Resolución UAE-CRA No. 406 de 2026

(02 de julio de 2026)

"Por medio de la cual se ordena la apertura del Proceso de Selección Abreviada Por Subasta Inversa No. 03 de 2026".

LA SUBDIRECTORA ADMINISTRATIVA Y FINANCIERA DE LA COMISIÓN DE REGULACIÓN DE AGUA POTABLE Y SANEAMIENTO BÁSICO (CRA)

En ejercicio de sus facultades legales, en especial de las conferidas por la Ley 80 de 1993, Ley 1150 de 2007, los Decretos 2882 de 2007, 2883 de 2007, el Decreto 1082 de 2015 y la Resolución UAE CRA No 523 de 2012, la Resolución UAE – CRA No. 301 del 24 de julio de 2025 y,

CONSIDERANDO:

La Comisión de Regulación de Agua Potable y Saneamiento Básico (CRA); es una entidad del orden nacional, adscrita al Ministerio Vivienda, Ciudad y Territorio, con autonomía administrativa, técnica y patrimonial, creada por la Ley 142 de 1994 con el fin de regular los monopolios en la prestación de los servicios públicos domiciliarios de acueducto, alcantarillado y aseo en Colombia, cuando la competencia no sea, de hecho, posible; y, en los demás casos, la de promover la competencia entre quienes presten servicios públicos, para que las operaciones de los monopolistas o de los competidores sean económicamente eficientes, no impliquen abuso de la posición dominante, y produzcan servicios de calidad.

De acuerdo con el Decreto 2650 de 2013, corresponde a la Oficina asesora de planeación y TIC's de la Comisión de Regulación de Agua Potable y Saneamiento Básico CRA, entre otras, las siguientes funciones:

"(…)

1. Dirigir y coordinar la administración de la Plataforma Tecnológica de la Institución".

El año 2026 marca un punto de inflexión en la sofisticación de las amenazas cibernéticas globales. Los ataques de ransomware han evolucionado hacia modelos de extorsión múltiple, comprometiendo simultáneamente la confidencialidad, la disponibilidad y la integridad de la información de las entidades públicas. Las vulnerabilidades críticas detectadas en plataformas de seguridad perimetral — incluidas múltiples CVEs activas en productos de fabricantes líderes en enero y abril de 2026— evidencian que ningún entorno tecnológico es inmune a la explotación de fallos de día cero.

El auge de amenazas persistentes avanzadas (APT) patrocinadas por actores estatales y grupos de cibercriminalidad organizada ha incrementado exponencialmente el riesgo para entidades del Gobierno Nacional. La CRA, como entidad regulatoria de servicios esenciales para el país, constituye un objetivo de alto valor estratégico, dado que custodia información sensible del sector de agua potable y saneamiento básico de Colombia.

En este entorno de amenaza creciente, el Gobierno Nacional ha reforzado el marco normativo a través del MSPI, las directrices del MinTIC y los estándares internacionales ISO 27001:2022 y NIST Cybersecurity Framework, exigiendo a las entidades públicas controles técnicos robustos, continuos y orquestados. Contar con una plataforma de análisis y correlación centralizada, vigente y respaldada por el fabricante, no es una opción deseable: es un requisito operativo crítico e indelegable.

La infraestructura de ciberseguridad de la CRA no es un componente aislado. Es un ecosistema tecnológico integrado por múltiples capas de protección que operan de forma simultánea y complementaria:

(…)

Cada uno de estos componentes genera, de manera individual y constante, miles de eventos de seguridad por segundo. Sin una plataforma de orquestación central que los correlacione e integre, estos eventos permanecen **aislados, fragmentados e inaccionables**, creando puntos ciegos críticos que los atacantes explotan con precisión. FortiAnalyzer no es simplemente un repositorio de logs; en el contexto del ecosistema multicapa de la CRA, actúa como el cerebro orquestador que dota de inteligencia y coherencia a cada una de las capas de seguridad desplegadas.

Correlación Cruzada entre Todos los Componentes.

La verdadera potencia de FortiAnalyzer radica en su capacidad de **correlacionar eventos de fuentes heterogéneas en tiempo real.** Un escenario típico de ataque avanzado en 2026 podría manifestarse así:

1. Un usuario conecta un dispositivo no autorizado a la **red inalámbrica (FortiAP)** → el evento queda registrado.

2. Desde ese dispositivo se realiza un escaneo interno de puertos → el **Firewall (FortiGate)** genera una alerta.

3. Se intenta acceder a una aplicación web institucional con credenciales comprometidas → el **WAF** bloquea y registra el intento.

4. Se detecta un comportamiento anómalo en un endpoint de la red → **FortiEDR** lo clasifica como posible ransomware en etapa temprana.

Sin FortiAnalyzer, estos cuatro eventos son tratados como incidentes independientes por operadores distintos, sin visibilidad del patrón de ataque coordinado. Con FortiAnalyzer, el sistema correlaciona automáticamente los cuatro eventos, construye la línea de tiempo del ataque, activa una alerta de incidente mayor y permite una respuesta orquestada e inmediata. Esta capacidad es la esencia del control A.16 (Gestión de Incidentes de Seguridad) de la ISO 27001:2022 y la función Detect & Respond del NIST CSF.

Visibilidad Total sobre la Red Inalámbrica (FortiAP)

Los Access Points representan uno de los vectores de ataque más explotados en entornos corporativos, por la dificultad de controlar los dispositivos que se conectan a ellos. FortiAnalyzer centraliza los registros de autenticación inalámbrica, detecta dispositivos rogue (no autorizados), identifica patrones de movimiento lateral desde la red Wi-Fi hacia la red cableada, y genera alertas tempranas ante intentos de asociación maliciosa. Sin esta visibilidad centralizada, la red inalámbrica de la CRA opera como un punto ciego en la superficie de ataque institucional.

Protección de Aplicaciones Web con Contexto (WAF)

Los logs generados por el WAF contienen información crítica sobre intentos de explotación de vulnerabilidades en los sistemas de información de la CRA. Sin embargo, un registro individual de WAF, sin contexto, puede parecer un intento fallido inofensivo. FortiAnalyzer cruza esos registros con las fuentes de inteligencia de amenazas de FortiGuard, identifica si la IP de origen está asociada a campañas de ataque conocidas, y determina si ese intento forma parte de una campaña persistente. Esta correlación convierte datos en inteligencia accionable, un requisito fundamental del MSPI para la gestión proactiva de riesgos de seguridad digital.

Respuesta a Incidentes en Endpoints con FortiEDR

FortiEDR detecta y bloquea amenazas en tiempo real sobre los endpoints de la entidad. Sin embargo, la investigación post-incidente, el análisis forense y la comprensión del alcance de un ataque requieren datos históricos correlacionados que solo FortiAnalyzer puede proveer. La integración FortiEDR–FortiAnalyzer permite reconstruir la cadena de ataque completa (kill chain), desde el vector de entrada hasta el impacto final, facilitando la respuesta legal y administrativa ante incidentes que deban ser reportados a la Policía

Nacional o la Fiscalía General de la Nación. Esto es crítico para preservar la cadena de custodia de la evidencia digital.

Situación Actual: Fin de Soporte del Equipo Vigente

El FortiAnalyzer 200F actualmente en operación alcanzará su Fin de Soporte (End of Support - EOS) a finales de junio de 2026. A partir de esa fecha, Fortinet cesará de manera definitiva:

- Emisión de parches de seguridad y actualizaciones de firmware.
- Soporte técnico TAC del fabricante (casos 24x7).
- Proceso de reemplazo de hardware por garantía (RMA).
- Actualizaciones de firmas FortiGuard para correlación de amenazas nuevas

La consecuencia directa e inmediata es que el cerebro orquestador del ecosistema de seguridad de la CRA quedará operando con inteligencia de amenazas desactualizada, incapaz de detectar los vectores de ataque que emerjan a partir de julio de 2026. Mientras los componentes individuales (Firewall, WAF, FortiEDR, FortiAP) continuarán generando eventos, la capacidad de correlacionarlos, interpretarlos y responder de manera coordinada se verá gravemente comprometida.

(…)

Adicionalmente, postergar la renovación más allá de la fecha de expiración implica costos de retroactividad significativos impuestos por el fabricante en el proceso de relicenciamiento.

Justificación Técnica del Nuevo Appliance a Adquirir

La solución a adquirir representa un salto generacional en capacidad de orquestación, rendimiento de procesamiento y resiliencia tecnológica, diseñado específicamente para ecosistemas de seguridad multicapa como el de la CRA.

Integración Nativa y Profunda con el Ecosistema Fortinet

FortiAnalyzer no es solo un analizador de logs genérico; es un **componente nativo y optimizado** de la arquitectura Fortinet Security Fabric, diseñado para orquestar, correlacionar y analizar datos de:

- **FortiGate** (firewalls de próxima generación).
- **FortiEDR** (seguridad de endpoint con respuesta detectada).
- **FortiAP** (infraestructura WiFi segura).
- **FortiWeb**, entre otros

Condicione técnicas de justificación para adquirir el FORTIANALIZER:

Dimensión	Justificación Técnica
Protocolos de integración	FortiAnalyzer usa protocolos **nativos Fortinet** (FortiProtobuf, FortiAPI) que no están documentados públicamente ni son compatibles con soluciones de terceros sin adaptadores costosos y poco fiables
Correlación de eventos	Algoritmos de correlación **pre-entrenados** para eventos Fortinet (ej. ataques a FortiGate + EDR + AP) que soluciones genéricas (Splunk, QRadar) no replican sin desarrollo manual extensivo
Automatización de respuestas	FortiAnalyzer puede **activar respuestas automatizadas** en FortiGate/FortiEDR (ej. bloquear IP, aislar endpoint) en <1 segundo; otras soluciones requieren integración manual con latencia >5 segundos

Cumplimiento Normativo Colombiano del Sector Público:

- **Resolución 551 de 2022** (Ministerio de TI colombiano): exige **registro centralizado, inalterable y correlacionado** de eventos de seguridad.
- **ISO 27001**: requiere análisis de logs con **correlación de amenazas** y reporte automatizado
- **NIST SP 800-53**: exige monitorización continua con capacidad de respuesta automatizada

Otras cualidades ofrecidas por el FortiAnalyzer:

- Reportes **pre-certificados** para cumplimiento normativo colombiano (incluyendo formatos exigidos por MinTIC).
- **WORM storage** (Write Once Read Many) para logs inalterables, requisito crítico de Resolución 551 2022.
- **Dashboards de cumplimiento** nativos para ISO 27001/NIST sin necesidad de desarrollo adicional.

Rendimiento y Escalabilidad Generacional

El nuevo appliance representa un salto generacional con:

(…)

Decisión técnica: Adquirir una solución de otro fabricante exigiría 3–5 a**ppliances adicionales**, incrementando costos de:

- Hardware (>+250%).
- Energía y espacio físico (+180%).
- Capacitación de personal (+200% por múltiples plataformas).

Economía de Operación y Reducción de Costos Totales

Mantener homogeneidad de marca genera:

Beneficio	Impacto Económico
Repuestos intercambiables	Tarjetas, módulos y software compartidos entre FortiGate/FortiAnalyzer/FortiEDR (-40% costo de inventario)
Soporte unificado	Un único contrato de soporte Fortinet (no 3–4 contratos con diferentes fabricantes)
Actualizaciones sincronizadas	FortiOS, FortiAnalyzer y FortiEDR se actualizan en sincronía sin rupturas de compatibilidad

(…)

La adquisición de FortiAnalyzer se justifica por ser la única solución que garantiza una integración nativa, completa y optimizada con la infraestructura de ciberseguridad Fortinet actualmente implementada en la Entidad, permitiendo la centralización, correlación y análisis en tiempo real de los eventos generados por componentes como FortiGate, FortiEDR y FortiAP. Su arquitectura utiliza protocolos propietarios de Fortinet, capacidades de correlación preconfiguradas y mecanismos de respuesta automatizada **que no pueden ser replicados por soluciones de terceros sin desarrollos adicionales, mayores costos de integración y riesgos operativos**. Asimismo, proporciona funcionalidades específicas para el cumplimiento de los requerimientos de monitoreo, trazabilidad y conservación de registros establecidos en la normativa vigente, incluyendo la Resolución 551 de 2022, ISO 27001 y NIST SP 800-53. En consecuencia, la adopción de una solución diferente generaría

incompatibilidades técnicas, pérdida de capacidades de automatización, mayores costos de operación y un incremento del riesgo asociado a la gestión integral de la seguridad de la información de la Entidad.

Adicionalmente, FortiAnalyzer ofrece un nivel superior de rendimiento y escalabilidad, permitiendo procesar grandes volúmenes de eventos de seguridad con baja latencia y una alta eficiencia en el uso de recursos de hardware y almacenamiento. **Esta capacidad reduce significativamente la necesidad de infraestructura adicional, optimiza los costos de soporte, administración y mantenimiento, y garantiza la continuidad operativa de la plataforma de seguridad institucional**. De igual forma, al mantener la homogeneidad tecnológica dentro del ecosistema Fortinet, se preserva la compatibilidad entre componentes, se simplifica la gestión del soporte especializado y se minimizan los riesgos derivados de integraciones con plataformas de terceros, las cuales podrían afectar la capacidad de detección, correlación y respuesta oportuna frente a incidentes de seguridad.

Capacidad de Procesamiento para un Ecosistema Multicapa

El nuevo appliance soporta hasta 200 GB de logs por día, con una tasa de recolección de 6.000 logs por segundo y análisis sostenido de 4.000 logs por segundo. Esta capacidad está dimensionada para absorber de forma simultánea los flujos de eventos del Firewall, los Access Points, el WAF y el FortiEDR, sin saturación ni pérdida de registros, incluso durante picos de tráfico o ataques de gran volumen (DDoS). Esto garantiza la visibilidad total y continua sobre el ecosistema de seguridad de la entidad.

Almacenamiento Seguro con Cifrado Nativo

Incorpora 16 TB de almacenamiento total en 4 discos con tecnología de auto-cifrado (Self-Encrypting Drives - SED), asegurando la protección de los registros de auditoría en reposo bajo estándares criptográficos alineados con el control A.10 (Criptografía) de la ISO 27001:2022. Mantiene hasta 50 días de datos analíticos en línea, esenciales para investigaciones forenses retrospectivas ante ataques APT de detección tardía.

Alta Disponibilidad y Resiliencia Operativa

Soporta configuración RAID 10 por defecto, garantizando tolerancia a fallos de disco sin interrupción del servicio de orquestación. Incluye un Módulo de Plataforma Confiable (TPM) que protege la integridad del proceso de arranque contra ataques de firmware, asegurando que el nodo central de visibilidad no pueda ser comprometido desde el nivel más bajo del sistema. Estas características son directamente compatibles con los lineamientos del Plan de Continuidad y Disponibilidad TIC de la CRA.

Escalabilidad y Compatibilidad con la Arquitectura Empresarial

Soporta la gestión integrada de hasta 800 dispositivos o dominios virtuales (VDOMs), con 4 puertos RJ45 Gigabit Ethernet y 2 puertos SFP de fibra óptica para integración flexible en la infraestructura de red. Esta capacidad garantiza que el crecimiento futuro del ecosistema tecnológico de la CRA —nuevos Access Points, expansión del WAF, incorporación de nuevos segmentos de red— pueda ser absorbido sin necesidad de reemplazar el equipo.

Alineación con el Marco Normativo Institucional

La renovación de esta plataforma de orquestación no es únicamente una decisión tecnológica. Es un compromiso institucional con la **seguridad del Estado**, la

confianza ciudadana y el cumplimiento de las obligaciones normativas de la CRA como entidad del Gobierno Nacional:

- **MSPI / MinTIC**: Mantiene operativos los controles de monitoreo continuo y gestión de incidentes exigidos para entidades públicas.
- **ISO 27001:2022**: Soporta los dominios A.8 (Activos), A.10 (Criptografía), A.12 (Operaciones), A.13 (Comunicaciones) y A.16 (Incidentes).
- **NIST CSF**: Habilita las funciones Identify, Detect, Respond y Recover con datos correlacionados de todo el ecosistema.
- **Plan de Continuidad TIC**: Garantiza la trazabilidad completa de eventos ante contingencias operativas.
- **Evidencia forense**: Preserva la cadena de custodia digital para procesos disciplinarios, legales o ante la Fiscalía

La CRA opera un ecosistema de seguridad multicapa conformado por Firewall, Access Points, WAF y FortiEDR que, de forma individual, ofrecen protección efectiva en cada capa. Sin embargo, es la plataforma de gestión y análisis centralizado la que integra, correlaciona y dota de inteligencia operativa a todo el ecosistema. Con la inminente llegada del fin de soporte del equipo vigente en junio de 2026, mantener esta solución desactualizada equivale a operar con el cerebro de seguridad de la entidad en estado de vulnerabilidad crítica. La adquisición inmediata del nuevo appliance de gestión centralizada es, por tanto, una decisión urgente, estratégica e impostergable para la CRA

Los productos y servicios por adquirir son bienes y servicios de común utilización con especificaciones técnicas, patrones de desempeño y calidad iguales o similares, que en consecuencia para el presente proceso pueden ser agrupados como bienes y servicios homogéneos para su adquisición pudiéndose definir, así como bienes y servicios de características técnicas uniformes.

El procedimiento de la Selección Abreviada a través de subasta inversa se realizará de forma electrónica de acuerdo con lo establecido en el artículo 2.2.1.2.1.2.2 (Modificado por el artículo 6 del Decreto 1860 de 2021) y siguientes del Decreto Reglamentario 1082 de 2015.

Finalmente, en cumplimiento de lo dispuesto en el Decreto 2883 de 2007, modificado por el Decreto 2412 de 2015 y la Resolución 844 del 1 de septiembre de 2016, la necesidad expuesta se encuentra incorporada en el consecutivo No. 026 del Plan Anual de Adquisiciones 2026, aprobado en el Comité de Expertos ordinario No. 01 del 2 de enero de 2026. De igual manera, según acta No. 028 del 11 de junio del 2026, el comité de contratación recomienda la presente contratación.

Es importante resaltar que una vez revisados los acuerdos marcos vigentes en Colombia Compra Eficiente, no existe acuerdo marco para este tipo de solución requerida por la Entidad.

Teniendo en cuenta lo anterior y que los bienes y servicios a contratar cumplen con las características técnicas uniformes, se considera conveniente adelantar un proceso de selección en la modalidad de Subasta Inversa conforme a lo establecido en el numeral 2º del artículo 2º, de la Ley 1150 de 2007 y artículo 2.2.1.2.1.2.2 del Decreto 1082 de 2015, modificado por el artículo 6 del Decreto 1860 de 2021, para contratar la adquisición de una solución integral para la gestión y análisis centralizado de la seguridad de infraestructura de red, la cual permite la consolidación y almacenamiento seguro de registros y eventos generados por los dispositivos de seguridad, facilitando un monitoreo en tiempo real de la superficie de ataque y la identificación proactiva de amenazas.

De igual manera, el literal a), Numeral 2, del Artículo 2, de la Ley 1150 de 2007, dispone como causal de selección abreviada la subasta inversa para la adquisición o suministro de bienes y servicios de características técnicas uniformes y de común utilización por parte de las entidades que corresponden a aquello que poseen las mismas especificaciones técnicas, con independencia de su diseño o de sus características descriptivas, y comparten patrones de desempeño y calidad objetivamente definidos. Esta disposición ha sido reglamentada en el artículo 2.2.1.2.1.2.2 del Decreto 1082 de 2015, modificada por el artículo 6 del Decreto 1860 de 2021, en el cual se establece el procedimiento a seguir en tal caso.

El presente proceso de Selección Abreviada Por Subasta Inversa se regirá por la Constitución Política, las leyes de la República de Colombia y en especial por la Ley 80 de 1993, la Ley 1150 de 2007, la Ley 1882 de 2018, la Ley 1474 de 2011, el Decreto 1082 de 2015, el Decreto 1860 de 2021, Decreto 287 de 2026, manuales y documentos tipo de Colombia Compra Eficiente y demás normas que la complementen, adiciones o reglamenten.

De acuerdo con lo establecido en el artículo 8º de la Ley 1150 de 2007 y en los artículos 2.2.1.1.1.7.1. y 2.2.1.1.2.1.4 del Decreto 1082 de 2015, el día 19 de junio de 2026 la COMISIÓN publicó en el SECOP II los documentos del proceso: (i) aviso de convocatoria, (ii) los estudios y documentos previos, (iii) El proyecto de pliego de condiciones y sus anexos por el termino de cinco (5) días hábiles, plazo durante el cual se recibieron observaciones y estas fueron resueltas por escrito como mensaje público.

De conformidad con lo establecido en artículo 12 de la Ley 1150 de 2007, modificado por el artículo 34 de Ley 2069 de 2020, reglamentado por los artículos 2.2.1.2.4.2.2 y 2.2.1.2.4.2.4 del Decreto 1082 de 2015, modificado por el artículo 5 del Decreto 1860 de 2021, el presente proceso de selección **NO** se limitará a Mipymes, como quiera que durante el termino establecido en el cronograma del proceso se recibieron dos (2)manifestaciones por parte de las firmas **DATASEC S.A.S** e **IOSERVICES SAS,** sin embargo, la solicitud de la firma **DATASEC S.A.S.,** no viene firmada por el revisor fiscal que se evidencia en el certificado de libertad y tradición adjunto por el proveedor, incumpliendo lo establecido en el numeral 4.2. del Pliego de condiciones y lo señalado en el artículo 5 del Decreto 1861 de 2021 que modificó la Subsección 2 de la Sección 4 del Capítulo 2 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015.

Que en mérito de lo expuesto, la Subdirectora Administrativa y Financiera de la Comisión de Regulación de Agua Potable y Saneamiento Básico (CRA);

RESUELVE:

ARTÍCULO PRIMERO. Ordenar la apertura del Proceso de Selección Abreviada Por Subasta Inversa No. 03 de 2026, cuyo objeto es: *"026-ADQUISICIÓN DE UNA SOLUCIÓN INTEGRAL PARA LA GESTIÓN Y ANÁLISIS CENTRALIZADO DE LA SEGURIDAD DE LA INFRAESTRUCTURA DE RED, LA CUAL PERMITE LA CONSOLIDACIÓN Y ALMACENAMIENTO SEGURO DE REGISTROS Y EVENTOS GENERADOS POR LOS DISPOSITIVOS DE SEGURIDAD, FACILITANDO UN MONITOREO EN TIEMPO REAL DE LA SUPERFICIE DE ATAQUE Y LA IDENTIFICACIÓN PROACTIVA DE AMENAZAS"*.

ARTÍCULO SEGUNDO. La Comisión de Regulación de Agua Potable y Saneamiento Básico (CRA) determinó que el valor total del presupuesto oficial para el presente proceso será hasta por la suma de **CIENTO CUARENTA Y NUEVE MILLONES NOVECIENTOS NOVENTA Y DOS MIL SEISCIENTOS SESENTA Y CUATRO PESOS M/CTE ($149.992.664) INCLUIDO IVA,** todos los impuestos y la

totalidad de los costos directos e indirectos a que haya lugar, respaldado con el Certificado de Disponibilidad No. 22826 del 17 de junio de 2026.

Parágrafo: Las propuestas no podrán exceder el valor del presupuesto oficial para el presente proceso, so pena de RECHAZO de la misma.

ARTÍCULO TERCERO. El pliego de condiciones definitivo, los estudios previos y demás documentos del proceso se podrán consultar y descargar en el del Sistema Electrónico de Contratación Pública –SECOP II-

Todos los interesados y/o proponentes tendrán la obligación de revisar el Portal Único de Contratación y/o SECOP II, para verificar la expedición de cualquier tipo de documento relacionado en el pliego de condiciones del presente proceso.

Conforme a los parámetros establecidos por Colombia Compra Eficiente, el cronograma se fijará en Portal Único de Contratación Pública SECOP II.

ARTÍCULO CUARTO. Convóquese a las veedurías ciudadanas a fin de que efectúen el control social del presente proceso de contratación, para lo cual se suministrará la información y documentación pertinente que se requiera para el adecuado cumplimiento de su función. Lo anterior, en cumplimiento de lo establecido en el artículo 270 de la Constitución Política de Colombia y demás normas concordantes, al igual que lo dispuesto en el numeral 5 del artículo 2.2.1.1.2.1.5. del Decreto 1082 de 2015.

ARTÍCULO QUINTO. La presente resolución rige a partir de la fecha de su expedición.

Dada en Bogotá D.C., a los dos (02) días del mes de julio de 2026.

PUBLÍQUESE Y CÚMPLASE

MARY ISABEL CRISTANCHO BÁEZ
Subdirectora Administrativa y Financiera

Proyectó: Luis Fabian Marin Arias – Abogado SAF

Revisó: Jose Luis Rojas Yoque – Profesional Especializado SAF