



INFORME DE ACTIVIDADES DEL CONTRATO

**CONTRATO NUMERO
2022-0792**

Mayo 01 al 31 de 2026

versión	Observaciones	Fecha	Responsable
1.0	Versión Inicial	01/06/2026	Francisco Javier Pulido

Tabla de contenido

1.	INTRODUCCIÓN	9
2.	OBJETIVO DEL INFORME	11
3.	ALCANCE	12
4.	AVANCE TÉCNICO	13
4.1.	CONECTIVIDAD Y RED DE COMUNICACIONES	13
4.1.1.	CANALES INSTALADOS EN EL MES Y ENTREGABLES	14
4.1.2.	DESPLIEGUE DE DIRECCIONES IP V6	15
4.1.3.	RECOMENDACIONES	16
4.2.	CENTRO DE DATOS.....	16
4.2.1.	CENTRO DE DATOS PRINCIPAL	16
4.2.1.1.	APLICACIONES	16
4.2.1.1.1.	<i>Principales Hallazgos y Alertas Críticas.....</i>	18
4.2.1.2.	BASES DE DATOS	20
4.2.1.3.	SITIO WEB “PORTAL ICETEX”	24
4.2.2.	CENTRO DE DATOS ALTERNO.....	28
4.2.2.1.	HOSTING VIRTUAL (IAAS)	28
4.2.2.2.	DATA GUARD BASES DE DATOS MEGACENTER	31
4.2.2.3.	SERVICIOS DE HOUSING – DATACENTER ALTERNO	32
4.2.3.	CONCLUSIONES	32
4.3.	SEGURIDAD INFORMÁTICA	32
4.3.1.	GESTIÓN Y FORTALECIMIENTO DE LA SEGURIDAD PERIMETRAL.....	34
4.3.2.	MONITOREO DE SEGURIDAD Y RESPUESTA ANTE INCIDENTES	34
4.3.3.	GESTIÓN OPERATIVA Y SOPORTE DE SEGURIDAD	35
4.3.4.	PLATAFORMAS ADMINISTRADAS	35
4.3.4.1.	FORTIGATE TRIARA.....	36
4.3.4.2.	FORTIGATE AGUAS	38
4.3.4.3.	FORTIGATE MEDELLÍN	40
4.3.4.4.	FORTIWEB 2000F	40
4.3.4.5.	FORTIWEB 2000E.....	40
4.3.4.6.	FORTIWEB CLOUD DRP	40
4.3.4.7.	FORTISANDBOX.....	41
4.3.4.8.	FORTISIEM.....	41
4.3.4.9.	SOPHOS ENDPOINT	42
4.3.5.	RECOMENDACIONES DE SEGURIDAD PARA EL ICETEX.	43

4.3.6.	SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC).....	44
4.3.6.1.	INDICADORES DE COMPROMISO (THREAD HUNTING):	45
4.3.6.2.	ALERTAS O INCIDENTES DE SEGURIDAD DETECTADOS	46
4.3.6.2.1.	CATEGORÍA SEGURIDAD.....	46
4.3.6.2.2.	CATEGORÍA DISPONIBILIDAD	47
4.3.6.2.3.	AMENAZAS DE CIBERSEGURIDAD	49
4.3.6.3.	THREAT HUNTING.....	50
4.3.6.4.	ANÁLISIS DE MARCA OSINT	51
4.3.7.	ANÁLISIS DE VULNERABILIDADES ICETEX	54
4.3.7.1.	CONSOLIDADO GENERAL DE VULNERABILIDADES	55
4.3.7.2.	CONCLUSIONES	57
4.4.	SERVICIOS DE NUBE	57
4.4.1.	PRINCIPALES AVANCES TÉCNICOS.....	57
4.4.2.	COMPORTAMIENTO FINANCIERO DEL ENTORNO AZURE	58
5.	GESTION DE LA EJECUCIÓN CONTRACTUAL.....	59
6.	GESTION PRESUPUESTAL	59
7.	GESTION ADMINISTRATIVA	60
7.1.	PROFESIONALES.....	60
8.	SERVICIO DE COLABORACIÓN	61
9.	GESTION DE RIESGOS Y PROBLEMAS	63
10.	INDICADORES CLAVE DE DESEMPEÑO	63
10.1.	ANS POR DISPONIBILIDAD DE CANALES DE COMUNICACIONES	63
10.2.	CANAL DE REPLICACIÓN (TRIARA – MEGACENTER).....	66
10.3.	ANS POR DISPONIBILIDAD DE SERVIDORES	67
10.4.	DISPONIBILIDAD TRIARA PARA LOS SERVICIOS DE PÁGINA WEB ICETEX.....	68
10.4.1.	ANÁLISIS COMPONENTE LIFERAY PRODUCCIÓN	73
10.5.	BACKUP SERVIDORES TRIARA	73
11.	CONTROL DE CAMBIOS	75
12.	PLAN DE TRABAJO DE LOS PROXIMOS MESES	75
13.	PLAN DE ENTREGA	76
14.	OBSERVACIONES RELEVANTES	76
15.	RECOMENDACIONES DEL CONTRATISTA AL ICETEX	77
15.1.	NETWORKING	77
15.2.	APLICACIONES	77

15.3.	SEGURIDAD.....	79
15.4.	BASES DE DATOS.....	80
15.5.	INTEGRADOR DE NUBE	81
16.	EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC	82
16.1.	AUMENTO DE LA CAPACIDAD DE ANCHO DE BANDA EN ALGUNAS DE LAS SEDES DE LA ENTIDAD	82
16.2.	TB DE CAPACIDAD DE ALMACENAMIENTO	82
16.3.	“WIFI” PARA LA GENTE EN 14 SEDES	83
17.	CONCLUSIONES.....	83
18.	ANEXOS	85

Indice de Tablas

TABLA 1 CASOS ATENDIDOS NETWORKING COMPARATIVO MES ANTERIOR	15
TABLA 2 CONSUMO DE RECURSO DE HARDWARE MAYO	17
TABLA 3 CONSUMO DE RECURSO DE HARDWARE ABRIL	17
TABLA 4 CONSUMO DE RECURSO DE HARDWARE MARZO	17
TABLA 5 VIGENCIA DE LOS CERTIFICADOS DIGITALES	18
TABLA 6 INVENTARIO PRINCIPALES SERVIDORES PRODUCCIÓN	19
TABLA 7 SERVIDORES Y SCHEMAS ADMINISTRADOS	20
TABLA 8 ESTADO BD ORACLE.....	21
TABLA 9 CRECIMIENTO DE LAS BASES DE DATOS EN LOS ÚLTIMOS 8 MESES	24
TABLA 10 TOP 10 PORTALES MÁS UTILIZADOS.....	25
TABLA 11 ESTADO LICENCIAMIENTO PORTAL WEB ICETEX	27
TABLA 12 SERVICIOS REPLICADOS – DATACENTER ALTERNO-MEGACENTER	30
TABLA 13 TOP 5 MÁQUINAS MAYOR TASA DE TRANSFERENCIA	30
TABLA 14 TOP 5 MÁQUINAS MENOR TASA DE TRANSFERENCIA	30
TABLA 15 DISPONIBILIDAD DE SERVICIOS DE HOUSING – DATA CENTER ALTERNO	32
TABLA 16 DETALLE PLATAFORMAS SEGURIDAD ADMINISTRADAS INFOTIC.....	35
TABLA 17 LICENCIAMIENTO FORTIGATE	36
TABLA 18 LICENCIAMIENTO FORTIWEB	40
TABLA 19 CONFIGURACIÓN FORTISANDBOX 1000D	41
TABLA 20 RECOMENDACIONES DE SEGURIDAD	44
TABLA 21 COMPARATIVO – INDICADORES DE COMPROMISO	45
TABLA 22 COMPARATIVO ALERTAS DE SEGURIDAD	46
TABLA 23 TOTAL DE CASOS GESTIONADOS	52
TABLA 24 VULNERABILIDADES ENCONTRADAS	56
TABLA 25 COMPARATIVO COMPORTAMIENTO FINANCIERO AZURE (ABRIL-MAYO).....	58
TABLA 26 EJECUCIÓN PRESUPUESTAL	60
TABLA 27 PERFILES Y ACTIVIDADES.....	61
TABLA 28 GRUPO ADMINISTRATIVO	61
TABLA 29 DISTRIBUCIÓN MÓDULOS DE VIDEOCONFERENCIA POR SEDE.....	62
TABLA 30 DISPONIBILIDAD DE CANALES	66
TABLA 31 DISPONIBILIDAD CANALES “INTERNET PARA LA GENTE”	66
TABLA 32 DISPONIBILIDAD CANALES SDWAN.....	66
TABLA 33 CÓDIGOS RELACIONADOS DISPONIBILIDAD SERVICIOS EN HOUSING – DATACENTER PRINCIPAL	68
TABLA 34 DISPOSITIVOS EN HOUSING – DATACENTER PRINCIPAL	68
TABLA 35 DISTRIBUCIÓN TRIMESTRAL DE ACCESO POR USUARIOS.....	69
TABLA 36 PLANES DE TRABAJO	76
TABLA 37 BALANCE GENERAL ACTIVIDADES EJECUTADAS PLAN DE ENTREGA	76
TABLA 38 CAPACIDADES DE ALMACENAMIENTO CONTRATADO	82
TABLA 39 CAPACIDADES DE ALMACENAMIENTO APROVISIONADO	82
TABLA 40 WIFI PARA LA GENTE INSTALADOS.....	83
TABLA 42 ANEXOS	86

Índice de Ilustraciones

ILUSTRACIÓN 1 DISPONIBILIDAD DEL CLÚSTER	14
ILUSTRACIÓN 2 DISPONIBILIDAD DEL CLUSTER	22
ILUSTRACIÓN 3 DISPONIBILIDAD DE LAS BASES DE DATOS PRINCIPALES ICTXCYC Y APOTEOSYS	22
ILUSTRACIÓN 4 CASOS DEL PROYECTO GESTIONADOS ARANDA BASES DE DATOS	23
ILUSTRACIÓN 5 TRÁFICO GENERAL DE LOS PORTALES.....	25
ILUSTRACIÓN 6 UPTIME: PORTAL WEB WEB.ICETEX.GOV.CO [99,761%]	26
ILUSTRACIÓN 7 REPORTES DE REPLICACIÓN SRM A SITIO ALTERNO – MAYO 2026	29
ILUSTRACIÓN 8 FECHAS CON MAYOR REPLICACIÓN	30
ILUSTRACIÓN 9 EVIDENCIA DATAGUARD REPLICADO A MEGACENTER BD.....	31
ILUSTRACIÓN 10 - CASOS OPERADOR DE SEGURIDAD	32
ILUSTRACIÓN 11 DIAGRAMA DE LA ARQUITECTURA DE SEGURIDAD	33
ILUSTRACIÓN 12 TOPOLOGÍA DE WAF CLOUD USADO EN PORTALES DE MEDELLÍN	34
ILUSTRACIÓN 13 CONSUMO CANAL MPLS - PROMEDIO 168,34 MBPS [INR0185 CLARO(MPLS_DC)]	36
ILUSTRACIÓN 14 CONSUMO CANAL INTERNET SEDES - PROM 18 MBPS WAN-SEDES-ICETEX [INR0264 (INTE_SEDES_ICTX)]	37
ILUSTRACIÓN 15 CONSUMO CANAL INTERNET DATACENTER -PROM 66,58 MBPS [INTERNET_DC_INR0000320 (INET_CLARO)] ...	37
ILUSTRACIÓN 16 FILTRADO – WEB – (FORTIGATE – TRIARA)	37
ILUSTRACIÓN 17 INSPECCIÓN – SSL – (FORTIGATE – TRIARA)	38
ILUSTRACIÓN 18 ANTIVIRUS Y ANTIMALWARE – PERIMETRAL (FORTIGATE – TRIARA)	38
ILUSTRACIÓN 19 CONSUMO CANAL MPLS AGUAS - PROMEDIO 41,37 MBPS (PORT7)	39
ILUSTRACIÓN 20 FILTRADO-WEB-(FORTIGATE-AGUAS).....	39
ILUSTRACIÓN 21 INSPECCIÓN-SSL-(FORTIGATE-AGUAS)	39
ILUSTRACIÓN 22 ANTIVIRUS Y ANTIMALWARE-PERIMETRAL-(FORTIGATE-AGUAS)	39
ILUSTRACIÓN 23 CONSUMO CANAL MPLS MEDELLÍN	40
ILUSTRACIÓN 24 TRÁFICO GENERAL DE LOS PORTALES	41
ILUSTRACIÓN 25 LICENCIAMIENTO FORTISIEM	41
ILUSTRACIÓN 26 FORTISIEM PERFORMANCE POR PROCESOS.....	42
ILUSTRACIÓN 27 ESTADO SEGURIDAD SOPHOS	43
ILUSTRACIÓN 28 TOTAL DE ALERTAS DE SEGURIDAD	46
ILUSTRACIÓN 29 TOP 5 DE ALERTAS DE SEGURIDAD ALTAS.....	47
ILUSTRACIÓN 30 TOP 5 DE ALERTAS DE SEGURIDAD MEDIAS	47
ILUSTRACIÓN 31 TOTAL DE ALERTAS DE DISPONIBILIDAD	47
ILUSTRACIÓN 32 TOP 5 DE ALERTAS DE DISPONIBILIDAD ALTAS.....	48
ILUSTRACIÓN 33 TOP DE ATAQUES PERMITIDOS.....	49
ILUSTRACIÓN 34 TOP DE ATAQUES DENEGADOS	49
ILUSTRACIÓN 35 PRINCIPALES PUERTOS ENTRANTES POR CONEXIONES Y BYTES V3 (TRAFICO PERMITIDO)	50
ILUSTRACIÓN 36 PRINCIPALES PUERTOS SALIENTES POR CONEXIONES Y BYTES V3 (TRAFICO PERMITIDO).....	50
ILUSTRACIÓN 37 REPORTES THREAT HUNTING	51
ILUSTRACIÓN 38 INCIDENTES POR TIPO DE AMENAZA.....	51
ILUSTRACIÓN 39 CRONOGRAMA DETALLADO EJECUCIÓN DE PRUEBAS ANÁLISIS DE VULNERABILIDADES	54
ILUSTRACIÓN 40 CONSOLIDADO GENERAL DE VULNERABILIDADES	55
ILUSTRACIÓN 41 MÉTRICA DE VISITANTES PORTAL WEB WEB.ICETEX.GOV.CO	69
ILUSTRACIÓN 42 MÉTRICA ADQUISICIÓN USUARIOS PORTAL WEB WEB.ICETEX.GOV.CO	70

ILUSTRACIÓN 43 MÉTRICA DE USUARIO POR PAÍS - PORTAL WEB WEB.ICETEX.GOV.CO	70
ILUSTRACIÓN 44 MÉTRICA DE CIUDADES DE COLOMBIA- PORTAL WEB WEB.ICETEX.GOV.CO.....	70
ILUSTRACIÓN 45 NODO 1 CPU	71
ILUSTRACIÓN 46 NODO 1 MEMORIA	72
ILUSTRACIÓN 47 NODO 1 ALMACENAMIENTO.....	72
ILUSTRACIÓN 48 EVIDENCIA BACKUP SERVIDORES RESUMEN GENERAL BACKUPS.....	74
ILUSTRACIÓN 49 EVIDENCIA BACKUP SERVIDORES RESUMEN BACKUPS Y SU ESTADO.....	74
ILUSTRACIÓN 50 HISTÓRICO CONSOLIDADO USO DE DISCOS SERVIDOR ICTXSRVNETCOR01.....	79

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 31 de Mayo 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 soporta y garantiza 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 Mayo de 2023 y el 19 de Mayo 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 17,2% de ejecución.

Durante el mes de mayo de 2026, la operación del contrato 2022-0792 presentó niveles adecuados de disponibilidad y continuidad. No obstante, se identificaron riesgos críticos asociados a infraestructura obsoleta, saturación de almacenamiento en servidores clave, licenciamiento vencido o próximo a vencer en plataformas de seguridad y limitaciones en herramientas SIEM. Se recomienda priorizar acciones inmediatas en renovación tecnológica, gestión de capacidad y fortalecimiento de seguridad.

El análisis técnico en síntesis puede señalar que la operación mantiene estabilidad general, con adecuados niveles de disponibilidad en servicios críticos.

Por lo anterior, se detectan riesgos como los que se mencionan a continuación:

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

- Riesgo de indisponibilidad por obsolescencia tecnológica.
- Riesgo de seguridad por licencias vencidas.
- Riesgo de pérdida de información por saturación de almacenamiento.
- Riesgo operacional por falta de monitoreo integral SIEM.

Ante los riesgos detectados, la correcta operatividad está expuesta a fallas en cualquier momento por obsolescencia, mayor exposición a vulnerabilidades, incremento de incidentes, riesgo de indisponibilidad, dependencia de soporte limitado, posibles incompatibilidades futuras, falta de soporte ante cualquier incidente que impida su solución inmediata, por lo cual, la gestión es principalmente reactiva, dado que existen brechas estructurales que incrementan el riesgo operativo, especialmente en seguridad, almacenamiento y renovación tecnológica.

En aras de mitigar los riesgos detectados se requiere de acciones estratégicas inmediatas que permitan resolver los anteriores riesgos. La evolución del contrato dependerá de la capacidad de transición desde una gestión reactiva hacia un modelo preventivo y optimizado.

Lo anterior, es debido a que la entidad opera actualmente con una infraestructura tecnológica obsoleta, lo que hace indispensable implementar un plan estructurado de renovación tecnológica por prioridades:

- **Equipos de red obsoletos:** la mayoría con más de 15 años en operación.
- **Ciclo de vida vencido:** Infraestructura en estado EOL/EOS.
- **Sistemas operativos desactualizados** y sin soporte.
- **Software legado:** Aplicaciones sobre *.NET Classic* sin soporte vigente.

La infraestructura de conectividad evidencia altos niveles de cobertura con los siguientes resultados:

- 100% de canales principales implementados.
- 96.55% de canales Backup instalados.
- Cobertura WIFI en sedes.

Respecto al frente de seguridad, tal como se ha comentado, presenta avances operativos, pero existe una brecha importante entre las capacidades actuales y el nivel de protección requerido para una entidad crítica.

Frente al componente de respaldo y continuidad operativa es uno de los componentes más maduros y estables del servicio.

El componente cloud presenta un nivel de gestión técnica avanzado y orientado a buenas prácticas, tal como se muestra a continuación:

- Assessment cloud con 96% de cumplimiento.
- Reducción de costos del 81.9%.
- Optimización de recursos.
- Fortalecimiento de políticas cloud.
- Mejoras de resiliencia y seguridad.

2. OBJETIVO DEL INFORME

Presentar las actividades ejecutadas por INFOTIC durante el periodo del 01 al 31 de mayo 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 híbrido o multi-nube.
- **Servicios Conexos:**
Detalle de actividades complementarias relacionadas con la infraestructura tecnológica, como soporte técnico de los componentes anteriormente descritos, 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 31 de mayo 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 alternativo (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 Alternativo 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 híbrida. 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

Los canales de conectividad operaron de manera estable. Las únicas excepciones críticas de disponibilidad corresponden a la sede de **San Andrés** (afectada por fluctuaciones extremas de energía en el rack de comunicaciones que obligaron al apagado preventivo de equipos) y caídas puntuales en enlaces específicos (Cartagena, Tumaco). Se ha gestionado de manera continua los casos reportados que afectan directamente los canales o la herramienta de monitoreo.

Durante el presente periodo se gestionaron y cerraron un total de 18 solicitudes de soporte e incidentes, lo que representa un leve decremento frente a las 20 del mes anterior.

Se solventaron el 100% de las vulnerabilidades asignadas al área de redes en el último ciclo. Se está a la espera de un nuevo escaneo por parte de ICETEX.

En cuanto a la solicitud de Control de Accesos (Requerimiento Bizagi/ORI) de restringir accesos a 12 funcionarios de la Oficina de Relaciones Internacionales (ORI), se determinó que la mayoría labora en modalidad remota con equipos personales. Se entregó la información de direccionamiento MAC viable y se aclararon las limitaciones técnicas de visibilidad sobre redes externas.

Se implementó un ajuste en los firewalls para priorizar el tráfico de Microsoft Teams, asignando un ancho de banda garantizado (mínimo 50 Mbps / máximo 150 Mbps) para mejorar la experiencia de usuario.

Se completó con éxito la inducción, entrega de credenciales, documentación y accesos al Ingeniero Walter, quien se integró al equipo de Networking de INFOTIC.

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 y entrega de informes conforme a los lineamientos periódicos de ICETEX.

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.

A continuación se encuentra el link del inventario de equipos:

[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 puede consultar en el siguiente link con el nombre “TOPOLOGIA ICETEX VISIO_V4_2”

<https://ICETEX.sharepoint.com/sites/Infraestructura/Documentos%20compartidos/Forms/AllItems.aspx?id=%2Fsites%2FInfraestructura%2FDocumentos%20compartidos%2FTOPOLOGIAS%20DE%20AGUAS&viewid=2cd2befc%2D9f50%2D42c3%2Db53a%2D74e0122a42e3>

Se comparte una visualización del diagrama:

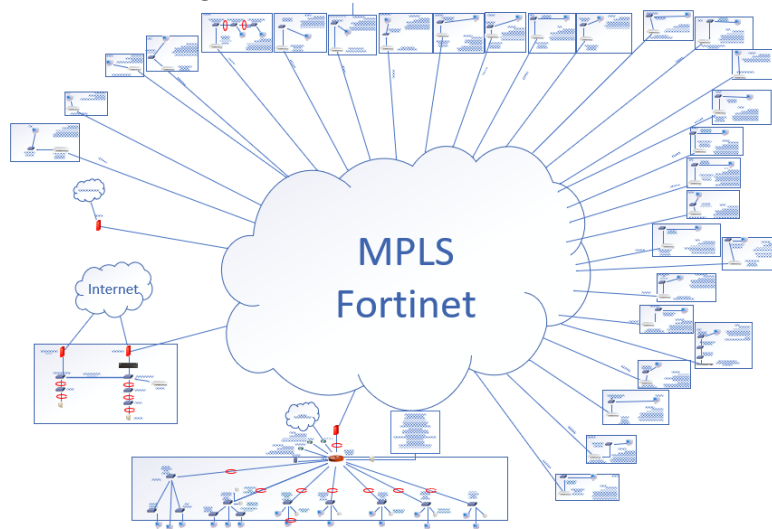


Ilustración 1 Disponibilidad del clúster

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.

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

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 Mayo 2026.pdf](#)

Solicitudes Nuevas Instalación de canales. En el periodo no se han recibido solicitud de instalación de nuevos canales, durante este mes se culminó la reimplementación de los canales SD-WAN de acuerdo a los requerimientos del ICETEX en las sedes de aguas, Mocoa, Leticia y San Andres.

Los casos atendidos durante el mes están disponibles en el siguiente enlace: [Registro Aranda Mayo 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
Mayo	18

Tabla 1 Casos atendidos Networking comparativo mes anterior

4.1.2. Despliegue de direcciones IP V6

Se ha alcanzado el 100% de ejecución en las pruebas de conectividad IPv6 para los canales de las 32 sedes. Se realizó un trabajo articulado entre el Infotíc, Icetex y ComWare.

Finalizada la fase de canales, el apoyo se centró en la implementación de IPv6 en los servidores, el Portal ICETEX y demás aplicaciones de la entidad. En el caso del servidor MIRA (implementado en meses anteriores), el proceso concluyó con éxito; sin embargo, este mes cuando se continuo con la aplicación de Aranda hubo un hallazgo crítico y el proveedor confirmó que no cuenta con soporte nativo para IPv6. Como acción de mitigación, Icetex indicó que se coordinará con el área de Seguridad el diseño de un mecanismo de transición mediante NAT64, adoptando el mismo modelo técnico utilizado previamente en MIRA.

4.1.3. Recomendaciones

Renovación de Equipos: Los equipos activos de red se encuentran en estado EOL (End-of-Life) y EOS (End-of-Sale). Al contar con más de 15 años de antigüedad, carecen de soporte o garantía del fabricante. Se reitera la recomendación urgente a ICETEX de adquirir nueva infraestructura para evitar fallos catastróficos.

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 periodo se evidenció un incremento en el volumen de casos gestionados en comparación con el mes anterior. Se atendieron de forma satisfactoria un total de **9 solicitudes críticas** distribuidas de la siguiente manera:

- **3 Tareas de Cambio:** Destacando el paso a producción del servicio *Windows Deceval* y los despliegues en aplicaciones clave (*Cuentas Abandonadas, Portal Transaccional, Pago Anticipado y Beneficios*).
- **6 Requerimientos de Acceso y Soporte:** Gestión de permisos institucionales y accesos FTP para personal autorizado.
- **Cumplimiento:** El 100% de los casos fueron solucionados, cerrados y cuentan con su respectivo soporte documental en PDF.

La validación del visor de eventos (logs) de los servidores principales de producción (*ICTXSRVNETCOR01, ICTXSRVAPPSMIX1, ICTXSRVMOODLE, ICTXSRVDCVAL01 y ICTXSRVPASARELADEPAGOS*) ratifica un **comportamiento operativo normal**. No se detectaron fallas críticas, errores de seguridad ni anomalías de rendimiento.

El consumo de recursos de hardware en los últimos tres meses (Marzo - Mayo 2026) se mantiene estable y dentro de los umbrales seguros de operación, excepto para el **ICTXSRVNETCOR01*** en tema de almacenamiento:

Servidor Principal	Tendencia Memoria RAM (Mayo)	Tendencia CPU (Mayo)	Estado Operativo
ICTXSRVNETCOR01	73%	28%	Alerta en Almacenamiento
ICTXSRVAPPSMIX1	70%	30%	Estable
ICTXSRVDCVAL01	50%	20%	Estable
ICTXSRVAPPSMIX2	53%	27%	Estable
ICTXSRVMOODLE	46%	33%	Estable

Tabla 2 Consumo de recurso de hardware Mayo

Servidor Principal	Tendencia Memoria RAM (Abril)	Tendencia CPU (Abril)	Estado Operativo
ICTXSRVNETCOR01	75%	33%	Alerta en Almacenamiento
ICTXSRVAPPSMIX1	65%	10%	Estable
ICTXSRVDCVAL01	40%	15%	Estable
ICTXSRVAPPSMIX2	50%	15%	Estable
ICTXSRVMOODLE	40%	20%	Estable

Tabla 3 Consumo de recurso de hardware Abril

Servidor Principal	Tendencia Memoria RAM (Marzo)	Tendencia CPU (Marzo)	Estado Operativo
ICTXSRVNETCOR01	70%	25%	Alerta en Almacenamiento
ICTXSRVAPPSMIX1	75%	30%	Estable
ICTXSRVDCVAL01	65%	10%	Estable
ICTXSRVAPPSMIX2	60%	20%	Estable
ICTXSRVMOODLE	55%	15%	Estable

Tabla 4 Consumo de recurso de hardware Marzo

4.2.1.1.1. Principales Hallazgos y Alertas Críticas

El servidor crítico **ICTXSRVNETCOR01**, que aloja componentes esenciales de la operación (*CargueArchivos*, *ConciliacionesIES*, *TransunionAPI*, *PasarelaKushki*, *PortalTransaccional*, *WsDynamics*, entre otros), presenta una **saturación del 97% de capacidad en su Unidad F**. Esta condición representa un riesgo inminente para la estabilidad y disponibilidad de las aplicaciones web e integraciones institucionales.

- **Intervención Inmediata de Almacenamiento:** Evaluar alternativas técnicas inmediatas (ampliación de disco virtual, depuración de logs históricos o migración de archivos antiguos a un almacenamiento secundario) para restablecer un margen operativo seguro.

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 Mayo2026.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.

Certificados SSL: 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 mantiene un control estricto sobre el ciclo de vida, vigencia y renovación de los certificados digitales para los subdominios bajo la raíz *icetex.gov.co*. A continuación, se presenta el estado de estos:

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

Tabla 5 Vigencia de los certificados digitales

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

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	IP	SISTEMA OPERATIVO	SERVIDOR WEB	MEMORIA RAM	CPU	ALMACENAMIENTO
ICTXSRVNETCOR01	192.168.51.165	Windows Server 2016 Standard 64-bit	IIS	27GB	16VCPU	2TB
ICTXSRVAPPSMIX1	192.168.51.135	Windows Server 2019 Standard 64-bit	IIS	12GB	4VCPU	200GB
ICTXSRVDCVAL01	192.168.51.17	Windows Server 2016 Standard 64-bit	Apache Tomcat	8GB	4VCPU	140GB
MIRA	192.168.20.4	Windows Server 2008 R2 Enterprise 64-bit	IIS	32GB	12VCPU	1,6TB
KIOSKODIGITAL	192.1.1.22	Windows Server 2008 R2 Enterprise 64-bit	IIS	16GB	4VCPU	650GB
SRV_APLIC	192.1.1.4	Windows Server 2003 R2 Standard Edition	IIS	4GB	6VCPU	550GB
ICTXSRVMOODLE	192.168.51.82	Windows Server 2019 Standard 64-bit	IIS	12GB	6VCPU	250GB
ICTXSRVAPPSMIX2	192.168.51.139	Windows Server 2019 Standard 64-bit	Tarea programada CustomWindowsServiceNovacion	8GB	4VCPU	150GB
ICTXSRVpasareladepagos	192.168.51.211	Windows Server 2022 Standard 64-bit	IIS	16GB	8VCPU	800GB

Tabla 6 Inventario principales servidores producción

De acuerdo con lo anterior, también se anexa archivo de inventario en cual se consolida información relacionada con los servidores asociados a aplicaciones institucionales, incluyendo su ambiente, estado operativo, direcciones de acceso (URLs), configuración de red, tecnologías utilizadas, así como aspectos de seguridad, pertenencia a dominio, estado de actualización y configuraciones generales de cada servidor [Inventario General Servidores.xlsx](#)

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

Durante este mes se verificaron, pero no se instalaron, los paquetes acumulativos y de seguridad críticos de Microsoft (Windows Server 2016, 2019 y 2022). Esto se debió a que no se pudieron gestionar los controles de cambio respectivos, ya que ICETEX no cuenta actualmente con un especialista en virtualización. Por lo tanto, es necesario reactivar estos procesos mediante ventanas de mantenimiento programadas (RFC), considerando que dichas actualizaciones son indispensables para mitigar los riesgos asociados a vulnerabilidades conocidas.

En el informe de los especialistas de soluciones, se presenta un resumen detallado de los hallazgos por servidor encontrados a la fecha, 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.

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		ASM 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

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

DRP - PRODUCCION		BASES DE DATOS	VERSION
GRID Infraestructure		ASM user grid	19.13.0.0.0
192.1.2.80		ICTXCYPD	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

OEN		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 7 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	5.751
ICETEX	11.0.2.0.4	210
APLICATI	11.0.2.0.4	247
APOTEOSY	11.0.2.0.4	484
VIGIAPRD	19.29.0.0	236
LIFERAY LIFERAYPDB	19.29.0.0	32

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

LANDICTX	19.29.0.0	615
SGDEA	19.29.0.0	177

Tabla 8 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 695 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 Mayo 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 archivolog, 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 19C, ICTXCYC 19C Core de crédito cierre mensual).
- Se realizaron actividades de tuning base de datos de control doc se ejecuta un afinamiento de un top de consultas de esta bd que tenían un costo de ejecución bastante elevado, realizando la creación de índices y aplicando las recomendaciones del optimizador de Oracle para mejor su rendimiento
- Se ejecutaron los cierres de las bases de datos del core solicitado por él cliente.

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

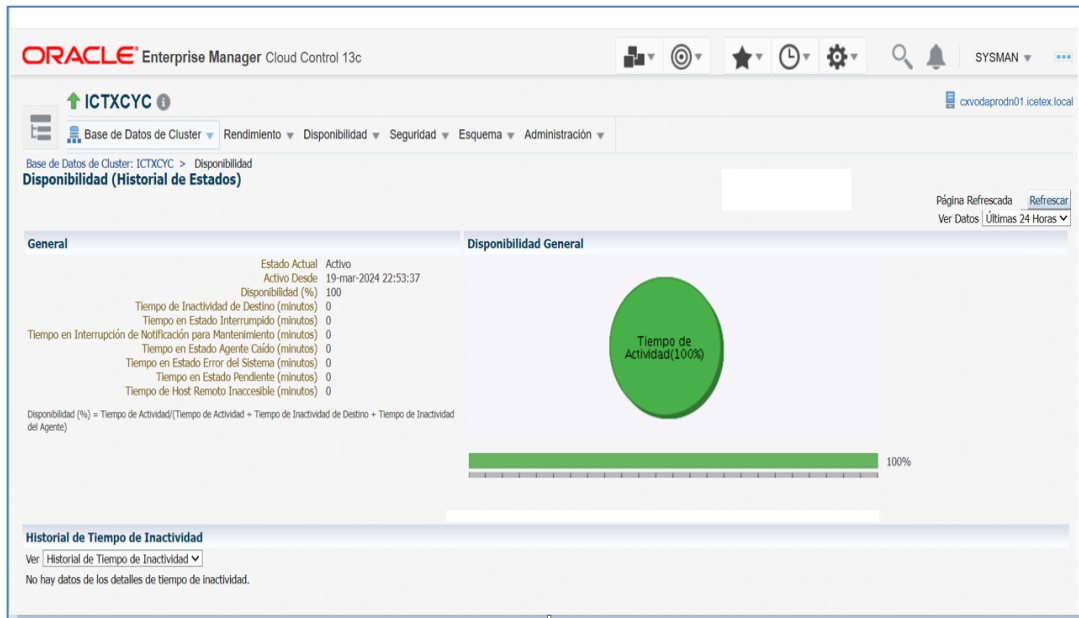


Ilustración 2 Disponibilidad del cluster

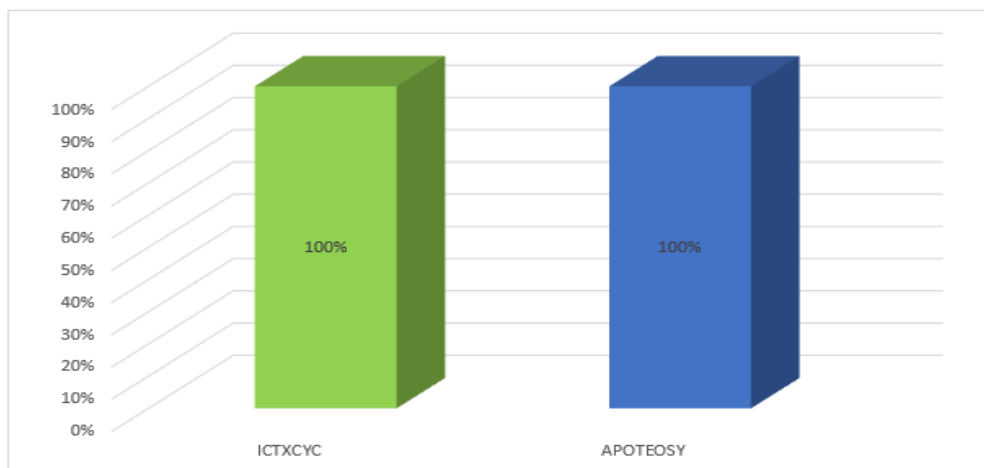


Ilustración 3 Disponibilidad de las Bases de Datos principales ICTXCYC y APOTEOSY

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 esta 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:

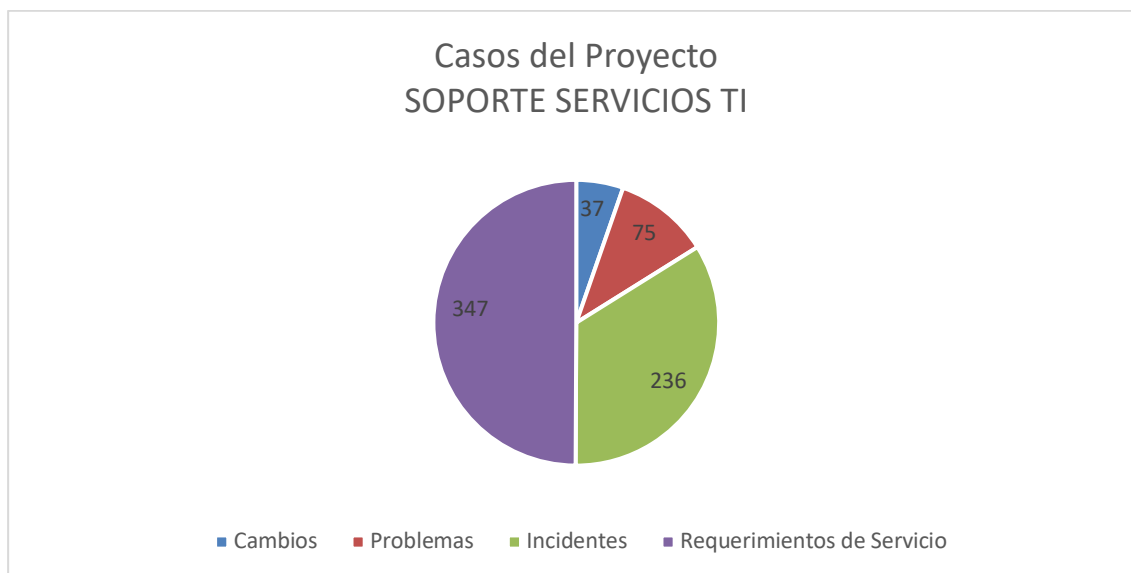


Ilustración 4 Casos del proyecto Gestionados Aranda Bases de datos

Desde Bases de datos se tienen las siguientes recomendaciones:

Se identifica la necesidad de crear las tareas y cronologías para la **migración de las bases de datos que aún operan en la versión Oracle 11G** (ICTXCYC, ICETEX, APLICATI, APOTEOSY). Al ser una versión fuera de soporte por parte del fabricante, representa un riesgo de cumplimiento y seguridad. Se recomienda su actualización a la versión **19C o superior**.

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. La información es obtenida a través de la herramienta OEM (Oracle Enterprise Manager). El espacio ocupado se encuentra expresado en Gigas.

BASE DE DATOS	"OCT-2025"	"NOV 2025"	"DICIEMBRE 2025"	ENERO 2026	FEBRERO 2026	"MARZO 2026"	"ABRIL 2026"	"MAYO 2026"
ICTXCYC	4,923	4,925	4,996	5,259	5,445	5,647	5,663	5,751
ICETEX	206	207	207	209	209	209	209	210
APLICATI	243	243	244	244	245	245	245	247
APOTEOSY	481	481	481	482	483	483	484	484
VIGIAPRD	175	178	188	200	211	217	230	236
LIFERAY LIFERAYPDB	8	8	8	23	23	24	30	32
LANDICTX	529	554	584	596	612	615	615	615
SGDEA	140	143	147	151	155	159	165	177
TOTAL==>	6,705.00	6,738.56	6,855.06	7,164.44	7,383.57	7,599.00	7,641.00	7,752.00
CRECIMIENTO		33.56	116.50	309.38	219.13	215.43	42.00	111.00

Tabla 9 Crecimiento de las bases de datos en los últimos 8 meses

Con las capacidades actuales se puede soportar la operación por lo menos un año más, si se mantienen las tasas de crecimiento.

4.2.1.2.3. Replicación Bases de Datos Oracle

Durante el mes de Mayo 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 ajustó la configuración de la retención de los ARCHIVE LOGS con el fin de soportar la solución de GCP (SERVINFORMACION); al final del mes esta configuración se ha mantenido estable y actualmente ya no esta afectando los mecanismos de replicación del servidor.

4.2.1.3. Sitio Web "Portal Icetex"

Durante el mes de Mayo 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 Mayo 2026.pdf](#)

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

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.

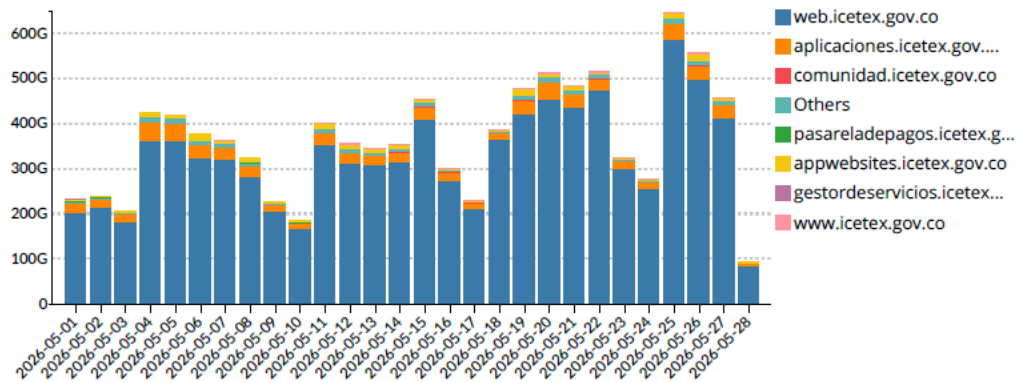


Ilustración 5 Tráfico General De Los Portales

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	254.854.563	86,13%
2	aplicaciones.icetex.gov.co	26.273.542	8,88%
3	www.icetex.gov.co	7.968.355	2,69%
4	pasareladepagos.icetex.gov.co	3.570.973	1,21%
5	gestordeservicios.icetex.gov.co	1.363.192	0,46%
6	crmweb.icetex.gov.co:777	513.686	0,17%
7	comunidad.icetex.gov.co	325.717	0,11%
8	appwebsites.icetex.gov.co	285.610	0,10%
9	webhook.icetex.gov.co	238.475	0,08%
10	www.icetex.gov.co:443	47.031	0,02%

Tabla 10 Top 10 Portales más utilizados

En cuanto a la disponibilidad del portal web de la entidad se presentan unos uptime de 99.761% como se evidencia en la siguiente gráfica:

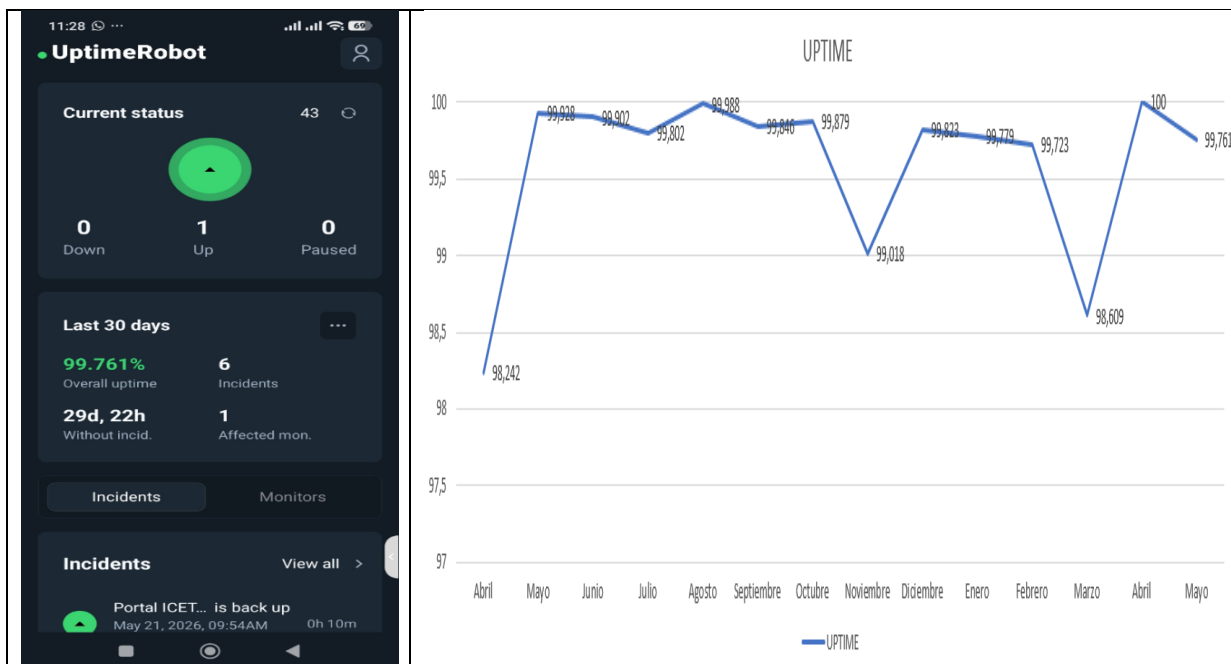


Ilustración 6 UPTIME: Portal WEB web.icetex.gov.co [99,761%]

Durante el mes de mayo se atendieron 7 requerimientos en la mesa de servicios, de los cuales 3 casos fueron escalados por error, dos requerimientos de redireccionamientos solicitados por Sandra Nocua de la OCM y un caso de ajuste de código Freemarker en la plantilla del contenido web.

Durante el mes de mayo no se atendieron incidentes en la mesa de servicios.

Durante el mes de mayo no se atendió gestión de cambios, se procedió con la anulación del caso de abril N° 27111, debido a que los especialistas de Claro siguen trabajando en la actividad de migración de las máquinas del portal ICETEX, en el momento que confirmen una fecha se procede con la creación de un nuevo caso de cambio y la exposición ante el comité.

Por último, los casos SD Claro aumentaron en un 33.33%, los casos SD corresponden a consumo momentáneo de file System en la partición raíz / de los nodos 1 y 2 del portal ICETEX y apoyo al especialista de balanceador para redireccionamiento de dos URLS, solicitud por parte de la OCM.

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

SERVICIO	LICENCIAMIENTO	
	FECHA DE INICIO	FECHA DE EXPIRACIÓN
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 11 Estado Licenciamiento Portal Web Icetex

4.2.1.3.1. Comportamiento del portal WEB

Se evidencia una alta concentración de usuarios desde Colombia, especialmente desde Bogotá y Barranquilla. El idioma predominante es español, seguido de inglés.

El portal mantiene una fuerte orientación hacia usuarios nacionales.

Existe tráfico internacional relevante desde Estados Unidos, lo que sugiere necesidad de mantener optimización global y monitoreo CDN. El acceso móvil supera el acceso desde computadores.

4.2.1.3.2. Recomendación:

- Priorizar estrategias Mobile First.
- Optimizar carga de banners, videos y componentes dinámicos para dispositivos Android y navegadores Chrome/Safari.

4.2.1.3.3. Alertas de consumo alto de CPU

Durante el mes de mayo se varias alertas de consumo de CPU atribuibles a:

- Publicación de becas.
- Fondos de administración.
- Créditos.
- Actualizaciones de contenido WEB.

Picos más relevantes de consumos de CPU

- 17 mayo: 58.70%.
- 19 mayo: 63.36%.
- 27 mayo: 67.85%.

4.2.1.3.4. Observaciones:

Existe correlación directa entre publicaciones masivas y aumento de CPU.

El nodo 1 presenta cargas superiores al nodo 2.

- Los procesos Java son el principal consumidor de recursos.

Aunque no hubo indisponibilidad, varios eventos alcanzaron consumos cercanos al 100% en ventanas prolongadas, se recomienda programar publicaciones masivas fuera de horarios pico. Adicional se retoman los reinicios controlados de los servicios del portal debido a la intermitencia presentada en la mañana del jueves 21 de mayo, en el análisis realizado por el Web master la causa del incidente podría estar asociada con alguno de los siguientes escenarios:

- Descargas masivas de archivos PDF, XLSX, DOCX o imágenes.
- Subida de información al portal.
- Procesamiento de contenidos web.
- Lectura o procesamiento de archivos ZIP.
- Export / Import de contenidos.
- Publicaciones de sitios.
- Contenidos web guardados como borrador.

Como medida preventiva, y con el fin de evitar indisponibilidad en el servicio del portal institucional, se reanuda el plan de reinicios controlados cada 20 días de los dos nodos de Liferay, así como de los servicios asociados de Elasticsearch, conformado por los tres nodos, y el NFS.

Mas detalles de la operación del portal se puede consultar en el [Informe Mensual InfoTIC Webmaster Mayo 2026.pdf](#)

4.2.2. Centro de Datos Alterno

4.2.2.1. Hosting Virtual (IaaS)

En el transcurso del mes de Mayo, 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 Mayo 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	May 31, 2026	47.75 MB	5 minutes
Grupo de protección: PG_INFOTIC_6 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0228_INFOTIC_REP	OK	1 of 1	May 31, 2026	31.29 MB	1 hour
INR0229_INFOTIC_REP	OK	1 of 1	May 31, 2026	72.82 MB	1 hour
Grupo de protección: PG_INFOTIC_1 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0233_INFOTIC_REP	OK	3 of 3	May 31, 2026	93.27 MB	1 hour
Grupo de protección: PG_INFOTIC_4 (3)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0238_INFOTIC_REP	OK	2 of 2	May 31, 2026	89.77 MB	1 hour
INR0239_INFOTIC_REP	OK	2 of 2	May 31, 2026	46 MB	1 hour
INR0243_INFOTIC_REP	OK	2 of 2	May 31, 2026	23.78 GB	1 hour
Grupo de protección: PG_INFOTIC_3 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0244_INFOTIC_REP	OK	1 of 1	May 31, 2026	78.59 MB	1 hour
INR0245_INFOTIC_REP	OK	1 of 1	May 31, 2026	5.02 MB	5 minutes
Grupo de protección: PG_INFOTIC_2 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0249_INFOTIC_REP	OK	2 of 2	May 31, 2026	6.72 MB	5 minutes

Ilustración 7 Reportes de replicación SRM a Sitio Alterno – Mayo 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	ictxisgesbd	Sisgestion	INR0228_INFOTIC_REP
3	INR0206	ictxisgesapp	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

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

No.	INR Replicación	Host name	Servicio	VirtualMachine MEGACENTER
9	INR0218	icetexbogliferayserver1	Portal productivo (liferay)	INR0243_INFOTIC_REP
10	INR0215	icetexboglxdarumasrv1	DARUMA	INR0244_INFOTIC_REP
11	INR0213	icetexboglxdarumasrv2	DARUMA	INR0245_INFOTIC_REP
12	INR0214	icetexboglxroad1	XROAD	INR0249_INFOTIC_REP

Tabla 12 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 OPENSIFT 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	375,640
INR0226	Mira	5,599
INR0233	icetexboglxorfeo1	2,978
INR0229	ictxsisgesapp	2,203
INR0244	icetexboglxdarumasrv1	2,007

Tabla 13 TOP 5 máquinas mayor tasa de transferencia

INR	HOSTNAME	GB
INR0245	icetexboglxdarumasrv2	0,188
INR0249	icetexboglxroad1	0,357
INR0238	icetexbogliferaynfs	1,142
INR0239	icetexbogelasticserver1	1,298
INR0228	ictxsisgesbd	1,425

Tabla 14 TOP 5 máquinas menor tasa de transferencia

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

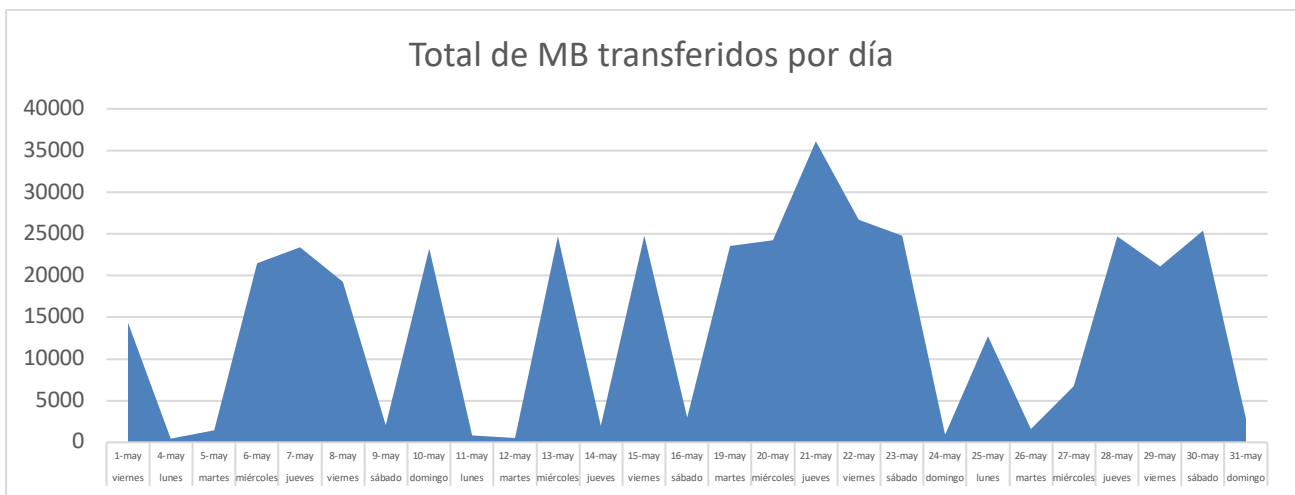


Ilustración 8 Fechas con mayor replicación

El comportamiento del tráfico de replicación durante el mes de Mayo 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 **95.62% del tráfico total** del mes que fue 375,640.00 MB (aprox. **376GB**)
- El tráfico total de replicación en Mayo fue de 392,835.82 MB (~392.84 GB).
- El fuerte incremento registrado entre marzo y abril (+71.11%) consolidó el retorno a un estado de alta demanda. Durante el mes de mayo, la tendencia al alza continuó de forma incremental, alcanzando un nuevo máximo de 392,835.82 MB (+9.10% respecto al mes anterior).
- Día de mayor tráfico: El jueves 21 de mayo, alcanzando un pico crítico de 36,108.62 MB (generados casi en su totalidad —35,350.00 MB— por el servidor INR0243).
- Día de menor tráfico: el día con menor tráfico neto registrado fue el domingo 4 de mayo con 480.48 MB, seguido muy de cerca por el martes 12 de mayo con 501,77 MB (atribuido al componente INR0249).

4.2.2.2. DataGuard Bases de Datos Megacenter

Durante el mes de Mayo 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 Mayo 2026.pdf](#)

```

10.1.18.120 - Conexión a Escritorio remoto
oracle@cxvodacontg011:~
[oracle@cxvodacontg011 ~]$ ps -fea |grep pmon
oracle 502 1 0 Feb28 ? 00:31:23 ora_pmon_DBPIVOT
oracle 16529 1 0 Apr21 ? 00:10:45 ora_pmon_SGDEAD
oracle 16690 1 0 Mar23 ? 00:19:38 ora_pmon_LIFERAYD
oracle 17217 1 0 May14 ? 00:05:43 ora_pmon_IXTCYCD
grid 21929 1 0 Feb28 ? 00:19:17 asm_pmon_ASM
oracle 24229 1 0 Apr09 ? 00:21:37 ora_pmon_APOTEOSP
oracle 24483 6607 0 09:25 pts/5 00:00:00 grep --color=auto pmon
oracle 27395 1 0 Feb28 ? 00:25:15 ora_pmon_LANDICTD
oracle 29573 1 0 Apr23 ? 00:11:21 ora_pmon_VIGIADTG
[oracle@cxvodacontg011 ~]$ . oraenv
ORACLE_SID = [IXTCYCD] ?
ORACLE_BASE environment variable is not being set since this
information is not available for the current user ID oracle.
You can set ORACLE_BASE manually if it is required.
Resetting ORACLE_BASE to its previous value or ORACLE_HOME
The Oracle base remains unchanged with value /oracle/app/oracle/product/product/11.2.0/dbhome_1
[oracle@cxvodacontg011 ~]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.4.0 Production on Sat May 30 09:25:20 2026
Copyright (c) 1982, 2013, Oracle. All rights reserved.

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production
With the Partitioning, Automatic Storage Management, OLAP, Data Mining
and Real Application Testing options

SQL> sta faply

  Thread Last Sequence Received Last Sequence Applied TIME RECEIVED TIME APPLIED
  -----
1 299238 247379 299238 30/05/2026 09:22 30/05/2026 09:22
2 247379 247379 247379 30/05/2026 09:22 30/05/2026 09:22

SQL> sta uaply

  Thread Last Sequence Received Last Sequence Applied Difference
  -----
1 299238 299238 299238 0
2 247379 247379 247379 0

SQL>

```

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 alerno en Medellín, las cuales estuvieron disponibles todo el mes de Mayo 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 15 Disponibilidad de Servicios de Housing – Data Center Alterno

4.2.3. Conclusiones

Actualmente, la gestión de capacidad opera de forma reactiva en lugar de preventiva. Se requiere que el HS formalice políticas de capacity planning y ejecute la depuración de datos históricos.

4.3. Seguridad informática

Para este mes, los casos gestionados por el área de Seguridad corresponde a un (1) caso y siete (7) tareas.



Ilustración 10 - Casos Operador de Seguridad

Se llevaron a cabo diversas actividades relacionadas con la administración y gestión de la seguridad perimetral de la entidad.

- Se realizó la validación y análisis de los diferentes bloqueos generados por la aplicación Sophos.
- Se realizó un análisis detallado a los reportes enviados por el SOC.

- El grupo de Seguridad participó en diferentes sesiones técnicas de apoyo a la resolución de Incidentes o requerimientos y atendió los diferentes requerimientos del Grupo de Seguridad del Icetex.
- Los eventos relacionados con intentos de acceso no autorizado fueron gestionados y mitigados oportunamente.
- El monitoreo continuo realizado por el SOC permitió una detección temprana y una respuesta ágil, reduciendo el riesgo de afectación a los servicios institucionales.
- La validación realizada sobre la herramienta de seguridad Sophos permitió identificar y gestionar adecuadamente los bloqueos presentados, evidenciando un monitoreo activo y un control eficiente sobre las políticas de seguridad. Esto contribuye a minimizar falsos positivos y garantizar que las operaciones no se vean afectadas por restricciones innecesarias, manteniendo al mismo tiempo la protección del entorno.
- Las gestiones adelantadas para restablecer la conectividad y permitir la extracción de respaldos mediante Commvault reflejan una adecuada coordinación técnica y capacidad de respuesta ante incidentes operativos. Este proceso asegura la disponibilidad y resguardo de la información crítica, fortaleciendo las estrategias de respaldo y recuperación de datos.
- La documentación generada y las sesiones realizadas para la entrega de los equipos de seguridad al Icetex evidencian un proceso organizado de transferencia de conocimiento y activos.

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.

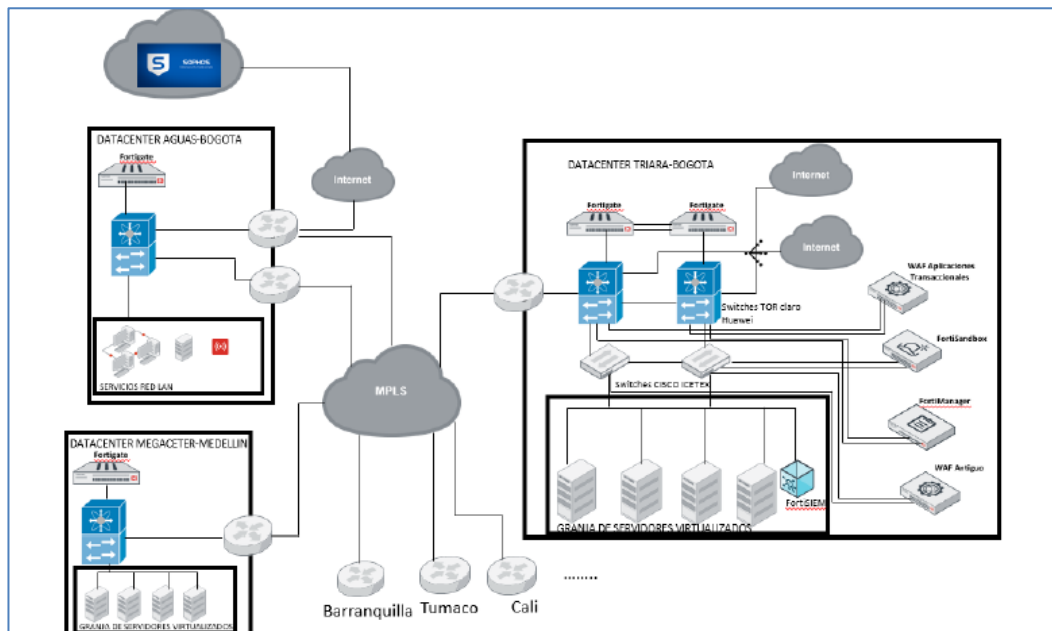


Ilustración 11 Diagrama de la Arquitectura de Seguridad

En la ilustración 12, 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.

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

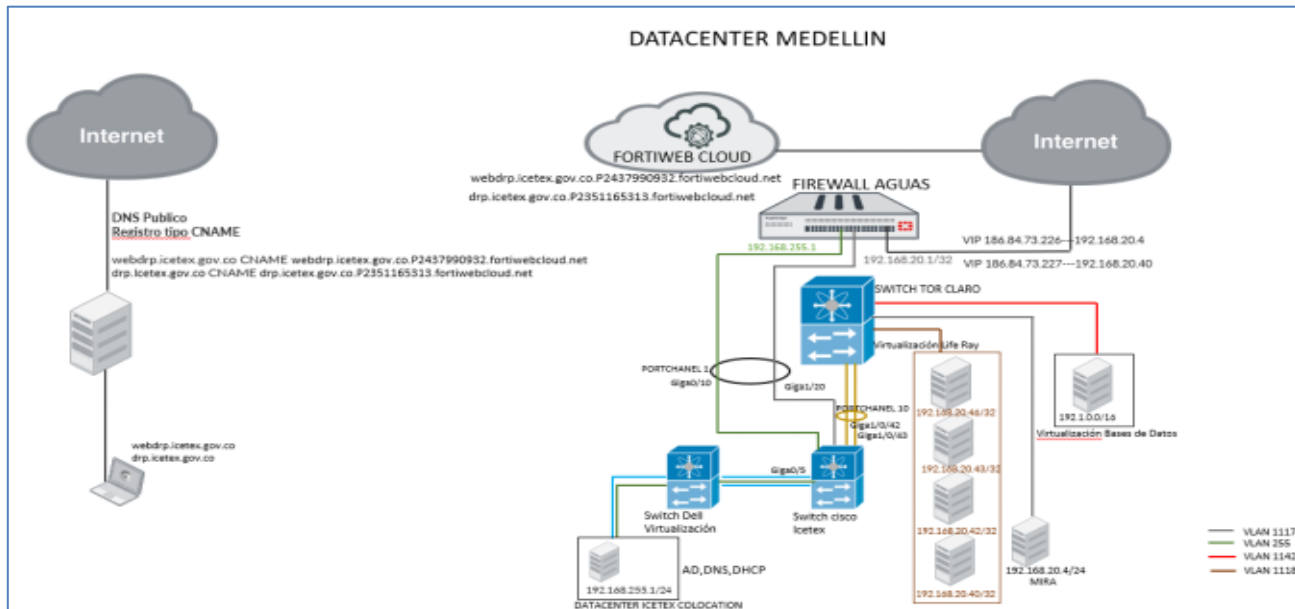


Ilustración 12 Topología de WAF Cloud usado en portales de Medellín

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.

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

- Aplicación de QOs, para la aplicación Teams, desde la red de Tecnología en la sede Aguas.
- Afinamiento de los perfiles de navegación de la entidad.
- Afinamiento para el uso de la aplicación AnyDesk, para el personal técnico de Comware.

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.

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 16 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 17 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:

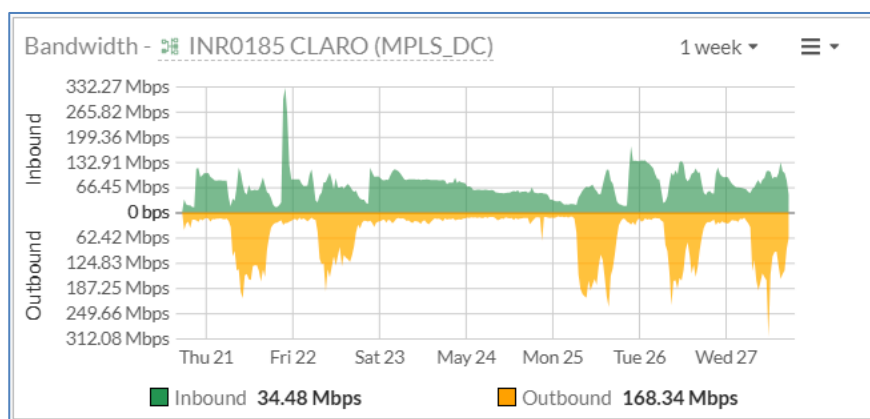


Ilustración 13 Consumo canal MPLS - promedio 168,34 Mbps [INR0185 CLARO(MPLS_DC)]

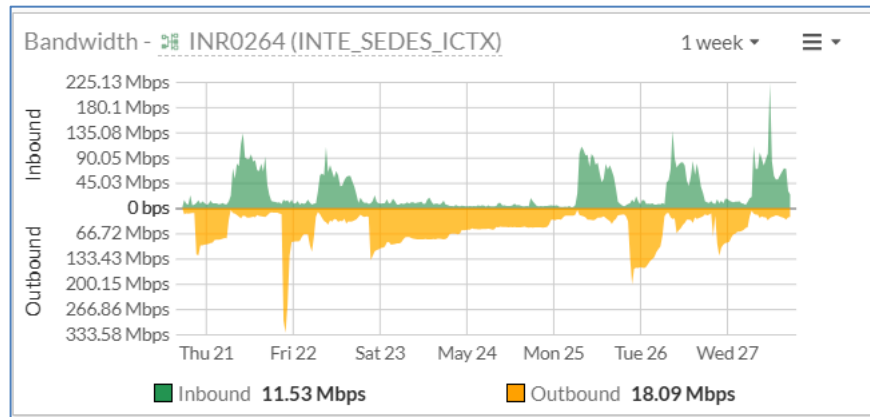


Ilustración 14 Consumo canal Internet Sedes - Prom 18 Mbps WAN-SEDES-ICETEX [INR0264 (INTE_SEDES_ICTX)]

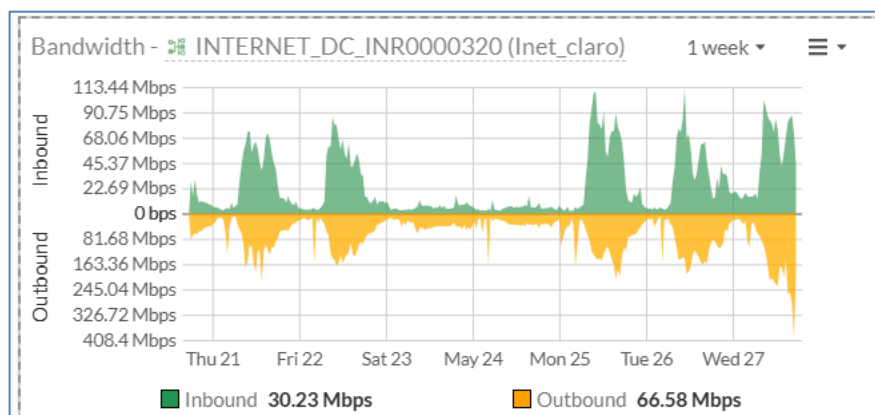


Ilustración 15 Consumo Canal INTERNET DATACENTER -Prom 66,58 Mbps [INTERNET_DC_INR0000320 (Inet_claro)]

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	3
WEB WF-Sede_Ibague_YT	27022025/InfoTIC/Tarea Aranda 517214 (17458) Se solicita el acceso a youtube	2
WEB WF-Tesorería	Perfil con restricciones específicas por auditoría.	7
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 16 Filtrado – WEB – (FortiGate – Triara)

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

Name	Read Only	Comments	Ref.
SSL certificate-inspection	🔒	Read-only SSL handshake inspection profile.	610
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.	436
SSL Prueba certificate-inspection		Read-only SSL handshake inspection profile.	27

Ilustración 17 Inspección – SSL – (FortiGate – Triara)

Name	Comments	Ref.
AV AV-FSB	HTTP,SMTP FULL FSB	105
AV AV-HTTP	HTTP con FSB	34
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 18 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:

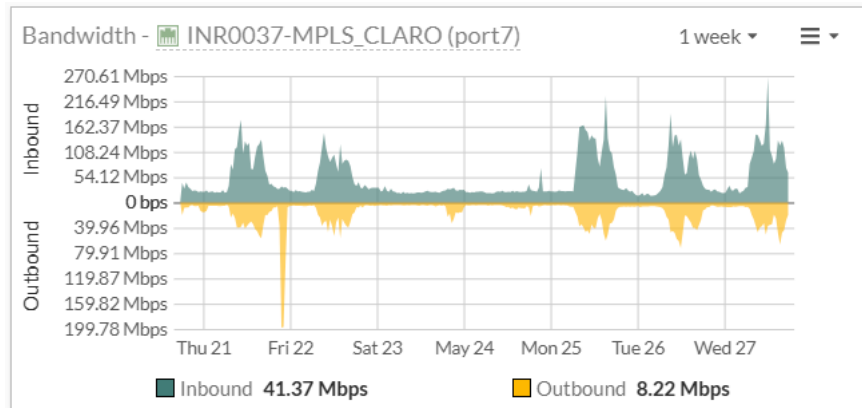


Ilustración 19 Consumo Canal MPLS Aguas - promedio 41,37 Mbps (Port7)

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	2
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 20 Filtrado-Web-(FortiGate-Aguas)

Name	Read Only	Comments	Ref.
SSL certificate-inspection	🔒	Read-only SSL handshake inspection profile.	451
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.	344

Ilustración 21 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 22 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 23, que la interfaz de la MPLS del Data Center de Medellín no presenta tráfico debido a que este se tiene como Data Center Alterno.

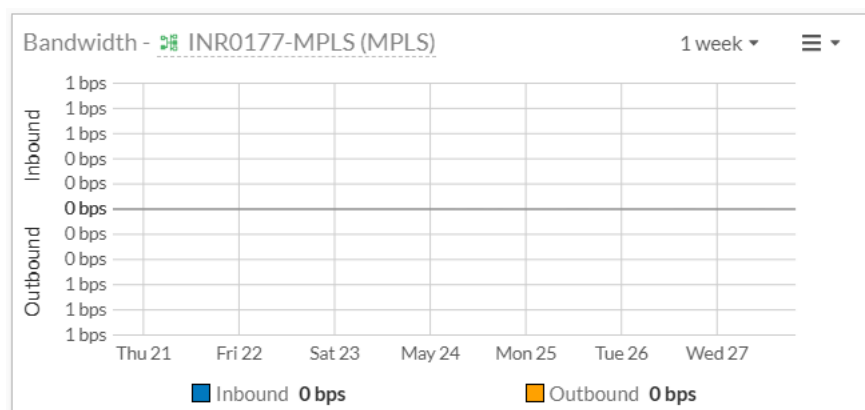


Ilustración 23 Consumo Canal MPLS Medellín

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 Ictetex	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)	192.168.9.1.10	No	Si	1/06/2026	Triara	N/A	N/A	N/A

Tabla 18 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.

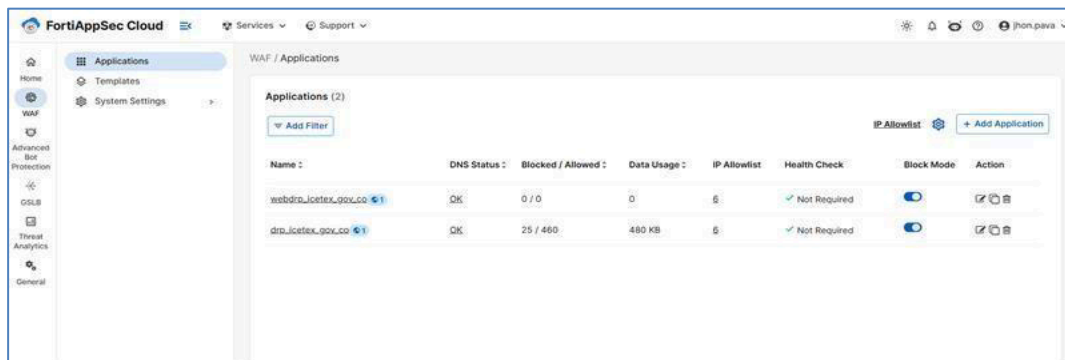


Ilustración 24 Tráfico General de los portales

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 Ictetex	Licenciamiento	Fin Licenciamiento	DC	End Of Order	Last Service Extension	End of support
FortiSandBox 1000D	10.0.0.24.9	Si	No	1/06/2023	Triara	2/04/2019	2/04/2023	2/04/2024

Tabla 19 Configuración FortiSandBox 1000D

4.3.4.8. FortiSIEM

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

General Usage Nodes			Upload License
Serial Number:	FSMP000000001340		
Hardware ID:	4212F192-BEF3-61AB-F30D-4EAF9DE2E3F6		
License Hardware ID:	4212F192-BEF3-61AB-F30D-4EAF9DE2E3F6		
License Type:	Enterprise		
FIPS Mode:	Disabled		
Automation Service:	Disabled		
Attribute	Value	Expiry	
Devices	200	Perpetual	
Total EPS	2000	Perpetual	
Agents	100	Perpetual	
UEBA	75	Perpetual	
IOC Service	Expired	Apr 19, 2026	
Maintenance and Support	Expired	Apr 19, 2026	
High Availability Service	N/A	N/A	
Automation Service	N/A	N/A	

Ilustración 25 licenciamiento FortiSIEM

A continuación, se presenta el desempeño por procesos:

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

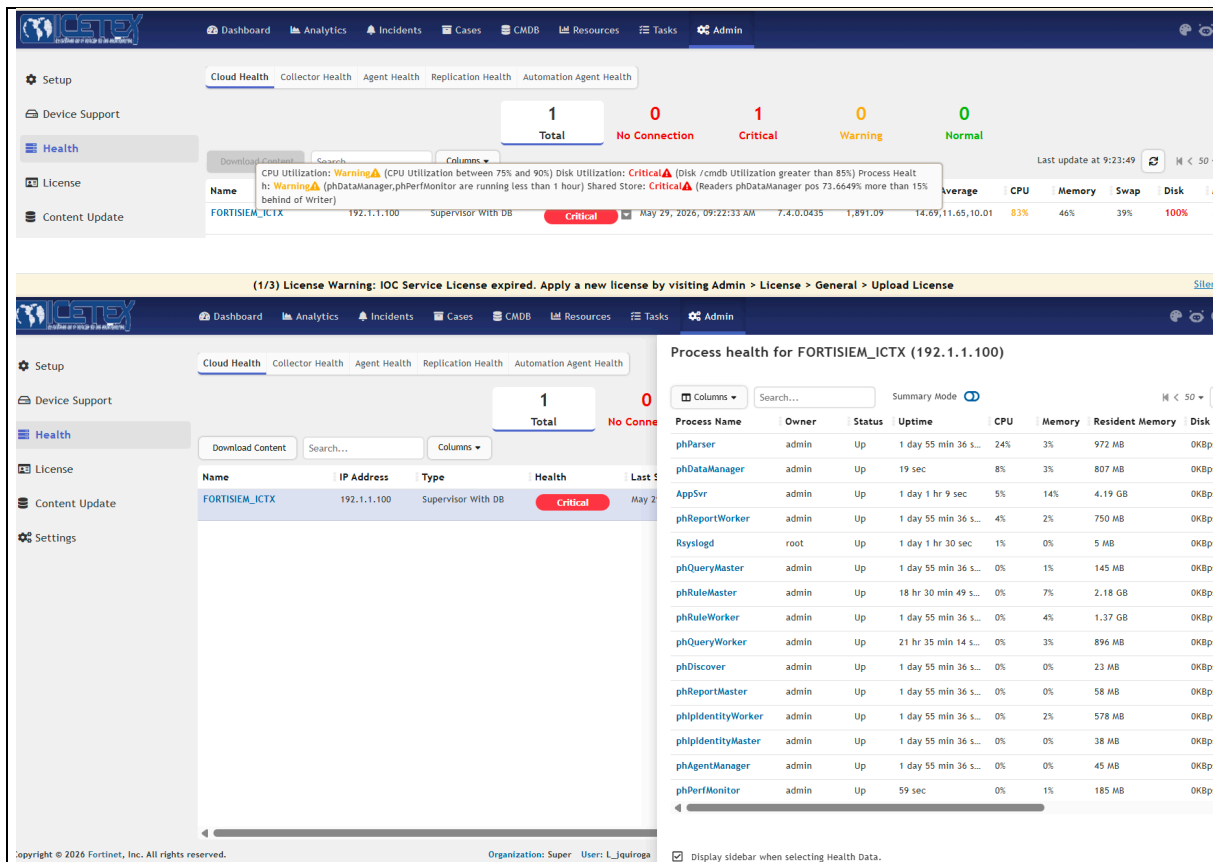


Ilustración 26 FortiSIEM Performance por procesos

El análisis del estado actual del FortiSIEM evidencia alertas críticas relacionadas con la saturación de memoria y almacenamiento en disco. Con el objetivo de mitigar riesgos y garantizar la continuidad operativa, se reitera la necesidad de realizar una ampliación de recursos del sistema.

4.3.4.9. Sophos EndPoint

En la ilustración 27, se observa un resumen del estado de Seguridad del Endpoint donde actualmente Al Revisar políticas asignadas En Sophos Central:

Endpoint Protection → Políticas

Algunas características de la herramienta no están aplicadas en las políticas asignadas en los dispositivos en los módulos de:

Threat Protection

Web Control

Peripheral Control

Device Encryption

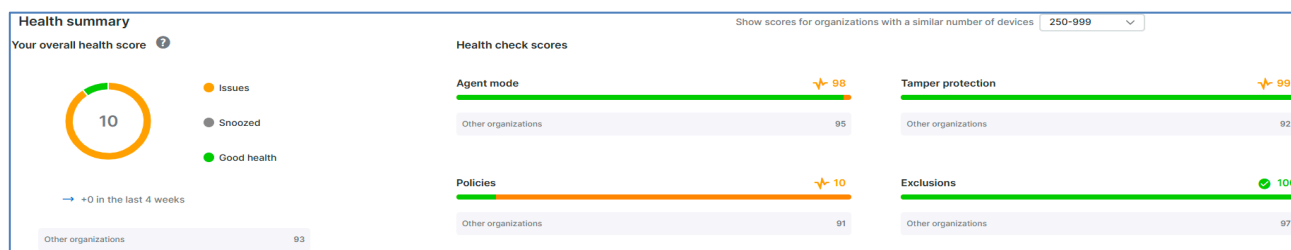


Ilustración 27 Estado Seguridad Sophos

En la sección 6.6.1 del informe de seguridad [Informe Mensual InfoTIC Seguridad Mayo 2026.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.	Crítica	Informes Mensuales	N/A	N/A

Recomendación	Estado	Criticidad	Fuente	Asunto	Personal de ICETEX a quien se notificó
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 Ictex	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
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 Ictex	Líder infraestructura / Especialista Desarrollo / Especialista de seguridad / Especialista de seguridad / Grupo Coordinación de Infraestructura Tecnológica / Profesional de tecnología

Tabla 20 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 anomalías 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

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

- 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 InfoTIC Seguridad Mayo 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)	Mayo	Abril	Marzo	Febrero	Enero
IOC – Malware DOMINIOS	6.047	6.047	6.047	6.047	6.047
IOC – Malware IPs	11.167	11.167	11.167	11.119	11.119
IOC – Malware HASH	1.627	1.627	1.627	1.627	1.627
IOC – Malware URL	4.564	4.564	4.564	4.564	4.564

Tabla 21 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 mayo 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:

Severity	Cantidad de Alertas
Medium	58,297
High	1,305
Low	822

Ilustración 28 Total de alertas de seguridad

Durante el período evaluado de 60.424 alertas de seguridad identificadas, se presentaron con criticidad ALTA un total de 1,305 equivalentes al 2% 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 6 meses, se presenta a continuación:

Alertas Seguridad	Mayo	Abril	Marzo	Febrero	Enero	Diciembre
High	1.305	1.279	1.565	2.213	1.674	1.198
Medium	58.297	150.439	92.076	153.406	137.305	50.794
Low	822	949	756	1.356	1.775	856

Tabla 22 comparativo Alertas de Seguridad

Durante el período evaluado las alertas de seguridad con criticidad ALTA, aumento con relación a periodos anteriores un 2% y las alertas medias mayo se observó una reducción del 61% en las alertas de severidad Media en comparación con abril . En el documento [Informe Mensual SOC-TH ICETEX mayo 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 5 se presenta a continuación:

Chart	Criticidad de las alertas	Event Name	Criticidad de las alertas	Attack Tactic	Cantidad de Alertas
☒	High	Concurrent Failed Authentications To Same Account From Multiple Countries	9	Credential Access	892
☒	High	Critical large Outbound Transfer To Outside My Country ICETEX - WX N3	9		138
☒	High	Successful VPN Logon From Outside My Country WXN2	9	Credential Access	71
☒	High	Brute Force Host Login Success CUSTOM 8/10/2021	9		46
☒	High	Repeated Multiple Logon Failures: Server	9	Credential Access	29

Ilustración 29 Top 5 de Alertas de Seguridad Altas

Chart	Criticidad de las alertas	Event Name	Criticidad de las alertas	Attack Tactic	Cantidad de Alertas
☒	Medium	Windows successful file access	5	Impact,Collection	47,739
☒	Medium	Group Policy Object Modified	7	Privilege Escalation,Defense Evasion	2,801
☒	Medium	Windows: AD User Enumeration	5	Discovery	2,141
☒	Medium	Large Inbound Transfer From Outside My Country	8	Command And Control	1,144
☒	Medium	Alerta Domain Controller Hora Oficina	8		1,058

Ilustración 30 Top 5 de Alertas de Seguridad Medias

Durante el período evaluado se presentaron 58.297 alertas de seguridad con criticidad MEDIA.

4.3.6.2.2. Categoría Disponibilidad

A continuación, se relacionan las alertas presentadas en el periodo analizado, definiendo el top de los que han tenido mayor concurrencia. solo se analizan las alertas relacionadas con la operación y correlación de eventos.

Severity	Cantidad de alertas
Medium	7,242
Low	153
High	115

Ilustración 31 Total de alertas de disponibilidad

Durante el período evaluado se presentaron 115 alertas de disponibilidad con criticidad ALTA, a continuación, 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 presentaron:

Chart	Criticidad	Event Name	Attack Tactic	Criticidad	Cantidad de alertas
☒	High	FortiSIEM EventDB event store failed		10	16
☒	High	Excessive Destination Windows DC Replication Failure		9	14
☒	High	Excessive Source Windows DC Replication Failure		9	14
☒	High	Network Device Hardware Critical		9	13
☒	High	Network Device Down: no ping response - WX N3	Impact	10	12

Ilustración 32 Top 5 de Alertas de Disponibilidad Altas

Alerta: FortiSIEM EventDB event store failed

Esta alerta se genera cuando Fortinet FortiSIEM tuvo un fallo al almacenar eventos en su base de datos de eventos (EventDB). Esto puede deberse a problemas de disco, falta de espacio, corrupción de base de datos, alta carga del sistema o fallos de conectividad entre componentes. La consecuencia principal es la posible pérdida o retraso en el registro de logs y eventos de seguridad, afectando el monitoreo y la correlación de incidentes.

Alerta: Excessive Destination Windows DC Replication Failure

Esta alerta señala un número excesivo de fallos en la replicación de un Controlador de Dominio (DC) de destino en entornos Microsoft Active Directory. Significa que el servidor no está recibiendo correctamente actualizaciones desde otros controladores de dominio, lo que puede generar inconsistencias en usuarios, políticas o autenticaciones. Las causas comunes incluyen problemas de red, DNS, servicios detenidos o errores de autenticación entre DCs.

Alerta: Excessive Destination Windows DC Replication Failure

Esta alerta señala un número excesivo de fallos en la replicación de un Controlador de Dominio (DC) de destino en entornos Microsoft Active Directory. Significa que el servidor no está recibiendo correctamente actualizaciones desde otros controladores de dominio, lo que puede generar inconsistencias en usuarios, políticas o autenticaciones. Las causas comunes incluyen problemas de red, DNS, servicios detenidos o errores de autenticación entre DCs.

Alerta: Network Device Hardware Critical

Esta alerta indica que un dispositivo de red ha reportado una condición crítica de hardware (como fallas en CPU, memoria, temperatura, ventiladores o fuentes de poder), lo cual puede comprometer seriamente su funcionamiento y la disponibilidad de la red; se recomienda verificar el estado del equipo a través de sus interfaces de gestión, validar condiciones físicas (energía, ventilación, ambiente), y si es necesario, aplicar medidas como reducción de carga, failover a equipos redundantes o reemplazo de hardware; además, es clave escalar al proveedor o soporte técnico, asegurar respaldos de configuración y mantener monitoreo continuo para prevenir una caída total del servicio.

4.3.6.2.3. Amenazas de Ciberseguridad

- Top Ataques IPS

Se representa el Top de los ataques IPS permitidos y denegados detectados por los dispositivos de ciberseguridad perimetral.

Se recomienda el bloqueo de los ataques de severidad alta detectados por el IPS y verificar los eventos o alertas de severidad media.

3.1.1 FortiGate: Top IPS Ataques Permitidos - WX						
Reporting Device	Attack Name	Signature Id	Severity	Firewall Action	COUNT(Matched Events)	
57 DC_FG_MST_ICETEX	DNS PTR Records Scan	51391	Low	detected	1,389	
57 DC_FG_MST_ICETEX	SSL Anonymous Ciphers Negotiation	43544	Low	detected	40	

Ilustración 33 Top de Ataques Permitidos

3.1.1 FortiGate: Top IPS Ataques Denegados - WX						
Reporting Device	Attack Name	Signature Id	Severity	Firewall Action	COUNT(Matched Events)	
57 DC_FG_MST_ICETEX	Apache Log4j Error Log Remote Code Execution	51006	Medium	dropped	3,010	
57 DC_FG_MST_ICETEX	Nmap Script Scanner	45360	Medium	dropped	1,124	
57 DC_FG_MST_ICETEX	Kubernetes Ingress NGINX Controller Remote Code Execution	57679	Medium	dropped	372	
57 DC_FG_MST_ICETEX	ZGrab Scanner	48805	Medium	dropped	272	
57 DC_FG_MST_ICETEX	ALFA TEaM Web Shell	53229	Medium	dropped	270	
57 DC_FG_MST_ICETEX	MS IIS ShortName Vulnerability Scanner	47145	Medium	dropped	236	
DCAGUAS_FG_MST_ICETEX	Nmap Script Scanner	45360	Medium	dropped	111	
57 DC_FG_MST_ICETEX	Telerik Web UI RadAsyncUpload Handling Arbitrary File Upload	48789	Medium	dropped	109	
57 DC_FG_MST_ICETEX	Masscan Scanner	44778	Medium	dropped	76	
57 DC_FG_MST_ICETEX	Censys.io Scanner	50899	Medium	dropped	73	
57 DC_FG_MST_ICETEX	Java Debug Wire Protocol Insecure Configuration	44187	Medium	dropped	70	
57 DC_FG_MST_ICETEX	Apache HTTP Server cgi-bin Path Traversal	50825	Medium	dropped	64	
57 DC_FG_MST_ICETEX	Vite server fs.deny.raw.Arbitrary File Read	57942	Medium	dropped	31	
DCAGUAS_FG_MST_ICETEX	Apache Log4j Error Log Remote Code Execution	51006	Medium	dropped	30	
57 DC_FG_MST_ICETEX	Mirai Botnet	43191	Medium	dropped	27	

Ilustración 34 Top de Ataques Denegados

- Top Ataques WEB

No se identifican ataques permitidos ni eventos IPS denegados durante el periodo evaluado, lo que evidencia un entorno sin actividad maliciosa detectada a nivel perimetral

- Top Perímetro

A continuación se presentan el TOP de los eventos o tráfico de red organizado por los puertos TCP/UDP que más recibieron o enviaron bytes hacia Internet.

IP Protocol	Destination TCP/UDP Port	COUNT(Matched Events)	SUM(Sent Bytes64)	SUM(Received Bytes64)	SUM(Total Bytes64)
6 (TCP)	443 (HTTPS)	16,302,379	4.06 TB	13.44 TB	17.5 TB
17 (UDP)	443	478,335	56.41 GB	421.25 GB	477.66 GB
17 (UDP)	53 (DOMAIN)	343,863	48.25 GB	84.33 GB	132.58 GB
6 (TCP)	80 (HTTP)	165,771	7 GB	222.28 GB	229.29 GB
6 (TCP)	5228	23,650	686.12 MB	879.36 MB	1.52 GB
6 (TCP)	5222	20,620	2.11 GB	4.79 GB	6.91 GB
6 (TCP)	440 (SGCP)	19,772	77.35 MB	499.28 MB	576.63 MB
6 (TCP)	777	18,061	29.7 MB	16.85 MB	46.55 MB
6 (TCP)	49667	13,165	2.74 GB	3.93 GB	6.68 GB
6 (TCP)	993 (IMAPS)	12,160	19.59 MB	79.79 MB	99.38 MB

Ilustración 35 Principales Puertos Entrantes por Conexiones y Bytes V3 (Tráfico Permitido)

IP Protocol	Destination TCP/UDP Port	COUNT(Matched Events)	SUM(Sent Bytes64)	SUM(Received Bytes64)	SUM(Total Bytes64)
6 (TCP)	443 (HTTPS)	106,193,828	40.6 TB	39.49 TB	80.09 TB
17 (UDP)	443	20,426,288	12.77 TB	4.2 TB	16.97 TB
17 (UDP)	53 (DOMAIN)	17,227,149	7.52 GB	14.71 GB	22.24 GB
6 (TCP)	80 (HTTP)	6,175,802	135.94 GB	1.59 TB	1.72 TB
17 (UDP)	3478	4,169,218	21.3 TB	11.05 TB	32.36 TB
6 (TCP)	5228	3,556,541	310.44 GB	405.83 GB	716.28 GB
6 (TCP)	587 (SUBMISSION)	1,258,959	4.64 GB	2.07 GB	6.71 GB
17 (UDP)	4000 (ICQ)	1,073,485	25.41 GB	56.43 GB	81.85 GB
17 (UDP)	123 (NTP)	842,173	35.69 GB	35.54 GB	71.24 GB
6 (TCP)	8810	816,570	153.04 GB	146.24 GB	299.28 GB

Ilustración 36 Principales Puertos Salientes por Conexiones y Bytes V3 (Tráfico Permitido)

4.3.6.3. Threat Hunting

Se lleva a cabo el proceso de "Threat Hunting" de manera proactiva mediante la realización de boletines de ciber amenazas y la utilización de la plataforma MISP (Malware Information Sharing Platform) del First (Forum of Incident Response Team). En este procedimiento, se realiza una búsqueda activa de Indicadores de Compromiso (IoC) asociados a las principales amenazas que tienen relevancia a nivel mundial. Estos IoC son posteriormente cargados en el Sistema de Gestión de Eventos e Información de Seguridad (SIEM) para llevar a cabo la correlación con los registros de actividad (logs) de la entidad ICETEX.

El objetivo fundamental es detectar y mitigar posibles amenazas antes de que se materialice un incidente de seguridad. A continuación, se presentan los resultados obtenidos durante el periodo de monitoreo en relación al tráfico detectado proveniente de la entidad en interacción con estos actores maliciosos:

Tableros de control de amenazas con tráfico desde o hacia IoC maliciosos.

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

Los siguientes indicadores de compromiso - IoC fueron recopilados por intercambio de información con algunas instituciones del Estado Colombiano, inteligencia de amenazas en plataformas públicas o privadas, como el FIRST, CISA, CSIRT'S y caza de amenazas en plataformas de ciberseguridad.

La información de los estos tableros de control también es monitoreada a través de las siguientes reglas o casos de uso que generan alertas en el FortiSIEM y son enviadas al ICETEX por medio reportes.

Active	Severity	Name	Description
☒	9 - HIGH	Trafico Permitido desde IP IoC Maliciosas - WX Nivel3	Detección de Trafico permitido desde direcciones IP relacionadas en Indicadores de Compromiso - IoC de Malware recopilados por WX Nivel3. Lo anterior indica intentos de conexión a equipos infectados desde servidores de comando y control (C&C) o indicios de exploración para futuras amenazas.
☒	9 - HIGH	Trafico permitido hacia IoC Ransomware MarioLocker - WX N3	Detección de comportamiento sospechoso referente al Ransomware Mario Locker de acuerdo a los IoC recopilados por WX Nivel 3
☒	9 - HIGH	Trafico Permitido o Denegado Hacia IoC Maliciosas - WX Nivel3	Detección de Trafico permitido o denegado hacia Dominios, IP, HASH y URL, relacionadas en Indicadores de Compromiso - IoC de Malware recopilados por WX Nivel3. Lo anterior indica que el equipo con IP Origen probablemente esta infectado por malware y esta intentando conexiones a servidores de comando y control (C&C) independientemente si fue negado o permitido el trafico. 09/01/24 Se excluye IoC de Ransomware MarioLocker.

Ilustración 37 Reportes Threat Hunting

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 22 posibles amenazas de las 37,6k que fueron encontradas y analizadas automáticamente por la plataforma de monitoreo. A estas 22 posibles amenazas se les realizó una revisión y análisis interno, de sus características, datos e información.

Adicionalmente, durante el periodo se registró un total de 37 casos resueltos.

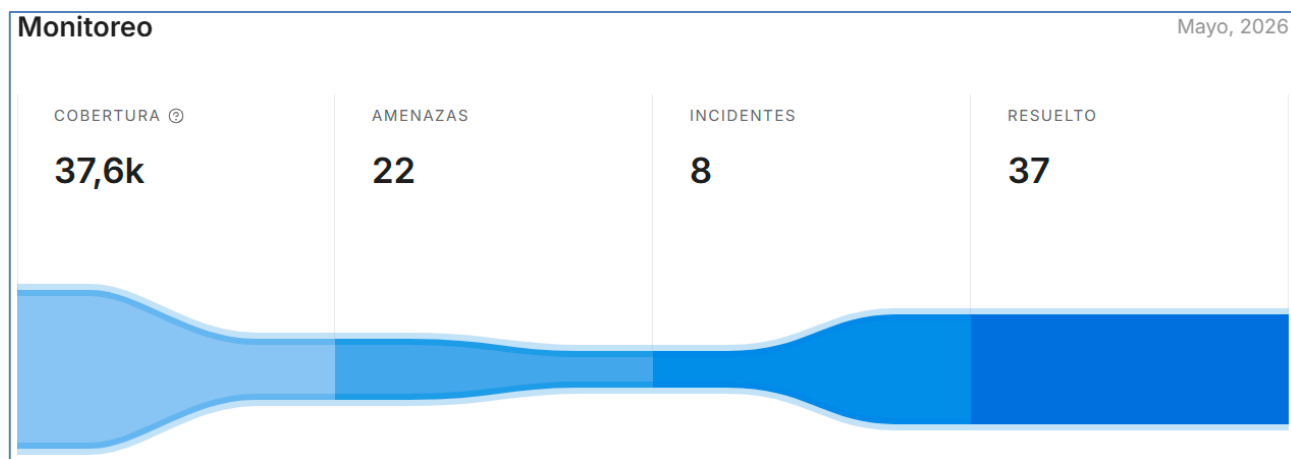


Ilustración 38 Incidentes por Tipo de Amenaza

Durante el periodo evaluado se detectó 08 incidentes de los cuales, 05 están relacionados con Actividad sospechosa en sitio web, 01 con Aplicación móvil falsa, 01 con Phishing y 01 con Producto falso o venta irregular.

En resumen se realizó el análisis a 26 casos o tickets generados por la Plataforma, a continuación, se detalla el total de tickets analizados y el estado actual de ellos:

CLASIFICACIÓN DE LA ALERTA	ESTADO RESUELTO	ESTADO NO RESUELTO	ESTADO EN TRATAMIENTO	ESTADO DESCARTADA	ESTADO EN CUARENTENA	TOTAL GENERAL
FRAUDES DIGITALES	1	0	1	1	0	3
FUGA DE DATOS	0	0	0	10	0	10
DEEP & DARK WEB	5	0	0	0	0	5
CTI	0	0	7	0	0	7
PIRATERÍA ONLINE	0	0	0	1	0	1
TOTAL GENERAL	6	0	8	12	0	26

Tabla 23 Total de casos gestionados

Para revisar mas detalladamente remitirse al reporte [Informe Mensual MARCA-OSINT ICETEX Mayo 2026.pdf](#)

4.3.6.4.1. Recomendaciones Generales

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

- Se recomienda validar si el perfil en mención está autorizado por la entidad, en caso de no ser así, se recomienda que, por parte del área legal del ICETEX, denuncien directamente en la red social el perfil para que sea eliminado.
- Se recomienda a los usuarios estar atentos y reportar cualquier cuenta en redes sociales que pueda estar infringiendo las normas de la marca. Al incentivar su participación, se fortalece la capacidad de detectar de manera temprana y responder rápidamente a posibles casos de suplantación de identidad.
- Como medida preventiva, se sugiere bloquear las URLs de las cuentas sospechosas en las herramientas de control y en el firewall de la organización. Esta acción ayudará a prevenir el acceso a dichas cuentas, reduciendo el riesgo de recibir mensajes spam o quejas de los usuarios relacionadas con cuentas fraudulentas.
- Es esencial realizar campañas de concienciación tanto internas como externas para informar al personal y al público en general sobre la importancia de proteger la marca de la institución. Esto incluye proporcionar pautas claras sobre el uso adecuado de la marca en redes sociales y otros canales de comunicación oficiales.

- Una vez realizadas las acciones correspondientes, se solicita responder el correo 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.

Con respecto a los casos de Exposición de infraestructura - recordar las medidas a considerar:

- Validar que todos los servicios expuestos sean estrictamente necesarios para la operación.
- Restringir el acceso a los servicios mediante controles de red, como listas blancas de IP o acceso a través de VPN.
- Implementar configuraciones seguras en los servicios web, incluyendo el uso de protocolos cifrados y actualizaciones constantes.
- Realizar pruebas de seguridad periódicas para identificar vulnerabilidades en aplicaciones expuestas.
- Verificar el uso del puerto 23 (Telnet) y deshabilitarlo en caso de no ser requerido, reemplazándolo por protocolos seguros como SSH.
- Revisar y fortalecer las reglas de firewall para minimizar la exposición innecesaria de servicios.
- Se recomienda mantener un proceso de monitoreo continuo que permita detectar periódicamente nuevas exposiciones o cambios en la superficie de ataque.

- Se recomienda realizar auditorías periódicas de configuración para revisar puertos, servicios y políticas de seguridad en el perímetro de la infraestructura.

Continuar fortaleciendo la gestión y seguimiento de los casos reportados, teniendo en cuenta que en los últimos meses se ha evidenciado una reducción significativa en los incidentes pendientes de tratamiento.

Mantener el monitoreo continuo sobre perfiles falsos, dominios similares y actividades sospechosas en sitios web, con el fin de prevenir posibles campañas de suplantación o fraude dirigidas a usuarios de la entidad.

Validar periódicamente las acciones implementadas sobre los casos en tratamiento, con el objetivo de confirmar la efectividad de las medidas aplicadas y evitar reincidencias.

Fortalecer la articulación entre las áreas técnicas, de seguridad y comunicaciones para agilizar procesos de mitigación, bloqueo y cierre de incidentes reportados por la plataforma.

4.3.7. Análisis de Vulnerabilidades ICETEX

Cronograma de actividades ejecutadas en el mes de Mayo:

 INFOTIC SOLUCIONES INTELIGENTES		 ICETEX Investigación en el servicio al cliente		Cronograma detallado ejecución de pruebas de análisis de vulnerabilidades			Versión: 1
Fecha de Inicio del Proyecto				viernes, 01/05/2026			
Actividad	Responsable	Cumplimiento	Fecha de inicio	Fecha Final	Días Hábiles	Franja horaria	
Ejecución 1 - 100 %	Wexler	100%	01/05/2026	11/11/2026	195		
Mes 1 - Mayo 2026	Wexler	100%	01/05/2026	31/05/2026	31	8:00 AM - 12:00M	
Pruebas de conectividad a los objetivos - Fase de reconocimiento.	Wexler	100%	01/05/2026	07/05/2026	7	8:00 AM - 12:00M	
Identificación de dispositivos- Fase enumeración	Wexler	100%	07/05/2026	13/05/2026	7	2:00 PM - 6:00 PM	
Identificación de vulnerabilidades - Fase de escaneo	Wexler	100%	14/05/2026	27/05/2026	14	8:00 AM - 12:00M	
Elaboración de informes - Fase de documentación	Wexler	100%	27/05/2026	31/05/2026	5	2:00 PM - 6:00 PM	
Socialización de los resultados	Wexler	100%	31/05/2026	03/06/2026	4	2:00 PM - 6:00 PM	

Ilustración 39 Cronograma detallado ejecución de pruebas análisis de vulnerabilidades

A continuación, se presenta el consolidado general de vulnerabilidades identificadas durante la ejecución del ejercicio de Ethical Hacking, clasificadas por nivel de severidad y analizadas en función de su impacto, recurrencia y criticidad técnica.

4.3.7.1. Consolidado General de Vulnerabilidades

Se agruparon las vulnerabilidades según su severidad (CRÍTICA, ALTA, MEDIA y BAJA), conforme al sistema de clasificación CVSS v3.1. Esta distribución permite una visualización rápida de la exposición al riesgo:

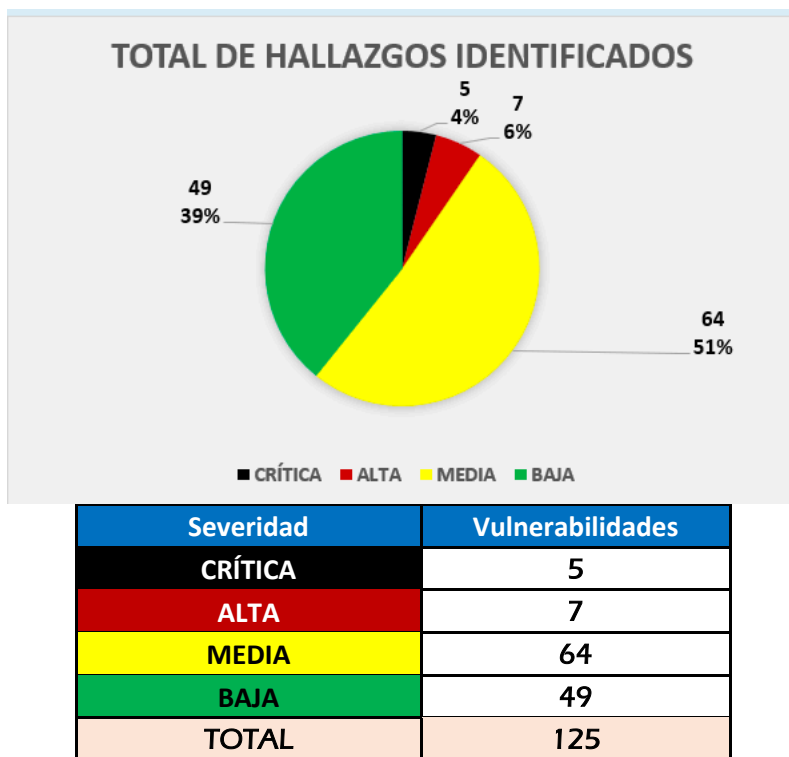


Ilustración 40 Consolidado General de Vulnerabilidades

Las pruebas del bloque mensual revelaron vulnerabilidades de tipo alto, medio y bajo en varios dispositivos de usuario final relacionadas con debilidades a nivel de configuración y versiones de servicios con vulnerabilidades conocidas. Estas fallas permitirían eventualmente la explotación remota de código en algunos casos y la posible pérdida de datos.

Para cada una de las siguientes vulnerabilidades se dan una recomendaciones que deben ser consideradas como parte de un plan de acción orientado a reducir la exposición a amenazas, mejorar la resiliencia de los sistemas y alinear la organización con estándares internacionales de ciberseguridad.(ver recomendaciones en el [INFORME TÉCNICO ANÁLISIS DE VULNERABILIDADES ICETEX \(Abril Mayo 2026\).pdf](#)

Categoría	Vunerabilidad
Vulnerabilidades Criticas	1. Unsupported Windows OS (remote)
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

Categoría	Vulnerabilidad
	2. Unsupported Web Server 3. VMware Aria Operations Multiple Vulnerabilities (VMSA-2024-0022)
Vulnerabilidades Altas	1. CGI Generic SQL Injection 2. Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote) 3. Microsoft Windows SMBv1 Multiple Vulnerabilities 4. MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) 5. SMB NULL Session Authentication 6. SSL Medium Strength Cipher Suites Supported (SWEET32) 7. OpenSSH < 10.3 Multiple Vulnerabilities
Vulnerabilidades Medias	1. .bash_history Files Disclosed via Web Server 2. Cross-Domain Misconfiguration 3. Falta de cabecera Anti-Clickjacking 4. Ausencia de Tokens Anti-CSRF 5. Browsable Web Directories 6. Cabecera Content Security Policy (CSP) no configurada 7. JQuery 1.2 < 3.5.0 Multiple XSS 8. CSP: script-src unsafe-inline inseguro en línea 9. Librería JS Vulnerable 10. Métodos HTTP TRACE / TRACK permitidos 11. PRTG Network Monitor < 20.1.57.1745 Information Disclosure (direct check) 12. Remote Desktop Protocol Server Man-in-the-Middle Weakness 13. SMB Signing not required 14. SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) 15. SSL Certificate Signed Using Weak Hashing Algorithm 16. SSL RC4 Cipher Suites Supported (Bar Mitzvah) 17. TLS Version 1.0, TLS Version 1.1 detección de protocolo 18. Web Application Potentially Vulnerable to Clickjacking. 19. Web Server HTTP Header Information Disclosure 20. Echo Service Detection: 21. Quote of the Day (QOTD) Service Detection
Vulnerabilidades Bajas	1. Terminal Services Encryption Level is not FIPS-140 Compliant 2. SSH Weak MAC Algorithms Enabled 3. SSH Weak Key Exchange Algorithms Enabled 4. SSH Server CBC Mode Ciphers Enabled 5. Falta Encabezado "X-Content-Type-Options" 6. Encabezado Strict-Transport-Security (HSTS) No establecido 7. Cookie Without SameSite Flag Detected 8. Cookie sin bandera "HttpOnly" 9. Cookie sin la bandera "secure"

Tabla 24 Vulnerabilidades encontradas

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

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

4.3.7.2. Conclusiones

La postura de ciberseguridad presenta avances operativos, pero existe una brecha importante entre las capacidades actuales y el nivel de protección requerido para una entidad como el ICETEX.

El informe reitera múltiples veces riesgos relacionados con:

- Licencias Fortinet vencidas.
- Capacidad insuficiente de FortiSIEM.
- Vulnerabilidades pendientes.
- Necesidad de fortalecer controles cloud.
- Falta de integración total de activos críticos al SIEM.
- Riesgos BYOD y equipos externos.

Impacto:

- Posibilidad de ataques cibernéticos.
- Pérdida de trazabilidad.
- Limitaciones de monitoreo.
- Riesgo reputacional y operativo.

4.4. Servicios de nube

Durante mayo de 2026, el rol Integrador de Nube ejecutó actividades orientadas al fortalecimiento operativo, técnico y financiero del entorno Microsoft Azure ICETEX, bajo los lineamientos del Cloud Adoption Framework y el Well Architected Framework. Las gestiones abarcaron frentes de estabilización de servicios productivos, definición de arquitecturas cloud, planeación estratégica de mediano plazo, gestión de incidentes técnicos y control financiero del entorno, alineadas con los objetivos institucionales de seguridad, continuidad operativa y sostenibilidad financiera de la plataforma.

4.4.1. Principales avances técnicos

Se avanzó significativamente en la estabilización del servicio de envío de correos transaccionales mediante Azure Communication Services, aplicando estrategias de control de volumen, warm-up gradual y priorización de destinatarios válidos. Estas acciones permitieron reducir los eventos de bloqueo, normalizar el comportamiento del servicio y consolidar un esquema de monitoreo de métricas que fortalece el caso técnico para el incremento de cuota gestionado ante Microsoft (TrackingID #2604160040009813). Paralelamente, se definieron los lineamientos técnicos para la migración controlada desde SendGrid hacia Azure Communication Services.

En el componente de arquitectura cloud, se ejecutó el análisis técnico y financiero comparativo entre las alternativas IaaS y Microsoft Fabric para la plataforma CRM ICETEX y sus componentes analíticos, concluyendo que el escenario IaaS resulta técnicamente viable y considerablemente más eficiente en costos para el workload analizado. Adicionalmente, se formalizó la entrega del Plan de Trabajo Azure ICETEX Mayo–Diciembre 2026, hoja de ruta priorizada que abarca identidad, red, almacenamiento, respaldo y continuidad, gobernanza, monitoreo y cumplimiento.

En materia de identidad y seguridad, se configuró el esquema de autenticación y autorización requerido para el acceso controlado al Data Warehouse de Microsoft Fabric mediante Microsoft Entra ID, se validaron las políticas de respaldo y recuperación de la plataforma DATAFONDOS en Azure, y se gestionó el escalamiento técnico formal con Microsoft Azure Support de un incidente de conectividad híbrida sobre VPN Site-to-Site relacionado con tráfico Oracle TNS hacia el datacenter on-premise (VM vm-dsdcp-manntis-prd).

4.4.2. Comportamiento financiero del entorno Azure

El entorno Microsoft Azure ICETEX Producción presentó durante mayo de 2026 un comportamiento financiero estable, manteniéndose dentro del rango esperado y consolidando la normalización del consumo posterior al pico registrado en marzo de 2026. El gasto total del periodo ascendió a USD 13,684.81, con una reducción del 2.7% frente al mes de abril y un margen significativo frente al presupuesto mensual definido de USD 20,300. Los principales componentes estructurales del gasto continúan siendo Storage (~45%) y Virtual Machines (~30%), con la región US East 2 concentrando el 84% del consumo total.

Concepto	Abril 2026 (USD)	Mayo 2026 (USD)	Variación
Storage	\$6,254.18	\$6,100.44	-\$153.74
Virtual Machines	\$4,287.92	\$4,154.31	-\$133.61
Microsoft Defender	\$695.20	\$681.50	-\$13.70
Backup	\$612.40	\$595.93	-\$16.47
GitHub	\$373.50	\$373.50	Sin variación
Otros servicios	\$1,844.10	\$1,779.13	-\$64.97
TOTAL EJECUTADO	\$14,067.30	\$13,684.81	-\$382.49 (-2.7%)
Presupuesto mensual	\$20,300.00	\$20,300.00	Dentro del rango
Margen disponible	\$6,232.70	\$6,615.19	+\$382.49

Tabla 25 Comparativo comportamiento financiero Azure (Abril-Mayo)

Mayo de 2026 refleja un entorno Azure institucional estable, controlado y alineado con buenas prácticas de operación cloud, consolidando avances importantes en seguridad, monitoreo, integración y sostenibilidad financiera. Las prioridades para el siguiente periodo incluyen la continuidad de la migración SendGrid hacia Azure Communication Services, la consolidación del documento definitivo de arquitectura CRM ICETEX, la ejecución de actividades priorizadas del Plan

de Trabajo Mayo–diciembre 2026, el seguimiento al incidente de conectividad híbrida con Microsoft Support y la validación previa al despliegue productivo del proyecto SNIBCE.

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 Mayo 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 mayo 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 EJECUTADO 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 EJECUTADO 2024
	\$10,466,332,286.04	\$ 8,888,383,619	\$480,000,000	\$0	\$480,000,000	\$1,587,413,017.00
	VALOR VIGENCIA 2025	VALOR EJECUTADO 2025	VALOR BOLSA VIGENCIA 2025	VALOR BOLSA EJECUTADO 2025	VALOR BOLSA NO EJECUTADO 2025	VALOR NO EJECUTADO 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 EJECUTADO 2026
Contrato Inicial	\$2,618,949,159.00		\$120,000,000		\$120,000,000	
OTROS14-Continuidad de Servicios por 8 meses	\$ 8.641.116.065					
Total Vigencia 2026	\$11.260.065.224,00	\$ 4.239.335.724	\$ 855.603.847	\$15.206.400	\$840.397.447	\$ 7.020.729.500
OTROS13-Adición Servicios	ITEM1 Arquitectura de Seguridad	ITEM2 Gestión 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	
OTROS13-Adición Servicios					\$ 2.761.480.370	

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

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	
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:	Marzo	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:	Marzo	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	
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	\$ 397.242.170	OTROSI4-Continuidad de Servicios por 8 meses
Pendiente- Pago No.2	Mes:	Mayo	De	2026	\$ 1.024.142.866	OTROSI4-Continuidad de Servicios por 8 meses
Pendiente- Pago No.2	Mes:	Mayo	De	2026	\$ 15.206.400	Bolsa
VALOR CAUSADO QUE NO SE HA PAGADO (valor a pagar factura)						\$ 1.024.142.866
VALOR TOTAL EJECUTADO (valor pagado + valor causado no pagado)						\$ 30.084.358.140
SALDO DEL CONTRATO (valor total del contrato – valor total ejecutado)						\$ 12.717.235.153
PORCENTAJE DE EJECUCIÓN						70,29%
* El valor causado no pagado corresponde a cuentas de cobro a facturas recibidas y aprobadas a satisfacción por el supervisor o interventor para su pago*						

Tabla 26 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 DB	Informe Mensual InfoTIC DBA Mayo 2026.pdf

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

Perfiles	Especialistas	Anexo
Especialista Web Máster	Juan Carlos Martinez	Informe Mensual InfoTIC Webmaster Mayo 2026.pdf
Especialista Integrador de nube	Carlos Barrera	Informe Mensual InfoTIC Integrador de Nube Mayo 2026.pdf
Especialistas de Seguridad Operador de Seguridad	Jhon Alveiro Pava González Edwin Morales Juan Carlos Quiroga asumió el rol Especialista de Seguridad desde el pasado 27 de Mayo de 2026 Héctor Rojas asumió el rol de Operador de Seguridad desde el 29 de mayo 2026	Informe Mensual InfoTIC Seguridad Mayo 2026.pdf
Especialistas de soluciones	Jose Francisco Escobar Escorcía Davis Alexander Mogollón Fandiño	Informe Mensual InfoTIC Administrador de Soluciones Mayo 2026.pdf
Especialista de Networking	Carlos Alberto Roldan Ríos Victor Manuel Castiblanco Sanchez - Apoyo Networking Walter eduardo pinilla tenorio asumio el rol de Apoyo Networking el 19 de mayo de 2026	Informe Mensual InfoTIC Administrador Redes Mayo 2026.pdf

Tabla 27 Perfiles y Actividades

El siguiente es el grupo administrativo que estuvo en el desarrollo de la operación del mes de Mayo 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 28 Grupo Administrativo

8. SERVICIO DE COLABORACIÓN

Durante el mes de Mayo, 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:

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

ÍTEM	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 movable 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 29 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.
- Disponibilidad de atención técnica para atender requerimientos que surjan para revisión de novedades presentadas.
- Se realizó actualización del sistema operativo de la OPS del módulo de la sede Aguas piso 7, Windows 10 a Windows 11.
- Informe mensual de operación y disponibilidad del servicio en las diferentes sedes, el cual se puede consultar en el link [Informe actividades Módulos videoconferencia ICETEX mayo 2026.pdf](#)

Durante el mes de Mayo, 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-32489.

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 Mayo 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 Mayo 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 Mayo 2026.xlsx](#)

Sede	Categoría	INR	BW	%MES
BOGOTAD.C.	Principal/FO(SedeAguas)	INR0037	400MB	100,00 %
	Backup /FO(SedeAguas)	INR0036	200MB	99,93%
	Principal/IPVPN(SedeChapinero)	INR0022	40MB	99,99 %
	Backup /IPVPN(SedeChapinero)	INR0020	25MB	100,00 %
	Principal/IPVPN(Angel)	INR0272	200MB	100,00 %
	Backup /IPVPN(Angel)	INR0273	200MB	100,00 %
IBAGUE	Principal/IPVPN	INR0073	20MB	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
LETICIA	Backup/IPVPN	INR0076	20MB	99,28 %
	Principal/Satelital	INR0000373	8MB	100,00 %
NEIVA	Principal/IPVPN	INR0039	20MB	100,00 %
	Backup/IPVPN	INR0041	10MB	100,00 %
TUNJA	Principal/IPVPN	INR0104	20MB	99,61%
	Backup/IPVPN	INR0106	5MB	99,80 %
VILLAVICENCIO	Principal/IPVPN	INR0085	20MB	100,00 %
	Backup/IPVPN	INR0084	10MB	100,00 %
ARMENIA	Principal/IPVPN	INR0074	20MB	100,00 %
	Backup/IPVPN	INR0072	10MB	99,85 %
MANIZALES	Principal/IPVPN	INR0088	20MB	99,99 %
	Backup/IPVPN	INR0087	10MB	100,00 %
MEDELLIN	Principal/IPVPN	INR0133	100MB	100,00 %
	Backup/IPVPN	INR0132	30MB	100,00 %
APARTADO	Principal/IPVPN	INR0144	20MB	98,72 %
PEREIRA	Principal/IPVPN	INR0079	20MB	100,00 %
	Backup/IPVPN	INR0077	20MB	100,00 %
QUIBDO	Principal/IPVPN	INR0014	20MB	99,42 %
	Backup/IPVPN			0,00%
BARRANQUILLA	Principal/IPVPN	INR0103	100MB	100,00 %
	Backup/IPVPN	INR0100	20MB	100,00 %
CARTAGENA	Principal/IPVPN	INR0109	20MB	93,87 %
	Backup/IPVPN	INR0107	10MB	99,49 %
MONTERIA	Principal/IPVPN	INR0080	20MB	100,00 %
	Backup/IPVPN	INR0081	10MB	100,00 %
RIOHACHA	Principal/IPVPN	INR0164	20MB	99,99 %
	Backup/IPVPN	INR0162	10MB	99,27 %
SANTAMARTA	Principal/IPVPN	INR0154	20MB	99,87 %
	Backup/IPVPN	INR0152	10MB	99,91 %
SINCELEJO	Principal/IPVPN	INR0095	20MB	100,00 %
	Backup/IPVPN	INR0097	5MB	100,00 %
SAN ANDRES	Principal/IPVPN	INR0000367 INR0000369	8MB	98,83 %
BARRANCABERMEJA	Principal/IPVPN			0,00%
SANGIL	Principal/IPVPN			0,00%
BUCARAMANGA	Principal/IPVPN	INR0062	30MB	100,00 %
	Backup/IPVPN	INR0061	20MB	100,00 %
CUCUTA	Principal/IPVPN	INR0044	20MB	100,00 %
	Backup/IPVPN	INR0047	10MB	100,00 %
VALLEDUPAR	Principal/IPVPN	INR0091	20MB	99,96 %
	Backup/IPVPN	INR0090	10MB	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
YOPAL	Principal/IPVPN	INR0121	20MB	100,00 %
	Backup/IPVPN	INR0123	10MB	93,77 %
ARAUCA	Principal/IPVPN	INR0110	20MB	99,94 %
CALI	Principal/IPVPN	INR0151	100MB	100,00 %
	Backup/IPVPN	INR0153	150MB	100,00 %
BUENAVENTURA	Principal/IPVPN	INR0051	10MB	98,81 %
MOCOIA	Principal/IPVPN	INR0135	10MB	99,32 %
	Backup/Satelital	INR0136	5MB	95,77 %
PASTO	Principal/IPVPN	INR0130	20MB	100,00 %
	Backup/IPVPN	INR0131	10MB	100,00 %
POPAYAN	Principal/IPVPN	INR0035	20MB	100,00 %
	Backup/IPVPN	INR0032	5MB	100,00 %
TUMACO	Principal/IPVPN	INR0147	20MB	91,18 %
DCTRIARA	MPLS PP	INR0266	1GB	100,00 %
	MPLS BK	INR0171	1GB	100,00 %
DCTRIARA	INTERNET BK	INR0221	800MB	0,00%
	INTERNET PP	INR0264	800MB	100,00 %
DCTRIARA	NOCclarodedidcado(DWDM)2GTri aramegacentro	INR0224	2GB	100,00%
CanalentreSitiopricipalelc etex-DirecciónGeneral- Aguas	Principal/IPVPN			0 %
	Backup/IPVPN			0 %
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%
BancodelaRepublicahasta EdificioDirecciónGeneral CETEX	UbicadoenDatacenterPrincipal.int erconectadoatravesderedMPLS	INR0000289	40MB	99,91 %
DECEVALhastaEdificiodel CETEXDirecciónGeneral.	UbicadoenDatacenterPrincipal.int erconectadoatravesderedMPLS	INR0000317	40MB	100,00 %
DECEVALhastaEdificiodel CETEXDirecciónGeneral.	UbicadoenDatacenterPrincipal.int erconectadoatravesderedMPLS(Ba ckup)	INR0000318	15MB	100,00 %
Salidadelportaleshttps:// portal.icetex.gov.co/port alywww.icetex.gov.cohaci ainternetencentrodecóm putoprincipal	InternetReversoparaPortales	INR0000320	1GB	100,00 %

Sede	Categoría	INR	BW	%MES
DCTRIARA	allotentralizado800Mtriara(equipo)	INR0270		100,00 %

Tabla 30 Disponibilidad de Canales

Durante el mes de Mayo 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	100,00 %
CALI	INTERNET PARA LA GENTE	INR0160	100,00 %
AGUAS	INTERNET PARA LA GENTE	INR0029	100,00 %
CHAPINERO	INTERNET PARA LA GENTE	INR0015	99,99 %
MEDELLIN	INTERNET PARA LA GENTE	INR0122	100,00 %
APARTADO	INTERNET PARA LA GENTE	INR0140	98,80 %
ARAUCA	INTERNET PARA LA GENTE	INR0115	99,94 %
LETICIA	INTERNET PARA LA GENTE	INR0000378	99,64 %
QUIBDO	INTERNET PARA LA GENTE	INR0021	99,42 %
RIOHACHA	INTERNET PARA LA GENTE	INR0159	100,00 %
SAN ANDRES	INTERNET PARA LA GENTE	INR0000368**	98,59 %
YOPAL	INTERNET PARA LA GENTE	INR0127	100,00 %
MOCOA	INTERNET PARA LA GENTE	INR0141	99,32 %

Tabla 31 Disponibilidad canales "Internet para la gente"

Canales Sdwan:

Sede	Codigo	Ancho de Banda	Disponibilidad
SDWANAGUAS	INR0033/000334	10MB	100,00%
SDWANMOCOA	INR0139/000333	10MB	99,32%
SDWANLETICIA	INR0000374	10MB	99,64 %
SDWANSANANDRES	INR0000371**	10MB	98,83 %

Tabla 32 Disponibilidad canales SDWAN

NOTA: INR0000368** INR0000371** Presentan disponibilidad por debajo del 80% sin embargo no debe realizarse el descuento del ANS teniendo en cuenta que la indisponibilidad no es atribuible al aliado CLARO sino un problema de fluido eléctrico en la sede como se evidencia en el CASO >> IM-SOPORTETI-31167 LA SEDE CUENTA CON ENERGÍA, PERO EL RACK DE COMUNICACIONES NO CUENTA CON FLUIDO ELÉCTRICO. POR FAVOR ESCALAR A RECURSOS FÍSICOS.

10.2. 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

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

la replicación de la información de los equipos de ICETEX, para el mes de Mayo continúa su funcionamiento correctamente sin novedades que afectaran la prestación del servicio. La evidencia se encuentra en el [Informe mensual replicacion Mayo 2026.pdf](#)

10.3. 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 [Reporte Monitoreo ICETEX Mayo_ELK.pdf](#) y [Disponibilidad Server_ELK_Mayo_2026.xlsx](#)

No	COD.	Etiquetas de fila	Disponibilidad
1	INR0278	cxvodacontg011	100,00%
2	INR0277	cxvodaprodn021	100,00%
3	INR0276	cxvodaprodn011	100,00%
4	INR0262	icetexboglxorfeo2.localdomain	100,00%
5	INR0260	icetexosbognfs1	100,00%
6	INR0259	INR0259_INFOTIC	99,99%
7	INR0258	INR0258_INFOTIC	0,00%
8	INR0257	INR0257_INFOTIC	100,00%
9	INR0256	INR0256_INFOTIC	100,00%
10	INR0255	INR0255_INFOTIC	100,00%
11	INR0254	INR0254_INFOTIC	100,00%
12	INR0253	bastion.localdomain	100,00%
13	INR0252	icetexosbognfs2	100,00%
14	INR0251	INR0251_INFOTIC	99,99%
15	INR0250	qasec	100,00%
16	INR0249	xroadsec	100,00%
17	INR0248	icetexboglxroad3	100,00%
18	INR0247	preprodsec	100,00%
19	INR0246	icetexboglxdarumatest	100,00%
20	INR0245	icetexboglxdarumasrv2	100,00%
21	INR0244	icetexboglxdarumasrv1	100,00%
22	INR0243	icetexbogliferaysrv1	100,00%
23	INR0242	icetexbogliferaysrv2	100,00%
24	INR0241	icetexbogelasticserver3	100,00%
25	INR0240	icetexbogelasticserver2	100,00%
26	INR0239	icetexbogelasticserver1	100,00%
27	INR0238	icetexbogliferaynfs	100,00%
28	INR0237	icetexbogbalsrv1-r	0,00%
29	INR0236**	ictxbogsvrpt1	100%
30	INR0235**	ictxbogsvrpt2	100%
31	INR0234	ictxprusisgapp	100%
32	INR0233	icetexboglxorfeo1.localdomain	100%

No	COD.	Etiquetas de fila	Disponibilidad
33	INR0229	ictxisgesapp	100%
34	INR0228	lctxisgesbd	100%
35	INR0226	mira	100%
36	INR0000322	lctxsrvctrldoc	99,98%
Balanceador Nodo 1	INR0197	TFM1412	100%
Balanceador Nodo 2	INR0197	TFM1407	100%

Tabla 33 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
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 34 Dispositivos en Housing – Datacenter Principal

10.4. Disponibilidad TRIARA para los servicios de página web Icetex

La disponibilidad del Portal Web institucional web.ICETEX.gov.co, en el mes de Mayo presentó un **UPTIME del [99,761%]** 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:

	Marzo	Abril	Mayo
Usuarios activos mes	600000	506000	495000
Usuarios nuevos	382000	324000	314000

	Marzo	Abril	Mayo
Tiempo de interacción (seg)	97	91	121

Tabla 35 Distribución trimestral de acceso por usuarios

El portal WEB cuenta con un total de 495 mil usuarios, con 314 mil usuarios nuevos. El tiempo de interacción medio es de 2 minutos y 1 segundo, señalando el interés de la audiencia en las diferentes páginas del portal web.icetex.gov.co.

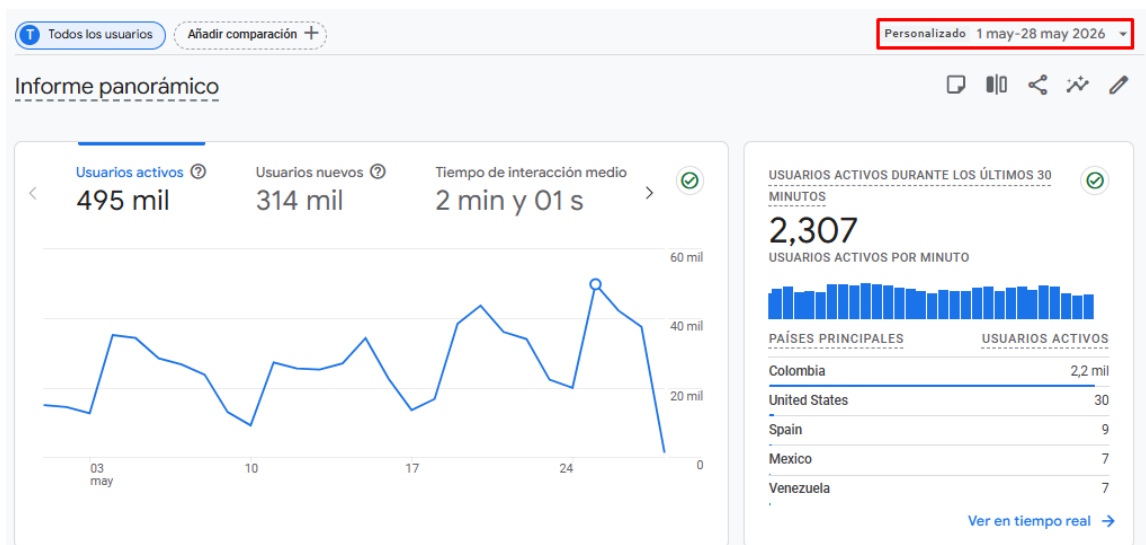
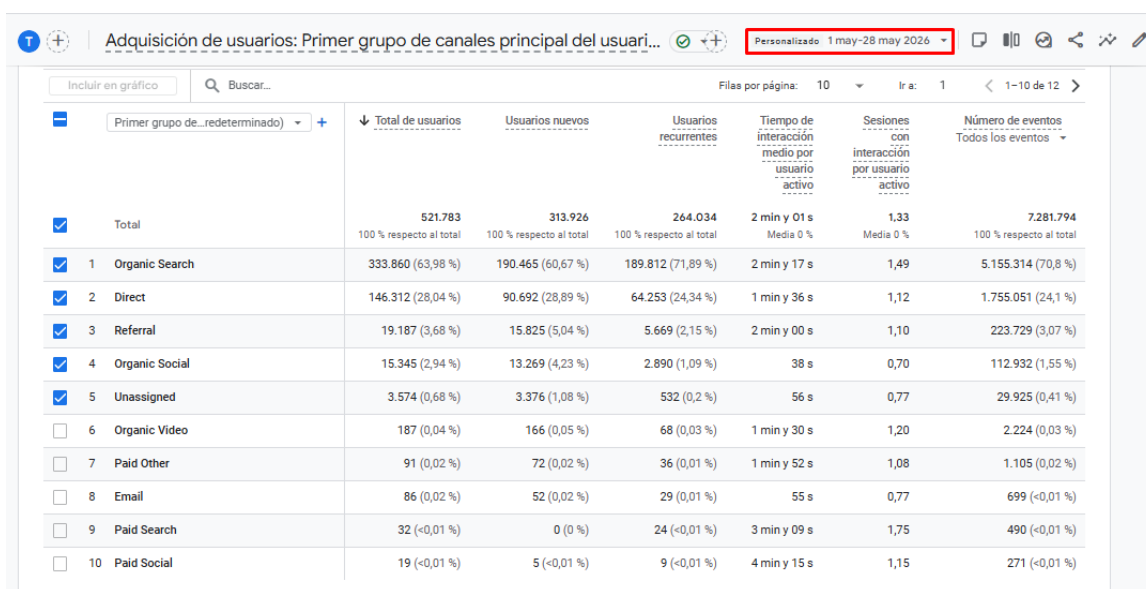


Ilustración 41 Métrica de visitantes Portal WEB web.ICETEX.gov.co

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:



Adquisición de usuarios: Primer grupo de canales principal del usuari... | Personalizado 1 may-28 may 2026

Incluir en gráfico | Buscar...

	Total de usuarios	Usuarios nuevos	Usuarios recurrentes	Tiempo de interacción medio por usuario activo	Sesiones con interacción por usuario activo	Número de eventos
Total	521.783 100 % respecto al total	313.926 100 % respecto al total	264.034 100 % respecto al total	2 min y 01 s Media 0 %	1,33 Media 0 %	7.281.794 100 % respecto al total
☒ 1 Organic Search	333.860 (63,98 %)	190.465 (60,67 %)	189.812 (71,89 %)	2 min y 17 s	1,49	5.155.314 (70,8 %)
☒ 2 Direct	146.312 (28,04 %)	90.692 (28,89 %)	64.253 (24,34 %)	1 min y 36 s	1,12	1.755.051 (24,1 %)
☒ 3 Referral	19.187 (3,68 %)	15.825 (5,04 %)	5.669 (2,15 %)	2 min y 00 s	1,10	223.729 (3,07 %)
☒ 4 Organic Social	15.345 (2,94 %)	13.269 (4,23 %)	2.890 (1,09 %)	38 s	0,70	112.932 (1,55 %)
☒ 5 Unassigned	3.574 (0,68 %)	3.376 (1,08 %)	532 (0,2 %)	56 s	0,77	29.925 (0,41 %)
☐ 6 Organic Video	187 (0,04 %)	166 (0,05 %)	68 (0,03 %)	1 min y 30 s	1,20	2.224 (0,03 %)
☐ 7 Paid Other	91 (0,02 %)	72 (0,02 %)	36 (0,01 %)	1 min y 52 s	1,08	1.105 (0,02 %)
☐ 8 Email	86 (0,02 %)	52 (0,02 %)	29 (0,01 %)	55 s	0,77	699 (<0,01 %)
☐ 9 Paid Search	32 (<0,01 %)	0 (0 %)	24 (<0,01 %)	3 min y 09 s	1,75	490 (<0,01 %)
☐ 10 Paid Social	19 (<0,01 %)	5 (<0,01 %)	9 (<0,01 %)	4 min y 15 s	1,15	271 (<0,01 %)

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

Ilustración 42 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.

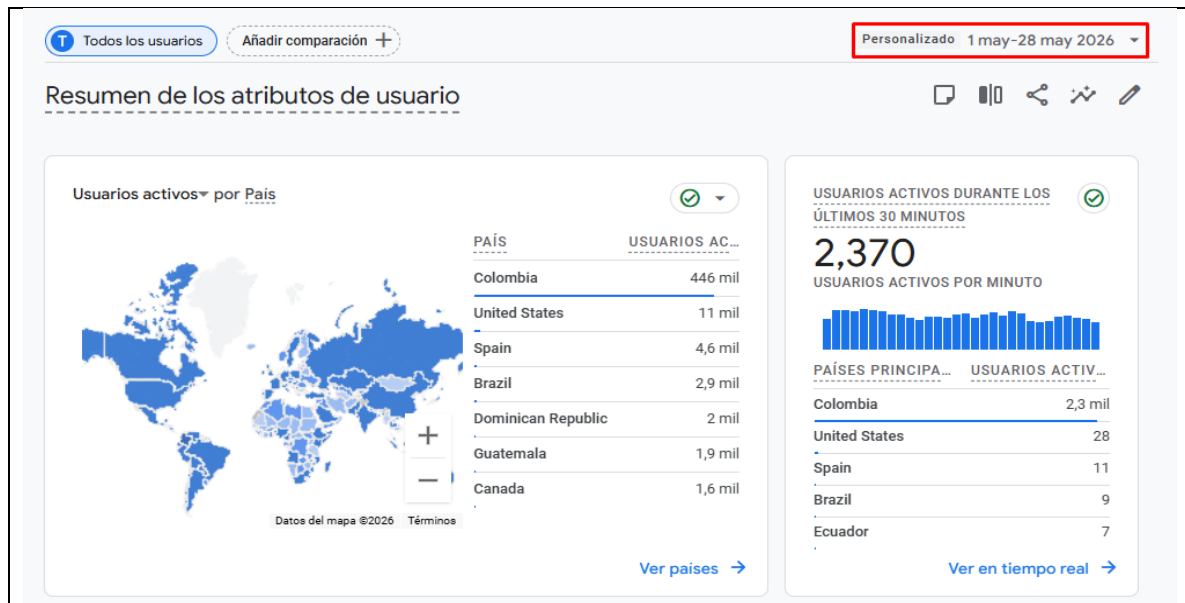


Ilustración 43 Métrica de usuario por país - Portal WEB web.ICETEX.gov.co

Detalles demográficos: Ciudad

Personalizado: 1 may-28 may 2026

	↓ Usuarios activos	Usuarios nuevos	Sesiones con interacción	Porcentaje de interacciones	Sesiones con interacción por usuario activo	Tiempo de interacción medio por usuario activo	Número de eventos
Total	495.225 100 % respecto al total	313.926 100 % respecto al total	659.084 100 % respecto al total	58,09 % Media 0 %	1,33 Media 0 %	2 min y 01 s Media 0 %	7.281.794 100 % respecto al total
1 Bogotá	178.112 (35,97 %)	110.777 (35,29 %)	243.140 (36,89 %)	56,38 %	1,37	2 min y 04 s	2.707.059 (37,18 %)
2 Barranquilla	46.980 (9,49 %)	22.660 (7,22 %)	60.844 (9,23 %)	55,55 %	1,30	1 min y 43 s	628.639 (8,63 %)
3 Medellín	38.259 (7,73 %)	19.727 (6,28 %)	40.868 (6,2 %)	57,37 %	1,07	1 min y 23 s	426.608 (5,86 %)
4 Cali	36.841 (7,44 %)	18.930 (6,03 %)	41.364 (6,28 %)	58,59 %	1,12	1 min y 41 s	440.935 (6,06 %)
5 (not set)	29.452 (5,95 %)	16.985 (5,41 %)	33.690 (5,11 %)	60,02 %	1,14	1 min y 47 s	352.117 (4,84 %)
6 Cartagena	16.114 (3,25 %)	7.428 (2,37 %)	20.197 (3,06 %)	59,17 %	1,25	1 min y 49 s	209.240 (2,87 %)
7 Montería	11.904 (2,4 %)	5.453 (1,74 %)	17.177 (2,61 %)	59,13 %	1,44	1 min y 48 s	175.481 (2,41 %)
8 Bucaramanga	8.612 (1,74 %)	4.492 (1,43 %)	10.054 (1,53 %)	59,41 %	1,17	1 min y 40 s	104.361 (1,43 %)
9 Sincelejo	7.294 (1,47 %)	3.283 (1,05 %)	11.533 (1,75 %)	58,38 %	1,58	2 min y 06 s	117.981 (1,62 %)
10 Pasto	7.217 (1,46 %)	3.449 (1,1 %)	9.454 (1,43 %)	62,78 %	1,31	2 min y 01 s	101.346 (1,39 %)

Ilustración 44 Métrica de ciudades de Colombia- Portal WEB web.ICETEX.gov.co

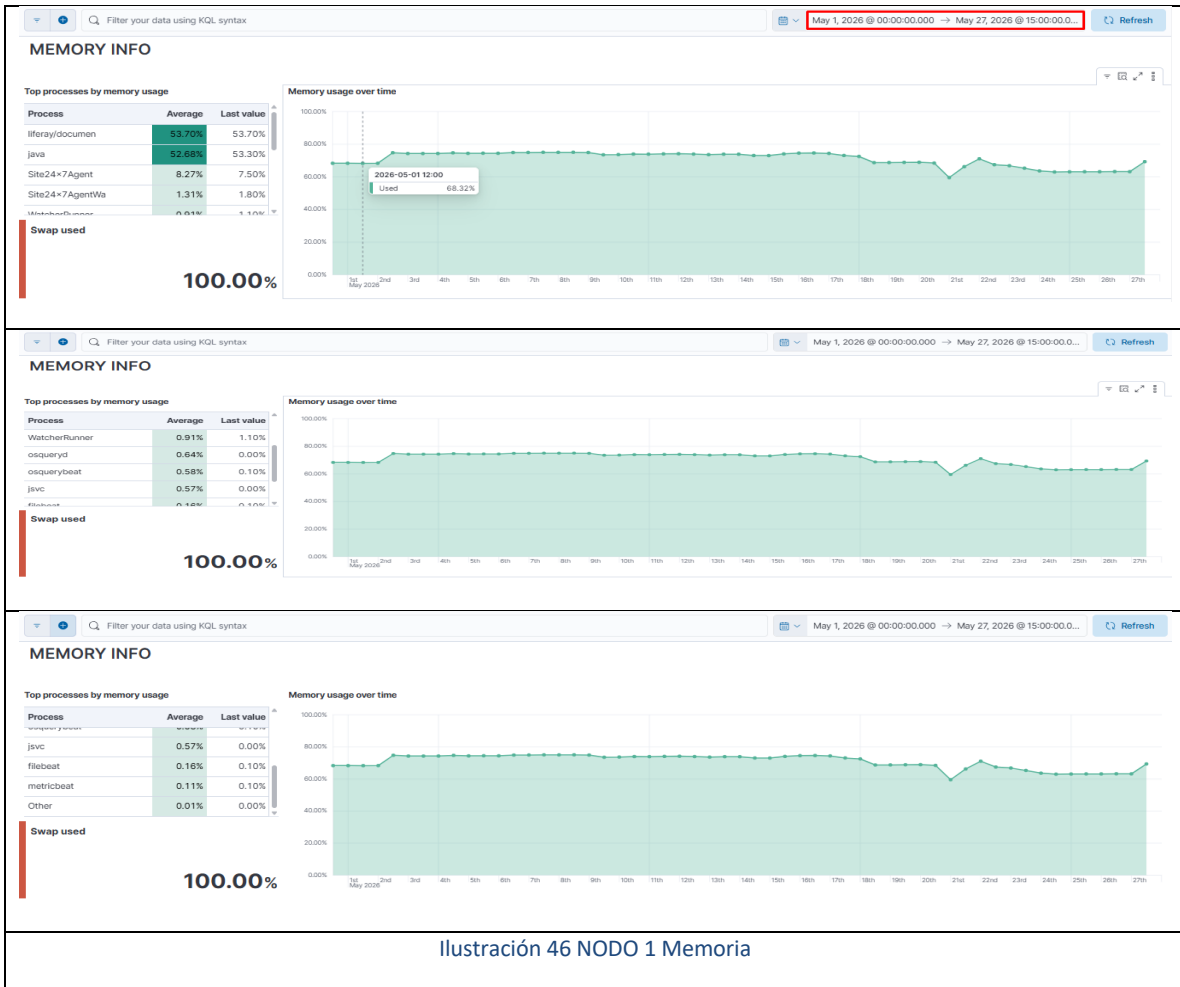
Sede principal-Bogotá, Colombia
 Calle 93B # 13-44, Segundo piso
 NIT:900.068.796-1
 Teléfono (+601) 7466000- 3185214505

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

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 Mayo desde las 00:00 horas hasta las 23:59 horas del 30 de Mayo de 2026.



Ilustración 45 NODO 1 CPU



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 Mayo 2026.pdf](#)

10.4.1. Análisis componente Liferay Producción

Como parte de las actividades desarrolladas desde la administración web, se realizó una revisión de la infraestructura tecnológica y el entorno de software del portal Liferay, abordando componentes clave para su seguridad y rendimiento sin que se identificaran hallazgos significativos. Por otra parte, de cara al proceso de migración a la versión 7.4 DXP, se hace indispensable que ICETEX gestione la adquisición de la suscripción de Red Hat 7.9 para el ambiente de pruebas. Asimismo, se requiere tramitar de manera anticipada la renovación del licenciamiento de Liferay (dos nodos) y Elasticsearch (tres nodos) —cuyo vencimiento está programado para octubre de 2026— con el objetivo de asegurar el respaldo y soporte técnico necesario durante dicha actualización.

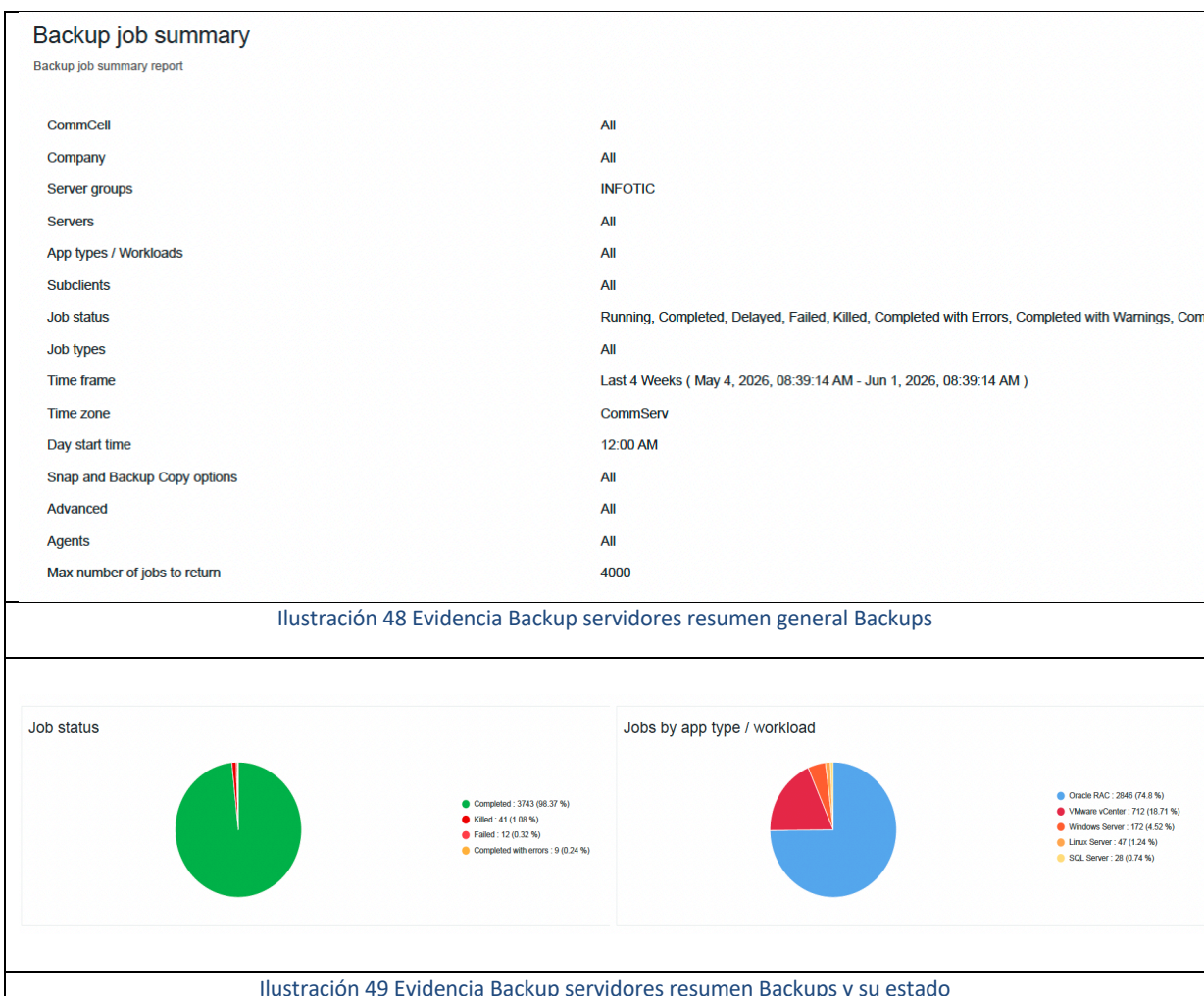
10.5. Backup Servidores Triara

Durante el mes de mayo se 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 Mayo 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 mayo 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 V7.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 Mayo el resultado de la ejecución de los Backups fue el siguiente:



El total del tamaño de la información respalda para el mes de Mayo corresponde a 216.55 TB, donde 98.37% se completó en el primer lanzamiento del robot con un total de 216.05 TB de información.

El 74.8% 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 3805 trabajos analizados, el 98,37% se completó con éxito.

- Tasa de éxito: 98.37 % (trabajos completados)
- Tasa de fracaso: 1.40% (trabajos fallidos o cancelados)

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

- Oracle RAC: El 74.8% de los trabajos de respaldo corresponden a este tipo de servidor, con un total de 2846 trabajos.
- VMware vCenter: El 18.71% de los trabajos pertenecen a este entorno, con 712 trabajos.
- Otros Servidores: Los trabajos de Windows Server, Linux Server y SQL Server representan el 4.52 %, 1.24 % y 0.74 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](#).

El servicio cuenta con una estrategia de respaldo y continuidad operativa sumamente madura y estable.

11. CONTROL DE CAMBIOS

Durante el mes de mayo no se presentaron actividades ante el comité de cambios para su revisión y aprobación. Quedamos a la espera de que ICETEX nos indique la disponibilidad de los recursos de virtualización de colocation para retomar las actualizaciones de sistema operativo de los servidores:

- ICTXSRVNETCOR01(192.168.51.165) aloja las aplicacionesPSE, CargueArchivos, CuentasAbandonadas, Cuentas Inactivas, Portal Transaccional y Transunion, las cuales están publicadas en internet y accedidas por usuarios externos.
- ICTXSRVPASARELA(192.168.51.211): aloja la aplicacionPSE
- ICTXSRVDCVAL01(192.168.51.170): aloja la aplicación Deceval, esencial para la integraciónconservicios financieros externos.

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 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	El 25 de mayo se llevó a cabo la socialización de la herramienta Falcon con ICETEX, obteniendo la aprobación por parte de la entidad. Actualmente, se está coordinando la programación para la desinstalación de Symantec y la correspondiente migración a Falcon, las cuales se ejecutarán dentro de las ventanas de mantenimiento y

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
				disponibilidad que se concierten con ICETEX.

Tabla 36 Planes de trabajo

13. PLAN DE ENTREGA

En atención a la prórroga del contrato, no fue viable continuar con el desarrollo del cronograma de entregas original. Sin embargo, para su conocimiento, nos permitimos remitir un balance detallado del estado de avance y las actividades que se han ejecutado 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 de verificación.
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 37 Balance General actividades ejecutadas Plan de entrega

El proyecto se encuentra en operación y muestra una estabilización progresiva, alineada con las iniciativas que adelanta el ICETEX. No obstante, persisten algunas situaciones que impactan la ejecución, particularmente en la gestión de personal, recursos de hardware insuficientes en equipos de collocation y componentes de seguridad.

14. 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.
- **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.

15. RECOMENDACIONES DEL CONTRATISTA AL ICETEX

15.1. 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.

15.2. 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 ha reportado el espacio empleado en la unidad F del servidor ICTXSRVNETCOR01, el cual llega a unos umbrales cercanos al 97% 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.

A continuación, se presenta un cuadro histórico consolidado del uso del almacenamiento en los discos del servidor ICTXSRVNETCOR01, correspondiente a los meses de marzo de 2026, abril de 2026 y mayo de 2026, seguido de observaciones y recomendaciones.

Disco	Métrica	mar-26	abr-26	may-26	Observaciones	Recomendaciones
C:	Espacio usado	53% (52.91 GiB)	67% (66.85 GiB)	67% (67.01 GiB)	En mar-26 el disco mantiene un comportamiento estable, con un 53% de uso y 46.60 GiB libres, evidenciando que las acciones implementadas continúan siendo efectivas y que no se presentan riesgos de saturación a corto plazo.	El disco C: se encuentra en estado óptimo. Se recomienda mantener políticas de limpieza periódica y monitoreo para evitar nuevamente escenarios de saturación, así como configurar alertas preventivas ante incrementos inusuales en el consumo.
	Espacio libre	46.60 GiB	32.66 GiB	32.50 GiB	En abr-26 el disco presenta un incremento considerable en su consumo, alcanzando un 67% de uso y reduciendo el espacio libre a 32.66 GiB, lo que indica un crecimiento significativo respecto a los meses anteriores. Aunque aún no se encuentra en estado crítico, se evidencia una tendencia que debe ser monitoreada para evitar degradación del estado óptimo previamente alcanzado.	
					En may-26 el volumen presenta un estado estable con un 33% de espacio libre (32.50 GB disponibles de 99.51 GB). No se evidencian alertas de capacidad en el momento de la revisión.	
F:	Espacio usado	97% (198 TiB)	97% (198 TiB)	97% (1.94 TiB)	En mar-26 el disco presenta un incremento adicional, alcanzando el 97% de uso y reduciendo el espacio libre a 70.56 GiB, lo que evidencia un agravamiento del estado crítico y un margen operativo cada vez más limitado.	El disco F: permanece en estado crítico sostenido con tendencia de deterioro. Se recomienda de forma prioritaria: Ampliación de capacidad del volumen Depuración o archivado de información Identificación de directorios de alto consumo (logs, backups, repositorios) Implementación de alertas críticas de uso Ya que existe riesgo alto de afectación a los servicios.
	Espacio libre	70.56 GiB	65.82 GiB	64.21 GiB	En abr-26 el disco continúa en estado crítico, manteniéndose en aproximadamente 97% de uso, con 65.82 GiB libres. Aunque se observa una leve variación en el espacio disponible, no representa una mejora estructural, confirmando una saturación sostenida con alto riesgo operativo y margen mínimo de crecimiento.	
					En may-26 se evidencia alta ocupación del volumen, contando únicamente con un 3% de espacio libre (64.21 GB disponibles de 2 TB). Se recomienda realizar validación y depuración de información para evitar posibles afectaciones en la operación o indisponibilidad de servicios.	
E:	Espacio usado	87% (56.70)	66% (42.18)	75% (48.54)	En mar-26 el disco continúa con la tendencia de crecimiento, alcanzando el 87% de uso y reduciendo el espacio libre a 8.30 GiB, confirmando un comportamiento sostenido de incremento y acercándose nuevamente a un escenario crítico.	El disco E: se encuentra con almacenamiento disponible.
	Espacio libre	8.30 GiB	22.08 GiB	16.46 GiB	En abr-26 el disco presenta una mejora significativa, reduciendo su uso a 66% y aumentando el espacio libre a 22.08 GiB, lo que sugiere la ejecución efectiva de actividades de depuración, liberación de espacio o rotación de información. Se recupera un estado operativo controlado, alejándose temporalmente del umbral crítico.	
					En may-26 el volumen presenta un 25% de espacio libre (16.46 GB disponibles de 65 GB). Aunque actualmente se encuentra operativo, se recomienda realizar	

Ilustración 50 Histórico consolidado uso de discos servidor ICTXSRVNETCOR01

15.3. 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.

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

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.

15.4. Bases De Datos

Establecer las tareas y el cronograma para la migración de las bases de datos 11g (fuera de soporte) a la versión 19c o superior.

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.

15.5. Integrador De Nube

- Mantener el monitoreo continuo del servicio Azure Communication Services, fortaleciendo el seguimiento de métricas de entregabilidad, failure rate y patrones de tráfico mientras se completa el proceso de incremento de cuota con Microsoft.
- Continuar con la implementación gradual de la migración desde SendGrid hacia Azure Communication Services bajo un esquema controlado de warm-up, priorización de destinatarios válidos y monitoreo permanente del servicio.
- Finalizar la recopilación de información técnica pendiente para consolidar el documento definitivo de arquitectura y dimensionamiento de la plataforma CRM y componentes analíticos en Azure.
- Dar continuidad a la ejecución del Plan de Trabajo Azure ICETEX Mayo–Diciembre 2026, priorizando actividades asociadas a seguridad, gobernanza, monitoreo y continuidad operativa.
- Implementar controles periódicos de revisión y renovación de secretos, credenciales y permisos configurados sobre Microsoft Entra ID y Microsoft Fabric, evitando riesgos asociados a expiración o exposición de accesos.
- Continuar fortaleciendo la estrategia de respaldo y recuperación de plataformas críticas en Azure, incluyendo validaciones periódicas de restauración y tiempos estimados de recuperación operativa.
- Mantener el seguimiento técnico al incidente de conectividad híbrida Azure–OnPremise junto con Microsoft Support, validando nuevas pruebas y posibles ajustes sobre infraestructura de red y seguridad.
- Validar con las áreas responsables la alternativa técnica más adecuada para la implementación de certificados SSL institucionales en Azure, considerando costos, escalabilidad, seguridad y facilidad operativa.
- Continuar con el análisis técnico y financiero previo al despliegue productivo del proyecto SNIBCE, validando especialmente riesgos de seguridad, dependencias tecnológicas y costos operativos asociados.
- Mantener el seguimiento mensual del comportamiento financiero de la suscripción Azure ICETEX Producción, identificando oportunidades de optimización de costos sobre servicios estructurales como almacenamiento, máquinas virtuales y monitoreo.

16. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC

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

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

En mayo de 2024 finalizó la ampliación de sedes y el aumento de ancho de banda (Anexo #2), cambio que se evidencia en SolarWinds y se valida mensualmente en la facturación de ICETEX.

16.2. TB de capacidad de almacenamiento

Durante la fase de implementación, se realizó la entrega de las capacidades de almacenamiento definidas contractualmente, las cuales se detallan a continuación:

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 38 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 39 Capacidades de almacenamiento provisionado

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 Mayo no se recibieron desde el Icetex solicitudes de pruebas de restauración.

16.3. “Wifi” para la gente en 14 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 40 WIFI para la gente instalados

17. 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.
- Se consolidó la preparación para migrar los correos transaccionales a Azure Communication Services (mejorando la entregabilidad) y finalizó la definición técnica/financiera de la arquitectura Cloud para el CRM de ICETEX.
- Se formalizó el Plan de Trabajo Azure Mayo–Diciembre 2026, estableciendo las prioridades en seguridad, gobernanza, monitoreo y continuidad operativa de la nube institucional.
- El análisis comparativo determinó que Microsoft Fabric es una alternativa más eficiente en costos y técnicamente viable frente a IaaS para los workloads analíticos; además, se fortalecieron sus accesos mediante Microsoft Entra ID.
- Se validaron con éxito las políticas de backup y recuperación de la plataforma DATAFONDOS en Azure, garantizando la protección de la información.
- Se escaló formalmente ante el soporte de Microsoft un fallo de conectividad híbrida (tráfico Oracle TNS sobre VPN) y se entregaron propuestas para la validación de certificados SSL y la infraestructura del proyecto SNIBCE para mitigar riesgos preproducción.
- El consumo del entorno Azure se mantuvo estable y bajo control durante mayo, consolidando la normalización del gasto tras el incremento extraordinario registrado en marzo de 2026.

18. ANEXOS

Tema	SubTema	Anexo
Almacenamiento	Backups Diarios	Backups diarios Mayo 2026 Backup Diario
	Informe de Backups	Consolidado mensual Backups Mayo 2026 Consolidado Mensual de Backups mayo 2026.pdf Informe Backups mes de Mayo 2026.pdf Politica Backup Icetex V7.xlsx ReporteMensualCintasInfotc 2026-05-29.html
Aplicaciones	Informes de actividades	Informe actividades Módulos videoconferencia ICETEX Mayo 2026 Informe actividades Módulos videoconferencia ICETEX mayo 2026.pdf Informe mensual Administrador de Soluciones Mayo 2026 Informe Mensual InfoTIC Administrador de Soluciones Mayo 2026.pdf Informe mensual Administrador Web Master Mayo 2026 Informe Mensual InfoTIC Webmaster Mayo 2026.pdf Informe mensual Integrador Nube Mayo 2026 Informe Mensual InfoTIC Integrador de Nube Mayo 2026.pdf
Bases De Datos		Informe mensual Administrador de Bases de datos Mayo 2026 Informe Mensual InfoTIC DBA Mayo 2026.pdf
Ejecución Presupuestal		Conciliación Mayo consolidado Conciliación Mayo consolidado 2026.xlsx Informe de Gestión Servicio Mayo 2026 Informe de Gestion Servicio Mayo 2026.pdf Informe de Gestion Servicio Mayo 2026.docx
Seguridad		Informe Mensual MARCA-OSINT ICETEX Mayo 2026 Informe Mensual MARCA-OSINT ICETEX Mayo 2026.pdf Anexo Informe Mensual MARCA-OSINT ICETEX Mayo 2026.xlsx Informe Mensual Seguridad Mayo 2026 Informe Mensual InfoTIC Seguridad Mayo 2026.pdf Informe Mensual SOC - ICETEX Mayo 2026 Informe Mensual SOC-TH ICETEX mayo 2026.pdf Informe Tecnico Analisis de Vulnerabilidades Abril-Mayo 2026

Tema	SubTema	Anexo
		INFORME TÉCNICO ANÁLISIS DE VULNERABILIDADES ICETEX (Abril Mayo 2026).pdf Matriz de Vulnerabilidades Icetex Abril-Mayo 2026 Matriz de Vulnerabilidades ICETEX ABRIL 2026.xlsx
Soporte Y Monitoreo	Canales	ANS Mayo 2026 ANS Mayo 2026.xlsx Informe mensual Administrador de Networking Mayo 2026 Informe Mensual InfoTIC Administrador Redes Mayo 2026.pdf Informe Mensual Disponibilidad Mayo2026 Reporte Mensual Disponibilidad INFOTIC Mayo 2026.pdf
	Gráficas de consumo	Informe Mensual ALLOT Mayo 2026 Graficas de consumo Mayo 2026 – ALLOT INFOTIC.xls
Data center Alterno	Replicación	Informe mensual replicación Mayo 2026 Informe mensual replicacion Mayo 2026.pdf Reportes diarios Mayo 2026 Replicaciones
Data Center Principal		Reporte Monitoreo ICETEX Mayo 2026-ELK Reporte Monitoreo ICETEX Mayo ELK.pdf Data ELK Disponibilidad Server ELK Mayo 2026.xlsx

Tabla 41 Anexos

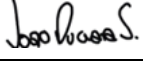
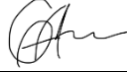
Revisión técnica

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



INFOTIC
SOLUCIONES INTELIGENTES

REVISÓ	FIRMAS
SANDRA MILENA GARCIA HERNANDEZ CONTRATISTA GRUPO DE INFRAESTRUCTURA	
JOAO DO NELSON DUCUARA CONTRATISTA GRUPO DE INFRAESTRUCTURA	
GERMAN MANUEL DIAZ CONTRATISTA GRUPO DE INFRAESTRUCTURA	

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