proveedor seleccionado.
 - d) Copia de Registro Único del Contribuyente (RUC)
 - e) Copia del Certificado de Cumplimiento Tributario vigente
 - f) Copia de Cédula de Identidad (en caso de personas físicas)
 - g) Copia de los estatutos de la empresa u otro documento de conformación, debidamente registrado por las autoridades competentes en el país de origen y las escrituras de las modificaciones del mismo. En el caso de Sociedades Anónimas deberán presentar adicionalmente el acta de la última asamblea y los nombres de los directores en funciones. (en caso de personas jurídicas)
 - h) Poder otorgado ante Escribano Público al (a los) firmante(s) de la oferta. En aquellos casos en que el estatuto especifique la representación de la firma, no será necesaria la presentación de este documento. (en caso de personas jurídicas)
 - i) Copia de contratos y/o facturaciones de venta y/o recepciones finales a efectos de demostrar la experiencia en servicios de monitoreo, gestión y respuesta ante incidentes de seguridad, por un monto equivalente al 50 % como mínimo del monto total ofertado en la presente licitación, dentro de los 3 últimos años (2023, 2024 y/o 2025)
 - j) Copia de certificados o constancias de servicios satisfactorios, emitidas por al menos 5 (cinco) Instituciones Públicas y/o Privadas, a efectos de demostrar al menos 5 (cinco) años de experiencia en el mercado en la prestación de los servicios requeridos, donde se comprueben los siguientes servicios: (i) servicios de auditorías de vulnerabilidades o



Crédito Agrícola de Habilitación CAH

Proyecto 1005229.
Fortalecimiento Institucional del CAH

pentesting, (ii) servicios de gestión y respuesta ante incidentes cibernéticos relacionados a compromisos de sistemas web, ransomware, DoS, Escaneos/Fuerza Bruta, Malware, etc., (iii) Servicios de asesorías en ciberseguridad relacionadas arquitecturas de ciberseguridad y/o desarrollo de documentación relacionada a ciberseguridad. Se aclara que no será necesario que en la constancia o certificado se mencionen todos los servicios, siempre y cuando se demuestre al menos 1 (una) experiencia para cada servicio requerido.

- k) Copia de Certificado de Gestión de Calidad (CSG) según la norma ISO 9001 y/o de Gestión de Servicios de IT (ITSM) según la norma 20000
- l) Copia de Certificado de Calidad ISO 27001 vigente
- m) Currículum Vitae del personal a ser asignado para esta contratación (debidamente firmado)
- n) Declaración jurada donde declare que cumplirá con las especificaciones técnicas y con los plazos de entrega de los servicios.
- o)

La difusión de la presente Solicitud de Cotización se realiza mediante: **Publicación**

1. Lugar y fecha de recepción de ofertas completas, en un (1) original y [1] copia completa del original:

SDC/1005229/001/2026 "Servicio de Centro de Operaciones de Seguridad"

Unidad Ejecutora del Proyecto

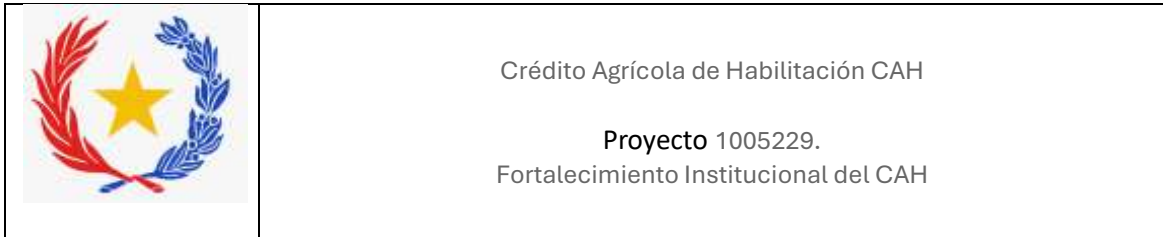
Gerencia de Area de Planificación

Crédito Agrícola de Habilitación

Dirección: Carios 362 c/ William Richarson

[Plazo máximo, 22/05/2026 15:00 hs]

2. Las descripciones de los ítems detallados en la sección Especificaciones Técnicas son las mínimas exigidas, no serán consideradas las ofertas que no alcancen estos requerimientos.
3. Su propuesta debe especificar claramente: descripción detallada del/de los ítems(s) ofertado(s), folletos o literatura descriptiva de los ítems, precio, plazo de entrega, garantía de los bienes y período de validez de la oferta.
4. Será responsabilidad de los Oferentes sufragar todos los gastos relacionados con la preparación y presentación de ofertas. El Comprador no será responsable en ningún caso por dichos costos, cualquiera sea la forma en que se realice el proceso de compra o su resultado.
5. Todo Oferente que requiera aclaración al presente proceso de compra, podrá solicitarla por escrito a cah.planificacion@gmail.com a más tardar 15/05/2026 15:00 hs Las respuestas serán enviadas a todas las firmas oferentes a más tardar 18/05/2026 15:00 Hs. A partir de la



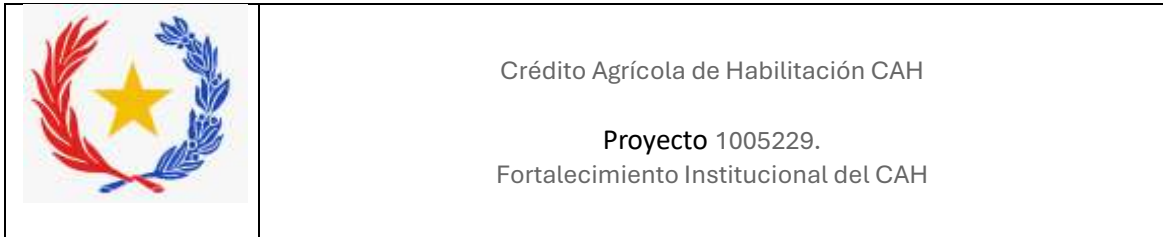
fecha de comunicación de las respuestas, las mismas formarán parte y serán leídas conjuntamente con la Solicitud de Cotización.

6. El Proyecto, podrá por cualquier causa y en cualquier momento antes de que venza el plazo de presentación de ofertas, modificar los documentos de la Solicitud de Cotización mediante enmiendas, ya sea a solicitud de Proyecto o en atención a aclaraciones solicitadas por los Oferentes.
7. Precio de la oferta: los precios cotizados deberán expresarse en Guaraníes, IVA incluido. Los precios indicados en la oferta incluirán todos los costos, gastos, riesgos, responsabilidades y obligaciones en que el oferente deba incurrir. No se aceptarán precios reajustables. Los precios expresados en modalidad plaza deberán indicarse en precio neto y por separado los montos correspondientes a impuestos aplicables.
8. Forma de pago al/los Proveedor/es: los pagos se harán efectivos en Guaraníes, mediante cheque de plaza o transferencia a la cuenta bancaria que el Proveedor indique en su oportunidad.

Los pagos se realizarán de la siguiente forma:

El Proyecto hará efectivos los pagos antes indicados, dentro de los diez (10) días hábiles siguientes de recibida la factura/documentación correspondiente.

9. Previa firma de la correspondiente Orden de Compra el Proveedor deberá presentar una Garantía de Fiel Cumplimiento de Contrato. La garantía (póliza o aval bancario) será emitida por un banco legalmente establecido y ejecutable en Paraguay, en Guaraníes por un monto equivalente al diez (10%) por ciento del valor de la adquisición. El documento se emitirá a nombre del Crédito Agrícola de Habilitación (CAH) y su vigencia excederá en treinta (30) días calendario adicionales a la fecha prevista de finalización de la prestación de los servicios. La garantía será devuelta al Proveedor una vez cumplida la prestación de los servicios a entera satisfacción del Proyecto.
 10. Salvo casos de fuerza mayor debidamente comprobados por el Proyecto, si el Proveedor se atrasara en el cumplimiento de sus obligaciones con relación al plazo de entrega estipulado en su propuesta, se hará pasible a una multa equivalente al medio por ciento (0.5%) del monto total de su oferta por cada día calendario de atraso, multa que será descontada de la factura correspondiente de pago, hasta un máximo de un 10% del valor total del contrato.
 11. A partir de la fecha de firma de la Orden de Compra, el Proveedor se obliga a la prestación de los servicios a entera satisfacción del Proyecto. El Proyecto, podrá rechazar el material que no cumpla con las especificaciones mínimas exigidas en la presente Solicitud y que no correspondan a las presentadas en la oferta, asumiendo el Proveedor las responsabilidades totales para su sustitución.
-



12. El período de garantía de los bienes, contado a partir de la fecha de entrega de los mismos, será de mínimo (*número*) (*años/meses*) para los ítems (*número*). Dentro del plazo de garantía el Proveedor se obliga a la corrección de defectos en un máximo de cuarenta y ocho (48) horas. (NO APLICA)
13. Lugar de entrega de los bienes según se indica en la Sección 2-Formulario de Especificaciones Técnicas mínimas requeridas.
14. Los oferentes deberán cotizar los *ítems completos*. La adjudicación se realizará a nivel de *ítem*, pudiéndose adjudicar el mismo en forma total o parcial en función al presupuesto estimado por el Proyecto. Las condiciones de la oferta presentada por el oferente se considerarán válidas tanto en caso de adjudicación total como adjudicación parcial.
15. El Comité de Evaluación designado para el proceso de evaluación, verificará en primera instancia, el cumplimiento de la documentación legal, especificaciones técnicas y requerimientos mínimos solicitados, aquellas ofertas que cumplan con lo requerido obtendrán la habilitación técnica y por tanto sus ofertas económicas serán consideradas para adjudicación. La adjudicación recaerá sobre el *ítem* evaluado como más bajo, esto es, el de menor precio entre las ofertas técnicamente habilitadas.
16. El Proyecto, se reserva el derecho de rechazar todas o alguna de las ofertas presentadas.
17. El Proyecto, se reserva el derecho de aumentar o disminuir al momento de adjudicar el contrato la cantidad de bienes consignada en la lista correspondiente hasta en un 25% sin que varíen los precios unitarios y otras estipulaciones y condiciones.
18. El Proyecto, dentro del plazo de vigencia de validez de las ofertas notificará a todas los oferentes los resultados de la evaluación. A partir de la fecha de notificación de resultados, los oferentes dispondrán de un plazo de cinco (5) días hábiles para dar vista al Informe de Recomendación de Adjudicación y solicitar aclaraciones, presentar reclamos, etc. Luego de dicho plazo y de no mediar solicitudes de aclaración o reclamos se procederá a la firma de la/s correspondiente/s Orden de Compra con la/s firma/s adjudicataria/s.
19. El mecanismo formal de solución de diferencias que se aplicará en el marco de la presente solicitud de cotización, así como durante el período contractual será el siguiente:

Solución amigable: En caso de haber cualquier divergencia o controversia de carácter técnico entre el Proyecto y el Proveedor en relación con el Contrato o de la ejecución de los servicios o después de su terminación, y ya sea antes o después de la terminación, resolución, abandono o incumplimiento del Contrato, las partes harán lo posible por llegar a una solución amigable de todas las controversias mediante negociaciones directas en el plazo de quince (15) días calendario.

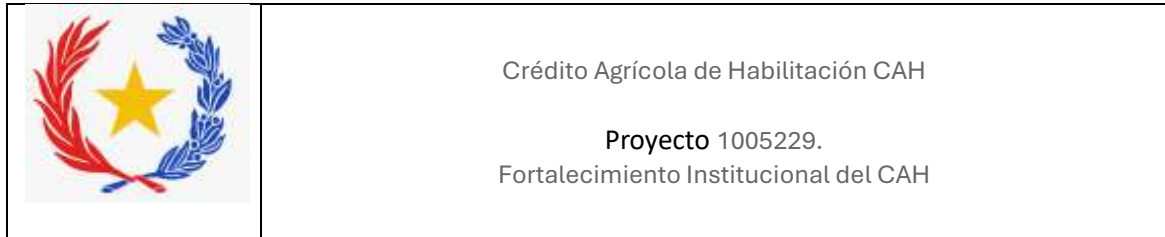


Crédito Agrícola de Habilitación CAH

Proyecto 1005229.

Fortalecimiento Institucional del CAH

Arbitraje Comercial: A menos que la disputa, controversia o reclamación entre las partes mencionada *supra* se pueda resolver amigablemente conforme a lo dispuesto en el párrafo precedente del presente artículo dentro de los sesenta (60) días de que una de las partes hubiere recibido de la otra una petición de arreglo amigable, dicha disputa, controversia o reclamación será sometida a arbitraje por cualquiera de las partes de conformidad con el Reglamento de Arbitraje de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional que estuviera vigente en esa oportunidad, incluidas las disposiciones sobre ley aplicable. El tribunal arbitral no podrá conceder indemnizaciones punitivas. El laudo arbitral que se pronuncie como resultado de ese arbitraje será la resolución definitiva y vinculante de la controversia, reclamación o disputa entre las partes.



Sección 2 (a) - ESPECIFICACIONES TÉCNICAS MÍNIMAS REQUERIDAS Y OFERTADAS DE LA SDC.

-
-

ESPECIFICACIONES TÉCNICAS MÍNIMAS REQUERIDAS

ESPECIFICACIONES TÉCNICAS MÍNIMAS REQUERIDAS		Unidad de medida	Cantidad
Todos los bienes deberán cumplir con los siguientes requisitos mínimos			
Ítem	Descripción		
1	SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC)	Mes	6

SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

1. ANTECEDENTES

El Crédito Agrícola de Habilitación (CAH) , en cumplimiento de las normativas y leyes vigentes en la República, incluyendo la Resolución MITIC Nro. 277/2020 y las recomendaciones de los marcos de trabajo y estándares internacionales, busca contratar los servicios de una empresa especializada en ciberseguridad para servicios de monitoreo, gestión y respuesta ante incidentes de seguridad 24x7x365 de los nodos de su infraestructura crítica, a través de un servicio SOC (Security Operation Center) y Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) que permita generar alertas tempranas en cuanto a tráfico malicioso, posibilidades de accesos no autorizados o gestación de ataques cibernéticos, garantizando la confidencialidad, integridad y disponibilidad de la información en los sistemas críticos.

2. OBJETIVOS

El objetivo de este llamado es contratar un servicio externalizado que apoye al Crédito Agrícola de Habilitación (CAH) en la operación, vigilancia y gestión continua de la seguridad de la información, de acuerdo con las buenas prácticas establecidas en los estándares internacionales aplicables.

El servicio deberá abarcar, como mínimo:

- Monitoreo y análisis continuo de eventos de seguridad para detectar actividades anómalas y posibles amenazas en tiempo real.
- Identificación y evaluación permanente de amenazas y vulnerabilidades, garantizando una comunicación oportuna y acciones preventivas.
- Gestión integral de incidentes de seguridad, cubriendo todo su ciclo de vida: registro, análisis, contención, recuperación y lecciones aprendidas.
- Generación de reportes e indicadores periódicos que apoyen el seguimiento, la toma de decisiones y la mejora continua del sistema de seguridad de la información.
- Asesoramiento especializado para fortalecer el Sistema de Gestión de Seguridad de la Información y optimizar los controles implementados.

3. ALCANCE DEL PROYECTO

Los servicios proporcionados por el SOC deben incluir, pero no estar limitados a:



Crédito Agrícola de Habilitación CAH

Proyecto 1005229.
Fortalecimiento Institucional del CAH

1. Monitoreo constante de los sistemas de información y la infraestructura de red del Crédito Agrícola de Habilitación (CAH) .
2. Análisis de registros de seguridad (logs) y alertas de seguridad generadas por sistemas y aplicaciones.
3. Detección y análisis de comportamientos, Trazabilidad de actividades sospechosas.
4. Respuesta a incidentes, incluyendo la coordinación con el personal interno para la mitigación de amenazas.
5. Generación de informes periódicos de seguridad que incluyan análisis de amenazas, incidentes y recomendaciones de mejora.
6. Asesoramiento y apoyo en la implementación de mejores prácticas de seguridad cibernética.
7. Cumplimiento con normativas y regulaciones de seguridad aplicables al Crédito Agrícola de Habilitación (CAH). En especial al Manual de Gobierno y Control de Tecnología de la Información Normado por Banco Central del Paraguay.

4. CONFIDENCIALIDAD Y SEGURIDAD DE DATOS SENSIBLES.

El SOC deberá garantizar el cumplimiento estricto de los principios de confidencialidad, integridad y disponibilidad de la información, implementando y manteniendo controles técnicos, organizativos y procedimentales adecuados para proteger los datos bajo su custodia. Dichos controles deberán alinearse con estándares internacionales de seguridad de la información, asegurando la protección frente a accesos no autorizados, uso indebido, alteración, pérdida o divulgación de la información.

Para tal propósito, el oferente que resulte adjudicado deberá firmar las siguientes Clausulas al inicio de la prestación de sus servicios.

1.Cláusula de confidencialidad reforzada

El SOC deberá garantizar la confidencialidad de toda la información, registros, eventos, incidentes y datos a los que tenga acceso durante la prestación del servicio.

Dicha información no podrá ser divulgada, transferida ni utilizada para fines distintos a los establecidos en el contrato, salvo autorización expresa del cliente o requerimiento legal debidamente fundamentado.

2.Cláusula de segregación de información del cliente

El SOC deberá garantizar la segregación lógica y/o física de la información correspondiente a cada cliente, asegurando que los datos, registros y eventos de seguridad no sean accesibles ni visibles por terceros ni por otros clientes del servicio.

3.Cláusula de retención y custodia de log

A. Generación y Registro de Eventos

El SOC deberá garantizar la recopilación, registro y almacenamiento de los logs generados por los sistemas, aplicaciones, dispositivos de red, plataformas de seguridad y demás componentes incluidos dentro del alcance del servicio de monitoreo.

B. Integridad y Protección de los Logs

Los registros deberán almacenarse de manera que se preserve su integridad, confidencialidad y disponibilidad, evitando su alteración, eliminación no autorizada o pérdida. Para ello, se podrán emplear mecanismos como:

- Control de acceso restringido
- Sellado temporal (timestamp)
- Hash o mecanismos de verificación de integridad
- Almacenamiento seguro o inmutable (WORM o equivalente)


C. Periodo de Retención

Los logs deberán conservarse durante un período mínimo de 36 meses, salvo que normativas regulatorias, requerimientos legales o investigaciones de seguridad requieran un plazo mayor.

D. Custodia y Responsabilidad

El SOC será responsable de la custodia segura de los logs, garantizando su disponibilidad para:

- investigaciones de incidentes de seguridad

	<p style="text-align: center;">Crédito Agrícola de Habilitación CAH</p> <p style="text-align: center;">Proyecto 1005229. Fortalecimiento Institucional del CAH</p>
---	---

- auditorías internas o externas
- requerimientos regulatorios
- análisis forense digital

E. Acceso a los Registros

El acceso a los logs estará restringido únicamente a personal autorizado y debidamente autenticado. Todo acceso deberá quedar registrado y ser auditado.

F. Entrega y Preservación de Evidencias

En caso de incidentes de seguridad, investigaciones o requerimientos legales, el SOC deberá proporcionar los registros relevantes, preservando la cadena de custodia y validez como evidencia digital.

G. Eliminación Segura

Una vez cumplido el período de retención establecido, los logs deberán eliminarse mediante procedimientos seguros que impidan su recuperación no autorizada.

5. REQUISITOS TÉCNICOS SOLICITADOS

El servicio operará en las instalaciones del Oferente para las funciones de monitoreo, operación y coordinación, en el horario de servicio 7x24x365.

El oferente debe tener en cuenta la provisión de todos los recursos necesarios para suministrar el servicio. La arquitectura necesaria para el funcionamiento estará totalmente a cargo del oferente, permitiéndose arquitectura híbrida (recursos en nube institucional o datacenter del Crédito Agrícola de Habilitación (CAH) y/o del oferente).

6. INVENTARIO DE EQUIPOS Y SERVICIOS EXISTENTES

Equipo / Plataforma		Cantidad
1	Cantidad total de usuarios nominales y de servicios	700
2	Cantidad de servidores físicos y virtuales	70
3	Estaciones de trabajo, laptops, dispositivos móviles	500
4	Sucursales	82
5	Firewall Borde	2

7. PLANILLA DE ESPECIFICACIONES TÉCNICAS

Requisito	Descripción	Cumple / No cumple
Generalidades	El oferente debe contar con todas las herramientas y servicios descritos en esta planilla de Especificaciones Técnicas para realizar el servicio solicitado por la contratante, quedando a su entera responsabilidad los recursos tecnológicos redundantes y de conectividad (mínimo 200 MBPS de subida y 40 MBPS de bajada) redundantes, necesarios para la prestación del servicio.	
	El servicio deberá integrar fuentes de inteligencia de amenazas externas, tanto públicas como privadas (por lo menos 1 (una) privada), que permitan enriquecer los eventos, generar indicadores de compromiso (IoC) y apoyar las decisiones de detección y respuesta. La selección de las fuentes será responsabilidad del oferente, quien deberá garantizar su actualización, relevancia y efectividad operativa.	



Crédito Agrícola de Habilitación CAH

Proyecto 1005229.

Fortalecimiento Institucional del CAH

	El servicio debe contar con un sistema de gestión de incidentes, que genere tickets sobre los mismos y las acciones de mitigación auditables, con interacción con el usuario para realizar confirmación de actividad sospechosa. Este sistema de gestión de incidentes debe tener la capacidad de identificar el equipo afectado, mantener un historial de eventos por cada equipo monitoreado y ofrecer estadísticas auditables. El esquema de notificaciones debe tener niveles de escalación de comunicaciones	
	El oferente debe realizar la transferencia tecnológica al personal técnico del Crédito Agrícola de Habilitación (CAH) en cuanto a las buenas prácticas de ciberseguridad	
	El oferente debe realizar análisis del comportamiento de la infraestructura administrada y monitoreada para correlacionar incidentes y determinar proactivamente problemas en la operación	
	Debe realizar análisis de tendencias sobre los eventos y plataformas monitoreadas.	
	Debe contar con informes de análisis de la capacidad de la infraestructura administrada para identificar tendencias para prevenir proactivamente incidentes y/o degradación del servicio.	
	Debe contar con un informe mensual detallado sobre alertas mundiales que puedan afectar la seguridad de la infraestructura monitoreada, así como las recomendaciones para elevar el nivel de la seguridad en la misma.	
Funcionalidades Básicas del Servicio	Debe contar con herramientas digitales para la gestión de eventos vía sistema de ticket, email, mensaje y/o teléfono.	
	Debe contar con herramientas y métodos para prevenir la fuga de información en todos los dispositivos utilizados para la provisión del servicio, incluyendo dispositivos portátiles que salgan de las instalaciones del SOC.	
	Debe almacenar y precautelar las bitácoras (logs) de los equipos y dispositivos utilizados para la provisión del servicio, para análisis cuando se requiera.	
	Debe contar con procesos de eliminación segura de la información que ya no se requiera para la provisión del servicio.	
	Debe garantizar la generación y conservación de copias de respaldo (backups) de toda la información producida por la plataforma SIEM, incluyendo —pero no limitándose a— las configuraciones del servicio y de los servidores SIEM, así como las reglas del servicio que se agreguen, modifiquen o eliminen, siguiendo la estrategia de respaldos 3-2-1	
	Para el servicio SOC se deben tener discriminados claramente los procesos, personas y roles que intervienen en las tareas de operación de seguridad, con las funciones de inteligencia de amenazas, monitoreo, correlación y análisis de tendencias en seguridad en niveles SOC L1, L2 y L3.	
	El servicio SOC debe contar con procesos de priorización de atención de incidentes, los cuales se deben basar en una metodología clara de riesgos e impacto.	
	El oferente debe contar con su propio equipo de CSIRT (Computer Security Incident Response Team)	
	El esquema de operación del SOC debe contar con un DRP (Disaster Recovery Plan) que garantiza la continuidad del servicio.	
	El SOC debe contar con procesos definidos para la detección, categorización y alertamiento temprano y oportuno de incidentes de seguridad, así como una matriz de escalamiento identificando al personal clave de la contratante que debe ser involucrado.	
El oferente deberá realizar pruebas de vulnerabilidad periódicas y, de corresponder, pruebas de intrusión planificadas, con una frecuencia mínima anual o a requerimiento de la institución, según criticidad y alcance definido.		



Crédito Agrícola de Habilitación CAH

Proyecto 1005229.

Fortalecimiento Institucional del CAH

Servicio de Gestión, Correlación y Monitoreo de Logs, Eventos, Alarmas e Incidentes	El SOC debe ser capaz de procesar, monitorear y correlacionar todas las fuentes de datos descritas en la sección "INVENTARIO DE EQUIPOS Y SERVICIOS EXISTENTES EN EL Crédito Agrícola de Habilitación (CAH)", siendo posible incluso un aumento de al menos un 30%, sin pérdidas de logs o eventos.	
	EL SOC debe tener la capacidad de recibir logs en formato crudo (RAW) a través de los siguientes mecanismos:	
	- Syslog (TCP o UDP).	
	- Transferencia remota de archivos con logs crudos por SCP (Secure Copy), SFTP (Secure FTP).	
	- Archivos de logs en sistemas de archivos remotos mediante NFS y CIFS.	
	- APIs.	
	La remisión de los eventos hacia el SOC debe ser realizada a través del protocolo de transporte TCP y con técnicas de cifrado SSL (Secure Sockets Layer). Toda la comunicación, además, debe estar encriptada a nivel de VPN SSL / ipsec redundante con el Crédito Agrícola de Habilitación (CAH).	
	Debe ser factible enviar eventos y logs en tiempo real hacia el servicio de gestión y correlación. También debe ser factible el envío bajo demanda en modalidad asíncrona, según requerimientos del Crédito Agrícola de Habilitación (CAH).	
	El servicio debe proveer los componentes de recolección automática a nivel de software que permitan, desde el origen, la normalización completa de los eventos, es decir únicamente enviarán hacia el servicio de monitoreo los eventos previamente estructurados en campos específicos para la correlación, retención, análisis y reporte de los eventos.	
	Los componentes que realizan la recolección de eventos deben utilizar el protocolo TCP como medio de transporte hacia el servicio de correlación, verificando constantemente el estado de la conexión por medio de un pulso o Heartbeat. Ante la eventual pérdida de la conexión entre el componente de recolección y el motor de correlación, el primero deberá almacenar de forma inmediata los eventos bajo una cache de tamaño configurable hasta que se reanude dicha conexión, realizando la transmisión de los eventos hasta vaciar el cache.	
	La transmisión de los datos entre los componentes recolectores de eventos y el motor de correlación debe utilizar mecanismos de compresión de datos.	
	Debe ser posible configurar controles de uso de ancho de banda para el envío de los eventos recolectados, así como priorizar las transacciones críticas para su envío inmediato.	
	Debe ser posible el filtrado de eventos particulares desde el origen, con lo que se reducirá el volumen de eventos que recibirá el motor de correlación en conformidad a la publicación NIST SP 800-92.	
El servicio debe permitir correlacionar la información de Accesos a nivel perimetral (Firewalls), junto con las vulnerabilidades detectadas a nivel de equipos, esto con el fin de simular propagaciones de malware y explotaciones (exploits) de vulnerabilidades.		
El servicio debe ser capaz de detectar fluctuaciones en la recepción de logs por fuente de información y proveer el estado de la conectividad de los mismos al motor de correlación (UP/DOWN).		
El servicio debe ofrecer mecanismos de búsquedas rápidas, eficientes y que permitan ser exportadas a formatos tales como CSV.		



Crédito Agrícola de Habilitación CAH

Proyecto 1005229.

Fortalecimiento Institucional del CAH

El servicio debe incluir la provisión de herramientas y conectores orientados a gestionar el ciclo completo de un incidente desde su detección, análisis, escalamiento, cierre y documentación (con archivos de evidencias adjuntas), con la finalidad de generar una base de conocimiento para los analistas. La herramienta debe ser capaz de correlacionar los eventos con los Activos de Información de la Entidad.	
El servicio debe soportar, procesar y almacenar 12 meses de información en línea como mínimo.	
El servicio debe ser alimentado por fuentes de inteligencia externas de amenazas que contengan listas de reputación (IP) y/o dominios catalogados como sospechosos para la generación de indicadores de compromiso (IoC).	
El motor analítico de la solución SIEM utilizada por el SOC debe permitir identificar patrones anómalos de comportamiento por usuario y/o IP.	
El servicio debe incluir la generación de indicadores de compromiso para cada activo monitoreado, basándose en los ataques recibidos y el uso de amenazas identificadas.	
Debe ser capaz de identificar al menos los siguientes ataques e información de los ataques (lista enunciativa, no exhaustiva):	
- Accesos no autorizados.	
- Denegación de servicio.	
- Explotación de vulnerabilidades.	
- Fuerza bruta/login.	
- Escaneo de puertos.	
- Principales orígenes de ataque.	
- Principales destinos de ataque.	
- Ubicación geográfica del ataque.	
- Orígenes/destinos reportados por fuentes de inteligencia de seguridad.	
- Acceso por parte de los usuarios a dominios diferentes a los autorizados.	
Debe ser capaz de detectar el uso de aplicaciones o accesos a la plataforma que no concuerden con el patrón histórico de uso o acceso.	
Debe ser capaz de recolectar eventos de aplicaciones, sistemas o plataformas no predefinidas, usando para ellos alguna característica de parsing.	
El servicio debe realizar correlación de incidentes de seguridad, con capacidad de integrar inteligencia derivada de incidentes similares en el sector o región relacionada al Crédito Agrícola de Habilitación (CAH).	
El servicio debe tener la posibilidad de integrar las vulnerabilidades detectadas por el Crédito Agrícola de Habilitación (CAH) con el monitoreo y correlación y se deben declarar incidentes ante vulnerabilidades detectadas.	
Debe mantener un respaldo de la lista de reglas de detección de amenazas o eventos de seguridad utilizadas por el SIEM, y notificar cuando las mismas son dadas de baja o de alta (nuevas reglas).	
El oferente deberá proveer una plataforma SIEM madura y ampliamente utilizada en entornos corporativos, desarrollada y mantenida por una comunidad o fabricante reconocido a nivel internacional.	
El oferente será responsable del soporte técnico integral de la plataforma SIEM durante toda la vigencia contractual, garantizando:	
- Actualizaciones periódicas	
- Corrección de vulnerabilidades	
- Escalamiento técnico	




Crédito Agrícola de Habilitación CAH

Proyecto 1005229.

Fortalecimiento Institucional del CAH

	<ul style="list-style-type: none"> – Continuidad operativa – Cumplimiento de los SLA establecidos 	
SOAR	El servicio de SOC debe incorporar al menos una herramienta de Orquestación / automatización (SOAR) que permita a los analistas de operaciones trabajar casos junto a los analistas de manejo de incidentes. Las herramientas de SOAR debe ser interoperable con todos los demás elementos del proyecto que el Oferente propone y las que están mencionadas en las presentes especificaciones.	
	El servicio de SOAR debe incluir y/o el proveedor encargarse de la configuración y personalización de los conectores para una cantidad ilimitada playbooks, sin costo adicional.	
	El proveedor debe ofrecer una capacitación en el uso y manejo del SOAR y en el lenguaje de construcción de playbooks.	
Inteligencia de Amenazas	El proveedor debe implementar un servicio cuya plataforma o módulo de inteligencia de amenazas (CTI) integre las diversas fuentes de inteligencia, tanto públicas como privadas (provistas como parte del servicio de centro de operaciones de seguridad SOC)	
	El sistema debe permitir la creación, actualización y distribución de listas dinámicas de indicadores (como direcciones IP, dominios y hashes) para reforzar las políticas de seguridad. Estas listas deben poder integrarse con el SIEM y el SOAR, automatizando bloqueos y respuestas ante incidentes.	
	El mecanismo debe asegurar sincronización en tiempo real y control centralizado, garantizando que los cambios se propaguen de forma segura y eficiente en todos los dispositivos y plataformas conectadas.	
	Además, debe permitir la gestión granular de cada lista para mantener la trazabilidad y la efectividad en la respuesta ante amenazas.	
	El servicio debe contar con observables (base de información de incidentes propias del SOC) los cuales permitan comparar IP (fuente o destino), usuarios, procesos, nombre de host, URL, dominios, archivos, hash y cualquier potencial componente de un evento de seguridad para construir nuevos IoC (indicadores de compromiso) sin la necesidad de fuentes externas de inteligencia de amenazas. El servicio debe permitir usar los datos del score de riesgos, la prioridad del evento, la urgencia, impacto del negocio, importancia del usuario o activo afectado para priorizar cual debe ser el primer evento de la cola a ser tratado por todo el ciclo de procesos que hacen parte del ejercicio de respuesta a incidentes de ciberseguridad.	
Respuesta a Incidentes, Analítica y Capacidades de Contención	Debe contar con un Centro de Incidentes que permita la intercomunicación entre los diferentes componentes del servicio.	
	El Centro de Incidentes debe contar con la capacidad de categorizar los eventos de seguridad detectados y correlacionados por el servicio.	
	El Centro de Incidentes debe permitir ejecutar ciclos o procesos de respuesta a incidentes de forma paralela, los cuales pueden ser ejecutados de forma automática o manual por el grupo de respuesta a incidentes.	
	El oferente deberá contar con capacidades técnicas y procedimentales para la adquisición, análisis y preservación de evidencias digitales, de forma remota y local, sobre sistemas Windows, Linux	
	Las capacidades podrán implementarse mediante herramientas propias, de código abierto o comerciales, siempre que se garantice:	

	<p>Crédito Agrícola de Habilitación CAH</p> <p>Proyecto 1005229.</p> <p>Fortalecimiento Institucional del CAH</p>
---	--

	<ul style="list-style-type: none"> – Integridad de la evidencia – Cadena de custodia – Trazabilidad de acciones – Documentación de resultados 	
Plantel Técnico	Debe contar con un equipo que garantice todo lo solicitado en las Especificaciones Técnicas conforme a lo establecido en la Sección de Capacidad Técnica del PBC.	
	Reemplazo de Profesionales: Se aclara que el Crédito Agrícola de Habilitación (CAH) se reserva el derecho de solicitar el reemplazo de profesionales durante la ejecución del contrato, si los mismos no cumplen con el desempeño esperado. El nuevo profesional propuesto deberá contar con la aprobación del Crédito Agrícola de Habilitación (CAH), estando obligado a cumplir con el mismo perfil original solicitado o superior.	
	Una vez recibida la solicitud de reemplazo de personal por parte del Crédito Agrícola de Habilitación (CAH), el oferente adjudicado deberá considerar hasta un máximo de 45 (cuarenta y cinco) días calendario, para la incorporación de este profesional sin afectar la continuidad del servicio, salvo orden expresa de la institución en la solicitud de reemplazo.	
Acuerdo de Nivel de Servicio (SLA)	Tiempo de Servicio: 24/7/365	
	Tiempo de notificación ante incidentes detectados por el proveedor o reportados por la Institución: ≤ 60 (sesenta) minutos	
	Asistencia in situ ante incidentes críticos: ≤ 2 (dos) horas	

8. EXPERIENCIA REQUERIDA

Con el objetivo de calificar la experiencia del oferente, se considerarán los siguientes índices:


- Demostrar la experiencia en servicios de monitoreo, gestión y respuesta ante incidentes de seguridad de la presente contratación, con copia de contratos y/o facturaciones de venta y/o recepciones finales por un monto equivalente al 50 % como mínimo del monto total ofertado en la presente licitación, dentro de los 3 últimos años (2023, 2024 y/o 2025)
- El oferente deberá demostrar al menos 5 (cinco) años de experiencia en el mercado en la prestación de los servicios requeridos, mediante la presentación de certificados o constancias de servicios satisfactorio, emitidas por al menos 5 (cinco) Instituciones Públicas y/o Privadas, donde se comprueben los siguientes servicios:
 - Servicios de auditorías de vulnerabilidades o pentesting
 - Servicios de gestión y respuesta ante incidentes cibernéticos relacionados a compromisos de sistemas web, ransomware, DoS, Escaneos/Fuerza Bruta, Malware, etc.
 - Servicios de asesorías en ciberseguridad relacionadas arquitecturas de ciberseguridad y/o desarrollo de documentación relacionada a ciberseguridad.

Se aclara que no será necesario que en la constancia o certificado se mencionen todos los servicios, siempre y cuando se demuestre al menos 1 (una) experiencia para cada servicio requerido.

9. CAPACIDAD TÉCNICA

El oferente deberá proporcionar evidencia documentada que demuestre su cumplimiento con los siguientes requisitos de capacidad técnica:

1. El oferente deberá poseer certificados de Gestión de Calidad (CSG) según la norma ISO 9001 y/o de Gestión de Servicios de TI (ITSM) según la norma 20000, para garantizar estándares internacionales de calidad para el cumplimiento de los servicios.
2. El oferente deberá poseer certificación de Calidad ISO 27001 vigente, con el objetivo de cumplir con los más altos estándares de seguridad de la información, preservando la confidencialidad, integridad y disponibilidad de la información relacionada con la convocan

	<p style="text-align: center;">Crédito Agrícola de Habilitación CAH</p> <p style="text-align: center;">Proyecto 1005229.</p> <p style="text-align: center;">Fortalecimiento Institucional del CAH</p>
---	--

3. Con el fin de garantizar un nivel mínimo de competencia técnica en ciberseguridad, se exige que el personal técnico asignado cuente con certificaciones reconocidas internacionalmente. El oferente deberá contar con los siguientes perfiles técnicos:

1 (un) SOC Manager / CSIRT Director:	con título de maestría en Ciberseguridad, con habilidades avanzadas en Cyber Defensa y Threat Hunting, y al menos 2 (dos) certificaciones emitidas por instituciones de reconocimiento internacional (tales como CompTIA, ISC2, EC-Council, entre otras), con una experiencia mínima de cinco (5) años desempeñando funciones en el rubro.
1 (un) Coordinador de Ciberseguridad:	3 (tres) años de experiencia en el rubro con certificaciones en sistema de gestión y auditoría conforme a la norma ISO/IEC 27001, quien será el responsable de la coordinación general del servicio y de los informes a ser remitidos entre el Banco y el proveedor.
2 (dos) Analistas de Ciberseguridad L1	2 (dos) años de experiencia relevante en el rubro con certificaciones en ciberseguridad. Se aceptarán certificaciones emitidas por entidades reconocidas del sector, incluyendo plataformas de formación técnica especializada como Hack The Box, PortSwigger Academy, TryHackMe, entre otras, que cuenten con reconocimiento en la comunidad profesional de ciberseguridad.
2 (dos) Analistas de Ciberseguridad L2	2 (dos) años de experiencia en el rubro con título de diplomado o especialización en ciberseguridad, o con al menos 2 (dos) certificaciones de nivel intermedio o avanzado en ciberseguridad, emitidas por alguna Institución internacionalmente reconocida (CompTIA, ISC2, EC-Council, etc.).
1 (un) Arquitecto / Ingeniero de Ciberseguridad	<p>Ingeniero y/o Licenciado en Informática o afines con 3 (tres) años de experiencia en el rubro con certificaciones emitidas por alguna Institución internacionalmente reconocida (CompTIA, ISC2, EC-Council, etc.).</p> <p>Contar con al menos 3 (tres) de las siguientes certificaciones: CISSP, CND, C)SWAE, SSCP, PenTest+, CEH o similares.</p> <p>Certificaciones oficiales o acreditaciones técnicas equivalentes en la plataforma SIEM</p> <p>a ser utilizada, emitidas por el fabricante, comunidad o programas reconocidos</p>

Estos técnicos deberán residir en el País y ser del staff permanente del oferente con una antigüedad mínima de 12 meses, demostrable con planilla de IPS (Instituto de Previsión Social) y/o Contrato profesional vigente, en la cual se demuestre la dependencia laboral.

4. El oferente deberá presentar Declaración jurada donde declare que cumplirá con las especificaciones técnicas y con los plazos de entrega de los servicios.



Crédito Agrícola de Habilitación CAH

Proyecto 1005229.
Fortalecimiento Institucional del CAH

Sección 2 (b) – DECLARACIÓN JURADA DE CUMPLIMIENTO DE ESPECIFICACIONES TÉCNICAS

Yo, [NOMBRE COMPLETO DEL REPRESENTANTE LEGAL], con cédula de identidad N° [NÚMERO], en mi carácter de representante legal de la empresa [NOMBRE DE LA EMPRESA], con RUC N° [NÚMERO], bajo fe de juramento declaro lo siguiente:

Que, en el marco del proceso de contratación denominado “[NOMBRE DEL PROCESO / LICITACIÓN]”, me comprometo expresa e irrevocablemente a cumplir en su totalidad con todas las especificaciones técnicas, requisitos, condiciones y características establecidas en el Pliego de Bases y Condiciones, así como en sus anexos y documentos complementarios.


Asimismo, declaro que los servicios ofertados cumplen plenamente con los estándares de calidad exigidos, y que cuento con la capacidad técnica, operativa y logística necesaria para garantizar su correcta provisión dentro de los plazos y condiciones estipulados.

Me responsabilizo por la veracidad de la información proporcionada en la presente declaración, asumiendo las consecuencias legales correspondientes en caso de falsedad u omisión.

En prueba de conformidad, firmo la presente declaración jurada en la ciudad de [CIUDAD], a los [DÍA] días del mes de [MES] del año [AÑO].

Nombre del Oferente _____

Firma del Oferente _____

	<p>Crédito Agrícola de Habilitación CAH</p> <p>Proyecto 1005229. Fortalecimiento Institucional del CAH</p>
---	--

Sección 2 (c) -LISTA DE PRECIOS DE BIENES Y SERVICIOS CONEXOS DE LA SDC

Nombre del Oferente _____

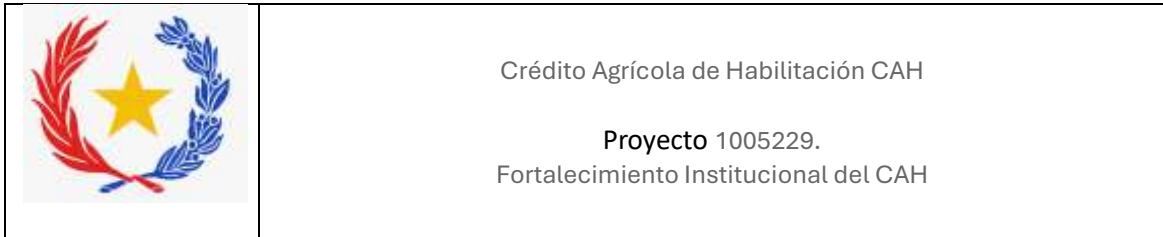
Fecha _____

Número de la Solicitud de Cotización _____

Firma del Oferente _____

Breve descripción de los bienes (y servicios conexos ofertados)	Cantidad	Precio unitario (modalidad) (moneda))	Precio total (modalidad) (moneda)
1. SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) – (MESES)	6				
		Precio neto (moneda)			
		Impuestos (moneda)			
		Precio total modalidad (moneda)			
Precio total (modalidad Incoterm) (moneda)					

* En caso de discrepancia entre el precio unitario y el precio total, prevalecerá el precio unitario.



Sección 2 (c) - CARTA DE PRESENTACIÓN DE LA SDC

Estimados señores:

Tras haber examinado las Condiciones Especiales y las Especificaciones Técnicas de la Solicitud de Cotización No. *(indicar numero y nombre)* los suscritos ofrecemos proveer y entregar *(indicar breve descripción del/de los items/lotés y servicios ofertados)* de conformidad con los diseños, condiciones y especificaciones por la suma de *(indicar monto total de la oferta en palabras y cifras)* en modalidad *(indicar modalidad)* o el monto que se determine por adjudicación parcial con base al formulario de oferta que se adjunta a la presente propuesta y que forma parte integrante de ella.

Si nuestra oferta es aceptada, nos comprometemos a iniciar las entregas dentro de *(indicar número)* días calendario y a completar la entrega de todos los artículos dentro de los *(indicar número)* días calendario siguientes a la fecha de firma de la orden de compra. A su vez, en caso de ser requerido, nos comprometemos a entregar una garantía bancaria por un monto de por lo menos el (Número) por ciento del total de la adquisición para asegurar el debido cumplimiento de la misma.

Convenimos en mantener esta oferta por un período de *(indicar número)* días calendario a partir de la fecha fijada para la apertura de ofertas, la oferta nos obligará y podrá ser aceptada en cualquier momento antes de que expire el período indicado.

Esta oferta, junto con la aceptación por escrito incluida en la notificación de adjudicación, constituirá un contrato obligatorio hasta que se prepare y firme una orden de compra formal.

Fecha:

Firma y aclaración de firma:

En calidad de:

Legalmente autorizado para firmar la oferta en nombre de:



Crédito Agrícola de Habilitación CAH

Proyecto 1005229.
Fortalecimiento Institucional del CAH

Sección 3 - MODELO DE ORDEN DE COMPRA DE LA SDC

ORDEN DE COMPRA DE BIENES y/o SERVICIOS CONEXOS

N°

		<i>(Número y Nombre del proceso de compra)</i> Solicitado por:	
Emitida por: [Datos del Proyecto]		Entregar en:	
Persona de contacto:		Persona contacto:	
Proveedor (nombre y dirección): Tel: Fax:		Forma e instrucciones de embarque:	
Persona Contacto:			
Forma de pago:		Fecha de entrega:	
Breve Descripción de los bienes y/o Servicios Conexos	Cantidad	Precio Unitario (modalidad y moneda)	Precio Total (modalidad y moneda)
		Sub-Total	
		Impuestos	
		Total (modalidad y moneda)	

Acuerdo del Proveedor:	[Número y Nombre del Proyecto]	Condiciones especiales:
Empresa:		



Crédito Agrícola de Habitación CAH

Proyecto 1005229.
Fortalecimiento Institucional del CAH

Firma:		
Aclaración:		
Fecha:	Fecha:	CUENTA PRESUPUESTAL