CORPOURABA
CONSECUTIVO: 300-34-01.59-5933
Fecha: 02-09-2026 Hora: 10:29 AM Folios:None

ESTRUCTURA INFORME CORPOURABA

Período de análisis: 19.07.2026 a el 18.08.2026

Diccionario de terminología:

PUA: Potential Unwanted Application, Aplicación potencialmente no deseada

Heartbeat: Es la forma en la que las máquinas hacen un chequeo en el que validan sin el dispositivo remoto aún se encuentra operando o “VIVO”

Endpoint: Software de cliente final que se instala en las máquinas de los usuarios

Firewall: Dispositivo de red capaz de realizar inspección profunda de paquetes IP

Sophos central: Sistema de gestión sophos centralizado

Zero trust: tendencia filosófica en Ciberseguridad en la que no se confía en ningún dispositivo de red

Web filtering: Filtrado Web, práctica en la que se bloquean sitios web no deseados en tráfico corporativo de una organización

VLAN: Virtual LAN (Local Area Network) red de área local

RSTP: Rapid Spanning Tree Protocol, protocolo que evita los bucles a nivel de capa 2

WPA: WI-FI protected Access acceso protegido por contraseña

IoC (Indicators Of Comprimise) Un indicador de Compromiso es una posible amenaza contra el sistema.

I/O: Entradas y salidas.

***Logs**: registros*

***UPTIME**: tiempo de actividad*

Eavesdropping*: interceptación no autorizada de comunicaciones privadas, ya sean conversaciones de voz o tráfico de datos digitales.*

Guest Time: cantidad de tiempo que el procesador dedica a ejecutar código dentro de una máquina virtual **.**

Botnets: cantidad de dispositivos conectados a internet (como computadoras, teléfonos o aparatos inteligentes) que han sido infectados con un *software* malicioso o realizar una tarea específica.

***High memory utilization**: Alto consumo de memoria.*

ELEMENTOS DE RED

1.1. Identificación de riesgos del cableado estructurado

1.1.1. Cumplir con el programa periódico de revisiones de elementos de red, elaborado desde el área de TI, visitas periódicas y reportes de usuarios, etc., con el fin de Identificar, reportar y/o reparar, de ser el caso, daños que afecten el flujo de datos en la red, tales como cortes en el cableado, daños en conectores UTP, Patch cords, Jack, path panel, switches, enrutadores, etc.

Durante el periodo del 19 de julio al 18 de agosto del 2026, las capas de conmutación y enrutamiento de la red central registraron un desempeño impecable, alcanzando una **disponibilidad del 100%** y manteniéndose completamente libres de incidentes e interrupciones de gravedad.

El factor determinante para este resultado fue la implementación de un **esquema de monitoreo híbrido**. Esta estrategia no solo permitió supervisar la infraestructura en tiempo real, sino que facultó al sistema para anticipar y neutralizar anomalías en la transmisión de datos antes de que impactaran la operación. Gracias a esta capacidad proactiva, las desviaciones menores de rendimiento fueron corregidas de manera automatizada e inmediata.

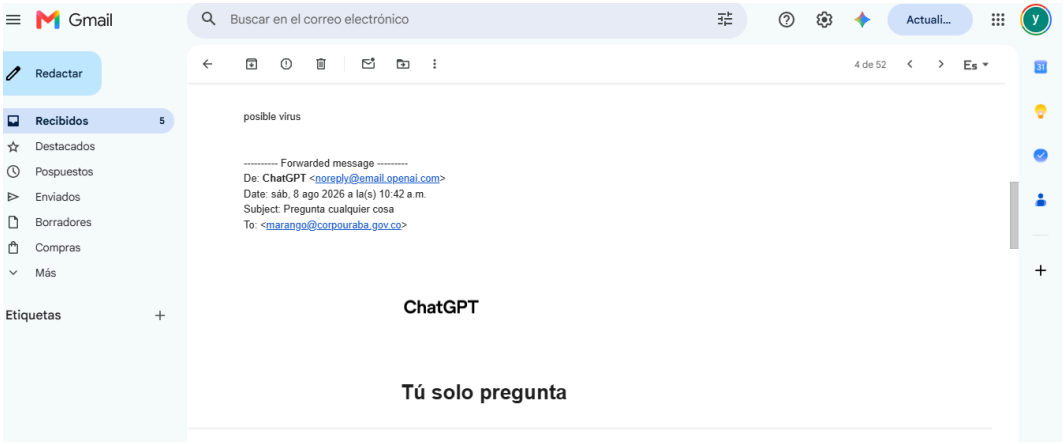
La ausencia total de fallas repetitivas demuestra la madurez alcanzada por la infraestructura, la cual opera actualmente bajo parámetros óptimos de eficiencia y seguridad. En conclusión, contamos con un ecosistema digital robusto y altamente resiliente

que garantiza la continuidad del negocio y brinda a la organización un entorno de trabajo confiable, respaldado por un soporte técnico de primer nivel.

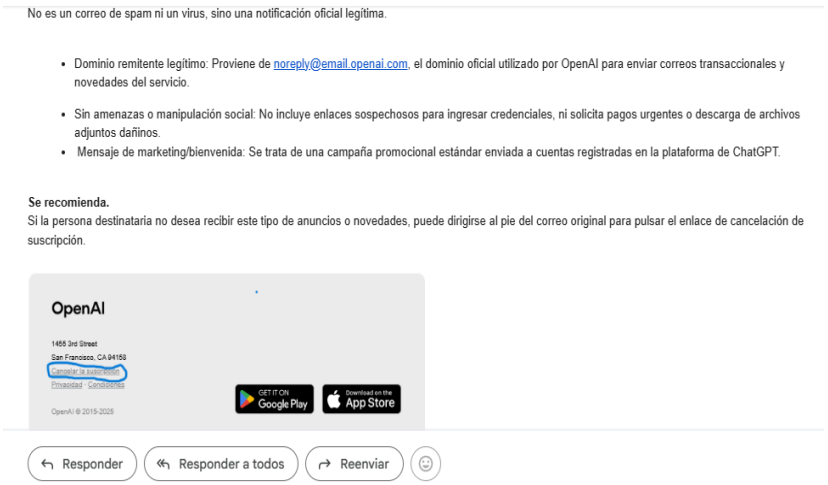
1.1.2. Coordinar con el oficial de seguridad la presentación de reportes ante incidentes de seguridad graves o muy graves al CSRIT.

Coordinación con el oficial de seguridad para el reporte de incidentes ante el CSIRT.

Entre el 19 de julio al 18 de agosto del 2026, nuestra plataforma tecnológica operó con total normalidad y máxima protección. Gracias a la gestión preventiva, no se reportaron eventos de seguridad ni amenazas graves, pero sí se presentaron alertas, 1 por email .



Pero se identificó que no es un correo de spam ni un virus, sino una notificación oficial legítima. se le dio respuesta al remitente y se le recomendó hacer la **cancelación de la suscripción.**


No es un correo de spam ni un virus, sino una notificación oficial legítima.

- Dominio remitente legítimo: Proviene de noreply@email.openai.com, el dominio oficial utilizado por OpenAI para enviar correos transaccionales y novedades del servicio.
- Sin amenazas o manipulación social: No incluye enlaces sospechosos para ingresar credenciales, ni solicita pagos urgentes o descarga de archivos adjuntos dañinos.
- Mensaje de marketing/bienvenida: Se trata de una campaña promocional estándar enviada a cuentas registradas en la plataforma de ChatGPT.

Se recomienda.
Si la persona destinataria no desea recibir este tipo de anuncios o novedades, puede dirigirse al pie del correo original para pulsar el enlace de cancelación de suscripción.

Adicionalmente ya se iniciará con la implementación de una **campaña de ciberseguridad** para capacitar a los funcionarios en la detección de correos maliciosos.

el primer paso a seguir es la sensibilización con la siguiente imagen



1.2. Propuestas de mejoras en el cableado estructurado

1.2.1. Generar informes mensuales para identificar y reportar riesgos para el cableado y/o los equipos de cómputo por el uso de extensiones eléctricas, adecuaciones de infraestructura, arreglos eléctricos, goteras o inundaciones, etc.

Durante el periodo del 19 de julio al 18 de agosto del 2026, la rápida expansión de la plataforma tecnológica ha desbordado los límites operativos de la infraestructura física actual, creando estrangulamientos en la red que restringen el rendimiento institucional.

Congestión e inestabilidad en la Red de Datos El cableado estructurado ha alcanzado un nivel de saturación severo. El recurso continuo a soluciones improvisadas y puentes temporales para integrar el nuevo equipamiento ha mermado la calidad de las señales, afectando directamente la constancia y velocidad de los servicios de datos.

Exposición a Fallas y Riesgos Eléctricos La insuficiencia de puntos de contacto eléctrico ha masificado el uso de adaptadores y extensiones. Esta condición expone a las instalaciones a contingencias graves como sobrecargas o incendios, poniendo en riesgo directo el material informático, el flujo continuo de las operaciones y la custodia de los datos estratégicos.

Con el objetivo de eliminar estos riesgos desde su origen y garantizar el cumplimiento de estándares normativos, se plantean los siguientes compromisos técnicos:

Sustitución e Integración de Red: Retirar por completo las conexiones improvisadas e instalar un esquema de cableado estructurado, continuo y respaldado por certificaciones técnicas.

Redistribución Energética: Desarrollar un plan de balance de carga eléctrica ajustado a los niveles reales de demanda y volumen de dispositivos por área.

Alineación Normativa y Regulatoria: Modernizar las redes de potencia y conectividad en estricto apego a las directrices de seguridad industrial, protección civil y previsión de crecimiento futuro.

Atender estas restricciones físicas no representa una simple actualización de sistemas; se trata de una **estrategia de gestión de riesgos indispensable** para resguardar la operatividad, blindar el patrimonio tecnológico y asegurar el desarrollo sin interrupciones de la organización.

1.2.2. Acompañar en el cumplimiento del plan para la transición de IPv4 a IPv6

Durante el periodo evaluado del 19 de julio al 18 de agosto de 2026, Corpourabá determinó mantener la operación de su

infraestructura bajo el protocolo IPv4. Esta postura obedece a un análisis de costo-beneficio enfocado en la estabilidad operativa y la mitigación de riesgos, considerando que la arquitectura presente satisface totalmente los requerimientos tecnológicos de la entidad y no existen exigencias regulatorias inmediatas para una migración obligatoria.

Optimización de Recursos: Diferir la adopción de IPv6 permite canalizar el presupuesto y las capacidades del equipo técnico hacia iniciativas de mayor impacto inmediato, como el fortalecimiento de la ciberseguridad y la mejora continua de los servicios de atención ciudadana.

Reducción de Riesgos Operativos: Se evitan eventuales caídas del servicio o fallos de interoperabilidad derivados de configuraciones apresuradas, garantizando la continuidad del negocio en un entorno estable.

Alineación Normativa Continua: La organización mantiene un seguimiento constante de los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), asegurando que la eventual transición hacia IPv6 se realice de manera programada, gradual y segura cuando la regulación o el crecimiento de la red así lo exijan.

El uso continuado de IPv4 constituye una decisión táctica prudente que resguarda la estabilidad operativa de la corporación sin comprometer la preparación futura para la evolución tecnológica del Estado.

1.3. Análisis de consumo de red por funcionarios y estabilidad del servicio

La gestión de la interfaz **ether4–WAN–TIGO** eleva la administración de red a un nivel de gobernanza estratégica mediante un modelo proactivo basado en datos. Al integrar la supervisión del consumo con políticas de Calidad de Servicio (QoS), la entidad blinda sus procesos críticos frente a fallas externas, optimiza el presupuesto al ajustar el ancho de banda contratado a la demanda real, asegura el cumplimiento de los acuerdos SLA y consolida una infraestructura tecnológica robusta para impulsar la transformación digital.

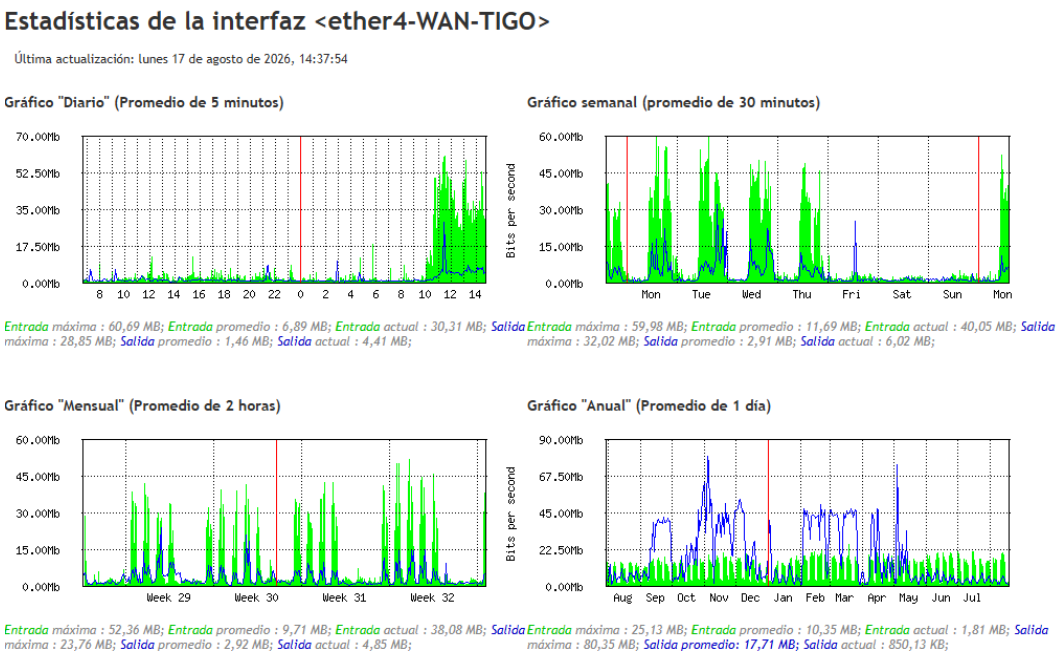


Gráfico "Diario" (Promedio de 5 minutos)

Tráfico de Entrada:
Máximo: 60,69 Mb/s
Promedio: 6,89 Mb/s
Actual: 30,31 Mb/s

Comportamiento: Mantiene niveles residuales/bajos (por debajo de 5 Mb/s) desde las 16:00 hasta aproximadamente las 10:00 del día siguiente. A partir de las 10:00 - 11:00 AM se observa un incremento vertical drástico, alcanzando picos que superan los 50 Mb/s y rozan los 60 Mb/s.

Tráfico de Salida:
Máximo: 28,85 Mb/s
Promedio: 1,46 Mb/s
Actual: 4,41 Mb/s

Comportamiento: Se mantiene estable y bajo casi todo el período, con un pico sutil coincidente con el inicio de la jornada laboral/operativa matutina.

Gráfico Semanal (Promedio de 30 minutos)

Tráfico de Entrada:
Máximo: 59,98 Mb/s

Promedio: 11,69 Mb/s
Actual: 40,05 Mb/s

Comportamiento: Presenta un patrón laboral sumamente marcado de lunes a jueves, con ráfagas recurrentes de tráfico que llegan a 45–60 Mb/s durante horas hábiles. Los días viernes, sábado y domingo el consumo cae radicalmente a niveles casi nulos, activándose el lunes.

Tráfico de Salida:
Máximo: 32,02 Mb/s
Promedio: 2,91 Mb/s
Actual: 6,02 Mb/s

Comportamiento: Acompaña los picos de descarga en días hábiles con valores moderados (5–15 Mb/s) y registra un evento puntual/aislado el día viernes sin demanda sostenida.

Gráfico "Mensual" (Promedio de 2 horas)

Tráfico de Entrada:
Máximo: 52,36 Mb/s
Promedio: 9,71 Mb/s
Actual: 38,08 Mb/s

Comportamiento: Refleja con claridad la regularidad de los ciclos semanales: 4 o 5 bloques intensos de actividad seguidos de valles correspondientes a fines de semana. Los picos máximos consolidados oscilan entre 30 Mb/s y 52 Mb/s.

Tráfico de Salida:
Máximo: 23,76 Mb/s
Promedio: 2,92 Mb/s
Actual: 4,85 Mb/s

Comportamiento: Sigue la misma simetría temporal del tráfico descendente, manteniéndose controlado por debajo de los 15–23 Mb/s en los momentos de mayor actividad.

Gráfico "Anual" (Promedio de 1 día)

Tráfico de Entrada:
Máximo: 25,13 Mb/s
Promedio: 10,35 Mb/s
Actual: 1,81 Mb/s

Comportamiento: Debido al promedio diario, las ráfagas se suavizan, mostrando un consumo base constante entre 10 Mb/s y 20 Mb/s sostenidos a lo largo de todo el año.

Tráfico de Salida:
Máximo: 80,35 Mb/s
Promedio: 17,71 Mb/s
Actual: 850,13 Kb/s

Comportamiento: Registra un comportamiento atípico en el periodo transcurrido entre octubre y mayo, donde el tráfico de salida (upload) superó históricamente al tráfico de entrada, alcanzando promedios diarios de hasta 80 Mb/s, patrón que disminuyó significativamente hacia la mitad del año actual.

Conclusión

El enlace opera predominantemente para descarga (Inbound), con picos de ~60 Mb/s en horarios de trabajo.
Existe una suspensión casi total del uso de ancho de banda durante noches y fines de semana.
La interfaz responde dentro de parámetros saludables para el perfil de consumo actual, con capacidad para procesar ráfagas de hasta 60 Mb/s sin saturación permanente.

1.3.1. Generar informe sobre los usuarios que consumen más GB en Internet y las páginas más visitadas

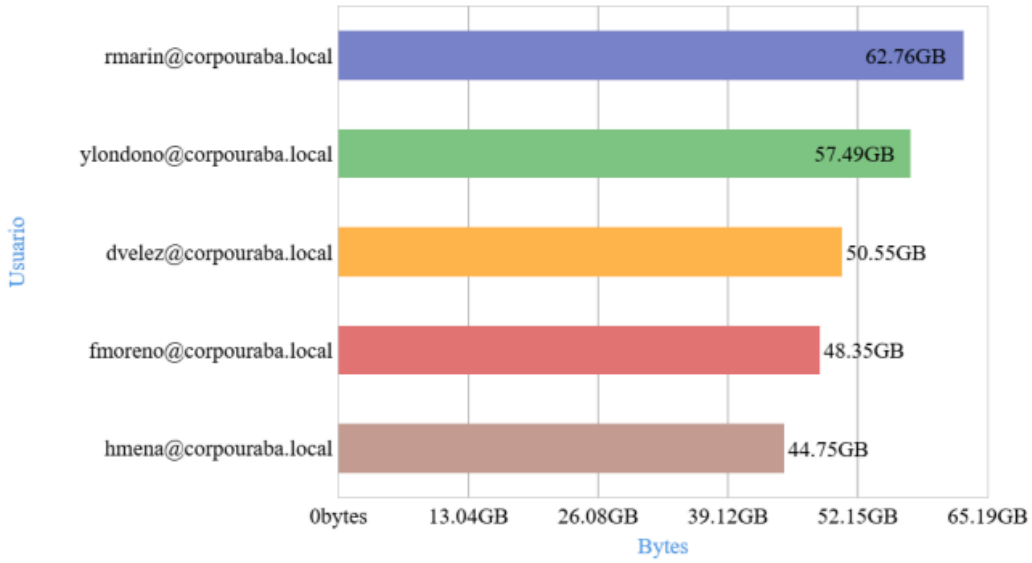
Durante el período comprendido entre el 19 de julio al 18 de agosto del 2026, el Firewall Sophos XGS2100 registró un tráfico total aproximado de 1,46 TB, de acuerdo con el informe oficial “Riesgos y uso de aplicaciones de usuarios”, generado directamente desde la plataforma de seguridad perimetral

https://drive.google.com/file/d/1ufP6jX8flp9WHjioyRi6p9F3Linxmn7h/view?usp=sharing

Usuarios con mayor consumo de datos

Durante el periodo del 19 de julio al 18 de agosto de 2026 se observa una concentración del tráfico en cuentas institucionales

determinadas, las cuales registran picos de consumo recurrentes vinculados a servicios en la nube o transferencia de datos. En contraste, el resto de los usuarios presenta un comportamiento de red equilibrado y estandarizado

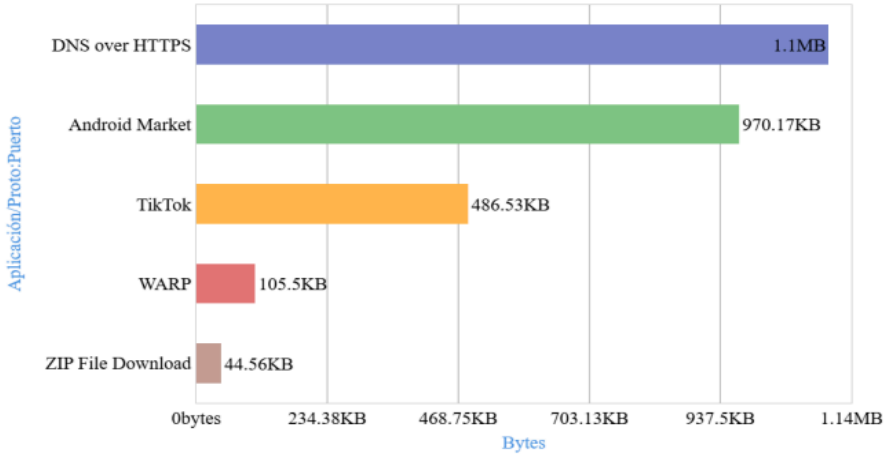


USUARIO	ÉXITOS	BYTES
rmarin@corpouraba.local	645651	62.76 GB
ylondono@corpouraba.local	182721	57.49 GB
dvelez@corpouraba.local	389476	50.55 GB
fmoreno@corpouraba.local	84606	48.35 GB
hmena@corpouraba.local	145073	44.75 GB

El gráfico de barras horizontales representa el consumo de almacenamiento en gigabytes (GB) de cinco usuarios del dominio `corpouraba.local`, mostrando una distribución decreciente donde el usuario `rmarin@corpouraba.local` encabeza la lista con el mayor consumo equivalente a 62.76 GB, seguido por `ylondono@corpouraba.local` con 57.49 GB, `dvelez@corpouraba.local` con 50.55 GB, `fmoreno@corpouraba.local` con 48.35 GB, y finalmente `hmena@corpouraba.local` con el menor uso registrado dentro del grupo, alcanzando 44.75 GB.

Aplicaciones y categorías con mayor consumo

Este gráfico de barras detalla el consumo de tráfico por **Aplicación/Protocolo:Puerto**, permitiendo identificar qué servicios específicos están utilizando el ancho de banda en este segmento. A diferencia de las gráficas anteriores de gigabytes (GB), aquí los valores son mínimos (**Megabytes y Kilobytes**)

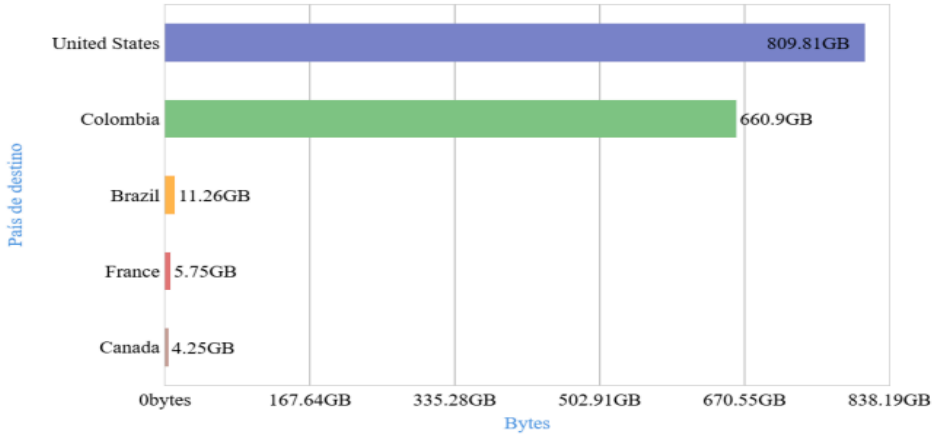


APLICACIÓN/PROTO:PUERTO	RIESGO	ÉXITOS	BYTES
DNS over HTTPS	5	907	1.1 MB
Android Market	4	1393	970.17 KB
TikTok	4	137	486.53 KB
WARP	5	122	105.5 KB
ZIP File Download	4	9	44.56 KB

El gráfico de barras horizontales ilustra el consumo de tráfico de red, clasificado por la categoría **Aplicación/Proto:Puerto**, donde **DNS over HTTPS** encabeza el volumen de transferencia con el mayor consumo **1.1 MB**, seguido de cerca por **Android Market** con **970.17 KB**; en una escala intermedia se ubica **TikTok** con **486.53 KB**, mientras que **WARP** y **ZIP File Download** representan los valores más reducidos con tan solo **105.5 KB** y **44.56 KB** respectivamente.

Destinos / páginas más visitadas

En cuanto a los destinos del tráfico, el informe evidencia que la mayor parte de las conexiones se dirigieron a servidores ubicados en los siguientes países:



PAÍS DE DESTINO	ÉXITOS	BYTES
United States	12392241	809.81 GB
Colombia	966819	660.9 GB
Brazil	41910	11.26 GB
France	28452	5.75 GB
Canada	7024	4.25 GB

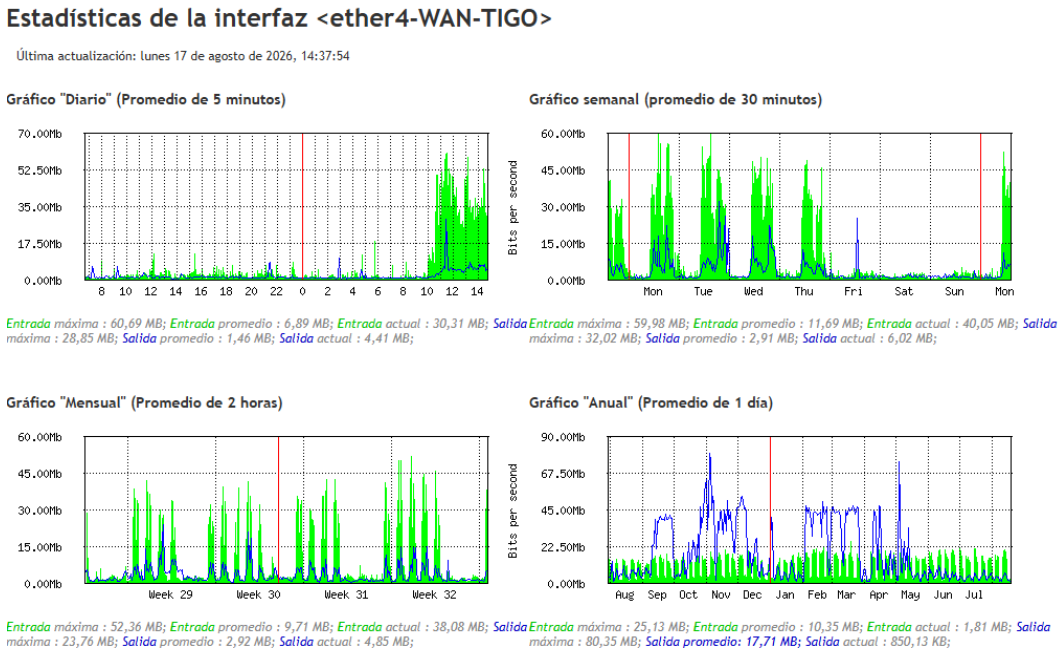
El gráfico muestra la distribución del tráfico de red saliente hacia diferentes países de destino. La gran mayoría del consumo se concentra en **United States**, que lidera el volumen con **809.81 GB**, seguido por **Colombia** con **660.9 GB**; en contraste, los demás países registran participaciones drásticamente menores, con **Brazil** en **11.26 GB**, **France** con **5.75 GB** y **Canada** al final del listado con **4.25 GB**. Este patrón de tráfico es propio de entornos corporativos actuales, donde el predominio de las conexiones hacia EE. UU. responde al uso continuo de servicios en la nube, herramientas de colaboración empresarial, soluciones de almacenamiento y plataformas de streaming alojadas en CDNs o servidores de esa región. En paralelo, el volumen hacia Colombia evidencia la interacción recurrente con portales y sistemas gubernamentales locales, mientras que los flujos menores hacia Europa y Latinoamérica suelen asociarse a actualizaciones automáticas o telemetría de sistemas.

Para optimizar el uso de la red y fortalecer la seguridad, es aconsejable establecer reglas de filtrado geográfico en el firewall que bloqueen conexiones no esenciales con países ajenos a la operación, garantizando así que el ancho de banda se destine de manera prioritaria a las actividades de la organización.

Ver anexo: Riesgos y uso de aplicaciones de usuarios_AGOSTO2026

1.3.2. Gráficos y análisis de los picos de consumo y caídas de internet en todas las sedes

Territorial Centro:



Análisis de tráfico – Interfaz ether4 (WAN – TIGO)

Durante el período comprendido entre el 19 de julio de 2026 y el 18 de agosto de 2026, se realizó el seguimiento y análisis del comportamiento del tráfico de red correspondiente a la interfaz ether4 – WAN – TIGO, la cual soporta la conectividad a Internet de la entidad.

Gráfica Diaria

El gráfico diario muestra un comportamiento de tráfico fuertemente concentrado en la jornada laboral diurna, donde la descarga registra un pico máximo de 60,69 Mb y la subida alcanza los 28,85 Mb, destacando una actividad intensa que se dispara a partir de las 10:00 y se extiende hasta pasadas las 14:00 horas con valores actuales de 30,31 Mb de entrada y 4,41 Mb de salida. En contraste, las horas de la madrugada y la noche muestran un tráfico plano e insignificante que apenas despega del eje cero con promedios de apenas 6,89 Mb en entrada y 1,46 Mb en salida, reflejando una inactividad casi total fuera del horario operativo.

Gráfica Semanal

La dinámica semanal confirma un patrón de consumo fuertemente acoplado a la semana laboral, con días de alto estrés de lunes a jueves donde la descarga registra picos de hasta 59,98 Mb y la subida alcanza los 32,02 Mb. A partir del viernes y extendiéndose a lo largo de todo el fin de semana, el tráfico cae a un nivel residual cercano a cero, registrando valores mínimos en ambos sentidos hasta la reactivación observada el lunes posterior con tráfico actual de 40,05 Mb de entrada y 6,02 Mb de salida.

Gráfica Mensual

En el comportamiento mensual, la red sostiene una periodicidad regular en forma de "peine" con valles marcados en los fines de semana y ráfagas verticales constantes de descarga durante los días laborables, alcanzando un pico máximo de entrada de 52,36 Mb con un promedio de 9,71 Mb. Por su parte, el tráfico de salida se mantiene significativamente más bajo y deprimido durante todo el mes, registrando un promedio de apenas 2,92 Mb y un pico puntual de 23,76 Mb, lo que evidencia un uso predominantemente orientado al consumo/descarga de datos.

Gráfica Anual

El histórico de los últimos doce meses evidencia un cambio de comportamiento drástico centrado entre los meses de septiembre y diciembre, periodo en el cual el canal registró una intensificación masiva del tráfico de subida con un pico absoluto de 80,35 Mb y un elevado promedio de 17,71 Mb. Este fenómeno de exportación de datos contrasta con el tráfico de entrada, que se mantuvo sumamente estable y acotado durante todo el año con un promedio

constante de 10,35 Mb y un límite máximo de 25,13 Mb, retornando a partir de mayo a un régimen de consumo moderado.

Territorial Caribe:

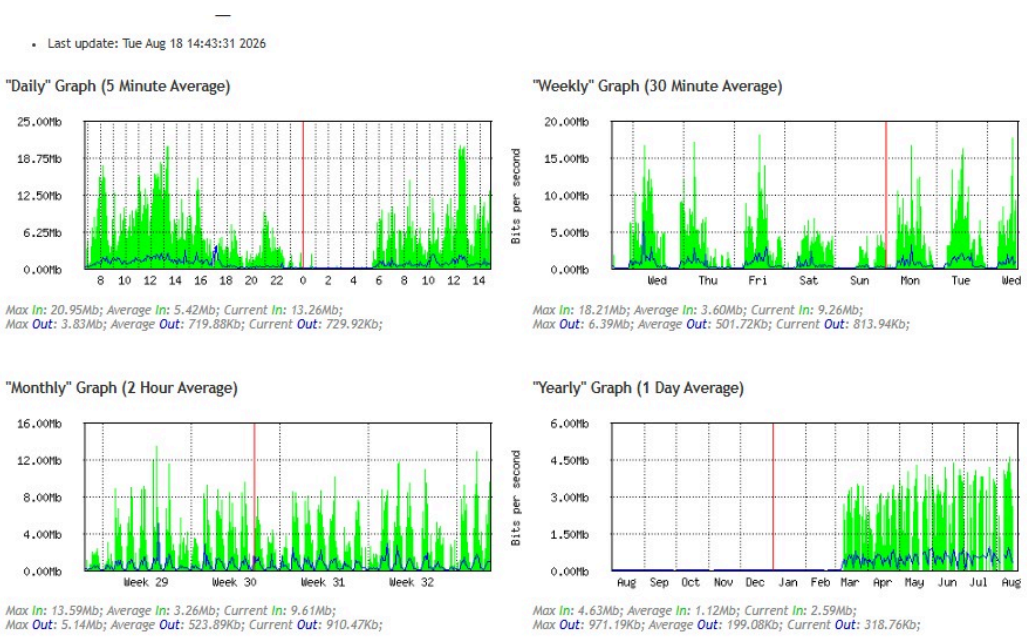


Gráfico Diario (5 Minutos)

El tráfico de entrada muestra un consumo enfocado en horario laboral con picos de hasta 20.95 Mb/s entre las 13:00 y las 14:00 horas, un promedio de 5.42 Mb/s y un nivel actual de 13.26 Mb/s, registrando una caída total del flujo entre las 00:00 y las 05:00 horas. Por su parte, el tráfico de salida permanece considerablemente más bajo y constante, con un máximo registrado de 3.83 Mb/s, un promedio de 719.88 Kb/s y una tasa actual de 729.92 Kb/s.

Gráfico Semanal (30 Minutos)

Esta vista refleja un comportamiento cíclico semanal con alta demanda de entrada en días hábiles (miércoles a viernes y lunes a martes) y un desplome drástico durante el fin de semana, alcanzando un máximo de 18.21 Mb/s, un promedio de 3.60 Mb/s y un valor actual de 9.26 Mb/s. El tráfico saliente acompaña esta

periodicidad laboral con picos máximos de 6.39 Mb/s, un promedio de 501.72 Kb/s y una lectura actual de 813.94 Kb/s.

Gráfico Mensual (2 Horas)

El análisis mensual evidencia la regularidad de las fluctuaciones de consumo semana a semana (semanas 29 a 32), con picos máximos de entrada que llegan a los 13.59 Mb/s, un promedio de 3.26 Mb/s y una tasa actual de 9.61 Mb/s. El flujo saliente mantiene una proporción asimétrica muy inferior a la carga de bajada, con un máximo registrado de 5.14 Mb/s, un promedio de 523.89 Kb/s y un nivel actual de 910.47 Kb/s.

Gráfico Anual (1 Día)

El registro anual indica una inactividad total del enlace desde agosto hasta mediados de febrero, momento en que el servicio se habilita e inicia un incremento sostenido de tráfico entrante con picos de 4.63 Mb/s, un promedio de 1.12 Mb/s y un estado actual de 2.59 Mb/s. La salida sigue el mismo patrón de puesta en marcha, con un máximo de 971.19 Kb/s, un promedio anual de 199.08 Kb/s y un nivel actual de 318.76 Kb/s.

Territorial Nutibara

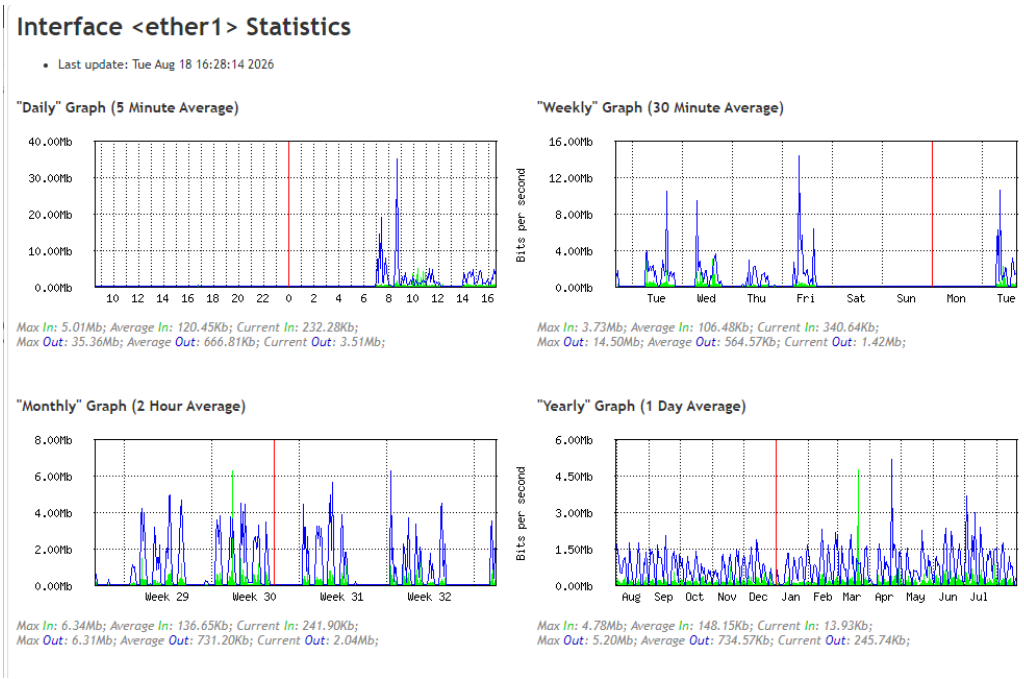


Gráfico Diario

El consumo diario muestra un periodo de inactividad total de 00:00 a 06:00 horas, seguido por un inicio brusco de actividad a las 07:00 que alcanza su pico máximo de subida de 35.36 Mb alrededor de las 08:00 horas, para luego estabilizarse en un flujo moderado de salida de aproximadamente 3.51 Mb durante la tarde, manteniendo la descarga en niveles muy bajos (máximo de 5.01 Mb y promedio de 120.45 Kb).

Gráfico Semanal

La actividad semanal se concentra de forma exclusiva durante los días laborales, registrando el volumen más alto el día viernes con un pico de subida de 14.50 Mb, mientras que el sábado y el domingo muestran consumo nulo, lo que confirma un patrón de tráfico estrictamente operativo o empresarial.

Gráfico Mensual

A lo largo de las semanas 29 a 32 se observa una clara regularidad cíclica compuesta por bloques de 5 días de consumo activo seguidos de 2 días de inactividad total, manteniendo un promedio constante de subida cercano a los 731.20 Kbps y alcanzando picos balanceados tanto de bajada (6.34 Mb) como de subida (6.31 Mb).

Gráfico Anual

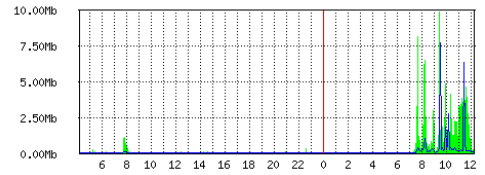
La tendencia anual refleja un comportamiento sumamente estable y predecible mes a mes, con un promedio de salida sostenido de 734.57 Kbps, destacándose únicamente dos eventos atípicos: un pico máximo de descarga de 4.78 Mb ocurrido en el mes de marzo y el pico anual más alto de subida registrado en abril con 5.20 Mb.

Territorial Urrao

Estadísticas de la interfaz <ether1>

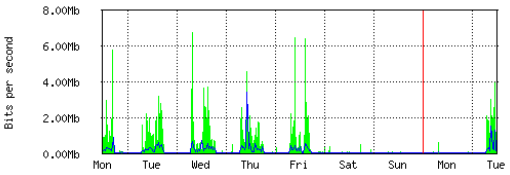
- Última actualización: martes 18 de agosto de 2026, 12:12:18

Gráfico "Diario" (Promedio de 5 minutos)



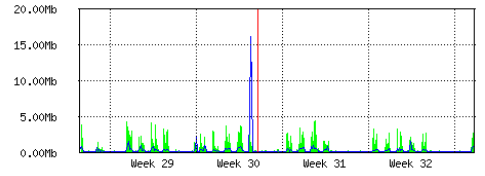
Entrada máxima : 9,92 MB; Entrada promedio : 351,38 KB; Entrada actual : 192,32 KB; Salida máxima : 7,72 MB; Salida promedio : 80,52 KB; Salida actual : 69,28 KB;

Gráfico semanal (promedio de 30 minutos)



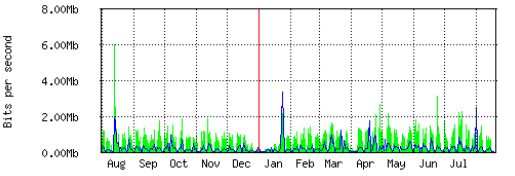
Entrada máxima : 6,76 MB; Entrada promedio : 463,00 KB; Entrada actual : 1,16 MB; Salida máxima : 3,42 MB; Salida promedio : 94,61 KB; Salida actual : 110,47 KB;

Gráfico "Mensual" (Promedio de 2 horas)



Entrada máxima : 4,39 MB; Entrada promedio : 581,90 KB; Entrada actual : 2,63 MB; Salida máxima : 16,26 MB; Salida promedio : 195,84 KB; Salida actual : 654,64 KB;

Gráfico "Anual" (Promedio de 1 día)



Entrada máxima : 6,00 MB; Entrada promedio : 671,29 KB; Entrada actual : 19,13 KB; Salida máxima : 3,37 MB; Salida promedio : 197,58 KB; Salida actual : 4,20 KB;

Gráfica Diaria

El tráfico diario de la interfaz muestra un comportamiento activo concentrado en las horas de la mañana, donde la descarga registra un pico máximo de 9,92 MB y la subida alcanza los 7,72 MB. A partir de las 8:00 hasta pasadas las 12:00 horas se observa el mayor nivel de ráfagas, registrando en el momento actual 192,32 KB de entrada y 69,28 KB de salida. Por el contrario, durante la tarde, noche y madrugada el tráfico se reduce a niveles prácticamente nulos, manteniendo un promedio bajo de 351,38 KB de entrada y 80,52 KB de salida.

Gráfica Semanal La dinámica semanal refleja un flujo fuertemente alineado con los días hábiles de la semana, observándose repuntes recurrentes con un pico máximo de descarga de 6,76 MB y de subida de 3,42 MB. En contraste, durante el fin de semana la gráfica muestra un comportamiento plano y residual cercano a cero. Para el día martes en curso, la interfaz presenta un tráfico reactivado con valores actuales de 1,16 MB de entrada y 110,47 KB de salida, con promedios semanales de 463,00 KB y 94,61 KB respectivamente.

Gráfica Mensual

Durante el último mes, la red ha mantenido un consumo predominantemente moderado y estructurado en los días laborales. Sin embargo, destaca un evento atípico registrado en la semana 30, donde el tráfico de subida experimentó un pico crítico de 16,26 MB, superando ampliamente a la descarga máxima del mes 4,39 MB de Entrada. Fuera de ese evento puntual, el canal se mantiene orientado al consumo regular con un promedio mensual de 581,90 KB de entrada y 195,84 KB de salida.

Gráfica Anual

El histórico anual revela un patrón operativo estable con ráfagas constantes de bajada que promedian 671,29 KB de entrada y un consumo máximo sostenido a lo largo de los meses. Destaca un pico inicial de descarga de 6,00 MB al principio del periodo, seguido por un evento puntual de subida a mediados de enero que alcanzó un máximo anual de 3,37 MB. Durante el resto del año, el tráfico se ha conservado controlado y acotado, registrando un promedio general de salida de 197,58 KB.

2. MONITOREO, SOPORTE Y ANÁLISIS DE RED

2.1. Reporte de instalación de nuevos elementos de Red y manejo del centro de datos.

No se reportó la instalación de elementos nuevos durante este periodo.

2.1.1. Instalar y/o configurar nuevos elementos de red tales como switches, routers, etc... (exceptuando nuevos puntos de red)

No se registraron instalaciones adicionales de elementos de red durante este periodo.

2.1.2. Coordinar el orden y limpieza del centro de datos y reportar oportunamente novedades con respecto a aires acondicionados o

equipos. Para ello deberá coordinar con el área de almacén acorde con lo documentado por el SGC.

Durante este período, no se realizaron tareas de limpieza.

3. SERVIDORES DE APLICACIONES

3.1. Administrar y gestionar los servidores físicos de aplicaciones

3.1.1. Garantizar su accesibilidad y continuidad. El soporte de las aplicaciones en su código fuente y funcionamiento deberá ser brindado por los proveedores de estas.

Entre el periodo del 19 de julio y el 18 de agosto de 2026, la infraestructura tecnológica operó de forma impecable y sin incidentes críticos. Este desempeño confirma la solidez de la red y la acertada gestión de recursos, garantizando la continuidad del negocio y una experiencia fluida para los usuarios al procesar todo el volumen transaccional sin contratiempos.

3.1.2. Diagnosticar el funcionamiento de los servidores y sus partes identificando posibles cambios en hardware o software que puedan afectar los servicios. Acompañar a los funcionarios de la corporación en las características de los equipos o partes a actualizar, e instalar los equipos o partes que se adquieran

A continuación, se detalla el estado actual, la utilización y las necesidades de los recursos de los servidores.

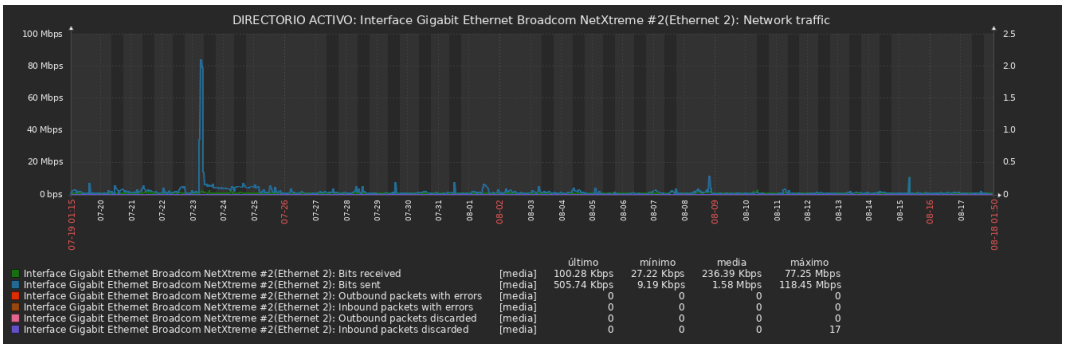
Recomendaciones:

Optimizar e incrementar la memoria RAM es clave para la estabilidad del servidor en picos de alta demanda. Al prevenir la saturación de memoria, se evitan caídas del servicio, se garantiza un procesamiento simultáneo eficiente y se asegura una experiencia continua para el usuario.

Directorio Activo

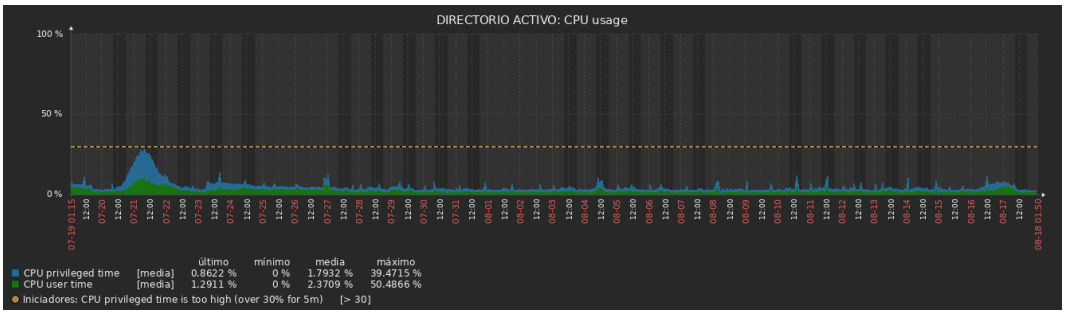


Refleja un estado operativo sumamente crítico en la unidad C:, al registrar un consumo de almacenamiento del 98.93%, 921.2 GB utilizados sobre un total de 931.14 GB. Esta saturación deja un margen libre insignificante de apenas 9.94 GB 1.07%, lo cual compromete de forma directa el rendimiento y la estabilidad del sistema al impedir la gestión adecuada de archivos temporales, memoria virtual y actualizaciones del sistema. Ante esta falta extrema de espacio, resulta indispensable realizar una intervención técnica inmediata —como la limpieza de archivos innecesarios, depuración de registros o ampliación de la capacidad de almacenamiento— para prevenir fallas en los servicios del directorio activo y evitar la corrupción de datos.

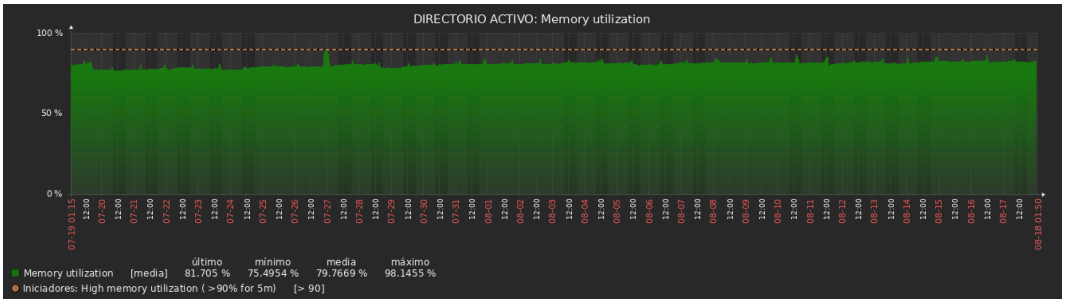


Muestra un comportamiento generalmente bajo y estable durante la mayor parte del periodo del 19 de julio al 18 de agosto, con un consumo promedio de **1.58 Mbps** para los datos enviados y **236.39 Kbps** para los recibidos . Sin embargo, destaca un pico atípico muy pronunciado registrado el **23 de julio**, donde el tráfico saliente alcanzó un máximo de **118.45 Mbps** (con 77.25 Mbps en recepción), además de algunos picos menores aislados a lo largo del mes. En cuanto a la salud y estabilidad del canal, no se

registran paquetes con errores ni descartados en la transmisión saliente o entrante manteniéndose en cero, a excepción de un valor puntual máximo de 17 paquetes descartados en entrada, lo que confirma un rendimiento de red limpio sin problemas de pérdida de paquetes.



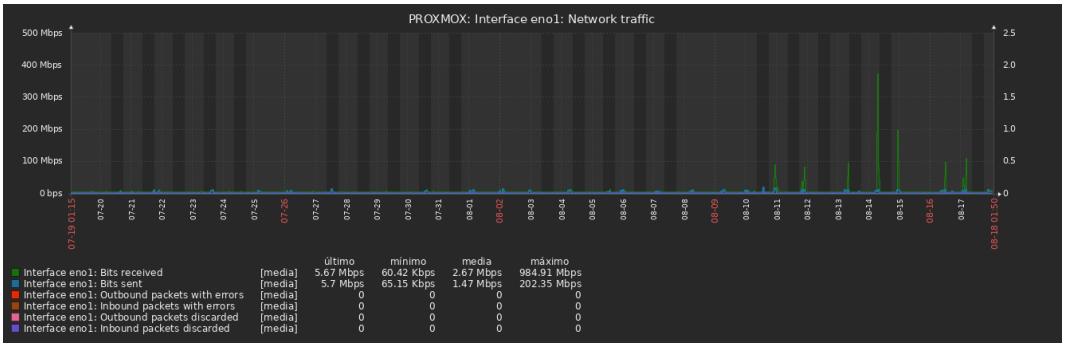
La CPU del servidor de Directorio Activo se mantiene en niveles significativamente bajos y estables durante la mayor parte del periodo de observación del 19 de julio al 18 de agosto, registrando promedios reducidos del **2.37%** en el tiempo de usuario y del **1.79%** en el tiempo privilegiado o de kernel. El único evento relevante ocurre entre el **21 y 22 de julio**, cuando la actividad aumenta sensiblemente hasta superar la línea de umbral del 30% asignada al tiempo privilegiado, alcanzando picos máximos del **50.49%** de uso de usuario y **39.47%** de uso privilegiado; fuera de esta elevación temporal y de leves repuntes muy puntuales, el servidor opera sin sobrecargas de procesamiento.



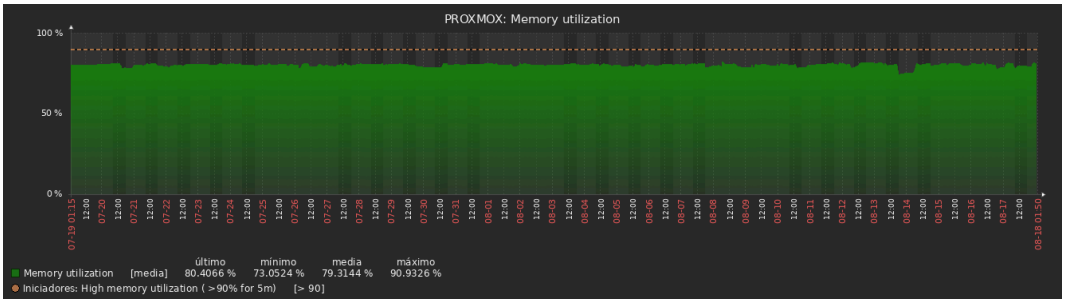
La memoria RAM en el servidor de Directorio Activo refleja un uso sostenido y constante, operando con un promedio elevado del **79.77%** y oscilando en su punto más bajo cerca del **75.50%** . A lo largo de todo el periodo, el consumo se mantiene de forma uniforme cerca del umbral de alerta del 90%, registrando únicamente un pico máximo puntual del **98.15%** alrededor del **27**

de julio donde sobrepasa dicha línea de advertencia antes de estabilizarse nuevamente en sus valores promedio habituales.

Proxmox



El gráfico del tráfico de red para la interfaz "eno1" en el servidor Proxmox muestra un comportamiento predominantemente bajo y estable a lo largo del mes, registrando un promedio de **2.67 Mbps** para los datos recibidos y **1.47 Mbps** para los enviados. No obstante, el tráfico de entrada presenta una actividad con picos muy pronunciados a partir del **11 de agosto**, alcanzando su punto máximo más alto alrededor del **14 de agosto** con **984.91 Mbps**, acompañado por un máximo de datos salientes de **202.35 Mbps**. A pesar de estas ráfagas intensas de transferencia, la red mantiene una estabilidad impecable al no registrar ningún paquete con errores ni descartado en la transmisión entrante o saliente. todos en cero.

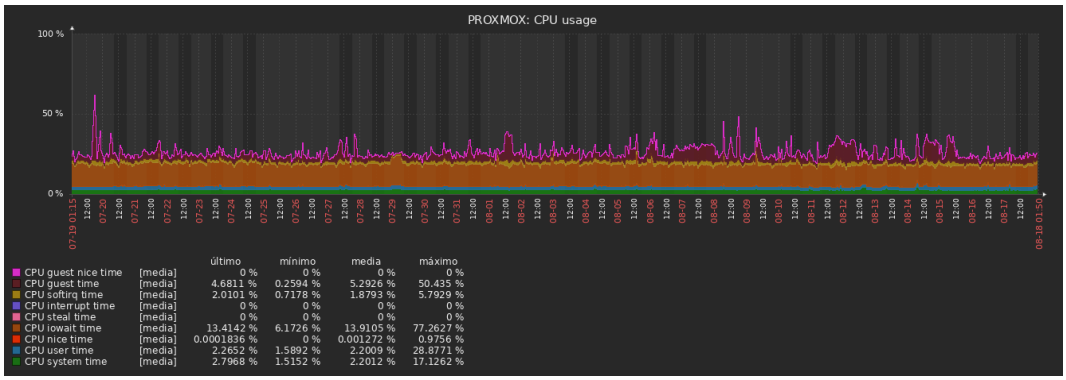


El gráfico refleja un uso sumamente estable y constante de la memoria RAM en el servidor Proxmox durante todo el periodo analizado 19 de julio al 18 de agosto, manteniendo un consumo promedio general del **79.31%** y fluctuando dentro de un rango bastante acotado con un mínimo del **73.05%**. A lo largo de todo el

mes, la utilización de memoria se ubica de forma continua cerca de la línea punteada de advertencia del 90%, registrando únicamente un pico máximo puntual del **90.93%** que superó levemente dicho umbral de alerta antes de retornar a sus niveles habituales.



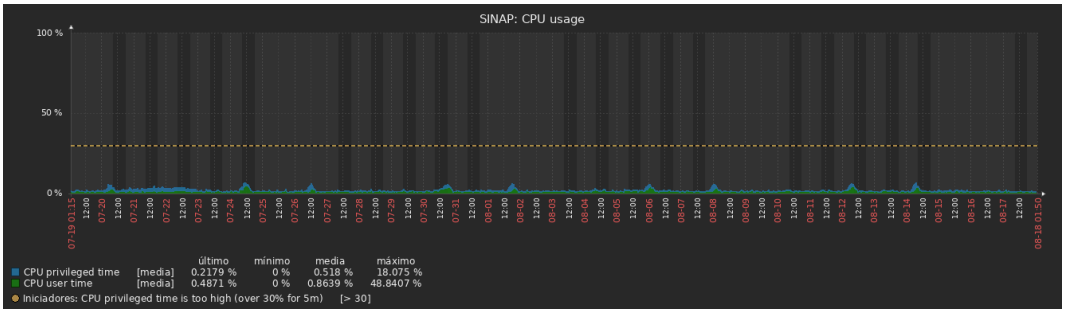
Muestra un estado de almacenamiento moderadamente comprometido pero bajo control del servidor Proxmox, indicando un espacio total disponible de 93.99 GB. De esta capacidad, el espacio ocupado asciende a 67.81 GB, lo que equivale a un 72.14% de utilización total, dejando un margen disponible aproximado del 27.86% 26.18 GB para el almacenamiento restante en el sistema.



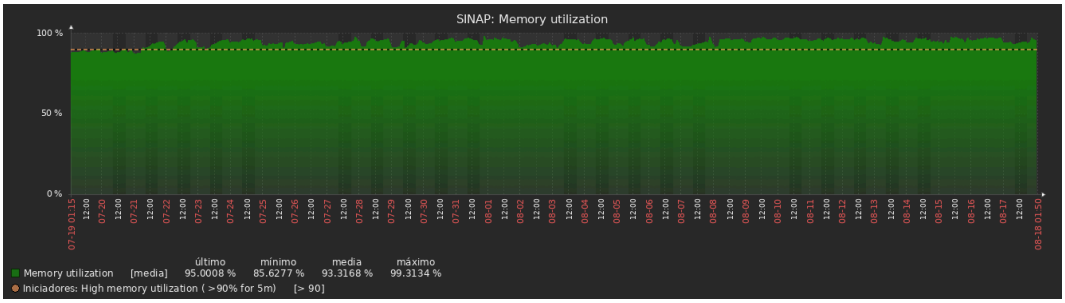
El uso del procesador en el servidor Proxmox entre el 19 de julio y el 18 de agosto, donde el consumo está compuesto mayoritariamente por el tiempo de espera de entrada/salida de disco, con un promedio del 13.91% y picos máximos de hasta 77.26%, seguido por el tiempo consumido por las máquinas virtuales con una media del 5.29% y un máximo puntual del 50.44% al inicio del periodo. Por su parte, métricas de carga base como el tiempo del sistema y de usuario se mantienen con promedios bajos del 2.20% y 2.20% respectivamente, mientras que el tiempo asignado a interrupciones por software registra una media del

1.88%; el resto de métricas permanecen en 0% o valores casi nulos.

Sinap

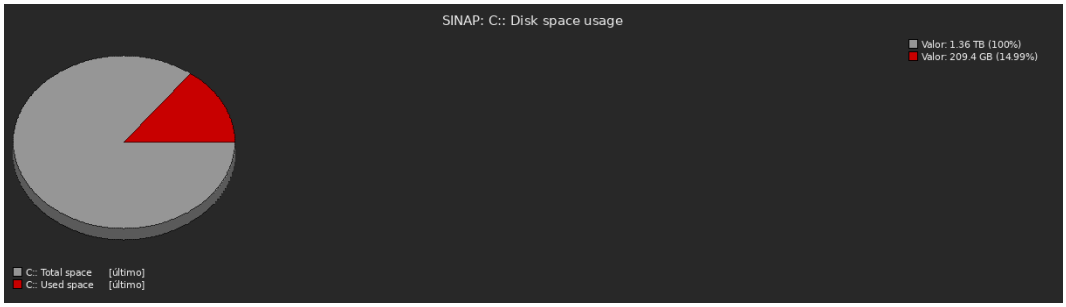


El gráfico muestra un uso de CPU extremadamente bajo y estable para el sistema **SINAP** durante el periodo analizado del 19 de julio al 18 de agosto, manteniendo tanto el tiempo de CPU privilegiado como el tiempo de usuario por debajo del 1% en sus valores promedio. Aunque se observan pequeños picos periódicos en la métrica de tiempo de usuario que alcanzan un máximo de 48.84%, estos son puntuales e insignificantes, ya que el consumo general se encuentra muy lejos de la línea de alerta del 30% marcada por el iniciador. En conclusión, el servidor se encuentra funcionando holgadamente, sin saturación ni cuellos de botella en la capacidad de procesamiento.

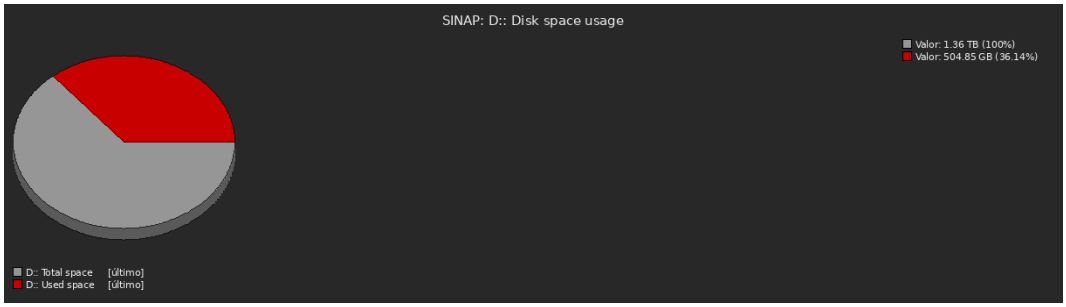


El gráfico refleja una alta utilización de la memoria RAM en el servidor **SINAP** de forma sostenida a lo largo de todo el periodo del 19 de julio al 18 de agosto, registrando un promedio de **93.31%**, un mínimo de **85.62%** y picos máximos de **99.31%**. La mayor parte del tiempo, el consumo se mantiene por encima de la línea de umbral de alerta del **90%**, lo que indica un uso intensivo y constante de la

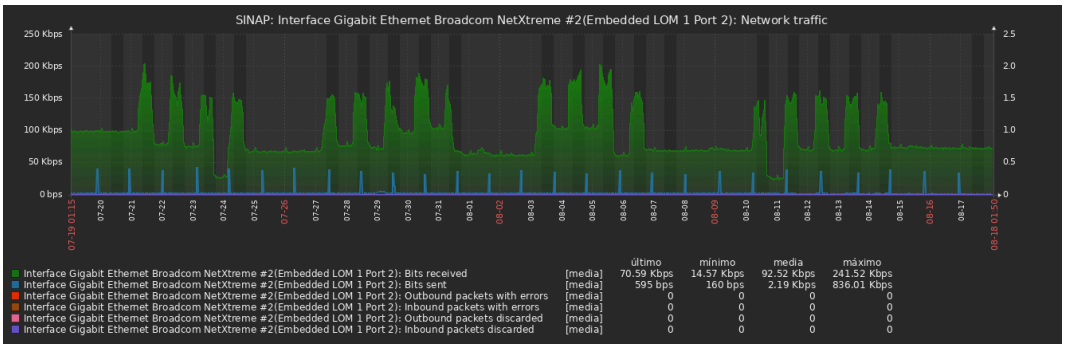
memoria que podría dejar al sistema con poco margen operativo ante cargas puntuales de trabajo.



El servidor SINAP muestra el espacio en almacenamiento de la unidad principal **C:** donde se evidencia un nivel de ocupación bajo y saludable: de una capacidad total de **1.36 TB**, únicamente se encuentran en uso **209.4 GB**. Esto significa que el sistema dispone de más del **85%** de almacenamiento libre, por lo que cuenta con suficiente margen operativo para el almacenamiento de archivos, registros y datos a futuro sin riesgo de saturación a corto plazo.

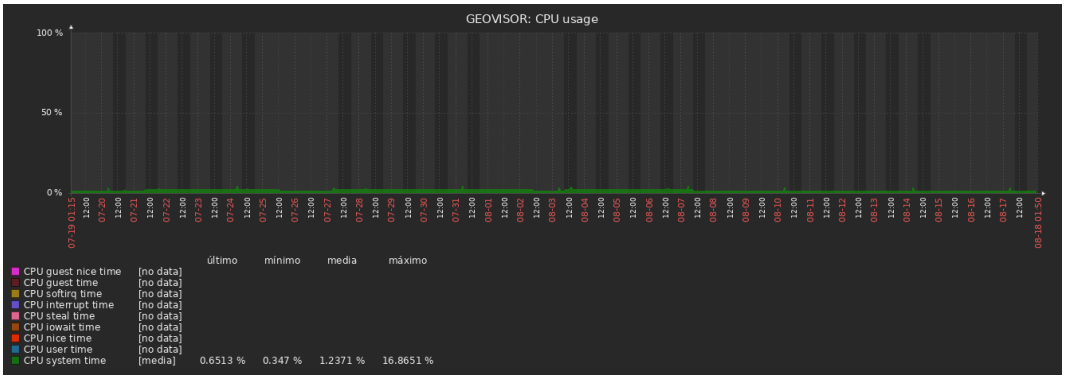


El gráfico refleja un estado saludable en el almacenamiento de la unidad secundaria **D:** del servidor **SINAP**, registrando un uso moderado de **504.85 GB** que equivale al **36.14%** de su capacidad total de **1.36 TB**. Esto deja disponible casi un **64%** del volumen, lo que garantiza un amplio margen operativo para la gestión de datos, respaldos o almacenamiento adicional sin representar ningún riesgo de saturación a corto o mediano plazo.

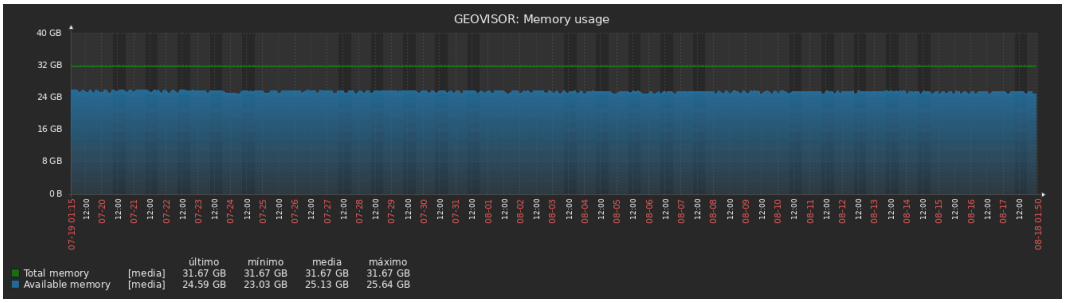


El gráfico de tráfico de red para la interfaz del servidor **SINAP** evidencia un consumo de ancho de banda extremadamente bajo en relación con la capacidad del enlace, registrando un promedio de transmisión entrante de **92.52 Kbps** con picos máximos de **241.52 Kbps**, y un tráfico saliente mínimo con una media de **2.19 Kbps** y picos periódicos de hasta **836.01 Kbps**. Asimismo, se observa un comportamiento operativo ideal al registrar **0** paquetes descartados o con errores, lo que confirma una conectividad estable, limpia y sin pérdida de datos ni congestión en la interfaz.

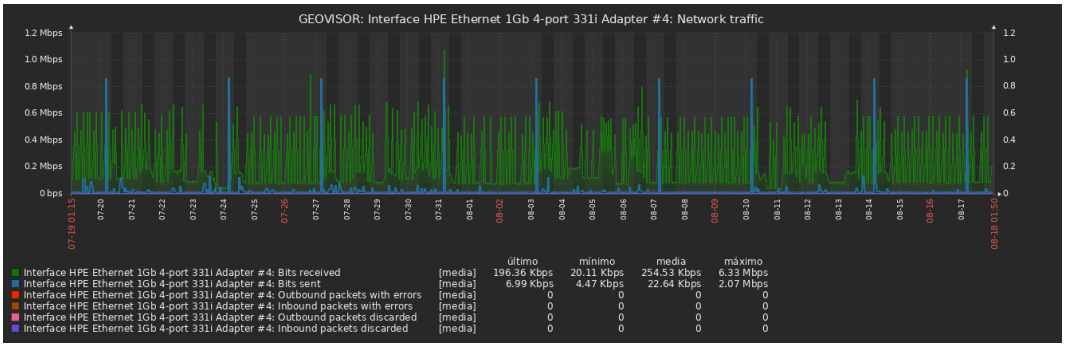
Geovisor



El gráfico de uso de CPU del servidor GEOVISOR para el periodo evaluado del 19 de julio al 18 de agosto evidencia una carga de trabajo sumamente baja y constante, registrando un promedio de 1.2371% de tiempo de sistema y un mínimo de 0.347%. Incluso su punto de consumo máximo registrado se mantiene apenas en 16.8651%, ubicándose muy por debajo de cualquier umbral de alerta o sobrecarga, lo que confirma que el procesador cuenta con una amplia holgura operativa y trabaja sin cuellos de botella ni estrés computacional.

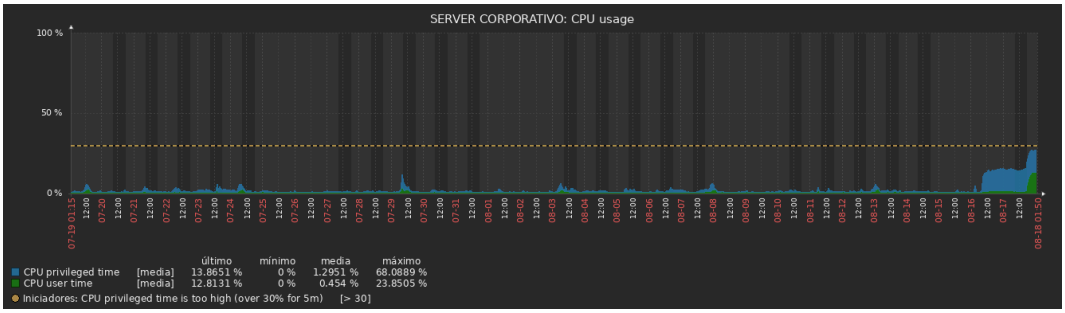


El gráfico muestra un estado de memoria altamente óptimo y estable en el servidor GEOVISOR durante el periodo del 19 de julio al 18 de agosto, donde sobre una capacidad total instalada de 31.67 GB, la memoria disponible mantiene una media de 25.13 GB. Esto indica que el sistema opera utilizando únicamente entre 6 GB y 8.6 GB aproximadamente, disponiendo de casi un 80% de memoria libre, lo que garantiza un excelente rendimiento sin ningún riesgo de saturación o cuello de botella en RAM.

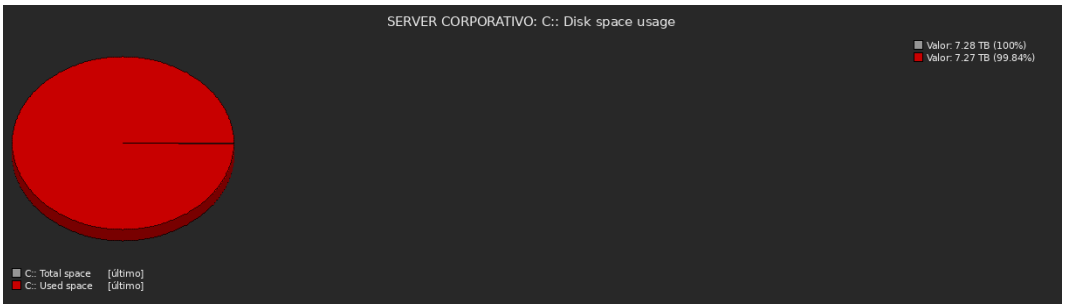


El gráfico de tráfico de red para la interfaz HPE Ethernet 1Gb 4-port 331i Adapter #4 del servidor GEOVISOR muestra un consumo de ancho de banda muy bajo y controlado en comparación con la capacidad total de la tarjeta, registrando un promedio de recepción de 254.53 Kbps con un pico máximo puntual de 6.33 Mbps, y un tráfico de salida con una media de 22.64 Kbps y máximos de 2.07 Mbps. Adicionalmente, el desempeño de la interfaz es completamente limpio al registrar 0 paquetes con errores o descartados, lo que ratifica una transmisión de datos estable, eficiente y libre de problemas de red.

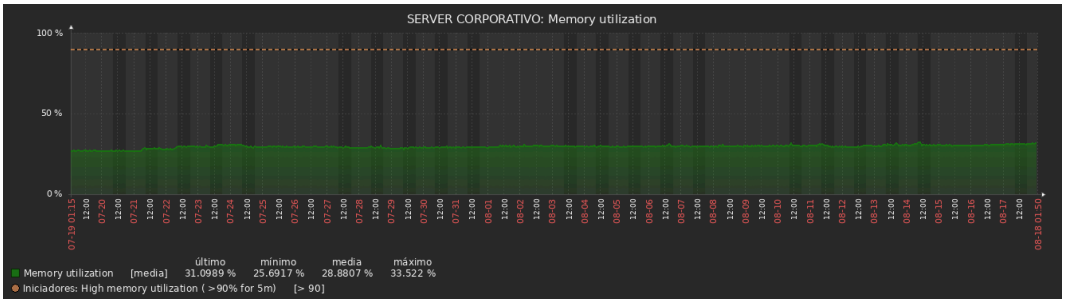
Adoc



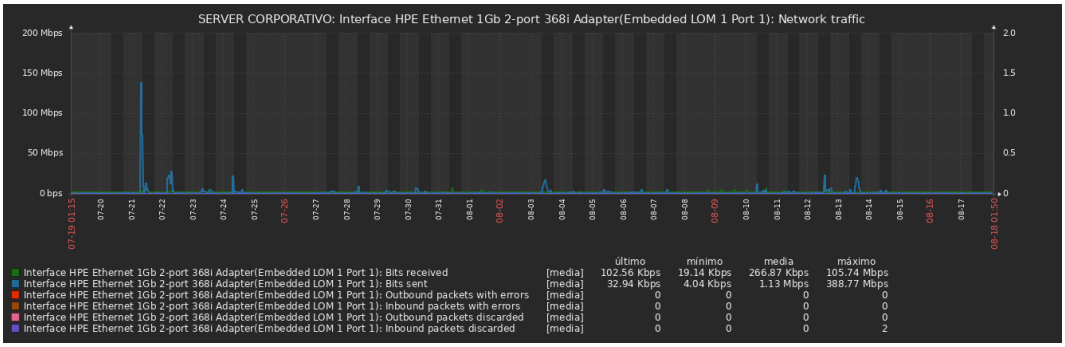
El gráfico de uso de CPU para el **SERVER CORPORATIVO** refleja un comportamiento general bajo con un incremento notable hacia el final del periodo evaluado del 19 de julio al 18 de agosto, manteniendo promedios globales moderados de **1.2951%** en tiempo privilegiado y **0.454%** en tiempo de usuario. Sin embargo, se observa un pico máximo significativo en el tiempo privilegiado que alcanza el **68.0889%**, impulsado principalmente por el repunte visible entre el 16 y el 18 de agosto, periodo en el que la actividad superó temporalmente la línea de umbral del **30%** fijada por el iniciador de alerta, sugiriendo un aumento puntual en las tareas del sistema o kernel al cierre del análisis.



Muestra el estado crítico del almacenamiento en el disco C: del servidor corporativo, evidenciando que la unidad está prácticamente llena al alcanzar un 99.84% de su capacidad. De un espacio total de 7.28 TB, ya se encuentran ocupados 7.27 TB, lo que deja un margen de maniobra prácticamente nulo, apenas unos 10 GB libres. Esta situación representa una alerta roja operativa de alta prioridad, ya que la falta de espacio en el disco principal puede provocar un colapso inminente del sistema, errores críticos en los servicios y la imposibilidad de guardar nuevos datos, requiriendo una intervención técnica inmediata para liberar espacio o expandir el almacenamiento.



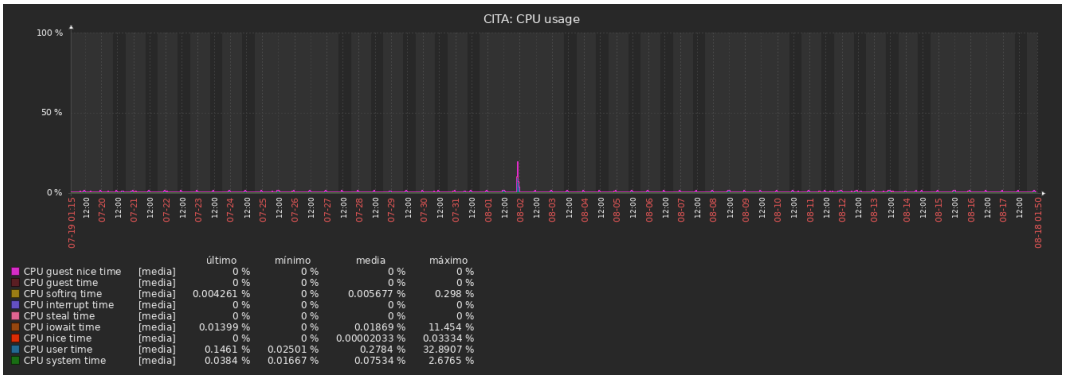
El gráfico de utilización de memoria RAM para el **SERVER CORPORATIVO** muestra un comportamiento sumamente estable y óptimo durante todo el periodo analizado 19 de julio al 18 de agosto, registrando un promedio de consumo del **28.8807%**, con un valor mínimo de **25.6917%** y un pico máximo de apenas **33.522%**. La ocupación se mantiene de forma uniforme muy por debajo de la línea de alerta del **90%** establecida por el iniciador de *High memory utilization*, lo que demuestra que el servidor cuenta con un amplio margen de recursos de memoria libres para responder eficientemente a las operaciones del sistema.



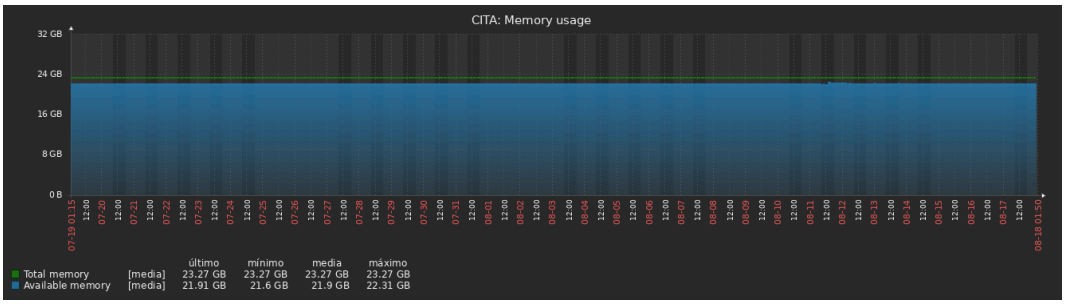
El tráfico de red para la interfaz **HPE Ethernet 1Gb 2-port 368i Adapter Port 1** del **SERVER CORPORATIVO** muestra un comportamiento operativo bajo y estable en general, registrando un promedio de transmisión saliente de **1.13 Mbps** y de recepción de **266.87 Kbps**. No obstante, se observan picos puntuales de actividad saliente notable alrededor del 21 de julio que alcanzaron un máximo de **388.77 Mbps**, los cuales se normalizaron rápidamente durante el resto del periodo evaluado. Finalmente, la calidad de la conexión es óptima al no registrar paquetes con errores y presentar apenas **2** paquetes entrantes descartados, lo

que confirma una comunicación fluida y sin problemas de congestión o degradación de red.

Cita



El gráfico de uso de CPU del servidor **CITA** refleja una carga de trabajo sumamente baja e inactiva durante la gran mayoría del periodo analizado 19 de julio al 18 de agosto, registrando un promedio de tiempo de usuario de apenas **0.2784%** y de sistema de **0.07534%**. El único evento destacable es un pico aislado registrado hacia el 2 de agosto donde el tiempo de usuario alcanzó un máximo de **32.8907%**, acompañado por un ligero incremento en la espera de E/S de **11.454%**, los cuales se normalizaron de inmediato. En conclusión, el procesador opera con total holgura, manteniéndose prácticamente desocupado y sin presentar síntomas de saturación.

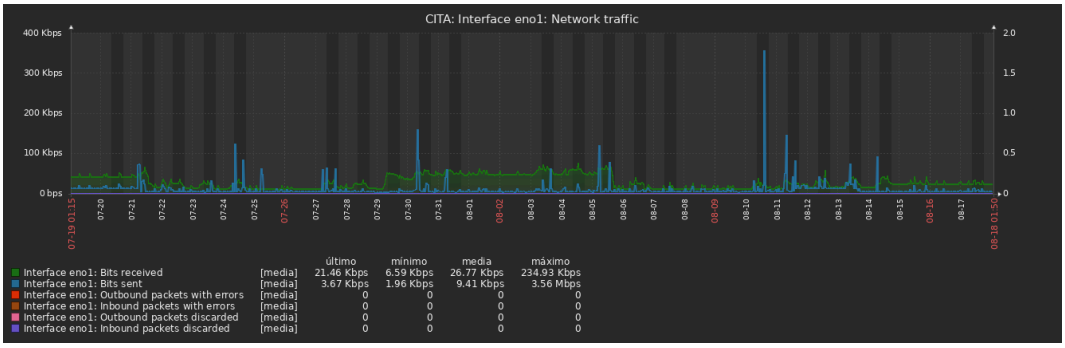


El uso de memoria RAM sumamente óptimo y plano en el servidor CITA durante el periodo del 19 de julio al 18 de agosto, donde de una capacidad total de 23.27 GB, la memoria disponible se mantiene de forma prácticamente lineal en un promedio de 21.9

GB. Esto demuestra que el sistema opera consumiendo tan solo alrededor de 1.37 GB de memoria, ofreciendo una disponibilidad sostenida superior al 94%, lo que garantiza un rendimiento impecable sin el menor riesgo de saturación en este recurso.

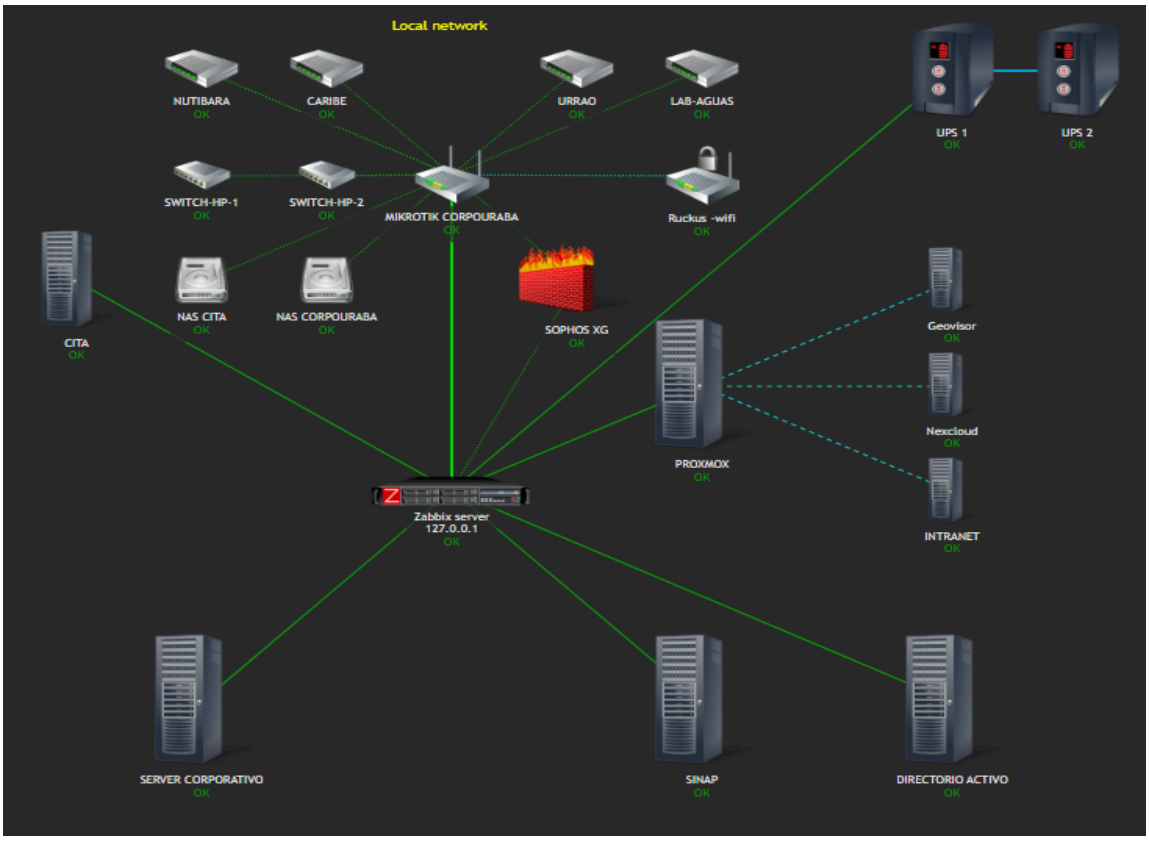


El disco del sistema CITA correspondiente al último registro de monitoreo, muestra una elevada ocupación en la partición raíz (/) del servidor CITA, donde de un espacio total disponible de 1.64 TB, se encuentran utilizados 1.43 TB, lo que representa el 87.25% del volumen. Esta situación deja un remanente libre de tan solo el 12.75%, por lo que se sugiere realizar labores de depuración de registros, archivos temporales o una ampliación de almacenamiento en el corto plazo para evitar un posible agotamiento de disco y comprometer la operatividad del sistema.



El tráfico de red en la interfaz eno1 del servidor CITA, evidencia un flujo de datos sumamente bajo y estable a lo largo del periodo evaluado 19 de julio al 18 de agosto, registrando un promedio de recepción de 26.77 Kbps con picos de hasta 234.93 Kbps, y un promedio de envío de 9.41 Kbps. Aunque se observan picos esporádicos de transmisión saliente, destacando uno registrado el 10 u 11 de agosto que alcanzó un máximo de 3.56 Mbps, el

consumo general se mantiene en niveles mínimos e insignificantes respecto a la capacidad de la interfaz. Finalmente, el estado de la comunicación es limpio al no presentar registros de paquetes descartados ni errores en la transmisión.

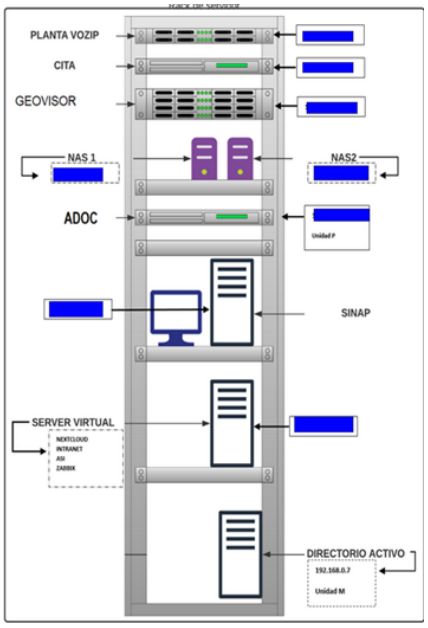


La infraestructura de red institucional ha sido diseñada bajo un modelo de alta disponibilidad, cuyo objetivo central es garantizar que la conectividad y el acceso a la información nunca sean un obstáculo para la operación. Esta arquitectura integra servidores de alto rendimiento y unidades de almacenamiento masivo (NAS) en un ecosistema unificado, el cual se encuentra blindado perimetralmente por tecnología Sophos XG. Esta capa de seguridad no solo protege los activos digitales contra amenazas externas, sino que asegura la integridad de la información corporativa en todo momento.

Para transitar de una gestión reactiva a una estrategia de prevención, la organización utiliza la plataforma Zabbix como eje central de monitoreo. Esta herramienta nos proporciona una

visibilidad total y en tiempo real del estado de los activos, permitiéndonos identificar y mitigar cualquier anomalía antes de que afecte la productividad de los usuarios. En esencia, contamos con una red resiliente, protegida y supervisada que garantiza la continuidad del servicio y el cumplimiento de los estándares institucionales más exigentes.

Diagrama de servidores



La infraestructura central de TI se encuentra en el rack de servidores, donde se garantiza una gestión optimizada y la seguridad de todos los recursos críticos. Este espacio aloja componentes esenciales como:

- Servidores de Aplicaciones: PLANTA VOZIP, CITA, GEOVISOR, ADOC y SINAP
- Almacenamiento: Unidades NAS 1 y NAS 2.
  Nas1: copia de seguridad corporativo intranet
  Nas2: copia de seguridad base de datos sinapv6 y cita
- Virtualización: Servidor Proxmox.
- Servicios Centrales: Directorio Activo.
- Continuidad Operativa: Sistemas de respaldo energético.

La configuración actual es estática y solo está sujeta a modificaciones

para la integración de nuevas infraestructuras o la implementación de las actualizaciones de seguridad necesarias.

3.1.3. Establecer acceso remoto a los servidores a los proveedores que lo requieran.

La corporación suspendió la creación de nuevos accesos remotos para terceros como estrategia preventiva para reducir la superficie de ataque. Al alinearse con el principio de mínimo privilegio, se mitigaron vectores de riesgo externos y se blindó la infraestructura crítica.

3.1.4. Verificar que los servicios montados en los servidores y que presten servicios a los funcionarios, contratistas y/o terceros de forma remota funcione normalmente, si se presentan fallos en el servidor y/o las conexiones priorizar su respuesta.

Durante el periodo reciente, el departamento de TI garantiza la continuidad total de los servicios para el personal y los contratistas, logrando una disponibilidad ininterrumpida. No obstante, las métricas de rendimiento han detectado debilidades técnicas que, a pesar del éxito operativo actual, representan un riesgo latente y exigen una intervención prioritaria para evitar futuras caídas del sistema.

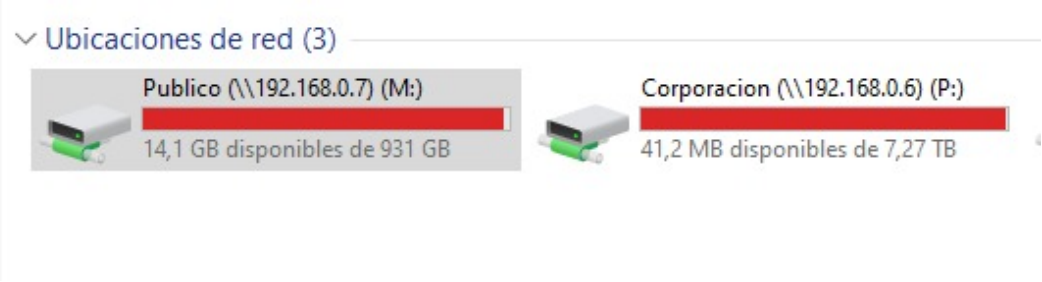
Diagnóstico de la Infraestructura Crítica.

CNT	DESCRIPCIÓN	RAM	HDD	SO	PROCESADOR	EOL HARDWARE	EOL SOFTWARE	APLICATIVOS	REFERENCIA	ESTADO	OBSERVACIONES
1	PLANTA	4 GB	1TB	CentOS Linux	XEON E3-1220 V3 3,10 ghz	2024	2024	TELEFONIA IP	Proliant DL320e Gen8 v2	No es crítico	La planta telefónica puede continuar bajo estas condiciones
2	CITA	24 GB	2 TB	CentOS Linux	XEON E5 -2603 V4 1,70GHz	2025	2024	CITA	Proliant DL120 Gen 9	No es crítico	
3	GEOVISOR	32 GB	3 TB	WIN SERVER 2016	XEON silver 4108 1,80 GHz	2024	2027	GEOVISOR	Proliant DL380 Gen10	No es crítico	
4	NAS 1	1 GB	3 TB	Firmware basado en Linux	Marvell ARMADA 1.33 GHz	2023	N/A	DATA NO ESTRUCTURADA	Buffalo TeraStation TS3400D	74.16% en uso	Se debe realizar un proceso de depuración de la información
5	NAS 2	2 GB	4 Disk x	Firmware basado	Intel Atom D2550	2026	N/A	DATA NO ESTRUCTURADA	Buffalo TeraStation TS5400D	91.74% en uso	Urgente se debe realizar un

			3TB	en Linux							proceso de depuración de la información
6	ADOC	32 GB	7TB	win Server 2019	XEON bronze 3106 1,70GHz	2029	2029	ADOC	Proliant DL160 Gen10	CRÍTICO, Uso del disco al 99.84%	
7	**PROXMOX**	**16 GB**	**1TB**	**Debian Linux**	**XEON E5-2603 v3 1,60GHz**	**2025**	**N/A**	**INTRANET ASI ZABIIX /PROXMOX**	**PROLIANT ML30 GEN9**	**CRÍTICO, uso de la RAM 90.93%**	
8	**SINAP**	**8 GB**	**3TB**	**Win Server 2012 R2**	**XEON E3-1220 V5 3,0GHz**	**2025**	**2025**	**SINAP BASE DE DATOS ORACLE**	**PROLIANT ML30 GEN9**	**CRÍTICO, uso de la RAM CRÍTICO, uso de la RAM 99.31%**	**Se debe migrar de forma urgente**
9	**DIRECTORIO ACT**	**20 GB**	**1 TB**	**Win Server 2012**	**XEON E5-2620 2,0GHz**	**2024**	**2025**	**DIRECTORIO ACTIVO**	**Proliant ML350p Gen8**	**CRITICO, 98.93% de uso del disco y la RAM 98.15%**	**Se debe migrar de forma urgente**

En la actualidad, los nodos que soportan sistemas críticos incluyendo **SINAP, Proxmox**, **directorio activo** presentan una saturación crítica en la memoria RAM. Esta limitación técnica está generando latencias significativas, las cuales obstaculizan la agilidad de los procesos operativos internos y el procesamiento de datos.

A esta situación se suma el agotamiento del espacio de almacenamiento en las unidades de red y servicios de directorio (**M:, P:, ADOC y Directorio Activo**). Haber alcanzado este límite no sólo restringe la gestión documental, sino que sitúa a la entidad en un escenario de alta vulnerabilidad frente a posibles bloqueos del sistema o pérdida de integridad en las bases de datos.



Adicionalmente a la obsolescencia del hardware, la corporación presenta obsolescencia en varios de los sistemas operativos actualmente implementados, particularmente versiones como Windows Server 2012/2012 R2 y distribuciones Linux sin soporte vigente. Esta situación incrementa significativamente el riesgo operativo y de ciberseguridad institucional.

Los sistemas operativos EOL dejan de recibir:

- Parches de seguridad críticos.
- Correcciones de vulnerabilidades conocidas.
- Actualizaciones de compatibilidad.
- Soporte técnico del fabricante.
- Mejoras de estabilidad y rendimiento.
- Actualizaciones de protocolos de autenticación y cifrado.

Riesgos de ciberseguridad

La utilización de sistemas operativos obsoletos expone la infraestructura tecnológica a:

- Vulnerabilidades explotables públicamente.
- Ataques de ransomware (Riesgo materializado en el servidor de directorio activo durante la segunda semana del mes de Mayo de 2026).
- Escalamiento de privilegios.
- Compromiso del Directorio Activo.
- Robo de credenciales institucionales.
- Acceso no autorizado a servicios internos.
- Exposición de servicios críticos conectados a Internet.

En el caso específico de Windows Server 2012/2012 R2, Microsoft finalizó su soporte oficial en octubre de 2023, lo que implica ausencia total de actualizaciones de seguridad regulares.

Con el objetivo de blindar la **continuidad operativa** y proteger la productividad de funcionarios y aliados, se requiere una actualización urgente de las capacidades de hardware. Esta estrategia de intervención se articula bajo tres objetivos fundamentales:

Prevención Crítica: Eliminar los riesgos de colapso sistémico por falta de recursos físicos.

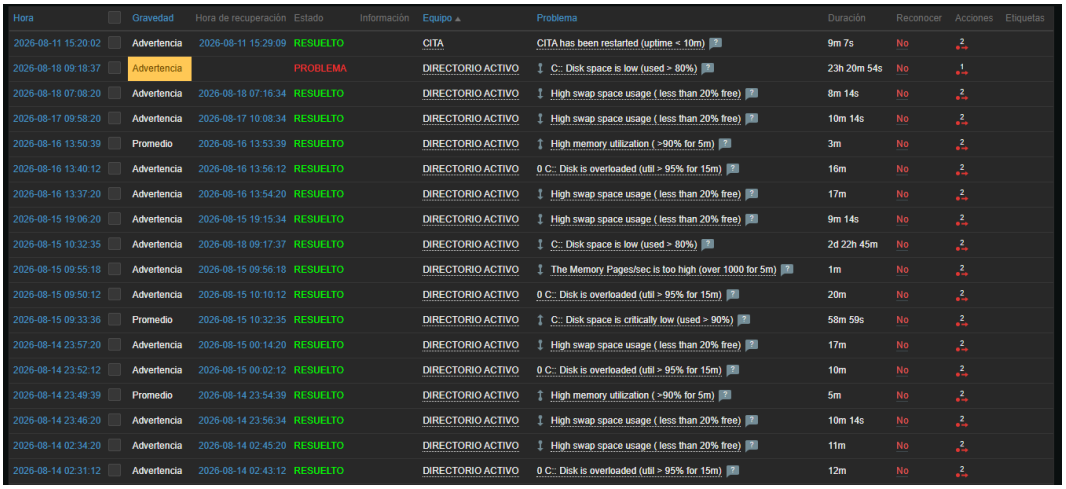
Eficiencia Operativa: Restaurar la velocidad de respuesta de las plataformas institucionales.

Sostenibilidad y Crecimiento: Proveer una infraestructura robusta capaz de absorber la demanda actual y futura de la organización.

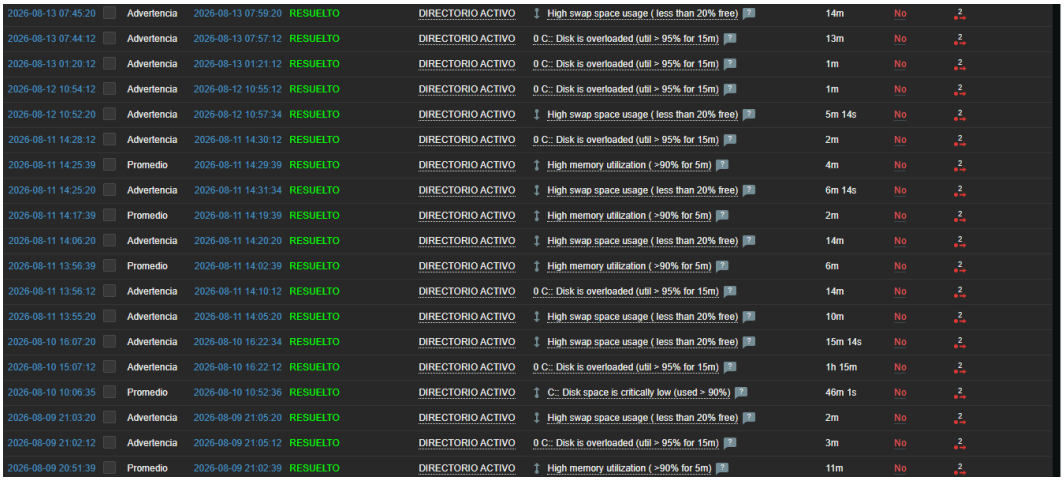
4. ACCESO A INTERNET Y VOZ CORPORATIVA

4.1. Realizar actividades relacionados con el soporte al servicio de acceso a Internet

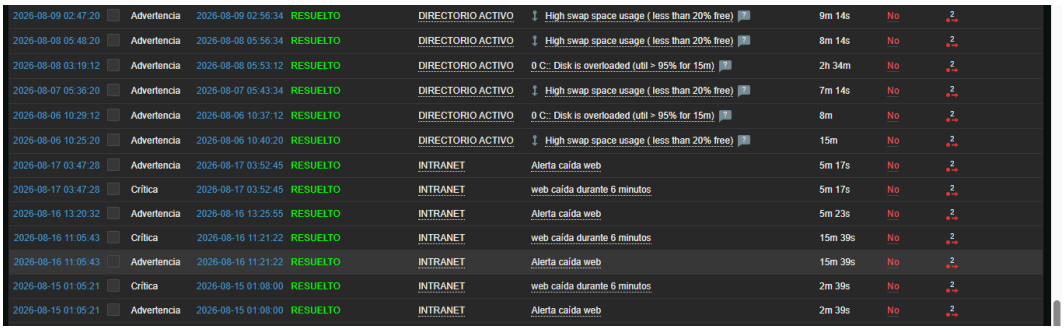
En el período evaluado, se registraron varias interrupciones, como se observa en la imagen adjunta.



Hora	Gravedad	Hora de recuperación	Estado	Información	Equipo	Problema	Duración	Reconocer	Acciones	Etiquetas
2026-08-11 15:20:02	Advertencia	2026-08-11 15:29:09	RESUELTO		CITA	CITA has been restarted (uptime < 10m)	9m 7s	No	2	
2026-08-18 09:18:37	Advertencia		PROBLEMA		DIRECTORIO ACTIVO	C:: Disk space is low (used > 80%)	23h 20m 54s	No	1	
2026-08-18 07:08:20	Advertencia	2026-08-18 07:16:34	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	8m 14s	No	2	
2026-08-17 09:58:20	Advertencia	2026-08-17 10:08:34	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	10m 14s	No	2	
2026-08-16 13:50:39	Promedio	2026-08-16 13:53:39	RESUELTO		DIRECTORIO ACTIVO	High memory utilization (>90% for 5m)	3m	No	2	
2026-08-16 13:40:12	Advertencia	2026-08-16 13:56:12	RESUELTO		DIRECTORIO ACTIVO	0 C:: Disk is overloaded (util > 95% for 15m)	16m	No	2	
2026-08-16 13:37:20	Advertencia	2026-08-16 13:54:20	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	17m	No	2	
2026-08-15 19:06:20	Advertencia	2026-08-15 19:15:34	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	9m 14s	No	2	
2026-08-15 10:32:35	Advertencia	2026-08-18 09:17:37	RESUELTO		DIRECTORIO ACTIVO	C:: Disk space is low (used > 80%)	2d 22h 45m	No	2	
2026-08-15 09:55:18	Advertencia	2026-08-15 09:56:18	RESUELTO		DIRECTORIO ACTIVO	The Memory Pages/sec is too high (over 1000 for 5m)	1m	No	2	
2026-08-15 09:50:12	Advertencia	2026-08-15 10:10:12	RESUELTO		DIRECTORIO ACTIVO	0 C:: Disk is overloaded (util > 95% for 15m)	20m	No	2	
2026-08-15 09:33:36	Promedio	2026-08-15 10:32:35	RESUELTO		DIRECTORIO ACTIVO	C:: Disk space is critically low (used > 90%)	58m 59s	No	2	
2026-08-14 23:57:20	Advertencia	2026-08-15 00:14:20	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	17m	No	2	
2026-08-14 23:52:12	Advertencia	2026-08-15 00:02:12	RESUELTO		DIRECTORIO ACTIVO	0 C:: Disk is overloaded (util > 95% for 15m)	10m	No	2	
2026-08-14 23:49:39	Promedio	2026-08-14 23:54:39	RESUELTO		DIRECTORIO ACTIVO	High memory utilization (>90% for 5m)	5m	No	2	
2026-08-14 23:46:20	Advertencia	2026-08-14 23:56:34	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	10m 14s	No	2	
2026-08-14 02:34:20	Advertencia	2026-08-14 02:45:20	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	11m	No	2	
2026-08-14 02:31:12	Advertencia	2026-08-14 02:43:12	RESUELTO		DIRECTORIO ACTIVO	0 C:: Disk is overloaded (util > 95% for 15m)	12m	No	2	



2026-08-13 07:45:20	Advertencia	2026-08-13 07:59:20	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	14m	No	2	
2026-08-13 07:44:12	Advertencia	2026-08-13 07:57:12	RESUELTO		DIRECTORIO ACTIVO	0 C:: Disk is overloaded (util > 95% for 15m)	13m	No	2	
2026-08-13 01:20:12	Advertencia	2026-08-13 01:21:12	RESUELTO		DIRECTORIO ACTIVO	0 C:: Disk is overloaded (util > 95% for 15m)	1m	No	2	
2026-08-12 10:54:12	Advertencia	2026-08-12 10:55:12	RESUELTO		DIRECTORIO ACTIVO	0 C:: Disk is overloaded (util > 95% for 15m)	1m	No	2	
2026-08-12 10:52:20	Advertencia	2026-08-12 10:57:34	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	5m 14s	No	2	
2026-08-11 14:28:12	Advertencia	2026-08-11 14:30:12	RESUELTO		DIRECTORIO ACTIVO	0 C:: Disk is overloaded (util > 95% for 15m)	2m	No	2	
2026-08-11 14:25:39	Promedio	2026-08-11 14:29:39	RESUELTO		DIRECTORIO ACTIVO	High memory utilization (>90% for 5m)	4m	No	2	
2026-08-11 14:25:20	Advertencia	2026-08-11 14:31:34	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	6m 14s	No	2	
2026-08-11 14:17:39	Promedio	2026-08-11 14:19:39	RESUELTO		DIRECTORIO ACTIVO	High memory utilization (>90% for 5m)	2m	No	2	
2026-08-11 14:06:20	Advertencia	2026-08-11 14:20:20	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	14m	No	2	
2026-08-11 13:56:39	Promedio	2026-08-11 14:02:39	RESUELTO		DIRECTORIO ACTIVO	High memory utilization (>90% for 5m)	6m	No	2	
2026-08-11 13:56:12	Advertencia	2026-08-11 14:10:12	RESUELTO		DIRECTORIO ACTIVO	0 C:: Disk is overloaded (util > 95% for 15m)	14m	No	2	
2026-08-11 13:55:20	Advertencia	2026-08-11 14:05:20	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	10m	No	2	
2026-08-10 16:07:20	Advertencia	2026-08-10 16:22:34	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	15m 14s	No	2	
2026-08-10 15:07:12	Advertencia	2026-08-10 16:22:12	RESUELTO		DIRECTORIO ACTIVO	0 C:: Disk is overloaded (util > 95% for 15m)	1h 15m	No	2	
2026-08-10 10:06:35	Promedio	2026-08-10 10:52:36	RESUELTO		DIRECTORIO ACTIVO	C:: Disk space is critically low (used > 90%)	46m 1s	No	2	
2026-08-09 21:03:20	Advertencia	2026-08-09 21:05:20	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	2m	No	2	
2026-08-09 21:02:12	Advertencia	2026-08-09 21:05:12	RESUELTO		DIRECTORIO ACTIVO	0 C:: Disk is overloaded (util > 95% for 15m)	3m	No	2	
2026-08-09 20:51:39	Promedio	2026-08-09 21:02:39	RESUELTO		DIRECTORIO ACTIVO	High memory utilization (>90% for 5m)	11m	No	2	



2026-08-09 02:47:20	Advertencia	2026-08-09 02:56:34	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	9m 14s	No	2	
2026-08-08 05:48:20	Advertencia	2026-08-08 05:56:34	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	8m 14s	No	2	
2026-08-08 03:19:12	Advertencia	2026-08-08 05:53:12	RESUELTO		DIRECTORIO ACTIVO	0 C:: Disk is overloaded (util > 95% for 15m)	2h 34m	No	2	
2026-08-07 05:36:20	Advertencia	2026-08-07 05:43:34	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	7m 14s	No	2	
2026-08-06 10:29:12	Advertencia	2026-08-06 10:37:12	RESUELTO		DIRECTORIO ACTIVO	0 C:: Disk is overloaded (util > 95% for 15m)	8m	No	2	
2026-08-06 10:25:20	Advertencia	2026-08-06 10:40:20	RESUELTO		DIRECTORIO ACTIVO	High swap space usage (less than 20% free)	15m	No	2	
2026-08-17 03:47:28	Advertencia	2026-08-17 03:52:45	RESUELTO		INTRANET	Alerta caída web	5m 17s	No	2	
2026-08-17 03:47:28	Crítica	2026-08-17 03:52:45	RESUELTO		INTRANET	web caída durante 6 minutos	5m 17s	No	2	
2026-08-16 13:20:32	Advertencia	2026-08-16 13:25:55	RESUELTO		INTRANET	Alerta caída web	5m 23s	No	2	
2026-08-16 11:05:43	Crítica	2026-08-16 11:21:22	RESUELTO		INTRANET	web caída durante 6 minutos	15m 39s	No	2	
2026-08-16 11:05:43	Advertencia	2026-08-16 11:21:22	RESUELTO		INTRANET	Alerta caída web	15m 39s	No	2	
2026-08-15 01:05:21	Crítica	2026-08-15 01:08:00	RESUELTO		INTRANET	web caída durante 6 minutos	2m 39s	No	2	
2026-08-15 01:05:21	Advertencia	2026-08-15 01:08:00	RESUELTO		INTRANET	Alerta caída web	2m 39s	No	2	

Hay 1 alerta activa no resuelta (PROBLEMA activo desde el 18 de agosto) relacionada con espacio en disco en el servidor DIRECTORIO ACTIVO.

Equipos Afectados: DIRECTORIO ACTIVO, INTRANET y CITA.

Patrón Principal: El servidor de Directorio Activo presenta saturación recurrente de recursos (memoria RAM, memoria de intercambio/swap y espacio en disco I/O).

DIRECTORIO ACTIVO (Criticidad Alta)

Espacio en Disco Alerta Activa: Mantiene la alerta C:: Disk space is low (used > 80%) en estado de PROBLEMA activo con más de 23 horas de duración. Previamente alcanzó niveles de Critically low > 90% y episodios donde la utilización de I/O de disco superó el 95% durante más de 15 minutos .

Consumo de Memoria y Swap: Presenta caídas constantes en la memoria de intercambio (High swap space usage < 20% free) combinadas con picos de memoria RAM (High memory utilization > 90% for 5m) y paginación excesiva (Memory Pages/sec is too high).

Causa Raíz Probable: El agotamiento del disco físico $C:$ obliga al sistema a recurrir a paginación en memoria swap, generando un cuello de botella en la memoria RAM y en la E/S del disco.

INTRANET (Criticidad Media)

Caídas del Servicio Web: Muestra múltiples eventos de Crítica y Advertencia indicando caídas del sitio web (web caída durante 6 minutos / Alerta caída web).

Intermitencia: Se registraron caídas sistemáticas los días 15, 16 y 17 de agosto, con tiempos de recuperación de entre 2 y 15 minutos.

CITA (Criticidad Baja / Resuelto)

Reinicio de Sistema: Evento puntual resuelto de reinicio del equipo (CITA has been restarted, uptime < 10m) el 11 de agosto con una duración de 9 minutos.

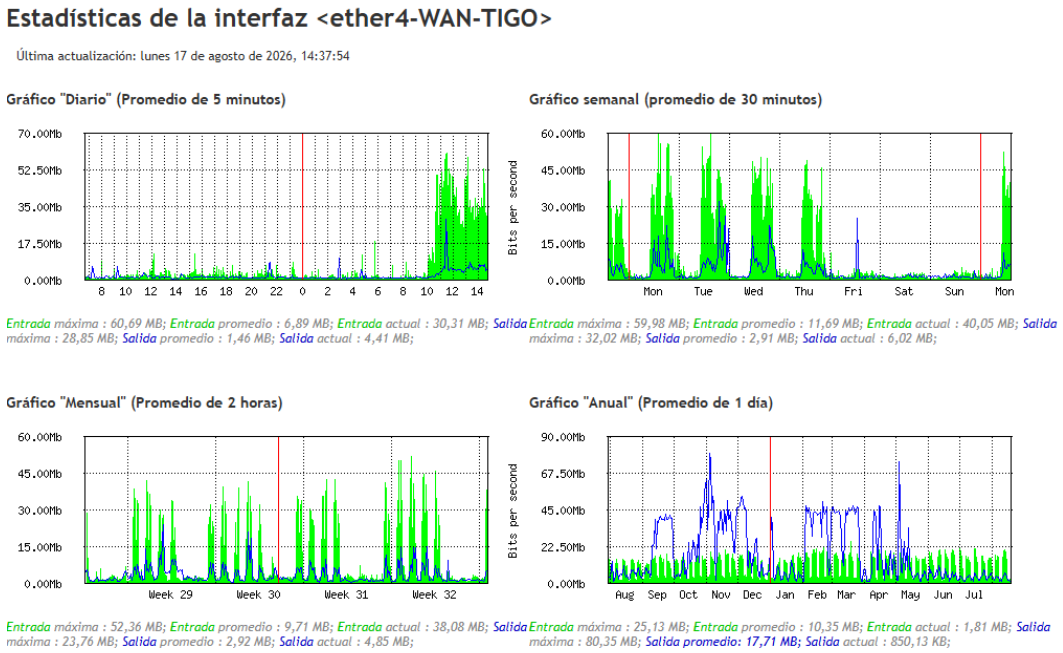
Recomendaciones de Acción

Atención Inmediata: Liberar espacio de almacenamiento en la unidad C: de DIRECTORIO ACTIVO, eliminar logs antiguos, archivos temporales o depurar bases de datos del sistema.

Optimización de Memoria: Evaluar un incremento de memoria RAM física en el servidor DIRECTORIO ACTIVO para mitigar la saturación de memoria swap y paginación.

CONSUMO DE INTERNET RED LAN CABLEADA: Durante este periodo, se llevó a cabo un seguimiento continuo del consumo de internet en la red cableada, identificándose picos estables que concuerdan con la velocidad contratada con el proveedor TIGO UNE.

A continuación, el histórico de consumo:



El enlace ether4-WAN-TIGO se ha consolidado como un recurso fundamental para la conectividad, demostrando una notable capacidad de respuesta y resiliencia ante picos de demanda operativa y procesos de soporte. Las métricas de tráfico confirman que este canal posee la solvencia necesaria para gestionar la concurrencia de la red de manera eficiente, siempre que se garantice la robustez del hardware que lo sustenta para mantener su estabilidad a largo plazo.

Gráfica Diaria

El comportamiento diario refleja una marcada concentración de la actividad durante la jornada laboral. El tráfico de descarga alcanza un pico máximo de 60,69 Mb, mientras que la subida registra hasta 28,85 Mb, observándose una transmisión intensa entre las 10:00 y las 14:00 horas con valores recientes de 30,31 Mb de entrada y 4,41 Mb de salida. En contraste, durante la noche y la madrugada el consumo es prácticamente nulo, registrando promedios mínimos de apenas 6,89 Mb de bajada y 1,46 Mb de subida.

Gráfica Semanal

A nivel semanal se ratifica la dependencia del horario hábil: de lunes a jueves se presentan los mayores niveles de demanda, con picos de 59,98 Mb en descarga y 32,02 Mb en carga. A partir del viernes y durante todo el fin de semana, el tráfico cae a valores marginales cercanos a cero, reactivándose el lunes siguiente con registros actuales de 40,05 Mb de bajada y 6,02 Mb de subida.

Gráfica Mensual

La gráfica mensual muestra una estructura periódica continua, caracterizada por caídas drásticas los fines de semana y ráfagas constantes de descarga en días laborables. El tráfico de entrada alcanza un pico máximo de 52,36 Mb con un promedio de 9,71 Mb. Por su parte, el tráfico saliente permanece significativamente contenido, con un promedio de 2,92 Mb y un máximo puntual de 23,76 Mb, lo que confirma un perfil enfocado principalmente en la descarga de información.

Gráfica Anual

El historial del último año evidencia una alteración notable entre septiembre y diciembre, periodo en el que se registró un incremento masivo en el tráfico de subida, alcanzando un pico absoluto de 80,35 Mb y un promedio de 17,71 Mb. Este comportamiento de exportación de datos contrasta con el volumen de entrada, que se mantuvo estable a lo largo del año con un promedio de 10,35 Mb y un techo de 25,13 Mb, retornando a un régimen de consumo moderado a partir de mayo.

Recomendaciones de Capacidad y Optimización

Es necesario aumentar el ancho de banda de 60 Mbps a un mínimo de 300 Mbps debido a que la demanda actual alcanza picos por encima de los 60 Mbps. Esta saturación genera cuellos de botella que provocan latencia, pérdida de paquetes y ponen en riesgo la integridad de los respaldos de datos realizados en horarios nocturnos y fines de semana. La modernización del enlace permitirá pasar de una postura reactiva a una de alta disponibilidad, garantizando que la infraestructura soporte el crecimiento sostenido del flujo de datos registrado por la corporación.

Esta inversión estratégica es fundamental para proteger la continuidad del negocio y asegurar que la productividad del personal no se vea limitada por una red obsoleta.

por el momento para evitar la saturación del canal y garantizar el rendimiento óptimo de la infraestructura, se recomienda implementar políticas de Calidad de Servicio (QoS) y priorización de tráfico que limiten el consumo no esencial durante los picos críticos de la jornada laboral y, de manera muy especial, durante el evento crítico de consumo observado entre las 18:00 y las 20:30 horas. Dado que el horario nocturno, la madrugada y los fines de semana presentan una inactividad casi absoluta, es altamente aconsejable reprogramar las tareas pesadas de absorción de datos, las descargas periódicas de información identificadas en el patrón mensual y cualquier proceso de copia de seguridad para que se ejecuten estrictamente en estas ventanas de tiempo inactivas.

Optimización y Priorización de Tráfico

Implementar configuraciones de Calidad de Servicio (QoS) en la interfaz ether4-WAN-TIGO para dar máxima prioridad al tráfico de las plataformas esenciales (SINAP/CITA). Con esta medida se garantiza la continuidad y estabilidad de los servicios críticos, previniendo degradaciones de rendimiento incluso durante picos de consumo de datos o actividades de soporte técnico en la red.

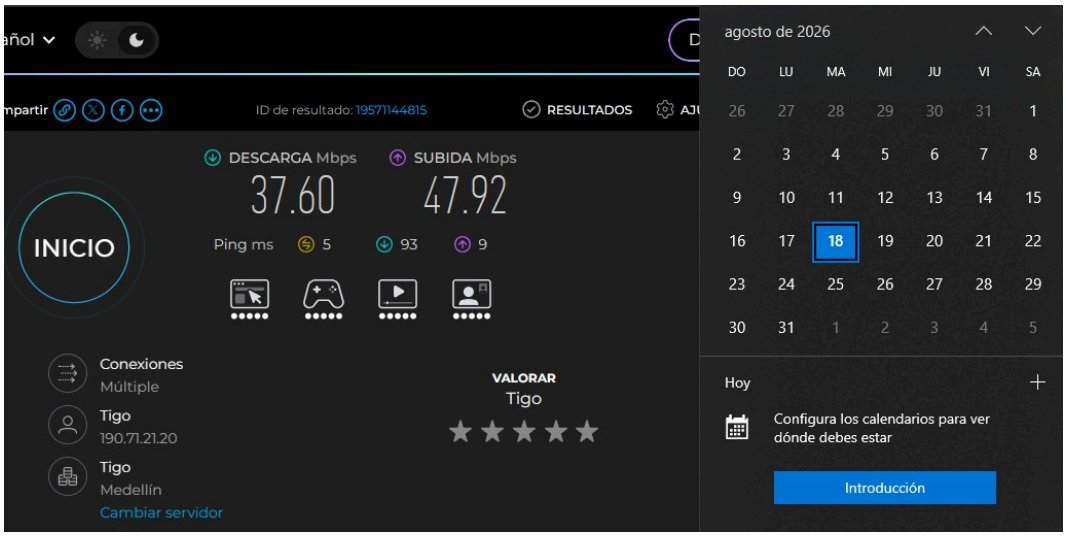
Monitoreo y Alertas Proactivas

Configurar notificaciones automáticas basadas en el protocolo SNMP dirigidas al equipo de TI, las cuales se activarán de manera preventiva al superar el 85% de capacidad en el ancho de banda o en el almacenamiento de los servidores. Esta estrategia busca

anticiparse a posibles saturaciones o caídas de la infraestructura, facilitando acciones correctivas inmediatas que mitiguen cualquier impacto en la experiencia del usuario final.

CONSUMO DE INTERNET RED INALÁMBRICA: CONTRATISTAS

La arquitectura **Wi-Fi_Admin** redefine la movilidad como un activo de seguridad. Su función principal es crear un **perímetro lógico** que blinda la red LAN, separando el tráfico de gestión de las amenazas potenciales. Al combinar una autenticación estricta con la segmentación de datos, la empresa garantiza que la libertad de movimiento de los administradores no genera brechas de seguridad ni degrade el rendimiento de los procesos críticos.



El análisis de rendimiento de red realizado el 18 de agosto de 2026 muestra un enlace de conexión a Internet provisto por Tigo con un comportamiento asimétrico favorable para la transmisión de datos salientes. La conexión alcanzó una velocidad de subida de 47.92 Mbps, superando a la velocidad de descarga de 37.60 Mbps. Esta capacidad de ancho de banda resulta adecuada para entornos operativos que requieren carga frecuente de archivos, videollamadas de alta definición y actividades de colaboración en la nube sin degradación en el flujo continuo de trabajo.

En cuanto a la calidad y estabilidad de la infraestructura, se registró una latencia base óptima de 5 ms y un impacto mínimo en la subida con 9 ms, lo que garantiza un tiempo de respuesta

inmediato para servicios interactivos. No obstante, se detectó un incremento de la latencia durante la descarga activa hasta los 93 ms, señalando una ligera congestión por amortiguación bajo saturación de tráfico entrante. A pesar de esta variación puntual, el canal presenta un desempeño general eficiente y estable para las exigencias de conectividad estándar.

4.1.1. Soporte y mantenimiento semestral a los equipos de administración de acceso a Internet.

En este periodo no se realizaron mantenimientos, pero se realizó cambio de internet y red en el laboratorio.

4.1.2. Aplicación de políticas de acceso mediante la red LAN y la red Wifi:

La implementación de Redes de Área Local Virtuales (VLANs) trasciende la mera organización administrativa; constituye la ejecución táctica del Principio de Menor Privilegio en las capas de enlace y de red.

Segmentación Lógica de Red y Control de Tráfico Al aislar lógicamente los departamentos, se reduce sustancialmente la superficie de exposición ante posibles ataques. Si un equipo resulta comprometido, la amenaza permanece confinada en su respectiva subred, impidiendo el movimiento lateral hacia la infraestructura crítica o el núcleo del sistema. Asimismo, esta división permite aplicar reglas de Calidad de Servicio (QoS) a medida, reservando ancho de banda garantizado para las aplicaciones esenciales frente al tráfico ordinario.

Protección del Entorno Inalámbrico La implementación del protocolo WPA2 o superior constituye la base mínima para una red Wi-Fi corporativa segura. Mediante la integración del algoritmo de cifrado AES, se previene la interceptación no autorizada (*eavesdropping*), garantizando que los datos transmitidos por el medio inalámbrico permanezcan ininteligibles ante accesos no permitidos.

Estrategia de Seguridad en Capas. La resiliencia operativa se logra articulando múltiples niveles de protección interconectados:

Nivel de Aplicación (Sophos): Se encarga del control de identidades y la inspección de tráfico web, frenando código malicioso y amenazas avanzadas antes de que impacten en los equipos finales.

Nivel de Red y Transporte (MikroTik): Funciona como núcleo de enrutamiento de alto rendimiento, optimizando el flujo de información, reduciendo cuellos de botella y manteniendo la continuidad de la conectividad.

Sostenibilidad y Evolución Tecnológica Una infraestructura optimizada y protegida redefine el valor del área de TI, convirtiéndola en un aliado estratégico para el desarrollo institucional:

Continuidad e Innovación: Al disminuir la frecuencia de fallas e incidentes, el personal técnico abandona las tareas reactivas de contingencia y orienta sus recursos hacia iniciativas de modernización tecnológica.

Optimización Presupuestaria: La estabilidad del entorno prolonga la vida útil de los equipos y minimiza el gasto en soporte técnico correctivo, asegurando un uso más eficiente de la inversión en TI.

4.1.3. Coordinación y gestión con el contratista del acceso ante incidentes y daños.

No se requirió la contratación de servicios externos para la atención de incidentes o daños durante este periodo.

4.2. Realizar actividades relacionadas con el soporte al servicio de Voz Corporativa IP.

Alta Disponibilidad y Continuidad en Telefonía IP La estabilidad y firmeza del sistema de telefonía IP responden a un diseño de infraestructura pensado para la resiliencia y el uso continuo. Al eliminar las interrupciones operativas y optimizar el tráfico de datos, la plataforma se afirma como un recurso clave para la agilidad institucional y la toma de decisiones, previniendo gastos de emergencia o costos no planificados. Esta solidez técnica se fortalece mediante actualizaciones periódicas y mantenimiento

preventivo, corrigiendo vulnerabilidades antes de que comprometan la privacidad y confidencialidad de los datos.

Eficiencia Operativa e Impacto Institucional Más allá de la optimización tecnológica, la madurez de la voz sobre IP reduce los costos de mantenimiento y las solicitudes de soporte correctivo. Al exigir una intervención mínima del personal técnico, el sistema previene riesgos operativos y potencia la productividad cotidiana de la organización. Esto permite reorientar la capacidad analítica y los recursos hacia los objetivos principales de la entidad, con el respaldo de un canal de comunicación continuo y alineado con exigentes estándares de seguridad.

4.2.1. Soporte y mantenimiento semestral al Servidor

Aplazar los mantenimientos preventivos programados responde a la adopción de una estrategia centrada en la confiabilidad y no a una falta de supervisión. En entornos informáticos actuales, las manipulaciones innecesarias en sistemas estables pueden generar fallas inducidas, como la degradación prematura de componentes recién manipulados o desajustes de configuración. Al fundamentar las decisiones en el monitoreo en tiempo real y el análisis predictivo, se protege el equilibrio operativo de la plataforma, evitando intervenciones en equipos sin evidencia de desgaste para resguardar la disponibilidad del servicio.

4.2.2. Aplicación de políticas de uso y acceso a usuario final

La migración de antivirus basados en firmas hacia soluciones EDR con *deep learning* resulta clave ante ataques modernos, como el *ransomware* y las amenazas de día cero, capaces de eludir las defensas tradicionales. Mediante Sophos Intercept X, se habilita el análisis de comportamiento y heurística en tiempo real en los equipos de trabajo. Esta inteligencia distribuida frena acciones maliciosas —incluyendo el cifrado no autorizado de datos— en el propio endpoint, resguardando la información en su origen y acortando sensiblemente el tiempo de respuesta ante incidentes.

Protección Perimetral y Segmentación (Firewall Sophos XGS2100)

La integración del Sophos XGS2100 como eje de la red atiende a la necesidad de mantener visibilidad completa bajo un esquema de *Zero Trust*. Frente al predominio del tráfico cifrado (HTTPS/TLS), la inspección profunda de paquetes previene que los flujos de red oculten cargas maliciosas. Paralelamente, la segmentación en Capas 2 y 3 mediante VLANs y microsegmentación funciona como una barrera táctica: ante la eventual vulneración de un equipo o subred, la amenaza queda aislada lógicamente, conteniendo su avance hacia servidores o activos críticos.

Control de Terceros y Riesgo en la Cadena de Suministro

La regulación del acceso para personal externo resulta crítica para evitar vulnerabilidades en la cadena de suministro. La exigencia de validaciones técnicas previas a dispositivos de terceros (sistemas actualizados, parches vigentes y licencias al día) asegura que los equipos ajenos cumplan con los mismos criterios de higiene digital aplicados internamente. Este filtro preventivo evita el ingreso accidental de malware y convierte el acceso remoto o presencial de colaboradores externos en un canal seguro.

Gobernanza de TI y Cumplimiento Normativo

La consolidación de herramientas defensivas y controles bajo un modelo unificado de Gobernanza de TI fortalece la continuidad operativa de la organización. Una estrategia de defensa en profundidad protege la confidencialidad, integridad y disponibilidad de la información de forma integral. Asimismo, la alineación con estándares internacionales como ISO 27001 eleva el nivel de cumplimiento normativo, reduce el riesgo de caídas operativas y proyecta confianza ante *stakeholders*, posicionando al área de TI como un motor estratégico de valor.

4.2.3. Coordinación y gestión con el contratista del acceso ante incidentes y daños.

El rendimiento destacado de la infraestructura responde al paso de un enfoque reactivo hacia una gestión técnica preventiva. La consolidación de altos niveles de disponibilidad permitió resguardar

las operaciones y eliminar los costos vinculados a fallas críticas, prescindiendo por completo del soporte externo de urgencia y la tramitación de garantías con terceros.

Confiabilidad Técnica e Impacto Institucional

El registro de cero incidentes en la plataforma de cómputo y almacenamiento evidencia la efectividad del monitoreo continuo y las rutinas de mantenimiento preventivo. Esta firmeza operativa protege la integridad de los datos y asegura la disponibilidad del servicio, liberando la capacidad del equipo para enfocarse en iniciativas de innovación y el logro de los objetivos estratégicos de la entidad.

4.2.4. Mantener, actualizar y/o reconfigurar el servidor para que la troncal telefónica funcione adecuadamente y permita el funcionamiento adecuado de las extensiones telefónicas.

La intervención en la plataforma de telefonía IP fortalece simultáneamente la infraestructura interna y la troncal externa, garantizando comunicaciones estables mediante la actualización de su núcleo y el ajuste de los protocolos de señalización. Este proceso elimina vulnerabilidades previas y erradica la pérdida de paquetes, logrando una transmisión de voz clara e ininterrumpida. La reingeniería aplicada dota al sistema de una alta capacidad de escalabilidad, permitiendo absorber la expansión futura de la organización sin degradar la calidad del servicio.

La transición hacia un modelo preventivo fundamentado en la supervisión analítica de registros fortalece la continuidad del negocio al anticipar y mitigar anomalías antes de que afecten la operación. Esta estrategia minimiza las interrupciones no planificadas y resguarda la productividad del personal. Como resultado, la infraestructura de VoIP alcanza un nivel superior de disponibilidad y estabilidad, ofreciendo a los usuarios una experiencia de comunicación continua, ágil y transparente.

4.2.5. Configurar extensiones telefónicas de los funcionarios a los que se le asigna y atender problemas de comunicación.

En el periodo comprendido del 19 de julio al 18 de agosto del 2026 se presentaron dificultades de comunicación en la oficina de aguas con la extensión, la cual se le dio solución cambiando el conector KRJ45 y se le configuró el teléfono.

4.3. Atender fallas y requerimientos en un tiempo máximo de 2 horas hábiles, dependiendo de la criticidad de esta y que sea reportada dentro del horario laboral de CORPOURABA.

El reporte de gestión de tickets correspondiente al periodo del 19 de julio al 18 de agosto de 2026 evidencia una alta efectividad operativa en la atención de solicitudes, destacando el área de Soporte con 57 requerimientos abiertos y 55 cerrados tasa de resolución del 96.5%, aunque registra 16 casos atrasados con tiempos promedio de servicio y respuesta de 48.9 y 58.8 horas, respectivamente. Por su parte, el departamento de Maintenance gestionó un único caso, cerrándose con éxito en un tiempo promedio de servicio y respuesta de 46.0 horas. En términos generales, la operación refleja una notable capacidad de resolución del volumen de casos entrantes, sugiriendo la necesidad de ajustar la asignación de recursos en Soporte para optimizar los tiempos de respuesta y reducir el acumulado de tickets atrasados.

Rango: July 19, 2026 - August 18, 2026 (America/Bogota)

Departamento | Temas | Agente

Departamento	Abierto	Asignado	Atrasado	Cerrado	Reabierto	Borrado	Tiempo de Servicio	Tiempo de Respuesta
Soporte	57	0	16	55	0	0	48.9	58.8
Maintenance	1	0	0	1	0	0	46.0	46.0

Análisis General de Demanda y Resolución

El reporte por temas de ayuda registrado entre el 19 de julio y el 18 de agosto de 2026 evidencia una alta concentración de la carga operativa en soporte de hardware y consultas de usuario, sumando un total de 58 tickets abiertos y 53 cerrados. La categoría con mayor demanda fue *Soporte Impresoras y Scaners* con 23 casos, seguida por *Consulta general* con 14 requerimientos. A pesar de mantener una alta tasa de cierre en ambas áreas, estas dos categorías acumularon la mayor cantidad de demoras, registrando 11 de los 16 tickets atrasados del periodo y tiempos promedio de respuesta superiores a las 65 horas.

Eficiencia Operativa y Tiempos de Atención

El desempeño del servicio refleja marcadas variaciones según la naturaleza del requerimiento. Mientras que las incidencias críticas de conectividad e infraestructura como *Problemas de Red* y *Daño telefónico* se resolvieron de forma óptima en un promedio de 10.5 a 10.8 horas sin generar atrasos, áreas como *Soporte Correo electrónico* e *Informar de un problema* presentaron tiempos atípicos que superaron las 140 horas por caso. En general, la operación demuestra capacidad para absorber el volumen entrante de solicitudes, pero requiere ajustar la asignación de recursos para reducir los cuellos de botella en soporte perimétrico e impresiones.

Rango: July 19, 2026 - August 18, 2026 (America/Bogota)

Departamento | **Temas** | Agente

Temas de ayuda	Abierto	Asignado	Atrasado	Cerrado	Reabierto	Borrado	Tiempo de Servicio	Tiempo de Respuesta
Soporte Impresoras y Scaners	23	0	7	23	0	0	55.6	67.3
Report a Problem	1	0	0	1	0	0	46.0	46.0
Consulta general	14	0	4	13	0	0	57.1	65.7
Problemas de Red	4	0	0	4	0	0	10.8	10.8
Capacitación/Recomendaciones	7	0	2	7	0	0	41.2	49.3
Problemas con la M Y P	3	0	1	3	0	0	16.3	21.0
Soporte Correo electronico	1	0	1	1	0	0	143.0	143.0
Daño telefonico	2	0	0	2	0	0	10.5	10.5
Daño de equipo Computo	1	0	0	1	0	0	0.0	0.0
Informar de un problema	2	0	1	1	0	0	141.0	141.0

5. SISTEMAS, POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD

5.1. Gestión de usuarios creados y eliminados, siguiendo los procesos de seguridad.

5.1.1. Asignar usuario y contraseña para el acceso a la red y/o los aplicativos corporativos a los funcionarios, contratistas o usuarios que sean autorizados por alguno de los directivos, utilizando exclusivamente el formato del SGC designado para ello.

Durante este periodo del 19 de julio al 18 de agosto de 2026 se realizó la creación de los siguientes usuarios.

CREACION DE USUARIOS	
NOMBRE COMPLETO	USUARIO
Georgina Andrea Gamboa Díaz	ggamboa
Sandy Madera Gomez	smadera
Heiler Andres Rios Cuesta	hrios
Luz Janny Rodriguez Castellar	ljrodriguez
Yeferson Paniagua Pulgarin	ypaniagua
Milsis Yodalis Caicedo Chala	mcaicedo
Sammy Corrales Jaramillo	scorrales

5.1.2. Eliminar y/o desactivar los accesos a los funcionarios o contratistas bien sea por ausencia temporal (por solicitud enviada a la oficina de talento humano, contratación, el supervisor o el jefe inmediato) o definitiva (al momento de la firma del formato de retiro).

En lo que respecta a la gestión de identidades y accesos, se informa que durante el periodo reportado se realizó la eliminación o desactivación de las cuenta de usuarios:

USUARIOS O ACCESOS DESACTIVOS
kiris@corpouraba.gov.co

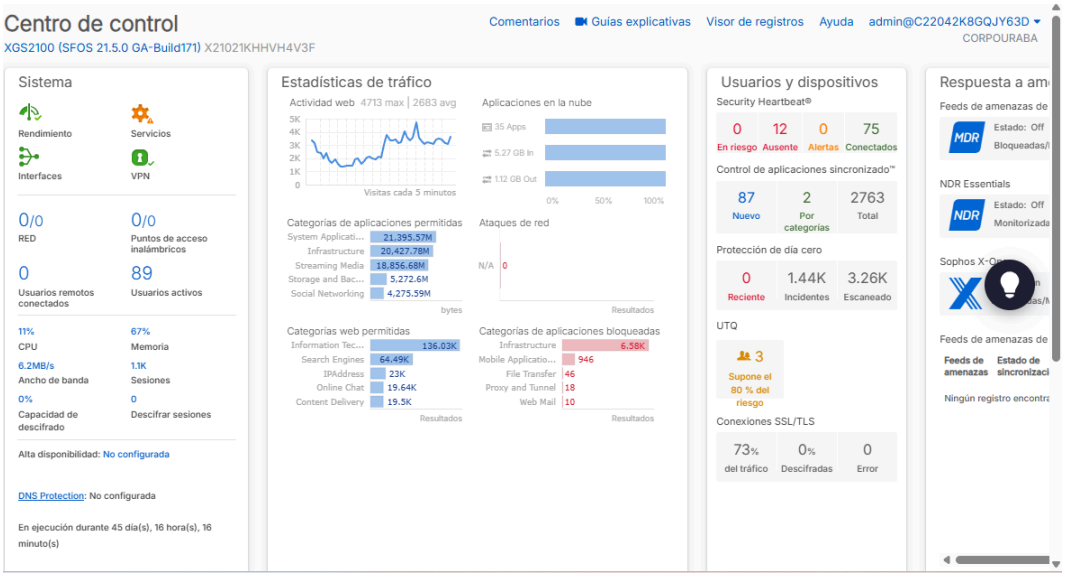
5.1.3. Asigna acceso por VPN a los funcionarios o contratistas autorizados por su superior inmediato o supervisor.

Durante el periodo evaluado, los accesos remotos se gestionaron mediante canales virtuales cifrados, asegurando la confidencialidad e integridad de la información en tránsito. De igual forma, las políticas de control de acceso y el filtrado de navegación web promovieron un uso adecuado y eficiente de los recursos tecnológicos institucionales.

A pesar de las contingencias de red registradas en la sede de Urrao, la infraestructura de seguridad perimetral mantuvo un comportamiento sólido e ininterrumpido. Las defensas bloquearon de manera efectiva cualquier intento de acceso no autorizado, garantizando un entorno digital protegido y la continuidad de las actividades para los funcionarios.

5.2. Realizar actividades para mantener la seguridad perimetral de la corporación:

A continuación, se presenta una gráfica del dashboard del Firewall

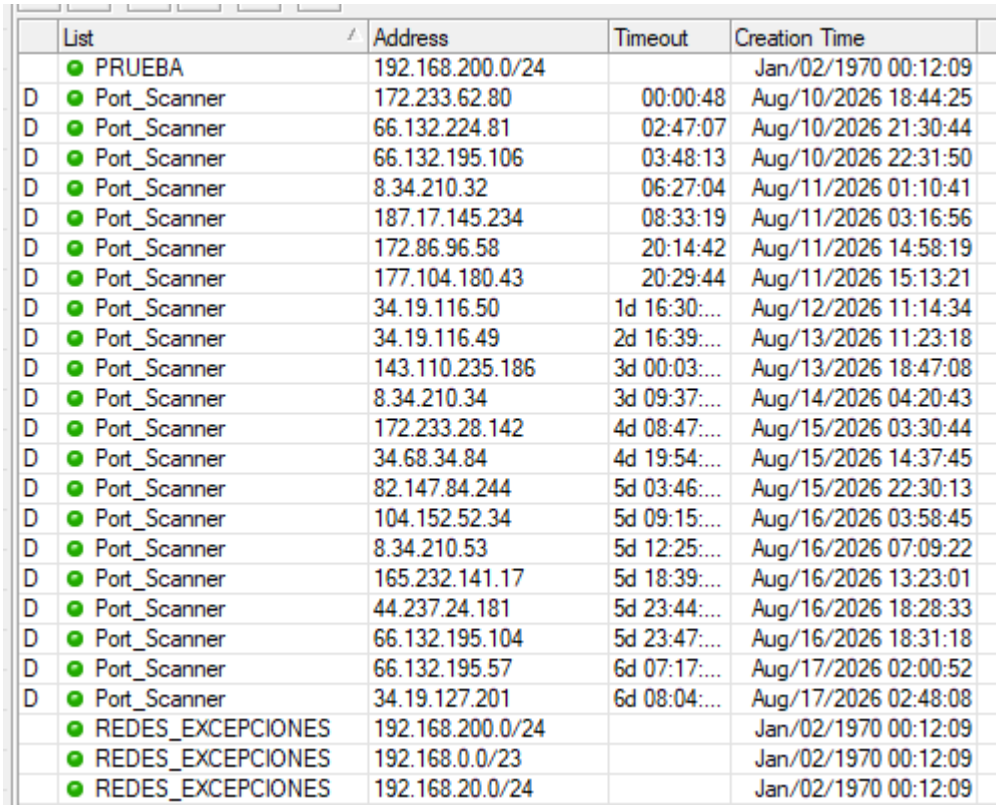


El centro de control del firewall Sophos XGS2100 en CORPOURABA evidencia una infraestructura operativamente estable y con suficiente capacidad de cómputo, registrando un tiempo de actividad continuo de más de 45 días. El consumo de recursos mantiene un margen óptimo de rendimiento con un uso de CPU del 11% y un 67% de memoria RAM, gestionando de forma fluida un ancho de banda de 6.2 MB/s, 1.1K sesiones activas y 89 usuarios conectados. La actividad en la nube alcanza un intercambio de datos de 5.27 GB de entrada y 1.12 GB de salida a través de 35 aplicaciones, donde la mayor carga de transferencia se concentra en aplicaciones del sistema, infraestructura y servicios de streaming. Asimismo, las herramientas de filtrado mantienen un control riguroso sobre las peticiones salientes, destacando el bloqueo preventivo de 6.58K intentos en categorías de infraestructura y cerca de mil accesos no permitidos relacionados con aplicaciones móviles y herramientas de evasión como *proxies* y túneles.

Estado de Seguridad y Control de Amenazas

En materia de ciberseguridad, el ecosistema perimetral reporta una postura sólida y libre de riesgos activos, registrando cero ataques de red directos y cero dispositivos comprometidos entre los 75

equipos conectados mediante *Security Heartbeat*®. A través de los mecanismos de protección de día cero, la plataforma ha analizado un acumulado de 3.26K elementos con 1.44K incidentes evaluados sin detectar amenazas recientes. No obstante, el diagnóstico identifica áreas clave para la optimización técnica: el 73% del tráfico de la red transita bajo cifrado SSL/TLS sin inspección o descifrado activo (0%), lo que podría generar puntos ciegos ante contenido malicioso oculto. Adicionalmente, el indicador de amenaza del usuario, revela que un grupo crítico de solo 3 usuarios concentra el 80% del riesgo en la organización, al tiempo que funciones avanzadas de resiliencia como la alta disponibilidad, la protección DNS y la inspección profunda de datos permanecen pendientes de configuración.



	List	Address	Timeout	Creation Time
	PRUEBA	192.168.200.0/24		Jan/02/1970 00:12:09
D	Port_Scanner	172.233.62.80	00:00:48	Aug/10/2026 18:44:25
D	Port_Scanner	66.132.224.81	02:47:07	Aug/10/2026 21:30:44
D	Port_Scanner	66.132.195.106	03:48:13	Aug/10/2026 22:31:50
D	Port_Scanner	8.34.210.32	06:27:04	Aug/11/2026 01:10:41
D	Port_Scanner	187.17.145.234	08:33:19	Aug/11/2026 03:16:56
D	Port_Scanner	172.86.96.58	20:14:42	Aug/11/2026 14:58:19
D	Port_Scanner	177.104.180.43	20:29:44	Aug/11/2026 15:13:21
D	Port_Scanner	34.19.116.50	1d 16:30:...	Aug/12/2026 11:14:34
D	Port_Scanner	34.19.116.49	2d 16:39:...	Aug/13/2026 11:23:18
D	Port_Scanner	143.110.235.186	3d 00:03:...	Aug/13/2026 18:47:08
D	Port_Scanner	8.34.210.34	3d 09:37:...	Aug/14/2026 04:20:43
D	Port_Scanner	172.233.28.142	4d 08:47:...	Aug/15/2026 03:30:44
D	Port_Scanner	34.68.34.84	4d 19:54:...	Aug/15/2026 14:37:45
D	Port_Scanner	82.147.84.244	5d 03:46:...	Aug/15/2026 22:30:13
D	Port_Scanner	104.152.52.34	5d 09:15:...	Aug/16/2026 03:58:45
D	Port_Scanner	8.34.210.53	5d 12:25:...	Aug/16/2026 07:09:22
D	Port_Scanner	165.232.141.17	5d 18:39:...	Aug/16/2026 13:23:01
D	Port_Scanner	44.237.24.181	5d 23:44:...	Aug/16/2026 18:28:33
D	Port_Scanner	66.132.195.104	5d 23:47:...	Aug/16/2026 18:31:18
D	Port_Scanner	66.132.195.57	6d 07:17:...	Aug/17/2026 02:00:52
D	Port_Scanner	34.19.127.201	6d 08:04:...	Aug/17/2026 02:48:08
	REDES_EXCEPCIONES	192.168.200.0/24		Jan/02/1970 00:12:09
	REDES_EXCEPCIONES	192.168.0.0/23		Jan/02/1970 00:12:09
	REDES_EXCEPCIONES	192.168.20.0/24		Jan/02/1970 00:12:09

La información compartida corresponde a las listas de direcciones IP configuradas en un dispositivo de red MikroTik RouterOS, en donde se evidencian dos tipos de registros claramente diferenciados. En el primer bloque destaca la acumulación dinámica de direcciones IP públicas clasificadas bajo la etiqueta **Port_Scanner**, creadas automáticamente a partir de reglas del Firewall encargadas de detectar escaneos de puertos en tiempo real. La tabla muestra una constante actividad maliciosa o de

exploración proveniente de internet entre los días 10 y 17 de agosto de 2026, asignándoles un tiempo de vida temporal de hasta 7 días antes de caducar. Esto evidencia una estrategia activa de ciberseguridad defensiva, bloqueando o mitigando intentos de intrusión de hosts externos que intentan mapear los servicios vulnerables del router o de la red interna.

Por otro lado, la segunda sección expone las reglas estáticas registradas bajo el nombre **REDES_EXCEPCIONES** junto con una entrada inicial de prueba denominada **PRUEBA**, las cuales abarcan rangos de red privada como `192.168.200.0/24`, `192.168.0.0/23` y `192.168.20.0/24`. Estas entradas no cuentan con un temporizador y presentan una fecha de creación genérica `Jan/02/1900` o `Jan/02/1970`, lo cual es un comportamiento típico en dispositivos MikroTik cuando se aplican configuraciones antes de la sincronización del tiempo mediante un servidor NTP. La finalidad de esta lista es servir como una "Lista Blanca" dentro de las reglas del cortafuegos, permitiendo que el tráfico proveniente o dirigido a estas subredes locales quede excluido de las restricciones de seguridad, evitando falsos positivos o bloqueos accidentales contra los usuarios e infraestructura legítima de la organización.

5.2.1. Actualizar y/o instalar las licencias adquiridas por la corporación para la seguridad perimetral (Antivirus, Antispam, Firewall y API), tanto en las consolas como en los equipos de usuario final que apliquen.

Durante el período evaluado no se realizó la renovación de las licencias de seguridad perimetral Sophos, ya que estas licencias fueron instaladas en periodos anteriores.

5.2.2. Se prioriza la seguridad de la VPN con autenticación de doble vía o mediante conexión directa entre enrutadores

La arquitectura de red propuesta es técnicamente sólida y se alinea con los estándares modernos de Defensa en Profundidad y Confianza Cero, ya que no deposita la seguridad en una sola barrera. Por un lado, la implementación de túneles VPN Site-to-Site garantiza la confidencialidad e integridad de los datos en tránsito mediante cifrado robusto, neutralizando eficazmente cualquier

intento de interceptación entre la oficina principal y las sedes regionales. Por el otro, la exigencia de Autenticación de Doble Factor a través de Sophos Authenticator actúa como un control de identidad crítico, blindando el acceso remoto contra credenciales comprometidas y asegurando de manera categórica que solo el personal autenticado e inequívocamente validado pueda interactuar con la infraestructura interna.

Al fusionar este canal de transporte seguro con políticas estrictas de control de acceso, la organización no solo reduce drásticamente su superficie de ataque, sino que también garantiza la continuidad del negocio y la alta disponibilidad de sus recursos críticos. Esta sinergia técnica evita interrupciones operativas causadas por intrusiones o brechas de seguridad, permitiendo que los sistemas sigan operando con total fluidez incluso en escenarios de alta exigencia o congestión de la red. Además, este enfoque estructurado y auditable facilita el cumplimiento de normativas de seguridad de la información, proyectando una infraestructura tecnológica madura, resiliente y preparada para enfrentar las amenazas cibernéticas actuales de forma proactiva.

5.2.3. Informar y corregir oportunamente los incidentes de seguridad informática tales como virus, ataques de denegación de servicio, accesos no autorizados, y otros relevantes.

When	Threat Name	Event	Severity	Alert	Device
2026-08-18T17:27:25-05:00	HollowProcess	'HollowProcess' malicious behavior prevented in Windows PowerShell	Low	No	admin
2026-08-18T16:20:28-05:00	Lockdown	'Lockdown' exploit prevented in Canva-Setup-1.123.1.exe	Low	No	JOHANNA-juridica
2026-08-14T08:32:52-05:00	Mal/HTMLGen-A	Access was blocked to "positiva-chat.vercel.app" because of "Mal/HTMLGen-A".	Low	No	DESKTOP-6H84027
2026-08-13T17:24:28-05:00	Mal/JSInject-SG	Access was blocked to "www.merida.tecnm.mx" because of "Mal/JSInject-SG".	Low	No	SGAA-elizabeth
2026-08-12T22:52:33-05:00	Mal/HTMLGen-A	Access was blocked to "moonlighthathel.org" because of "Mal/HTMLGen-A".	Low	No	SGAA-ANA-RAVE
2026-08-12T22:22:21-05:00	Mal/HTMLGen-A	Access was blocked to "spendsdetachment.com" because of "Mal/HTMLGen-A".	Low	No	SGAA-ANA-RAVE
2026-08-12T22:19:16-05:00	Mal/HTMLGen-A	Access was blocked to "unlairouting.com" because of "Mal/HTMLGen-A".	Low	No	SGAA-ANA-RAVE
2026-08-12T22:19:14-05:00	Mal/HTMLGen-A	Access was blocked to "workdeadlinededicate.com" because of "Mal/HTMLGen-A".	Low	No	SGAA-ANA-RAVE
2026-08-12T16:56:01-05:00	Mal/HTMLGen-A	Access was blocked to "backend.biosolutions.com.co" because of "Mal/HTMLGen-A".	Low	No	JOSE-LABORATORIO
2026-08-12T15:23:34-05:00	Mal/Generic-S	Malware detected: 'Mal/Generic-S' at 'C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe'	Medium	No	correo
2026-08-12T14:02:22-05:00	Mal/HTMLGen-A	Access was blocked to "loadway.best" because of "Mal/HTMLGen-A".	Low	No	Control-interno
2026-08-12T13:03:04-05:00	DynamicShellcode	'DynamicShellcode' exploit prevented in Node.js JavaScript Runtime	Low	No	ERIKA-JURIDICA
2026-08-12T09:45:32-05:00	Mal/HTMLGen-A	Access was blocked to "loadway.best" because of "Mal/HTMLGen-A".	Low	No	JURIDIC-ERIKAH
2026-08-12T07:30:55-05:00	Mal/HTMLGen-A	Access was blocked to "loadway.best" because of "Mal/HTMLGen-A".	Low	No	CARMEN-PLANEACION
2026-08-11T11:03:04-05:00	Exec_19e (T1218.005)	'Exec_19e (T1218.005)' malicious behavior detected in 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe'	High	No	PARAMO-SAF
2026-08-11T09:40:49-05:00	Mal/HTMLGen-A	Access was blocked to "loadway.best" because of "Mal/HTMLGen-A".	Low	No	NUTIBARA-mariaisabel
2026-08-10T16:56:36-05:00	Lockdown	'Lockdown' exploit prevented in Microsoft Edge	Low	No	FLORA-ALVARO
2026-08-10T08:18:41-05:00	Mal/HTMLGen-A	Access was blocked to "loadway.best" because of "Mal/HTMLGen-A".	Low	No	flora-2
2026-08-06T17:07:11-05:00	Mal/HTMLGen-A	Access was blocked to "loadway.best" because of "Mal/HTMLGen-A".	Low	No	SGAA-Secretaria

2026-08-05T21:08:27-05:00	Mal/HTMLGen-A	Access was blocked to "veintones.com" because of "Mal/HTMLGen-A".	Low	No	LAPTOP-R4QR61M3
2026-08-04T15:09:57-05:00	Mal/HTMLGen-A	Access was blocked to "loadway.best" because of "Mal/HTMLGen-A".	Low	No	CONTRATACION-HECTOR
2026-08-03T08:09:13-05:00	Mal/HTMLGen-A	Access was blocked to "adexchangerapid.com" because of "Mal/HTMLGen-A".	Low	No	eperez-nutibara
2026-07-29T17:37:30-05:00	Mal/HTMLGen-A	Access was blocked to "universityshocksooner.com" because of "Mal/HTMLGen-A".	Low	No	eperez-nutibara
2026-07-29T17:33:03-05:00	Mal/HTMLGen-A	Access was blocked to "artistapirata.app" because of "Mal/HTMLGen-A".	Low	No	ComunicacionesCORPOURABA
2026-07-29T06:14:50-05:00	DynamicShellcode	'DynamicShellcode' exploit prevented in Node.js JavaScript Runtime	Low	No	MIRLEYS-JURIDICA
2026-07-28T10:35:28-05:00	Cleanup_3b (T1059.003)	'Cleanup_3b (T1059.003)' malicious behavior detected in 'c:\users\dgarrido\appdata\local\temp\f6f30898-4a19-4d4e-b109-6f734e5ddaa1_impuesto predial pendiente de turbo - antioquia.zip.aa1\impuesto predial pendiente de turbo - antioquia.bat'	High	No	OSMANY-ALMACEN
2026-07-28T10:35:28-05:00	Evade_53a (T1036)	'Evade_53a (T1036)' malicious behavior detected in 'C:\Users\dgarrido\AppData\Roaming\SetupFiles\vijewyufveonabghulluonouceyasi.exe'	High	No	OSMANY-ALMACEN
2026-07-28T10:35:21-05:00	Cleanup_3b (T1059.003)	'Cleanup_3b (T1059.003)' malicious behavior detected in 'c:\users\dgarrido\appdata\local\temp\4a40a0de-8ebe-489c-bf0b-83bf38cbd0d5_impuesto predial pendiente de turbo - antioquia.zip.0d5\impuesto predial pendiente de turbo - antioquia.bat'	High	No	OSMANY-ALMACEN
2026-07-28T10:35:21-05:00	Cleanup_3a (T1059.001)	'Cleanup_3a (T1059.001)' malicious behavior detected in 'c:\users\dgarrido\appdata\local\temp\aqxuklgowzoifs.ps1'	High	No	OSMANY-ALMACEN
2026-07-28T10:35:21-05:00	Cleanup_11a (T1059.010)	'Cleanup_11a (T1059.010)' malicious behavior detected in 'c:\users\dgarrido\appdata\roaming\setupfiles\wwmaw'	High	No	OSMANY-ALMACEN
2026-07-28T08:28:31-05:00	Mal/HTMLGen-A	Access was blocked to "workdeadlinededicate.com" because of "Mal/HTMLGen-A".	Low	No	SGAA-EDINSON
2026-07-27T10:52:21-05:00	Lockdown	'Lockdown' exploit prevented in Canva-Setup-1.123.0.exe	Low	No	JOHANNA-juridica
2026-07-27T10:27:58-05:00	Mal/HTMLGen-A	Access was blocked to "spendsdetachment.com" because of "Mal/HTMLGen-A".	Low	No	SGAA-EDINSON
2026-07-27T09:11:16-05:00	Generic Reputation PUA	PUA detected: 'Generic Reputation PUA' at 'C:\Users\aramirez\Downloads\wps_office_inst.exe'	Medium	No	FLORA-ALVARO
05:00	Lockdown	'Lockdown' exploit prevented in Microsoft Excel	Low	No	PARAMO-SAF

El registro de eventos de seguridad (SIEM/EDR) muestra actividad detectada entre el 27 de julio y el 18 de agosto de 2026. A pesar de que los controles automatizados han bloqueado la mayoría de los eventos de severidad baja, existen **incidentes críticos activos y persistentes de severidad alta** que requieren intervención técnica inmediata.

hallazgos Clave y Nivel de Riesgo

Criterio	Resumen del Hallazgo	Nivel de Riesgo
Ataque de Phishing Focalizado (Impuesto Predial)	Infección deliberada en el equipo OSMANY-ALMACEN vía archivo .zip con ingeniería social local (impuesto predial pendiente de turbo - antioquia). Ejecución de scripts Malicious PowerShell/LNK.	**CRÍTICO / ALTO**

Abuso de PowerShell / Ejecución Malik	Ejecución de comportamiento malicioso en powershell.exe detectado en el servidor/equipo crítico PARAMO-SAP (Exec_190).	**CRÍTICO / ALTO**
Aplicaciones Potencialmente No Deseadas (PUA)	Descarga de herramientas no autorizadas como *WPS Office*.	**MEDIO**
Navegación / Mal/HTMLGen-A	Intentos continuos de conexión a dominios maliciosos (ej. loadway.best, worlddeadlinededicate.com).	**BAJO** (Bloqueado)

Análisis Detallado de Incidentes Críticos

Infección Activa por Phishing Local (OSMANY-ALMACEN)

- **Fecha:** 2026-07-28 10:45:21 - 10:45:28
- **Vectores y Amenazas:** Cleanup_1b, Evade_1a, Cleanup_11a.
- **Detalle:** El usuario abrió un archivo descargado (...impuesto predial pendiente de turbo - antioquia.zip.bat), activando scripts persistentes en carpetas del sistema (AppData\Local\Temp y AppData\Roaming). Incluye evasión de defensas (Evade_1a) y tareas de persistencia (cleanup_11a).

Amenaza en Infraestructura Core (PARAMO-SAP)

- **Fecha:** 2026-08-11 13:05:04
- **Amenaza:** Exec_190 (T1218.005)
- **Detalle:** Comportamiento malicioso detectado en el binario nativo de Windows (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe). Indica un posible ataque *Living off the Land* (LotL) intentando ejecutar comandos o scripts maliciosos directamente en el servidor/equipo del sistema SAP.

Actividad PUA y Gestión de Software Unverified

Equipos: COMTIC PLANEACIÓN, FLORA-ALVARO.

Detalle: Se identificó la descarga e instalación de herramientas como wps_office_inst.exe.

5.2.4. Tomar las acciones para que, en caso de ser incidentes que afecten la seguridad, informar inmediatamente al oficial de seguridad de la información, controlar el incidente, evitar su replicación, controlar los daños y/o alertar a los usuarios y/o a las autoridades respectivas

La continuidad y estabilidad de la infraestructura digital se mantuvieron gracias a un enfoque de seguridad integral que unió la automatización técnica con la capacitación del personal.

Protección tecnológica: Se implementaron sistemas de defensa autónomos y un monitoreo perimetral permanente que neutralizaron ataques externos y escaneos de puertos en tiempo real, sin requerir intervención manual.

Factor humano: Los programas de formación preventiva capacitaron al personal para detectar y mitigar a tiempo amenazas avanzadas como el *phishing*.

Este blindaje conjunto de la tecnología y el talento humano aseguró la protección de los datos institucionales y la continuidad operativa, cerrando el periodo sin fallas críticas en los sistemas.

Recomendación:

Para ejecutar el plan de contención, se debe aislar de forma inmediata de la red a los equipos **OSMANY-ALMACEN** y **PARAMO-SAP**, procediendo con la reinstalación del sistema operativo del primero por riesgo de persistencia y la auditoría de eventos de PowerShell (Event ID 4104) en el segundo. Complementariamente, se deben endurecer las políticas de seguridad mediante AppLocker/SRP para bloquear la ejecución de scripts y archivos comprimidos en carpetas de usuario (`AppData`,

`Downloads`, `Temp`), además de revocar privilegios administrativos locales para prevenir el uso de herramientas no autorizadas.

5.2.5. Realizar informe mensual de incidentes presentados, indicando las acciones para su corrección y ejecutando charla con los funcionarios involucrados.

El informe confirma la solidez de las defensas digitales al neutralizar automáticamente amenazas como *exploits* y sitios web peligrosos, garantizando la continuidad del negocio. Este soporte técnico se combinó con una estrategia educativa que utilizó los incidentes detectados para brindar capacitación personalizada y asistencia directa al personal, transformando los riesgos en aprendizaje práctico para fortalecer la cultura preventiva y proteger tanto los sistemas como al equipo humano

5.2.6. Verificar que todos los equipos corporativos cuenten con la instalación completa y vigente de las actualizaciones de seguridad del sistema operativo y del antivirus.

Mantenimiento y Refuerzo de la Seguridad Informática Corporativa

La robustez institucional de la organización es el resultado directo de una infraestructura tecnológica automatizada y preventiva. Con Sophos Endpoint como base defensiva, la entidad supera el esquema reactivo convencional para adoptar un modelo capaz de detener amenazas avanzadas en tiempo real de forma autónoma. Esta capacidad operativa minimiza la dependencia de la supervisión manual continua, protegiendo los activos digitales y consolidando la ciberseguridad como un eje estratégico fundamental para preservar la operatividad y la continuidad del negocio.

Asimismo, la sostenibilidad de este esquema de protección se fundamenta en una eficiente gestión de recursos y mitigación de riesgos. Durante el proceso de renovación paulatina del equipamiento informático, la organización aplica políticas de endurecimiento y actualización prioritaria en los dispositivos más vetustos. Esta táctica integral previene vulnerabilidades en la fase de transición, garantizando que todos los puntos de la red conserven la seguridad necesaria para resguardar la información

crítica del organismo.

5.2.7. Verificar que los equipos que no son de la Corporación y que quieran conectarse a la red principal de la corporación (Admin) tengan instalada la licencia legal de antivirus (versión pagada) y si es funcionario en teletrabajo que el software del equipo sea legal.

Durante el período evaluado no se presentó una solicitud de conexión a la red principal de equipos externos a la corporación.

6. EQUIPOS DE USUARIO FINAL

6.1. Resumen de atención de la mesa de servicio

6.1.1. Establecer el servicio de atención al usuario en sitio (Instalaciones de la Entidad) o remoto (territoriales), prestado por recurso humano con formación, experiencia, habilidades y conocimientos específicos y relacionados en servicios de soporte de TI.

El actual esquema de soporte técnico impulsa la productividad institucional gracias a un equipo capacitado para resolver de forma autónoma incidencias de nivel 1 y 2. Su modelo híbrido combina la atención presencial e inmediata en la sede principal con asistencia remota para las oficinas territoriales, garantizando un servicio equitativo y eficiente.

Esta estrategia optimiza los recursos al reducir costos operativos y tiempos de desplazamiento mediante herramientas digitales como videollamadas. Así, la organización asegura la estabilidad tecnológica y el cumplimiento de sus objetivos en todas sus sedes.

6.1.2. Este es el punto de contacto inicial del usuario con la mesa de servicios de TI, dotado con las herramientas técnicas de hardware y software especializado para el registro y atención de los tickets presentados por los funcionarios y contratista, debe permitir el acceso remoto de equipos de cómputo, además del puesto de

trabajo (mobiliario y herramientas) necesario para la prestación del servicio.

Entre el 19 de julio y el 18 de agosto de 2026, la Mesa de Servicios de TI de COMTIC se consolidó como el pilar fundamental del soporte tecnológico en CORPOURABÁ. Mediante la unificación del servicio, se estableció un marco de gestión que garantiza una atención rápida, clara y totalmente rastreable. El trabajo conjunto de personal capacitado y recursos tecnológicos de vanguardia impulsa la transformación digital como motor directo de la eficiencia en la institución.

La implementación de OsTicket va más allá del simple seguimiento de tiquetes, convirtiéndose en una herramienta clave para la documentación y la inteligencia de datos. Este enfoque analítico permite evolucionar de un soporte reactivo a una gestión predictiva. De este modo, la información histórica de los incidentes se aprovecha para tomar decisiones informadas, optimizar la asignación de recursos y corregir fallas de infraestructura antes de que afecten la operación regular.

La capacidad de respuesta de la entidad se incrementó sustancialmente gracias a la asistencia remota controlada. Este esquema elimina las limitaciones por distancia física y disminuye los tiempos perdidos por traslados, brindando soporte en tiempo real para sostener la productividad. La combinación de esta atención a distancia con una infraestructura de red de alta disponibilidad asegura la continuidad operativa de las áreas críticas frente a eventualidades.

El verdadero valor de una arquitectura tecnológica radica en su capacidad de adaptarse al crecimiento organizacional sin generar cuellos de botella. La flexibilidad y escalabilidad de la Mesa de Servicios ratifican su importancia, ya que permiten absorber un mayor volumen de solicitudes preservando los niveles de servicio. Esto garantiza que las herramientas tecnológicas continúen impulsando el logro de los objetivos y el mantenimiento de las exigencias de calidad institucional.

6.1.3. Implementar el sistema de control de solicitudes mediante el uso de tickets (aplicativo con acceso a todos los funcionarios).

La puesta en marcha oficial de la plataforma **OsTicket (v1.18.2)** representa un avance significativo en la evolución tecnológica de la entidad, al establecer un entorno de gestión de servicios caracterizado por su alta capacidad de seguimiento y eficacia. El uso de esta versión en particular asegura la firmeza operativa del sistema y permite el aprovechamiento de herramientas de diagnóstico y generación de informes que convierten las asistencias técnicas en información clave para la planeación estratégica.

Al unificar el soporte técnico exclusivamente mediante el enlace institucional **http://soporte.corpouraba.gov.co/upload**, se establece un medio de contacto oficial que evita la fragmentación de las peticiones y asegura que cada trámite cuente con un registro detallado desde el inicio hasta su cierre. Esta organización permite que el área de TI de **COMTIC** funcione como un pilar de transparencia y responsabilidad, proporcionando a los integrantes de **CORPOURABÁ** un acceso uniforme, rápido y totalmente verificable para la atención de sus requerimientos digitales.

6.1.4. Atender las solicitudes realizadas por correo o telefónicamente y capacitar a los usuarios para que las presenten por el sistema de tickets.

La transición desde los canales tradicionales (correo y teléfono) hacia la plataforma unificada OsTicket v1.18.2 está plenamente justificada, ya que erradica la dispersión de información y el riesgo de pérdida de datos inherentes a los métodos convencionales. Al centralizar de forma obligatoria todas las solicitudes en un único punto de contacto y respaldar este cambio con un Programa Integral de Formación, la organización no solo asegura la continuidad operativa, sino que instaura una cultura de rigor, transparencia y seguridad. Este control estricto permite supervisar con precisión los Acuerdos de Niveles de Servicio (SLA), garantizando que cada requerimiento técnico reciba una atención puntual, organizada y medible que optimiza la productividad del departamento de TI.

Por otra parte, el verdadero valor estratégico de este ecosistema digital radica en su capacidad para transformar el soporte técnico cotidiano en un activo de inteligencia institucional. Al consolidar un

repositorio unificado y preciso de incidentes, el sistema trasciende el simple registro operativo para convertir los datos estadísticos en Indicadores Clave de Desempeño (KPIs) y capacidades analíticas profundas. Esta visibilidad predictiva y estructurada dota a la alta gerencia de herramientas fundamentales para la planificación a largo plazo y la toma de decisiones informadas, garantizando una infraestructura de servicios flexible, eficiente y alineada con los más altos estándares de excelencia corporativa.

6.1.5. Atender las solicitudes por orden de registro y priorizar los problemas graves que afecten la seguridad informática de la corporación, el servicio o la seguridad del funcionario, posibles pérdidas de equipos, entre otras.

El modelo de gestión de la Mesa de Servicios está plenamente justificado porque logra un equilibrio óptimo entre la justicia operativa y la mitigación de riesgos críticos dentro de la organización. Al fundamentar la atención en el orden cronológico, se instituye un flujo de trabajo transparente y equitativo para todos los funcionarios; sin embargo, al complementar esta base con un sistema de categorización por impacto y una línea prioritaria para la Alta Dirección, el soporte técnico deja de ser un simple tramitador de turnos para convertirse en un escudo estratégico. Esta flexibilidad es indispensable, ya que anteponer las fallas que amenazan la seguridad digital, la continuidad del negocio o las herramientas de la gobernanza ejecutiva asegura que los recursos técnicos limitados se concentren exactamente donde el daño institucional podría ser mayor, protegiendo la estabilidad general y garantizando que la tecnología respalde sin interrupciones la misión de la entidad.

6.1.6. Dar prioridad a las solicitudes realizadas por los directivos de la entidad.

El modelo de soporte prioritario implementado por COMTIC trasciende la mera resolución de incidentes técnicos para posicionarse como un mecanismo de resguardo estratégico, cuyo fin es sostener la continuidad de la Alta Dirección. Dado que los ejecutivos concentran el flujo de información y la toma de

decisiones, cualquier interrupción en sus herramientas digitales representa un riesgo directo para la gobernanza de la entidad.

Al garantizar una respuesta inmediata y continua ante fallas informáticas, se mitigan contingencias que podrían obstaculizar el cumplimiento de las metas institucionales. De este modo, la atención tecnológica especializada actúa como un facilitador clave de la gestión operativa, asegurando que el liderazgo directivo mantenga el dinamismo, la precisión y la fluidez requeridos para responder a las exigencias del entorno.

6.1.7. Presentar y analizar informes mensuales sobre los tickets ingresados y resueltos con tiempo de respuesta.



Rango: July 19, 2026 - August 18, 2026 (America/Bogota)

Departamento | Temas | Agente

Departamento	Abierto	Asignado	Atrasado	Cerrado	Reabierto	Borrado	Tiempo de Servicio	Tiempo de Respuesta
Soporte	57	0	16	55	0	0	48.9	58.8
Maintenance	1	0	0	1	0	0	46.0	46.0

En el periodo comprendido entre el 19 de julio y el 18 de agosto de 2026, el desempeño de los departamentos de soporte técnico y mantenimiento muestra una disparidad abrumadora en cuanto al volumen de gestión y la carga operativa. El departamento de Soporte concentra la gran mayoría de la actividad con un total de 57 casos abiertos y 55 cerrados, lo que evidencia una alta dinámica de resolución, aunque también enfrenta una presión considerable reflejada en los 16 tickets que se encuentran actualmente atrasados. Esta sobrecarga contrasta notablemente con el área de Maintenance, la cual registra una participación mínima con apenas un caso abierto y un caso cerrado, sin reportar ningún tipo de retraso. En cuanto a las métricas de eficiencia temporal, el departamento de Soporte presenta un tiempo de servicio de 48.9 y un tiempo de respuesta de 58.8, cifras ligeramente superiores a las de Maintenance, que mantiene un promedio de 46.0 tanto en tiempo de servicio como de respuesta. Estos datos sugieren que, a pesar de gestionar un flujo masivo de incidencias que supera exponencialmente al de mantenimiento, el departamento de Soporte logra sostener tiempos operativos relativamente estables, aunque la acumulación de casos atrasados requiere una

optimización en la asignación de recursos para evitar cuellos de botella a corto plazo.

6.2. Diligenciamiento de los conceptos de baja de los equipos y periféricos, firmados por alguno de los profesionales.

Durante el periodo del 19 de julio del 2026 al 18 de agosto de 2026 no se presentaron bajas en equipos.

6.2.1. Habilitar, Configurar e Instalar equipos nuevos de usuario final: computadores, impresoras, periféricos, software (sistema operativo, Antivirus, lectores pdf, controladores y licencias de office entre otros).

Durante este periodo se instaló una impresora nueva en la dependencia de flora.

HP LaserJet MFP M426fdw

6.2.2. Realizar el mantenimiento preventivo a 30 equipos de usuario final, incluyendo periféricos como impresoras, escáner y proyectores de video.

Durante este periodo no se realizó mantenimiento preventivo.

6.2.3. Mantenimiento y limpieza:

Mantenimiento y Limpieza de Equipos de Usuario Final

Durante el ciclo comprendido entre el 19 de julio y el 18 de agosto de 2026, se pretende continuar con el cronograma de mantenimiento preventivo y correctivo.

Sede	Procesos	Mayo				Junio				Julio				Agosto			
		SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4
Apartadó	Fauna		x	x													
	Aguas				x	x											
	Financiera						x										
	Juridica							x	x								
	SCGA									x							
	Planeación									x							
	Impresora/Escaner																x
Hogar de paso											x						
Laboratorio											x						
San Pedro												x					
Atrato*													x				
Cañasgorda														x			
Urrao															x		
Caribe																x	
*Sede Atrato debe hacer llegar los equipos de computo al area de TI Apartadó																	

Mantenimiento y Limpieza del Centro de Datos

Durante este período, no se realizaron tareas de limpieza en el Centro de Datos..

6.2.4. Otras labores adicionales:

En este periodo, la operación alcanzó con precisión las metas establecidas gracias a la mitigación oportuna de riesgos. Al no registrarse imprevistos ni demandas extraordinarias, se gestionan con eficiencia los recursos financieros y el personal. Esto confirma que los procesos actuales son efectivos y garantizan el cumplimiento de los compromisos institucionales sin desvío de recursos.

6.3. Realizar el mantenimiento correctivo a los equipos de TI de la corporación.

Durante este período se realizó mantenimiento correctivo a dos impresoras de la dependencia o subdirección de Gestión Ambiental (SGA)





6.3.1. Presentar el diagnóstico y presupuesto para reparación y suministro de repuestos. (Los costos de los diagnósticos que requieran efectuarse por fuera de la Corporación serán asumidos por esta incluyendo el transporte).

Durante este período no se realizó el diagnóstico de equipos de impresión.

6.3.2. Suministro de repuestos y/o partes de equipos identificados en los diagnósticos previa aprobación del estudio de mercado por parte del supervisor del contrato, visto bueno del subdirector y disponibilidad de recursos.

Durante el período del 19 de julio al 18 de agosto del 2026 no se suministro repuestos o partes de equipos

6.3.3. Identificar equipos próximos a obsolescencia.

Equipos identificados como obsoletos (persisten)

Placa /serie	Último inventario	Computador	Usuario	Sistema Operativo	RAM (MB)	CPU (MHz)	Año
258	15/05/2025 13:32	SGAA-EDUARDOO	sguardo	Microsoft Windows 10 Pro	16384	3401	2013
443	19/05/2025 15:39	NEG-AMANDA	aescobar	Microsoft Windows 10 Pro	8192	3401	2012
765	19/05/2025 13:25	JURIDIC-YANETH		Microsoft Windows 10 Pro	8192	3401	2013

887	16/05/2025 5:11	FLORA-ALVARO		Microsoft Windows 10 Pro	8192	3401	2013
962	19/05/2025 17:18	PLANEA-RICAURTE	rmiranda	Microsoft Windows 7 Professional	6144	2901	2013
0587	19/05/2025 12:40	LABORATORIO-HP	dcuervo	Microsoft Windows 7 Professional	8192	3601	2014
337	25/04/2025 14:55	FLORA-FLOR	fbedoya	Microsoft Windows 7 Professional	4096	2701	2016

6.3.4. Identificar equipos que puedan re-potenciarse.

Tras una auditoría de rendimiento, se identificaron estaciones de trabajo con un desempeño inferior a los estándares operativos necesarios.(persisten)

Situación actual: Equipos con desempeño por debajo del estándar debido a obsolescencia de componentes de almacenamiento (Discos Mecánicos).

Usuarios afectados: Valencia, Álvaro Ramírez, Amanda Escobar.

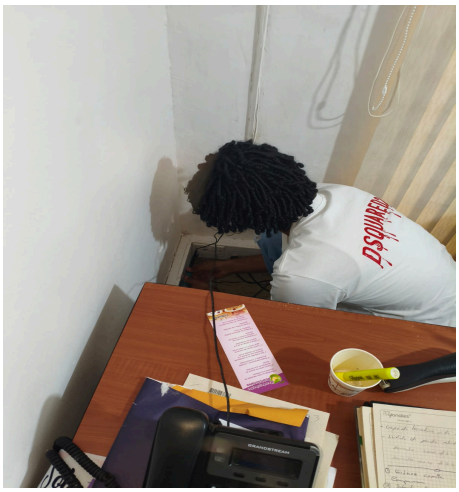
Solución propuesta: Implementación de unidades de estado sólido (SSD).

Beneficio esperado: Eliminación de cuellos de botella en el procesamiento y optimización del tiempo laboral.

esperemos que los mantenimientos correctivos y preventivos podamos identificar otros equipos.

6.3.5. Realizar la reparación de equipos (desktop, laptop, impresoras entre otros) siempre y cuando puedan ser reparados por personal del contratista directamente en sitio (los repuestos deben ser suministrados por la Corporación).

Durante el periodo reportado, se han realizado soporte a equipos a daños leves, que se les ha dado solución inmediata. y mantenimiento y limpieza impresoras





6.3.6. Actualizar la hoja del bien que se encuentra en el SGC cada que se realice un cambio de partes y/o se dé de baja un equipo de la corporación.

Se han actualizado las hojas de vida del personal con las modificaciones correspondientes.

El siguiente enlace permite acceder a la información actualizada:

https://drive.google.com/drive/folders/1JPF5oYTm-hNqx2ZF1LQIxbIhVRzsnxYB?usp=drive_link

6.3.7. Realizar la capacitación para la operación de equipos y dispositivos administrados por el contratista.

La ciberseguridad actual exige más que tecnología; requiere fortalecer el factor humano. Por ello, hemos reforzado nuestro plan de acción mediante la capacitación continua del personal para identificar y neutralizar amenazas proactivamente. Al combinar herramientas técnicas avanzadas, protocolos actualizados y un equipo preparado, consolidamos un entorno de trabajo seguro donde la prevención y la reducción de riesgos forman parte de la cultura diaria. con la estrategia de sensibilización para identificar amenazas o correos maliciosos a través de campañas de ciberseguridad que se inicia a partir del mes de agosto.

7. VISITAS DE SEGUIMIENTO

Asistentes:
Director Corpouraba
Coordinador del Contrato: Juan Carlos Camacho

TEMAS:

- Revisión de la Infraestructura TIC

La revisión de la infraestructura TIC evidencia riesgos concentrados en tres frentes: obsolescencia de servidores y sistemas operativos, saturación de recursos en servicios críticos y capacidad insuficiente de conectividad. En paralelo, existen necesidades de modernización del portal web, red Wi-Fi, respaldo eléctrico, auditorio y red de datos del área de Flora.

Se recomienda ejecutar la intervención por etapas, priorizando continuidad operativa y ciberseguridad antes que las mejoras de experiencia de usuario considerando lo siguiente:

Prioridad	Iniciativa	Riesgo que atiende	Decisión recomendada
P1 – Urgente	Servidores SINAP, Directorio Activo y Proxmox	Obsolescencia, saturación y continuidad	Aprobar diseño/migración y ventana de ejecución
P1 – Urgente	Internet principal	Capacidad insuficiente / disponibilidad	Validar 200 Mbps, SLA y redundancia
P2 – Prioritaria	Portal web institucional	Cumplimiento, seguridad, accesibilidad y experiencia	Aprobar alcance por fases y criterios de aceptación
P2 – Prioritaria	Red Wi-Fi sede principal	Obsolescencia y cobertura	Validar diseño RF, licencias y PoE
P2 – Prioritaria	Baterías de UPS	Pérdida de autonomía	Programar reemplazo preventivo
P3 – Necesaria	Audio y video auditorio	Disponibilidad y operación	Cerrar diagnóstico y especificaciones
P3 – Necesaria	Red de datos – Flora	Riesgo físico y capacidad	Corregir puntos en riesgo y ordenar gabinete

7.1. Inspección visual y operativa de los elementos de red (equipos, datos y energía) en el centro de datos para incluir las observaciones y recomendaciones en el informe respectivo.

El crecimiento continuo del equipo humano en la organización hace indispensable una actualización profunda de la infraestructura técnica para impedir que el rezago tecnológico límite la eficiencia operativa. En la actualidad, el alto tráfico en las redes y la exigencia sobre los sistemas eléctricos constituyen un riesgo significativo que afecta el rendimiento del personal calificado, al no proveer un entorno digital fluido y confiable. Para dar respuesta a esta necesidad, la modernización prevista para el Centro de Datos propone una evolución hacia un esquema de alta disponibilidad con estándares de última generación, diseñado para gestionar el incremento en la demanda de forma flexible y mantener el rendimiento constante de los servicios. Con la eliminación de fallas e interrupciones recurrentes, esta intervención protege tanto la seguridad de la información como los activos de la entidad, al tiempo que establece una base adaptable que asegura la estabilidad de las operaciones y el alcance efectivo de las metas institucionales.

7.2. Inspección visual y operativa de los elementos de red (equipos, datos y energía) de los usuarios finales en las instalaciones de la Corporación para incluir las observaciones y recomendaciones en el informe respectivo.

La actualización integral de los sistemas de energía y redes representa una medida prioritaria e insustituible para neutralizar los riesgos operativos, jurídicos e institucionales derivados de redes sobrecargadas y conexiones vulnerables. Mantener esquemas temporales de conectividad incrementa la posibilidad de fallas críticas, interrupciones en el flujo de información y eventos de seguridad física que ponen en peligro la estabilidad de la entidad. La adopción de normativas y estándares internacionales en estos componentes clave permite evolucionar hacia una arquitectura robusta, preventiva y de fácil crecimiento, al tiempo que proporciona la base tecnológica que el equipo de trabajo con especial énfasis en los contratistas vinculados requiere para desempeñarse con máxima eficiencia y sin contratiempos,

protegiendo así el patrimonio tecnológico y asegurando el alcance continuo de las metas estratégicas.

Leonardo Fabio Sandoval Lozano.
Ing COMTIC S.A.S. director Contrato 200-10-01-12-0197-2026

YANETH GONZALEZ CHALA
CC. No. 39.313.351 de Turbo

Ingeniero Especializado
gonzalezchala@hotmail.com

Gestor Daniel Felipe Payares
administrador@corpouraba.gov.co