INVITACIÓN PÚBLICA

SOLICITUD DE OFERTAS PARA LA RENOVACIÓN DEL LICENCIAMIENTO ANTIVIRUS-Crowstrike

CONTRATANTE: COOPERATIVA FINANCIERA DE ANTIOQUIA CFA

FECHA
4 de septiembre de 2025

1. ALCANCE Y OBJETO DE LA INVITACIÓN:

CFA está interesado en recibir su oferta para la renovación de la **RENOVACIÓN DEL LICENCIAMIENTO ANTIVIRUS CROWSTRIKE** no se aceptarán otras marcas.

Recibir una propuesta que cumpla con los requisitos solicitados por CFA Cooperativa Financiera para la protección de Endpoints.

Quienes puedan cumplir con la prestación del servicio solicitado, deberán enviar una OFERTA en la cual se contemplen todos los términos, requerimientos y requisitos de la presente Invitación. Dicha oferta constituirá el soporte del CONTRATO que para este efecto se suscriba entre ambas partes**.**

CFA no está obligado a seleccionar a ningún oferente y la evaluación que hará de los parámetros para llevar a cabo la selección se hará de acuerdo a sus particulares necesidades.

CFA en cualquier momento podrá cancelar el proceso de evaluación de oferentes y revocar la presente invitación sin que haya lugar al pago de ningún tipo de indemnización

2. REQUERIMIENTOS TECNICOS

- Se requieren 700 licencias para endpoints que permita incluir sistemas operativos como IOS, Linux y Windows. No debe ser una limitante la cantidad por sistemas operativos, esto quiere decir que se podrán utilizar las 700 licencias para servidores o para linux o para IOS.
- Se requiere de una solución cien por ciento (100%) nube, la cual permita la administración centralizada de estaciones de trabajo y servidores, inclusive si estos se encuentran distribuidos de forma remota.
- La solución debe tener conexión de manera web con doble factor de autenticación
- La solución debe tener conexiones estándar contra aplicaciones y permitir conectarse a nuestro SIEM Logrhythm.
- La aplicación debe permitir generar informes de inventario de dispositivos y estado de salud.
- La solución no debe involucrar hardware o virtualización.
- La solución no debe generar costos operacionales en las premisas, DC o infraestructura de proveedores cloud que pertenezcan a la compañía.
- Si se requieren módulos o funcionalidades adicionales no se deben desplegar consolas o agentes adicionales
- La solución debe contar con dos componentes generales para su operación y correcto desempeño:

- Consola única central 100% nube(cloud) para administración y operación de todos los módulos ofrecidos y futuros.
- Sensores/software que serán instalados en estaciones de trabajo y servidores.
- La solución debe utilizar un mecanismo de comunicación seguro basado en protocolo SSL vía puerto 443 para facilidad de operación con capacidad de limitar el acceso a la consola y grupos de direcciones IP.
- Se requiere que se utilice un único agente EDR/AV en el dispositivo, el cual no requiere ser reiniciado en su instalación como desinstalación
- El proceso de despliegue del sensor debe ser compatible (GPO / PowerShell) .
- El consumo de recursos del agente debe ser en promedio 1% de CPU y no debe tener requerimientos de hardware específicos para su funcionamiento. Sólo se garantizará los recursos para el funcionamiento de las aplicaciones productivas en los dispositivos
- No debe requerir actualizaciones de patrones/ firmas/comportamientos. La solución debe estar basada en AI/ML (Inteligencia Artificial / Machine Learning) se aceptan combinaciones de modelo de firmas/heurística u otros mecanismos no especificados, que deben trabajar en línea o fuera de línea
- La plataforma debe tener la capacidad de poder instalarse en presencia de otra plataforma de antivirus sin interferir en la operación como también no debe requerir reiniciar el equipo tanto en laptop como en servidores. Como no requerir configurar exclusiones/excepciones en el proceso de despliegue inicial
- La solución debe tener la capacidad de integración vía API REST. Esta API debe ser Bi-Direccional.
- La plataforma debe tener la capacidad de configuración de IOCs para su bloqueo o permiso de ejecución de forma personalizada o automatizada vía API.
- La consola de gestión debe dar visibilidad, detalles y reportes de información de alertas, detecciones, de toda la actividad de los dispositivos hasta 90 días consulta en segundos.
- La plataforma debe tener la capacidad de dar el detalle de la telemetría de las alertas y detecciones para poder tener un contexto de los ataques mediante análisis retrospectivos y reconstrucción de los eventos y procesos mediante un árbol de procesos de forma: Gráfica, listado de actividades entre otros.
- La plataforma debe poder establecer control y comunicación directa por medio de línea de comandos con los sensores (win/linux/Mac) a fin de poder ejecutar comandos, correr scripts, saber el estado de procesos, conexiones, sacar archivos, o llevar archivos, reiniciar y otros comandos que permitan acelerar un análisis forense con el acceso directo a los equipos sin herramientas de terceros
- El despliegue de agentes/sensores se debe hacer sobre sistemas operativos:

- Windows7 7SP1 y superiores
- Windows 2008 R2 S1 y superiores
- Linux en distribuciones soportadas (Amazon 1 y 2, CentOs, Oracle, RHEL, SUSE, openSUSE, Ubuntu, Debian, elrepo, Flatcar, IBM, Alma, rocky)
- MAC (BigSur, Monterey, Ventura)"
- Uso de la inteligencia de amenazas basado en la identificación de cómo los adversarios o adversarios actúan en sus campañas para poder identificar TTPs atribuibles a grupos de ciberataques
- Capacidades de detección y prevención de:
- Detección y prevención de virus/malware conocido y desconocido o día cero
- Detección y prevención de TTPs (mitre) en la explotación de vulnerabilidades
- Detección y prevención por indicadores de ataque (File-less attacks)
- Capacidad de independizar la detección de la prevención por políticas
- Identificación y prevención de actividad sospechosa (procesos, registro, script, comandos, drivers)
- Identificación y prevención de procesos de borrado de backup, cifrado, borrado de copias de volúmenes usado por los ataques de Ransomware basado en comportamiento
- Identificación y prevención de movimientos laterales y Accesos a credenciales
- Identificación y prevención de ataques y explotación de vulnerabilidades día cero"
- Capacidades de detección de TTPs en post ejecución como:
    - Capacidad de realizar remediación por indicadores de ataques para evitar persistencia de procesos maliciosos (ASEP)
    - Administración de cuarentena de artefactos para liberar o eliminar de los dispositivos
- La plataforma debe tener capacidad de desarrollar actividades forenses como:
    - Contar con un acceso remoto (vía línea de comando) a los equipos que tengan el agente instalado con perfil de administrador validado vía MFA para incorporar un control dual.
    - Permitir la ejecución de comandos ya integrados de forma remota, y a través de una lista muestre el uso de cada uno de ellos.
- Contar con comandos de recolección de datos que permitan dar paso a investigaciones. Los comandos requeridos son:
    - Explorar el sistema de archivos y extraer archivos.
    - Lista de procesos en ejecución.
    - Extraer el registro de eventos de Windows.
    - Consultar registro de Windows.
    - Enumere las conexiones de red actuales y la configuración de la red.
    - Extraer la memoria de un proceso (memory dump).

- Que cuente con comandos de remediación que permitan reacción sobre una acción puntual. Los comandos requeridos son:
    - Eliminar un archivo.
    - Terminar un proceso (Kill process)
    - Eliminar o modificar la clave o el valor del registro de Windows.
    - Enviar scripts programados
    - Enviar y recibir archivos por demanda"
- La solución deberá contar con la capacidad de aislar una activo (Endpoint/Server) de forma remota, bloqueando así cualquier comunicación externa a la computadora con excepción a la comunicación con la propia consola de gestión de la solución.
- La solución debe hacer un mapeo de alertas basado en el modelo de MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®)
- La solución debe tener la capacidad de crear grupos con la finalidad de ser utilizados en la definición de políticas al menos por dominio, Sistema Operativo, Unidad Organizacional, versión del agente, tipo de equipo, ubicación, esto basado en la metadata de los dispositivos registrados.
- La organización en grupos de forma atomàtica o manual basado en reglas o filtros de acuerdo a los atributos de los dispositivos
- La plataforma debe tener la capacidad de integración con plataforma de inteligencia de terceros de forma nativa como Virus Total, Darktrace.
- La solución debe contar con un módulo de antivirus de próxima generación con la capacidad de detección y bloqueo de nuevas tácticas, técnicas y procedimientos empleados por los grupos de cibercriminales.
- La solución debe contar como mínimo los siguientes elementos de análisis y características:
    - Capacidad de bloqueo de la ejecución de código malicioso, bloqueo exploits de día cero, terminación (Kill) procesos y actividades de comando y control.
    - Capacidad de protección aún cuando los equipos no cuenten con conectividad a la nube.
    - Capacidad de protección de antimalware sin la necesidad de utilizar firmas de Antivirus, ni actualizaciones de IOCs de comportamiento. No se permiten soluciones basadas en firmas o detección de IOC únicamente.
    - Aprendizaje maquina (machine learning en inglés) de forma local en cada punto final con Sistema operativo Microsoft Windows y Mac OS
    - Bloqueo de procesos identificados por la inteligencia del fabricante como maliciosos.
    - Detección y prevención de explotaciones de tipo Force DEP, Heap Spray preallocation, Force ASLR, SEH Ovewrite protection, NULL Page Allocation, Remote library Loading, Untrusted font.
    - Detección y prevención de scripts o comandos maliciosos vía powershell o CMD, entre otros incluyendo al menos lo siguiente:

- Cadenas ejecutadas dinámicamente vía el cmdlet “invoke-expression”
- Comandos vía –EncodedCommand.
- Detección y prevención de intentos de borrado de respaldos del sistema (volume shadow copy por sus siglas en inglés) comúnmente realizado por ataques de ransomware.
- Detección y prevención de los procesos de cifrado de archivos relacionados a extensiones usadas por ransomware.
- Detección y prevención de procesos asociados a accesos indiscriminados al sistema de archivos asociados a ransomware.
- Detección y prevención de movimientos laterales.
- Detección y prevención de intentos de robo de credenciales.
- Detección y prevención de intentos de elevación de privilegios.
- Detección y prevención de intentos de uso de “sticky keys”.
- Detección y prevención de intentos de ejecución de archivos sospechosos y/o código malicioso creados por los programas de navegación a internet (web browsers por sus siglas en inglés).
- Detección y prevención de intentos de ejecución de rutinas de javascript por línea de comandos vía rundll32.exe"

- La plataforma debe incluir un módulo de automatización tipo SOAR nativo que permita desarrollar Playbooks, para la automatización de actividades de respuesta como: Aislamiento automático de dispositivos, enriquecimiento de inteligenci, auto triage notificaciones personalizadas, plugins con plataformas de inteligencia, ITSM como ServiceNow, Google Slack, Microsoft Teams, email, Webhooks, lanzar scripts de forma remota, entre otros
- La plataforma debe permitir la definición de roles personalizados para cumplir con los controles de acceso asignados a los administradores, auditores o terceros que deben ingresar a la consola cómo permitir el acceso mediante MFA e integración con SSO.
- El licenciamiento de la plataforma se debe basar por el promedio de sensores activos en un periodo de un mes y no por el número de sensores desplegados.
- Los procesos de desinstalación de los sensores deben usar un token de autorización aleatorio, no se acepta el uso de passwords o contraseñas para proteger ante la desinstalación de los agentes
- CONTROL DE DISPOSITIVOS USB Y PERIFÉRICOS
- Tener la capacidad de controlar los dispositivos USB en su ejecución, lectura o escritura como su bloqueo completo para evitar el movimiento de archivos no autorizados, para sistemas windows y MAC
- Tener la capacidad de consultar que tipos de objetos son copiados o escritos en los dispositivos de almacenamiento
- Tener la capacidad de configuración de políticas de auditoría para monitoreo de toda la actividad de dispositivos externos, esto no debe requerir el despliegue de software adicional sobre los despliegues iniciales

- Tener la capacidad de crear reglas por clase y excepciones por ID de proveedor, ID de producto o número de serie.
- Debe tener la capacidad de informar automáticamente el tipo de dispositivo conectado con información del fabricante, nombre del producto y número de serie.
- Se deben contar con dashboards para poder ver la actividad de dispositivos externos como: Audio/video, Imaging, Mass Storge, Mobiles (MTP/PTP), impresoras, Wireless (Bluetooth), Any Class
- Se deben configurar de forma personalizada la notificación que le aparece a los usuarios cuando se realizar alguna restricción en el acceso
- INVESTIGACIÓN FORENSE Y CACERÍA DE AMENAZAS PROACTIVA
- Sistema de detección y respuesta de puntos finales con monitoreo continuo para poder tener visibilidad de actividad anómala, respuesta y desarrollo de actividad forense para evitar potenciales brechas o compromiso en las operaciones. Se deben integrar un sistema de analítica y correlación para realizar análisis retrospectivos
- Que permita acceso instantáneo al "quién, qué, cuándo, dónde y cómo" de un ataque.
- Que la solución EDR permite detectar incidentes automáticamente sin requerir ningún ajuste o configuración antes de estar en pleno funcionamiento.
- Que tenga la posibilidad de realizar búsquedas personalizadas sobre las detecciones que se remontan a 90 días o más para buscar amenazas de manera proactiva y que los resultados de las consultas se devuelva en cinco segundos o menos.
- Que brinde protección contra fallas silenciosas (que se producen cuando un ataque se desliza a través de las soluciones de seguridad sin que se active ninguna alarma) y que registre todas las actividades de interés de un equipo tanto en tiempo real como después del hecho.
- Que recopile información constantemente en tiempo real, para asegurar que la información mostrada sea siempre la más actual y relevante. Ej. Si durante un incidente se tiene la dirección IP original, cuando se analice el incidente y el dispositivo cambia de IP se pueda tener el registro del cambio y la dirección actual en caso de tener que que conectarse directamente desde la misma consola.
- Que ofrezca la posibilidad de Zero Trust Assessment (ZTA) para determinar el estado del equipo en la organización. Es decir que evalúe el nivel de seguridad en cuanto parámetros de seguridad del sistema operativo y políticas de seguridad de prevención
- Que permita desarrollar reglas o indicadores que identifican y previenen ataques sin archivos que aprovechan los malos comportamientos y que con el tiempo ajuste y amplíe los indicadores integrados.
- Que incluya Indicadores de Ataque por sus siglas IOA, incluso permite crear reglas de IOA personalizadas en la plataforma, Como bloqueos de

procesos, archivos, dominios o Ips dependiendo ejecuciones de comandos archivos o procesos antecesores

- Para la creación de las reglas personalizadas deberá especificar el "tipo de regla" y seleccionar acciones como: operaciones de creación de procesos, creación de archivos, conexión de red y nombre de dominio.
- Para las detecciones de dichas reglas de IOA, tenga la capacidad de buscar las detecciones provocadas por una regla específica.
- "Tener la capacidad de realizar búsquedas proactivas (hunting) para eventos de cambios registrados por la telemetría de la plataforma, en un rango o periodo de tiempo específico ejemplos:
- - realizar búsquedas de nuevos servicios o tareas programados a alrededor de un proceso de en investigación
- - realizar búsquedas de cambios en llaves de registros, accesos remotos, logins alrededor de un proceso, equipo, IP o dominio específico "
- Visualización de incidentes calificados por la plataforma que correlacione las detecciones y actividades asociadas al incidentes, asignando el indicador de riesgo del impacto del incidente
- la plataforma debe mostrar en forma gráfica el incidente relacionando los dispositivos impactados, procesos y línea de tiempo en la que ocurren los eventos relacionados tanto bloqueados como observados que tiene relación con el incidente
- La plataforma debe mostrar geolocalización de accesos o direccionamiento público relacionado con la actividad de los dispositivos investigados
- La solución de permitir consultar información de metadatos relacionados con un artefacto investigado para ampliar el proceso de investigación y consulta un alcance de 7 o superior días antes de la consulta
- La solución debe permitir la exportación de eventos en formato CSV y json
- La plataforma debe brindar la opción de involucrar servicios de fábrica para actividades de threat hunting cómo MDR en caso de requerirse a futuro para tener búsquedas proactivas sobre detecciones y anomalías en el entorno del cliente
- La solución debe realizar el envío de la telemetría en tiempo real y consultada inclusive aún si los dispositivos están fuera de línea esto por un periodo de al menos 7 días o superior
- "La información de telemetría debe ser colectada 7x24, la información a tomar debe incluir como mínimo +400 tipos de eventos entre ellos:
- - Process - Token info events, Creations, Injections, Grandparent, Parent, Child relationships.
- - Network - Close, Connect, Listen, Receive/Accept for IP4/IP6.
- - File - Writes, deleted, rename, open and info
- - Registry - ASEP. Updates, Dumps, Impersonation
- - User - Logon, Logoff, Failed attempts
- - DLL - Injection and reflection attempts,
- - Detalle de los dispositivos incluido pero no limitado a:

- - OS - OU Attributes, Hostname, Device type, OS Version, Manufacturer, Model
- - Network - MAC, Local and External IP, Neighbors"
- La solución debe permitir la configuración de consultas personalizadas utilizando un lenguaje de consulta estándar y documentado, Estas consultas pueden ser personalizadas y programadas para poder ser utilizadas como reportes vía correo electrónico
- "La solución debe proveer búsquedas preconfiguradas en los siguientes aspectos como mínimo:
- - Host Search, Hash Search, User Search, Source IP Search, Bulk Hash Search, Bulk Domain Search, Event Search, powershell hunting, linux hunting, ASEP keys, - A/V Detection Report
- - Vistas de caceria de amenazas como mínimo (CMD Line and ASEP Activity, Executables Running from Recycle Bin or Temp. Directories, Files Written to Removable Media, Firewall Set Rules, PowerShell Hunt, Scheduled Task Registered)
- - Visiblidad de actividad (Logon Activities, Remote and Network Logon Activities and Graphs, Unique Hosts Connecting to Countries Map)"
- La solución debe permitir ejecutar de manera remota scripts powershell y cmd
- La solución debe permitir al administrador tomar cualquier archivos del host con la finalidad de realizar análisis
- Actualmente CFA cuenta con la solución de crowdstrike como antivirus, si se contempla un agente diferente, se deberá contemplar mano de obra para distribución e instalación de todos los agentes.
- Actualmente CFA cuenta con la solución de crowdstrike como antivirus, si se contempla un agente diferente, se deberá contemplar tiempo de capacitación para el personal de CFA.
- Actualmente CFA cuenta con la solución de crowdstrike como antivirus, si se contempla un agente diferente, se deberá contemplar tiempo para garantizar la integración con nuestro SIEM Logrhythm.
- Si se presenta un antivirus diferente a Crowstrike el proponente debera entregar una carta certificada por fabricante indicando cumplir con todos los requisitos anteriores mencionados que apliquen al software.
- Se requiere una propuesta para la adquisición de 700 licencias para endpoints. El licenciamiento deberá ser totalmente flexible, permitiendo la asignación de estas licencias a cualquier dispositivo final, incluyendo, pero no limitado a:
    - Estaciones de trabajo y laptops (Windows, macOS)
    - Servidores (Windows, Linux)
    - La oferta debe ser presentada con opciones para una vigencia de 1, 2 y 3 años. La administración de las 700 licencias no debe estar restringida por tipo de sistema operativo o rol del equipo.

Prestación del Servicio: La prestación del servicio se ejecutará con los propios medios y personal del oferente, con total autonomía en los trabajos y demás actividades propias del servicio contratado, garantizando el cumplimiento de las **políticas de seguridad de la información y acuerdos de confidencialidad** de la organización. Se valorará la inclusión de una cláusula de **transferencia de conocimiento** al equipo interno de la organización.

3. OBLIGACIONES DEL PROPONENTE

El Proponente que sea seleccionado, deberá cumplir con las siguientes obligaciones las cuales estarán estipuladas en el contrato que se suscriba entre ambas partes:

1. Cumplir con el objeto del contrato en los términos pactados con suma diligencia y cuidado.
2. Cumplir y atender los requerimientos del CFA en los términos que EL PROPONENTE tenga disponibilidad
3. Cumplir con la obligación de confidencialidad pactada en el Contrato
4. Cumplir las condiciones legales para la prestación de los servicios contratados
5. Mantener vigentes y actualizadas durante la prestación del servicio las pólizas y garantías enumeradas en el Contrato.
6. Suministrar CFA los elementos necesarios para el cumplimiento del objeto contractual, para la conectividad al servicio.
7. Prestar la debida colaboración CFA, suministrando información sobre los aspectos que requiera para el desarrollo de las actividades de modo que se le facilite el cumplimiento del objeto del Contrato.
8. EL PROPONENTE se obliga a cumplir con los requerimientos de Seguridad y Calidad de la información exigidos en las Circulares, proferidas por la Superintendencia Financiera de Colombia y cualquier norma que la modifique o reemplace y en especial las contenidas en los anexos de seguridad de la información y computación en la nube.
9. Acatar las instrucciones y recomendaciones que le imparta CFA para que la prestación del servicio contratado se ajuste a las necesidades y expectativas de CFA.
10. Obrar con diligencia en los asuntos encomendados y garantizar una óptima calidad en todos los servicios contratados de acuerdo con lo establecido en el Contrato, la Propuesta y los Acuerdos de Niveles de Servicio.
11. Contar con los recursos necesarios para prestar adecuadamente el servicio contratado.
12. Garantizar que el personal de EL PROPONENTE para desarrollar las labores asignadas cumpla con las normas y reglamentaciones que rigen la actividad respectiva y que tales personas son lo suficientemente experimentadas, hábiles e idóneas para realizarlas.
13. Las demás relacionadas con el objeto del contrato o que se deriven de la

naturaleza de este Contrato.

14. EL CONTRATISTA en ocasión de la relación contractual y operativa se compromete a realizar la apertura de una cuenta de ahorros con CFA COOPERATIVA FINANCIERA, en la cual, se realizarán los pagos correspondientes a la prestación del servicio del presente contrato.

4. PERSONAL, SEGURIDAD SOCIAL Y PARAFISCALES

EL PROPONENTE se compromete a utilizar en la instalación o suministro de los bienes o servicios, a sus propios trabajadores, para lo cual reconoce que dispone de autonomía técnica, directiva y financiera. Como consecuencia el personal que utilice para el cumplimiento de su Oferta será dependiente suyo y no adquiere ningún vínculo laboral con CFA, razón por la cual correrán exclusivamente por su cuenta todas las obligaciones laborales, prestaciones sociales e indemnizaciones, que se generen con relación al personal empleado. De lo anterior, CFA solicitará las respectivas constancias al momento de suscribir el contrato.

El PROPONENTE deberá prever dentro de sus costos el recurso humano necesario para cumplir con la programación presentada en su propuesta, la cual debe corresponder a las fechas establecidas. De igual forma deberá tener en cuenta que no habrá ningún reconocimiento por horas extras diurnas o nocturnas, trabajos dominicales o festivos, como consecuencia de dar cumplimiento a la ejecución de dicho programa de trabajo.

CFA se reserva el derecho de solicitar por escrito el retiro de sus instalaciones de cualquier persona que a su juicio sea perjudicial para el buen desarrollo de los trabajos.

EL PROPONENTE es responsable del cumplimiento por parte de sus trabajadores de la hora de ingreso y salida durante la ejecución del proyecto en las instalaciones de **CFA,** pudiendo este ser modificado, ampliado o alterado para garantizar el cumplimiento de la programación. Así como el personal y equipos que EL PROPONENTE estime necesario para la correcta ejecución. Todo previamente concertado con **CFA.**

EL PROPONENTE es responsable del cuidado de sus equipos.

5. PLAZOS

Las fechas en que se desarrollará esta invitación son de acuerdo al siguiente cuadro:

ACTIVIDAD	TIEMPO	FECHA
Presentación de Propuestas	11 días	Lunes, 15 de septiembre de 2025

ACTIVIDAD	TIEMPO	FECHA
Cierre de la invitación Pública.	11 días	Lunes, 15 de septiembre de 2025
Selección de la propuesta	4 días	Viernes, 19 de septiembre de 2025

El documento de Oferta se presentará máximo hasta el día **15 de septiembre del año 2025**, y se puede presentar de las siguientes formas:

- De forma física en sobre cerrado y dirigido a ALEXANDER OCAMPO LOPEZ, a la dirección CRA 65 No. 48 -162 Medellín - Antioquia (CFA COOPERATIVA FINANCIERA) .

-De forma digital al correo electrónico **contratacion@cfa.com.co**

La oferta debe estar suscrita por quien tenga facultades de Representación Legal, acompañada de los documentos que se relacionan en la presente invitación.

CFA se reserva el derecho de llamar a sustentar las propuestas en caso de requerir mayor ampliación o aclaración de algún punto de las propuestas enviadas, en cuyo caso no se entenderá que existe una contraoferta o una aceptación de la propuesta modificada.

6. DOCUMENTOS A PRESENTAR Y CONTENIDO DE LA OFERTA:

EL PROPONENTE deberá ser una compañía de carácter Nacional o en el caso de ser una compañía Extranjera deberá tener una representación en Colombia legalmente constituida, demostrando tener una logística de distribución adecuada y una capacidad para el cumplimiento de los plazos y responsabilidades.

La Oferta presentada por EL PROPONENTE, corresponde a un documento digital o físico, el cual debe contener como mínimo los requisitos requeridos en la presente invitación o deberá señalar expresamente que EL PROPONENTE se adhiere integralmente a los términos de la presente invitación. Tal documento deberá contener todas las condiciones que EL PROPONENTE propone para que rija la relación entre las partes en el evento de ser aceptada la Oferta.

DOCUMENTOS PARA PRESENTACIÓN DE LA PROPUESTA

EL PROPONENTE deberá remitir los siguientes documentos que harán parte integral de la propuesta:

1. Carta suscrita por el representante legal donde se acepten expresamente los términos y condiciones establecidos en esta invitación
2. Oferta comercial que contenga la relación de los bienes o servicios a prestar, el precio total y la forma de pago.
3. Acuerdo de niveles de servicios.(ANS)
4. Certificado de existencia y representación legal no mayor a 30 días.
5. Fotocopia de la cédula de ciudadanía del Representante legal
6. Certificación escrita de los dos (2) principales clientes.
7. Copia del RUT actualizado.
8. Certificado de que se encuentran al día en los aportes a la seguridad social integral o aportes parafiscales del último mes expedido por el revisor fiscal o firmado por el representante legal para las entidades que no estén obligadas a tener revisor fiscal.

Si EL PROPONENTE lo desea, puede añadir información no solicitada, pero no puede omitir la aquí considerada.

7. VIGENCIA DE LA OFERTA PRESENTADA

La Oferta comercial presentada por los proponentes deberá tener una vigencia igual a 60 días, contados a partir de la entrega por parte de EL PROPONENTE a CFA

8. ASPECTOS LEGALES

El proponente que resulte seleccionado en el presente proceso de invitación pública, además de la suscripción del contrato, se obligará suscribir o constituir los siguientes documentos:

- **POLIZAS**

EL PROPONENTE deberá constituir a favor de **CFA** las siguientes garantías en caso de ser seleccionado, expedidas por una Compañía de Seguros legalmente establecida y aceptada por CFA

PÓLIZA	VALOR ASEGURADO	VIGENCIA HASTA	OBSERVACIONES
Cumplimiento	20% V. Contrato	Durante el Contrato, más 3 meses.	Entregar con el Contrato.
Pago de prestaciones y Salarios	10% V. Contrato	Durante el Contrato, más 3 años.	Entregar con el Contrato.

Ciberseguridad	10% V. Contrato	Durante el Contrato, más 3 meses.	Entregar con el Contrato.
Calidad del Servicio	20% V. Contrato	Durante el Contrato, más 3 meses.	Entregar con el Contrato.

- **ACUERDO DE NIVELES DE SERVICIO:**

El proponente presentará junto a la propuesta, un documento denominado "Acuerdo niveles de servicio" en el cual estipulará las condiciones del soporte, el personal designado, canales de atención, horarios y demás elementos que rijan la relación y comunicación continua entre las partes para la correcta ejecución del contrato.

- **ANEXO:**

A la suscripción del contrato, el proveedor seleccionado deberá dar estricto cumplimiento a los lineamientos normativos en lo referente a la protección de datos y seguridad de la información a nivel general y en materia de almacenamiento y procesamiento de información en la nube, debido a que CFA es una entidad vigilada por la Superintendencia Financiera de Colombia (SFC). Por lo anterior, ambas partes deberán suscribir el anexo correspondiente.

9. SOLICITUD DE ACLARACIONES O INFORMACIÓN ADICIONAL

NOMBRES	CARGO	TELÉFONO	C. ELECTRÓNICO
Jhony Alexander Gonzalez Henao	**Oficial de seguridad**	**604 4441827 ext 11501**	**jagonzalez@cfa.com.co**