UNIÓN TEMPORAL **UT HC-WX SEGURIDAD 2025**

Heimcore | WEXLER

ASSESSMENT
INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI



INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI
ASSESSMENT INFRAESTRUCTURA FORTINET

ASSESSMENT
INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI

Tabla de Contenido

1. INTRODUCCIÓN 3
2. ALCANCE 3
3. DISPOSITIVOS PARA ACTUALIZAR Y AFINAR 3
4. EVALUACIÓN PRELIMINAR DE CONFIGURACIONES A REALIZAR 3
4.1 ANALISIS DISPOSITIVO FORTIANALYZER 4

1. INTRODUCCIÓN

La información es uno de los activos más importantes por su alto impacto y valor, para la entidad IGAC, por esto, es necesario contar con aliados de negocios que permitan mantener un nivel de seguridad, a través del desarrollo de proyectos que propicien una transformación digital cibersegura. Con el fin de socializar los avances relacionados, se presenta este informe, que tiene como propósito mostrar el plan de Afinamiento a realizar para el servicio de seguridad de los dispositivos Fortinet en el cual, se presentan actividades de configuraciones a ejecutar.

2. ALCANCE

Optimizar y fortalecer la configuración de seguridad de la plataforma FortiAnalyzer mediante la revisión, configuración y actualización exhaustiva del equipo actual FAZ 400E, garantizando una protección eficaz contra amenazas cibernéticas y asegurando un rendimiento óptimo de la red.

3. DISPOSITIVOS PARA ACTUALIZAR Y AFINAR

El presente documento es de carácter informativo y tiene como finalidad identificar el estado actual de los dispositivos Fortinet de la entidad. Para dar cumplimiento al contrato, se llevarán a cabo los ajustes sugeridos en conjunto con el equipo de TI de la IGAC, cuyas actividades serán incluidas en un plan de trabajo que será enviado de manera oportuna.

En la ilustracion1, se presentan los equipos a los que se les realizará actualización y afinamiento:

Equipo o Plataforma	Ubicación	Vencimiento
FortiAnalyzer 400E	Sede Principal	27/11/2025

Ilustración - Equipos para actualizar y afinar

4. EVALUACIÓN PRELIMINAR DE CONFIGURACIONES A REALIZAR

Esta fase implica un examen detallado y metódico de las configuraciones actuales, destinado a identificar áreas de mejora, adecuaciones necesarias y oportunidades de optimización. Es un paso esencial para garantizar que las implementaciones futuras sean coherentes, efectivas y alineadas con las necesidades de la organización.

4.1 ANALISIS DISPOSITIVO FORTIANALYZER

Información general del sistema

En la sección de System Information se identifican los siguientes datos relevantes del equipo:

- Modelo: FortiAnalyzer 400E
- Modo de operación (HA Status): Standalone
- Versión de firmware: v7.4.7, build 2685 (Mature)
- Tiempo de operación (Uptime): 185 días, 15 horas, sin reinicios recientes
- Último respaldo de configuración: 26 de enero de 2026
- Hora del sistema: Correctamente sincronizada al momento de la revisión
- Operación: Analyzer
- Alta Disponibilidad: Standaalone

La versión de firmware instalada corresponde a una versión estable (Mature), lo cual es adecuado desde el punto de vista de estabilidad. Sin embargo, se recomienda validar compatibilidad con versiones actuales de FortiOS y mejores prácticas vigentes durante el proceso de afinamiento.

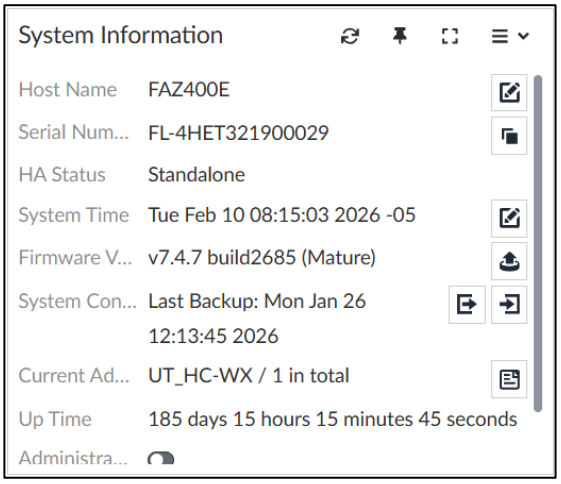


Ilustración – Información del sistema

Estado de recursos del sistema

De acuerdo con la revisión del panel de System Resources, el equipo FortiAnalyzer 400E presenta los siguientes niveles de utilización:

- Uso promedio de CPU: 85% Este valor se considera elevado y sostenido, lo que puede impactar el desempeño general del sistema, especialmente en procesos de correlación, generación de reportes y consultas de logs. Este comportamiento sugiere la necesidad de un afinamiento de cargas, revisión de tareas programadas y volúmenes de registros procesados.
- Uso de memoria: 36% El consumo de memoria se encuentra dentro de rangos normales y no evidencia, al momento de la revisión, una condición de saturación o presión sobre este recurso.
- Uso de disco: 41% La utilización del almacenamiento es adecuada, con capacidad disponible suficiente para la retención de logs. No obstante, se recomienda validar las políticas de retención y rotación como parte del proceso de optimización.

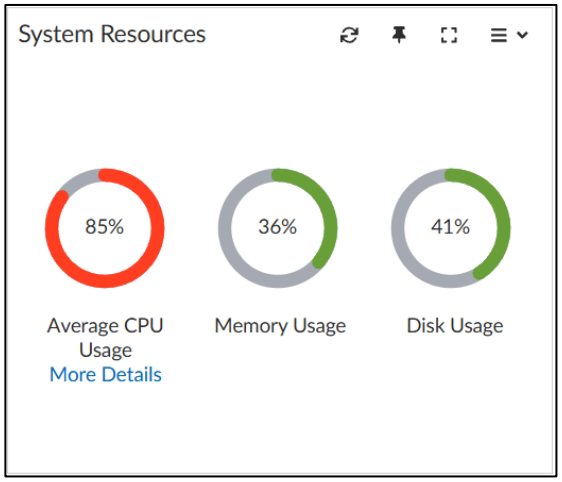


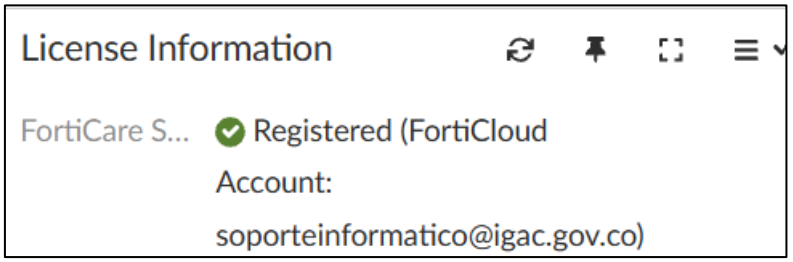
Ilustración – Recursos del sistema

Estado de licenciamiento

Se identifica que la licencia del FortiAnalyzer se encuentra vencida desde noviembre de 2025. Esta condición puede limitar funcionalidades clave, tales como:

- Actualizaciones de firmware y parches de seguridad
- Soporte técnico del fabricante
- Acceso a capacidades avanzadas de análisis y reportes

Se recomienda regularizar el licenciamiento como parte prioritaria del proceso de optimización, con el fin de garantizar el soporte, la seguridad y el correcto funcionamiento de la plataforma.



Account ID	soporteinformatico@igac.gov.co
Company	INSTITUTO GEOGRAFICO AGUSTIN CODAZZI - IGAC (Named/G/ELZ)
Hardware	Expired (Expires 2025-11-27)
Enhanced Support	Expired (Expires 2025-11-27)

Ilustración – Licencia del sistema

ADOMS

Durante la revisión de la configuración del FortiAnalyzer 400E, se constató que el sistema cuenta con un único ADOM activo, correspondiente al ADOM root, el cual se encuentra configurado como tipo Fabric.

El ADOM root tiene asignado un volumen de almacenamiento de 4 TB, destinado a la recepción y retención de registros (logs) de los dispositivos integrados. Actualmente, el FortiAnalyzer gestiona tres (3) dispositivos, los cuales corresponden a tres VDOMs, todos asociados al mismo ADOM.

No se identificaron ADOMs adicionales ni dispositivos de otros tipos registrados en la plataforma, lo que indica una estructura simplificada y centralizada de administración y análisis de eventos.

Name	ADOM Type	Allocated Storage	Devices
Security Fabric (1)			
root	Fabric	4 TB	3 Devices (including 3 VDOMs) >
FortiGates (0)			
Other Device Types (0)			

Ilustración – ADOMs del sistema

ADMINISTRADORES

- Se evidencian los siguientes usuarios administradores con acceso al dispositivo Fortianalyzer y perfil Super_User, en ese sentido, se sugiere validar si corresponden con los usuarios autorizados para el ingreso al sistema.

Name	Type	Profile	ADOMs	Trusted IPv4 Hosts
System Administrator (5)				
admin	LOCAL	Super_User	All ADOMs	0.0.0.0/0.0.0.0
daniel.dussan	LDAP	Super_User	All ADOMs	0.0.0.0/0.0.0.0
juan.tellez	LDAP	Super_User	All ADOMs	0.0.0.0/0.0.0.0
admin2	LOCAL	Super_User	All ADOMs	0.0.0.0/0.0.0.0
UT_HC-WX	LOCAL	Super_User	All ADOMs	0.0.0.0/0.0.0.0

Ilustración - Usuarios Administradores

AUTENTICACIÓN REMOTA – LDAP

El equipo cuenta con un servidor de autenticación remota configurado bajo el protocolo LDAP (Lightweight Directory Access Protocol), identificado como "SERVER_LDAP". Esta configuración permite centralizar la gestión de accesos utilizando las credenciales existentes en el Directorio Activo de la organización.

Name	Type	ADOM	Details
SERVER_LDAP	LDAP	FortiWeb, root	172.19.0.11:3268/sAMAccountName: DC=dcigac,DC=local

Ilustración – Configuración de protocolo LDAP

RAID MANAGEMENT

El sistema FortiAnalyzer 400E opera actualmente bajo un esquema de almacenamiento RAID-10, compuesto por cuatro unidades físicas de 2.8 TB cada una. Esta configuración proporciona un balance óptimo entre redundancia de datos y velocidad de escritura/lectura, fundamental para el procesamiento de logs de alto volumen. A la fecha, el equipo dispone de un 59% de espacio libre, lo que indica una capacidad saludable para la operación inmediata, aunque supeditada a la correcta gestión de cuotas de los dispositivos vinculados.

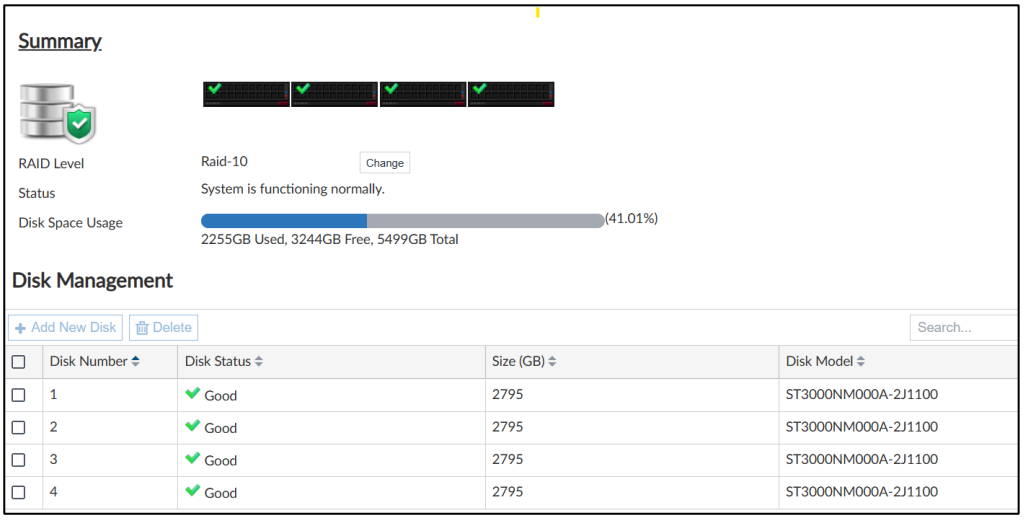


Ilustración – Arreglo de discos

MAIL SETTINGS

Actualmente, el FortiAnalyzer no dispone de un perfil de servidor SMTP configurado (No record found). Esta carencia técnica limita significativamente las capacidades de notificación y entrega automatizada de la plataforma.

En ese sentido, se sugiere habilitar un servidor de correo seguro para el envío de notificaciones de manera automática, como por ejemplo los Reportes.

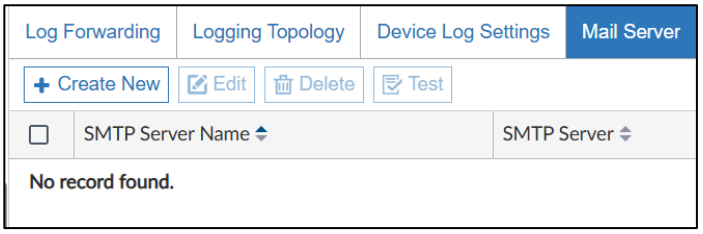


Ilustración – Configuración mail server

SMTP

Se evidencia que actualmente no existe en servidor SMTP configurado, se recomienda configurar el servidor para el monitoreo del Fortianalyzer a nivel de red y disponiblidad.



Ilustración - Servicio SNMP

ADMINISTRACIÓN DE DISPOSITIVOS

El estado actual del inventario de dispositivos en el FortiAnalyzer 400E muestra una discrepancia significativa entre los equipos gestionados y las solicitudes de conexión entrantes:

- Dispositivos Autorizados: Se evidencian únicamente 3 dispositivos configurados e integrados dentro de la plataforma.
- Dispositivos No Autorizados: Se identifican 26 dispositivos en estado "Unauthorized". Estos corresponden a equipos que están intentando enviar logs al FortiAnalyzer pero que no han sido admitidos formalmente en la base de datos de administración.

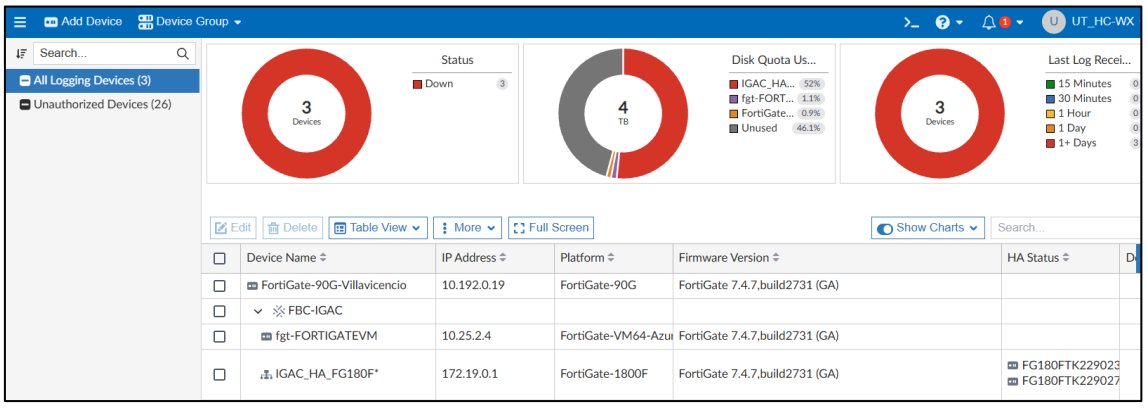


Ilustración - Administración de dispositivos

REPORTES

A nivel de reportes, se evidenció la existencia de reportes específicos actualmente configurados en el FortiAnalyzer, los cuales generan información detallada sobre los eventos y actividades de los dispositivos integrados. No obstante, el contenido, alcance y periodicidad de dichos reportes requieren ser analizados y validados directamente por la entidad, con el fin de determinar si la

información presentada se encuentra alineada con las necesidades operativas, de seguridad y de gestión.

Este análisis permitirá definir qué métricas, indicadores y niveles de detalle aportan valor real para la toma de decisiones, así como identificar oportunidades de ajuste, personalización o consolidación de reportes, optimizando su utilidad y reduciendo la generación de información innecesaria.

Heimcore				
Informe de Ciberseguridad	Spanish		Previous Month	All Devices
Informe Periódico de Servicio	Spanish		Previous Month	All Devices
Reporte de Politicas por destino y puertos	English		Previous Month	IGAC_HA_FG180F
Reporte de Politicas por origen destino y puertos	English		Previous 30 Days	fgt-FORTIGATEVM

Ilustración - Configuración de reportes

RECOMENDACIONES Y CONCLUSIONES

- La versión de firmware instalada corresponde a una versión estable (Mature), lo cual es adecuado desde el punto de vista de estabilidad. Sin embargo, se recomienda validar constantemente nuevas versiones FortiOS liberadas por parte del fabricante.
- Se sugiere validar constantemente el consumo de recursos como Memoria, CPU y Disco, ya que al momento de la revisión el FAZ 400E, presentaba alto consumo de Memoria y Disco.
- Se recomienda regularizar el licenciamiento como parte prioritaria del proceso de optimización, con el fin de garantizar el soporte, la seguridad y el correcto funcionamiento de la plataforma.
- Se recomienda validar la configuración de nuevos ADOMs que permita segmentar el registro de Logs de plataformas diferentes a firewall Fortigate.
- Con respecto a los usuarios Administradores, se sugiere validar regularmente los usuarios adminstradores de la plataforma con el objetivo de garantizar el acceso sólo al personal autorizado.
- Se sugiere asegurar el acceso de usuarios administradores con trust host.
- Se recomienda la configuración de un perfil SMTP para garantizar el envío de reportes vía correo electrónico.
- Se sugiere realizar el monitoreo de la plataforma FortiAnalyzer a través de un perfil SNMP en caso de contar con una herramienta de monitoreo NOC.