VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

INVITACIÓN PÚBLICA

SOLICITUD DE OFERTAS PARA UN SOFTWARE DE CIFRADO Y DLP

CONTRATANTE: COOPERATIVA FINANCIERA DE ANTIOQUIA CFA

FECHA
06 de Julio de 2026

1. **ALCANCE Y OBJETO DE LA INVITACIÓN:**

CFA está interesado en recibir su oferta para adquirir un SOFTWARE DE CIFRADO Y DLP en Endpoints (Windows y Mac), de acuerdo al siguiente objeto:

- CFA está interesado en recibir su oferta para contratar un software de CIFRADO Y DLP en (Windows y Mac).

Características del Contrato: El proveedor deberá suministrar una solución que cubra las siguientes necesidades para 600 dispositivos dentro de los cuales hay sistemas operativos Windows y IOS:

- **CIFRADO**
  - **Capacidad, Arquitectura y Despliegue**
    - **Capacidad**: La solución debe incluir el licenciamiento, aprovisionamiento y soporte con capacidad de cobertura total para un mínimo de 600 dispositivos finales (endpoints) concurrentes.
    - **Consola Web**: La plataforma de administración, configuración de políticas de cifrado, visualización de eventos y gestión de claves de recuperación debe ser 100% basada en entorno Web (HTTPS), accesible de forma segura mediante un navegador de internet.
    - **Flexibilidad de Agente**: El software de cifrado puede operar mediante un agente independiente en el endpoint. No es un requisito obligatorio que comparta el mismo agente o archivo ejecutable con otras soluciones de seguridad de la entidad, siempre y cuando no genere conflictos de estabilidad en el sistema operativo.
  - **Gestión de Cifrado de Disco Completo (Full Disk Encryption)**
    - **Gestión Nativa del Propietario**: La solución propuesta debe tener la capacidad técnica de tomar el control, administrar, configurar y auditar centralizadamente las herramientas de cifrado nativas del propietario del sistema operativo: Microsoft BitLocker para entornos Windows y Apple FileVault para entornos macOS.
    - **Custodia de Claves**: Gestión automatizada y almacenamiento seguro de las claves de recuperación de los discos cifrados en la base de datos centralizada de la solución, permitiendo la recuperación remota por parte de los administradores de TI en caso de bloqueo del usuario.

    - **Estándar de Cifrado**: Soporte para algoritmos estándar de la industria, utilizando como mínimo el estándar AES de 256 bits.

- **Cifrado de Archivos, Carpetas y Medios Extraíbles**
  - **Cifrado de Medios Extraíbles**: Capacidad de forzar el cifrado automático o condicional de cualquier archivo que sea copiado hacia un dispositivo de almacenamiento extraíble (USB o discos externos), permitiendo la lectura del archivo fuera de la red de la entidad únicamente mediante autenticación segura (contraseña o certificado).
  - **Cifrado Selectivo**: Capacidad de cifrar de manera selectiva archivos o carpetas específicas en el endpoint o en recursos de red compartidos, garantizando que solo los usuarios autorizados tengan acceso a la llave de descifrado.
- **Auditoría y Reportes**
  - **Logs de Auditoría**: La solución debe registrar de forma inalterable (Logs) todas las acciones realizadas por los administradores (ej. extracción de llaves de recuperación) y los eventos de los usuarios (ej. intentos fallidos de autenticación).
  - **Cumplimiento**: El sistema debe contar con reportes de cumplimiento técnico que demuestre el porcentaje de dispositivos cifrados con éxito, alineados con estándares como ISO 27001 y normativas de protección de datos.

- La solución de cifrado debe contar con un mecanismo de protección del sector de arranque (Pre-boot) tolerante a fallos por apagados abruptos o cortes de energía. En caso de bloqueo del sistema operativo, la plataforma debe permitir la recuperación remota de la estación mediante un método de desafío-respuesta (Challenge-Response) a través de la consola web o un portal de autoservicio para el usuario, sin requerir la reinstalación del agente ni la pérdida de datos.
- Para garantizar la estabilidad del sistema operativo ante actualizaciones de software (Windows/macOS), la solución NO debe utilizar un motor de cifrado propietario para el disco completo. Debe gestionar obligatoriamente el componente nativo del sistema operativo (Microsoft BitLocker / Apple FileVault). Si el agente de administración presenta fallos o desactualizaciones, el sistema operativo debe continuar operando con normalidad y permitir el descifrado seguro a través de las herramientas nativas del propietario
- El oferente debe proveer una herramienta de recuperación autónoma (ISO ejecutable / USB Booteable) que permita a los administradores locales de TI acceder al disco, diagnosticar y descifrar la información en frío en caso de un fallo crítico del sistema operativo, evitando el traslado físico del hardware a la sede central.

- El o los agentes instalados en el endpoint para las funciones de DLP y Cifrado deben ser de arquitectura ligera. El consumo conjunto de recursos en estado de ejecución activa (escaneo de fondo, monitoreo de puertos y gestión de cifrado) no podrá exceder el **3% de uso de CPU** ni **120 MB de memoria RAM** en condiciones normales de operación, garantizando el no impacto en el rendimiento de la máquina del usuario.

- **DLP**
  - **Capacidad, Arquitectura y Despliegue**
    - Capacidad: La solución debe incluir el licenciamiento, aprovisionamiento y soporte con capacidad de cobertura total para un mínimo de 600 dispositivos finales (endpoints) concurrentes, garantizando la protección tanto dentro como fuera de la red corporativa.
    - Consola Web: Toda la plataforma de administración, configuración de políticas de seguridad, visualización de alertas, reportería y gestión de incidentes debe ser 100% basada en entorno Web (HTTPS).
    - Flexibilidad de Agente: El software de DLP puede operar mediante un agente independiente en el endpoint. No es un requisito obligatorio que comparta el mismo agente o archivo ejecutable con otras soluciones de seguridad de la entidad (como el cifrado), siempre y cuando no genere conflictos de estabilidad en el sistema operativo.
  - **Descubrimiento y Clasificación Automática (Data Discovery & Classification)**
    - **Etiquetado Automático**: La solución debe tener la capacidad de realizar etiquetado (tagging) y clasificación automática de la información en el momento de su creación, modificación o almacenamiento, basándose en el análisis de su contenido (reglas de negocio, diccionarios, expresiones regulares). Este proceso no debe depender de la acción manual del usuario.
    - **Escaneo en Reposo**: Capacidad de realizar escaneos programados o en tiempo real en repositorios de almacenamiento local, unidades de red compartidas y servicios de almacenamiento en la nube para identificar y clasificar datos sensibles en reposo.
    - **Técnicas de Análisis**: Soporte para la identificación de datos mediante múltiples técnicas avanzadas: expresiones regulares (RegEx), diccionarios predefinidos (números de identificación, tarjetas de crédito), huellas digitales de archivos (Exact Data Matching - EDM) y metadatos de clasificación.
  - **Vectores de Monitoreo y Protección (Data in Motion / Data in Use)**

- **Protección en el Endpoint**: Capacidad de monitorear y bloquear la copia o transferencia de información sensible hacia dispositivos de almacenamiento extraíbles (USB), unidades de CD/DVD, almacenamiento local no autorizado y portapapeles (Copy-Paste).
- **Protección en Red y Web**: Capacidad de interceptar, analizar y bloquear la transferencia de datos sensibles a través de tráfico HTTP/HTTPS (subidas a nubes públicas, webmails), protocolos de transferencia de archivos (FTP/SFTP) y aplicaciones de mensajería corporativa o personal.

- **Auditoría, Reportes e Incidentes**
  - **Registro de Eventos**: La solución debe registrar de forma inalterable (Logs) todas las acciones realizadas por los administradores y los eventos de seguridad generados por los usuarios (bloqueos, alertas, intentos de fuga).
  - **Integración SIEM**: Capacidad de exportar logs en formatos estándar (Syslog, CEF) para su fácil integración con herramientas de correlación de eventos de terceros (SIEM / SOAR)
  - **Cumplimiento Normativo**: El sistema debe contar con plantillas de reportes preconfiguradas orientadas al cumplimiento de estándares internacionales de seguridad y privacidad como ISO 27001, GDPR, PCI-DSS o normativas locales de protección de datos personales.

1. CheckList: El proponente deberá entregar una lista de chequeo especificando el cumplimiento de cada uno de los puntos anteriormente indicados.
2. 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.
3. Plazo y Cronograma de Implementación
   a. Periodo de Implementación: El proponente seleccionado dispondrá de un plazo mínimo de treinta (60) días calendario, contados a partir de la firma del acta de inicio, para completar la fase de despliegue y puesta a punto.
4. Condición de Aceptación

   La implementación se considerará finalizada únicamente cuando la organización emita un Acta de Conformidad Técnica, tras verificar que la herramienta escanea y cifrado correctamente los equipos.

5. 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 60 días.

Garantía de Servicio: Si transcurridos los 60 días el proveedor no ha logrado la implementación tecnicas por causas imputables a su tecnología, la organización se reserva el derecho de rescindir el contrato sin que esto genere obligación de pago alguno 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.	06 de Julio de 2026
Cierre Invitación Pública.	24 de Julio de 2026
Selección de la propuesta	31 de Julio de 2026

El documento de Oferta se presentará máximo hasta el día **24 de julio** 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