INFORME DE ACTIVIDADES DEL CONTRATO

CONTRATO NUMERO

2022-0792

Abril 01 al 30 de 2026

versión	Observaciones	Fecha	Responsable
1.0	Versión Inicial	01/05/2026	Francisco Javier Pulido

Tabla de contenido

1. INTRODUCCIÓN 8
2. OBJETIVO DEL INFORME 8
3. ALCANCE 9
4. AVANCE TÉCNICO 10
4.1. CONECTIVIDAD Y RED DE COMUNICACIONES 10
4.1.1. CANALES INSTALADOS EN EL MES Y ENTREGABLES 12
4.1.2. DESPLIEGUE DE DIRECCIONES IP V6 13
4.1.3. RECOMENDACIONES 15
4.2. CENTRO DE DATOS 15
4.2.1. CENTRO DE DATOS PRINCIPAL 15
4.2.1.1. APLICACIONES 15
4.2.1.2. BASES DE DATOS 19
4.2.1.3. SITIO WEB "PORTAL ICETEX" 23
4.2.2. CENTRO DE DATOS ALTERNO 25
4.2.2.1. HOSTING VIRTUAL (IAAS) 25
4.2.2.2. DATAGUARD BASES DE DATOS MEGACENTER 28
4.2.2.3. SERVICIOS DE HOUSING – DATACENTER ALTERNO 29
4.3. SEGURIDAD INFORMÁTICA 29
4.3.1. GESTIÓN Y FORTALECIMIENTO DE LA SEGURIDAD PERIMETRAL. 31
4.3.2. MONITOREO DE SEGURIDAD Y RESPUESTA ANTE INCIDENTES 31
4.3.3. GESTIÓN OPERATIVA Y SOPORTE DE SEGURIDAD 31
4.3.4. PLATAFORMAS ADMINISTRADAS 32
4.3.4.1. FORTIGATE TRIARA 33
4.3.4.2. FORTIGATE AGUAS 35
4.3.4.3. FORTIGATE MEDELLÍN 37
4.3.4.4. FORTIWEB 2000F 37
4.3.4.5. FORTIWEB 2000E 37
4.3.4.6. FORTIWEBCLOUD DRP 38
4.3.4.7. FORTISANDBOX 38
4.3.4.8. FORTISIEM 39
4.3.4.9. SOPHOS ENDPOINT 40
4.3.5. RECOMENDACIONES DE SEGURIDAD PARA EL ICETEX. 41
4.3.6. SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) 42

4.3.6.1. INDICADORES DE COMPROMISO (THREAD HUNTING): 43
4.3.6.2. ALERTAS O INCIDENTES DE SEGURIDAD DETECTADOS 43
4.3.6.2.1. CATEGORÍA SEGURIDAD 44
4.3.6.2.2. CATEGORÍA DISPONIBILIDAD 45
4.3.6.2.3. AMENAZAS DE CIBERSEGURIDAD 45
4.3.6.3. THREAT HUNTING 45
4.3.6.4. ANÁLISIS DE MARCA OSINT 45
4.3.7. ANÁLISIS DE VULNERABILIDADES ICETEX 48
4.4. SERVICIOS DE NUBE 48
5. GESTION DE LA EJECUCIÓN CONTRACTUAL 50
6. GESTION PRESUPUESTAL 50
7. GESTION ADMINISTRATIVA 52
7.1. PROFESIONALES 52
8. SERVICIO DE COLABORACIÓN 53
9. GESTION DE RIESGOS Y PROBLEMAS 54
10. INDICADORES CLAVE DE DESEMPEÑO 55
10.1. ANS POR DISPONIBILIDAD DE CANALES DE COMUNICACIONES 55
10.1.1. CANAL DE REPLICACIÓN (TRIARA – MEGACENTER) 58
10.2. ANS POR DISPONIBILIDAD DE SERVIDORES 58
10.2.1. DISPONIBILIDAD TRIARA PARA LOS SERVICIOS DE PÁGINA WEB ICETEX 60
10.2.2. ANÁLISIS COMPONENTE LIFERAY PRODUCCIÓN 65
10.2.3. BACKUP SERVIDORES TRIARA 65
11. CONTROL DE CAMBIOS 67
12. PLAN DE TRABAJO DE LOS PROXIMOS MESES 68
13. PLAN DE ENTREGA 68
13.1. OBSERVACIONES RELEVANTES 69
14. RECOMENDACIONES DEL CONTRATISTA AL ICETEX 70
14.1. NETWORKING 70
14.2. APLICACIONES 70
14.3. SEGURIDAD 71
14.4. BASES DE DATOS 72
14.5. INTEGRADOR DE NUBE 73
15. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC 73
15.1. AUMENTO DE LA CAPACIDAD DE ANCHO DE BANDA EN ALGUNAS DE LAS SEDES DE LA ENTIDAD 73

15.2. TB DE CAPACIDAD DE ALMACENAMIENTO 73
15.3. “WIFI” PARA LA GENTE EN 19 SEDES 74
16. CONCLUSIONES 75
17. ANEXOS 77

Indice de Tablas

TABLA 1 CASOS ATENDIDOS NETWORKING COMPARATIVO MES ANTERIOR 13
TABLA 2 LISTADO DE DIRECCIONES IP V6 ASIGNADAS A LAS OFICINAS 14
TABLA 3 VIGENCIA DE LOS CERTIFICADOS DIGITALES 17
TABLA 4 INVENTARIO PRINCIPALES SERVIDORES PRODUCCIÓN 18
TABLA 5 SERVIDORES Y SCHEMAS ADMINISTRADOS 19
TABLA 6 ESTADO BD ORACLE 20
TABLA 7 CRECIMIENTO DE LAS BASES DE DATOS EN LOS ÚLTIMOS 8 MESES 23
TABLA 8 TOP 10 PORTALES MÁS UTILIZADOS 25
TABLA 9 ESTADO LICENCIAMIENTO PORTAL WEB ICETEX 25
TABLA 10 SERVICIOS REPLICADOS – DATACENTER ALTERNO-MEGACENTER 27
TABLA 11 TOP 5 MÁQUINAS MAYOR TASA DE TRANSFERENCIA 27
TABLA 12 TOP 5 MÁQUINAS MENOR TASA DE TRANSFERENCIA 27
TABLA 13 DISPONIBILIDAD DE SERVICIOS DE HOUSING – DATA CENTER ALTERNO 29
TABLA 14 DETALLE PLATAFORMAS SEGURIDAD ADMINISTRADAS INFOTIC 32
TABLA 15 LICENCIAMIENTO FORTIGATE 32
TABLA 16 LICENCIAMIENTO FORTIWEB 38
TABLA 17 CONFIGURACIÓN FORTISANDBOX 1000D 39
TABLA 18 RECOMENDACIONES DE SEGURIDAD 42
TABLA 19 COMPARATIVO – INDICADORES DE COMPROMISO 43
TABLA 20 COMPARATIVO ALERTAS DE SEGURIDAD 44
TABLA 21 EJECUCIÓN PRESUPUESTAL 52
TABLA 22 PERFILES Y ACTIVIDADES 52
TABLA 23 GRUPO ADMINISTRATIVO 53
TABLA 24 DISTRIBUCIÓN MÓDULOS DE VIDEOCONFERENCIA POR SEDE 53
TABLA 25 DISPONIBILIDAD DE CANALES 57
TABLA 26 DISPONIBILIDAD CANALES "INTERNET PARA LA GENTE" 58
TABLA 27 CÓDIGOS RELACIONADOS DISPONIBILIDAD SERVICIOS EN HOUSING – DATACENTER PRINCIPAL 59
TABLA 28 DISPOSITIVOS EN HOUSING – DATACENTER PRINCIPAL 60
TABLA 29 DISTRIBUCIÓN TRIMESTRAL DE ACCESO POR USUARIOS 60
TABLA 30 CONTROLES DE CAMBIO ABRIL 67
TABLA 31 PLANES DE TRABAJO 68
TABLA 32 BALANCE GENERAL ACTIVIDADES EJECUTADAS PLAN DE ENTREGA 69
TABLA 33 CAPACIDADES DE ALMACENAMIENTO CONTRATADO 74
TABLA 34 CAPACIDADES DE ALMACENAMIENTO APROVISIONADO 74
TABLA 35 WIFI PARA LA GENTE INSTALADOS 75
TABLA 36 WIFI PARA LA GENTE PENDIENTES 75
TABLA 37 ANEXOS 78

INFOTIC
SOLUCIONES INTELIGENTES

Indice de Ilustraciones

ILUSTRACIÓN 1 DISPONIBILIDAD DEL CLÚSTER 12
ILUSTRACIÓN 2 DISPONIBILIDAD DEL CLUSTER 21
ILUSTRACIÓN 3 DISPONIBILIDAD *DE LAS BASES DE DATOS PRINCIPALES ICTXCYC Y APOTEOSYS* 21
ILUSTRACIÓN 4 CASOS DEL PROYECTO GESTIONADOS ARANDA BASES DE DATOS 22
ILUSTRACIÓN 5 UPTIME: PORTAL WEB WEB.ICETEX.GOV.CO [100%] 24
ILUSTRACIÓN 6 TRÁFICO GENERAL DE LOS PORTALES 24
ILUSTRACIÓN 7 REPORTES DE REPLICACIÓN SRM A SITIO ALTERNO – ABRIL 2026 26
ILUSTRACIÓN 8 FECHAS CON MAYOR REPLICACIÓN 27
ILUSTRACIÓN 9 EVIDENCIA DATAGUARD REPLICADO A MEGACENTER BD 28
ILUSTRACIÓN 10 DIAGRAMA DE LA ARQUITECTURA DE SEGURIDAD 30
ILUSTRACIÓN 11 TOPOLOGÍA DE WAF CLOUD USADO EN PORTALES DE MEDELLÍN 30
ILUSTRACIÓN 12 CONSUMO CANAL MPLS - PROMEDIO 71 MPPSG [INR0185 CLARO(MPLS_DC)] 33
ILUSTRACIÓN 13 CONSUMO CANAL INTERNET SEDES - PROM 90.68 MBPS WAN-SEDES-ICETEX [INR0264 (INTE_SEDES_ICTX)] 33
ILUSTRACIÓN 14 CONSUMO CANAL INTERNET DATACENTER [INTERNET_DC_INR0000320 (INET_CLARO)] 34
ILUSTRACIÓN 15 FILTRADO – WEB – (FORTIGATE – TRIARA) 34
ILUSTRACIÓN 16 INSPECCIÓN – SSL – (FORTIGATE – TRIARA) 35
ILUSTRACIÓN 17 ANTIVIRUS Y ANTIMALWARE – PERIMETRAL (FORTIGATE – TRIARA) 35
ILUSTRACIÓN 18 CONSUMO CANAL MPLS AGUAS - PROMEDIO 44.72 MBPS 36
ILUSTRACIÓN 19 FILTRADO-WEB-(FORTIGATE-AGUAS) 36
ILUSTRACIÓN 20 INSPECCIÓN-SSL-(FORTIGATE-AGUAS) 36
ILUSTRACIÓN 21 ANTIVIRUS Y ANTIMALWARE-PERIMETRAL-(FORTIGATE-AGUAS) 37
ILUSTRACIÓN 22 CONSUMO CANAL MPLS MEDELLÍN 37
ILUSTRACIÓN 23 TRÁFICO GENERAL DE LOS PORTALES 38
ILUSTRACIÓN 24 LICENCIAMIENTO FORTISIEM 39
ILUSTRACIÓN 25 FORTISIEM PERFORMANCE POR PROCESOS 40
ILUSTRACIÓN 26 ESTADO SEGURIDAD SOPHOS 40
ILUSTRACIÓN 27 TOTAL DE ALERTAS DE SEGURIDAD 44
ILUSTRACIÓN 28 TOP 10 DE ALERTAS DE SEGURIDAD ALTAS 45
ILUSTRACIÓN 29 INCIDENTES POR TIPO DE AMENAZA 46
ILUSTRACIÓN 30 INCIDENTES POR FRAUDES DIGITALES 46
ILUSTRACIÓN 31 INCIDENTES POR FUGA DE DATOS 47
ILUSTRACIÓN 32 INCIDENTES MÓDULO DEEP & DARK WEB 47
ILUSTRACIÓN 33 MÉTRICA DE VISITANTES PORTAL WEB WEB.ICETEX.GOV.CO 60
ILUSTRACIÓN 34 MÉTRICA ADQUISICIÓN USUARIOS PORTAL WEB WEB.ICETEX.GOV.CO 61
ILUSTRACIÓN 35 MÉTRICA DE USUARIO POR PAÍS - PORTAL WEB WEB.ICETEX.GOV.CO 62
ILUSTRACIÓN 36 MÉTRICA DE CIUDADES DE COLOMBIA- PORTAL WEB WEB.ICETEX.GOV.CO 62
ILUSTRACIÓN 37 NODO 1 CPU 63
ILUSTRACIÓN 38 NODO 1 MEMORIA 64
ILUSTRACIÓN 39 NODO 1 ALMACENAMIENTO 65
ILUSTRACIÓN 40 EVIDENCIA BACKUP SERVIDORES RESUMEN GENERAL BACKUPS 66
ILUSTRACIÓN 41 EVIDENCIA BACKUP SERVIDORES RESUMEN BACKUPS Y SU ESTADO 66
ILUSTRACIÓN 42 HISTÓRICO CONSOLIDADO USO DE DISCOS SERVIDOR ICTXSRVNETCOR01 71

1. INTRODUCCIÓN

Este informe contiene la información relacionada con las actividades ejecutadas por INFOTIC con ocasión de la celebración del contrato 2022-0792, durante el periodo comprendido entre el 01 al 30 de Abril de 2026. Para tal fin se cuenta con la información generada por el grupo de 10 especialistas y 3 profesionales administrativos con los cuales se soportan y garantizan la atención de servicios especializados descritos en el alcance del proyecto como son:

- Conectividad y red de comunicaciones
- Centro de Datos
- Seguridad informática
- Servicios de nube
- Servicios Conexos

A la fecha, el contrato 2022-0792, que en su **CLÁUSULA PRIMERA. – OBJETO**, establece *"contratar los servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el ICETEX",* presenta el siguiente avance en las fases establecidas en **CLÁUSULA NOVENA. – ENTREGABLES:**

- Firma del Acta de Inicio suscrita el 30 de diciembre del 2022, con fecha de iniciación del 19 de enero del 2023. Cumplida al 100%.
- Fase de Transición. Que comprendió desde el 19 de enero hasta el 31 de Marzo de 2023. Esta fase se encuentra cumplida al 100%.
- Fase de operación. La etapa inicial, comprendida entre el 1 de abril de 2023 y el 18 de abril de 2026, culminó con una ejecución del 100%. Tras la firma de un Otrosí, la operación se extendió hasta el 19 de diciembre de 2026. A la fecha, esta nueva fase presenta un avance del 5% de ejecución, correspondiente a los 12 días transcurridos dentro del periodo de prórroga.

El presente informe, correspondiente al mes de Abril del 2026, describe los servicios realizados durante el periodo por el equipo de profesionales y las herramientas tecnológicas asignadas y dispuestas por INFOTIC para desempeñar las funciones y atender los requerimientos del ICETEX según lo establecido en el contrato.

2. OBJETIVO DEL INFORME

Presentar las actividades ejecutadas por INFOTIC durante el periodo del 01 al 30 de Abril de 2026, con el fin de determinar el estado, la gestión, evolución y la disponibilidad de los servicios especializados prestados al ICETEX en virtud de la ejecución del contrato, para lo cual se han

considerado la recolección de mediciones desde las herramientas de monitoreo, el análisis y la producción de informes y reportes periódicos sobre cada una de las gestiones y demás informes especiales sobre los servicios prestados.

El presente informe comprende:

- **Administración de Seguridad, Redes y Telecomunicaciones:**
  Descripción de las acciones ejecutadas en la gestión de redes y telecomunicaciones, con énfasis en la estabilidad, disponibilidad y optimización de la infraestructura.
  Reporte de incidentes de seguridad, su impacto y las medidas correctivas implementadas.

- **Conectividad y Red de comunicaciones:**
  Estado de las redes LAN/WAN, su desempeño y disponibilidad.
  Indicadores de tráfico, calidad de servicio (QoS) y balanceo de cargas.

- **Centro de Datos:**
  Estado de operación de los centros de datos, incluyendo disponibilidad, desempeño de servidores, almacenamiento y virtualización.
  Acciones de mantenimiento preventivo y correctivo realizadas.

- **Seguridad Informática:**
  Medidas implementadas para proteger la información y la infraestructura, como monitoreo, control de acceso, actualizaciones y parches de seguridad.

- **Servicios de Nube:**
  Reporte de uso de servicios en la nube, desempeño y cumplimiento de niveles de servicio (SLA).
  Descripción de servicios implementados o integrados en el entorno hibrido o multi-nube.

- **Servicios Conexos:**
  Detalle de actividades complementarias relacionadas con la infraestructura tecnológica, como soporte técnico de los componentes anteriormente descriptos, gestión de incidentes con el seguimiento del servicio de SOC y herramientas Threat Hunting y continuidad del servicio en el marco del componente DRP.

3. ALCANCE

El alcance comprende la descripción de las actividades de los servicios especializados durante el periodo del 01 al 30 de Abril conforme a los frentes definidos por el ICETEX, así:

- **Conectividad y red de comunicaciones**
  Este informe presenta el estado del servicio que comprende los componentes exigidos de la arquitectura de conectividad, comunicaciones, software, hardware y dispositivos de seguridad

informática, mínimos necesarios para la operación de los servicios establecidos en el contrato 2022-0792.

- **Centro de datos**

  El informe presenta el estado de los dos (2) Centros de Datos que contempla el proyecto ICETEX: un (01) centro de cómputo principal (TRIARA) y un (01) centro de cómputo secundario o alterno (MEGACENTER), en los cuales se debe garantizar la disponibilidad de los servicios alojados allí, cumpliendo las condiciones mínimas tales como temperatura, seguridad, cableado estructurado, path-cord para conexión de servidores y demás appliance de la operación, así como unidades de racks (gabinetes exclusivos para ICETEX) requeridas, conexiones eléctricas, entre otras.

- **Seguridad informática**

  El presente informe describe las actividades del periodo que se realizaron con el fin de proveer el servicio de seguridad informática a nivel de administración y gestión para los equipos de seguridad de propiedad del ICETEX, para los servicios On–Premise y para la implementación de controles de seguridad especificados por el modelo de seguridad digital de la Entidad, conforme a los lineamientos legales u otros a fin de fortalecer la seguridad informática de la Entidad.

  Este servicio de administración y gestión debe incluir, pero sin limitarse a ello la implementación - instalación de configuraciones, actualizaciones de software, análisis de dispositivos de red, análisis de procesos, procedimientos, actividades, método y reglas a fin de proteger la infraestructura que soporta la información del ICETEX contra riesgos que afecten su integridad, disponibilidad y confidencialidad.

- **Servicios de nube**

  El informe presenta el estado y detalle de los Servicios de Data Center Principal y Alterno los cuales se encuentra bajo la modalidad de Housing y todos los servicios requeridos para nube privada, dejando claro que a través del contrato se busca integrar servicios de nube pública e hibrida. A la fecha todos los recursos actuales se están usando sin sobre dimensionamientos.

- **Servicios conexos**

  Se definen como los servicios vinculados a la operación y que son necesarios para garantizar su Calidad, Confiabilidad, Continuidad y Seguridad.

4. AVANCE TÉCNICO

4.1. Conectividad y Red de Comunicaciones

La operación de los canales de conectividad se mantuvo estable, garantizando los anchos de banda requeridos por ICETEX. Se ha gestionado de manera continua los casos reportados que afectan directamente los canales o la herramienta de monitoreo y nos encontramos en la gestión de la instalación de los canales pendientes.

Durante el presente periodo y a fin de destacar se atendieron un total de 20 solicitudes, con respecto al mes anterior hubo un Incremento de 12 casos ya que se atendieron 8 solicitudes en el mes anterior

En cuanto a la gestión de vulnerabilidades, todas las detectadas en el último escaneo han sido corregidas. Estamos a la espera de los resultados de un nuevo escaneo para atender cualquier vulnerabilidad adicional que se identifique. Respecto a la implementación de IPv6, se ha trabajado con los especialistas de seguridad en las pruebas correspondientes. Asimismo, se ha avanzado en la documentación he entrega de informes conforme a los lineamientos periódicos de ICETEX.

Los casos escalados durante el mes, así como el estado del canal pendiente por instalar, se encuentra descrito en el numeral **4.1.1. Canales instalados en el mes y entregables.**

La gestión de dispositivos de red es el proceso mediante el cual se gestionan y controlan los dispositivos de red, desde computadoras, servidores y teléfonos móviles hasta conmutadores y máquinas virtuales.

Esto incluye la implementación, la operación y el mantenimiento de todos los dispositivos físicos y virtuales que conforman la infraestructura de red. Actualmente los equipos de red están en buen estado, pero se encuentran en EOL and EOS (End-of-Sale and End-of-Life) esto quiere decir que los equipos ya no cuentan con garantía por parte del fabricante y tampoco son vendidos por los mismos se recomienda al Icetex adquirir equipos nuevos ya que la infraestructura actual cuenta con más de 15 años de antigüedad

inventario de equipos.xlsx
https://icetex.sharepoint.com/:x:/r/sites/Infraestructura/_layouts/15/Doc.aspx?sourcedoc=%7BD8EB1425-7A43-4FA2-8B11-38665423B9B3%7D&file=inventario%20de%20equipos.xlsx&action=default&mobileredirect=true

La topología actualizada, a la fecha, se encuentra en el siguiente enlace:

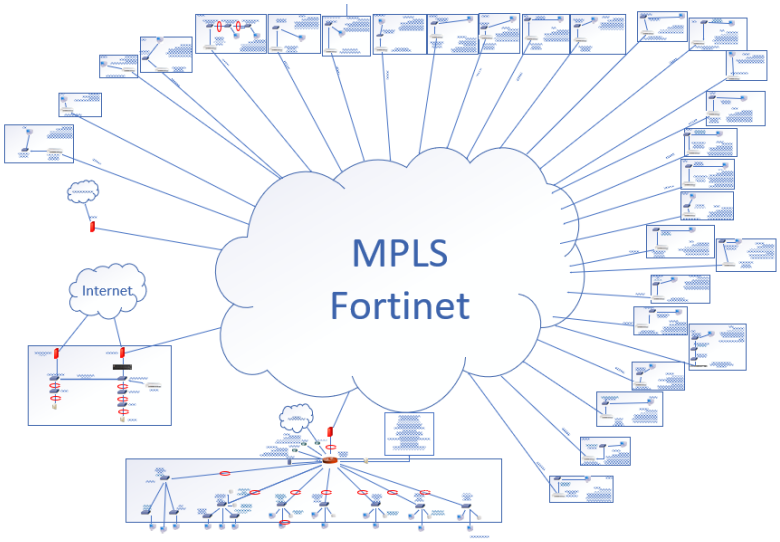


Ilustración 1 Disponibilidad del clúster

TOPOLOGIAS DE AGUAS

A fin de garantizar un adecuado funcionamiento, se ha previsto que el equipo de especialistas de seguridad procederá a configurar reglas en los firewalls, para las direcciones IPV6, empleando como guía las que se encuentran productivas a la fecha con direccionamiento IPV4. El plan de trabajo previsto puede ser consultado en el informe de nuestro especialista de networking.

Finalmente, a solicitud del ICETEX, se les remitió la segmentación de la red del edificio AGUAS- Sede principal.

4.1.1. Canales instalados en el mes y entregables

Durante el periodo de reporte no se han adelantado instalación de canales tanto principales como de backup.

Canales Principales. A la fecha, se ha instalado un total de 40 de los 43 canales MPLS principales previstos en la línea base. De los tres canales restantes, uno corresponde al canal entre el Sitio principal e ICETEX - Dirección General – Aguas, cuya instalación fue descartada por ICETEX. Los otros dos canales faltantes están relacionados con sedes donde ICETEX aún no dispone de oficinas, específicamente en Barrancabermeja y San Gil.

En resumen, hasta la fecha se ha completado la instalación del 100% de los canales principales de comunicación en las sedes especificadas en la línea base del contrato.

Canales de Backup. De los 32 canales de Backups previstos en la línea base, se han instalado 30, lo que representa un avance del 96,55%, sin embargo podemos considerar el 100% de la instalación

completada porque el canal pendiente la instalación correspondía al canal de Backup para la oficina en Quibdó y un canal entre el sitio principal e ICETEX - Dirección General - Aguas, cuyas instalaciones ya fue descartada por ICETEX.

Canales de internet para la gente. El servicio de "internet para la gente" ha sido implementado en las 14 sedes solicitadas según el anexo técnico, logrando así un cumplimiento del 100% de lo previsto.

Anchos de banda. Los canales instalados cuentan con el 100% del ancho de banda contratado. Se lleva a cabo un monitoreo mensual de la disponibilidad de estos canales mediante la herramienta SolarWinds, generando un informe correspondiente que está disponible en el siguiente enlace: Reporte Mensual Disponibilidad INFOTIC Abril 2026.pdf

Solicitudes Nuevas Instalación de canales. En el periodo no se han recibido solicitud de instalación de nuevos canales, pero si se adelantaron mesas técnicas, al interior de la operación, con el fin de entregar configurados los canales SD-WAN de acuerdo a los requerimientos del ICETEX, labor que se espera finalizar en el mes de Abril 2026.

Los casos atendidos durante el mes están disponibles en el siguiente enlace:
Registro Aranda Abril 2026.xlsx

Todos los casos fueron gestionados exclusivamente a través de la herramienta Aranda, sin que se registrara atención por otros medios.

Mes	No. Casos
Enero	7
Febrero	16
Marzo	8
Abril	20

Tabla 1 Casos atendidos Networking comparativo mes anterior

4.1.2. Despliegue de direcciones IP V6

Se efectuó el despliegue de dirección IPv6 sede y se adelantaron pruebas de navegación empleando un PC de un funcionario en la sede respectiva. A la fecha las sedes realizadas son:

Consecutivo	Sede	Pruebas seguridad	Horario	Observación
1	Aguas	27/08/2025	0:00	Realizadas
2	Chapinero Bogotá	9/09/2025	0:00	Realizadas
3	Cali Prueba 2	29/09/2025	0:00	Realizadas
4	Medellín	2/10/2025	0:00	Realizadas

Consecutivo	Sede	Pruebas seguridad	Horario	Observación
5	Buenaventura	3/10/2025	0:00	Realizadas
6	Quibdó	7/10/2025	0:00	Realizadas
7	Riohacha	9/10/2025	0:00	Realizadas
8	Montería	10/10/2025	0:00	Realizadas
9	Bucaramanga	16/10/2025	0:00	Realizadas
10	Popayán	17/10/2025	0:00	Realizadas
11	Pereira	20/10/2025	0:00	Realizadas
12	Valledupar	21/10/2025	0:00	Realizadas
13	Santa Marta	23/10/2025	0:00	Realizadas
14	Barranquilla	24/10/2025	0:00	Realizadas
15	Sincelejo	28/10/2025	0:00	Realizadas
16	Tumaco	30/10/2025	0:00	Realizadas
17	Cúcuta	4/11/2025	0:00	Realizadas
18	Villavicencio	6/11/2025	0:00	Realizadas
19	Tunja	7/11/2025	0:00	Realizadas
20	Cartagena	11/11/2025	0:00	Realizadas
21	Armenia	13/11/2025	0:00	Realizadas
22	Arauca	14/11/2025	0:00	Realizadas
23	Pasto	18/11/2025	0:00	Realizadas
24	Ibagué	20/11/2025	0:00	Realizadas
25	Apartado	21/11/2025	0:00	Realizadas
26	Mocoa	24/11/2025	0:00	Realizadas
27	Yopal	26/11/2025	0:00	Realizadas
28	Manizales	1/12/2025	0:00	Realizadas
29	Neiva	1/12/2025	0:00	Realizadas
30	Ocaña	3/12/2025	0:00	No realizar pruebas de ipv6
31	Puerto Inírida	3/12/2025	0:00	No realizar pruebas de ipv6
32	Puerto Carreño	3/12/2025	0:00	No realizar pruebas de ipv6
33	Florencia	5/12/2025	0:00	No realizar pruebas de ipv6
34	Leticia	5/12/2025	0:00	No realizar pruebas de ipv6
35	Sincelejo	5/12/2025	0:00	Realizadas
36	San Andrés	No se realizará	0:00	No realizar pruebas de ipv6
37	Ángel Bogotá	Pendiente	0:00	Realizadas

Tabla 2 Listado de direcciones IP V6 asignadas a las oficinas

4.1.3. Recomendaciones

Renovación de Equipos: Se sugiere llevar a cabo la actualización de los equipos de la entidad, ya que muchos de ellos se encuentran obsoletos y carecen de soporte por parte del fabricante, lo que podría afectar el rendimiento y la seguridad de la infraestructura.

Reemplazo de Equipos Dañados: se debe notificar a ICETEX que actualmente no hay disponibilidad de equipos de red adicionales para reemplazos futuros en caso de que surjan nuevos daños.

Renovación y Certificación de Cableado: Se recomienda realizar una renovación o sustitución del cableado en diversos puntos de la entidad, dado que la infraestructura de cableado es muy antigua. Se sugiere también llevar a cabo una certificación del nuevo cableado para garantizar su calidad y desempeño.

Mantenimiento de Infraestructura: Considerando el estado actual de la infraestructura en las sedes, es crucial llevar a cabo un mantenimiento integral de los equipos y del cableado, así como proceder a la renovación de los dispositivos de red, para asegurar un funcionamiento óptimo y prevenir fallas futuras.

4.2. Centro de Datos

4.2.1. Centro de Datos Principal

4.2.1.1. Aplicaciones

Durante el mes de Abril de 2026, se atendieron un total de un total de 7 solicitudes, todas documentadas con sus respectivas evidencias. A continuación, se presenta el detalle de estas:

Las actividades desarrolladas estuvieron enfocadas principalmente en:

4.2.1.1.1. Actualización y publicación de archivos en producción:
Se realizaron actividades de actualización y publicación de archivos asociados a las aplicaciones institucionales, incluyendo modificaciones en archivos ASP, publicación del Portal Transaccional y actualizaciones relacionadas con el módulo de Desembolsos, asegurando la correcta implementación de cambios solicitados y la disponibilidad de los servicios en ambiente productivo.

4.2.1.1.2. Gestión de incidentes y soporte técnico:
Se atendieron solicitudes de soporte relacionadas con la copia de fuentes de aplicaciones y ajustes requeridos para garantizar la operación normal de los sistemas institucionales.

4.2.1.1.3. Gestión de accesos y permisos

Se gestionó la asignación de permisos FTP para usuario institucional, garantizando un acceso seguro y controlado conforme a las políticas establecidas.

Con el fin de garantizar el funcionamiento de las soluciones de manera eficiente y segura, se han revisado el estado de actualización de los parches de los sistemas operativos, y se presentó el control de cambio 27028 el cual fue aplazado debido a que el ICETEX no contaba, en su momento, con especialistas de virtualización.

En cuanto al desempeño de los servidores a nivel de sistema operativo Windows Server, se sigue identificado que el servidor ICTXSRNSTCOR01 en donde se aloja la aplicación (es) CargueArchivos, ConciliacionesIES, Condonaciones, TransunionAPI, VotoElectronico, WebServiceServicioPasarelaKushki, WebSiteCondonacion, WebSitePortalTransaccional, WsApiSolicitudes, WsConciliacionesIES, WsCuentasAbandonaadasAPI, WsDynamics, WsPasarela y WsPortalTransaccional presenta, en su unidad F, un espacio de uso del 97% generando un riesgo para el adecuado funcionamiento de la misma, por lo cual se recomienda al ICETEX revisar las políticas de respaldo sobre esa información, si se están ejecutando y alternativas para optimizar dicho espacio.

Con respecto al resto de servidores administrados, estos se encuentran en estado estable, sin eventos críticos, únicamente registros informativos normales.

Se continua con la actualización del inventario de los servidores con los servicios que allí se prestan, el cual puede ser consultado en el siguiente enlace Revision_IIS_Abril2026.xlsx

En cuanto a las actividades de validación de logs, se procedió a efectuar una revisión del visor de eventos en los servidores identificando que:

- Los registros analizados corresponden principalmente a eventos informativos, relacionados con operaciones normales del sistema y de las aplicaciones hospedadas.
- No se detectaron eventos críticos ni errores que comprometan la estabilidad, seguridad o el rendimiento de los servicios en los servidores evaluados.
- Se identificaron eventos habituales como:
    - Inicios y cierres de sesión.
    - Tareas programadas completadas.
    - Validaciones exitosas de servicios.
    - Estados normales de servicios de red y aplicaciones web.

Por otra parte, se realizó un análisis de los eventos y logs que se registran en el Event Viewer del sistema operativo del nuevo servidor aprovisionado asociado al registro DNS aplicaciones.icetex.gov.co, en el cual se evidencian que los errores registrados a nivel de aplicación fueron superados con éxito.

De acuerdo con esta revisión podemos concluir que la infraestructura de servidores se encuentra en estado estable, sin indicios de fallas críticas ni anomalías relevantes en el periodo revisado. Este resultado refleja un funcionamiento adecuado de los sistemas, sin necesidad de acciones correctivas inmediatas.

Además, con base a los registros de los últimos tres meses (enero a Abril de 2026), el consumo de memoria RAM y CPU en los servidores administrados en producción se ha mantenido dentro de los parámetros normales y controlados, por lo que en general los niveles registrados no representan riesgo de saturación ni alertas críticas.

Con el objetivo de asegurar la protección de la información y la confidencialidad de las comunicaciones realizadas a través de los diferentes servicios web de la entidad, se lleva a cabo un control detallado sobre los certificados SSL asignados a los subdominios bajo el dominio institucional icetex.gov.co. A continuación, se presenta el estado de estos:

No	Sitio Web	Subdominio (icetex.gov.co)	Fecha creación	Fecha revocación	Tipo SSL Asignado
1	Pasarela de pagos	webhook.icetex.gov.co	16/10/2025	25/10/2026	RapidSSL RSA CA
2	Pagos PSE	pasareladepagos.icetex.gov.co	18/11/2025	18/11/2026	Wildcard Rapid SSL RSA CA
3	Web Service RNEC	rnec.icetex.gov.co	18/11/2025	18/11/2026	Wildcard Rapid SSL RSA CA
4	Colección de Aplicaciones	aplicaciones.icetex.gov.co	18/12/2025	18/12/2025	Secure Site Pro EV SSL
5	Portal Institucional	web.icetex.gov.co	18/12/2025	18/12/2025	Secure Site Pro EV SSL
6	Portal DECEVAL - Pagaré	pagare.icetex.gov.co	18/12/2025	18/12/2025	Secure Site Pro SSL
7	Portal C&CETEX	www.icetex.gov.co	18/12/2025	18/12/2025	Secure Site Pro EV SSL
8	Colección de Web Services Internos	appwebservices.icetex.gov.co	18/12/2025	18/12/2025	Secure Site Pro SSL
9	Wildcard	*.icetex.gov.co	18/11/2025	18/11/2026	Wildcard Rapid SSL RSA CA

Tabla 3 Vigencia de los certificados digitales

Este control es fundamental para garantizar la disponibilidad y seguridad de los servicios ofrecidos a los usuarios, cumpliendo con las políticas institucionales de ciberseguridad y buenas prácticas en la administración de infraestructura tecnológica.

Esta información permite una supervisión efectiva del ciclo de vida de los certificados, facilitando la planeación de renovaciones y la mitigación de riesgos asociados a certificados expirados o mal gestionados. El detalle del estado de los certificados y sus fechas de expiración puede ser consultado en el informe de nuestros especialistas de soluciones.

La siguiente tabla detalla las características técnicas de los principales servidores en producción, especificando información clave como: nombre del servidor, dirección IP, sistema operativo, tipo de servidor web utilizado, así como los recursos de hardware disponibles (memoria RAM, capacidad de procesamiento – CPU, y almacenamiento).

Esta información es esencial para la toma de decisiones relacionadas con la administración de recursos, optimización de cargas de trabajo, y cumplimiento de políticas de seguridad y disponibilidad.

Servidor	Sitio Web	App Pool	Estado	Puerto(s)	Certificado SSL	Seguridad (Headers)	Logging	Framework	Reciclaje	Actualización / Alta	Worker Processes Máximo
ICTXSRVNETCOR01(192.168.51.165)	AliviosyestimulosApi	AliviosyestimulosApi	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si, 29h	Última act. 15/08/2024	1
	ApiAlivioSimulador	ApiAlivioSimulador	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si, 29h	Última act. 13/09/2024	1
	ApiSimuladorMasivo	ApiSimuladorMasivo	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si, 29h	Última act. 31/03/2025	1
	ApisSolicitud	apisolicitudes	Activo	6370	N/A	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si, 7:00 AM,10:00 AM,1:00 PM,4:00 PM	Última act. 02/04/2025	1
	CargueArchivos	ICETEX_CargueArchivos	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	M,10:00 AM,11:00 AM,1:00 PM,3:00 PM	Sin cambios	1
	ConciliacionesIES	WebSiteConciliacionesIES	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si,6:00 AM	Última act. 19/06/2024	1
	Condonaciones	WsCondonaciones	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si, 29h	Última act. 28/11/2023	1
	CondonacionesVFA	WebSiteCondonacionesVFA	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si,4:00 AM	Sin cambios	1
	ConsultaPlanBeneficios	ConsultaPlanBeneficiosFront	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	No	Sin cambios	1
	ConsultaPlanBeneficiosAPI	ConsultaPlanBeneficiosApi	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si, 29h	Sin cambios	1
	CuentasAbandonadas	WebSiteCuentasAbandonadas	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si,6:00 AM	Sin cambios	1
	CuentasInactivas	CIAAPI	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	:00 AM,11:00 AM,1:00 PM,3:00 PM,5:00	Última act. 19/03/2025	1
	CuentasInactivasFront	CIFront	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	No	Última act. 17/12/2024	1
	CuentasInactivasPreCIAPI	CIAPIPreCI	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si, 29h	Última act. 3/4/2024	1
	CuentasInactivasPreCIFront	CIFrontPreCI	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	No	Última act. 3/4/2024	1
	DatosContacto	DatosContacto	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si, 29h	Última act. 31/10/2024	1
	EnvioNotificacion	EnvioNotificacion	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	No	Última act. 18/12/2024	1
	Estufuturo	WebSiteEsTuFuturo	Inactivo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	No	Sin cambios	1
	FormularioVDIES	FormularioVDIES	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	No	Sin cambios	1
	IMAI	WebServiceIMAI	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	No	Sin cambios	1
	Institucional	WebSiteInstitucionalMicrositios	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	No	Sin cambios	1
	LegalizacionIES	LegalizacionIES	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	No	Sin cambios	1
	LoginPortalTransaccionalApi	LoginPortalTransaccionalApi	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si, 29h	Última act. 4/11/2024	1
	LoginPortalTransaccionalFront	LoginPortalTransaccionalFront	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	No	Última act. 4/11/2024	1
	MEACFront	MEACFront	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	No	Última act. 17/12/2024	1
	RegistroUsuarioPJ	WebSiteRegistroUsuariosPersonaJuridica	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si,6:00 AM	Sin cambios	1
	SarlaftApi	SarlaftApi	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si, 29h	Sin cambios	1
	SarlaftFront	SarlaftFront	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si, 29h	Sin cambios	1
	ServicioApiRestCore	ServicioApiRestCore	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	No	Sin cambios	1
	ServicioApiRestTigal	ServicioApiRestTigal	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	No	Sin cambios	1
	ServicioMigracionIcetex	ServicioMigracionIcetex	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si, 29h	Última act. 4/2/2025	1
	SNIBCE	WebSiteEsTuFuturo	Inactivo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	No	Sin cambios	1
	TransunionAPI	TransunionAPI	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si, 29h	Última act. 9/1/2025	1
	VotoElectronico	WebSiteVotoElectronico	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si,6:00 AM	Sin cambios	1
	WebServiceServicioPasarelaKushki	WebServiceServicioPasarelaKushki	Activo	443	Válido - 16/10/2025	X-Frame-Options SAMEORIGIN	Si	.NET 4.0	Si,6:00 AM	Última act. 1/5/2024	1
	WebSiteCondonacion	WebSiteCondonacion	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si,6:00 AM	Sin cambios	1
	WebSitePortalTransaccional	PortalTransaccionalWebSite	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si,5:00 AM	Última act. 26/12/2024	1
	WebsitePSE	WebSitePSE	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si,6:00 AM	Última act. 7/3/2024	5
	WsApiSolicitudes	WebServiceApiSolicitudes	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	M,11:00 AM,1:00 PM,2:00 PM,3:00 PM	Sin cambios	1
	WsConciliacionesIES	WebServiceConciliacionesIES	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si, 29h	Última act. 20/04/2024	1
	WsCuentasAbandonaadasAPI	WebServiceWsCuentasAbandonadasAPI	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si,6:00 AM	Última act. 31/10/2024	1
	WsDynamics	ActualizacionMasivaDynamics	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si, 29h	Sin cambios	1
	WsGestorVDIESApi	WsGestorVDIES	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	No	Sin cambios	1
	WsPasarela	WebServicePasarela	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	Si,6:00 AM	Sin cambios	1
	WsPortalTransaccional	PortalTransaccionalWebService	Activo	443	Valido 4/12/2025	X-Frame-Options -Strict-Transport-Security	Si	.NET 4.0	:00 AM,11:00 AM,1:00 PM,3:00 PM,5:00	Última act. 16/04/2025	1
ICTXSRVAPPMIX1 Webservices (192.168.51.137)	WsGestorDocumentalAPI	WebServiceWsGestorDocumentalAPI	Activo	443	Valido 3/12/2025	X-Frame-Options -SAME ORIGIN	Si	.NET 4.0	Si,6:00 AM	Última act. 15/08/2024	1
	WsServicioIntegracionVigia	WebServicesWsServicioIntegracionVigia	Activo	443	Valido 3/12/2025	X-Frame-Options -SAME ORIGIN	Si	.NET 4.0	Si,6:00 AM	Última act. 13/09/2024	1
	WsServicioIntegracionCensoIndigena	sServicesWsServicioIntegracionCensoIndig	Activo	443	Valido 3/12/2025	X-Frame-Options -SAME ORIGIN	Si	.NET 4.0	Si,6:00 AM	Última act. 31/03/2025	1
	WsApiServicelcetex	WebServiceWsApiServicelcetex	Activo	443	Valido 3/12/2025	X-Frame-Options -SAME ORIGIN	Si	.NET 4.0	Si,6:00 AM	Última act. 02/04/2025	1
	WsConsultaResoluciones	WebServicesWsConsultaResoluciones	Activo	443	Valido 3/12/2025	X-Frame-Options -SAME ORIGIN	Si	.NET 4.0	Si,6:00 AM	Sin cambios	1
	WsProxiCore	WebServiceWsProxiCore	Activo	443	Valido 3/12/2025	X-Frame-Options -SAME ORIGIN	Si	.NET 4.0	Si,6:00 AM	Última act. 28/11/2023	1
	WsPortalTransaccionalBus	WebServicesWsPortalTransaccionalBus	Activo	443	Valido 3/12/2025	X-Frame-Options -SAME ORIGIN	Si	.NET 4.0	Si,6:00 AM	Sin cambios	1
	WsGestorDocumental	WebServicesWsGestorDocumentaL	Activo	443	Valido 3/12/2025	X-Frame-Options -SAME ORIGIN	Si	.NET 4.0	Si,6:00 AM	Sin cambios	1
	WsSFCObtenerQuejas	WebServicesWsSFCObtenerQuejas	Activo	443	Valido 3/12/2025	X-Frame-Options -SAME ORIGIN	Si	.NET 4.0	Si,6:00 AM	Sin cambios	1
	WsOrquestadorSFC	WebServicesOrquestadorSFC	Activo	443	Valido 3/12/2025	X-Frame-Options -SAME ORIGIN	Si	.NET 4.0	Si,6:00 AM	Sin cambios	1
	WsBusicifes	WebServiceBusicifes	Activo	443	Valido 3/12/2025	X-Frame-Options -SAME ORIGIN	Si	.NET 4.0	Si,6:00 AM	Última act. 19/03/2025	1
	WsServicioIntegracionMEN	WebServiceWsServicioIntegracionMEN	Activo	443	Valido 3/12/2025	X-Frame-Options -SAME ORIGIN	Si	.NET 4.0	Si,6:00 AM	Última act. 3/4/2024	1
	WsServicioIntegracionSisben	WsServicioIntegracionSisben	Activo	443	Valido 3/12/2025	X-Frame-Options -SAME ORIGIN	Si	.NET 4.0	Si,6:00 AM	Última act. 31/10/2024	1
	WsServicioCCD	WebServiceWsServicioCCD	Activo	443	Valido 3/12/2025	X-Frame-Options -SAME ORIGIN	Si	.NET 4.0	Si,6:00 AM	Última act. 18/12/2024	1
ICTXSRVAPPMIX1 Websistes(192.168.51.136)	WsAdministrativaFondoCovid19	WsAdministrativaFondoCovid19	Activo	443	Valido 17/11/2025	NO	Si	.NET 4.0	Si,6:00 AM	Sin cambios	1
	WsDesembolsos	WsDesembolsos	Activo	443	Valido 17/11/2025	NO	Si	.NET 4.0	CADA HORA DE 7 AM A 7 PM	Sin cambios	1
	WsCargueMasivoEstados	WsCargueMasivoEstados	Activo	443	Valido 17/11/2025	NO	Si	.NET 4.0	Si,6:00 AM	Sin cambios	1
	WsReporteador	WsReporteador	Activo	443	Valido 17/11/2025	NO	Si	.NET 4.0	CADA 2 HORA DE 8 AM A 8 PM	Última act. 4/11/2024	1
	WsReporteadorMacros	WsReporteadorMacros	Activo	443	Valido 17/11/2025	NO	Si	.NET 4.0	Si, CADA 60 MIN	Última act. 17/12/2024	1
	WsArquitecturaEmpresarial	WsArquitecturaEmpresarial	Activo	443	Valido 17/11/2025	NO	Si	.NET 4.0	Si,6:00 AM	Sin cambios	1
	EmailCredenciales	EmailCredenciales	Activo	443	Valido 17/11/2025	NO	Si	.NET 4.0	Si, 29h	Sin cambios	1
	ApiDesembolsos	ApiDesembolsos	Activo	443	Valido 17/11/2025	NO	Si	.NET 4.0	Si, 29h	Sin cambios	1
ICTXSRVAPPMIX1 Rnec (192.168.51.135)	WebServiceWsRnec	WebServiceWsRnec	Activo	443	Valido 16/10/2025	NO	Si	.NET 4.0	Si,6:00 AM	Sin cambios	1
ICTXSRVMOODLE (192.168.51.182)	ComunidadIcetexApi	ComunidadIcetexApi	Activo	443	Valido 17/11/2025	NO	Si	.NET 4.0	Si,6:00 AM	Última act. 28/11/2024	1
	ComunidadIcetexFront	ComunidadIcetexFront	Activo	443	Valido 17/11/2025	NO	Si	.NET 4.0	Si,6:00 AM	Última act. 28/11/2024	1

Tabla 4 Inventario principales servidores producción

Se realizó la verificación de las actualizaciones instaladas en los servidores Windows ICTXSRVNETCOR01, ICTXSRVAPPSMIX1, ICTXSRVDCVAL01, ICTXSRVMOODLE y ICTXSRVAPPSMIX2, identificando que se encuentran al día.

En el informe de los especialistas de soluciones, se presenta un resumen detallado de los hallazgos por servidor, identificando los puntos cumplidos, las áreas de mejora y las recomendaciones correspondientes para asegurar el cumplimiento de estándares mínimos de protección en cada entorno revisado.

Durante el mes de Abril de 2026, se realizaron actividades orientadas a la verificación, validación y fortalecimiento de la configuración de seguridad (hardening) en servidores críticos de la infraestructura institucional tales como: ICTXSRVNETCOR01, ICTXSRVAPPSMIX1, ICTXSRVDCVAL01 y ICTXSRVMOODLE. Estas acciones forman parte del compromiso continuo con las buenas prácticas de seguridad de la información y buscan mitigar riesgos derivados de configuraciones débiles o vulnerabilidades conocidas.

El proceso incluyó la revisión técnica de parámetros clave del sistema operativo, con respecto al componente de seguridad Windows Defender Firewall, conforme a lineamientos establecidos en guías de seguridad de Microsoft y CIS Benchmarks.

Se lograron aplicar ajustes en los servidores, sin embargo, aún se encuentran pendientes de validación otras configuraciones de endurecimiento, entre ellas:

- Activación obligatoria del firewall.
- Bloqueo de conexiones entrantes por defecto.
- Restricción de reglas locales de firewall y seguridad.

Teniendo en cuenta que los servidores involucrados soportan múltiples aplicaciones, servicios e integraciones institucionales, se considera necesario realizar una validación técnica conjunta antes de aplicar cualquier cambio en ambientes productivos, con el fin de evitar afectaciones operativas o indisponibilidad de servicios.

Por lo anterior, se solicita el acompañamiento y validación por parte de los equipos de desarrollo de aplicaciones, especialistas de seguridad, proveedores o terceros involucrados (si aplica).

Anexos: Ajustes de hardening en políticas de seguridad y firewall.pdf
Ajustes de hardening en políticas de seguridad y firewall v2.pdf

4.2.1.2. Bases de Datos

La administración de base de datos se efectúa sobre los siguientes servidores:

RAC - PRODUCCION		BASES DE DATOS	VERSION
GRID Infraestructure		ASMn user grid	19.29.0.0.0
SCAN (DNS): odaprod-scan		ICTXCYC	11.0.2.0.4
IP1: Pública 192.1.2.70		ICETEX	11.0.2.0.4
IP2: Pública 192.1.2.71		APLICATI	11.0.2.0.4
IP3: Pública 192.1.2.72		APOTEOSY	11.0.2.0.4
NODO 1	NODO 2	VIGIAPRD	19.29.0.0
IP4: Pública 192.1.2.73	IP5: Pública 192.1.2.74	LIFERAY LIFERAYPDB	19.29.0.0
IP6: Privada 10.20.30.11	IP7: Privada 10.20.30.21	LANDICTX	19.29.0.0
IP8: Virtual 192.1.2.76	IP9: Virtual 192.1.2.77	SGDEA	19.29.0.0
		APOTNEW	11.2.0.4

DRP - PRODUCCION	BASES DE DATOS	VERSION
GRID Infraestructure	ASM user grid	19.13.0.0.0
192.1.2.80	ICTXCYCD	11.0.2.0.4
	ICETEXD	11.0.2.0.4
	APLICATID	11.0.2.0.4
	APOTEOSD	11.0.2.0.4
	VIGIADTGD	19.29.0.0
	LIFERAYD	19.29.0.0
	LANDICTD	19.29.0.0
	APOTNEWD	11.0.2.0.4
	SGDEA	19.29.0.0

CALIDAD TEST	BASES DE DATOS	VERSION
GRID Infraestructure	ASM user oracle	19.13.0.0.0
192.168.51.97	APOTPRU	11.2.0.4
	APLICATI	11.2.0.4
	ICETEX	11.2.0.4
	VIGIAV2	11.2.0.4
	LANDICTX	19.29.0.0
	LIFERAY	19.29.0.0
	SGDEA	19.29.0.0
	VIGIAPRD	19.29.0.0

OEM	BASES DE DATOS	VERSION
10.1.4.96	EMCLOUD	12.2.0.1.0

PRUEBAS	BASES DE DATOS	VERSION
GRID Infraestructure	ASM user grid	19.13.0.0.0
10.1.4.95 o 10.1.4.98	APOTPRU	11.0.2.0.4
	APOTNEW	11.0.2.0.4
	APOT	11.0.2.0.4
	sicci	11.0.2.0.4
	VIGIAPRD	19.19.0.0
	ICTXQA	11.0.2.0.4
	ICTXQA19	19.19.0.0

Tabla 5 Servidores y Schemas Administrados

A continuación, se presenta un cuadro resumen con el estado actual de las bases de datos administradas:

BASES DE DATOS	VERSION	TAMAÑO
ASMn user grid	19.29.0.0.0	GB
ICTXCYC	11.0.2.0.4	5.663
ICETEX	11.0.2.0.4	209
APLICATI	11.0.2.0.4	245
APOTEOSY	11.0.2.0.4	484
VIGIAPRD	19.29.0.0	230
LIFERAY LIFERAYPDB	19.29.0.0	30
LANDICTX	19.29.0.0	615
SGDEA	19.29.0.0	165

Tabla 6 Estado BD Oracle

Resultado del proceso de administración se destacan las siguientes actividades:

- Durante el presente periodo y a fin de destacar se atendieron un total de 760 solicitudes (Problemas, cambios, requerimientos, incidentes,)
- Con el fin de garantizar el funcionamiento de los sistemas manejadores de bases de datos (RDBMS) administrados, se han revisado el estado de actualización de los parches.
- Se administraron las bases de datos Oracle de producción, desarrollo y calidad del ICETEX en versiones 11G y 19C durante el mes de abril de 2026.
- Se realizaron los mantenimientos de los espacios de los filesystem /oracle /grid /opt /DATOS de las maquinas donde se encuentran alojados los binarios las bases de datos para su correcto funcionamiento.
- Se validaron los respaldos de las bases de datos de los archivelog, Backups incrementales y Backups completos o full.
- Se validó la replicación de las bases de datos del Datacenter Bogotá a centro alterno de Medellín Megacenter.
- Se realizaron las restauraciones solicitadas por ICETEX de ambiente de producción a ambiente de desarrollo (Apoteosys, ICTXCYC Core de crédito cierre mensual).

La disponibilidad del Clusterware BD para el mes de Abril de 2026 fue del 100% como se evidencia en la siguiente ilustración:

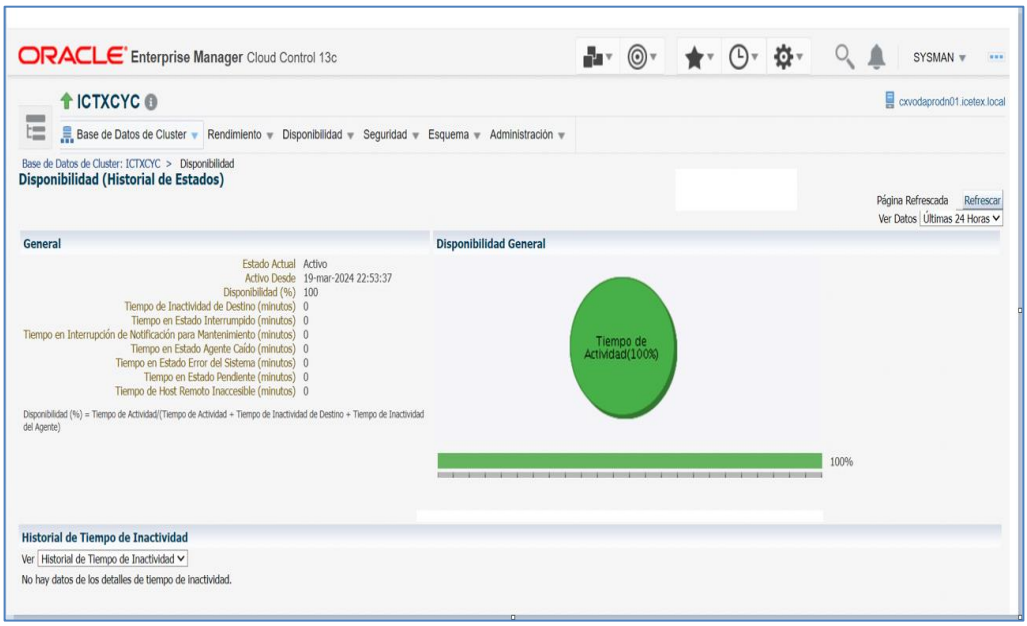


Ilustración 2 Disponibilidad del cluster

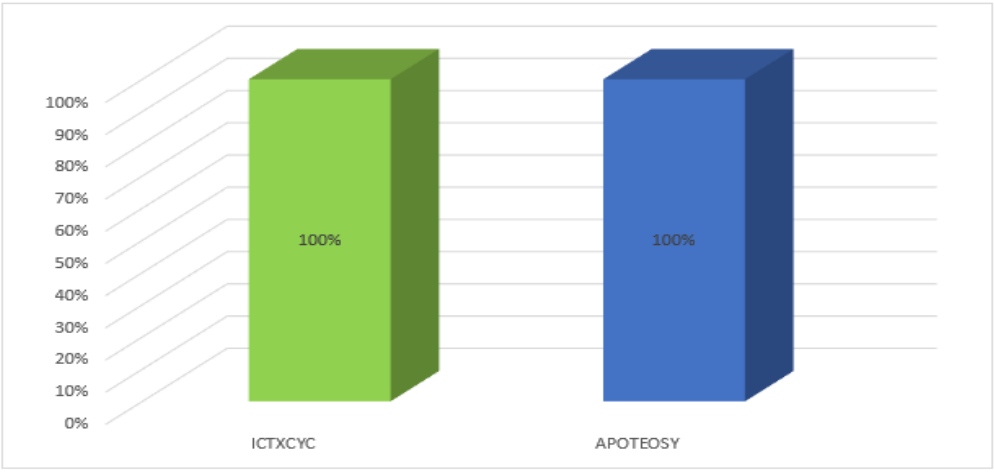


Ilustración 3 Disponibilidad *de las Bases de Datos principales ICTXCYC y APOTEOSYS*

Se ha informado al ICETEX la carencia de recursos en el server de BD 10.1.4.95 para igualar los recursos del ambiente de pruebas a los de producción ya que en estos momentos la BD SICCI se encuentra funcionando con menos de ¼ de los recursos que el ambiente presenta en producción y los usuarios ya han escalado el tema en varias ocasiones, a nivel de BD se generó el análisis para el crecimiento de los recursos que se requieren sean asignados a nivel de S.O para posteriormente asignar estos a la BD SICCI.

La versión de base de datos 11 G ya no tiene soporte por Oracle la versión que en este momento tiene soporte es 19C y, en la actualidad, se cuentan con 5 base de datos operando en esta versión.

Se ha brindado soporte, al equipo de sistemas de información del ICETEX, en el proceso de migración a la versión 19c, siendo la base de datos con la que se dio inicio APOTEOSYS en el mes de agosto y hemos apoyado en las tareas que se adelantan con respecto a CICETEX.

Las versiones disponibles del motor ORACLE son las siguientes:

- Oracle Database 26ai: La versión más reciente orientada a inteligencia artificial, que reemplaza a la 23ai.
- Oracle Database 23ai (23c): Versión de soporte a largo plazo (Long Term Release) centrada en IA y desarrollo, con soporte premier ampliado.
- Oracle Database 21c: Versión de "Innovación" diseñada para características de vanguardia como blockchain tables y soporte nativo de JSON, con soporte limitado.
- Oracle Database 19c: Considerada la versión más estable y recomendada para producción, con soporte a largo plazo vigente hasta el 31 de diciembre de 2029. Para las bases de datos que se encuentran en este versión, hemos efectuado la actualización a la versión 19.29.

Resulta imperativo que, por parte de los responsables de cada uno de los sistemas del ICETEX, se continúe con la planificación y ejecución organizada de las migraciones de las bases de datos, asegurando una adecuada coordinación técnica, la mitigación de riesgos operativos y la continuidad de los servicios asociados.

4.2.1.2.1. Casos del proyecto Gestionados por Bases de datos:

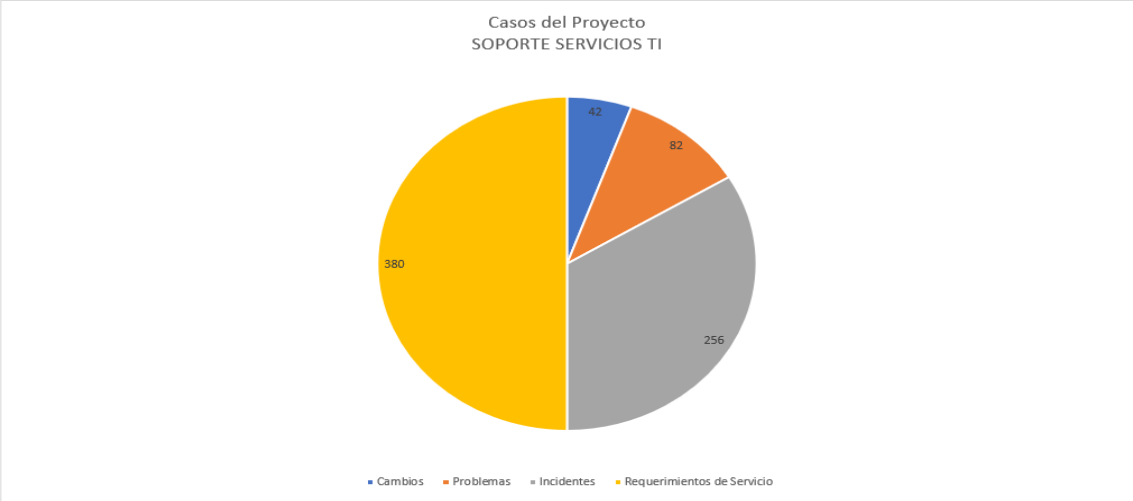


Ilustración 4 Casos del proyecto Gestionados Aranda Bases de datos

Desde Bases de datos se tienen las siguientes recomendaciones:

- Se debe aumentar los espacios de Megacenter del DataGuard por la apertura de las bases de datos para consulta.

- Sólo quedan 120G disponibles, recurso que podría alcanzar sólo para un mes de actividad.

- Se deben crear las tareas y cronologías para migrar las bases de datos que se encuentran en versión 11G fuera de soporte a la versión 19C o mayor.

4.2.1.2.2. Almacenamiento Servidores Oracle:

A continuación, se presenta el consumo del almacenamiento disponible, por cada una de las bases de datos administradas:

BASE DE DATOS	"SEPT 2025	"OCT-2025	"NOV 2025	"DICIEMBRE 2025"	ENERO 2026	FEBRERO 2026	"MARZO 2026	"ABRIL 2026"
ICTXCYC	4,774	4,923	4,925	4,996	5,259	5,445	5,647	5,663
ICETEX	206	206	207	207	209	209	209	209
APLICATI	243	243	243	244	244	245	245	245
APOTEOSY	480	481	481	481	482	483	483	484
VIGIAPRD	166	175	178	188	200	211	217	230
LIFERAY LIFERAYPDB	8	8	8	8	23	23	24	30
LANDICTX	529	529	554	584	596	612	615	615
SGDEA	136	140	143	147	151	155	159	165
TOTAL==>	6,542.00	6,705.00	6,738.56	6,855.06	7,164.44	7,383.57	7,599.00	7,641.00
CRECIMIENTO		163.00	33.56	116.50	309.38	219.13	215.43	42.00

Tabla 7 Crecimiento de las bases de datos en los últimos 8 meses

4.2.1.2.3. Replicación Bases de Datos Oracle

Durante el mes de Abril de 2026 se continuó con la replicación permanente de las BD Oracle al Datacenter alterno de acuerdo con las políticas establecidas, utilizando el Oracle Active Data Guard el cual garantiza una alta disponibilidad, protección de datos y recuperación ante desastres.

Se informa que se ha accedido a configurar, la retención de, los ARCHIVE LOGS con el fin de soportar la solución de GCP (SERVINFORMACION); no obstante, esta configuración ha venido generando afectaciones en los mecanismos de replicación del servidor, impactando su desempeño y estabilidad, por lo que se hace necesario evaluar ajustes o alternativas que mitiguen dicha situación.

4.2.1.3. Sitio Web “Portal Icetex”

Durante el mes de Abril se continuo con el monitoreo permanente a los portales sobre los que opera el ICETEX, manteniendo, las alertas y reportes a tiempo en caso de que se presentara algún evento que pudiera ocasionar una interrupción en la prestación de los servicios que se ofrecen a través de los portales, este informe se encuentra detallado en el documento Informe Mensual InfoTIC Seguridad Abril2026.pdf

En cuanto a la disponibilidad del portal web de la entidad se presentan unos uptime superiores al 100% como se evidencia en la siguiente gráfica:

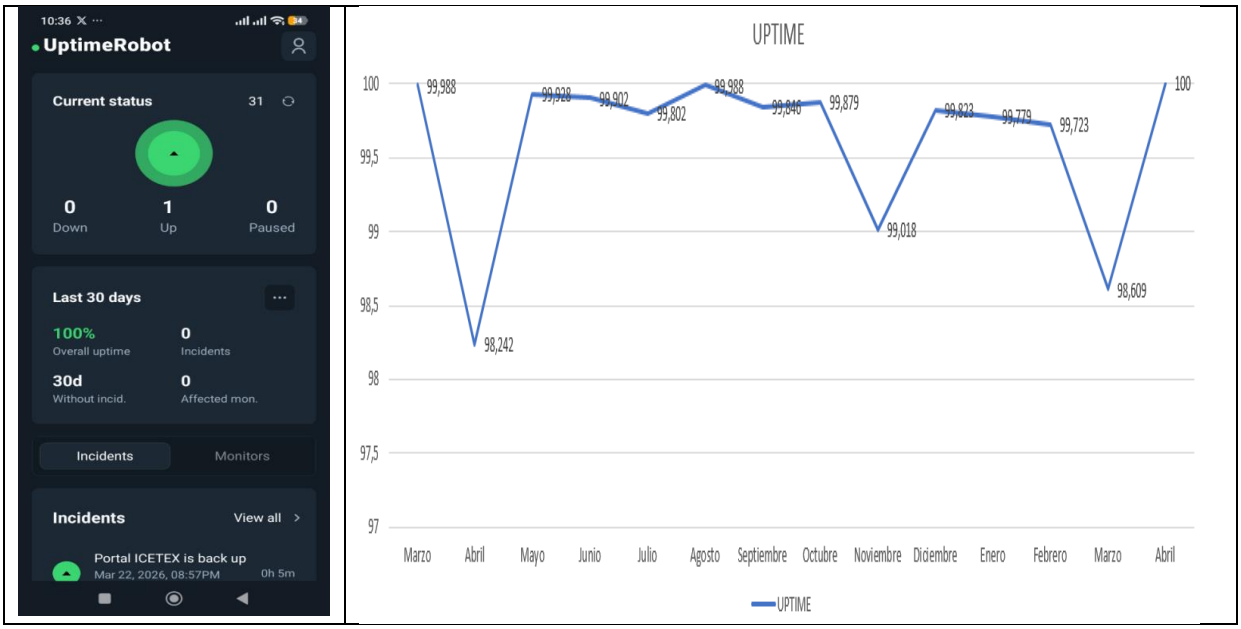


Ilustración 5 UPTIME: Portal WEB web.icetex.gov.co [100%]

Durante en el mes de Abril no se escalaron requerimientos al especialista WebMAster en la mesa de servicios.

Por último, los casos SD Claro disminuyeron en un 72.72%, los casos corresponden a consumo momentáneo de CPU y solicitud de acompañamiento de virtualización para revisión de minutograma de migración de VMs - Portal ICETEX.

En el mes, se presenta un promedio de 1200GB de tráfico general hacia los portales protegidos por el FortiWeb donde el portal de web.icetex.gov.co y www.icetex.gov.co fueron los más utilizados en este periodo, lo cual es un comportamiento normal para este tipo de transacciones de acuerdo con la actividad de los usuarios y las convocatorias vigentes.

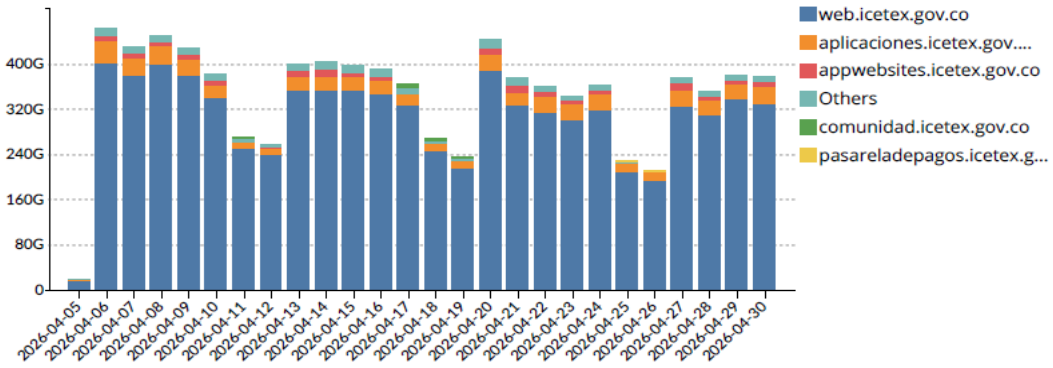


Ilustración 6 Tráfico General De Los Portales

En cuanto a los portales más utilizados, la estadística del presente mes es la siguiente:

#	HTTP Host	Hits	% of Total
1	web.icetex.gov.co	203,541,467	83.65%
2	aplicaciones.icetex.gov.co	26,041,563	10.70%
3	www.icetex.gov.co	7,051,043	2.90%
4	pasareladepagos.icetex.gov.co	3,036,749	1.25%
5	gestordeservicios.icetex.gov.co	1,471,739	0.60%
6	crmweb.icetex.gov.co:777	709,329	0.29%
7	comunidad.icetex.gov.co	499,278	0.21%
8	appwebsites.icetex.gov.co	338,187	0.14%
9	webhook.icetex.gov.co	200,845	0.08%
10	sip.icetex.gov.co	38,255	0.02%

Tabla 8 Top 10 Portales más utilizados

El estado del licenciamiento es el siguiente:

SERVICIO	LICENCIAMIENTO	
	FECHA DE INICIO	FECHA DE EXPIRACIÓN
Liferay 7 .3.10 GA1 – Nodo 1	18 de septiembre de 2025 a las 19:00 horas	17 de octubre de 2026 a las 19:00 horas
Liferay 7 .3.10 GA1 – Nodo 2	18 de septiembre de 2025 a las 19:00 horas	17 de octubre de 2026 a las 19:00 horas
Liferay 7.3.10 GA1 – Ambiente de pruebas	18 de septiembre de 2025 a las 19:00 horas	17 de octubre de 2026 a las 19:00 horas
NFS	Licencia Open Source.	Licencia Open Source.
Elasticsearch – Nodo 1	14 de agosto de 2025 a las 00:00 horas	31 de octubre de 2026 a las 23:59:59 horas
Elasticsearch – Nodo 2	14 de agosto de 2025 a las 00:00 horas	31 de octubre de 2026 a las 23:59:59 horas
Elasticsearch – Nodo 3	14 de agosto de 2025 a las 00:00 horas	31 de octubre de 2026 a las 23:59:59 horas

Tabla 9 Estado Licenciamiento Portal Web Icetex

4.2.2. Centro de Datos Alterno

4.2.2.1. Hosting Virtual (IaaS)

En el transcurso del mes de Abril, se mantuvo en constante replicación las máquinas virtuales configuradas, estos servidores se replicaron desde el origen en Triara hasta Megacenter usando la herramienta nativa de VMware, Site Recovery Manager (SRM) el detalle de las máquinas virtuales replicadas se puede evidenciar en el Informe mensual replicacion Abril 2026.pdf cuyo reporte refleja el consolidado de los informes mensuales y que se están entregando periódicamente, a continuación se puede ver el último reporte diario del mes.

Site Recovery Manager - Estado Replicas INFOTIC

Actualmente el SRM (**vcsatriara-ext.datacenterdhs.local -> vcmegacenter.datacenterdhs.local**) cuenta con **10** replicas

General

Name	Count
OK	10

Grupo de protección: PG_INFOTIC_7 (1)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0226_INFOTIC_REP	OK	5 of 5	Apr 30, 2026	710.37 MB	5 minutes

Grupo de protección: PG_INFOTIC_6 (2)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0228_INFOTIC_REP	OK	1 of 1	Apr 30, 2026	57.11 MB	1 hour
INR0229_INFOTIC_REP	OK	1 of 1	Apr 30, 2026	48.78 MB	1 hour

Grupo de protección: PG_INFOTIC_1 (1)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0233_INFOTIC_REP	OK	3 of 3	Apr 30, 2026	50.22 MB	1 hour

Grupo de protección: PG_INFOTIC_4 (3)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0238_INFOTIC_REP	OK	2 of 2	Apr 30, 2026	62.14 MB	1 hour
INR0239_INFOTIC_REP	OK	2 of 2	Apr 30, 2026	39.08 MB	1 hour
INR0243_INFOTIC_REP	OK	2 of 2	Apr 30, 2026	13.84 GB	1 hour

Grupo de protección: PG_INFOTIC_3 (2)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0244_INFOTIC_REP	OK	1 of 1	Apr 30, 2026	78.11 MB	1 hour
INR0245_INFOTIC_REP	OK	1 of 1	Apr 30, 2026	8.25 MB	5 minutes

Grupo de protección: PG_INFOTIC_2 (1)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0249_INFOTIC_REP	OK	2 of 2	Apr 30, 2026	22.7 MB	5 minutes

Ilustración 7 Reportes de replicación SRM a Sitio Alterno – Abril 2026

En la siguiente tabla se detallan los servidores con sus correspondientes servicios los cuales están siendo replicados a Megacenter:

No.	INR Replicación	Host name	Servicio	VirtualMachine MEGACENTER
1	INR0204	Mira	Portal Web	INR0226_INFOTIC_REP
2	INR0207	ictxsisgesbd	Sisgestion	INR0228_INFOTIC_REP
3	INR0206	ictxsisgesapp	Sisgestion	INR0229_INFOTIC_REP
4	INR0220	icetexboglxorfeo1	ORFEO	INR0233_INFOTIC_REP
5	INR0219 **	icetexboglxorfeo2	ORFEO	INR0262_INFOTIC_REP
6	INR0208 *	ICTXBOGSRVPT1	Portal Transaccional	INR0236_INFOTIC_REP
7	INR0210	icetexbogliferaynfs	Portal productivo (liferay)	INR0238_INFOTIC_REP
8	INR0217	icetexbogelasticserver1	Portal productivo (liferay)	INR0239_INFOTIC_REP
9	INR0218	icetexbogliferayserver1	Portal productivo (liferay)	INR0243_INFOTIC_REP
10	INR0215	icetexboglxdarumasrv1	DARUMA	INR0244_INFOTIC_REP

No.	INR Replicación	Host name	Servicio	VirtualMachine MEGACENTER
11	INR0213	icetexboglxdarumasrv2	DARUMA	INR0245_INFOTIC_REP
12	INR0214	icetexboglxxroad1	XROAD	INR0249_INFOTIC_REP

Tabla 10 Servicios replicados – Datacenter Alterno-Megacenter

**Se detiene la replicación INR0208 que corresponde a la Maquina INR0236- ICTXBOGSRVPT1, los recursos de esta última se distribuyen en TRIARA entre los servidores OPENSHIFT identificados con los códigos de servicio INR0259, INR0258 e INR0251.
**Se mantiene detenida la replicación INR0219 que corresponde a la máquina virtual INR0262 -icetexboglxorfeo2

A continuación se presentan las máquinas con mayores y menores tasas de transferencia:

INR	HOSTNAME	GB
INR0243	icetexbogliferayserver1	339,855
INR0226	Mira	7,572
INR0233	icetexboglxorfeo1	3,144
INR0244	icetexboglxdarumasrv1	2,185
INR0229	ictxsisgesapp	1,861

Tabla 11 TOP 5 máquinas mayor tasa de transferencia

INR	HOSTNAME	GB
INR0245	icetexboglxdarumasrv2	0,244
INR0249	icetexboglxxroad1	0,767
INR0238	icetexbogliferaynfs	1,433
INR0239	icetexbogelasticserver1	1,443
INR0228	ictxsisgesbd	1,585

Tabla 12 TOP 5 máquinas menor tasa de transferencia

En cuanto a las fechas con mayor replicación presentada podemos observar el siguiente comportamiento:

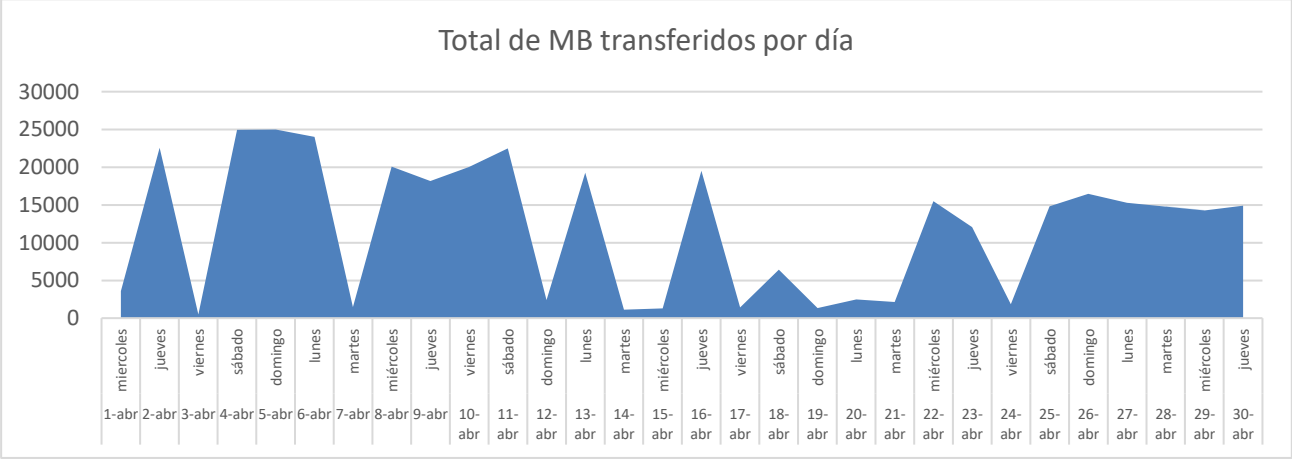


Ilustración 8 Fechas con mayor replicación

El comportamiento del tráfico de replicación durante el mes de Abril confirma una dinámica de carga por ráfagas, altamente vinculada a ciclos operativos específicos y a la actividad crítica de servidores puntuales.

- La transferencia de datos está altamente concentrada en la máquina virtual INR0243, esta VM representa aproximadamente el **95.5% del tráfico total** del mes que fue **339,855.39 MB** (aprox. **339GB**)

- El tráfico total de replicación en Abril fue de **360,087.94 MB (~360.09 GB)**.
- El fuerte incremento registrado entre febrero y marzo (210 GB) continuó su tendencia al alza en abril, alcanzando un nuevo máximo de 360 GB. Esta tendencia confirma la existencia de procesos de cierre de ciclo y tareas de mantenimiento pesado que generan una carga de escritura en disco significativamente mayor a principios de cada mes.
- La infraestructura ha dejado de mostrar la estabilización observada en febrero para retornar de forma sostenida a un estado de alta demanda.
- **El día de mayor tráfico** fue el **5 de Abril**, con un acumulado total de **24,983MB** (principalmente por INR0243).
- **El día de menor tráfico** fue 3 de abril (484,8 MB).

4.2.2.2. DataGuard Bases de Datos Megacenter

Durante el mes de Abril de 2026 se continuo con la replicación permanente de las BD Oracle al Datacenter alterno de acuerdo con las políticas establecidas, utilizando el Oracle Active DataGuard el cual garantiza una alta disponibilidad, protección de datos y recuperación ante desastres. Ver las evidencias en el documento Informe Mensual InfoTIC DBA Abril2026.pdf

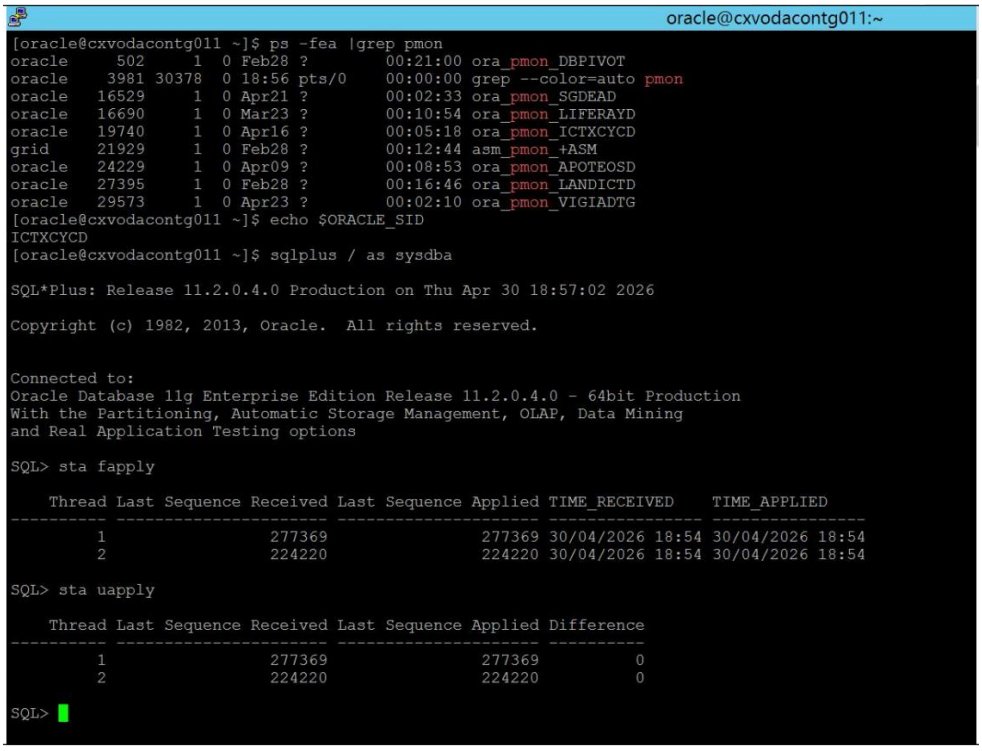


Ilustración 9 Evidencia DataGuard replicado a Megacenter BD

4.2.2.3. Servicios de Housing – Datacenter Alterno

A continuación, se presentan las máquinas alojadas en el Datacenter alterno en Medellín, las cuales estuvieron disponibles todo el mes de Abril al 100%:

No.	Dispositivo	Marca	Modelo
1	Switch CISCO	CISCO	3560
2	Switch DELL Networking	Dell	N4032 24 ports
3	Servidor rack Vmware	Dell	PowerEdge R630
4	Servidor rack Vmware	Dell	PowerEdge R630
5	Storage Controladora - SAN	Dell	CT-SC8000
6	Storage Controladora - SAN	Dell	CT-SC8000

Tabla 13 Disponibilidad de Servicios de Housing – Data Center Alterno

4.3. Seguridad informática

Durante el período evaluado, los eventos relacionados con intentos de acceso no autorizado fueron gestionados y mitigados oportunamente. El monitoreo continúo realizado por el SOC, junto con la correlación y análisis de eventos en FortiSIEM, permitió una detección temprana y una respuesta ágil, reduciendo el riesgo de afectación a los servicios institucionales.

Se llevó a cabo la actualización de las plataformas de seguridad a versiones estables, garantizando mayor protección frente a vulnerabilidades conocidas, mejoras en el rendimiento y alineación con buenas prácticas de ciberseguridad.

Se brindó acompañamiento técnico en la configuración de la VPN con el proveedor ANDSmartp, asegurando una comunicación segura, estable y acorde a los lineamientos de seguridad establecidos.

Se realizó la publicación del sitio pasareladepagos.icetex.gov.co, garantizando su disponibilidad y correcta configuración dentro de la infraestructura, contribuyendo a la continuidad y fortalecimiento de los servicios digitales ofrecidos.

A continuación, se presenta el diagrama de red que se tiene actualmente a nivel de los dispositivos de seguridad perimetral y el componente de antivirus Sophos.

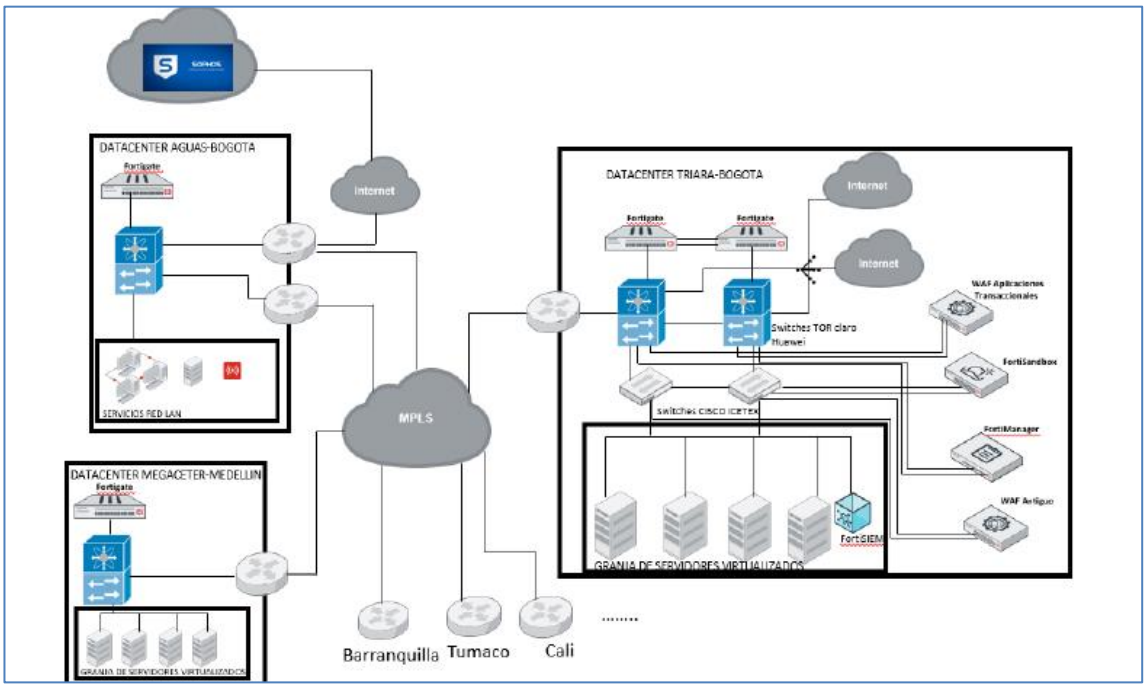


Ilustración 10 Diagrama de la Arquitectura de Seguridad

En la ilustración 11, se observa la implementación del WAF Cloud donde se utilizaron dos aplicaciones web para el DRP los cuales tienen como dominios: webdrp.icetex.gov.co y drp.Icetex.gov.co.

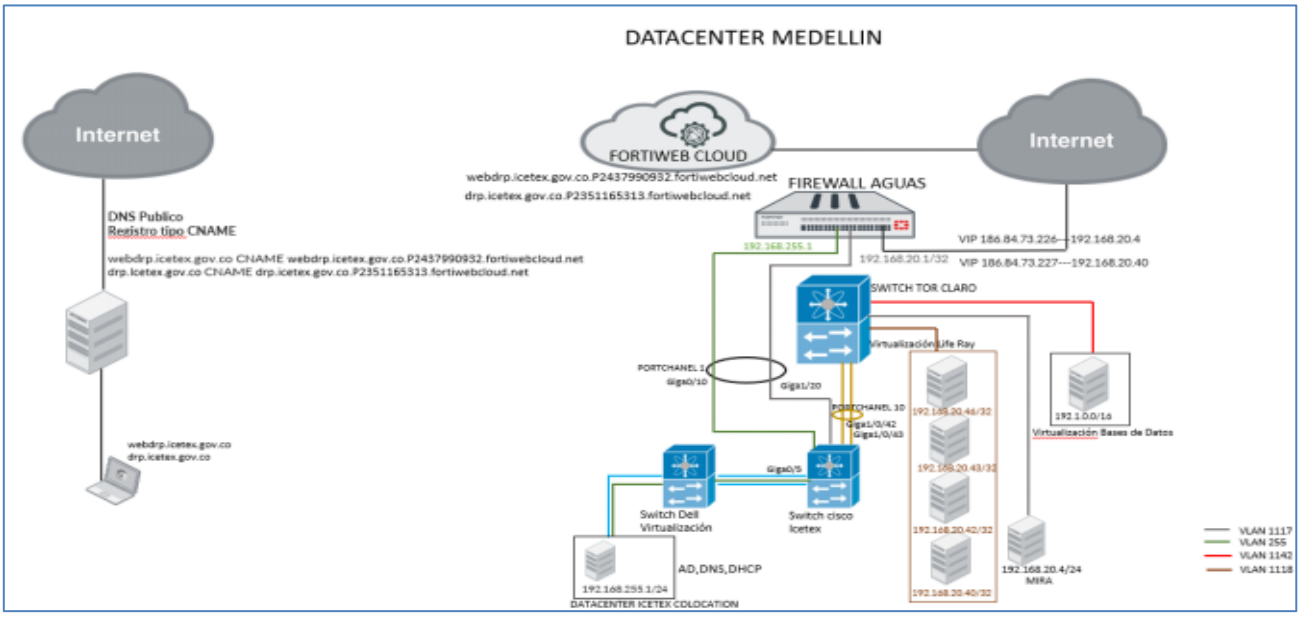


Ilustración 11 Topología de WAF Cloud usado en portales de Medellín

Respecto al firewall de la red de Aguas, se mantienen actualmente 541 políticas activas, las cuales continúan en proceso de evaluación con el propósito de consolidar configuraciones, eliminar reglas innecesarias y optimizar la operación de la red.

Las evidencias de esta gestión fueron incluidas en el numeral 6.2 del informe mensual de especialistas de seguridad del mes de abril, link: Informe Mensual InfoTIC Seguridad Abril2026.pdf

Durante el mes de Abril de 2026 se realizaron las actividades relacionadas con la administración y gestión de la seguridad perimetral:

4.3.1. Gestión y fortalecimiento de la seguridad perimetral.

Durante el mes de Abril de 2026, se llevaron a cabo diversas actividades relacionadas con la administración y gestión de la seguridad perimetral de la entidad.

- Configuración de nueva VLAN para la Mesa de Servicios.
- Afinamiento de los perfiles de navegación de la entidad.

4.3.2. Monitoreo de seguridad y respuesta ante incidentes

Se realizó un monitoreo constante de las plataformas de seguridad perimetral, asegurando la supervisión y el seguimiento oportuno de los eventos registrados.

Se atendieron los casos reportados por el SOC, proporcionando retroalimentación en aquellos que fueron identificados como falsos positivos, con el fin de apoyar los ajustes y afinamientos necesarios.

4.3.3. Gestión Operativa y soporte de seguridad

Se gestionaron y resolvieron oportunamente los casos reportados a través de la plataforma Aranda, así como las solicitudes recibidas por correo electrónico. El detalle de estas atenciones está documentado en secciones anteriores.

Se realizan ajustes en los permisos de accesos por vpn a las bases de datos de producción y desarrollo.

Atendiendo la solicitud, efectuada por parte del ICETEX, de habilitar la opción WAF USER TRACKING se procedió a establecer el alcance de la misma y se propuso el plan de trabajo, cuyas estimaciones preliminares están para una sola aplicación.

4.3.4. Plataformas Administradas

Las plataformas administradas por INFOTIC tanto las de propiedad del ICETEX como las que se encuentran en modalidad de IaaS son las siguientes:

SERIAL	MODELO	UBICACIÓN FÍSICA	OBSERVACIONES
FG6H0FTB22902021	FortiGate 600F	Aguas	Funciona como Firewall - Prestación como servicio infotic
FG180FTK22901087	FortiGate 1800F	Data Center Triara	Funciona como Firewall - Prestación como servicio infotic
FG180FTK22901182	FortiGate 1800F	Backup Data Center Triara	Funciona como Firewall - Prestación como servicio infotic
FG6H0FTB22902086	FortiGate 600F	Data Center Megacenter Medellín	Funciona como Firewall - Prestación como servicio infotic
FV-2KFTE21000029	FortiWeb 2000F	Data Center Triara	Función como WAF - Prestación como servicio infotic
FMG2HGTA22000550	FortiManager 200G	Data Center Triara	Prestación como servicio infotic
FSMP000000001340	FortiSIEM	Máquina Virtual vmware de cliente	Funciona como correlacionador de eventos - En VMware de Icetex
FV-2KE3117000046	FortiWeb 2000E	Data Center Triara	Función como WAF - Propiedad de Icetex
FV-2KE3117000032	FortiWeb 2000E	Data Center Triara	Función como WAF - Propiedad de Icetex
FSA1KD3A17000156	FortiSandbox 1000D	Data Center Triara	Funciona como Escaneo de archivos - Propiedad de Icetex
FAC1KD3A17000020	FortiAuthenticator 1000D	Data Center Triara	Funciona para autenticación y CA de certificados - Propiedad de Icetex
FAC1KD3A17000036	FortiAuthenticator 1000D	Data Center Triara	Propiedad de Icetex

Tabla 14 Detalle plataformas Seguridad administradas INFOTIC

A continuación, se presenta el estado actual de los tiempos de soporte y vigencias de los dispositivos FortiGate administrados:

Dispositivo	IP	Licenciamiento	Fin Licenciamiento	Datacenter
FW Fortigate 1800F (MST)	10.0.0.53	Si	18/05/2026	Triara
FW Fortigate 1800F (SLV)	10.0.0.53	Si	18/05/2026	Triara
FW FortiGate 600F	10.0.0.30	Si	1/06/2026	Megacenter
FW FortiGate 600F	10.1.100.33	Si	11/05/2026	Aguas

Tabla 15 Licenciamiento FortiGate

Se informa que las licencias asociadas a los dispositivos de seguridad próximos a vencer representan un riesgo significativo para la continuidad y estabilidad de la operación, toda vez que la expiración de las mismas puede limitar funcionalidades críticas relacionadas con protección, actualización de

firmas, soporte del fabricante, monitoreo y respuesta ante amenazas de ciberseguridad. Por lo anterior, se recomienda adelantar oportunamente las gestiones necesarias para su renovación, con el fin de evitar afectaciones en la prestación de los servicios y en los niveles de seguridad de la infraestructura tecnológica.

4.3.4.1. FortiGate Triara

A nivel de sistema, el firewall de Triara (FortiGate 1800F), no presenta afectaciones en cuanto a licenciamiento o performance.

El porcentaje de uso de la CPU y memoria se encuentra dentro de los estándares normales.

A continuación, se presentan los consumos en el presente mes:

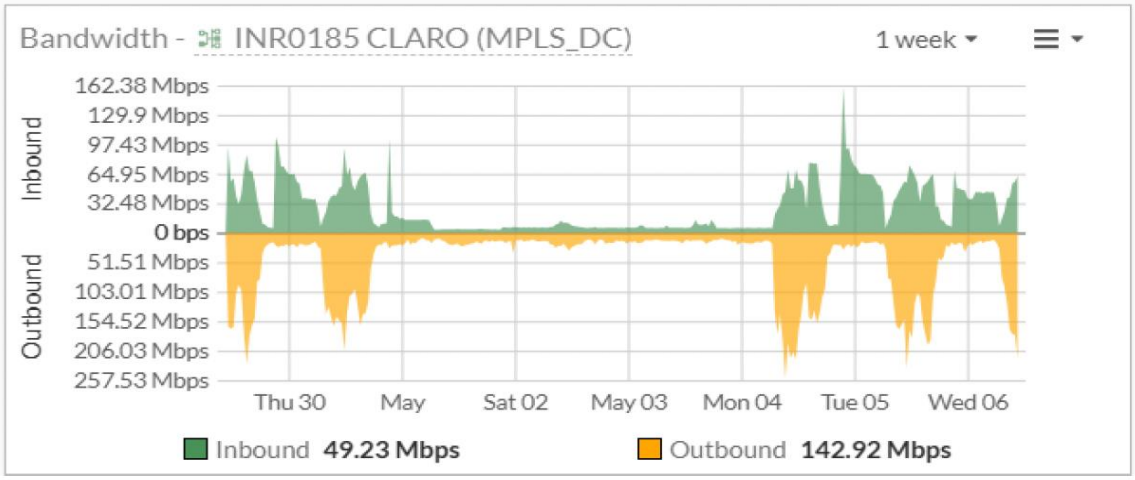


Ilustración 12 Consumo canal MPLS - promedio 71 MPPSG [INR0185 CLARO(MPLS_DC)]

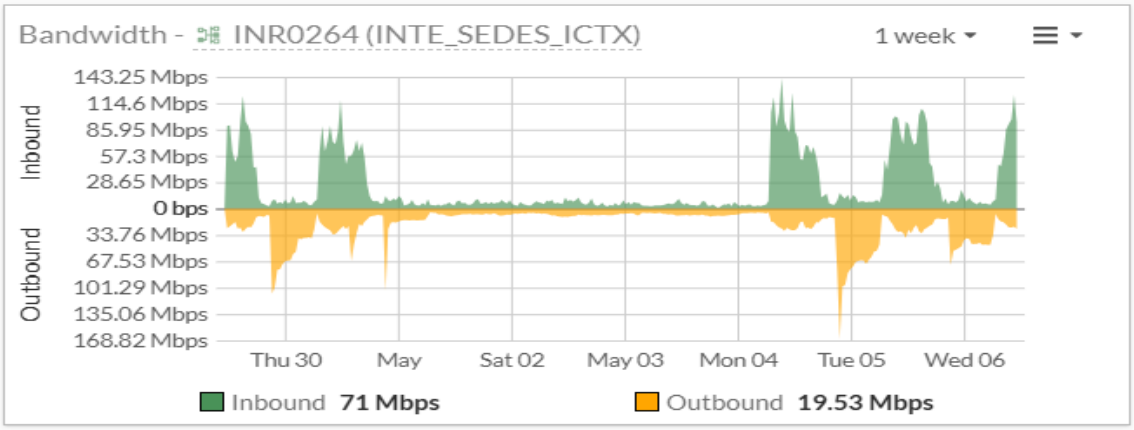


Ilustración 13 Consumo canal Internet Sedes - Prom 90.68 MBPS WAN-SEDES-ICETEX [INR0264 (INTE_SEDES_ICTX)]

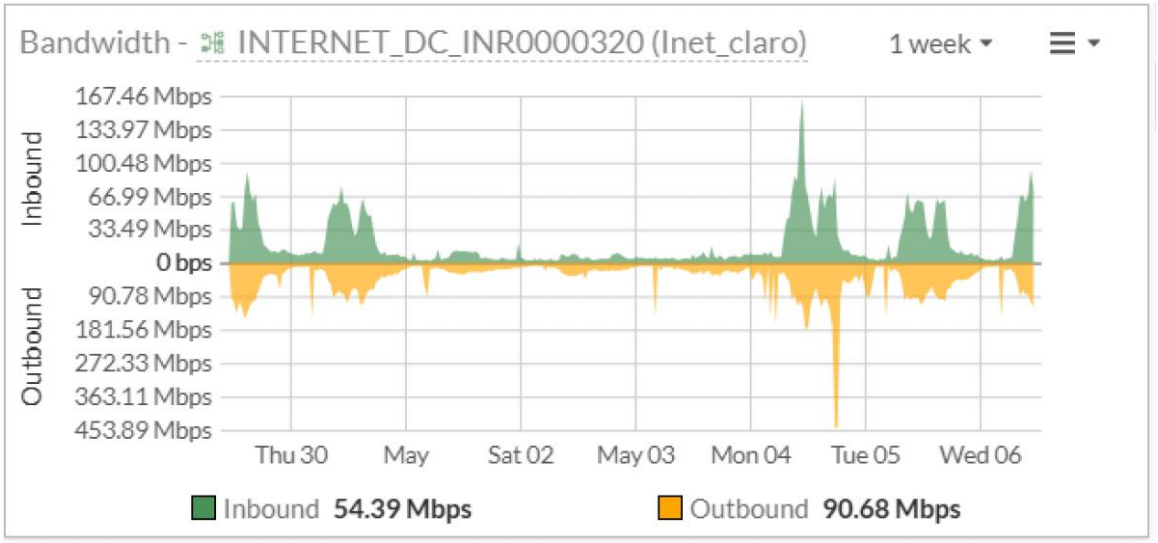


Ilustración 14 Consumo Canal INTERNET DATACENTER [INTERNET_DC_INR0000320 (Inet_claro)]

A nivel de perfiles de UTM (UTM son fragmentos de texto que se añaden al final de la URL y que sirven para rastrear, con mayor precisión, el origen de las visitas a una web), se tienen los siguientes perfiles para Web Filter, Antivirus y SSL Inspection actualmente:

Name	Comments	Ref.
WEB default	Perfil con las mínimas restricciones	0
WEB Mesa_de_Ayuda	Mesa_de_Ayuda	1
WEB Navegacionpcs_Comware	Perfil con restricciones	5
WEB Navegacionpcs_Comware_con_redes	Perfil con restricciones	2
WEB WF-Avanzado	Perfil para FSSO Navegación Avanzada	35
WEB WF-Comunicaciones	Perfil para FSSO comunicaciones	4
WEB WF-General	Perfil para todos	6
WEB WF-General_Sedes	Perfil para todos	2
WEB WF-Sede_Ibague_YT	27022025/InfoTIC/Tarea Aranda 517214 (17458) Se solicita el acceso a youtube	2
WEB WF-Tesoreria	Perfil con restricciones especificas por auditoria.	8
WEB WF-VIP	Perfil para FSSO Navegación_VIP	27
WEB WF-wetransfer	Perfil para FSSO Navegación Avanzada	2
WEB wifi-default	Perfil de FULL acceso para pruebas	1

Ilustración 15 Filtrado – WEB – (FortiGate – Triara)

Name	Read Only	Comments	Ref.
SSL Prueba certificate-inspection		Read-only SSL handshake inspection profile.	27
SSL certificate-inspection	🔒	Read-only SSL handshake inspection profile.	608
SSL certificate-inspection_2780		Read-only SSL handshake inspection profile.	2
SSL certificate-inspection_ICETEX		SSL para BUS de servicios	56
SSL certificate-inspection_IPv6		Read-only SSL handshake inspection profile.	1
SSL custom-deep-inspection		Customizable deep inspection profile.	0
SSL deep-inspection	🔒	Read-only deep inspection profile.	0
SSL no-inspection	🔒	Read-only profile that does no inspection.	433

Ilustración 16 Inspección – SSL – (FortiGate – Triara)

Name	Comments	Ref.
AV AV-FSB	HTTP,SMTP FULL FSB	105
AV AV-HTTP	HTTP con FSB	33
AV AV-HTTP&CIFS	HTTP,CIFS con FSB	7
AV AV-SMTP	SMTP FULL FSB	1
AV default	ALL con FSB	63
AV ICETEX		112
AV prueba2		91
AV wifi-default	ALL monitoreo sin FSB	1

Ilustración 17 Antivirus y Antimalware – Perimetral (FortiGate – Triara)

4.3.4.2. FortiGate Aguas

A nivel de sistema, el firewall de Aguas (FortiGate 600F), no presenta afectaciones en cuanto a licenciamiento o performance.

El porcentaje de uso de la CPU y memoria se encuentra dentro de los estándares normales.

A continuación se presentan los consumos en el presente mes:

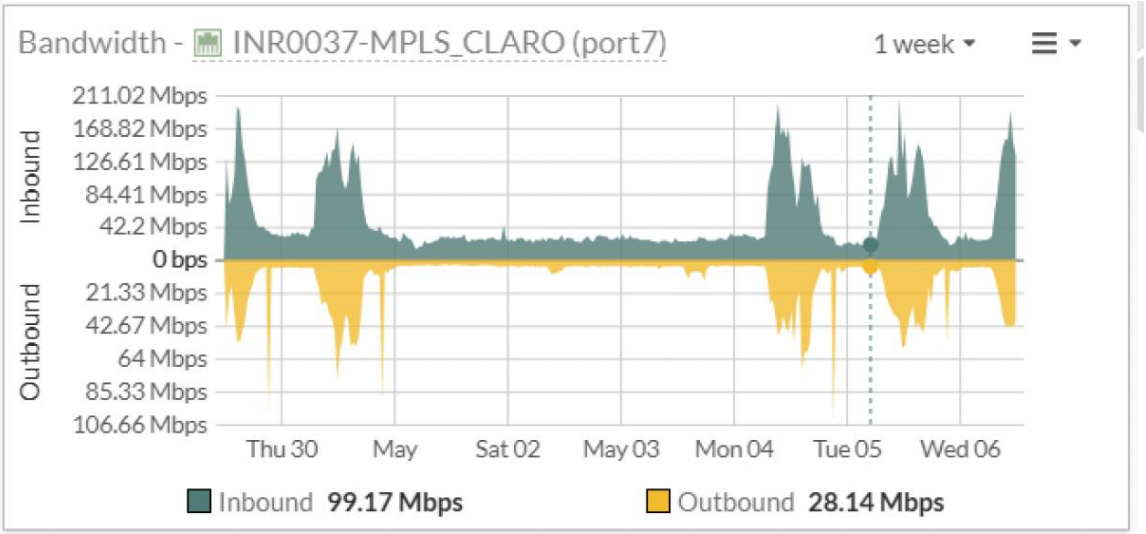


Ilustración 18 Consumo Canal MPLS Aguas - promedio 44.72 MBPS

A nivel de perfiles de UTM, se tienen los siguientes perfiles para Web Filter, Antivirus y SSL Inspección actualmente:

Name	Comments	Ref.
WEB default	Default web filtering.	0
WEB General_Icetex		89
WEB Mesa_de_Ayuda	Mesa_de_Ayuda	3
WEB monitor-all	Monitor and log all visited URLs, flow-based.	0
WEB VIP_FUNCIONARIOS		6
WEB wifi-default	Default configuration for offloading WiFi traffic.	1

Ilustración 19 Filtrado-Web-(FortiGate-Aguas)

Name	Read Only	Comments	R...
SSL certificate-inspection	🔒	Read-only SSL handshake inspection profile.	450
SSL certificate-inspection_WX		Read-only SSL handshake inspection profile.	11
SSL custom-deep-inspection		Customizable deep inspection profile.	0
SSL custom-deep-inspection_icetex		Customizable deep inspection profile.	0
SSL deep-inspection	🔒	Read-only deep inspection profile.	0
SSL no-inspection	🔒	Read-only profile that does no inspection.	340

Ilustración 20 Inspección-SSL-(FortiGate-Aguas)

Name	Comments	Ref.
AV-ICETEX		419
default	Scan files and block viruses.	7
wifi-default	Default configuration for offloading WiFi traffic.	1

Ilustración 21 Antivirus y Antimalware-Perimetral-(FortiGate-Aguas)

4.3.4.3. FortiGate Medellín

A nivel de sistema, el firewall de Medellín (FortiGate 600F), no presenta afectaciones en cuanto a licenciamiento o performance; actualmente se encuentra en la versión de FortiOS 7.4.11.

Se observa en la Ilustración 22, que la interfaz de la MPLS del Data Center de Medellín no presenta tráfico debido a que este se tiene como Data Center Alterno.

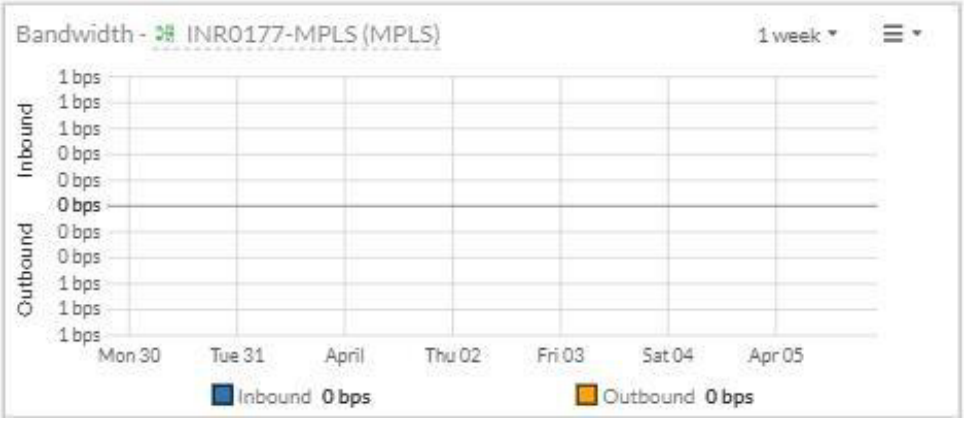


Ilustración 22 Consumo Canal MPLS Medellín

4.3.4.4. FortiWeb 2000F

A nivel de sistema del FortiWeb su versión de firmware se encuentra actualizada a la versión 7.6.7 la cual es una de las versiones actuales más estables.

4.3.4.5. FortiWeb 2000E

A nivel de sistema, el FortiWeb presenta su configuración actual y su versión de Firmware fue actualizada a la 7.6.5. Sin embargo, cabe aclarar que, a nivel de licenciamiento, los equipos no tienen un licenciamiento vigente en este momento.

Dispositivo	IP	Propiedad Icetex	Licenciamiento	Fin Licenciamiento	DC	End Of Order	Last Service Extension	End of support
Fortiweb1 2000E (WAF) (MST)	10.0.0.251	SI	No	20/06/2023	Triara	13/01/2022	13/01/2026	13/01/2027
Fortiweb2 2000E (WAF) (SLV)	10.0.0.251	SI	No	20/06/2023	Triara	13/01/2022	13/01/2026	13/01/2027
Fortiweb1 2000F (WAF)	192.168.91.10	No	Si	1/06/2026	Triara	N/A	N/A	N/A

Tabla 16 Licenciamiento FortiWeb

4.3.4.6. FortiWebCloud DRP

A nivel de sistema, el FortiWeb que se tienen en nube presenta su configuración la versión actual es 25.3.a, se encuentran pasando dos portales.

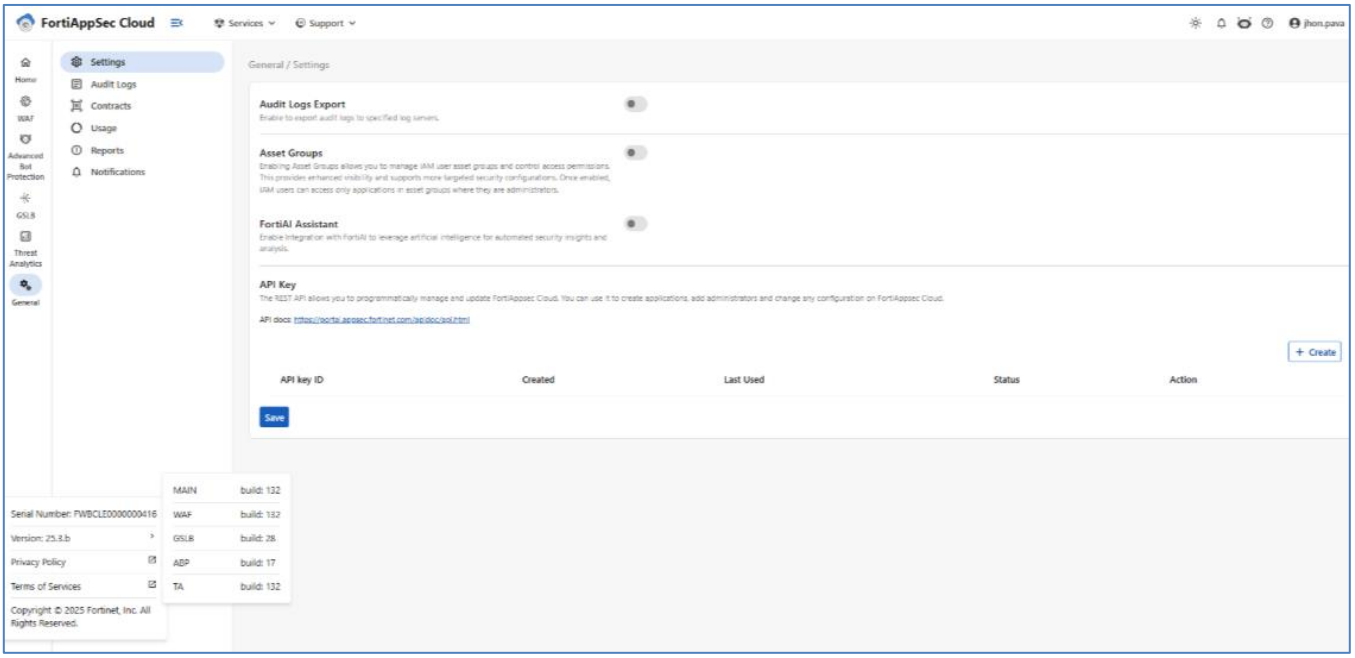


Ilustración 23 Tráfico General de los portales

4.3.4.7. FortiSandBox

A nivel de sistema, el Sandbox (FortiSandBox 1000D) muestra su configuración actual y su versión de firmware que actualmente se encuentra en la 3.2.4 siendo esta la última versión disponible para este dispositivo, ya que está en EOL (término empleado por el fabricante para describir un producto que pronto será reemplazado por una nueva generación de tecnología).

Dispositivo	IP	Propiedad Icetex	Licenciamiento	Fin Licenciamiento	DC	End Of Order	Last Service Extension	End of support
FortiSandbox 1000D	10.0.0.249	Si	No	1/06/2023	Triara	2/04/2019	2/04/2023	2/04/2024

Tabla 17 Configuración FortiSandBox 1000D

4.3.4.8. FortiSIEM

A continuación, se presenta el estado del licenciamiento del SIEM:

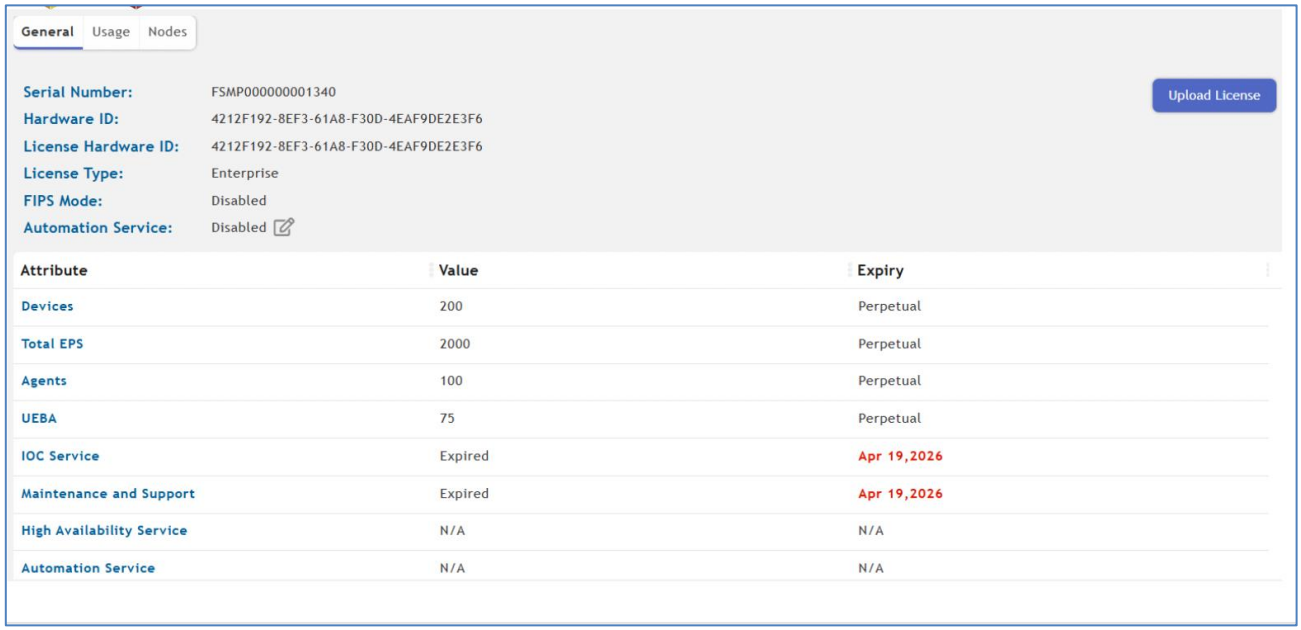


Ilustración 24 licenciamiento FortiSIEM

A continuación, se presenta el desempeño por procesos:

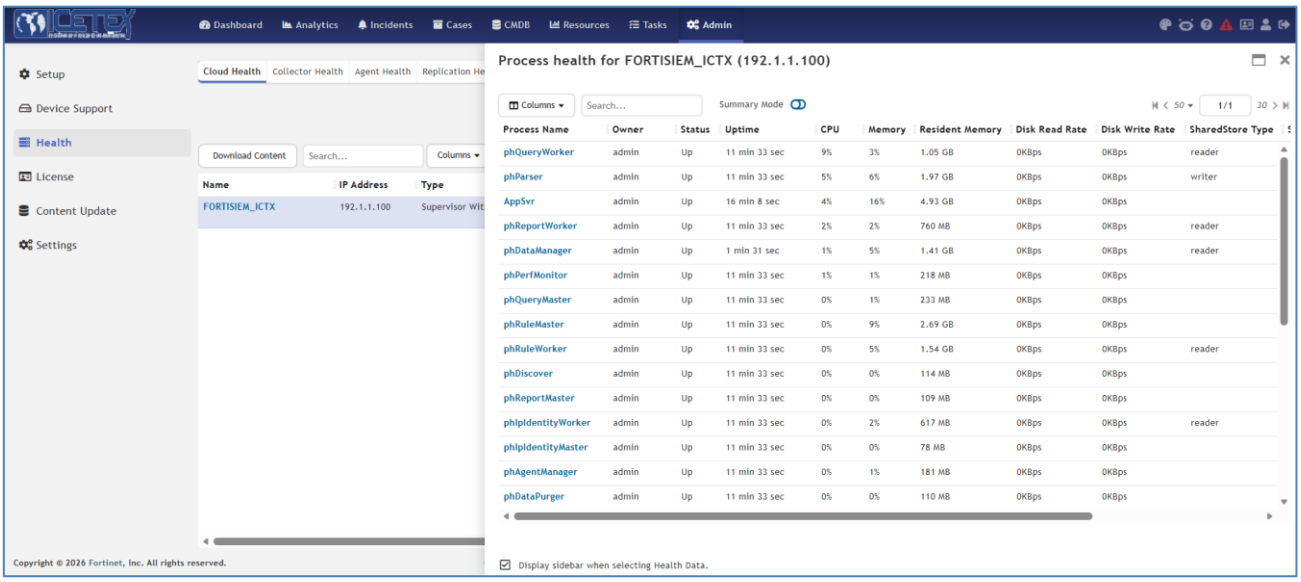


Ilustración 25 FortiSIEM Performance por procesos

4.3.4.9. Sophos EndPoint

En la ilustración 26, se observa un resumen del estado de Seguridad del Endpoint donde actualmente se están cumpliendo en un 100% los puntos de seguridad de la plataforma de Sophos indicando protección de equipos, políticas y exclusiones.

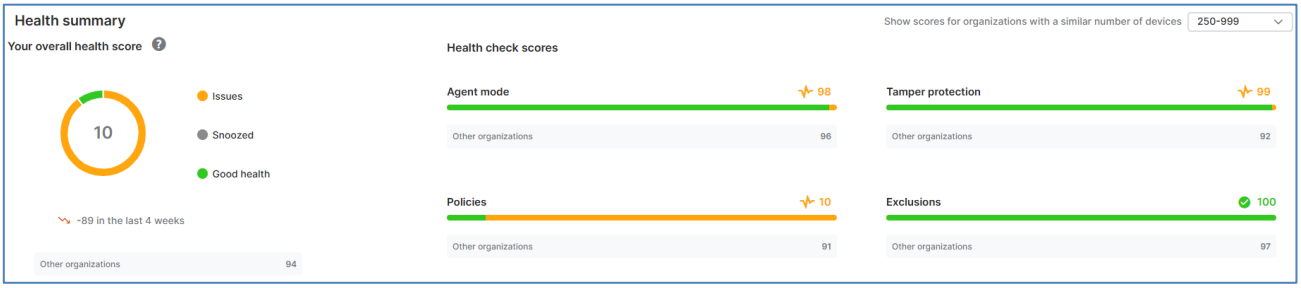


Ilustración 26 Estado Seguridad Sophos

En la sección 6.6.1 del informe de seguridad Informe Mensual InfoTIC Seguridad Abril2026.pdf se detallan las amenazas contenidas por la herramienta el Sophos instalado en los equipos ordenadores y servidores.

4.3.5. Recomendaciones de Seguridad para el ICETEX.

Recomendación	Estado	Criticidad	Fuente	Asunto	Personal de ICETEX a quien se notificó
Garantizar la segmentación de la red que permita claramente definir qué servicios deben ser alcanzados por cada usuario.	Como parte de las pruebas de IPv6, se están realizando pruebas de DHCPv6 en la red para que el servidor entregue direccionamiento IPv6 a las redes de la Entidad y que esta segmentación cumpla los estándares del protocolo IPv6.	Media	Informes Mensuales - sesiones	Segmentación Red ICETEX (Sesión Teams) / Segmentación de la red "Tesorería y Cartera" (Sesión Teams) / Validación de topología y segmentación Tesorería (Sesión Teams)	Grupo Coordinación de Infraestructura Tecnológica / Grupo Coordinación de Infraestructura Tecnológica / Especialista de seguridad
Se recomienda una tecnología que permita realizar análisis de tráfico de la red (NTA- Network Traffic Analysis.	En evaluación por parte de ICETEX.	Alta	N/A	N/A	N/A
Se recomienda una tecnología que permita la gestión o validación de privilegios de accesos (IAM). Evitar configurar usuarios y claves dentro de las aplicaciones de ICETEX.	En evaluación por parte de ICETEX.	Alta	N/A	N/A	N/A
Adquirir un equipo Firewall para correo para prevenir brechas de seguridad asociadas al uso del correo electrónico y que este es susceptible a muchos tipos de amenazas.	En evaluación por parte de ICETEX.	Alta	Informes Mensuales - sesiones	Reunión de pares de seguridad	Grupo Coordinación de Infraestructura Tecnológica / Grupo Coordinación de Infraestructura Tecnológica
Validar a nivel de punto final, los equipos que se han visto involucrados con comportamiento malicioso.	Se evalúa por parte de ICETEX. Se hace seguimiento por parte del SOC quien reporta comportamiento malicioso. Sin embargo, es necesario establecer políticas de conexión de equipos externos BYOD debido a que muchos de los casos reportados por el SOC vienen de equipos personales que no hacen parte de la Entidad.	Critica	Informes Mensuales	N/A	N/A
Integrar los equipos que hacen parte del proceso de pagos con el SIEM.	Se debe evaluar la capacidad del SIEM, se espera plan de mejora.	Media	Informes Mensuales - sesiones	Recursos de FORTISIEM CPU, Memoria y disco / Recomendaciones de arquitectura de FortiSIEM Icetex	Líder infraestructura / Especialista Desarrollo / Especialista de seguridad / Especialista de seguridad / Grupo Coordinación de Infraestructura Tecnológica / Profesional de tecnología
Evaluar los riesgos sobre las plataformas en la nube y considerar aplicar plataformas de seguridad para los ambientes cloud que cuenta la entidad ya que estos contienen servicios críticos para la misma.	En evaluación por parte de ICETEX.	Alta	N/A	N/A	N/A

Recomendación	Estado	Criticidad	Fuente	Asunto	Personal de ICETEX a quien se notificó
Se debe realizar la integración de los activos críticos de la compañía a la plataforma de SIEM, no se ha podido lograr por la falta de recursos de este.	En evaluación por parte de ICETEX.	Alta	Informes Mensuales - sesiones	Recursos de FORTISIEM CPU, Memoria y disco / Recomendaciones de arquitectura de FortiSIEM Icetex	Líder infraestructura / Especialista Desarrollo / Especialista de seguridad / Especialista de seguridad / Grupo Coordinación de Infraestructura Tecnológica / Profesional de tecnología

Tabla 18 Recomendaciones de Seguridad

4.3.6. Servicio de centro de Operaciones de Seguridad (SOC)

De acuerdo con las conexiones y las reglas configuradas sobre la herramienta de monitoreo SOC FortiSIEM, el cual analiza las alertas en busca de patrones de comportamiento inusuales; estas reglas estudian y conectan las alertas para evaluar su prioridad y confiabilidad. Actualmente el motor de búsqueda de amenazas está distribuido en cuatro criterios de búsqueda y correlación, los cuales son: compromiso del sistema, explotación e instalación de agentes maliciosos, entrega y ataque, reconocimiento y sondeo y finalmente advertencia ambiental o anormalidades detectadas sobre el rendimiento de la máquina. Dichos criterios distribuyen los alertas e incidentes de esta manera de acuerdo con el match que el sistema ejecute y categorice dentro de sus reglas de correlación previamente configuradas o implementadas por defecto. Las cuales detectan alertas e incidentes de tipo:

- Descarga de ejecutables sospechosos provenientes de un sitio de mala reputación
- Actividad de escaneo en la red, en función de descubrimiento de puertos
- Violación, infracción y vulneración de políticas de seguridad
- Detección de malware
- Detección de ataques (Fuerza Bruta, puerta trasera (Shell), Botnet o kit de explotación de un sitio malicioso, XSS, Inyección de SQL, DoS
- Monitoreo de alertas de autenticación
- Monitoreo de alertas de sistema
- Monitoreo de alarmas y alertas de seguridad
- Monitoreo de accesibilidad
- Monitoreo de bases de datos
- Alertas e incidentes de tráfico y navegación
- Alertas de acceso permitido a páginas web maliciosas o de baja reputación

A la fecha de presentación de este informe se encuentran definidas 2.382 reglas de seguridad, las cuales, tienen como fin reconocer cualquier posible vector de ataque, así como verificar que los equipos de seguridad perimetral (Firewall, IPS, NAC, etc.), estén bien configurados a nivel de sus políticas de seguridad.

Para los casos de uso de disponibilidad se cuenta con 174 reglas, que tienen como función principal alertar algún tipo de falla o indisponibilidad de los equipos de la entidad y hacer la respectiva notificación, en caso de requerirse, al ICETEX.

Para cualquier detalle relacionado con las reglas puede consultarse en el siguiente Informe Mensual SOC-TH ICETEX abril 2026.pdf

Para **THREAT HUNTING** específicamente son tres componentes: **Casos de Uso Seguridad, Indicadores de Compromiso y Tableros de control.**

4.3.6.1. Indicadores de compromiso (Thread Hunting):

Un indicador de compromiso puede venir dado bajo la forma de un nombre de archivo, el nombre de un proceso en el administrador de tareas, una URL o dirección IP, comportamiento anómalo en el tráfico web, intentos de inicio de sesión fallidos, entre otros tantos más.

Los siguientes indicadores son colectados por los Analistas del SOC, a través de convenios con el FISRT, con otros CSIRT, e Inteligencia y Caza Amenazas.

Indicadores de compromiso (IOC)	Abril	Marzo	Febrero	Enero
IOC – Malware DOMINIOS	6.047	6.047	6.047	6.047
IOC – Malware IPs	11.167	11.167	11.119	11.119
IOC – Malware HASH	1.627	1.627	1.627	1.627
IOC – Malware URL	4.564	4.564	4.564	4.564

Tabla 19 Comparativo – Indicadores de Compromiso

Después de efectuado el registro de alertas se considera y diseña la generación de alertas y niveles de criticidad, acorde con la experiencia del equipo consultor, aplicación de buenas prácticas y reuniones de trabajo efectuadas a nivel de infraestructura tecnológica alineado con el proceso de levantamiento de riesgos.

De acuerdo con las conexiones y las reglas configuradas sobre la herramienta de monitoreo SOC FortiSIEM, el cual analiza las alertas en busca de patrones de comportamiento inusuales; estas reglas estudian y conectan las alertas para evaluar su prioridad y confiabilidad.

En el Informe del SOC se presentan gráficas y tablas de los tipos de alertas presentados durante el periodo monitoreado de: Seguridad – Disponibilidad – Rendimiento, donde estos a su vez se encuentran distribuidos con niveles de severidad con tres colores:

- Rojo: severidad o criticidad ALTO (10-9)
- Amarillo: severidad o criticidad MEDIO (6-8)
- Verde: severidad o criticidad BAJO (1-5)

4.3.6.2. Alertas o Incidentes de Seguridad Detectados

En el documento Informe Mensual SOC-TH ICETEX abril 2026.pdf se ven las alertas generadas a lo largo del periodo monitoreado, dichas alertas se clasifican en 3 categorías principales de monitoreo,

las cuales corresponden a Seguridad, Disponibilidad y Rendimiento, a partir de este informe se presenta un resumen de las alertas de seguridad y se incluye amenazas cibernéticas, sin embargo, el detalle del tratamiento que se realizó a cada uno de los casos se debe revisar en el Informe mencionado anteriormente.

4.3.6.2.1. Categoría Seguridad

A continuación, se relacionan las alertas presentadas en el periodo analizado, definiendo el top de los que han tenido mayor concurrencia a nivel de seguridad:

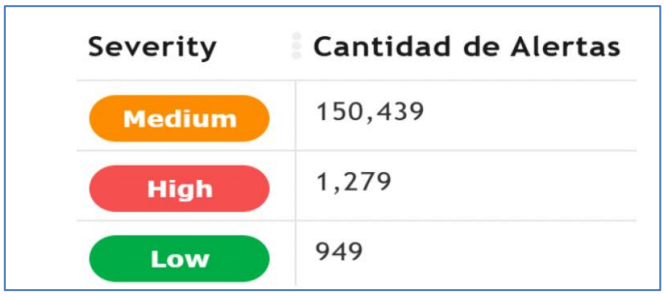


Ilustración 27 Total de alertas de seguridad

Durante el período evaluado de 151.727 alertas de seguridad identificadas, se presentaron con criticidad ALTA un total de 1.279 equivalentes al 0,8% del periodo. En el informe mensual del SOC, se puede observar la cantidad según el tipo de alerta y se realiza una descripción de los tipos de alertas que mayor cantidad de registros o que requieran una indagación más exacta. El comparativo, en los últimos 7 meses, se presenta a continuación:

Alertas Seguridad	Abril	Marzo	Febrero	Enero	Diciembre	Noviembre	Octubre
High	1.279	1.565	2.213	1.674	1.198	1.862	2.599
Medium	150.439	92.076	153.406	137.305	50.794	178.911	250.034
Low	949	756	1.356	1.775	856	1.076	2.556

Tabla 20 comparativo Alertas de Seguridad

Durante el período evaluado se presentaron 1.279 alertas de seguridad con criticidad ALTA, disminuyó con relación a periodos anteriores. En el documento Informe Mensual SOC-TH ICETEX abril 2026.pdf se presenta la cantidad según el tipo de alerta y se realiza una descripción de los tipos de alertas que mayor cantidad de registros o que requieran una indagación más exacta.

En cuanto a las alertas altas, el top 10 se presenta a continuación:

Tipo de Alerta	Severidad	Táctica	Cantidad de Alertas
Concurrent Failed Authentications To Same Account From Multiple Countries	9	Credential Access	673
Critical large Outbound Transfer To Outside My Country ICETEX- WX N3	9		149
System Exploit Detected by Network IPS	9		130
Brute_Force_Host_Login_Success_CUSTOMISADA_8_10_2021	9		87
Successful VPN Logon From Outside My Country WXN2	9	Credential Access	46
Denegacion_de_Servicios_desde_Internet_WX_Nivel3	9	Impact	39
Repeated Multiple Logon Failures: Server	9	Credential Access	34
Heavy UDP Port Scan: Single Host	9	Discovery	22
Multiple Distinct IPS Events From Same Src	9		14
Multiple Logon Failures: Database	9	Credential Access	12

Ilustración 28 Top 10 de Alertas de Seguridad Altas

Durante el período evaluado se presentaron 150.439 alertas de seguridad con criticidad MEDIA. Debido a las limitantes de recursos de la herramienta FortiSIEM no se puede realizar un análisis preciso de las alertas.

4.3.6.2.2. Categoría Disponibilidad

Debido a las limitantes de recursos de la herramienta FortiSIEM no se puede realizar un análisis preciso de las alertas.

4.3.6.2.3. Amenazas de Ciberseguridad

Debido a las limitantes de recursos de la herramienta FortiSIEM no se puede realizar un análisis preciso de las alertas.

4.3.6.3. Threat Hunting

Debido a las limitantes de recursos de la herramienta FortiSIEM no se puede realizar la extracción de información de este componente.

4.3.6.4. Análisis de Marca OSINT

Durante el periodo evaluado, la plataforma de monitoreo de protección de marca y OSINT – AXUR, reporta un total de 14 posibles amenazas de las 35,4k que fueron encontradas y analizadas automáticamente por la plataforma de monitoreo. A estas 14 posibles amenazas se les realizó una revisión y análisis interno, de sus características, datos e información.

Es importante resaltar que la plataforma de monitoreo realiza su labor a través de los siguientes módulos:

- fraudes digitales: Uso fraudulento de la marca.
- Fuga de datos: Credenciales y datos sensibles expuestos.
- Piratería Online: Ventas y distribuciones no autorizadas.
- Deep & Dark Web: Mención de la marca en entornos no indexados

Durante el periodo evaluado se detectó 05 incidentes de los cuales, 02 están relacionados con Actividad sospechosa en sitio web, 01 con Nombre de dominio similar, 01 con Perfil falso en red social y 01 con Exposición de secreto en código.

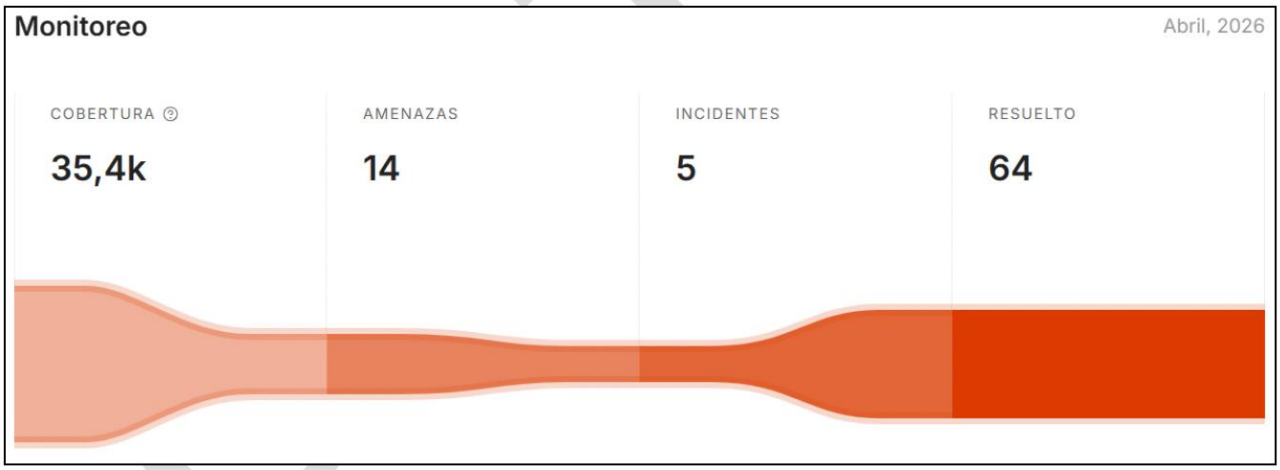


Ilustración 29 Incidentes por Tipo de Amenaza

En cuanto a fraudes digitales, durante el periodo evaluado, se presentó un total de 06 casos, de los cuales 03 casos fueron descartados, teniendo en cuenta que algunos no tenían relación y otros solo mencionaban la marca, 02 casos fueron reportados a la entidad y se encuentra en estado de tratamiento y 01 caso está en cuarentena. A continuación, se muestra la tabla con la información detallada.

KEY	FECHA DE DETECCIÓN	ESTATUS	TIPO	ESTADO	RESOLUCIÓN	FECHA DE CIERRE
EI8WLA	9/04/2026 14:24	Cuarentena	Nombre de dominio similar	Abierto	Cuarentena	
T8O45M	23/04/2026 3:43	En tratamiento	Perfil falso en red social	Abierto	Ninguna	
RUQGDA	9/04/2026 11:56	En tratamiento	Nombre de dominio similar	Abierto	Ninguna	
R9LEUH	3/04/2026 3:36	Cerrado	Perfil falso en red social	Cerrado	Descartada	6/04/2026 17:30
JC2E4S	1/04/2026 9:08	Cerrado	Uso fraudulento de marca	Cerrado	Descartada	1/04/2026 9:27
6VSS7O	3/04/2026 3:36	Cerrado	Perfil falso en red social	Cerrado	Descartada	6/04/2026 17:30

Ilustración 30 Incidentes por Fraudes Digitales

En cuanto a fuga de datos, durante el periodo evaluado, se presentaron 03 casos, de los cuales 02 casos fueron descartados, teniendo en cuenta que algunos no tenían relación con la entidad o solo se mencionaba la marca, el caso restante fue reportado a la entidad y se encuentra resuelto. A continuación, se muestra la tabla con la información detallada

KEY	FECHA DE DETECCIÓN	ESTATUS	TIPO	ESTADO	RESOLUCIÓN	FECHA DE CIERRE
LHQVST	16/04/2026 3:20	Cerrado	Exposición de secreto de código	Cerrado	Descartada	17/04/2026 10:42
I037X1	29/04/2026 12:10	Cerrado	Exposición de secreto de código	Cerrado	Descartada	30/04/2026 15:02
4AW4IZ	21/04/2026 3:21	Cerrado	Exposición de secreto de código	Cerrado	Resuelto	21/04/2026 14:58

Ilustración 31 Incidentes por Fuga de Datos

Durante el periodo evaluado, se presentó 01 caso, el cual fue descartado teniendo en cuenta que no tenía relación con la entidad.

Casos Relacionados con el módulo Deep & Dark Web. Durante el periodo evaluado, se presentó 03 casos, de los cuales 02 fueron reportados a la entidad y 01 caso fue descartado. A continuación, se muestra la tabla con la información detallada.

KEY	FECHA DE DETECCIÓN	ESTATUS	TIPO	ESTADO	RESOLUCIÓN	FECHA DE CIERRE
DHA1RA	28/04/2026 3:17	En tratamiento	Actividad sospechosa en sitio web	Abierto	Ninguna	
85URMB	28/04/2026 3:17	En tratamiento	Actividad sospechosa en sitio web	Abierto	Ninguna	
NCTJUH	29/04/2026 3:16	Cerrado	Actividad sospechosa en sitio web	Cerrado	Descartada	29/04/2026 10:04

Ilustración 32 Incidentes módulo Deep & Dark Web

No obstante, se mantiene el seguimiento continuo sobre este vector con el fin de detectar oportunamente cualquier eventualidad.

Los casos se encuentran detallados en el Informe Mensual SOC-TH ICETEX abril 2026.pdf

Con respecto a la gestión que se ha venido realizando, se recomienda hacer una retroalimentación de los casos reportados ya que no se ha tenido respuesta por del ICETEX, esto es con el fin de mitigar las brechas de seguridad detectadas a través de la plataforma de monitoreo de protección de marca y OSINT y para proceder con los cierres de casos.

Con respecto a los casos de Fraudes Digitales – Uso fraudulento de marca - recordar las medidas a considerar:

- Se recomienda notificar al área legal o de propiedad intelectual del ICETEX para que evalúe la posibilidad de solicitar la remoción del contenido o el cese del uso no autorizado de la marca. Aunque no se evidencia riesgo de phishing ni compromiso de información sensible, este tipo de uso indebido puede afectar la reputación corporativa o generar confusión entre los usuarios.
- Se recomienda mantener el monitoreo activo para detectar posibles reincidencias o la aparición de otros dominios, cuentas o páginas con características similares.

- Una vez realizadas las acciones correspondientes, se solicita responder vía correo electrónico para poder dar cierre al caso.

Con respecto a los casos de Fuga de Datos – fuga de código secreto- recordar las medidas a considerar:

- En caso de que el repositorio no sea de propiedad del cliente y contenga información sensible, se recomienda que el área legal del ICETEX contacte al administrador o webmaster correspondiente para solicitar de manera inmediata la eliminación de la información expuesta, o, en su defecto, restringir su acceso de forma privada.
- Asimismo, se sugiere revisar y fortalecer las políticas internas sobre el manejo, almacenamiento y distribución de información confidencial, con el propósito de prevenir futuras exposiciones.
- Finalmente, es indispensable verificar y confirmar que la información compartida o publicada tenga efectivamente carácter confidencial y que no deba estar disponible de manera pública.

4.3.7. Análisis de Vulnerabilidades ICETEX

Durante abril de 2026, se concertó la ejecución de los escaneos de vulnerabilidades para el mes de mayo. Las actividades se centrarán en un grupo de activos distribuidos de la siguiente manera:

- 17 BD
- 2 WAF
- 3 FW
- 4 URL
- 12 Servers

Esto con el fin de dar continuidad a las actividades de control, identificación de vulnerabilidades y fortalecimiento de la postura de seguridad tecnológica.

Se precisa que la programación correspondiente a los demás meses se encuentra actualmente en proceso de planeación por parte del ICETEX.

4.4. Servicios de nube

Durante el mes de abril de 2026, el rol de Integrador de Nube para ICETEX orientó sus actividades al fortalecimiento integral del entorno Microsoft Azure, abordando de manera estructurada aspectos críticos como seguridad, conectividad híbrida, gobernanza, optimización de costos, resiliencia y estabilidad operativa. Estas acciones se desarrollaron en el marco del Contrato 2022-0792, alineadas con buenas prácticas del Cloud Adoption Framework (CAF) y el Well-Architected Framework de Microsoft.

En el componente de mensajería, se logró estabilizar el servicio de envío de correos mediante Azure Communication Services, mitigando problemas de entregabilidad derivados de picos de tráfico asociados a procesos de autenticación y altos volúmenes de envío. A través de la implementación de controles de volumen, depuración de listas de destinatarios y análisis detallado de métricas consolidadas en reportes, se redujo significativamente la tasa de fallos, se mejoró la reputación del servicio frente a los proveedores de correo y se establecieron condiciones técnicas favorables para la aprobación de incremento de cuota por parte de Microsoft. Este proceso permitió además evolucionar hacia un modelo de gestión basado en datos, fortaleciendo el monitoreo continuo y la toma de decisiones informadas.

En materia de conectividad e integración, se gestionó la habilitación de accesos seguros mediante VPN SSL hacia recursos críticos en Azure, permitiendo la administración remota controlada bajo estándares de seguridad definidos. De igual manera, se avanzó en la integración de máquinas virtuales en la nube con el dominio corporativo on-premises, habilitando autenticación centralizada mediante Active Directory. Estas acciones consolidan el modelo de operación híbrida, mejoran la trazabilidad de accesos y fortalecen la continuidad operativa del entorno.

Desde la perspectiva de arquitectura y planeación tecnológica, se realizó la revisión técnica de la propuesta de migración de servidores a Azure, identificando inconsistencias en la estimación de costos y riesgos asociados al licenciamiento, especialmente en componentes críticos como Oracle Database. Este análisis permitió generar observaciones y recomendaciones que contribuyen a una toma de decisiones más precisa, evitando posibles impactos financieros y asegurando una planeación alineada con criterios técnicos sólidos.

Uno de los principales logros del periodo fue la ejecución del assessment integral de la infraestructura Azure, el cual alcanzó un nivel de cumplimiento del 96% sobre el plan de trabajo definido. Como resultado, se logró la depuración de recursos huérfanos, la reducción de la superficie de exposición pública, el fortalecimiento de la postura de seguridad mediante cierre de accesos críticos y la implementación de controles preventivos automatizados a través de Azure Policies. Asimismo, se optimizaron costos mediante la eliminación de recursos innecesarios, ajustes en almacenamiento y validación de beneficios de licenciamiento, y se mejoró la resiliencia del entorno mediante la normalización de backups, configuración de alertas y adopción de esquemas de redundancia zonal.

En el frente de gobernanza, se establecieron lineamientos para la estandarización de recursos, incluyendo la implementación de etiquetas obligatorias y la definición de políticas de control que permiten prevenir configuraciones inseguras en el futuro. Estas acciones contribuyen a la sostenibilidad operativa del entorno, mejoran la trazabilidad de los recursos y facilitan la administración centralizada del tenant.

Desde el punto de vista financiero, el comportamiento del mes de abril evidencia una reducción significativa del 81.9% en el costo total frente a marzo, pasando de USD 77,745.24 a USD 14,067.30.

Este cambio refleja la finalización de cargas intensivas asociadas a servicios específicos utilizados en el mes anterior y el retorno a un modelo de consumo más estable y controlado. El gasto se concentra nuevamente en componentes estructurales como almacenamiento y máquinas virtuales, con una distribución más equilibrada entre los diferentes grupos de recursos y regiones, lo que indica una recuperación del control financiero del entorno.

En términos generales, el mes de abril representa una transición clara desde un escenario de expansión intensiva hacia una fase de normalización, estabilización y control del entorno cloud. El resultado es una plataforma más segura, optimizada, gobernada y resiliente, con capacidades operativas estables y un comportamiento financiero predecible. Esto permite proyectar continuidad en la operación, reducción de riesgos y una gestión más eficiente y sostenible de los recursos tecnológicos en la nube para ICETEX en los próximos periodos.

5. GESTION DE LA EJECUCIÓN CONTRACTUAL

El contrato 2022-0792 con fecha de perfeccionamiento del acta de inicio del 30 de febrero del 2022, donde se establece un plazo del contrato de 39 meses, el cual se compone de una fase de transición de 3 meses y una fase de operación de 36 meses, el plazo comenzó a contar a partir de la firma del acta de inicio que fue el 12 de febrero del 2023, y la ejecución de los servicios en fase de operación desde el 1 de abril de 2024, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato, es de aclarar que la fase de transición no es facturable.

En el presente informe del mes de Abril del 2026 del proyecto, se encuentra en la fase de operación de los servicios contemplados en el alcance, para lo cual INFOTIC presenta:

- Informes de cada uno de los especialistas.
- Reportes e informes generados por cada uno de los aliados estratégicos sobre la gestión realizada.
- Las evidencias sobre las situaciones y acciones realizadas sobre eventos presentados en la operación de INFOTIC sobre la infraestructura del ICETEX.

6. GESTION PRESUPUESTAL

A continuación, se relacionan los pagos realizados por ICETEX a INFOTIC durante la ejecución del proyecto, de acuerdo con los informes presentados con la evidencia de las actividades realizadas:

EJECUCIÓN PRESUPUESTAL						
VALOR INICIAL DEL CONTRATO	**VALOR VIGENCIA 2023**	**VALOR EJECUTADO 2023**	**VALOR BOLSA VIGENCIA 2023**	**VALOR BOLSA EJECUTADO 2023**	**VALOR BOLSA NO EJECUTADO 2023**	**VALOR NO EJECUTAD0 2023**
$ 31.398.996.857,96	$7.856.847.477	$5,550,653,552.00	$360,000,000	$2,700,000	$357,300,000	$2,303,493,925.00
	VALOR VIGENCIA 2024	**VALOR EJECUTADO 2024**	**VALOR BOLSA VIGENCIA 2024**	**VALOR BOLSA EJECUTADO 2024**	**VALOR BOLSA NO EJECUTADO 2024**	**VALOR NO EJECUTAD0 2024**
	$10,466,332,286.04	$ 8,888,383,619	$480,000,000	$0	$480,000,000	$1,587,413,017.00

INFOTIC
SOLUCIONES INTELIGENTES

	VALOR VIGENCIA 2025	VALOR EJECUTADO 2025	VALOR BOLSA VIGENCIA 2025	VALOR BOLSA EJECUTADO 2025	VALOR BOLSA NO EJECUTADO 2025	VALOR NO EJECUTAD0 2025
	$13,237,277,006.00	$11,406,758,386	$480,000,000	$420,000,000	$60,000,000	$1,830,518,620.12
	VALOR VIGENCIA 2026	**VALOR EJECUTADO 2026**	**VALOR BOLSA VIGENCIA 2026**	**VALOR BOLSA EJECUTADO 2026**	**VALOR BOLSA NO EJECUTADO 2026**	**VALOR NO EJECUTAD0 2026**
Contrato Inicial	$2,618,949,159.00		$120,000,000	**0**	$120,000,000	0
OTROSI4-Continuidad de Servicios por 8 meses	**$ 8.641.116.065**					
Total Vigencia 2026	**$11.260.065.224,00**	$ 3.215.512.304	$120,000,000	**0**	$120,000,000	$ 8.044.552.920
OTROSI3-Adición Servicios	**ITEM1 Arquitectura de Seguridad**	**ITEM2 Gestion de Vulnerabilidades**	**ITEM3 Pruebas de Pentesting**	**ITEM4 Continuidad**		
$ 2.761.480.370	**$ 762.253.015**	**$275.243.152**	**$208.285.884**	**$1.515.698.319**		**Valores Totales**

CONCEPTO							***VALOR***
VALOR TOTAL DEL CONTRATO Inicial							***$ 31,398,996,857.96***
OTROSI3-Adición Servicios							***$ 2.761.480.370***
OTROSI4-Continuidad de Servicios por 8 meses							**$ 8.641.116.065**
VALOR TOTAL DEL CONTRATO							**$ 42.801.593.293**
VALOR PAGADO							
Pago No. 1 -	mes:	Abril	de	2023	$ 537.090.736,00		$ 20,628,979,988.10
Pago No. 2 -	mes:	Mayo	de	2023	$ 544.104.546,00		
Pago No. 3 -	mes:	Junio	de	2023	$ 596.978.314,00		
Pago No. 4 -	mes:	Julio	de	2023	$ 624.431.841,60		
Pago No. 5 -	mes:	Agosto	de	2023	$ 650.825.466,00		
Pago No. 6 -	mes:	Septiembre	de	2023	$ 661.959.450,00		
Pago No. 7 -	mes:	Octubre	de	2023	$ 641.792.285,00		
Pago No. 8 -	mes:	Noviembre	de	2023	$ 633,094,717.00		
Pago No. 9 -	mes:	Diciembre	de	2023	$ 663.076.196,00		
Pago No. 10 -	mes:	Enero	de	2024	$ 681.934.328,00		
Pago No. 11 -	mes:	Febrero	de	2024	$ 732,950,102.00		
Pago No. 12 -	mes:	Abril	de	2024	$ 733.890.372,09		
Pago No. 13 -	mes:	Abril	de	2024	$ 730,351,368.00		
Pago No. 14 -	mes:	Mayo	de	2024	$ 719,104,204.57		
Pago No. 15 -	mes:	Junio	de	2024	$ 713,673,218.00		
Pago No. 16 -	mes:	Julio	de	2024	$ 751,372,731.00		
Pago No. 17 -	mes:	Agosto	de	2024	$755,684,192.00		
Pago No. 18 -	mes:	Septiembre	de	2024	$ 752,502,515.00		
Pago No. 19 -	mes:	Octubre	de	2024	$ 770,522,532.00		
Pago No. 20 -	mes:	Noviembre	de	2024	$ 774,178,154.00		
Pago No. 21 -	mes:	Diciembre	de	2024	$ 772,219,902.00		
Pago No. 22 -	mes:	Enero	de	2025	$ 740,982,385.00		
Pago No. 23 -	mes:	Febrero	de	2025	$ 771,789,618.00		
Pago No. 24 -	mes:	Abril	de	2025	$ 786,219,135.00		
Pago No. 25 -	mes:	Abril	de	2025	$ 778,320,320.00		
Pago No. 26 -	mes:	Mayo	de	2025	$ 778,015,139.00		
Pago No. 27 -	mes:	Junio	de	2025	$ 776,103,223.00		
Pago No. 28 -	mes:	Julio	de	2025	$ 778,511,897.08		
Pago No. 29 -	mes:	Agosto	*de*	*2025*	$ 777,301,100.40		
Pago No.30 -	*mes:*	Septiembre	*de*	*2025*	$ 769,683,313.00		*Contrato Inicial**
Pago No. 30 -	*mes:*	Septiembre	*de*	*2025*	$420,000,000		**Bolsa**
Pago No. 1 -	*mes:*	Septiembre	*de*	*2025*	$120,882,259.89		**OTROSI-Adición Servicios****
Pago No. 31 -	*mes:*	Octubre	*de*	*2025*	$782,805,080.00		*Contrato Inicial**
Pago No.2 -	*mes:*	Octubre	*de*	*2025*	$120,882,259.89		**OTROSI-Adición Servicios****
Pago No.32 -	*mes:*	Noviembre	*de*	*2025*	$ 779,487,583		*Contrato Inicial**
Pago No. 3 -	*mes:*	Noviembre	*de*	*2025*	$594,225,142		**OTROSI-Adición Servicios****
Pago No. 4 -	*mes:*	Diciembre	*de*	*2025*	$1.305.083.859		**OTROSI-Adición Servicios****
Pago No.33 -	*mes:*	Diciembre	*de*	*2025*	$ 779,550,507		*Contrato Inicial**
Pago No.34 -	*mes:*	Enero	*de*	*2026*	$ 780.630.928		
Pago No.35	*mes:*	Febrero	*de*	*2026*	$ 783.420.281		

Sede principal-Bogotá, Colombia
Calle 93B # 13-44, Segundo piso
NIT:900.068.796-1
Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia
Cra. 24 No. 53ª-26 Arboleda Alta.
NIT: 900.068.796-1
Teléfono: (+606) 88612612

Pendiente- Pago No.36	*mes:*	Marzo	*de*	*2026*	$ 792.559.106		
Pendiente- Pago No.37	*Mes:*	Abril 1-18	*De*	*2026*	$ 470.362.652		*Contrato Inicial**
Pendiente- Pago No.1	*Mes:*	Abril 19-30	*De*	*2026*	$ 397.561.617		**OTROSI4-Continuidad de Servicios por 8 meses**
VALOR CAUSADO QUE NO SE HA PAGADO (valor a pagar factura)							$ 867.924.269
VALOR TOTAL EJECUTADO *(valor pagado + valor causado no pagado)*							**$ 29.060.534.720**
SALDO DEL CONTRATO *(valor total del contrato – valor total ejecutado)*							**$ 13.741.058.573**
PORCENTAJE DE EJECUCIÓN							67,90%
	** El valor causado no pagado corresponde a cuentas de cobro o facturas recibidos y aprobados a satisfacción por el supervisor o interventor para su pago**						

Tabla 21 Ejecución Presupuestal

7. GESTION ADMINISTRATIVA

7.1. Profesionales

El detalle de las actividades realizadas por cada uno de los ingenieros especialistas se puede consultar a continuación, en los siguientes links:

Perfiles	Especialistas	Anexo
Especialista Bases de datos DBA	Edgar Cobos Mayorga Johan Cardozo – Apoyo DBA	Informe Mensual InfoTIC DBA Abril2026.pdf
Especialista Web Máster	Juan Carlos Martinez	Informe Mensual InfoTIC Webmaster Abril2026.pdf
Especialista Integrador de nube	Carlos Barrera	Informe Mensual InfoTIC Integrador de Nube Abril2026.pdf
Especialistas de Seguridad	Jhon Alveiro Pava González Edwin Morales Juan Carlos Quiroga asumió el rol desde el pasado 27 de abril de 2026	Informe Mensual InfoTIC Seguridad Abril2026.pdf
Especialistas de soluciones	Jose Francisco Escobar Escorcia Davis Alexander Mogollón Fandiño	Informe Mensual InfoTIC Administrador de Soluciones Abril2026.pdf
Especialista de Networking	Carlos Alberto Roldan Ríos Victor Manuel Castiblanco Sanchez - Apoyo Networking	Informe Mensual InfoTIC Administrador de Redes Abril2026.pdf

Tabla 22 Perfiles y Actividades

El siguiente es el grupo administrativo que estuvo en el desarrollo de la operación del mes de Abril del 2026:

NOMBRE COMPLETO	ROL RESPONSABLE
María Victoria Suárez Osorio	Gerente de Servicio
Angie Paola Parra Bustos	Documentadora
Francisco Javier Pulido Fajardo	Gerente de Implementaciones

Tabla 23 Grupo Administrativo

8. SERVICIO DE COLABORACIÓN

Durante el mes de Abril, el servicio de módulos de videoconferencia en las distintas sedes de la entidad se mantuvo operativo sin interrupciones ni problemas. Se aseguró el correcto funcionamiento de cada módulo y se dispuso de apoyo técnico para garantizar su operatividad. A lo largo de este periodo, no se registraron reportes de falta de disponibilidad del servicio en ninguna de las sedes.

En la siguiente tabla, se relacionan las 10 soluciones de videoconferencia o salas virtuales y su distribución en Barranquilla, Bogotá, Bucaramanga, Cali y Medellín:

ÍTEMS	SERVICIO	CIUDAD	DIRECCIÓN	CANTIDAD
1	Sala de video conferencia o sala virtual (Tamaño 65")	Bogotá – Aguas	Carrera 3 No. 18-32 Piso 2, 4 y 6	3
2	Sala de video conferencia o sala virtual (Tamaño 65")	Bogotá – Ángel	Cl. 19 #6-68 piso 17	1
3	Sala de video conferencia o sala virtual (Tamaño 55")	Bogotá – Aguas	Carrera 3 No. 18-32 es una unidad movible por lo tanto no se puede especificar su piso de ubicación.	1
SEDES REGIONALES				
4	Sala de video conferencia o sala virtual (Tamaño 55")	Bogotá - Chapinero	Calle 57 No. 8-69 Local 46 - 48 y 50	1
5	Sala de video conferencia o sala virtual (Tamaño 55")	Barranquilla	Calle 70 #53-74 piso 3	1
6	Sala de video conferencia o sala virtual (Tamaño 55")	Bucaramanga	CR 29 # 45 - 45, Ofi. 703	1
7	Sala de video conferencia o sala virtual (Tamaño 55")	Cali	Calle 5 No. 66B - 67, Centro Cultural El Capitolio – Piso 3	1
8	Sala de video conferencia o sala virtual (Tamaño 55")	Medellín	Calle 52 No. 47-42 Piso 10 Ofi. 1002	1

Tabla 24 Distribución módulos de videoconferencia por sede

Las características se encuentran detalladas en el Anexo 01 - Especificaciones Técnicas Datacenter y Telecomunicaciones en el numeral 5.5.

Con el fin de evitar fallos, asegurar un rendimiento óptimo y prolongar la vida útil de los equipos, se llevan a cabo revisiones periódicas y mantenimientos preventivos necesarios para garantizar la continuidad del servicio y el correcto funcionamiento de cada módulo instalado en las sedes de Icetex.

Durante el mes se realizaron las siguientes actividades relacionadas al servicio de módulos de videoconferencia:

- Visita en sitio en sedes de Bogotá, para realizar pruebas de funcionamiento, verificación de actualizaciones pendientes, inspección de los módulos y posterior limpieza interna y externa de los componentes de cada módulo que se encuentra en la sede Aguas, Ángel y chapinero, para garantizar la prestación continua del servicio y validar que no se estén presentado novedades y/o incidencias.

- Se realizó actualización del sistema operativo de tres (3) OPS de los módulos de la sede Aguas, Windows 10 a Windows 11.

- Disponibilidad de atención a requerimientos que surjan para revisión de novedades presentadas.

- Informe mensual de operación del servicio y reporte técnico de visitas a sedes, el cual se puede consultar en el link Informe actividades Módulos videoconferencia ICETEX abril 2026.pdf.

Durante el mes de Abril, las sedes regionales (Cali, Barranquilla, Bucaramanga, Medellín y Chapinero) y las sedes de Bogotá (Aguas y Ángel) no reportaron incidencias de servicio ni requerimientos de soporte técnico. No obstante, se garantizó la disponibilidad permanente para atender cualquier solicitud relacionada con la solución de videoconferencia implementada. Cabe destacar que el ingreso para las visitas técnicas de rigor se gestionó mediante el caso RS-RecursosFisicos-26516.

9. GESTION DE RIESGOS Y PROBLEMAS

Se mantiene la matriz de riesgos establecida en meses pasados. Cabe destacar que la determinación de estos valores no sigue una regla estricta, y puede ser ajustada de acuerdo con las necesidades del proyecto.

A partir de la identificación del nivel de riesgo relacionado al proyecto ICETEX, se pueden implementar estrategias que permitan mitigarlo o, incluso, eliminar los posibles obstáculos a los que se pueda enfrentar el ICETEX Matriz de riesgos ICETEX.xlsx .

10. INDICADORES CLAVE DE DESEMPEÑO

10.1. ANS por Disponibilidad de canales de comunicaciones

Durante el mes de Abril de 2026, los canales principales y Backup instalados operaron de manera normal, se realizó monitoreo del servicio de los canales mediante la herramienta SolarWinds, el informe de disponibilidad es el que permite la revisión de los ANS y se tiene la línea base de los canales instalados con sus anchos de banda iniciales la cual se actualizando con las ampliaciones de las canales acordadas contractualmente, se tiene el reporte: Reporte Mensual Disponibilidad INFOTIC Abril 2026.pdf

También se puede consultar en el repositorio un documento en Excel con el análisis del comportamiento de los canales para el mes de febrero: ANS Abril 2026.xlsx

Sede	Categoría	INR	BW	%MES
BOGOTAD.C.	Principal/FO(SedeAguas)	INR0037	400MB	100,00 %
	Backup /FO(SedeAguas)	INR0036	200MB	100,00 %
	Principal/IPVPN(SedeChapinero)	INR0022	40MB	99,97 %
	Backup /IPVPN(Sedechapinero)	INR0020	25MB	99,98 %
	Principal/IPVPN(Angel)	INR0272	200MB	96,27 %
	Backup /IPVPN(Angel)	INR0273	200MB	99,73 %
IBAGUE	Principal/IPVPN	INR0073	20MB	100,00 %
	Backup/IPVPN	INR0076	20MB	98,73 %
LETICIA	Principal/Satelital	INR0000373	8MB	100,00 %
NEIVA	Principal/IPVPN	INR0039	20MB	99,90 %
	Backup/IPVPN	INR0041	10MB	99,86%
TUNJA	Principal/IPVPN	INR0104	20MB	99,69 %
	Backup/IPVPN	INR0106	5MB	98,44 %
VILLAVICENCIO	Principal/IPVPN	INR0085	20MB	100,00 %
	Backup/IPVPN	INR0084	10MB	99,97 %
ARMENIA	Principal/IPVPN	INR0074	20MB	99,44 %
	Backup/IPVPN	INR0072	10MB	99,33 %
MANIZALES	Principal/IPVPN	INR0088	20MB	100,00 %
	Backup/IPVPN	INR0087	10MB	99,64 %
MEDELLIN	Principal/IPVPN	INR0133	100MB	99,44 %
	Backup/IPVPN	INR0132	30MB	99,44 %
APARTADO	Principal/IPVPN	INR0144	20MB	99,46 %
PEREIRA	Principal/IPVPN	INR0079	20MB	100,00 %
	Backup/IPVPN	INR0077	20MB	100,00 %
QUIBDO	Principal/IPVPN	INR0014	20MB	99,85 %
	Backup/IPVPN			0,00%

INFOTIC
SOLUCIONES INTELIGENTES

Sede	Categoría	INR	BW	%MES
BARRANQUILLA	Principal/IPVPN	INR0103	100MB	100,00 %
	Backup/IPVPN	INR0100	20MB	100,00 %
CARTAGENA	Principal/IPVPN	INR0109	20MB	99,65 %
	Backup/IPVPN	INR0107	10MB	99,67 %
MONTERIA	Principal/IPVPN	INR0080	20MB	99,99 %
	Backup/IPVPN	INR0081	10MB	99,99 %
RIOHACHA	Principal/IPVPN	INR0164	20MB	100,00 %
	Backup/IPVPN	INR0162	10MB	98,73 %
SANTAMARTA	Principal/IPVPN	INR0154	20MB	99,83 %
	Backup/IPVPN	INR0152	10MB	99,96 %
SINCELEJO	Principal/IPVPN	INR0095	20MB	100,00 %
	Backup/IPVPN	INR0097	5MB	99,99 %
SANANDRES	Principal/IPVPN	INR0000367 INR0000369	8MB	94,77%
BARRANCABERMEJA	Principal/IPVPN			0,00%
SANGIL	Principal/IPVPN			0,00%
BUCARAMANGA	Principal/IPVPN	INR0062	30MB	99,87 %
	Backup/IPVPN	INR0061	20MB	99,87 %
CUCUTA	Principal/IPVPN	INR0044	20MB	99,56 %
	Backup/IPVPN	INR0047	10MB	99,54 %
VALLEDUPAR	Principal/IPVPN	INR0091	20MB	76,46 %
	Backup/IPVPN	INR0090	10MB	86,00 %
YOPAL	Principal/IPVPN	INR0121	20MB	99,89 %
	Backup/IPVPN	INR0123	10MB	99,98 %
ARAUCA	Principal/IPVPN	INR0110	20MB	99,89 %
CALI	Principal/IPVPN	INR0151	100MB	100,00 %
	Backup/IPVPN	INR0153	150MB	100,00 %
BUENAVENTURA	Principal/IPVPN	INR0051	10MB	99,62 %
MOCOA	Principal/IPVPN	INR0135	10MB	95,74 %
	Backup/Satelital	INR0136	5MB	95,81 %
PASTO	Principal/IPVPN	INR0130	20MB	99,94 %
	Backup/IPVPN	INR0131	10MB	99,97 %
POPAYAN	Principal/IPVPN	INR0035	20MB	100,00 %
	Backup/IPVPN	INR0032	5MB	99,98 %
TUMACO	Principal/IPVPN	INR0147	20MB	98,82 %
DCTRIARA	MPLS PP	INR0266	1GB	100,00 %
	MPLS BK	INR0171	1GB	99,57 %
DCTRIARA	INTERNET BK	INR0221	800MB	0,00%
	INTERNET PP	INR0264	800MB	100,00 %
DCTRIARA	NOCclarodedidcado(DWDM)2GTriara megacentro	INR0224	2GB	100,00%

Sede principal-Bogotá, Colombia
Calle 93B # 13-44, Segundo piso
NIT:900.068.796-1
Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia
Cra. 24 No. 53ª-26 Arboleda Alta.
NIT: 900.068.796-1
Teléfono: (+606) 88612612

Sede	Categoría	INR	BW	%MES
CanalentreSitiopricipalIcetex-DirecciónGeneral-Aguas	Principal/IPVPN			100,00 %
	Backup/IPVPN			100,00 %
BOGOTAD.C.	Internet(SedeAguas)	INR0034	70MB	100,00 %
DCMegacentro	DCMEGACENTER–CONTIGENCIA–MPLSPPAL	INR0177	500MB	100,00 %
	DCMEGACENTER–CONTIGENCIA–MPLSBK	INR0230	500MB	100,00 %
	Internet	INR0268	400MB	100,00 %
BancodelaRepublicahastaEdificioDirecciónGeneralICETEX	UbicadoenDatacenterPrincipal.interconectadoatravesderedMPLS	INR0000289	40MB	100,00 %
DECEVALhastaEdificiodelICETEXDirecciónGeneral.	UbicadoenDatacenterPrincipal.interconectadoatravesderedMPLS	INR0000317	40MB	100,00%
DECEVALhastaEdificiodelICETEXDirecciónGeneral.	UbicadoenDatacenterPrincipal.interconectadoatravesderedMPLS(Backup)	INR0000318	15MB	100,00%
Salidadelportaleshttps://portal.icetex.gov.co/portalywww.icetex.gov.cohaciainternetencentrodecómputoprincipal	InternetReversoparaPortales	INR0000320	1GB	100,00 %
DCTRIARA	allotentralizado800Mtriara(equipo)	INR0270		100,00 %

Tabla 25 Disponibilidad de Canales

Durante el mes de Abril de 2026 el servicio de Internet para la gente se prestó sin interrupciones en todas las catorce sedes contratadas donde ICETEX cuenta con oficina, las cuales se relacionan a continuación:

Sede	Categoría	INR	% Mes
BARRANQUILLA	INTERNET PARA LA GENTE	INR0094	100,00 %
BUCARAMANGA	INTERNET PARA LA GENTE	INR0057	99,87 %
CALI	INTERNET PARA LA GENTE	INR0160	99,99 %
AGUAS	INTERNET PARA LA GENTE	INR0029	100,00 %
CHAPINERO	INTERNET PARA LA GENTE	INR0015	99,98 %
MEDELLIN	INTERNET PARA LA GENTE	INR0122	99,45 %
APARTADO	INTERNET PARA LA GENTE	INR0140	99,46 %
ARAUCA	INTERNET PARA LA GENTE	INR0115	99,89 %
LETICIA	INTERNET PARA LA GENTE	INR0000378	100,00 %
QUIBDO	INTERNET PARA LA GENTE	INR0021	99,85 %
RIOHACHA	INTERNET PARA LA GENTE	INR0159	100,00 %

Sede	Categoría	INR	% Mes
SAN ANDRES	INTERNET PARA LA GENTE	INR0000368	94,75 %
YOPAL	INTERNET PARA LA GENTE	INR0127	99,92 %
MOCOA	INTERNET PARA LA GENTE	INR0141	95,74 %

Tabla 26 Disponibilidad canales "Internet para la gente"

Canales Sdwan:

Sede	Codigo	Ancho de Banda	Disponibilidad
SDWANAGUAS	INR0033/000334	10MB	100,00%
SDWANMOCOA	INR0139/000333	10MB	95,86%
SDWANLETICIA	INR0000374	10MB	100,00 %
SDWANSANANDRES	INR0000371	10MB	95,85 %

10.1.1. Canal de Replicación (Triara – Megacenter)

El proyecto tiene asignado un canal de comunicación con un ancho de banda de 2 Gbps, el cual se comunica en forma bidireccional entre los data centers de Triara y Megacenter, permitiendo generar la replicación de la información de los equipos de ICETEX, para el mes de Abril continúa su funcionamiento correctamente sin novedades que afectaran la prestación del servicio. La evidencia se encuentra en el Reporte_Monitoreo_ICETEX_Abril_ELK.pdf y en el archivo de Disponibilidad Server_ELK_Abril_2026.xlsx

10.2. ANS por Disponibilidad de servidores

La herramienta utilizada para el monitoreo de la disponibilidad de servidores es ELK y el informe correspondiente que permite la revisión de los ANS es la Disponibilidad Server_ELK_Abril_2026.xlsx
Disponibilidad Server_ELK_Abril_1-18_2026.xlsx
Disponibilidad Server_ELK_Abril_19-30_2026.xlsx

No	COD.	Etiquetas de fila	Disponibilidad 1 al 18 Abril	Disponibilidad 19 al 30 Abril
1	INR0278	cxvodacontg011	100,00%	100,00%
2	INR0277	cxvodaprodn021	100,00%	100,00%
3	INR0276	cxvodaprodn011	100,00%	100,00%
4	INR0262	icetexboglxorfeo2.localdomain	100,00%	100,00%
5	INR0260	icetexosbognfs1	100,00%	100,00%
6	INR0259	INR0259_INFOTIC	99,99%	100,00%
7	INR0258	INR0258_INFOTIC	0,00%	0,00%
8	INR0257	INR0257_INFOTIC	100,00%	100,00%
9	INR0256	INR0256_INFOTIC	100,00%	100,00%
10	INR0255	INR0255_INFOTIC	100,00%	100,00%
11	INR0254	INR0254_INFOTIC	100,00%	100,00%

No	COD.	Etiquetas de fila	Disponibilidad 1 al 18 Abril	Disponibilidad 19 al 30 Abril
12	INR0253	bastion.localdomain	100,00%	100,00%
13	INR0252	icetexosbognfs2	100,00%	100,00%
14	INR0251	INR0251_INFOTIC	100,00%	100,00%
15	INR0250	qasec	100,00%	100,00%
16	INR0249	xroadsec	100,00%	100,00%
17	INR0248	icetexboglxxroad3	100,00%	100,00%
18	INR0247	preprodsec	100,00%	100,00%
19	INR0246	icetexboglxdarumatest	100,00%	100,00%
20	INR0245	icetexboglxdarumasrv2	100,00%	100,00%
21	INR0244	icetexboglxdarumasrv1	100,00%	100,00%
22	INR0243	icetexbogliferayserver1	100,00%	100,00%
23	INR0242	icetexbogliferayserver2	100,00%	100,00%
24	INR0241	icetexbogelasticserver3	100,00%	100,00%
25	INR0240	icetexbogelasticserver2	100,00%	100,00%
26	INR0239	icetexbogelasticserver1	100,00%	100,00%
27	INR0238	icetexbogliferaynfs	100,00%	100,00%
28	INR0237	icetexbogbalserver1-r	0,00%	0,00%
29	INR0236**	ictxbogsrvpt1	100,00%	100,00%
30	INR0235**	ictxbogsrvpt2	100,00%	100,00%
31	INR0234	ictxprusisgapp	100,00%	100,00%
32	INR0233	icetexboglxorfeo1.localdomain	100,00%	100,00%
33	INR0229	ictxsisgesapp	100,00%	100,00%
34	INR0228	Ictxsisgesbd	99,97%	100,00%
35	INR0226	mira	100,00%	100,00%
36	INR0000322	Ictxsrvctrldoc	99,97%	100,00%
Balanceador Nodo 1	INR0197	TFM1412	100%	100,00%
Balanceador Nodo 2	INR0197	TFM1407	98,55%	98,96%

Tabla 27 Códigos relacionados Disponibilidad Servicios en Housing – Datacenter Principal

Los dispositivos de seguridad, switches, controladoras y Enclosure de almacenamiento que se encuentran en Housing en el Datacenter principal no presentaron indisponibilidad durante el mes:

#	Dispositivo	Marca	Modelo
1	FORTIWEB01	Fortinet	2000E
2	FORTIWEB02	Fortinet	2000E
3	FORTIAUTH01	Fortinet	1000D
4	FORTIAUTH02	Fortinet	1000D
5	FORTISANDBOX	Fortinet	1000D
6	Cisco 3650X	Cisco	WS-C3650-48TQ
7	Cisco 3560X SW	Cisco	WS-C3650-48TQ
8	Switch DELL Networking	Dell	N4032 24 ports

#	Dispositivo	Marca	Modelo
9	Controladora SAN Dell Compellent	Dell	SC8000
10	Controladora SAN Dell Compellent	Dell	SC8000
11	Enclosure Discos SAN	Dell	EN-SC200
12	Enclosure Discos SAN	Dell	EN-SC220
13	Enclosure Discos SAN	Dell	EN-SC200
14	Enclosure Discos SAN	Dell	EN-SC220
15	Enclosure Discos SAN	Dell	EN-SC220
16	Enclosure Discos SAN	Dell	EN-SC200
17	Enclosure Dell Blade – Principal 5 Servidor – Blade M1000, 6 IOM Slot B2 -Tarjeta Enclosure - M1000	Dell	M1000E

Tabla 28 Dispositivos en Housing – Datacenter Principal

10.2.1. Disponibilidad TRIARA para los servicios de página web Icetex

La disponibilidad del Portal Web institucional web.ICETEX.gov.co, en el mes de Abril presentó un **UPTIME del [100%]** tal como se evidencia en el numeral 4.2.1.3 Sitio Web "Portal Icetex"

El siguiente es el comportamiento a nivel de acceso al portal WEB durante el último trimestre:

	Febrero	Marzo	Abril
Usuarios activos mes	613000	600000	506000
Usuarios nuevos	425000	382000	324000
Tiempo de interacción (seg)	101	97	91

Tabla 29 Distribución trimestral de acceso por usuarios

El portal WEB cuenta con un total de 506 mil usuarios, con 324 mil usuarios nuevos. El tiempo de interacción medio es de 1 minutos y 31 segundos, señalando el interés de la audiencia en las diferentes páginas del portal web.icetex.gov.co.

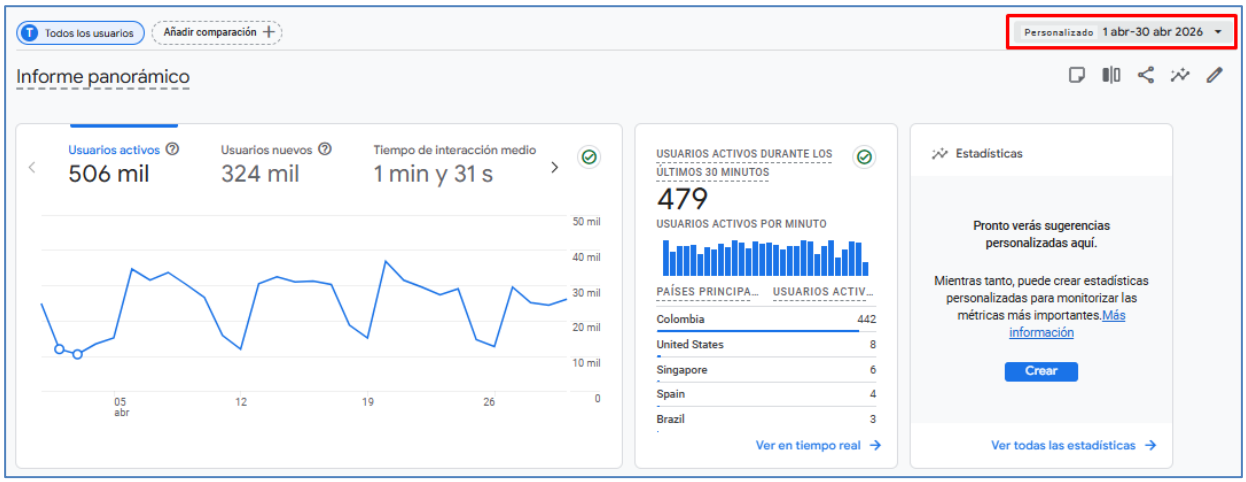
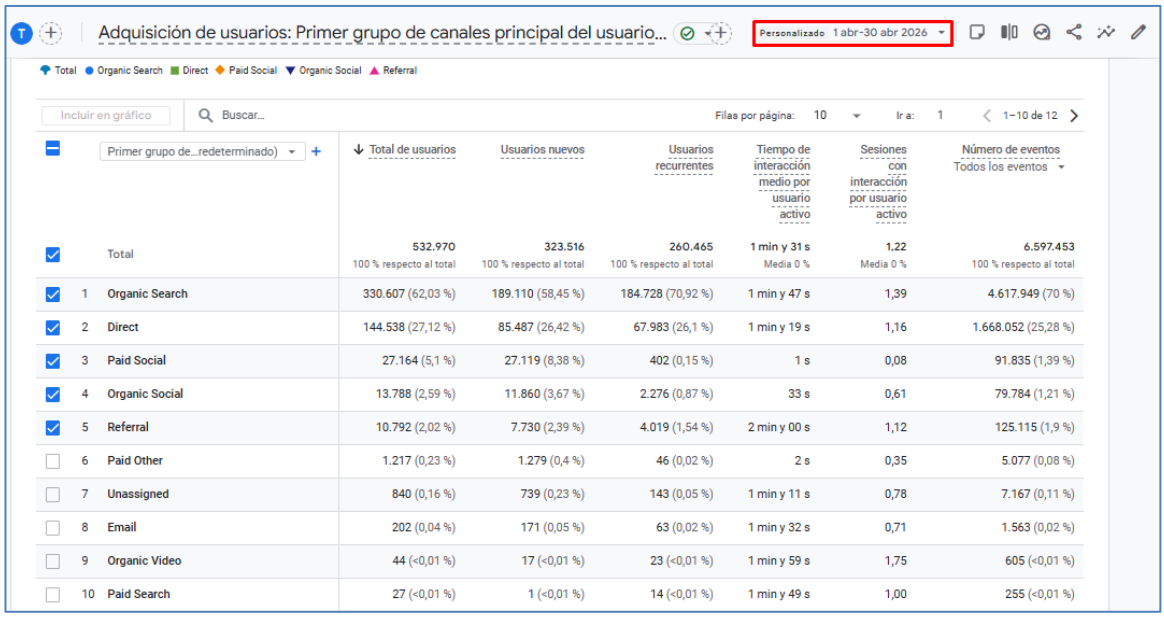


Ilustración 33 Métrica de visitantes Portal WEB web.ICETEX.gov.co

Métricas de adquisición de usuarios: el grupo de canales predeterminado de la sesión evidencia que las búsquedas orgánicas son la principal fuente de sesiones, destacando la importancia de la optimización para motores de búsqueda (SEO) en la estrategia general de adquisición de usuarios:



		Primer grupo de...redeterminado)	Total de usuarios	Usuarios nuevos	Usuarios recurrentes	Tiempo de interacción medio por usuario activo	Sesiones con interacción por usuario activo	Número de eventos Todos los eventos
☑		Total	532.970 100 % respecto al total	323.516 100 % respecto al total	260.465 100 % respecto al total	1 min y 31 s Media 0 %	1,22 Media 0 %	6.597.453 100 % respecto al total
☑	1	Organic Search	330.607 (62,03 %)	189.110 (58,45 %)	184.728 (70,92 %)	1 min y 47 s	1,39	4.617.949 (70 %)
☑	2	Direct	144.538 (27,12 %)	85.487 (26,42 %)	67.983 (26,1 %)	1 min y 19 s	1,16	1.668.052 (25,28 %)
☑	3	Paid Social	27.164 (5,1 %)	27.119 (8,38 %)	402 (0,15 %)	1 s	0,08	91.835 (1,39 %)
☑	4	Organic Social	13.788 (2,59 %)	11.860 (3,67 %)	2.276 (0,87 %)	33 s	0,61	79.784 (1,21 %)
☑	5	Referral	10.792 (2,02 %)	7.730 (2,39 %)	4.019 (1,54 %)	2 min y 00 s	1,12	125.115 (1,9 %)
☐	6	Paid Other	1.217 (0,23 %)	1.279 (0,4 %)	46 (0,02 %)	2 s	0,35	5.077 (0,08 %)
☐	7	Unassigned	840 (0,16 %)	739 (0,23 %)	143 (0,05 %)	1 min y 11 s	0,78	7.167 (0,11 %)
☐	8	Email	202 (0,04 %)	171 (0,05 %)	63 (0,02 %)	1 min y 32 s	0,71	1.563 (0,02 %)
☐	9	Organic Video	44 (<0,01 %)	17 (<0,01 %)	23 (<0,01 %)	1 min y 59 s	1,75	605 (<0,01 %)
☐	10	Paid Search	27 (<0,01 %)	1 (<0,01 %)	14 (<0,01 %)	1 min y 49 s	1,00	255 (<0,01 %)

Ilustración 34 Métrica adquisición usuarios Portal WEB web.ICETEX.gov.co

Métricas de usuario: Se evidencia que el país que más visita el portal WEB es Colombia, seguido de Estados Unidos. Por otra parte, la ciudad que más visita el portal WEB es Bogotá seguida de Barranquilla.
El idioma que predomina es el español seguido por el idioma inglés.

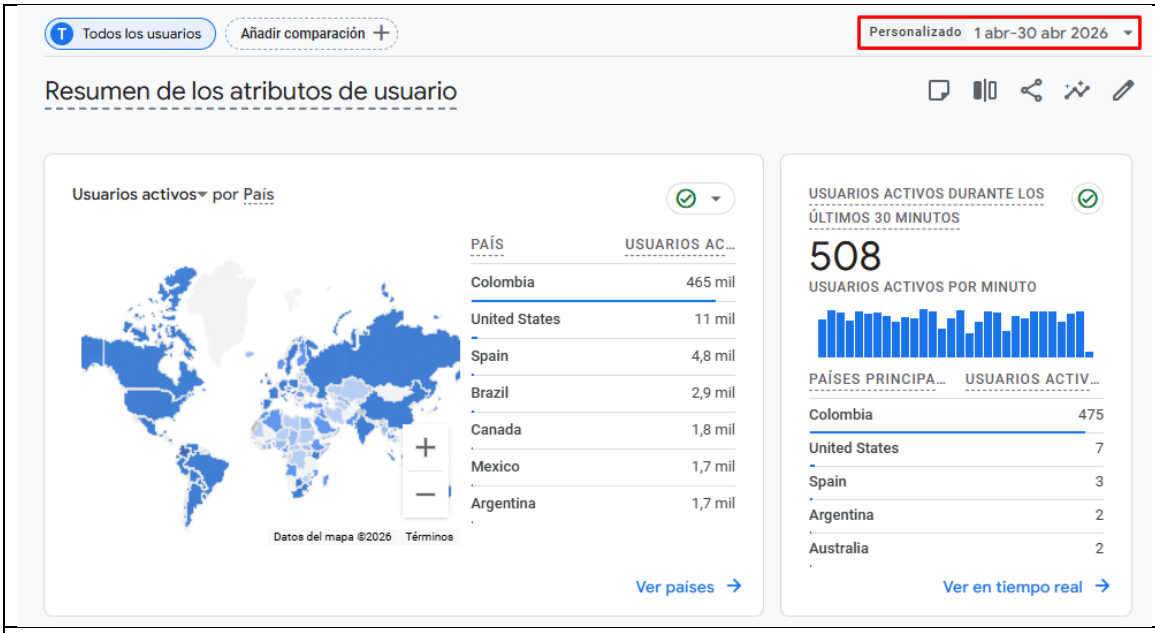


Ilustración 35 Métrica de usuario por país - Portal WEB web.ICETEX.gov.co

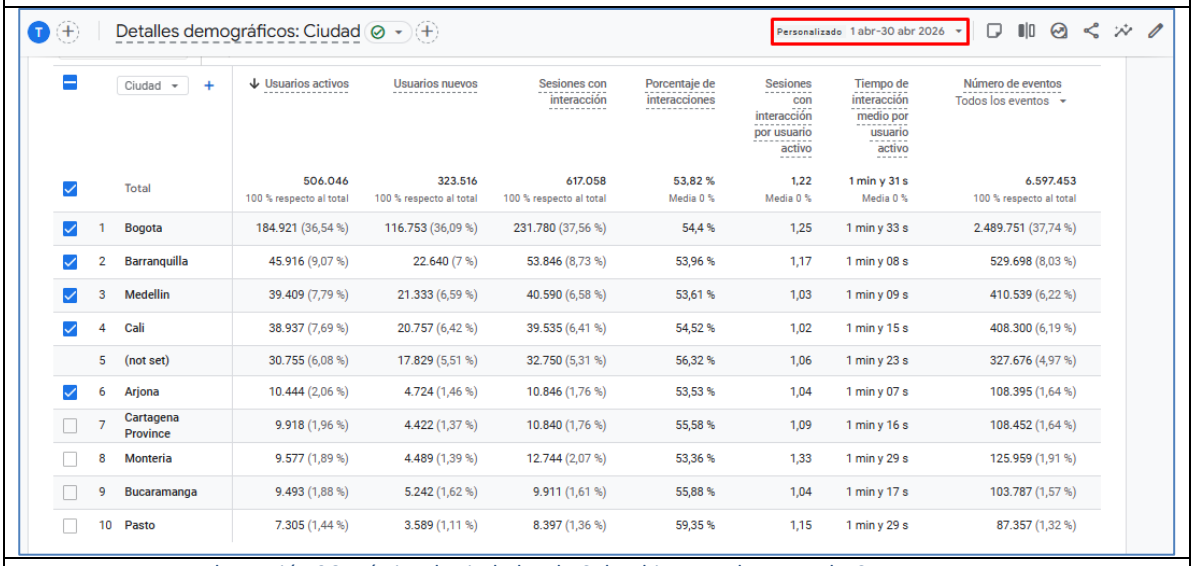


Ilustración 36 Métrica de ciudades de Colombia- Portal WEB web.ICETEX.gov.co

A continuación, se muestran las gráficas referentes a memoria RAM y almacenamiento en los nodos 1 y 2 del portal ICETEX desde el 1 de Abril desde las 00:00 horas hasta las 23:59 horas del 30 de Abril de 2026.

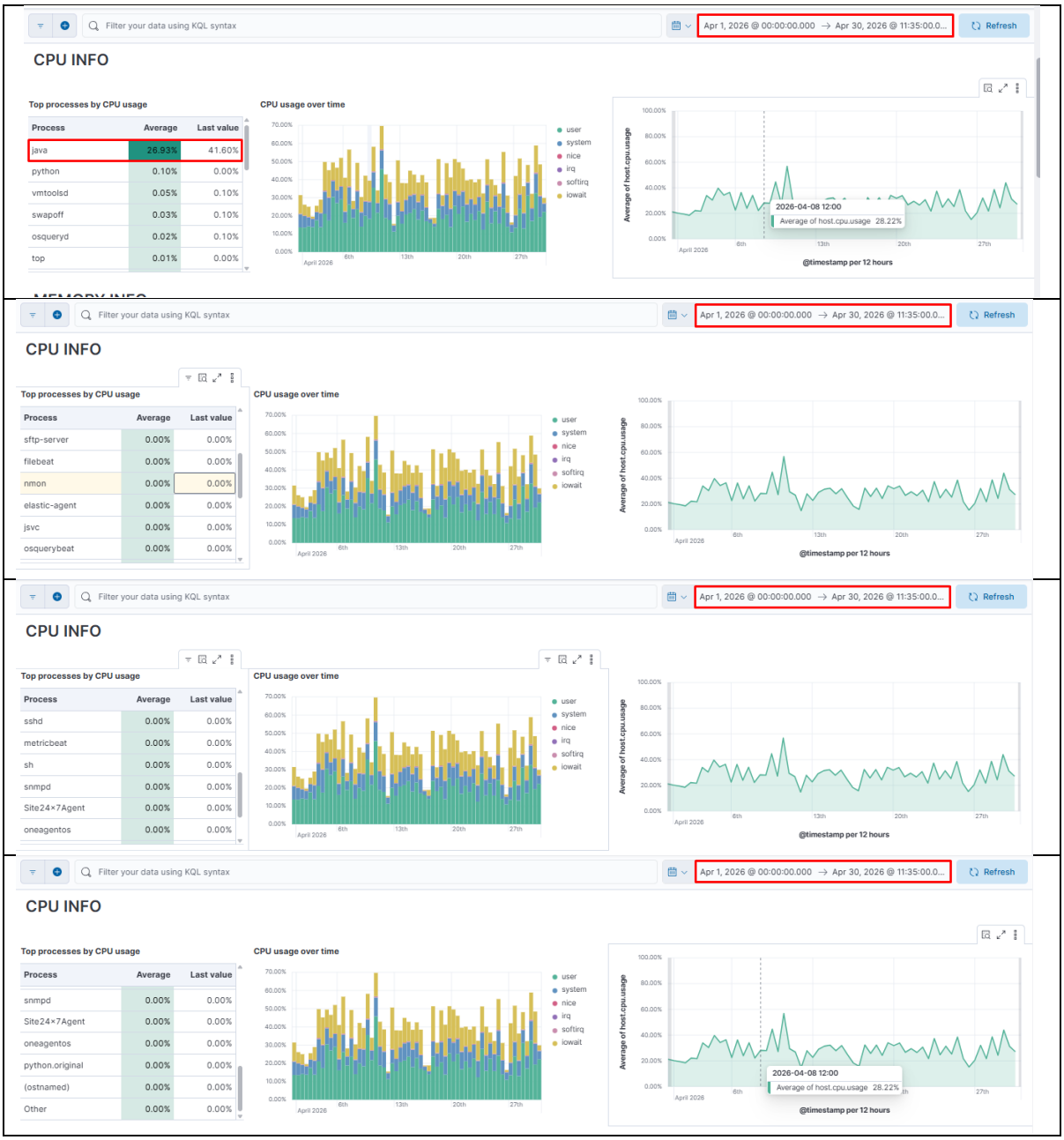


Ilustración 37 NODO 1 CPU

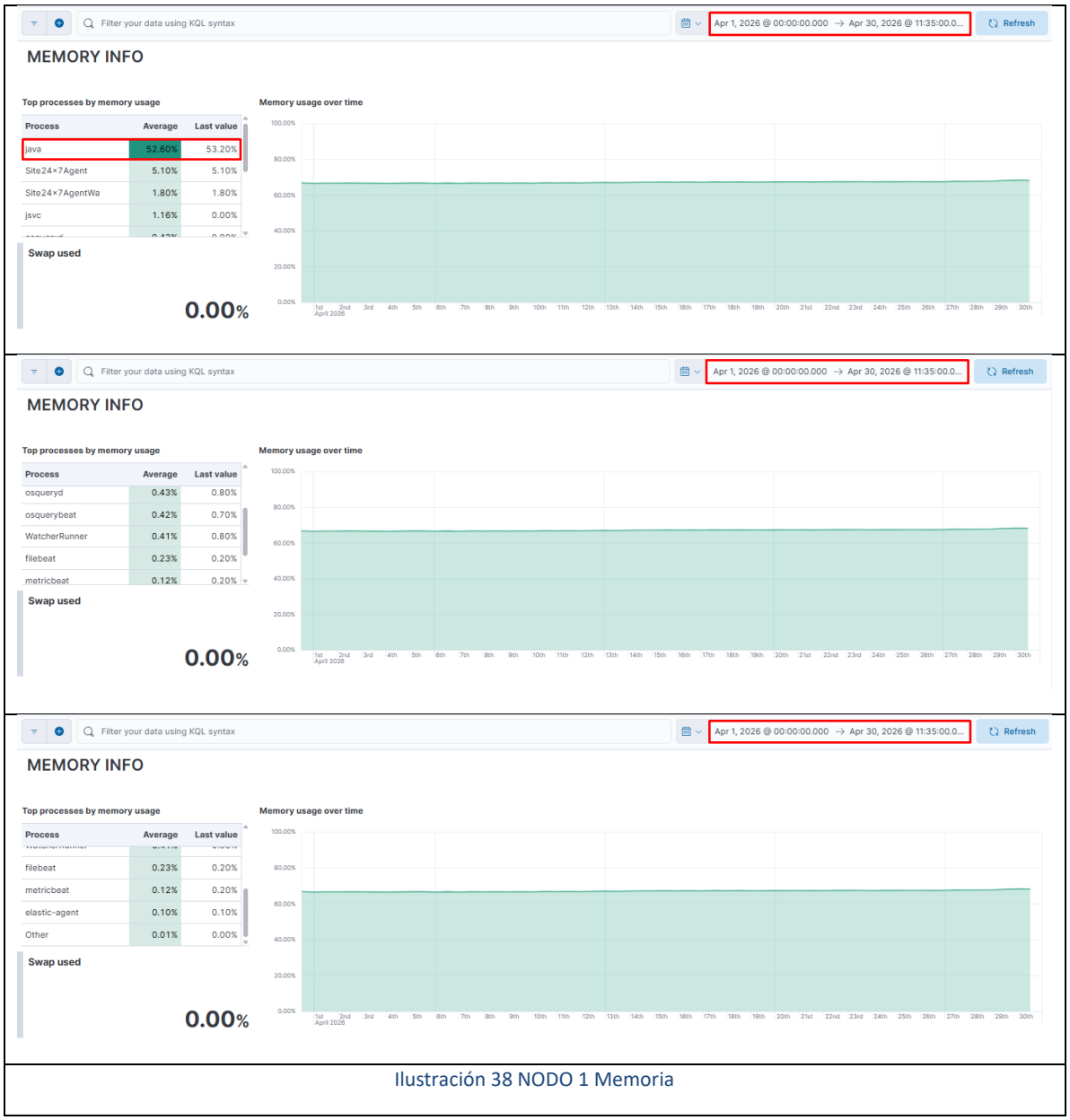


Ilustración 38 NODO 1 Memoria



Ilustración 39 NODO 1 Almacenamiento

Estos mismos recursos, para el nodo 2 se monitorean de igual manera. El detalle de los consumos y sus umbrales puede ser consultado en el informe de nuestro especialista web master Informe Mensual InfoTIC Webmaster Abril2026.pdf

10.2.2. Análisis componente Liferay Producción

Como parte de las actividades desarrolladas por el Web máster se realiza una revisión de la infraestructura tecnológica y el entorno de software del portal Liferay, abordando aspectos fundamentales para su óptimo rendimiento y seguridad sin encontrarse hallazgos significativos.

Se recomienda ampliar el almacenamiento de la partición raíz / de los tres nodos del Elasticsearch debido a identificación en los logs en indisponibilidades presentadas en el servicio indica que se encuentra con un escaso espacio en disco, esta ampliación le daría mayor estabilidad al funcionamiento de los tres nodos de Elasticsearch.

10.2.3. Backup Servidores Triara

Durante el periodo de febrerose realizaron los Backups de acuerdo con las políticas definida por el ICETEX, las cuales desde su inicio se implementaron en el Datacenter. Se puede verificar en el documento Informe Backups mes de Abril 2026.pdf que se genera con la guía de los diferentes reportes de Backups disponibles durante el mes y se adjunta el reporte de los backups que se genera automáticamente desde la herramienta de Backups Consolidado Mensual de Backups abril 2026.pdf

Dentro de las actividades del proyecto de servicios tecnológicos para ICETEX, se tiene la toma de copias de respaldo de la información creada, actualizada, reutilizada y procesada dentro de las diferentes actividades de la entidad la cual requiere para el desarrollo de sus actividades diarias, para lo cual se tiene como lineamiento principal la aplicación del anexo 22 donde se contempla las

diferentes variables para la toma de Backups y la política de Backups la cual se encuentra actualizada con la operación actual: Politica Backup Icetex V6.xlsx

Respecto a la gestión de medios, en este periodo se continua con la migración de respaldos hacia las cintas suministradas por Icetex (160 cintas LT07). Este proceso tiene como objetivo la restitución progresiva de los medios en préstamo y la consolidación del stock propio, asegurando así la capacidad de almacenamiento necesaria para cubrir los requerimientos hasta el cierre del contrato.

Para el mes de Abril el resultado de la ejecución de los Backups fue el siguiente:

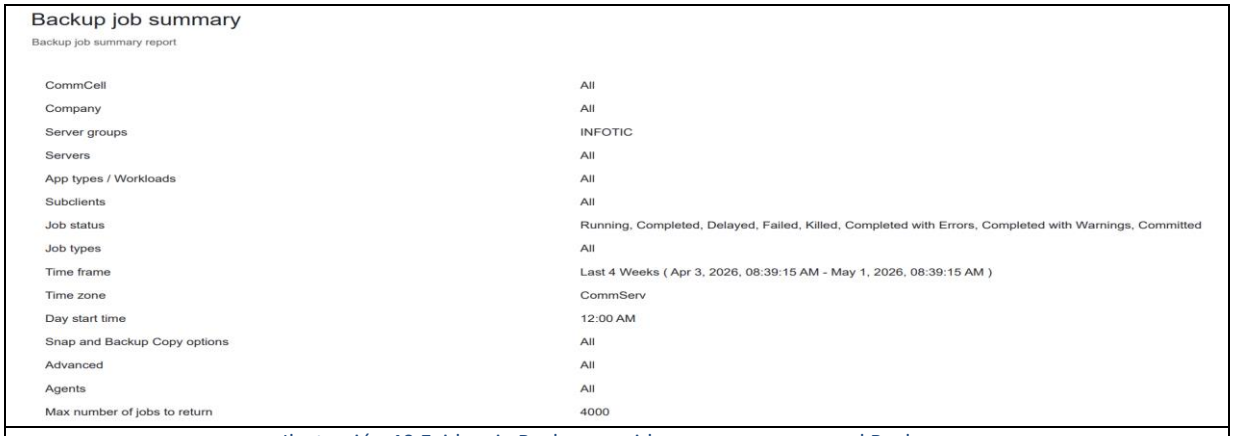


Ilustración 40 Evidencia Backup servidores resumen general Backups

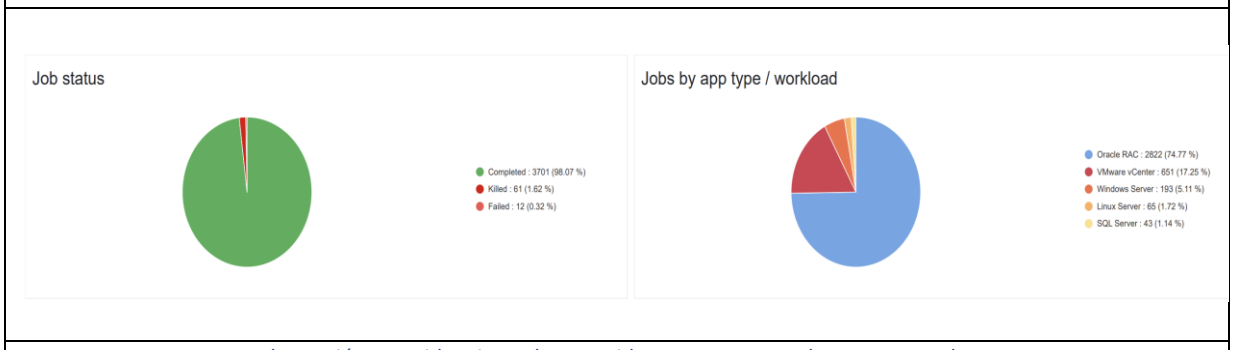


Ilustración 41 Evidencia Backup servidores resumen Backups y su estado

El total del tamaño de la información respalda para el mes de Abril corresponde a 236.36 TB, donde 98.07% se completó en el primer lanzamiento del robot con un total de 235.92 TB de información.

El 74.77% está representado en el respaldo dado a la información del Oracle RAC.

En el caso de los Backups que no fueron exitosos o que presentan algún tipo de problema son revisados de forma interna, subsanados y nuevamente tomados por el área correspondiente.

El análisis y conclusiones del comportamiento de los Backups para este mes es el siguiente:

De un total de 3774 trabajos analizados, el 98,07% se completó con éxito.

- Tasa de éxito: 98.07 % (trabajos completados)
- Tasa de fracaso: 1.94% (trabajos fallidos o cancelados)
- Oracle RAC: El 74.77% de los trabajos de respaldo corresponden a este tipo de servidor, con un total de 2822 trabajos.
- VMware vCenter: El 17.25% de los trabajos pertenecen a este entorno, con 651 trabajos.
- Otros Servidores: Los trabajos de Windows Server, Linux Server y SQL Server representan el 5.11 %, 1.72 % y 1.14 respectivamente.

La evidencia se genera diariamente en el reporte que se entrega de forma automática a los correos que el ICETEX solicitó y en el informe mensual se anexan todos los soportes y evidencias de la ejecución de las políticas de Backup, la política actualizada y vigente de la toma de Backup, se encuentra en el link del repositorio Backup Diario y el informe de Backups en la carpeta Informe de Backup.

11. CONTROL DE CAMBIOS

Durante el mes de Abril se presentaron al comité de cambios las siguientes actividades para su revisión y aprobación, en el cuadro se puede ver su estado:

No. Cambio	Alcance	Fecha De Creación o Aprobación	Fecha De Ejecución	Resultado	Observaciones
27111	Migración a nuevo host de las máquinas del portal ICETEX	24/04/2026	9/05/2026	Aprobado en CAB	Actividad En Proceso
27028	El cambioaplica a los siguientes servidores enentornode producción: •ICTXSRVNETCOR01(192.168.51.165aloja las aplicacionesPSE, CargueArchivos, CuentasAbandonadas, Cuentas Inactivas, Portal Transaccional yTransunion, las cuales estánpublicadas eninternet yaccedidaspor usuarios externos. •ICTXSRVPASARElа (192.168.51.211):): aloja la aplicacionPSE •ICTXSRVDCVAL01(192.168.51.170): aloja la aplicación Deceval, esencial para la integraciónconservicios financieros externos.	28/04/2026	30/04/2026	Exitoso	2026-03 Cumulative Update for Microsoft server operatingsystemversion21H2for x64-basedSystems (KB5078766) 2026-04 ServicingStackUpdate for Windows Server 2016for x64-basedSystems (KB5082089).

Tabla 30 Controles de cambio Abril

12. PLAN DE TRABAJO DE LOS PROXIMOS MESES

A continuación, se presenta el avance de cada uno de los temas y de los que se requiera se definirá un plan de trabajo:

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
Revisar las alternativas de solución respecto al licenciamiento de las herramientas de seguridad (perimetral y antivirus)	ICETEX	01-06-2025	31-03-2026	Esta situación implica riesgos críticos tanto a nivel de seguridad como de continuidad operativa, entre los que se destacan: • Falta de actualizaciones de seguridad críticas. • Mayor exposición a vulnerabilidades y ataques cibernéticos. • Incompatibilidad con software y hardware actualizado. • Ausencia de soporte oficial por parte del fabricante.
Verificar la configuración de los equipos de LAN y WAN que hace falta para el funcionamiento de IPv6.	ICETEX	01-12-2024	31-03-2026	INFOTIC ha finalizado las etapas de prueba y configuración. Actualmente, se ha avanzado en la implementación de las aplicaciones Control Doc. y Aranda. Cabe señalar que, aunque INFOTIC brindará todo el soporte técnico necesario, el despliegue final en estas plataformas depende de la gestión de los administradores designados por ICETEX.
Revisar la parametrización de restricción y los problemas ocasionados a la conexión, para activar el agente de antivirus en las bases de datos.	INFOTIC - ICETEX	01-12-2024	31-03-2026	Se programará la desinstalación de Symantec y la migración al antivirus Falcon, conforme a las ventanas de mantenimiento y disponibilidad que defina el ICETEX.

Tabla 31 Planes de trabajo

13. PLAN DE ENTREGA

En atención a la prórroga del contrato, no resultó procedente continuar con el desarrollo del plan de entrega inicialmente definido. No obstante, para efectos informativos, se remite un balance general del estado de avance y de las actividades ejecutadas a la fecha.

Aspecto	Estado	Observaciones
Conformación de equipos de trabajo	Cumplido Parcial	Aunque se designaron funcionarios para la celebración de las sesiones, no hubo designación formal de líderes técnicos por parte del ICETEX
Establecer una línea base para los componentes y listas de chequeo	Cumplido	Se adelantaron sesiones iniciales para la revisión de los componentes y las listas deverificación.
Establecimiento de un repositorio documental	Cumplido	Se definió, por parte del ICETEX, un recurso en SharePoint, para publicar todos los documentos. Por parte de INFOTIC se propuso una estructura documental, la cual fue avalada por el ICETEX.
Ejecución de Entrega	Cumplido	Se desarrollaron mas de 13 sesiones, con los distintos frentes, para revisar los documentos y su contenido. Se atendieron las observaciones efectuadas por parte del ICETEX.
Cierre	Suspendido	Debido a la prórroga del contrato

Tabla 32 Balance General actividades ejecutadas Plan de entrega

El proyecto se encuentra en operación evidenciando un nivel de estabilización progresivo en consonancia con los proyectos que adelante el ICETEX. No obstante, persisten situaciones que impactan la ejecución, particularmente en temas depersonal, backups y componentes de seguridad.

13.1. Observaciones relevantes

- **Permanencia en sitio:** Persisten inconvenientes en la asistencia del personal en sitio. Se requiere concertar horarios y permanencia según la cantidad de especialistas definidos contractualmente.
- **Backups:** Los respaldos solicitados para la infraestructura externa (AGUAS) se encuentran fuera del alcance del contrato. Para el resto de los servicios, se ha solicitado una sesión de trabajo para revisar el tema.
- **Replicación Data Guard Oracle:** Se presentan fallos en la replicación debido a ajustes técnicos (configuración de *archive logs*) solicitados específicamente por el ICETEX.
- **Riesgos de Seguridad:** Se reitera el riesgo crítico por el vencimiento de licencias de seguridad (Fortinet). Esta situación ha sido reportada en periodos previos y sigue pendiente de resolución.
- **Análisis de Vulnerabilidades:** Definición de un nuevo cronograma de escaneos para que nuestro equipo del SOC proceda con la programación de las actividades de análisis.

14. RECOMENDACIONES DEL CONTRATISTA AL ICETEX

14.1. Networking

- **Renovación de Equipos:** Se sugiere llevar a cabo la actualización de los equipos de la entidad, ya que muchos de ellos se encuentran obsoletos y carecen de soporte por parte del fabricante, lo que podría afectar el rendimiento y la seguridad de la infraestructura.

- **Reemplazo de Equipos Dañados:** Luego del daño del equipo en la sede de San Andrés, informa a ICETEX que actualmente no hay disponibilidad de equipos adicionales para reemplazos futuros en caso de que surjan nuevos daños.

- **Renovación y Certificación de Cableado:** Se recomienda realizar una renovación o sustitución del cableado en diversos puntos de la entidad, dado que la infraestructura de cableado es muy antigua. Se sugiere también llevar a cabo una certificación del nuevo cableado para garantizar su calidad y desempeño.

- **Mantenimiento de Infraestructura:** Considerando el estado actual de la infraestructura en las sedes, es crucial llevar a cabo un mantenimiento integral de los equipos y del cableado, así como proceder a la renovación de los dispositivos de red, para asegurar un funcionamiento óptimo y prevenir fallas futuras.

- **Aprovisionamiento de espacio**: Se ha reportado el espacio empleado en la unidad F del servidor ICTXSRVNETCOR01, el cual llega a unos umbrales cercanos al 94% poniendo en riesgo la disponibilidad de dicho servidor. Se recomienda, al ICETEX, validar las políticas de respaldo que se aplican sobre la información allí almacenada, así como evaluar la posibilidad de disponer de información histórica en otros medios de almacenamiento permitiendo liberar este espacio.

14.2. Aplicaciones

Es fundamental que todos los usuarios finales comprendan la importancia de canalizar sus solicitudes a través de la mesa de servicio de Aranda. Aunque estamos comprometidos en atender todas las peticiones que recibimos, gestionar las solicitudes de manera formal garantiza un seguimiento adecuado y evita la pérdida de información.

Existen aplicaciones que operan sobre el Framework .Net Classic, se recomienda que sean migradas a un Framework más actual y que cuente con soporte vigente. En la actualidad los ambientes de pruebas cuentan con Framework actualizado, lo que permite que las actualizaciones puedan validarse en estos ambientes controlados.

Existen aplicaciones que están implementadas en sistemas operativos obsoletos sean migradas a Servidores con sistemas operativos de versiones actuales y con soporte de Microsoft.

Se recomienda que cada aplicación web cuente con su propio servidor, ya que esto garantiza un mejor rendimiento y seguridad en el manejo de datos.

Se sigue identificado que el servidor ICTXSRVNETCOR01 presenta una situación crítica relacionada con el espacio en disco en la unidad F:\ la cual dispone únicamente de 69.4 GB libres de un total de 1.79 TB. Este espacio se encuentra comprometido principalmente por archivos antiguos de la aplicación CargueArchivos, almacenados desde el año 2019, por lo que se recomienda aplicar el aumento del almacenamiento en la ruta identificada o que se depuren archivos obsoletos por parte de los responsables de la aplicación, en dado caso que no se realicen estás dos sugerencias existe el riesgo de que el servidor quede sin espacio suficiente en esa partición, afectando gravemente el rendimiento, la estabilidad del sistema y la disponibilidad de la aplicación CargueArchivos, con posibles interrupciones en el servicio.

Se sigue identificado que el servidor ICTXSRVNETCOR01 presenta una situación crítica relacionada con el espacio en disco en la unidad E:\ la cual dispone únicamente de 4.82 GB libres de un total de 65 GB. Este espacio se encuentra comprometido principalmente por archivos antiguos que contienen todos los logs de las aplicaciones configuradas, por lo que se recomienda aplicar el aumento del almacenamiento en la ruta identificada, en dado caso que no se realice esta sugerencia existe el riesgo de que el servidor quede sin espacio suficiente en esa partición, afectando que no se registren más logs.

A continuación, se presenta un cuadro histórico consolidado del uso del almacenamiento en los discos del servidor ICTXSRVNETCOR01, seguido de observaciones y recomendaciones:

Disco	Métrica	jul-25	ago-25	sep-25	Observaciones	Recomendaciones
C:	Espacio usado	65% (66.6 GiB)	58% (58.1 GiB)	69% (68.97 GiB)	Se incrementó el uso en almacenamiento en comparación con el mes anterior en aproximadamente 11 GiB.	Considerar mover archivos no esenciales a otro volumen que dispongan desde el lado de infraestructura hacia almacenamiento secundario.
	Espacio libre	33.3 GiB	41.4 GiB	30.54 GiB		
F:	Espacio usado	92% (1.74 TiB)	95% (1.80 TiB)	96% (1.90 TiB)	Altísima ocupación constante (>90%), aunque mejora en septiembre debido al aumento del almacenamiento en 100GB	Urgente implementar políticas de depuración de archivos antiguos o inactivos.
	Espacio libre	146 GiB	89.4 GiB	72.91 GiB		Considerar expansión del volumen o migración de datos a almacenamiento secundario.
E:	Espacio usado	79% (51.7 GiB)	65% (42.5 GiB)	88% (57.08 GiB)	Aún se mantiene en zona de riesgo por encima del 80%.	Considerar mover archivos no esenciales a otro volumen que dispongan desde el lado de infraestructura hacia almacenamiento secundario.
	Espacio libre	13.3 GiB	22.4 GiB	7.92 GiB		Considerar expansión del volumen si requieren almacenar por mucho más tiempo los logs de las aplicaciones

Ilustración 42 Histórico consolidado uso de discos servidor ICTXSRVNETCOR01

14.3. Seguridad

Continuar con las respectivas socializaciones para realizar remediaciones tempranas y poder socializar o en su defecto, crear políticas cuando se detecten sus necesidades, por lo que se requiere

un análisis y levantamiento de información previa de lo cual para saber dónde se necesita y en qué procedimientos.

Implementación de TAGs a los recursos creados y existentes, paso que se debatirá posterior al análisis solicitado y entregado.

Analizar el inventario de aplicaciones en la entidad para darle un mejor uso a la nube Azure, este inventario debe tener versiones de lenguajes de programación, aun cuando el alcance es sólo Azure y sus políticas con mejores prácticas (gobernanza), es una oportunidad para que las buenas prácticas de la nube se apliquen también en los Datacenter de la entidad.

- Se debe trabajar en el perfilamiento de la navegación de acuerdo con lo entregado por ICETEX.
- Validar la autenticación de doble factor para todas las plataformas misionales del ICETEX.
- Realizar autenticación a través del LDAPS, para la gestión de las plataformas de seguridad.
- Realizar la contención automática de equipos que se identifiquen en la red como maliciosos.
- Realizar el aumento de recursos a la plataforma de FortiSIEM (CPU, Memoria y disco) y hacer un cambio de arquitectura con el objetivo de mejorar.
- Se debe realizar la integración de los activos críticos de la compañía a la plataforma de SIEM, no se ha podido lograr por la falta de recursos de este.
- Adquirir un equipo Firewall para correo para prevenir brechas de seguridad asociadas al uso del correo electrónico y que este es susceptible a muchos tipos de amenazas.
- Integrar los servidores de Directorio Activo con el SIEM.
- Garantizar la segmentación de la red que permita claramente definir qué servicios deben ser alcanzados por cada usuario.
- Se recomienda, que el ICETEX, adquiera una herramienta que permita realizar análisis de tráfico de la red (NTA- Network Traffic Analysis.
- Se recomienda una tecnología que permita la gestión o validación de privilegios de accesos (IAM). Evitar configurar usuarios y claves dentro de las aplicaciones de ICETEX.
- Validar a nivel de punto final, los equipos que se han visto involucrados con comportamiento malicioso.
- Integrar los equipos que hacen parte del proceso de pagos con el SIEM.
- Evaluar los riesgos sobre las plataformas en la nube y considerar aplicar plataformas de seguridad para los ambientes Cloud que cuenta la entidad ya que estos contienen servicios críticos para la misma.

14.4. Bases De Datos

Considerando el aumento en los espacios del área de recuperación del entorno de producción, se requiere escalar de manera equivalente la base de datos de réplica.

Las versiones disponibles del sistema manejador de base de datos ORACLE son Oracle Database 23 ai, Oracle Database 21c y Oracle Database 19c. No obstante que se dio inicio, al plan de migración de las bases de datos que se encuentran en versiones anteriores, se recomienda al ICETEX, que

analice la posibilidad de efectuar la migración sobre versiones más recientes con el fin de evitar ejecutar planes de migración con demasiada frecuencia.

14.5. Integrador De Nube

Se recomienda continuar con el plan de depuración de las configuraciones. Desde los últimos 2 meses se ha podido avanzar en estos aspectos.

- Se lograron avances sólidos en la optimización, ordenamiento y fortalecimiento de la infraestructura Microsoft Azure – ICETEX, consolidando un entorno productivo más organizado, seguro y alineado con buenas prácticas Cloud.
- Las actividades ejecutadas fortalecieron la gobernanza mediante la depuración de redes y grupos de recursos huérfanos, el ajuste de reglas NSG y el redimensionamiento de la VNet vm-app-home-vnet.
- La instrumentación de alertas preventivas y el aprovisionamiento de almacenamiento especializado mejoraron la observabilidad, permitiendo monitoreo oportuno de servicios críticos.
- La Reserva de Instancia aplicada a la VM vm-devops-agent representa un avance clave en eficiencia financiera, asegurando ahorros relevantes en el horizonte operativo.
- La documentación técnica consolidada para Datafondos refuerza la trazabilidad y asegura continuidad operativa bajo estándares de seguridad.
- La Solicitud Especial – Microsoft – ÁBACOS marca el inicio formal de la etapa de diseño y dimensionamiento del micrositio y plataforma educativa a migrar hacia ICETEX.
- El mes de Abril representó un progreso importante hacia la madurez operativa y de gobernanza del entorno Azure institucional, sentando bases para fases futuras de automatización, control de costos y consolidación arquitectónica.

15. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC

Con respecto a los valores agregados indicados contractualmente, se relaciona el estado:

15.1. Aumento de la capacidad de Ancho de Banda en algunas de las sedes de la Entidad

El proceso de ampliación de las sedes de la entidad se completó en el mes de abril de 2024 , permitiendo un aumento en la capacidad de ancho de banda conforme a lo establecido en el ANEXO # 2. esta información se puede evidenciar a través de la herramienta de monitoreo Solar Winds y se verifica mensualmente en la facturación de ICETEX.

15.2. TB de capacidad de almacenamiento

El almacenamiento definido contractualmente fue entregado en la fase de implementación por **Contrato** ingresaron las siguientes capacidades:

CONTRATADO			
Cod Servicio	**CIUDAD**	**ALCANCE**	**CAPACIDAD (TB)**
INR0194	TRIARA	Almacenamiento Centralizado 23 TB Tier 2	35
INR0193	TRIARA	Almacenamiento Centralizado 12 TB Tier 2.5	
INR0192	MEGACENTER	Almacenamiento Centralizado 15 TB Tier 2	25
INR0191	MEGACENTER	Almacenamiento Centralizado 10 TB Tier 2.5	
			60

Tabla 33 Capacidades de almacenamiento contratado

Aprovisionado se tienen las siguientes capacidades instaladas:

EJECUTADO		
TRIARA	**ALMACENAMIENTO APROVISIONADO (TB)**	Evidencia
Almacenamiento MVs VMware	49,6	RV Tools
Almacenamiento MVs KMV (BD)	10,9	RF1700669
TOTAL	**60,5**	
MEGACENTER	**ALMACENAMIENTO APROVISIONADO (TB)**	**Evidencia**
Almacenamiento MVs replicación VMware	19,4	RVTools
Almacenamiento MVs KMV (BD)	10,9	RF1700669
TOTAL	**30,3**	
TOTAL, ALMACENAMIENTO APROVISIONADO	**90,8**	

Tabla 34 Capacidades de almacenamiento aprovisionado

Se implementaron los 60TB que ingresaron por contrato y están en calidad de “préstamo” 30TB adicionales que están en DC Triara con máquinas virtuales clonadas, restauradas, apagadas o a la espera de actualización que consumen espacio.

En el almacenamiento aprovisionaron 3 TB como valor agregado de INFOTIC para realizar la prueba de restauración de Backups, durante el mes de Abril no se recibieron desde el Icetex solicitudes de pruebas de restauración.

15.3. “Wifi” para la gente en 19 sedes

Se ha estado llevando a cabo el cumplimiento contractual y hasta la fecha, se dispone de conexión wifi en las 14 sedes donde ICETEX tiene oficinas.

Enlace - Tipo medio	INR	BW- Mínimo Requerido (MBPS)	Ancho de Banda actual
BARRANQUILLA	**INR0094**	**10**	**10**
BUCARAMANGA	**INR0057**	**10**	**10**
CALI	**INR0160**	**10**	**10**
AGUAS	**INR0029**	**20**	**20**
CHAPINERO	**INR0015**	**20**	**20**
MEDELLIN	**INR0122**	**10**	**10**
APARTADO	**INR0140**	**10**	**10**
ARAUCA	**INR0115**	**10**	**10**
LETICIA	**INR0000378**	**10**	**10**
QUIBDO	**INR0021**	**10**	**10**
RIOHACHA	**INR0159**	**10**	**10**
SAN ANDRES	**INR0000368**	**10**	**10**
YOPAL	**INR0127**	**10**	**10**
MOCOA	**INR0141**	**10**	**10**

Tabla 35 WIFI para la gente instalados

Enlace - Tipo medio	INR	BW- Mínimo Requerido (MBPS)
Manizales	INR0088	10
Armenia	INR0074	10
Cartagena	INR0109	10
Sincelejo	INR0095	10
Pasto	INR0130	10

Tabla 36 WIFI para la gente pendientes

16. CONCLUSIONES

- El uso de autenticación de doble factor en las conexiones VPN de los funcionarios ayudaría a proteger mejor la información sensible y evitar accesos no autorizados.

- Administrar adecuadamente las contraseñas y permisos garantiza que solo las personas autorizadas accedan a información importante, reduciendo riesgos de seguridad.

- Configurar controles de acceso a la red basados en los servidores de la entidad permite restringir el acceso a ciertas áreas, evitando que los usuarios lleguen a sitios peligrosos.

- Optimizar los recursos del FortiSIEM facilitaría el monitoreo de sistemas clave como bases de datos, aplicaciones internas y equipos, permitiendo detectar problemas rápidamente y responder de forma oportuna.

- Ajustar las reglas de seguridad en la red ha permitido un mejor control sobre los recursos clave, asegurando que solo lo necesario esté disponible y fortaleciendo la protección.

- Implementar soluciones para gestionar quién puede conectarse a la red mejoraría la seguridad y reduciría el impacto de posibles incidentes.

- Los reportes del SOC han sido clave para detectar y corregir vulnerabilidades, evitando que amenazas afecten la infraestructura crítica de la entidad.

- Es fundamental contar con una persona desde ICETEX en temas de nube que pueda auditar y revisar autorizaciones, ya que su apoyo es crucial para abordar y resolver los hallazgos reportados, lo que permitirá avanzar en los proyectos relacionados con recursos en la nube. La falta de un responsable limita la capacidad de gestión y solución de problemas en este ámbito.

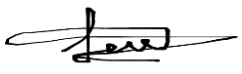
17. ANEXOS

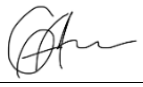
Tema	SubTema	Anexo
Almacenamiento	Backups Diarios	Backups diarios Abril 2026 (30 reportes) Backup Diario
	Informe de Backups	Consolidado mensual Backups Abril 2026 Consolidado Mensual de Backups abril 2026.pdf Informe Backups mes de Abril 2026.pdf Politica Backup Icetex_V6.xlsx
Aplicaciones	Informes de actividades	Informe actividades Módulos videoconferencia ICETEX Abril 2026 Informe actividades Módulos videoconferencia ICETEX abril 2026.pdf Informe mensual Administrador de Soluciones Abril 2026 Informe Mensual InfoTIC Administrador de Soluciones Abril2026.pdf Informe mensual Administrador Web Master Abril 2026 Informe Mensual InfoTIC Webmaster Abril2026.pdf Informe mensual Integrador Nube Abril 2026 Informe Mensual InfoTIC Integrador de Nube Abril2026.pdf
Bases De Datos		Informe mensual Administrador de Bases de datos Abril 2026 Informe Mensual InfoTIC DBA Abril2026.pdf
Ejecución Presupuestal		Conciliación Abril consolidado Conciliación_Abril_1-18_consolidado 2026.xlsx Conciliación_Abril_19-30_consolidado 2026.xlsx Informe de Gestión Servicio Abril 2026 Informe de Gestion Servicio Abril 2026.pdf Informe de Gestion Servicio Abril 2026.docx
Seguridad		Informe Mensual MARCA-OSINT ICETEX Abril 2026 Informe Mensual MARCA-OSINT ICETEX Abril 2026.pdf Anexo Informe Mensual MARCA-OSINT ICETEX Abril 2026.xlsx Informe Mensual Seguridad Abril 2026 Informe Mensual InfoTIC Seguridad Abril2026.pdf Acta Empalme ADMIN SEGURIDAD.pdf Informe Mensual SOC - ICETEX Abril 2026 Informe Mensual SOC-TH ICETEX abril 2026.pdf

Tema	SubTema	Anexo
		Declaración de cumplimiento en seguridad de la información – Contrato 2022-0792-20260422093521.pdf
Soporte Y Monitoreo	**Canales**	ANS Abril 2026 ANS_Abril_2026.xlsx Informe mensual Administrador de Networking Abril 2026 Informe Mensual InfoTIC Administrador de Redes Abril2026.pdf Informe Mensual Disponibilidad Abril2026 Reporte Mensual Disponibilidad INFOTIC Abril 2026.pdf
	Gráficas de consumo	Informe Mensual ALLOT Abril 2026 Graficas de consumo Abril 2026 – ALLOT INFOTIC.xls
Data center Alterno	**Replicación**	Informe mensual replicación Abril 2026 Informe mensual replicacion Abril 2026.pdf Reportes diarios Abril 2026 (30 reportes) Replicaciones
Data Center Principal		Reporte Monitoreo ICETEX Abril 2026-ELK Reporte Monitoreo ICETEX Abril_ELK.pdf Reporte Monitoreo ICETEX Abril_1-19_2026-ELK.pdf Reporte Monitoreo ICETEX Abril_20-30_2026-ELK.pdf Data ELK Disponibilidad Server_ELK_Abril_2026.xlsx Disponibilidad Server_ELK_Abril_1-19_2026.xlsx Disponibilidad Server_ELK_Abril_20-30_2026.xlsx

Tabla 37 Anexos

Revisión técnica

REVISÓ	FIRMAS
SANDRA MILENA GARCIA HERNANDEZ CONTRATISTA GRUPO DE INFRAESTRUCTURA	
JOAO DO NELSON DUCUARA CONTRATISTA GRUPO DE VOT	

REVISÓ	FIRMAS
GERMAN MANUEL DIAZ CONTRATISTA GRUPO DE INFRAESTRUCTURA	
NELSON JAVIER CASALLAS BELTRAN CONTRATISTA GRUPO DE INFRAESTRUCTURA	