Bogotá D.C., 25 de febrero de 2026

Señores
INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI – IGAC
Atención: **Ing. Roberto Pantoja**
Subdirector de Infraestructura Tecnológica
Supervisor del Contrato

Asunto: Solicitud de prórroga – Contrato No. **35177-2025** – UT **HC-WX SEGURIDAD 2025**

Respetado ingeniero Pantoja:

En el marco de la ejecución del Contrato No. 35177-2025, suscrito entre el **INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI – IGAC** y la **UT HC-WX SEGURIDAD 2025** (en adelante la "UT HEIMCORE – WEXLER" o "UT"), cuyo objeto es: **"Contratar la renovación del soporte, mantenimiento, garantía y licenciamiento de los dispositivos de seguridad perimetral Fortinet, así como la adquisición de componentes adicionales para robustecer los controles de seguridad de la Entidad",** me permito presentar solicitud formal de prórroga del plazo de ejecución, con fundamento en las consideraciones técnicas y operativas que se exponen a continuación.

CONSIDERACIONES

- El contrato contempla la renovación de soporte/licenciamiento de la plataforma Fortinet de seguridad perimetral del IGAC y la ejecución de actividades asociadas a Assessment, optimización, implementación, pruebas, puesta en producción y entrega de documentación e informes, conforme a lo establecido en el alcance contractual.

- De acuerdo con el anexo técnico, el proveedor debe realizar un levantamiento de información para dimensionar y programar las actividades de ASSESSMENT sobre las soluciones objeto de renovación, integrando equipos existentes y componentes con upgrade tecnológico, así como las nuevas funcionalidades requeridas por la Entidad.

- En desarrollo del contrato, la UT ha adelantado la coordinación y alistamiento de actividades; no obstante, se identificaron condiciones técnicas que incrementan la complejidad y el esfuerzo requerido para ejecutar correctamente el Assessment y el despliegue integral del servicio de acceso seguro basado en ZTNA, preservando la continuidad del servicio y la trazabilidad de las intervenciones.

1. ANTECEDENTES

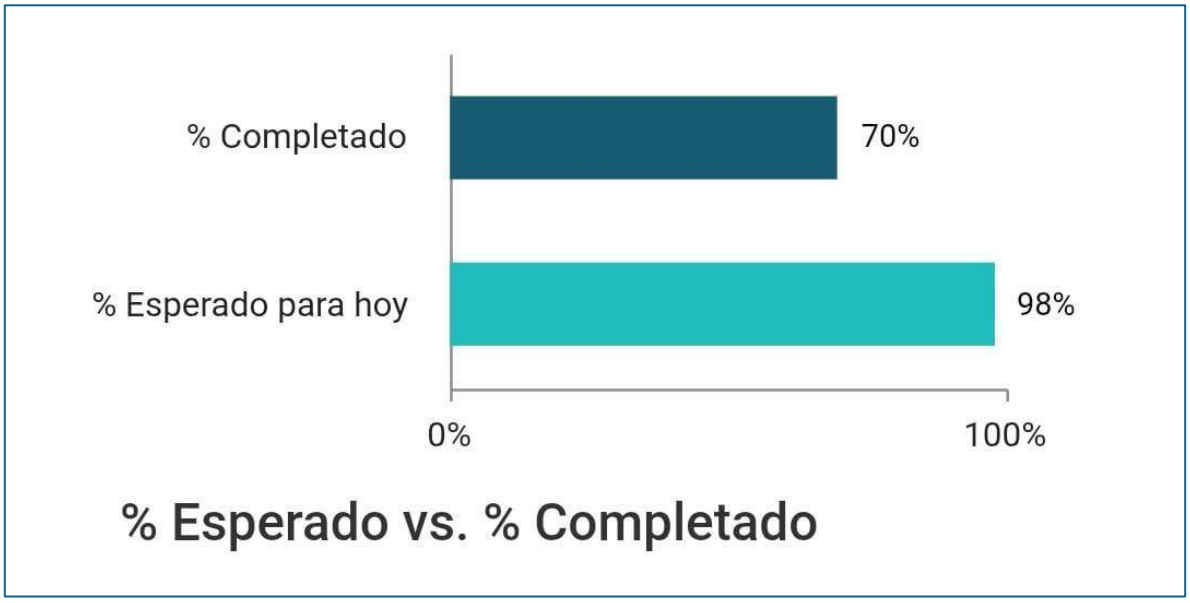
- La UT emitió solicitud de prórroga el día 19 de febrero del 2026 donde se solicitó prórroga del Contrato No. 35177-2025.

- El día 20 de febrero del 2026 se recibió respuesta a la solicitud con el memorando con radicado No. 2730SIT-2026-0000007-EE, relacionado con la primera solicitud de prórroga emitida el 19 de febrero del 2026.

- El día 23 de febrero la UT emitió respuesta al radicado No. 2730SIT-2026-0000007-EE, sin recibir respuesta, de momento, por parte de la entidad.

1.1. Estado de avance del proyecto (% de ejecución)

A la fecha, la UT ha ejecutado actividades de coordinación, levantamiento y preparación técnica asociadas al alcance, evidenciando un **avance global del setenta por ciento (70%)**. No obstante, conforme a la línea base del cronograma vigente, el **avance esperado a la fecha** corresponde al **noventa y ocho por ciento (98%)**, identificándose una brecha del **veintiocho por ciento (28%)**.



Dicha desviación no obedece a una falta de gestión, sino a dependencias técnicas y operativas propias de la ejecución en entornos productivos y con servicios críticos, en especial: (i) el nivel de complejidad del Assessment sobre infraestructura con condición de legado (legacy) y deuda técnica acumulada, y (ii) la necesidad de coordinar habilitaciones, ventanas de cambio, alistamiento de endpoints y pruebas de aceptación para alcanzar el 100% del despliegue y operación estable de ZTNA para 1.500 usuarios. En consecuencia, el ajuste de plazo se orienta a recuperar la senda del cronograma y asegurar la entrega

integral, verificable y documentada del alcance contractual.

2. CONSIDERACIONES Y JUSTIFICACIÓN TÉCNICA DE LA PRÓRROGA

La presente solicitud se sustenta en la necesidad de ajustar la línea base de ejecución (cronograma y ventanas técnicas) para asegurar el cumplimiento integral del alcance contractual, particularmente en lo relacionado con: (i) Assessment y optimización de la solución de seguridad perimetral, y (ii) despliegue y puesta en funcionamiento del servicio de acceso seguro basado en Zero Trust Network Access (ZTNA) con FortiClient EPP/ATP, en los términos exigidos por el IGAC.

2.1. Assessment sobre infraestructura SD-WAN / Firewalls en operación y con condición de legado

Conforme al anexo contractual, el Assessment debe incluir levantamiento de información, análisis de integraciones, evaluación de nuevas funcionalidades y necesidades del IGAC, y la formulación de una propuesta de ajustes de arquitectura y configuración respaldada en recomendaciones del fabricante y mejores prácticas; lo anterior, para aprobación del Supervisor del Contrato previo a la implementación y puesta en producción.

En este contexto, la realización del Assessment sobre los catorce (14) dispositivos indicados (FortiGate FWF-61F (12), FG-90G (2) y FortiGate 1800F) requiere un esfuerzo adicional debido a que parte de la plataforma corresponde a infraestructura en condición de legado (legacy) y con deuda técnica acumulada, lo cual incrementa la complejidad del análisis y de la definición de acciones de optimización, especialmente por:

- Heterogeneidad de versiones, políticas y configuraciones históricas, que obliga a validar compatibilidades, dependencias y comportamiento real en producción antes de proponer reconfiguraciones o afinamientos.

- Necesidad de realizar levantamiento detallado de políticas, objetos, rutas, reglas de SD-WAN, VPN (SSL y site-to-site), perfiles de seguridad, logging y telemetría, así como su integración con plataformas como FortiManager/FortiAnalyzer y/o SIEM, con el fin de determinar impactos y prevenir degradaciones del servicio.

- Requerimiento de ejecución bajo ventanas controladas de intervención, respaldos previos, verificación de procedimientos de rollback y realización de pruebas de funcionamiento, teniendo en cuenta que los equipos soportan conectividad y servicios críticos de la Entidad.

Adicionalmente, el clúster de FortiGate 1800F en HA requiere una actualización del firmware para llevar estos equipos a la última versión liberada 7.4.11, la cual es de vital importancia debido a que esta cubre vulnerabilidades críticas a nivel de FortiCloud SSO, pero para poder realizar esta actividad se requiere una ventana de mantenimiento con previo visto bueno y aprobación por parte del equipo de TI y coordinación con las áreas y sistemas publicados misionales, esto teniendo en cuenta que el proceso requiere el reinicio de los dos equipos FortiGate lo que generaría una interrupción momentánea de los servicios misionales de la Entidad lo que podría ocasionar corrupción en la información si no se hace bajo de manera controlada y coordinada con los administradores de los sistemas de información.

Las sugerencias para la corrección de las reglas como es el caso de las políticas que tienen como origen o destino el objeto "ALL" al igual que los servicios en "ALL" requieren en su gran mayoría del conocimiento de los administradores de RED y de Seguridad perimetral quienes son los que conocen a que recurso o área pertenece cada segmento a delimitar. Por parte de nosotros podemos acompañar y resolver las dudas que se tengan al respecto y proporcionar los mejores métodos para poder identificar los objetos que se podrían establecer en caso de que no se tenga claridad de que se debería permitir y que no, sin embargo, este es un proceso que puede llevar bastante tiempo ya que implica que se analice política por política (1.581 políticas) y se defina en conjunto que limitaciones se pueden establecer o si se deben dejar tal cual como están.

En consecuencia, se requiere un plazo adicional que permita culminar el Assessment con el nivel de detalle exigido, presentar el resultado con propuesta para aprobación, y posteriormente ejecutar la optimización y puesta en producción con pruebas y documentación completa, en cumplimiento de las obligaciones contractuales.

2.2. Despliegue completo y operación del servicio ZTNA (FortiClient EPP/ATP) para 1.500 usuarios

De igual forma, el alcance contractual establece la implementación de una solución de Servicios de Acceso Seguro basada en ZTNA, que permita validar continuamente la identidad del usuario y el estado del dispositivo antes de autorizar acceso a recursos on-premise y cloud. Adicionalmente, se exige el licenciamiento y soporte cotérmino hasta el 30 de noviembre de 2028, la entrega de certificados a nombre del IGAC y la constancia de que el servicio se encuentre instalado, configurado y puesto en funcionamiento.

Para alcanzar el 100% del despliegue de agentes y asegurar su operación estable, se requiere un plazo adicional considerando dependencias técnicas y operativas inherentes a este tipo de implementación, entre ellas:

- Habilitación de puertos, flujos y reglas de comunicación necesarias para el aprovisionamiento, registro, actualización y aplicación de políticas del agente, así como para la publicación y consumo seguro de los recursos bajo el modelo ZTNA.

- Disponibilidad y alistamiento de las máquinas y servicios involucrados (on-premise y/o cloud), validando conectividad, DNS, certificados, ruteo y resolución, además de la coordinación de ventanas de cambio para no afectar la operación institucional.

- Condiciones propias de endpoint y operación: permisos de instalación, compatibilidad, políticas corporativas, perfiles de seguridad y validaciones asociadas a postura del dispositivo para garantizar consistencia en la población objetivo.

- Ejecución de pruebas de funcionamiento y aceptación (acceso a aplicaciones internas, segmentación, validación de identidad y postura, comportamiento ante incumplimiento de postura, logging y trazabilidad), de forma que el servicio cumpla los criterios de seguridad, disponibilidad y confidencialidad definidos por la Entidad.

Por lo anterior, el ajuste de plazo se orienta a garantizar un despliegue completo, verificable y alineado con mejores prácticas, evitando reprocesos y mitigando riesgos operacionales asociados a la implementación parcial o a cambios no validados.

2.2.1 Validación técnica del modelo de licenciamiento ZTNA – Pruebas de laboratorio y confirmación con fabricante

Durante la fase de implementación del servicio ZTNA, y específicamente en el componente de licenciamiento asociado a FortiClient EMS, se identificó la necesidad de validar técnicamente el modelo de consumo de licencias requerido por la Entidad (modalidad basada en usuario para 1.500 usuarios).

Con el fin de evitar reprocesos en producción y garantizar cumplimiento estricto del alcance contractual, la UT dispuso un entorno controlado de laboratorio en nuestras oficinas, donde se realizó una simulación integral del esquema de despliegue bajo dos modalidades:

1. Licenciamiento basado en endpoint (por dispositivo).
2. Licenciamiento basado en usuario (user-based), direccionado a identidad y no a dispositivo.

2.2.1.1 Pruebas técnicas realizadas en laboratorio (Validación modalidad user-based)

En el entorno de pruebas se desplegó una arquitectura que incluyó:

- FortiGate con políticas ZTNA habilitadas.
- FortiClient EMS para administración centralizada.
- Integración con directorio (AD) para validación de identidad.
- Simulación de múltiples dispositivos por usuario.
- Validación de registro, aprovisionamiento y asignación automática de licencias.

Las pruebas incluyeron:

- Proceso de enrolamiento del agente bajo esquema identity-based.
- Validación de postura del endpoint (compliance check).
- Asignación dinámica de licencias por usuario con múltiples dispositivos.
- Pruebas de desconexión, cambio de dispositivo y reasignación.
- Verificación de consumo simultáneo bajo políticas ZTNA activas.
- Validación de telemetría y trazabilidad en FortiAnalyzer.

Durante estas pruebas se identificó que, aunque históricamente Fortinet manejó un esquema de licenciamiento user-based que permitía hasta dos (2) o tres (3) agentes por usuario, la versión actualmente disponible para adquisición y activación en plataforma ya no permite la asignación efectiva bajo esa modalidad.

Técnicamente se evidenció que:

- El consumo real en FortiClient EMS se realiza por endpoint registrado.
- El motor de conteo de licencias se basa en dispositivo activo y no en identidad lógica.
- No es posible consolidar múltiples endpoints bajo una única licencia de usuario.
- El sistema bloquea el aprovisionamiento cuando se supera el número de endpoints licenciados, independientemente de que pertenezcan al mismo usuario.

Adicionalmente, se realizaron pruebas de stress controlado para validar comportamiento ante despliegue masivo, confirmando que el dimensionamiento debe realizarse por endpoint efectivo para evitar indisponibilidad del servicio.

Este proceso tomó mayor tiempo del previsto debido a:

- Ajustes de arquitectura en laboratorio.
- Validación de diferentes versiones de firmware.
- Repetición de escenarios para descartar inconsistencias.

El objetivo fue garantizar que la solución implementada para el IGAC no generara riesgos de sub-licenciamiento, indisponibilidad o incumplimiento contractual.

2.2.1.2 Validación y confirmación directa con especialistas de Fortinet

Paralelamente a las pruebas internas, la UT sostuvo múltiples sesiones técnicas con especialistas de Fortinet en las líneas:

- Ingeniería preventa.
- Arquitectura de soluciones ZTNA.
- Especialistas de producto FortiClient EMS.
- Soporte técnico de segundo nivel.

Durante dichas sesiones se presentó:

- Arquitectura propuesta para IGAC.
- Alcance contractual requerido (1.500 usuarios).
- Referencia al contenido publicado en la documentación oficial donde se menciona modalidad de consumo por usuario con múltiples agentes.

Fortinet realizó revisión formal de la documentación pública que aún menciona el esquema user-based con máximo de agentes por usuario, confirmando que:

- Esa modalidad correspondía a un esquema comercial anterior.
- Fue retirada progresivamente del portafolio activo.
- Actualmente las suscripciones disponibles y soportadas operan bajo modelo endpoint-based.
- La plataforma EMS vigente no permite activar ni administrar consumo real bajo modalidad pura por usuario.

En consecuencia, el fabricante confirmó técnicamente que el único esquema viable y soportado es el licenciamiento por endpoint efectivo. Esta validación fue determinante para evitar:

- Riesgo contractual por incumplimiento de alcance.
- Eventuales sanciones por subdimensionamiento.
- Impacto en operación ZTNA al superar conteo permitido.

2.2.1.3. Incidencia en el cronograma y justificación de fuerza mayor técnica

El tiempo invertido en:

- Diseño y ejecución de laboratorio controlado.
- Validación comparativa de modelos de licenciamiento.
- Sesiones técnicas con múltiples especialistas del fabricante.
- Confirmación oficial del esquema soportado.

Generó una extensión no prevista inicialmente dentro del cronograma base, dado que se priorizó garantizar certeza técnica antes del despliegue masivo en ambiente productivo del IGAC.

Es importante resaltar que esta situación obedece a una condición externa asociada a cambios en el modelo comercial del fabricante, no informados oportunamente en la documentación pública, lo cual constituye un hecho sobreviniente y ajeno a la voluntad de la UT.

Adicionalmente, la ejecución del contrato se ha realizado sobre infraestructura en operación crítica, con ventanas restringidas y dependencias institucionales que limitan intervenciones inmediatas, lo cual configura condiciones operativas que pueden considerarse como circunstancias técnicas excepcionales que impactan el plazo inicialmente previsto.

3. SOLICITUD DE PRORROGA

Con fundamento en lo expuesto, de manera respetuosa solicitamos al IGAC aprobar la prórroga del plazo de ejecución del Contrato No. 35177-2025 hasta el treinta y uno (31) de marzo de 2026, con el fin de culminar en su totalidad las actividades de Assessment, optimización, implementación, pruebas, puesta en producción y entrega de documentación e informes, así como el despliegue completo del servicio ZTNA conforme al alcance contractual.

La prórroga solicitada no responde a falta de gestión ni a incumplimiento, sino a una actuación diligente orientada a:

- Validar técnicamente el modelo de consumo correcto.
- Garantizar cumplimiento contractual real.
- Evitar riesgos de indisponibilidad o incumplimiento.
- Asegurar un despliegue estable y verificable del servicio ZTNA para 1.500 usuarios.
- Cerrar el contrato con certeza técnica antes del 31 de marzo de 2026.

4. COMPROMISO DE LA UT HC-WX SEGURIDAD 2025

La **UT HEIMCORE – WEXLER (UT HC-WX SEGURIDAD 2025)** reitera su compromiso de ejecutar las actividades pendientes con estricta observancia de las recomendaciones del fabricante y mejores prácticas del mercado, garantizando:

- Coordinación permanente con el Supervisor del Contrato para la aprobación de resultados del Assessment, propuesta de ajustes, plan y cronograma de instalación.

- Ejecución de intervenciones bajo control de cambios, con respaldos previos, validación de procedimientos de contingencia/rollback y realización de pruebas que

garanticen la correcta puesta en marcha.

- Entrega oportuna y completa de la documentación y diagramas editables, así como del Informe de Assessment y Optimización en formatos editables de Office, incluyendo parámetros ajustados, arquitectura implementada y recomendaciones.

- Cumplimiento integral del alcance, procurando la continuidad operativa de los servicios y el cierre contractual a satisfacción del IGAC.

Agradecemos su atención y quedamos atentos a las indicaciones correspondientes para formalizar la prórroga mediante el instrumento contractual aplicable.

Cordialmente

JESUS ALBERTO FRANCO ACOSTA
Representante Legal UT HC-WX SEGURIDAD 2025
C.E. 582410
NIT: 902009528 - 1