VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

INVITACIÓN PÚBLICA

SOLICITUD DE OFERTAS PARA SERVICIO DE ANÁLISIS DE CÓDIGO ESTÁTICO Y DINÁMICO

CONTRATANTE: COOPERATIVA FINANCIERA DE ANTIOQUIA CFA

FECHA
14 de Mayo de 2026

1. ALCANCE Y OBJETO DE LA INVITACIÓN:

CFA está interesado en recibir su oferta para el servicio de SERVICIO DE ANÁLISIS DE CÓDIGO ESTÁTICO Y DINÁMICO, de acuerdo al siguiente objeto:

- CFA está interesado en recibir su oferta para contratar un servicio de análisis de código dinámico y estático para una aplicación en su versión Web y dispositivos móviles (Android y IOS).o.

Características del Contrato:

1. El proveedor deberá suministrar una solución híbrida (herramientas automatizadas + análisis experto) que cubra las siguientes dimensiones de seguridad:

    - SAST (Static Application Security Testing): Análisis profundo del código fuente para identificar vulnerabilidades antes de la ejecución.
    - DAST (Dynamic Application Security Testing): Pruebas de seguridad en tiempo de ejecución para aplicaciones web y móviles.
    - SCA (Software Composition Analysis): Identificación de vulnerabilidades en librerías de terceros y gestión de licencias de código abierto.
    - CSPM (Cloud Security Posture Management): Evaluación de la configuración de seguridad en infraestructura nube asociada al despliegue de las aplicaciones.
    - Secret Scanning: Detección automática de credenciales, llaves de API, tokens o secretos embebidos ("hardcoded") en el código.

2. INTEGRACIÓN CONTINUA Y DISPARADORES (TRIGGERS)
   Para garantizar que la seguridad sea parte del flujo de trabajo de desarrollo, la solución debe cumplir con:
    - Análisis por cada Commit / Pull Request: La herramienta debe integrarse de forma nativa con los repositorios de CFA (On-Premise) y disparar un escaneo automático cada vez que un desarrollador realice un Commit o una solicitud de cambio (Pull Request) en las ramas definidas.
    - Breaking Build (Quality Gates): Capacidad de bloquear automáticamente el proceso de construcción (Build) o impedir la fusión de ramas si se detectan vulnerabilidades de criticidad Alta o Crítica (según políticas de CFA).
    - Conectividad Segura: El proveedor debe establecer una conexión VPN punto a punto estable hacia la infraestructura de CFA para el acceso a los repositorios, garantizando la trazabilidad de los accesos.

3. Capacidades DevSecOps

- Integración con Ciclo de Vida: Capacidad nativa de integrarse con la rama de desarrollo (Git, Azure DevOps, GitLab o similar) mediante Webhooks o APIs.
- Capacidad de Breaking Build: El sistema debe permitir la configuración de umbrales de seguridad (Quality Gates). Si se detectan vulnerabilidades de criticidad Alta o Crítica, la solución debe ser capaz de detener automáticamente el pipeline de despliegue.
- Conectividad Segura (On-Premise): El proveedor deberá establecer una conexión VPN punto a punto (Site-to-Site o Client-to-Site) para acceder a los repositorios alojados en la infraestructura interna de la organización.
- Seguridad de la Información: El proponente debe garantizar que su infraestructura de análisis cuenta con equipos limpios, cifrado de disco y políticas de prevención de fuga de datos (DLP). No se permite el almacenamiento del código fuente fuera de los entornos autorizados tras finalizar el análisis.

4. Stack Tecnológico Obligatorio
   El servicio debe garantizar compatibilidad total y soporte técnico para el análisis de los siguientes lenguajes y frameworks:
   - Frontend: Angular (TypeScript).
   - Backend: .NET Core (C#).
   - Móvil (Híbrido): Xamarin Forms (C#) y Flutter (Dart).
   - Análisis Móvil Específico: Capacidad de realizar análisis estático y dinámico sobre binarios compiled (APK, AAB, IPA).

5. Plataforma de Gestión y Reportabilidad
   Se requiere una plataforma web (SaaS o On-Prem) para la gestión centralizada de hallazgos que permita:
   - Interacción con el Proveedor: Canal de comunicación directo dentro de cada hallazgo para aclaraciones técnicas.
   - Clasificación Estándar: Todas las vulnerabilidades deben estar categorizadas bajo el sistema CVSS v3.1/4.0 y mapeadas contra el OWASP Top 10.
   - Métricas de Gestión: Dashboards que muestren:
   - Cantidad de vulnerabilidades encontradas vs. Remediadas.
   - Tiempo promedio de remediación (MTTR).
   - Histórico de seguridad por proyecto/aplicación.
   - Exportación de Datos: Capacidad de exportar informes técnicos y ejecutivos en formatos PDF, CSV y XLSX.
   - Seguimiento: Capacidad de marcar hallazgos como "Falso Positivo" o "Riesgo Aceptado" con su respectiva justificación técnica.

6. Componente de Especialistas (Soporte Senior)

Acompañamiento Experto: El servicio no es solo el acceso a la herramienta; debe incluir el análisis de un experto humano que valide los hallazgos para eliminar falsos positivos antes de reportarlos.

- Re-Ataques Ilimitados: Posibilidad de solicitar re-escaneos y validaciones de remediación ilimitadas para confirmar que los parches aplicados por el equipo de desarrollo son efectivos.
- Revisiones Trimestrales: Realización de una reunión de comité técnica trimestral para presentar informes de postura de seguridad, tendencias y recomendaciones de mejora en el código.
- Eliminación de Falsos Positivos (Triaje): Un experto del proveedor deberá validar los hallazgos antes de ser reportados, asegurando que el equipo de desarrollo de CFA solo trabaje sobre riesgos reales.
- Plataforma de Gestión: Acceso a un dashboard con métricas de riesgo, historial de vulnerabilidades y capacidad de exportar reportes en PDF, CSV y XLSX.
- Clasificación de Riesgo: Todos los hallazgos deben utilizar el estándar CVSS v3.1/4.0.

7. Certificaciones de la Empresa/Herramienta:
    a. El proveedor debe acreditar que es partner certificado o cuenta con personal certificado en la herramienta de análisis automatizado propuesta.

8. Plazo y Cronograma de Implementación
    a. Periodo de Implementación: El proponente seleccionado dispondrá de un plazo mínimo de treinta (30) días calendario, contados a partir de la firma del acta de inicio, para completar la fase de despliegue y puesta a punto.
    b. Hitos de la Fase de Implementación: Durante este periodo, el proveedor deberá garantizar:
        i. Establecimiento y estabilización de la conexión VPN punto a punto.
        ii. Integración técnica con los repositorios de código (Angular, .NET Core, Flutter, Xamarin).
        iii. Configuración de los Quality Gates (Breaking Build) en el pipeline de CI/CD.
        iv. Carga y tunning inicial de las aplicaciones para la eliminación de falsos positivos masivos.
        v. Capacitación básica al equipo de desarrollo sobre el uso de la plataforma de gestión.

9. Condición de Aceptación

   La implementación se considerará finalizada únicamente cuando la organización emita un Acta de Conformidad Técnica, tras verificar que la herramienta escanea correctamente el código y que la plataforma de gestión visualiza los hallazgos según los niveles de criticidad exigidos.

10. Forma de Pago (Cláusula de Éxito)
    - Pago Sujeto a Implementación: La organización no realizará ningún desembolso económico inicial (anticipo).
    - Primer Pago: El primer pago (ya sea mensualidad, trimestre o hito según se defina) quedará condicionado a la entrega y aprobación de la fase de implementación de 30 días.

Garantía de Servicio: Si transcurridos los 30 días el proveedor no ha logrado la integración técnica con los repositorios On-Premise o el establecimiento de la VPN por causas imputables a su tecnología, la organización se reserva el derecho de rescindir el contrato sin que esto genere obligación de pago alguna por servicios no perfeccionados.

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

Los requerimientos técnicos son los siguientes:

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. Si hiciera falta alguna licencia adicional el PROPONENTE deberá especificar dentro de la propuesta.

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	FECHA
Apertura Invitación Pública.	14 de Mayo de 2026
Cierre Invitación Pública.	1 de Junio de 2026
Selección de la propuesta	10 de Junio de 2026

El documento de Oferta se presentará máximo hasta el día **1 de Junio** del año **2026**, y se puede presentar de la siguiente forma:

-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.
9. Estados Financieros del último año de cierre contable.
10. Certificación de experiencia firmado por el representante legal.
11. Certificación cumplimiento estándares de SGSST emitida por la ARL del proveedor.
12. Certificados que demuestren la adopción de prácticas del Objetivo de Desarrollo Sostenible (ODS, en caso de contar con los mismos)

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:

- **PÓLIZAS**

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.
Calidad del Servicio y elementos suministrados	20% V. Contrato	Durante el Contrato, más 3 meses.	Entregar con el Contrato.
Responsabilidad Extracontratual	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:**

Se informa desde el inicio de la invitación, para conocimiento de los oferentes que con la suscripción del contrato en caso de aplicar de conformidad con la materialización del servicio, 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, mismo que será suministrado y socializado con la materialización del proceso contractual con el proveedor seleccionado.

9. SOLICITUD DE ACLARACIONES O INFORMACIÓN ADICIONAL

NOMBRES	CARGO	TELÉFONO	C. ELECTRÓNICO
JHONY ALEXANDER GONZALEZ HENAO	**Oficial de seguridad**	**604 4441827 ext 12601**	**contratacion@cfa.com.co**