Bogotá D.C., 18 de marzo de 2026

Señores
INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI – IGAC
Atención: **Diego Fernando Melo**
Subdirector (e) de Infraestructura y supervisor del contrato

Asunto: Respuesta Radicado No. 2730SIT-2026-0000009-EE

En el marco de la ejecución del **Contrato No. 35177-2025**, suscrito entre el **INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI – IGAC** y la **UT HEIMCORE – WEXLER (UT HC-WX SEGURIDAD 2025)**, 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", nos permitimos dar respuesta formal al Radicado No. 2730SIT-2026-0000009-EE, atendiendo de manera puntual los requerimientos formulados por la Entidad.

Respuesta ZTNA

En atención a la solicitud de aclaración No. 1, y en cumplimiento de lo requerido respecto a precisar la disponibilidad del modelo de licenciamiento por usuario, su fecha de retiro y alternativa equivalente, nos permitimos emitir integrando los documentos aportados

Se precisa que el componente de ZTNA, según el alcance, debe asegurar el cumplimiento del esquema requerido por la Entidad. En ese sentido, y **dada la inconsistencia evidenciada**, se requiere soporte formal, así:

i. **Licenciamiento por usuario (1.500) – Soporte del fabricante. Allegar certificación/documento oficial del fabricante donde se indique:**

   - si el licenciamiento **User-Based** se encuentra disponible o no;
   - en caso de no estarlo, la **fecha exacta** a partir de la cual fue retirado o no soportado;
   - la alternativa oficial equivalente y sus condiciones."

Aclaración N°1:

Al respeto nos permitimos confirmar que se realizó reunión con el equipo técnico del fabricante Fortinet donde se nos confirma lo siguiente:

En documento adjunto que denominaremos **Anexo - 1 Ficha técnica oficial del fabricante Fortinet (Datasheet)** y con fecha de publicación noviembre 5 de 2025 como se evidencia nota al final de la página 12 de 12.

Se detalla los modelos de licenciamiento vigente del producto Forti Client ZTNA de la siguiente manera:

Order Information

You can order FortiClient based on the number of devices. The following table reflects the latest FortiClient device-based license packs.

EDITION	VPN/ZTNA	VPN/ ZTNA + EPP/ ATP	MANAGED	CHROMEBOOK
SaaS (Cloud Hosted EMS)				
25-pack	FC1-10-EMS05-428-01-DD	FC1-10-EMS05-429-01-DD	FC1-10-EMS05-485-01-DD	FC1-10-EMS05-403-01-DD
500-pack	FC2-10-EMS05-428-01-DD	FC2-10-EMS05-429-01-DD	FC2-10-EMS05-485-01-DD	FC2-10-EMS05-403-01-DD
2000-pack	FC3-10-EMS05-428-01-DD	FC3-10-EMS05-429-01-DD	FC3-10-EMS05-485-01-DD	FC3-10-EMS05-403-01-DD
10 000 pack	FC4-10-EMS05-428-01-DD	FC4-10-EMS05-429-01-DD	FC4-10-EMS05-485-01-DD	FC4-10-EMS05-403-01-DD
On Premise				
25-pack	FC1-10-EMS04-428-01-DD	FC1-10-EMS04-429-01-DD		FC1-10-EMS04-403-01-DD
500-pack	FC2-10-EMS04-428-01-DD	FC2-10-EMS04-429-01-DD		FC2-10-EMS04-403-01-DD
2000-pack	FC3-10-EMS04-428-01-DD	FC3-10-EMS04-429-01-DD		FC3-10-EMS04-403-01-DD
10 000 pack	FC4-10-EMS04-428-01-DD	FC4-10-EMS04-429-01-DD		FC4-10-EMS04-403-01-DD
FortiCare Best Practices Consultation Service				
25-999 endpoints		FC1-10-FCBPS-310-02-DD		
1000-9999 endpoints		FC2-10-FCBPS-310-02-DD		
10 000+ endpoints		FC5-10-FCBPS-310-02-DD		
Training Services				
Classroom - virtual ILT	FT-FCT			
Lab access - standard NSE training lab environment	FT-FCT-LAB			
NSE5 exam voucher	NSE-EX-SPL5			

You can order FortiClient based on the number of users. The following table reflects the latest FortiTrust user-based license ranges.

FORTITRUST USER-BASED LICENSE RANGES*				
SOLUTION	SKU LICENSE	VPN/ ZTNA	VPN/ ZTNA + EPP/ ATP	MANAGED VPN/ ZTNA + EPP/ ATP
Cloud-hosted EMS	50-499 users	FC2-10-EMS05-509-02-DD	FC2-10-EMS05-546-02-DD	FC2-10-EMS05-556-02-DD
	500-1999 users	FC3-10-EMS05-509-02-DD	FC3-10-EMS05-546-02-DD	FC3-10-EMS05-556-02-DD
	2000-9999 users	FC4-10-EMS05-509-02-DD	FC4-10-EMS05-546-02-DD	FC4-10-EMS05-556-02-DD
	10 000+ users	FC5-10-EMS05-509-02-DD	FC5-10-EMS05-546-02-DD	FC5-10-EMS05-556-02-DD

* A user-based license allows a single user to install and use FortiClient on up to three devices.

Con lo anterior se observa que existen tres modelos o formas de licenciar el producto:

- Modelo Cloud por dispositivo
- Modelo On premise por dispositivo
- Modelo Cloud por cantidad de usuarios

Las licencias están identificadas por un numero de parte o SKU como lo llama el fabricante, y dicho SKU depende de la cantidad de licencias que desee adquirir el cliente y de las características técnicas que requiera el cliente.

Para este caso puntualmente se elige el SKU FC2-10-EMS04-429-01 que corresponde al modelo ON PREMISE que incluye las funcionalidades VPN-ZTNA + EPP/ATP. Las cuales corresponden a la solicitud de la ficha técnica emitida por el IGAC.

Sin embargo, el equipo técnico del IGAC nos trasmite una duda que tienen con relación a que las licencias denominadas por “usuario” permiten hacer el uso de la misma licencia hasta en tres dispositivos con el mismo usuario. A lo cual el fabricante nos responde de la siguiente manera.

El modelo de licenciamiento denominado User-Based, que se ofrecía únicamente en modalidad **CLOUD,** y no en modalidad **ON PREMSE,** presento anuncio de salida del mercado desde el 03 de noviembre del año 2025 como consta en documento adjunto el cual denominamos **Anexo 2 - Ciclo de vida del producto.**

Lo ratifica en su ficha técnica oficial del producto emitida públicamente el 3 de marzo del 2026 como consta en la página 6/6. Del documento adjunto denominado **Anexo 3 - Ficha técnica 2026.**

Frequently Asked Questions

What is BPS and should I include it for new deals?

BPS allows customers access to on-demand consultation with FortiClient/EMS product experts on all topics including how to deploy FortiClient solutions, recommended stable product upgrade paths for their use cases, guidance on license upgrades, guidance on EMS migrations with minimum data loss and transparent end user experience, and more. Including the BPS service with every new customer deal is recommended so they have access to product experts for any questions and issues that may come up while using the product.

What is the easiest way to order?

Per-device packs are available for terms of one to five years. See the ordering examples on the previous pages for expansion, renewals, and upgrades.

Is FortiClient licensed per-user or per-device?

On-premise FortiClient EMS and FortiClient Cloud re licensed per-device/endpoint.

What happened to the SASE option? Why do the first two pages not show it?

All options are still available. See the FortiSASE Ordering Guide.

How do I upgrade from one FortiClient license to another?

You can perform upgrades using the co-term tool.

NOTE: Upgrades are not supported between on-premise and cloud EMS deployments.

Página 5/6 Anexo 3 Ficha técnica 2026

Siendo el modelo de licenciamiento **ON PREMISE** solicitado por la Entidad en su ficha técnica y cuyo número de parte de fabrica correspondiente, conforme a la tabla del documento oficial de Fortinet adjunto al número de parte FC2-10 EMS04-429-001 DD y el equivalente en modelo de licenciamiento por usuario en modalidad **CLOUD** el número de parte FC3-10EMS-509-02.

La **UT HC-WX SEGURIDAD 2025** en su oferta incluyo y entrego el modelo ON PREMISE FC2-10 EMS04-429-001 DD correspondiente a 1500 licencias solicitadas, sin embargo, el Fabricante Fortinet nos confirma que el modelo de licencias denominadas por usuario y que se ofrecían únicamente en modalidad CLOUD, ya no serán distribuidas a partir del año 2026 como consta en la carta adjunta denominada **Anexo 4 - Carta del fabricante** donde cita de la siguiente manera:

FORTINET

9 de marzo del 2026

Señores: Instituto Geográfico Agustín Codazzi - IGAC

Asunto: Certificación técnica productos Fortinet

Referencia: CTO 35177 DE 2025

Por medio de la presente, Fortinet, Inc. ("Fortinet") manifiesta que, al día de emisión de la presente, los productos FortiClient VPN/ZTNA y FortiClient EPP/ATP se comercializan bajo un modelo de licenciamiento bajo la figura *device-based* basado en paquetes disponibles en 25, 500, 2.000 y 10.000 dispositivos.

Los modelos de suscripción basados en usuarios previamente disponibles para despliegues *Cloud* han sido descontinuados para nuevas ventas, de acuerdo con los anuncios de ciclo de vida correspondientes.

Sin más por el momento, quedamos a sus órdenes para cualquier duda o aclaración.

Cordialmente.

En tal sentido la única alternativa oficial o equivalente que solicita el IGAC, y teniendo en cuenta que el fabricante no cuenta con otro modelo de venta de las licencias de FortiClient-ZTNA, es de adquirir las licencias bajo la modalidad que la UT Heimcore-Wexler, han entregado a la Entidad.

Confirmándose que técnicamente el producto es el mismo tanto para el modelo Cloud como el modelo On premise como consta en el documento adjunto **(Anexo 1 Ficha técnica oficial del fabricante Fortinet - Datasheet)** del presente comunicado.

Se confirma igualmente que el producto cuenta con características y funcionalidades técnicas iguales y cumple con las propias solicitadas en la ficha técnica emitida por el IGAC en el proceso licitatorio.

Desde la gestión del proyecto, es importante precisar que no se presentan cambios en la funcionalidad ni en el alcance técnico de la solución, sino únicamente en el modelo de comercialización definido por el fabricante.

En este sentido, el fabricante ha establecido que el modelo de licenciamiento tipo CLOUD por usuario dejará de ser ofertado, tal como se indica en el comunicado oficial adjunto denominado "**Anexo 4 - Carta del fabricante**".

Por lo anterior, el ajuste corresponde exclusivamente a un cambio en el esquema de licenciamiento, sin impacto en la operación, desempeño o capacidades de la solución implementada, garantizando así la continuidad del servicio bajo las nuevas condiciones comerciales definidas por el fabricante.

En resumen, el cliente IGAC solicito de manera explícita en la ficha técnica del proceso emitida por parte del IGAC cita puntualmente de la siguiente manera;

"El servicio FortiClient EPP/ATP se requiere para una cantidad de 1500 usuarios, que además incluya licenciamiento y soporte de fábrica de la solución contérmino hasta el 30 de noviembre de 2028 y la entrega de los certificados de renovación de licenciamiento, soporte y garantía. Y recibo a satisfacción del certificado de la suscripción y soporte a nombre del IGAC y que dicho servicio se encuentre debidamente instalado, configurado y puesto en funcionamiento), cumpliendo con las siguientes características:"

ADQUISICIÓN SOLUCIÓN COMO SERVICIO ZTNA RPP/ATP			
ITEM	**DESCRIPCIÓN**	**CARACTERISTICAS**	**CANTIDAD**
1	Control de Acceso Remoto	Subscripción para 1500 Usuarios, con servicios incluidos de (IPS, Web, DNS, SSL, Anti-Malware, ZTNA y soporte Premium.	1

Tabla 10: Especificaciones de Solución como Servicio ZTNA RPP/ATP

c. El proveedor de este servicio deberá contemplar su Instalación, configuración total de la solución entre ellas despliegue y configuración del EMS perfiles y reglas de ZTNA **RPP/ATP** (Integraciones de seguridad con Firewalls, Fortimanager, Fortianalyzer, VPN SSL, VPN Site to Site, Configuración Perfiles de Seguridad, Integración con SIEM , así como automatizaciones requeridas por la entidad).
d. La entidad actualmente cuenta con el servicio de SASE, el cual debe ser completamente desinstalado por el proveedor. Esta desinstalación deberá incluir todos los componentes de las soluciones Fortinet que diere lugar. Asi mismo, el proveedor deberá garantizar que la implementación de la solución de ZTNA no se vea afectada ni tenga interferencia con algún componente de SASE.
El servicio debe ser implementado en on-premise máquina virtual VM, y será administrado y gestionado por el IGAC. De acuerdo con el literal C.
e. El proveedor deberá proyectar y entregar toda la documentación generada en las actividades requeridas en este numeral.
f. El proveedor deberá prestar los servicios de soporte y mantenimientos preventivos y correctivos a que haya lugar durante el plazo del servicio, de acuerdo con lo indicado en el **numeral 3.4** del presente documento.
g. El proveedor deberá realizar todas las actividades tendientes a implementar, integrar y poner en operación el ZTNA con todas su

Cabe resaltar que dentro de la ficha o requerimientos técnicos no se menciona la necesidad por parte de la Entidad de cubrir hasta tres (3) dispositivos con la misma licencia y partiendo que el modelo que contaba con esta condición era netamente CLOUD por usuarios y que el mismo se dejó de comercializar, como lo mencionamos anteriormente, y que a pesar de que ese modelo permitía una sola licencia por usuario para hasta tres dispositivos, donde el acceso es granular y controlado por dispositivo, lo que implica que el proceso de autenticación y autorización se realiza de manera individual por cada máquina o endpoint.

En consecuencia, las credenciales no son reutilizables entre dispositivos, y el modelo restringe múltiples sesiones simultáneas desde diferentes equipos con el mismo usuario, garantizando así un mayor nivel de control y protección frente a accesos no autorizados, lo que quiere decir que no significa que con 1500 licencias pueda cubrir hasta 4500 usuarios. Con la adquisición que hiciera el IGAC bien fuera por usuario o por dispositivo solo contaría con 1500 licencias para 1500 usuarios.

Ahora bien, la **UT HC-WX SEGURIDAD 2025** como proveedores de la Entidad y entendiendo la necesidad expresada por parte del equipo técnico del IGAC, una vez presentada esta situación de la necesidad de contar con un mayor número de licenciamiento con el fin de cubrir un mayor número de dispositivos con la solución adquirida.

La **UT HC-WX SEGURIDAD 2025**, está en disposición de aumentar hasta mil (1000) licencias adicionales a las inicialmente contratadas, es decir entregaríamos 2.500 licencias en lugar de las 1500 contratadas, sin ningún tipo de cargo adicional para el IGAC conservando la misma fecha de vigencia para todas las licencias, es decir unificando a la fecha de soporte solicitada por el IGAC, con el único propósito de beneficiar a la Entidad en su capacidad de protección a nivel de ciberseguridad desde el usuario final y mitigar de esta manera los inconvenientes de entendimiento que se pudieron presentar en esta negociación.

Se adjuntan a la presente los siguientes documentos:

- Anexo 1: Ficha técnica del fabricante con fecha de emisión Nov 5-2025
- Anexo 2: Ciclo de vida del producto, anuncio de salida del producto Cloud
- Anexo 3: Ficha tecnica del fabricante 2026
- Anexo 4: Carta del fabricante salida del producto Cloud.

ii. Pruebas y validaciones. Allegar el soporte completo de las "pruebas" referidas por la UT: reportes, métricas, metodología, ambiente, resultados y conclusiones, y cómo estas prueban equivalencia funcional frente al requerimiento por usuario.

Aclaración N°2:

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:

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

En el **Anexo 5 - Pruebas de laboratorio**, se relacionan las actividades que fueron ejecutadas por el equipo implementador.

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.

iii. Equivalencia funcional. Allegar un análisis comparativo que demuestre, de manera técnica y verificable, que el esquema propuesto garantiza las mismas funcionalidades/alcances requeridos por IGAC, incluyendo cobertura por usuario, multidispositivo, postura, políticas, administración y trazabilidad.

Aclaración N°3:

Conforme a las explicaciones anteriormente mencionadas, nos permitimos ratificar los siguiente:

Dentro de la ficha técnica emitida por el IGAC no se menciona la necesidad de contar con un modelo de licenciamiento que le permitiere usar hasta tres dispositivos con una misma licencia. Razón por la cual la ingeniería de la UT ni la del fabricante tuvieron en cuenta este requerimiento solicitado posteriormente y de manera verbal por la Entidad.

Se reitera que la funcionalidad técnica es la misma tanto para el modelo CLOUD como para el modelo ON PREMISE solicitado por la Entidad. Y el producto entregado cumple tal cual lo solicitado en la ficha técnica emitida por el IGAC como se puede evidenciar en el **Anexo -1 Ficha técnica oficial del fabricante Fortinet (Datasheet)**, documento oficial del fabricante donde se detalla las características técnicas del producto.

Order Information

You can order FortiClient based on the number of devices. The following table reflects the latest FortiClient device-based license packs.

EDITION	VPN/ZTNA	VPN/ ZTNA + EPP/ ATP	MANAGED	CHROMEBOOK
SaaS (Cloud Hosted EMS)				
25-pack	FC1-10-EMS05-428-01-DD	FC1-10-EMS05-429-01-DD	FC1-10-EMS05-485-01-DD	FC1-10-EMS05-403-01-DD
500-pack	FC2-10-EMS05-428-01-DD	FC2-10-EMS05-429-01-DD	FC2-10-EMS05-485-01-DD	FC2-10-EMS05-403-01-DD
2000-pack	FC3-10-EMS05-428-01-DD	FC3-10-EMS05-429-01-DD	FC3-10-EMS05-485-01-DD	FC3-10-EMS05-403-01-DD
10 000 pack	FC4-10-EMS05-428-01-DD	FC4-10-EMS05-429-01-DD	FC4-10-EMS05-485-01-DD	FC4-10-EMS05-403-01-DD
On Premise				
25-pack	FC1-10-EMS04-428-01-DD	FC1-10-EMS04-429-01-DD		FC1-10-EMS04-403-01-DD
500-pack	FC2-10-EMS04-428-01-DD	FC2-10-EMS04-429-01-DD		FC2-10-EMS04-403-01-DD
2000-pack	FC3-10-EMS04-428-01-DD	FC3-10-EMS04-429-01-DD		FC3-10-EMS04-403-01-DD
10 000 pack	FC4-10-EMS04-428-01-DD	FC4-10-EMS04-429-01-DD		FC4-10-EMS04-403-01-DD
FortiCare Best Practices Consultation Service				
25-999 endpoints		FC1-10-FCBPS-310-02-DD		
1000-9999 endpoints		FC2-10-FCBPS-310-02-DD		
10 000+ endpoints		FC5-10-FCBPS-310-02-DD		
Training Services				
Classroom - virtual ILT	FT-FCT			
Lab access - standard NSE training lab environment	FT-FCT-LAB			
NSE5 exam voucher	NSE-EX-SPL5			

Ver página 11 Anexo 1 Ficha técnica 2025.

Bundles

FORTICLIENT EDITION	VPN / ZTNA	EPP / ATP	Managed Services	Chromebook
Zero Trust Security	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Chromebook
Zero Trust Agent with MFA	✓	✓	✓	
Security Posture Tagging Rules	✓	✓	✓	
Central Management via EMS or FortiClient Cloud	✓	✓	✓	✓
Dynamic Security Fabric Connector	✓	✓	✓	
Vulnerability Agent and Remediation	✓	✓	✓	
SSL VPN with MFA	✓	✓	✓	
IPSEC VPN with MFA	✓	✓	✓	
FortiGuard Web and Video Filtering	✓	✓	✓	✓
Cloud Access Security Broker (CASB)[1]	✓	✓	✓	
FortiPAM Support	✓	✓	✓	
Central Logging and Reporting[2]	✓	✓	✓	✓
Next Generation Endpoint Security				
Potentially Unwanted Applications		✓	✓	
AI powered NGAV		✓	✓	
Removable Media Control		✓	✓	
Automated Endpoint Quarantine		✓	✓	
Application Firewall[3]		✓	✓	
Software Inventory		✓	✓	
Ransomware Protection[4]		✓	✓	
FortiClient Cloud Sandbox (SaaS)[3]		✓	✓	
FortiSandbox Integration (PaaS/Public Cloud/On-premises)[3]	✓	✓	✓	
Managed FortiClient Service				
Endpoint Onboarding			✓	
Initial Provisioning			✓	
Security Fabric Setup/Integration			✓	
Vulnerability Monitoring			✓	

Ver Página 9 Anexo 1 Ficha Técnica 2025

Respuesta assesment:

En relación con lo manifestado por la Unión Temporal respecto a la necesidad de culminar el Assesment sobre la infraestructura SD-WAN, Firewalls y componentes asociados, la Supervisión se permite precisar lo siguiente:

Si bien el Assesment hace parte del alcance contractual, la solicitud de prórroga debe sustentarse en elementos objetivos y verificables que demuestren:

1. El estado real de avance del Assesment.
2. Las actividades ejecutadas y pendientes.
3. Las causas específicas que impidieron su culminación dentro del plazo inicialmente pactado.
4. La relación directa entre dichas causas y la necesidad de ampliar el plazo contractual

Aclaración No. 1 y 2:

Respecto al estado actual de los assesment y a las actividades que se han ejecutado, nos permitimos informar que:

- **FortiAnalyzer 400E**:
    - Informe de análisis entregado.
    - Los cambios necesarios han sido aplicados satisfactoriamente.
    - Pendiente: Definir las ventanas de mantenimiento para los cambios en los demás equipos de la infraestructura Fortinet.

- **FortiGate 1800F**:
    - Informe de análisis entregado.
    - Se ha completado el análisis técnico del dispositivo.
    - Pendiente: Aplicación de cambios de configuración y ajustes.

- **SDWAN** (FortiWiFi-61F y FortiGate-90G):
    - Informe de análisis entregado.
    - Los cambios y ajustes correspondientes han sido revisados.
    - Pendiente: Coordinar las ventanas de mantenimiento para las actualizaciones necesarias.

Resumen de la Actividad de los Assesment:

- **FortiAnalyzer 400E**: El análisis ha sido completado, y se han aplicado los cambios solicitados, con el equipo funcionando correctamente. Los cambios en el resto de los equipos Fortinet requieren ser programados en las ventanas de mantenimiento previamente definidas.

- **FortiGate 1800F y SDWAN (FortiWiFi-61F y FortiGate-90G)**: Se ha entregado el análisis, y se están gestionando las configuraciones finales y las actualizaciones de firmware.

Próximos Pasos:

- Definir las ventanas de mantenimiento para los cambios pendientes en la infraestructura Fortinet.
- Coordinar la implementación de los cambios en las fechas programadas.
- Realizar las pruebas correspondientes para verificar la correcta integración de los equipos después de los ajustes.

A continuación, se relaciona el resumen sobre la actividad de los assesment:

EQUIPO	Informe de Análisis	Entregado al IGAC	Cambios aplicados	AVANCE
FortiGate 1800F	SI	SI	NO	66%
FortiAnalyzer 400E	SI	SI	SI	100%
FortiManager 200G	NO	NO	NO	0%
SDWAN (FortiWiFi-61F y FortiGate-90G)	SI	SI	NO	66%
			Avance total	58%

Como soporte a estas actividades, se adjuntan los siguientes documentos:

- **Anexo 6 - Informe de análisis FortiAnalyzer 400E**
- **Anexo 7 - Informe de análisis FortiGate**

Aclaración No.3

Respecto a las circunstancias que impidieron su culminación dentro del plazo inicialmente pactado, informamos que, dentro de las actividades de este contrato, se requería priorizar y culminar la instalación, configuración, parametrización y puesta en marcha de los siete (7) equipos SDWAN nuevos, así como la configuración y puesta en marcha del FORTISIEM dada la criticidad de estos frentes para el funcionamiento integral de la red y la ciberseguridad de las territoriales. A raíz de esto, el equipo de la UT y el ingeniero asignado por parte del IGAC, suspendieron las actividades correspondientes a los assesment para volcar su atención en las actividades anteriormente mencionadas. Este cambio generó que la actividad de los assesment fuera retomada nuevamente a finales del mes de febrero, enfocándose inicialmente en los equipos de FortiGate 1800F, FortiAnalyzer 400E y los SDWAN (FortiWiFi-61F y FortiGate-90G).

En conclusión, el retraso en la ejecución de los assesment fue debido a la necesidad de atender tareas críticas y urgentes relacionadas con la infraestructura SDWAN y la configuración del SIEM, las cuales fueron priorizadas para asegurar la operatividad de la red y la ciberseguridad.

Aclaración No. 4

Teniendo en las circunstancias mencionadas anteriormente, se requiere ampliar el plazo contractual con el fin de concluir las actividades correspondientes al assesment de los equipos de FortiGate 1800F, FortiAnalyzer 400E y los SDWAN (FortiWiFi-61F y FortiGate-90G).

A continuación, damos un detalle de las actividades que se requieren ejecutar en conjunto con el cliente y el plazo requerido para la finalización de estas:

El assesment de seguridad se realizará sobre los equipos **FortiGate 1800F** y **SDWAN** del cliente, componentes críticos de su infraestructura de red, con el fin de ejecutar actividades de actualización de firmware, optimización de políticas de seguridad, revisión y ajustes de conectividad y configuraciones generales, las cuales de detallan a continuación:

- **Actualización de Firmware:** Se debe actualizar el firmware de los equipos a las versiones más recientes (7.4.11, 7.6.6 y 7.4.10, respectivamente) para mejorar la seguridad, la compatibilidad y la estabilidad del sistema. Estas actualizaciones se debe realizarse bajo una ventana de mantenimiento programada, ya que esta operación puede interrumpir temporalmente los servicios y debe ser realizada de manera controlada.

- **Revisión y Optimización de Políticas de Seguridad:** Se realizará una revisión exhaustiva de las políticas de acceso para identificar aquellas que permiten el tráfico "ALL" y representan un riesgo de seguridad, modificándolas para hacerlas más restrictivas. Además, se eliminarán políticas no utilizadas y se ajustarán las configuraciones inadecuadas. Este proceso requiere actualizar y documentar las políticas de seguridad, asegurando que los cambios no afecten las comunicaciones legítimas y estén alineados con las necesidades de seguridad del cliente

- **Verificación de Conectividad:** Se validará la conectividad de los equipos a través de la red MPLS y VPN, enfocándose en la sede de Manizales, con problemas de conexión. Si hay problemas con el ISP, se recomienda que el cliente verifique la conexión con su proveedor. Resolver los problemas puede requerir intervención del ISP y pruebas adicionales, por lo que el cliente debe estar disponible para coordinar y realizar las verificaciones necesarias.

- **Configuraciones generales:** Se optimizarán las configuraciones VPN (IPSEC y SSL), eliminando túneles no utilizados y deshabilitando el "Web Mode" en los portales SSL para mejorar la seguridad. Además, se verificará la conectividad en todas las sedes, especialmente en las que presentan problemas. Se trabajará con el cliente para asegurar que las configuraciones VPN no afecten el acceso necesario para las operaciones diarias, especialmente para usuarios remotos.

Debido al posible impacto sobre la operación, estas labores deben realizarse en horarios no hábiles para evitar afectaciones en los servicios esenciales.

A continuación, se presenta una tabla que relaciona las actividades a ejecutar y los tiempos estimados para su desarrollo, conforme a lo identificado en el informe de infraestructura Fortinet:

- **FortiGate 1800F**

Para los dos (2) equipos **FortiGate 1800F**, se deben realizar las siguientes actividades, las cuales fueron identificadas en el informe de análisis de la infraestructura de seguridad Fortinet del IGAC:

Equipo	FortiGate 1800F	**Total días**
No. Equipos	2	24

Actividades para realizar		**Tiempo estimado (en días)**
FortiGate 1800F (2 equipos)	**Actualización Firmware**	**6**
	Generación de Backup del FortiGate 1800F	1
	Pruebas de funcionamiento Pre-Actualización	1
	Instalación del Firmware 7,4,9 en el FortiGate 1800F	1
	Validación de actualización en los dos clústeres.	1
	Revisión sincronización a nivel de HA	1
	Pruebas de funcionamientos Post-Actualización	1
	Políticas	**14**
	Revisión y análisis de políticas que no tienen consumo.	2
	Eliminar las políticas de las cuales se determine que no son útiles ni necesarias.	2
	Revisión y análisis de políticas con respecto a sus Perfiles de Seguridad	2
	Establecimiento de prioridad en el uso de perfiles de seguridad	2
	Revisión y análisis de políticas con Origen en ALL.	2
	Delimitación de políticas para permitir solo las IPs y/o redes autorizadas.	2
	Delimitación de políticas para permitir que solo se puedan alcanzar las IPs necesarias.	2
	Configuraciones generales	**4**
	Configuración y/o Eliminación de Objetos que ya no se usan	2
	Revisión y análisis de Conexiones VPN IPSEC	2

- **SDWAN FortiWiFi-61F y FortiGate-90G**

Para los doce (12) equipos **FortiWiFi-61F**, se deben realizar las siguientes actividades, las cuales fueron identificadas en el informe de análisis de la infraestructura de seguridad Fortinet del IGAC.

Equipo	FortiWiFi-61F	**Total días**
No. Equipos	12	10

Actividades para realizar		**Tiempo estimado (en días)**
FortiWiFi-61F (12 equipos)	**Actualización Firmware**	**4**
	Generación de Backup del FortiWiFi-61F	1
	Pruebas de funcionamiento Pre-Actualización	1
	Instalación del Firmware 7,4,9 en el FortiWifi 61	1
	Pruebas de funcionamientos Post-Actualización	1
	Configuraciones generales	**4**
	Ajuste de parámetros de acceso a la interfaz gráfica de administración FortiWiFi-61F	2
	Puertos de gestión	2
	Verificación de Conectividad	**2**
	Validar la conectividad de los equipos a través de la red MPLS y VPN	1
	Verificar la conexión con el proveedor de servicios de Internet (ISP)	1

Para los dos (2) equipos **FortiGate-90G**, se deben realizar las siguientes actividades, las cuales fueron identificadas en el informe de análisis de la infraestructura de seguridad Fortinet del IGAC.

Equipo	FortiGate-90G	Total días
No. Equipos	2	4

Actividades para realizar		Tiempo estimado (en días)
FortiGate-90G (2 equipos)	**Actualización Firmware**	**2**
	Generación de Backup del FortiWiFi-61F	1
	Pruebas de funcionamiento Pre-Actualización	1
	Instalación del Firmware 7,4,9 en el FortiWifi 61F	1
	Pruebas de funcionamientos Post-Actualización	1
	Configuraciones generales	**1**
	Ajuste de parámetros de acceso a la interfaz gráfica de administración	1
	Puertos de gestión	1
	Verificación de Conectividad	**1**
	Validar la conectividad de los equipos a través de la red MPLS y VPN	1
	Verificar la conexión con el proveedor de servicios de Internet (ISP)	1

Considerando la totalidad de los equipos SDWAN, que incluyen doce (12) dispositivos FortiWiFi-61F, dos (2) dispositivos FortiGate-90G y dos (2) dispositivos FortiGate-1800F, se propone llevar a cabo las actividades necesarias en un plazo de 8 semanas, según lo detallado en el siguiente cronograma general.

Ejecución de Assesment IGAC	Sem 1	Sem 2	Sem 3	Sem 4	Sem 5	Sem 6	Sem 7	Sem 8
FortiGate 1800F								
FortiGate 1800F								
FortiWiFi-61F-Armenia								
FortiWiFi-61F-Neiva								
FortiWiFi-61F-Barranquilla								
FortiWiFi-61F-Manizales								
FortiWiFi-61F-Pereira								
FortiWiFi-61F-SantaMarta								

FortiWiFi-61F-Cúcuta								
FortiWiFi-61F-Popayan								
FortiWiFi-61F-Monteria								
FortiWiFi-61F-Valledupar								
FortiWiFi-61F-Florencia								
FortiWiFi-61F-Bucaramanga								
FortiGate-90G-Cali								
FortiGate-90G-Villavicencio								

De acuerdo con las descripciones anteriores, cada una de estas actividades es crucial para garantizar que la infraestructura Fortinet se mantenga segura, actualizada y funcionando correctamente. Por lo tanto, es necesario coordinar estas actividades con las sedes, asegurando la disponibilidad de recursos, la cual será esencial para validar y aprobar los cambios en tiempo real. Esto permitirá una implementación exitosa y sin interrupciones significativas en los servicios.

En consecuencia, en mi calidad de representante legal de la **UT HC-WX SEGURIDAD 2025**, identificada con **NIT 902.009.528 - 1**, me permito solicitar respetuosamente una prórroga en el tiempo de ejecución del contrato No. **35177 de 2025**, con el fin de garantizar el cumplimiento de las obligaciones aquí descritas. Se solicita que el plazo se amplie por **dos meses, apartir de la reanudación del contrato**.

Agradecemos su atención. Quedamos atentos a su validación del plan de acción y del cronograma propuesto, a fin de continuar con la ejecución y cierre de los entregables conforme a lo requerido por la Entidad.

A continuación, se incluyen los siguientes anexos que complementan la información solicitada:

Listado de Anexos:

- Anexo 1 - Ficha técnica oficial del fabricante Fortinet (Datasheet)
- Anexo 2 - Ciclo de vida del producto
- Anexo 3 - Ficha técnica 2026
- Anexo 4 - Carta del fabricante
- Anexo 5 - Pruebas de laboratorio
- Anexo 6 - Informe de análisis FortiAnalyzer 400E
- Anexo 7 - Informe de análisis FortiGate

Cordialmente

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