



INFORME DE ACTIVIDADES DEL CONTRATO

**CONTRATO NUMERO
2022-0792**

Julio 01 al 31 de 2026

versión	Observaciones	Fecha	Responsable
1.0	Versión Inicial	03/08/2026	Francisco Javier Pulido

Tabla de contenido

1.	INTRODUCCIÓN	8
2.	OBJETIVO DEL INFORME	9
3.	ALCANCE.....	10
4.	AVANCE TÉCNICO	11
4.1.	CONECTIVIDAD Y RED DE COMUNICACIONES.....	11
4.1.1.	CANALES INSTALADOS EN EL MES Y ENTREGABLES.....	13
4.1.2.	RECOMENDACIONES.....	14
4.2.	CENTRO DE DATOS	15
4.2.1.	CENTRO DE DATOS PRINCIPAL	15
4.2.1.1.	APLICACIONES.....	15
4.2.1.2.	BASES DE DATOS	19
4.2.1.3.	SITIO WEB “PORTAL ICETEX”	23
4.2.2.	CENTRO DE DATOS ALTERNO.....	26
4.2.2.1.	HOSTING VIRTUAL (IAAS)	26
4.2.2.2.	DATA GUARD BASES DE DATOS MEGACENTER	28
4.2.2.3.	SERVICIOS DE HOUSING – DATACENTER ALTERNO	29
4.2.3.	CONCLUSIONES.....	29
4.3.	SEGURIDAD INFORMÁTICA	30
4.3.1.	GESTIÓN Y FORTALECIMIENTO DE LA SEGURIDAD PERIMETRAL	32
4.3.2.	MONITOREO DE SEGURIDAD Y RESPUESTA ANTE INCIDENTES	32
4.3.3.	GESTIÓN OPERATIVA Y SOPORTE DE SEGURIDAD	32
4.3.4.	PLATAFORMAS ADMINISTRADAS	32
4.3.4.1.	FORTIGATE TRIARA	34
4.3.4.2.	FORTIGATE AGUAS	36
4.3.4.3.	FORTIGATE MEDELLÍN	38
4.3.4.4.	FORTIWEB 2000F	38
4.3.4.5.	FORTIWEB 2000E	38
4.3.4.6.	FORTIWEB CLOUD DRP	39
4.3.4.7.	FORTISANDBOX	39
4.3.4.8.	FORTISIEM	40
4.3.4.9.	SOPHOS ENDPOINT.....	41
4.3.4.10.	SIEM.....	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	46
4.3.6.2.3.	AMENAZAS DE CIBERSEGURIDAD.....	46
4.3.6.3.	THREAT HUNTING	46
4.3.6.4.	ANÁLISIS DE MARCA OSINT	47
4.3.7.	ANÁLISIS DE VULNERABILIDADES ICETEX.....	50
4.3.7.1.	USO DE SERVICIOS CON VERSIONES VULNERABLES CONOCIDAS	51
4.3.7.2.	RECOMENDACIONES DERIVADAS	52
4.3.7.3.	CONCLUSIONES.....	52
4.4.	SERVICIOS DE NUBE	53
4.4.1.	PRINCIPALES ACTIVIDADES Y LOGROS DEL MES.....	54
4.4.2.	CONCLUSIONES.....	54
4.4.3.	RECOMENDACIONES.....	54
5.	GESTION DE LA EJECUCIÓN CONTRACTUAL.....	55
6.	GESTION PRESUPUESTAL	55
7.	GESTION ADMINISTRATIVA	57
7.1.	PROFESIONALES	57
8.	SERVICIO DE COLABORACIÓN	57
9.	GESTION DE RIESGOS Y PROBLEMAS	59
10.	INDICADORES CLAVE DE DESEMPEÑO	59
10.1.	ANS POR DISPONIBILIDAD DE CANALES DE COMUNICACIONES	59
10.1.1.	CANAL DE REPLICACIÓN (TRIARA – MEGACENTER)	60
10.2.	ANS POR DISPONIBILIDAD DE SERVIDORES	60
10.2.1.	DISPONIBILIDAD TRIARA PARA LOS SERVICIOS DE PÁGINA WEB ICETEX	60
10.2.2.	ANÁLISIS COMPONENTE LIFERAY PRODUCCIÓN	65
10.2.3.	BACKUP SERVIDORES TRIARA	66
11.	CONTROL DE CAMBIOS	68
12.	PLAN DE TRABAJO DE LOS PROXIMOS MESES	69
13.	RECOMENDACIONES DEL CONTRATISTA AL ICETEX	69
13.1.	NETWORKING	69
13.2.	APLICACIONES.....	70

13.3.	SEGURIDAD	70
13.4.	BASES DE DATOS	71
13.5.	INTEGRADOR DE NUBE.....	71
14.	EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC	72
14.1.	AUMENTO DE LA CAPACIDAD DE ANCHO DE BANDA EN ALGUNAS DE LAS SEDES DE LA ENTIDAD.....	72
14.2.	TB DE CAPACIDAD DE ALMACENAMIENTO	72
14.3.	“WIFI” PARA LA GENTE EN 14 SEDES	73
15.	CONCLUSIONES	74
16.	ANEXOS.....	75

Indice de Tablas

TABLA 1 CASOS ATENDIDOS NETWORKING ULTIMO SEMESTRE	14
TABLA 2 CASOS ATENDIDOS ESPECIALISTAS DE SOLUCIONES MES JULIO	15
TABLA 3 VIGENCIA DE LOS CERTIFICADOS DIGITALES	17
TABLA 4 INVENTARIO PRINCIPALES SERVIDORES PRODUCCIÓN	18
TABLA 5 SERVIDORES Y SCHEMAS ADMINISTRADOS	19
TABLA 6 ESTADO BD ORACLE	19
TABLA 7 CRECIMIENTO DE LAS BASES DE DATOS EN LOS ÚLTIMOS 8 MESES.....	23
TABLA 8 TOP 10 PORTALES MÁS UTILIZADOS.....	25
TABLA 9 ESTADO LICENCIAMIENTO PORTAL WEB ICETEX	25
TABLA 10 SERVICIOS REPLICADOS – DATACENTER ALTERNO-MEGACENTER.....	27
TABLA 11 TOP 5 MÁQUINAS MAYOR TASA DE TRANSFERENCIA.....	27
TABLA 12 TOP 5 MÁQUINAS MENOR TASA DE TRANSFERENCIA.....	27
TABLA 13 DISPONIBILIDAD DE SERVICIOS DE HOUSING – DATA CENTER ALTERNO	29
TABLA 14 DETALLE PLATAFORMAS SEGURIDAD ADMINISTRADAS INFOTIC	33
TABLA 15 LICENCIAMIENTO FORTIGATE	33
TABLA 16 LICENCIAMIENTO FORTIWEB.....	39
TABLA 17 CONFIGURACIÓN FORTISANDBOX 1000D	40
TABLA 18 RECOMENDACIONES DE SEGURIDAD	44
TABLA 19 COMPARATIVO – INDICADORES DE COMPROMISO	45
TABLA 20 TOTAL DE CASOS GESTIONADOS SOC.....	49
TABLA 21 ACTIVOS FALTANTES.....	51
TABLA 22 COMPORTAMIENTO DE COSTOS (JUNIO - JULIO) 2026	53
TABLA 23 COMPORTAMIENTO DE COSTOS POR SERVICIO (JUNIO - JULIO) 2026	53
TABLA 24 EJECUCIÓN PRESUPUESTAL	56
TABLA 25 PERFILES Y ACTIVIDADES	57
TABLA 26 GRUPO ADMINISTRATIVO	57
TABLA 27 DISTRIBUCIÓN MÓDULOS DE VIDEOCONFERENCIA POR SEDE	58
TABLA 28 DISPOSITIVOS EN HOUSING – DATACENTER PRINCIPAL.....	60
TABLA 29 DISTRIBUCIÓN TRIMESTRAL DE ACCESO POR USUARIOS.....	61
TABLA 30 RESUMEN COMPORTAMIENTO DE BACKUPS JULIO	67
TABLA 31 CONTROLES DE CAMBIO ENERO.....	68
TABLA 32 PLANES DE TRABAJO	69
TABLA 33 CAPACIDADES DE ALMACENAMIENTO CONTRATADO.....	73
TABLA 34 CAPACIDADES DE ALMACENAMIENTO APROVISIONADO	73
TABLA 35 WIFI PARA LA GENTE INSTALADOS.....	74
TABLA 36 ANEXOS	76

Índice de Ilustraciones

ILUSTRACIÓN 1 DISPONIBILIDAD DEL CLÚSTER	12
ILUSTRACIÓN 2 DISPONIBILIDAD DEL CLUSTER	20
ILUSTRACIÓN 3 DISPONIBILIDAD DE LAS BASES DE DATOS PRINCIPALES ICTXCYC Y APOTEOSYS	21
ILUSTRACIÓN 4 CASOS DEL PROYECTO GESTIONADOS ARANDA BASES DE DATOS	22
ILUSTRACIÓN 5 UPTIME: PORTAL WEB WEB.ICETEX.GOV.CO [100%]	24
ILUSTRACIÓN 6 TRÁFICO GENERAL DE LOS PORTALES	24
ILUSTRACIÓN 7 REPORTES DE REPLICACIÓN SRM A SITIO ALTERNO – JULIO 2026	26
ILUSTRACIÓN 8 FECHAS CON MAYOR REPLICACIÓN.....	28
ILUSTRACIÓN 9 EVIDENCIA DATAGUARD REPLICADO A MEGACENTER BD	29
ILUSTRACIÓN 10 DIAGRAMA DE LA ARQUITECTURA DE SEGURIDAD.....	31
ILUSTRACIÓN 11 TOPOLOGÍA DE WAF CLOUD USADO EN PORTALES DE MEDELLÍN	31
ILUSTRACIÓN 12 CONSUMO CANAL MPLS - PROMEDIO 140MPPSG [INR0185 CLARO(MPLS_DC)]	34
ILUSTRACIÓN 13 CONSUMO CANAL INTERNET SEDES - PROM 120 MBPS WAN-SEDES-ICETEX [INR0264 (INTE_SEDES_ICTX)]	34
ILUSTRACIÓN 14 CONSUMO CANAL INTERNET DATACENTER [INTERNET_DC_INR0000320 (INET_CLARO)]	35
ILUSTRACIÓN 15 FILTRADO – WEB – (FORTIGATE – TRIARA)	35
ILUSTRACIÓN 16 INSPECCIÓN – SSL – (FORTIGATE – TRIARA)	36
ILUSTRACIÓN 17 ANTIVIRUS Y ANTIMALWARE – PERIMETRAL (FORTIGATE – TRIARA)	36
ILUSTRACIÓN 18 CONSUMO CANAL MPLS AGUAS - PROMEDIO 41.37 MBPS.....	37
ILUSTRACIÓN 19 FILTRADO-WEB-(FORTIGATE-AGUAS)	37
ILUSTRACIÓN 20 CONSUMO CANAL MPLS MEDELLÍN.....	38
ILUSTRACIÓN 21 TRÁFICO GENERAL DE LOS PORTALES	39
ILUSTRACIÓN 22 LICENCIAMIENTO FORTISIEM	40
ILUSTRACIÓN 23 FORTISIEM PERFORMANCE POR PROCESOS	41
ILUSTRACIÓN 24 ESTADO SEGURIDAD SOPHOS	42
ILUSTRACIÓN 25 ESTADO PLATAFORMA SIEM	42
ILUSTRACIÓN 26 INCIDENTES POR TIPO DE AMENAZA	47
ILUSTRACIÓN 27 INCIDENTES POR FRAUDES DIGITALES.....	47
ILUSTRACIÓN 28 INCIDENTES POR FUGA DE DATOS.....	48
ILUSTRACIÓN 29 INCIDENTES MÓDULO DEEP & DARK WEB	49
ILUSTRACIÓN 30 TOTAL HALLAZGOS ANÁLISIS DE VULNERABILIDADES.....	52
ILUSTRACIÓN 31 MÉTRICA DE VISITANTES PORTAL WEB WEB.ICETEX.GOV.CO.....	61
ILUSTRACIÓN 32 MÉTRICA ADQUISICIÓN USUARIOS PORTAL WEB WEB.ICETEX.GOV.CO	62
ILUSTRACIÓN 33 MÉTRICA DE USUARIO POR PAÍS - PORTAL WEB WEB.ICETEX.GOV.CO	62
ILUSTRACIÓN 34 MÉTRICA DE CIUDADES DE COLOMBIA- PORTAL WEB WEB.ICETEX.GOV.CO	63
ILUSTRACIÓN 35 NODO 1 CPU	64
ILUSTRACIÓN 36 NODO 1 MEMORIA	65
ILUSTRACIÓN 37 NODO 1 ALMACENAMIENTO	65
ILUSTRACIÓN 38 EVIDENCIA BACKUP SERVIDORES RESUMEN GENERAL BACKUPS	66
ILUSTRACIÓN 39 EVIDENCIA BACKUP SERVIDORES RESUMEN BACKUPS Y SU ESTADO	67

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 1 y el 31 de julio de 2026. Para tal fin se cuenta con la información generada por el grupo de 10 especialistas y 3 profesionales administrativos, con los cuales se soportan y garantizan la atención de servicios especializados descritos en el alcance del proyecto, como son:

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

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

- Firma del Acta de Inicio suscrita el 30 de diciembre del 2022, con fecha de iniciación del 19 de enero del 2023. Cumplida al 100%.
- Fase de Transición. Que comprendió desde el 19 de enero hasta el 31 de Marzo de 2023. Esta fase se encuentra cumplida al 100%.
- Fase de operación. La etapa inicial, comprendida entre el 1 de 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 que inicio el 20 de Abril presenta un avance del 42% de ejecución.

La entidad se encuentra operando sobre infraestructura tecnológicamente envejecida que requiere un plan formal de renovación tecnológica priorizada:

- Equipos de red con más de 15 años.
- Infraestructura en estado EOL/EOS.
- Sistemas operativos obsoletos.
- Aplicaciones sobre .NET Classic sin soporte vigente.

Esto genera:

- Mayor exposición a vulnerabilidades.
- Incremento de incidentes.

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.
- Dependencia de soporte limitado.
- Posibles incompatibilidades futuras

La infraestructura de conectividad evidencia altos niveles de cobertura:

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

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 crítica.

La estrategia 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.

- 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 julio 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.

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

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 julio 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 Alternos 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

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

Durante el presente periodo y a fin de destacar se atendieron un total de 16 solicitudes, con respecto al mes anterior hubo un decremento de 1 caso ya que se atendieron 17 solicitudes en el mes anterior.

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

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

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

[inventario de equipos.xlsx](#)

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

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

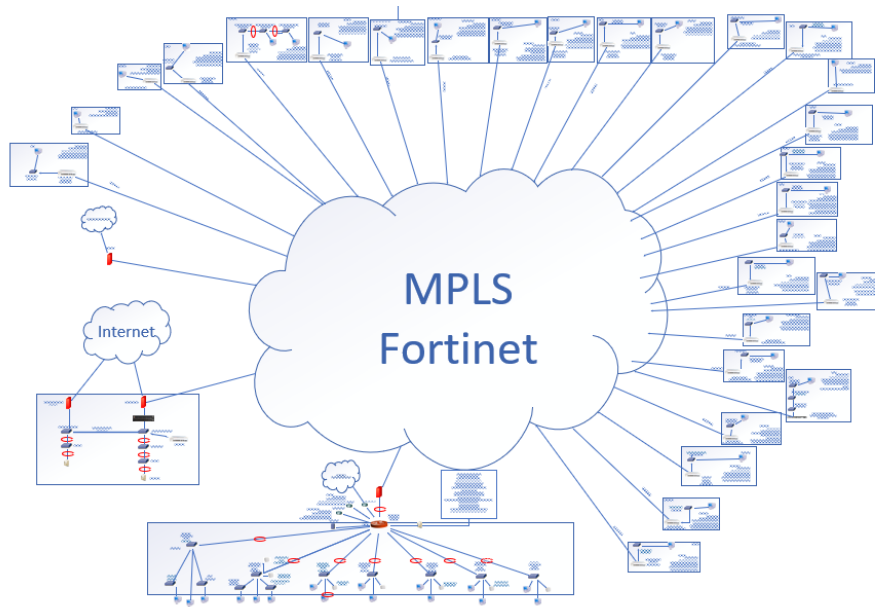


Ilustración 1 Disponibilidad del clúster

TOPOLOGIAS DE AGUAS

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

Se informa que se han adelantado las actividades técnicas necesarias para implementar el cifrado en la totalidad de los canales de comunicación, logrando avances significativos en el cumplimiento de este objetivo. No obstante, a la fecha persisten dificultades asociadas a la configuración del equipo ALLOT, las cuales han impedido culminar la implementación integral del esquema de cifrado.

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 consecuencia, se continúa trabajando en el análisis y ajuste de dicha configuración, con el fin de superar las limitaciones identificadas y completar el proceso conforme a los requerimientos técnicos y de seguridad establecidos.

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 han instalado 40 de los 43 canales MPLS principales definidos en la línea base del contrato. De los tres canales pendientes, uno corresponde al enlace entre el sitio principal e ICETEX – Dirección General (Aguas), cuya implementación fue descartada por la Entidad. Los dos restantes están asociados a sedes donde ICETEX actualmente no cuenta con operación (Barrancabermeja y San Gil), por lo que su instalación no procede.

En consecuencia, se puede afirmar que el 100% de los canales principales requeridos para las sedes activas contempladas en la línea base ha sido implementado.

Canales de Backup. De los 32 canales de Backup previstos en la línea base, se han instalado 30, lo que representa un avance del 96,55%. No obstante, el porcentaje efectivo de cumplimiento puede considerarse del 100%, debido a que los dos canales pendientes correspondían al respaldo para la sede de Quibdó y al enlace entre el sitio principal e ICETEX – Dirección General (Aguas), los cuales fueron descartados formalmente por ICETEX y, por tanto, no hacen parte del alcance ejecutable del proyecto.

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 Julio 2026.pdf](#)

Solicitudes Nuevas Instalación de canales. En el periodo no se han recibido solicitud de instalación de nuevos canales.

Los casos atendidos durante el mes están disponibles en el siguiente enlace: [Registro Aranda Julio 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
Febrero	16
Marzo	8
Abril	20
Mayo	18
Junio	17
Julio	16

Tabla 1 Casos atendidos Networking ultimo semestre

El área de Seguridad y Networking ha estado trabajando en conjunto con la empresa ComWare para realizar las pruebas de implementación de navegación IPv6. En este proceso, se configuraron las interfaces MPLS en todas las sedes para habilitar la comunicación entre ellas a través de IPv6. Adicional se realizará pruebas de conexión con los PCs de los funcionarios para probar la navegación en las sedes en IPv6 se cuenta con un Check List el cual fue abalado por el área de tecnologías de ICETEX.

4.1.2. Recomendaciones

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

Reemplazo de Equipos Dañados: Se informa a ICETEX que actualmente no se dispone de equipos de red adicionales para realizar reemplazos. En caso de presentarse nuevas fallas, esta limitación podría afectar los tiempos de respuesta y la continuidad del servicio, por lo que se recomienda evaluar la adquisición de equipos de respaldo.

Renovación y Certificación de Cableado: Se recomienda realizar la renovación o sustitución del cableado en diversos puntos de la entidad, dado que la infraestructura actual presenta un alto nivel de obsolescencia. Así mismo, se sugiere llevar a cabo la certificación del nuevo cableado, con el fin de garantizar su calidad, desempeño y cumplimiento de los estándares técnicos requeridos.

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

Como soporte de la gestión efectuada, cada actividad cuenta con su respectiva evidencia en formato PDF, permitiendo validar su ejecución y cierre conforme a los procedimientos y lineamientos establecidos por la organización, como se aprecia a continuación:

#	Fecha	Actividad	Estado	Evidencias
1	1/07/2026	Tarea TK-GAccesos-40201 – Solicitud de autorización de acceso servidor 10.1.18.65	Solucionado	Tarea TK-GAccesos-40201 – Solicitud de autorización de acceso servidor 10.1.18.65.pdf
2	3/07/2026	Tarea TK-GAccesos-40998 – Solicitud de acceso al servidor 10.1.18.65	Solucionado	Tarea TK-GAccesos-40998 – Solicitud de acceso al servidor 10.1.18.65.pdf
3	15/07/2026	Tarea TK-SoporteTI-43498 – Configuración de Google Recaptcha para el dominio de producción	Solucionado	Tarea TK-SoporteTI-43498 – Configuración de Google Recaptcha para el dominio de producción.pdf
4	16/07/2026	Tarea TK-SoporteTI-44228 – Ejecutar ETL de carga de datos diarios	Solucionado	Tarea TK-SoporteTI-44228 – Ejecutar ETL de carga de datos diarios.pdf
5	21/07/2026	Tarea TK-SoporteTI-44898 – Ejecutar ETL de carga de datos diarios	Solucionado	Tarea TK-SoporteTI-44898 – Ejecutar ETL de carga de datos diarios.pdf
6	22/07/2026	Tarea TK-SoporteTI-45413– Ejecutar ETL de carga de datos diarios	Solucionado	Tarea TK-SoporteTI-45413– Ejecutar ETL de carga de datos diarios.pdf

Tabla 2 Casos atendidos Especialistas de Soluciones mes Julio

Las actividades desarrolladas estuvieron enfocadas principalmente en:

4.2.1.1.1. Actualización y publicación de archivos en producción:

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

4.2.1.1.2. Gestión de incidentes y soporte técnico:

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

4.2.1.1.3. Gestión de accesos y permisos

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

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

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

El inventario de los servidores con los servicios que allí se prestan, puede ser consultado en el siguiente enlace [Revision IIS Julio2026.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.

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

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

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

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

Tabla 3 Vigencia de los certificados digitales

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

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

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

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



INFOTIC
SOLUCIONES INTELIGENTES

Servidor	Site Web	App Pool	Estado	Puerto(s)	Certificado SSL	Seguridad (headers)	Logging	Framework	Reciclaje	Actualización / Alta	Worker Processes
ICTSRVNETCOR01 (192.168.51.165)	AliviosyestmulosApi	AliviosyestmulosApi	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 29h	Ultima act. 15/08/2024	1
	ApiliviosSimulador	ApiliviosSimulador	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 29h	Ultima act. 13/09/2024	1
	ApiliviosiderManejo	ApiliviosiderManejo	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 29h	Ultima act. 31/03/2025	1
	Apiliviosiduc	Apiliviosiduc	Activo	6370	N/A	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 7:00 AM, 10:00 AM, 1:00 PM, 4:00 PM	Ultima act. 02/04/2025	1
	CaragueArchivos	ICTEX_CaragueArchivos	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	NO, 10:00 AM, 11:00 AM, 1:00 PM, 3:00 PM	Sin cambios	1
	CondicionesEIS	WebSiteCondicionesEIS	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 19/04/2024	1
	Condiciones	WwCondiciones	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 29h	Ultima act. 28/11/2023	1
	CondicionesVFA	WebSiteCondicionesVFA	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 4:00 AM	Sin cambios	1
	ConsultasBeneficios	ConsultasBeneficiosFront	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	No	Sin cambios	1
	ConsultasBeneficiosAPI	ConsultasBeneficiosAPI	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 29h	Sin cambios	1
	CuentasAbandonadas	WebSiteCuentasAbandonadas	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 6:00 AM	Sin cambios	1
	CuentasActivas	CIAPAPI	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	100 AM, 1:00 AM, 1:30 PM, 3:00 PM, 5:00 PM	Ultima act. 19/03/2025	1
	CuentasActivasFront	CIAPFront	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	No	Ultima act. 17/12/2024	1
	CuentasActivasPreCIAP	CIAPPreCI	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 29h	Ultima act. 3/4/2024	1
	CuentasActivasPreCIAPFront	CIAPPreCIFront	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	No	Ultima act. 3/4/2024	1
	DatosContacto	DatosContacto	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 29h	Ultima act. 31/03/2024	1
	EnvioNotificacion	EnvioNotificacion	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	No	Ultima act. 18/12/2024	1
	EisFuturo	WebSiteEisFuturo	Inactivo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	No	Sin cambios	1
	FormularioVDES	FormularioVDES	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	No	Sin cambios	1
	IMAI	WebServiceIMAI	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	No	Sin cambios	1
	Institucional	WebSiteInstitucionalMicrosites	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	No	Sin cambios	1
	LegislacionEIS	LegislacionEIS	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	No	Sin cambios	1
	LogInPortalTransaccionalApi	LogInPortalTransaccionalApi	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 29h	Ultima act. 4/11/2024	1
	LogInPortalTransaccionalFront	LogInPortalTransaccionalFront	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	No	Ultima act. 4/11/2024	1
	MEACFront	MEACFront	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	No	Ultima act. 17/12/2024	1
	RegistroUsuariosAPI	WebSiteRegistroUsuariosPersonalJuridica	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 6:00 AM	Sin cambios	1
	SantafApi	SantafApi	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 29h	Sin cambios	1
	SantafFront	SantafFront	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 29h	Sin cambios	1
	ServicioApilRestCore	ServicioApilRestCore	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	No	Sin cambios	1
	ServicioApilRestTigal	ServicioApilRestTigal	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	No	Sin cambios	1
	ServicioIntegracionEntes	ServicioIntegracionEntes	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 29h	Ultima act. 4/2/2025	1
	SHREC	WebSiteSHREC	Inactivo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	No	Sin cambios	1
	TransunionAPI	TransunionAPI	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 29h	Ultima act. 9/1/2025	1
	UnidadElectronica	WebSiteUnidadElectronica	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 6:00 AM	Sin cambios	1
	WebServiceServicioPasarelaKuhki	WebServiceServicioPasarelaKuhki	Activo	443	Valido - 16/10/2025	X-Frame-Options: SAME ORIGIN	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 1/5/2024	1
	WebSiteCondiciones	WebSiteCondiciones	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 6:00 AM	Sin cambios	1
	WebSitePortalTransaccional	PortalTransaccionalWebSite	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 26/12/2024	1
	WebSitePFI	WebSitePFI	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 7/1/2025	1
	WwApiliviosiduc	WebServiceApiliviosiduc	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	AM, 11:00 AM, 1:00 PM, 2:00 PM, 3:00 PM	Sin cambios	1
	WwCondicionesEIS	WebServiceCondicionesEIS	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 29h	Ultima act. 20/04/2024	1
	WwCuentasAbandonadasAPI	WebServiceWwCuentasAbandonadasAPI	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 31/03/2024	1
	WwDynamics	ActualizacionMasivaDynamics	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 29h	Sin cambios	1
	WwGestorVDESAPI	WwGestorVDES	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	No	Sin cambios	1
	WwPasadia	WebServicePasadia	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	SI, 6:00 AM	Sin cambios	1
	WwPortalTransaccional	PortalTransaccionalWebService	Activo	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	.NET 4.0	100 AM, 1:00 AM, 1:30 PM, 3:00 PM, 5:00 PM	Ultima act. 16/04/2025	1
WwGestorDocumentalAPI	WebServiceWwGestorDocumentalAPI	Activo	443	Valido 3/12/2025	X-Frame-Options: SAME ORIGIN	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 15/08/2024	1	
WwServicioIntegracionCensol	WebServiceWwServicioIntegracionCensol	Activo	443	Valido 3/12/2025	X-Frame-Options: SAME ORIGIN	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 13/09/2024	1	
WwServicioIntegracionCensolIntegres	WebServiceWwServicioIntegracionCensolIntegres	Activo	443	Valido 3/12/2025	X-Frame-Options: SAME ORIGIN	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 31/03/2025	1	
WwApiliviosiducFront	WebServiceWwApiliviosiducFront	Activo	443	Valido 3/12/2025	X-Frame-Options: SAME ORIGIN	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 02/04/2025	1	
WwConsultasResoluciones	WebServiceWwConsultasResoluciones	Activo	443	Valido 3/12/2025	X-Frame-Options: SAME ORIGIN	SI	.NET 4.0	SI, 6:00 AM	Sin cambios	1	
WwProxCore	WebServiceWwProxCore	Activo	443	Valido 3/12/2025	X-Frame-Options: SAME ORIGIN	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 28/11/2023	1	
WwPortalTransaccionalBus	WebServiceWwPortalTransaccionalBus	Activo	443	Valido 3/12/2025	X-Frame-Options: SAME ORIGIN	SI	.NET 4.0	SI, 6:00 AM	Sin cambios	1	
WwGestorDocumental	WebServiceWwGestorDocumental	Activo	443	Valido 3/12/2025	X-Frame-Options: SAME ORIGIN	SI	.NET 4.0	SI, 6:00 AM	Sin cambios	1	
WwSfObtenerQuijas	WebServiceWwSfObtenerQuijas	Activo	443	Valido 3/12/2025	X-Frame-Options: SAME ORIGIN	SI	.NET 4.0	SI, 6:00 AM	Sin cambios	1	
WwRequestadorSFC	WebServiceWwRequestadorSFC	Activo	443	Valido 3/12/2025	X-Frame-Options: SAME ORIGIN	SI	.NET 4.0	SI, 6:00 AM	Sin cambios	1	
WwSistemas	WebServiceWwSistemas	Activo	443	Valido 3/12/2025	X-Frame-Options: SAME ORIGIN	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 19/03/2025	1	
WwServicioIntegracionMEN	WebServiceWwServicioIntegracionMEN	Activo	443	Valido 3/12/2025	X-Frame-Options: SAME ORIGIN	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 3/4/2024	1	
WwServicioIntegracionSiben	WebServiceWwServicioIntegracionSiben	Activo	443	Valido 3/12/2025	X-Frame-Options: SAME ORIGIN	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 31/03/2024	1	
WwServicioCCP	WebServiceWwServicioCCP	Activo	443	Valido 3/12/2025	X-Frame-Options: SAME ORIGIN	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 18/12/2024	1	
WwAdministrativaFondoCovid19	WwAdministrativaFondoCovid19	Activo	443	Valido 17/11/2025	NO	SI	.NET 4.0	SI, 6:00 AM	Sin cambios	1	
WwDesembolsos	WwDesembolsos	Activo	443	Valido 17/11/2025	NO	SI	.NET 4.0	CADA HORA DE 7 AM A 7 PM	Sin cambios	1	
WwCaragueMasivosEstados	WwCaragueMasivosEstados	Activo	443	Valido 17/11/2025	NO	SI	.NET 4.0	SI, 6:00 AM	Sin cambios	1	
WwReportador	WwReportador	Activo	443	Valido 17/11/2025	NO	SI	.NET 4.0	CADA 2 HORAS DE 8 AM A 8 PM	Ultima act. 4/11/2024	1	
WwReportadorMacros	WwReportadorMacros	Activo	443	Valido 17/11/2025	NO	SI	.NET 4.0	SI, CADA 60 MIN	Ultima act. 17/12/2024	1	
WwRequestadorIntegracion	WwRequestadorIntegracion	Activo	443	Valido 17/11/2025	NO	SI	.NET 4.0	SI, 6:00 AM	Sin cambios	1	
EmailCredenciales	EmailCredenciales	Activo	443	Valido 17/11/2025	NO	SI	.NET 4.0	SI, 29h	Sin cambios	1	
ApiDesembolsos	ApiDesembolsos	Activo	443	Valido 17/11/2025	NO	SI	.NET 4.0	SI, 29h	Sin cambios	1	
WebServiceWwVirec	WebServiceWwVirec	Activo	443	Valido 16/10/2025	NO	SI	.NET 4.0	SI, 6:00 AM	Sin cambios	1	
ComunidadictexApi	ComunidadictexApi	Activo	443	Valido 17/11/2025	NO	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 28/11/2024	1	
ComunidadictexFront	ComunidadictexFront	Activo	443	Valido 17/11/2025	NO	SI	.NET 4.0	SI, 6:00 AM	Ultima act. 28/11/2024	1	

Tabla 4 Inventario principales servidores producción

En el presente mes no se han efectuado ajustes a las configuraciones de hardening.

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

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

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

4.2.1.2. 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 IP1: Pública 192.1.2.70 IP2: Pública 192.1.2.71 IP3: Pública 192.1.2.72		ICTXCYC	11.0.2.0.4
		ICETEX	11.0.2.0.4
		APLICATI	11.0.2.0.4
		APOTEOSY	11.0.2.0.4
		VIGIAPRD	19.29.0.0
NODO 1	NODO 2	LIFERAY LIFERAYPDB	19.29.0.0
IP4: Pública 192.1.2.73	IP5: Pública 192.1.2.74	LANDICTX	19.29.0.0
IP6: Privada 10.20.30.11	IP7: Privada 10.20.30.21	SGDEA	19.29.0.0
IP8: Virtual 192.1.2.76	IP9: Virtual 192.1.2.77	APOTNEW	11.0.2.0.4
CALIDAD TEST		BASES DE DATOS	VERSION
GRID Infraestructure		ASM user oracle	19.13.0.0.0
192.168.51.97		APOTPRU	11.0.2.0.4
		APLICATI	11.0.2.0.4
		ICETEX	11.0.2.0.4
		VIGIAV2	11.0.2.0.4
		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		ICTXCYC	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
OEM		BASES DE DATOS	VERSION
10.1.4.96		EMCLOUD	12.2.0.1.0
PRUEBAS		BASES DE DATOS	VERSION
GRID Infraestructure		ASM user grid	19.13.0.0.0
10.1.4.95 o 10.1.4.98		APOTPRU	11.0.2.0.4
		APOTNEW	11.0.2.0.4
		APOT	11.0.2.0.4
		sicci	11.0.2.0.4
		VIGIAPRD	19.19.0.0
		ICTXQA	11.0.2.0.4
		ICTXQA19	19.19.0.0

Tabla 5 Servidores y Schemas Administrados

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

BASES DE DATOS	VERSION	TAMAÑO
ASMn user grid	19.29.0.0.0	GB
ICTXCYC	11.0.2.0.4	6.137
ICETEX	11.0.2.0.4	210
APLICATI	11.0.2.0.4	248
APOTEOSY	11.0.2.0.4	488
VIGIAPRD	19.29.0.0	249
LIFERAY LIFERAYPDB	19.29.0.0	32
LANDICTX	19.29.0.0	654
SGDEA	19.29.0.0	187

Tabla 6 Estado BD Oracle

Resultado del proceso de administración se destacan las siguientes actividades:

- Durante el presente periodo y a fin de destacar se atendieron un total de 715 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 julio de 2026.
- Se realizaron los mantenimientos de los espacios de los filesystem /oracle /grid /opt /DATOS de las maquinas donde se encuentran alojados los binarios las bases de datos para su correcto funcionamiento.
- Se validaron los respaldos de las bases de datos de los archivelog, Backups incrementales y Backups completos o full.
- Se validó la replicación de las bases de datos del Datacenter Bogotá a centro alternativo de Medellín Megacenter.
- Se realizaron las restauraciones solicitadas por ICETEX de ambiente de producción a ambiente de desarrollo (Apoteosys, ICTXCYC Core de crédito cierre mensual).

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

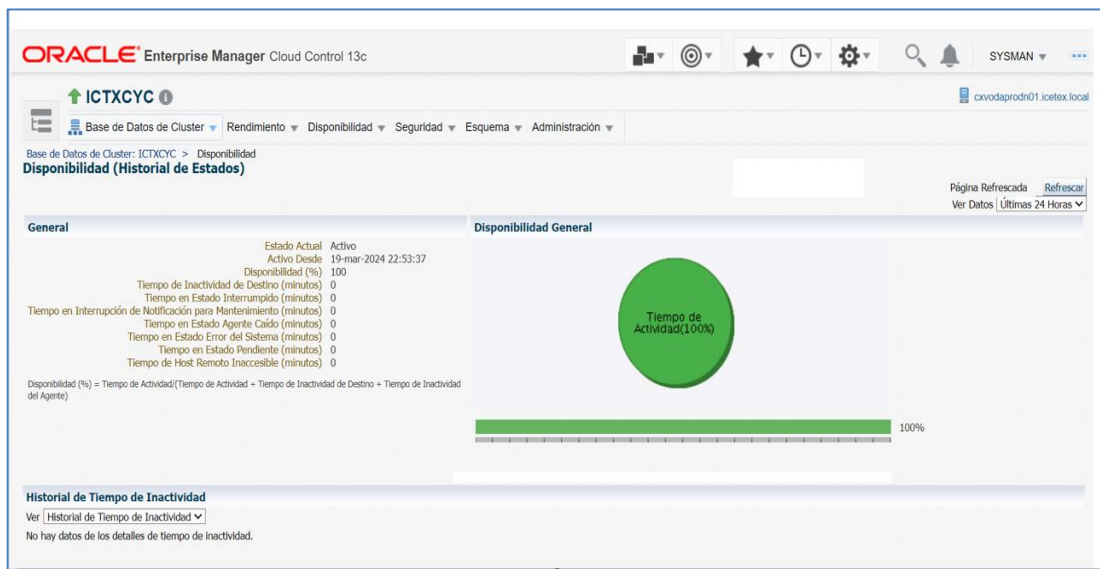


Ilustración 2 Disponibilidad del cluster

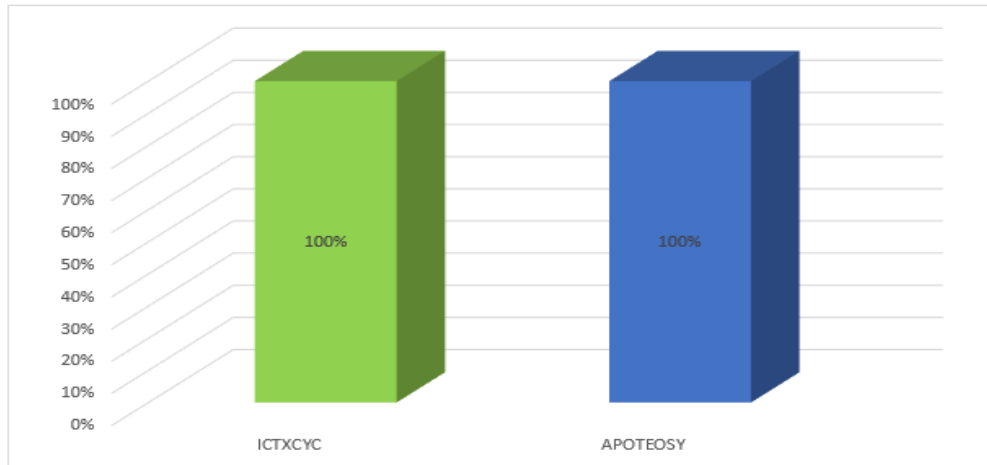


Ilustración 3 Disponibilidad de las Bases de Datos principales ICTXCYC y APOTEOSY

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 $\frac{1}{4}$ 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 ICETEX.

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.

La implementación del parche liberados por el fabricante Oracle 38291812 para el home de Oracle y de grid, están actualizados a la versión 19.29.0.0 para las bases de datos 19c servidores de producción cxvodaprodn011, cxvodaprodn021 y de contingencia cxvodacontg011

Se está programando la actualización del parche versión 19.31.0.0 para el mes de agosto, para lo cual se adelantaron pruebas en ambientes de certificación con resultados satisfactorios.

4.2.1.2.1. Casos del proyecto Gestionados por Bases de datos:

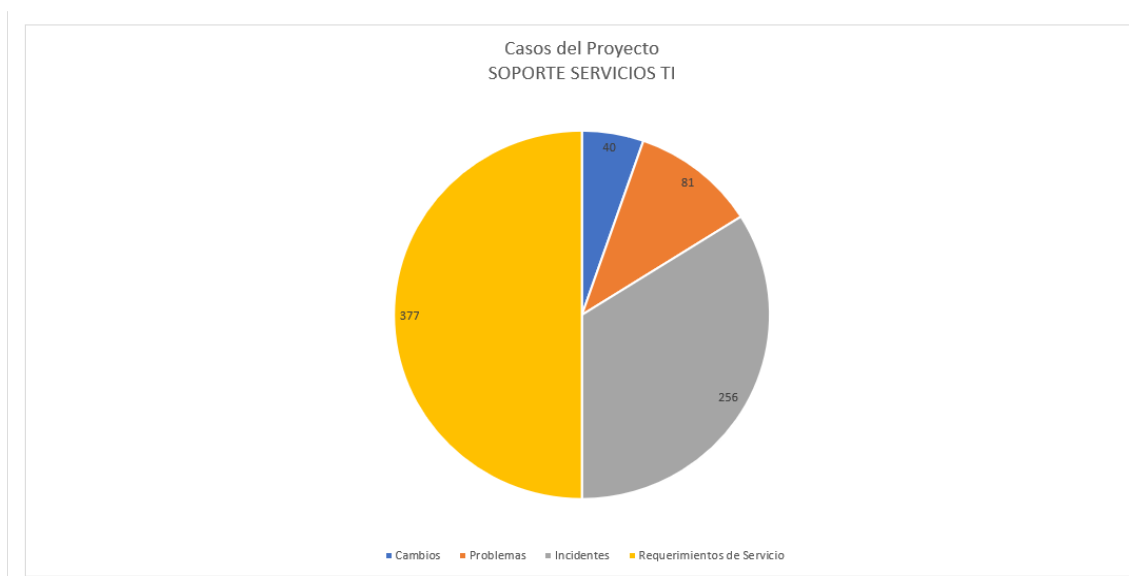


Ilustración 4 Casos del proyecto Gestionados Aranda Bases de datos

Desde Bases de datos se tienen las siguientes recomendaciones:

- Se debe aumentar los espacios de Megacenter del DataGuard por la apertura de las bases de datos para consulta.
- Sólo quedan 120G disponibles, recurso que podría alcanzar sólo para un mes de actividad.
- Se deben crear las tareas y cronologías para migrar las bases de datos que se encuentran en versión 11G fuera de soporte a la versión 19C o mayor.

4.2.1.2.2. Almacenamiento Servidores Oracle:

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

BASE DE DATOS	"DICIEMBRE 2025"	ENERO 2026	FEBRERO 2026	"MARZO 2026"	"ABRIL 2026"	"MAYO 2026"	"JUNIO 2026"	"JULIO 2026"
ICTXCYC	4,996	5,259	5,445	5,647	5,663	5,751	5,816	6,137
ICETEX	207	209	209	209	209	210	210	210
APLICATI	244	244	245	245	245	247	247	248
APOTEOSY	481	482	483	483	484	484	484	488
VIGIAPRD	188	200	211	217	230	236	245	249
LIFERAY LIFERAYPDB	8	23	23	24	30	32	32	32
LANDICTX	584	596	612	615	615	615	624	654
SGDEA	147	151	155	159	165	177	181	187
TOTAL==>	6,855.06	7,164.44	7,383.57	7,599.00	7,641.00	7,752.00	7,839.00	8,205.00
CRECIMIENTO		309.38	219.13	215.43	42.00	111.00	87.00	366.00

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

4.2.1.2.3. Replicación Bases de Datos Oracle

Durante el mes de julio de 2026 se continuó con la replicación permanente de las BD Oracle al Datacenter alternativo 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.

4.2.1.3. Sitio Web “Portal Icetex”

Durante este período, se concentraron los esfuerzos en tres áreas clave: la mejora constante de la experiencia del usuario, la optimización de la infraestructura técnica y la implementación de estrategias de contenido alineadas con las necesidades y expectativas de nuestra audiencia. Cada una de estas áreas ha exigido un enfoque cuidadoso y flexible, lo que nos ha permitido no solo cumplir con nuestros objetivos de gestión web, sino también superar diversas dificultades técnicas y de navegabilidad que surgieron.

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



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

Durante en el mes de Julio no se escalaron requerimientos al especialista WebMaster en la mesa de servicios, tampoco se gestionaron cambios.

Cabe resaltar, que las licencias de Liferay y Elasticsearch vencen en el mes de octubre, es necesario que el ICETEX comience a gestionar la renovación de las mismas.

En el mes, se presenta un promedio de 300GB de tráfico general hacia los portales protegidos por el FortiWeb donde el portal de web.icetex.gov.co y www.icetex.gov.co fueron los más utilizados en este periodo, lo cual es un comportamiento normal para este tipo de transacciones de acuerdo con la actividad de los usuarios y las convocatorias vigentes.

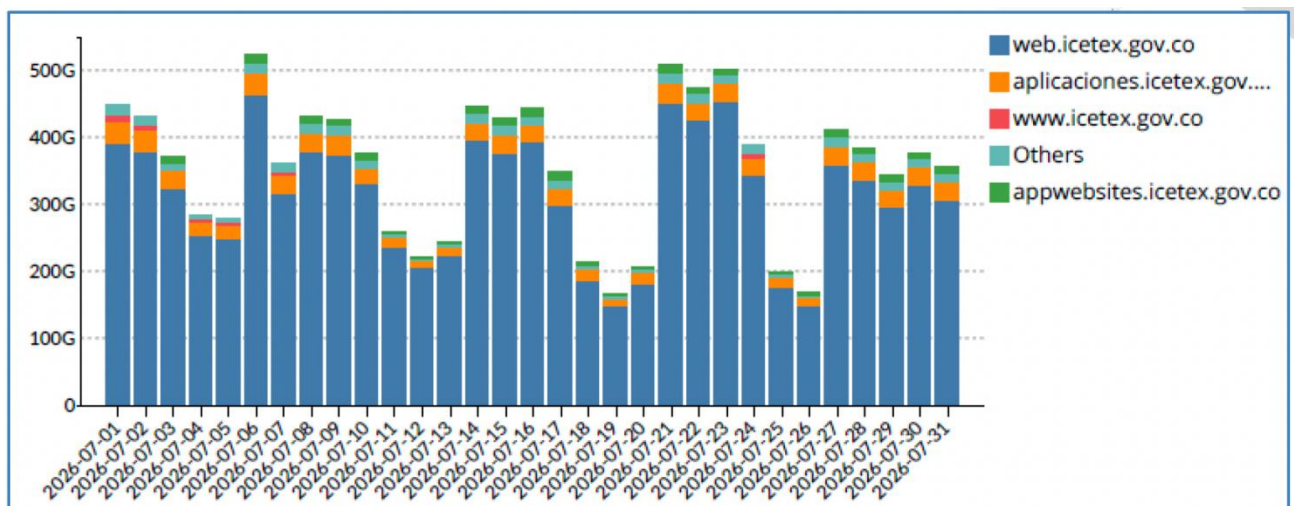


Ilustración 6 Tráfico General De Los Portales

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

#	HTTP Host	Hits	% of Total
1	web.icetex.gov.co	499,694,740	89.34%
2	aplicaciones.icetex.gov.co	34,155,539	6.11%
3	www.icetex.gov.co	17,048,812	3.05%
4	pasareladepagos.icetex.gov.co	4,264,740	0.76%
5	gestordeservicios.icetex.gov.co	2,073,340	0.37%
6	crmweb.icetex.gov.co:777	504,240	0.09%
7	appwebsites.icetex.gov.co	433,673	0.08%
8	comunidad.icetex.gov.co	359,898	0.06%
9	webhook.icetex.gov.co	302,393	0.05%
10	www.icetex.gov.co:443	51,466	0.01%

Tabla 8 Top 10 Portales más utilizados

El estado del licenciamiento es el siguiente:

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

Tabla 9 Estado Licenciamiento Portal Web Icetex

Se han adelantado las actividades técnicas necesarias para el aprovisionamiento y la configuración de un ambiente de pruebas del Portal Web sobre la infraestructura de nube de Microsoft Azure contratada por el ICETEX. Estas actividades comprenden la preparación de los recursos tecnológicos, la configuración de los componentes requeridos y la validación de las condiciones necesarias para disponer de un entorno que permita realizar pruebas funcionales, técnicas y de integración de

manera controlada, contribuyendo así a reducir riesgos antes de la implementación de cambios en el ambiente de producción.

4.2.2. Centro de Datos Alterno

4.2.2.1. Hosting Virtual (IaaS)

En el transcurso del mes de Julio, 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 Julio 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	Jul 31, 2026	678.47 MB	5 minutes
Grupo de protección: PG_INFOTIC_6 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0228_INFOTIC_REP	OK	2 of 2	Jul 31, 2026	53.38 MB	1 hour
INR0229_INFOTIC_REP	OK	1 of 1	Jul 31, 2026	82.98 MB	1 hour
Grupo de protección: PG_INFOTIC_1 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0233_INFOTIC_REP	OK	3 of 3	Jul 31, 2026	117.19 MB	1 hour
Grupo de protección: PG_INFOTIC_4 (3)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0238_INFOTIC_REP	OK	2 of 2	Jul 31, 2026	32.62 MB	1 hour
INR0239_INFOTIC_REP	OK	2 of 2	Jul 31, 2026	33.22 MB	1 hour
INR0243_INFOTIC_REP	OK	2 of 2	Jul 31, 2026	131.49 MB	1 hour
Grupo de protección: PG_INFOTIC_3 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0244_INFOTIC_REP	OK	1 of 1	Jul 31, 2026	84.82 MB	1 hour
INR0245_INFOTIC_REP	OK	1 of 1	Jul 31, 2026	8.3 MB	5 minutes
Grupo de protección: PG_INFOTIC_2 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0249_INFOTIC_REP	OK	2 of 2	Jul 31, 2026	9.63 MB	5 minutes

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

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

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
1	INR0204	Mira	Portal Web	INR0226_INFOTIC_REP
2	INR0207	ictxisgesbd	Sisgestion	INR0228_INFOTIC_REP
3	INR0206	ictxisgesapp	Sisgestion	INR0229_INFOTIC_REP
4	INR0220	icetexboglخورفو1	ORFEO	INR0233_INFOTIC_REP
5	INR0219 **	icetexboglخورفو2	ORFEO	INR0262_INFOTIC_REP
6	INR0208 *	ICTXBOGSRVPT1	Portal Transaccional	INR0236_INFOTIC_REP
7	INR0210	icetexbogliferaynfs	Portal productivo (liferay)	INR0238_INFOTIC_REP
8	INR0217	icetexbogelasticserver1	Portal productivo (liferay)	INR0239_INFOTIC_REP
9	INR0218	icetexbogliferayserver1	Portal productivo (liferay)	INR0243_INFOTIC_REP
10	INR0215	icetexboglxdarumasrv1	DARUMA	INR0244_INFOTIC_REP
11	INR0213	icetexboglxdarumasrv2	DARUMA	INR0245_INFOTIC_REP
12	INR0214	icetexboglxxroad1	XROAD	INR0249_INFOTIC_REP

Tabla 10 Servicios replicados – Datacenter Alterno-Megacenter

**Se detiene la replicación INR0208 que corresponde a la Máquina 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 -icetexboglخورفو2

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

INR	HOSTNAME	GB
INR0243	icetexbogliferayserver1	177,3
INR0226	Mira	6,2
INR0229	ictxisgesapp	2,7
INR0233	icetexboglخورفو1	2,3
INR0244	icetexboglxdarumasrv1	2,1

Tabla 11 TOP 5 máquinas mayor tasa de transferencia

INR	HOSTNAME	GB
INR0245	icetexboglxdarumasrv2	0,2
INR0249	icetexboglxxroad1	1,0
INR0238	icetexbogliferaynfs	1,1
INR0239	icetexbogelasticserver1	1,1
INR0228	ictxisgesbd	1,5

Tabla 12 TOP 5 máquinas menor tasa de transferencia

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

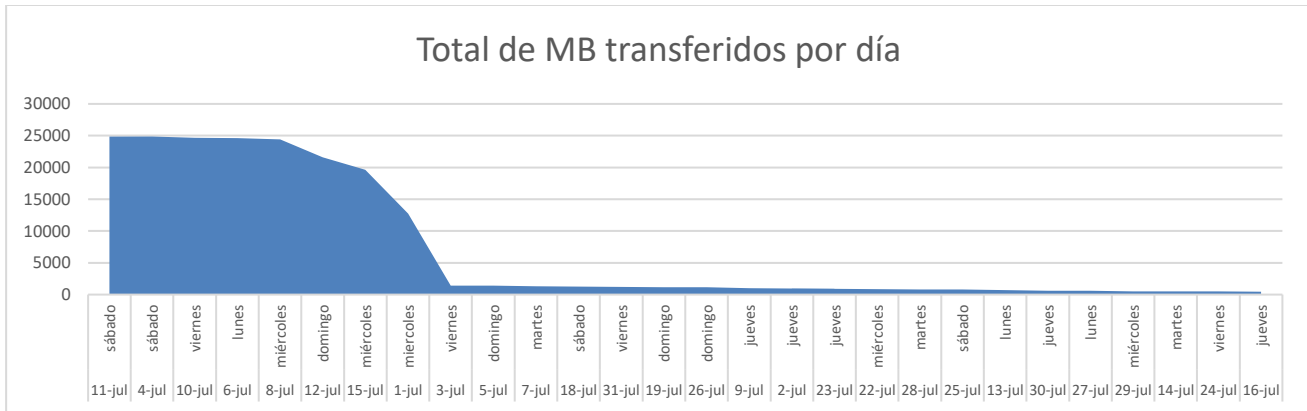


Ilustración 8 Fechas con mayor replicación

El comportamiento del tráfico de replicación durante el mes de julio 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 continua altamente concentrada en la máquina virtual INR0243, esta VM representa aproximadamente el **91% del tráfico total** del mes que fue **177,339.7 MB** (aprox. **177.3 GB**)
- El tráfico total de replicación en Julio fue de **195,573.51 MB (~195.57 GB)**.
- El **día de mayor tráfico** fue el **11 de Julio**, con un acumulado total de **24,858 MB** (principalmente por INR0243).
- El **día de menor tráfico** fue 16 de Julio (450,46 MB).

4.2.2.2. DataGuard Bases de Datos Megacenter

Durante el mes de julio de 2026 se continuo con la replicación permanente de las BD Oracle al Datacenter alternativo 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 Julio2026.pdf](#)

```

10.1.18.120 - Conexión a Escritorio remoto
oracle@cxvodacontg011:~$ ps -fea |grep pmon
oracle 1793 1 0 Jul11 ? 00:03:27 ora_pmon_LANDICTD
oracle 6363 1 0 Jul15 ? 00:02:31 ora_pmon_VIGIADTG
oracle 12780 1 0 Jul10 ? 00:04:43 ora_pmon_DBFIVOT
oracle 13289 1 0 Jul10 ? 00:03:10 ora_pmon_LIFERAYD
oracle 16792 1 0 Jul10 ? 00:03:11 ora_pmon_SGDEAD
oracle 18962 28719 0 20:27 pts/4 00:00:00 grep --color=auto pmon
grid 19787 1 0 Jul10 ? 00:02:29 asm_pmon_ASM
oracle 23294 1 0 Jul11 ? 00:04:55 ora_pmon_IXTXYCD
oracle 30158 1 0 Jul11 ? 00:04:56 ora_pmon_AFOEODS
[oracle@cxvodacontg011 ~]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.4.0 Production on Mon Aug 3 20:27:32 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 uapply

Thread Last Sequence Received Last Sequence Applied TIME RECEIVED TIME APPLIED
-----
1 355317 355317 03/08/2026 20:24 03/08/2026 20:24
2 300692 300692 03/08/2026 20:23 03/08/2026 20:23

Thread Last Sequence Received Last Sequence Applied Difference
-----
2 300692 300692 0
1 355317 355317 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 alterno en Medellín, las cuales estuvieron disponibles todo el mes de julio al 100%:

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

Tabla 13 Disponibilidad de Servicios de Housing – Data Center Alterno

4.2.3. Conclusiones

La gestión de capacidad actualmente es reactiva y no preventiva. Se requieren políticas formales de capacity planning y depuración de históricos por parte del ICETEX.

4.3. Seguridad informática

Durante el periodo del 01 al 31 de julio de 2026, se llevaron a cabo diversas actividades, relacionadas con la administración y gestión de los dispositivos de seguridad perimetral y/o antivirus de la entidad:

- Atención de requerimientos e incidentes asignados al Grupo de Seguridad Perimetral a través de la
- herramienta de gestión de casos Aranda.
- Validación y análisis de los diferentes bloqueos generados por la aplicación Sophos.
- Análisis detallado a los reportes enviados por el SOC.
- Acompañamiento en las sesiones técnicas del cliente y con los especialistas, para la resolución de incidentes o requerimientos.
- Atención a los diferentes requerimientos del Grupo de Seguridad de la información del ICETEX.

Durante el período evaluado, 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.

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

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

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

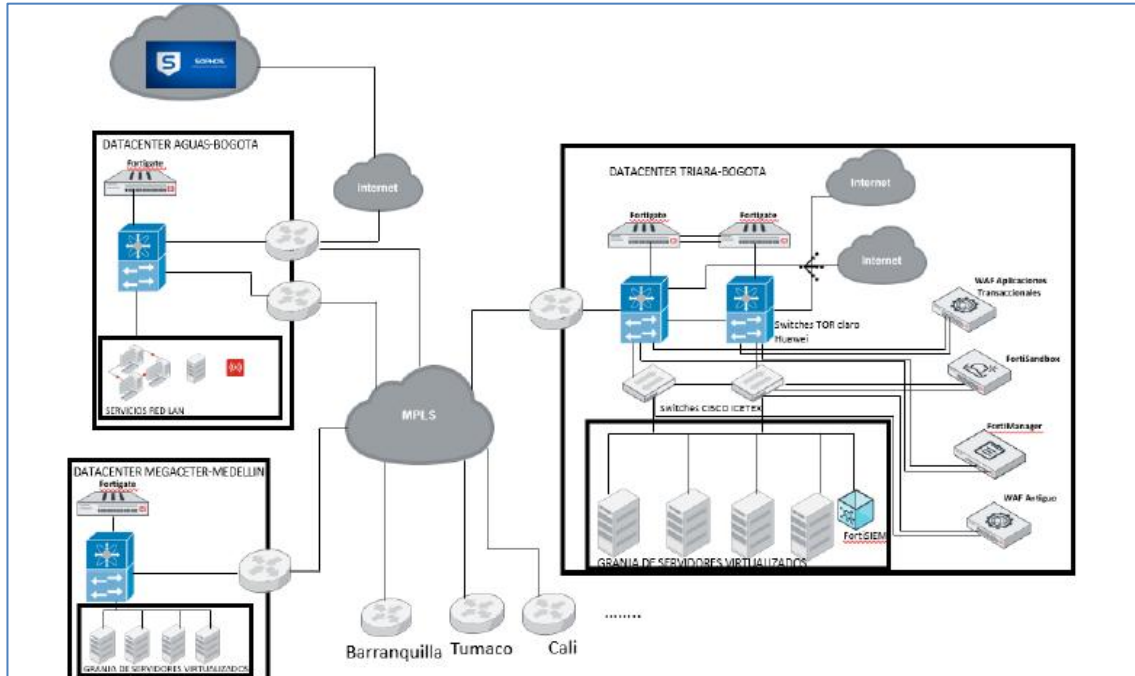


Ilustración 10 Diagrama de la Arquitectura de Seguridad

En la ilustración 11, se observa la topología correspondiente al centro de datos alterno.

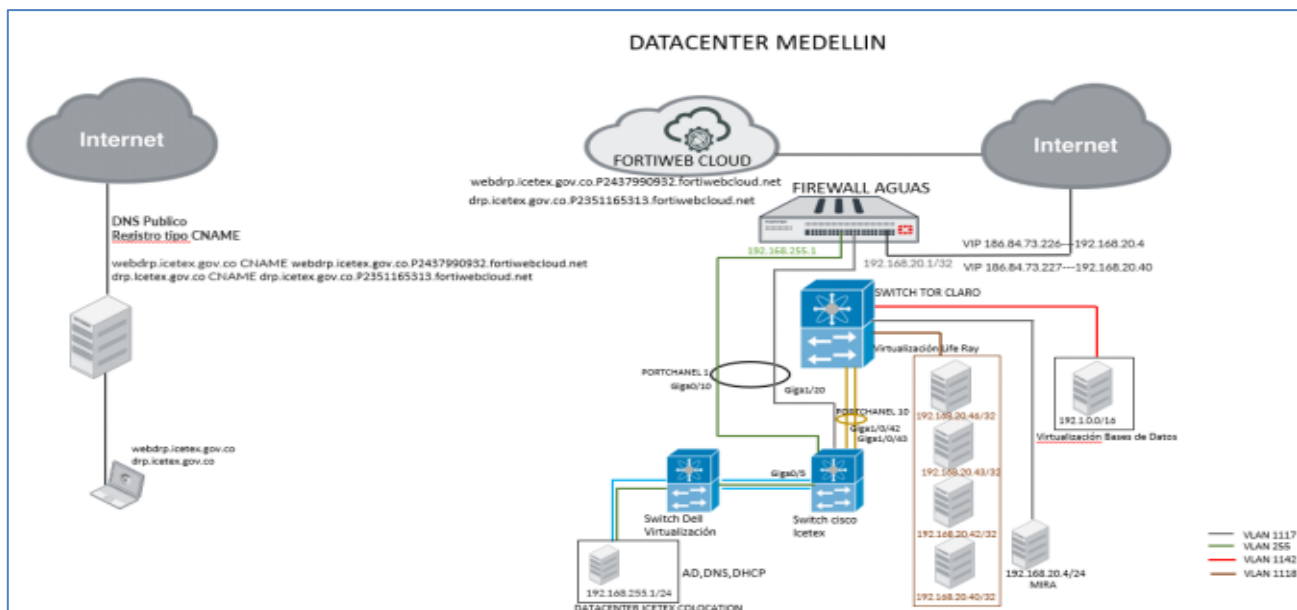


Ilustración 11 Topología de WAF Cloud usado en portales de Medellín

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

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

Las evidencias de esta gestión fueron incluidas en el numeral 6.2 del informe mensual de especialistas de seguridad del mes de julio, link: [Informe Mensual InfoTIC Seguridad Julio2026.pdf](#)

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

- Atención de requerimientos e incidentes asignados al Grupo de Seguridad Perimetral a través de la herramienta de gestión de casos Aranda.
- Validación y análisis de los diferentes bloqueos generados por la aplicación Sophos.
- Análisis detallado a los reportes enviados por el SOC.
- Acompañamiento en las sesiones técnicas del cliente y con los especialistas, para la resolución de incidentes o requerimientos.
- Atención a los diferentes requerimientos del Grupo de Seguridad de la información del ICETEX.

4.3.2. Monitoreo de seguridad y respuesta ante incidentes

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

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

4.3.3. Gestión Operativa y soporte de seguridad

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

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

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

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

Tabla 14 Detalle plataformas Seguridad administradas INFOTIC

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

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

Tabla 15 Licenciamiento FortiGate

Se advierte que el licenciamiento de los dispositivos de seguridad perimetral relacionados han expirado durante el mes de mayo y junio de 2026, situación que representa un riesgo significativo para la operación y la seguridad de la infraestructura tecnológica.

La ausencia de licencias vigentes ha impedido el acceso a actualizaciones de firmware, firmas de seguridad, servicios de prevención de amenazas y soporte del fabricante, incrementando la exposición a vulnerabilidades y afectando la capacidad de respuesta ante incidentes de ciberseguridad.

En consecuencia, se recomienda gestionar con carácter prioritario la renovación del licenciamiento de los equipos

4.3.4.1. FortiGate Triara

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

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

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

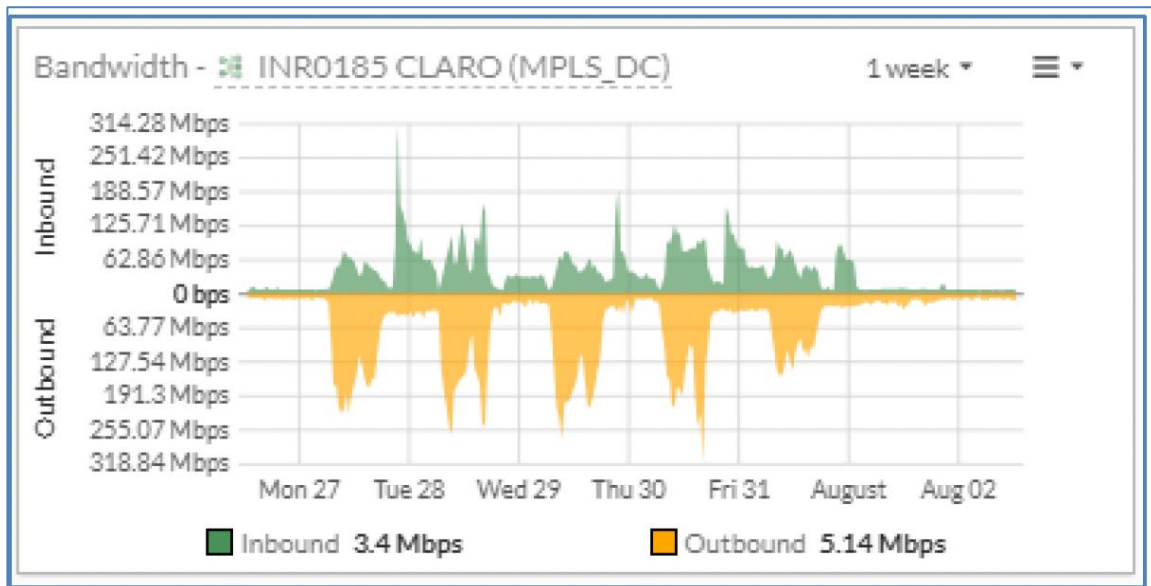


Ilustración 12 Consumo canal MPLS - promedio 140MPPSG [INR0185 CLARO(MPLS_DC)]

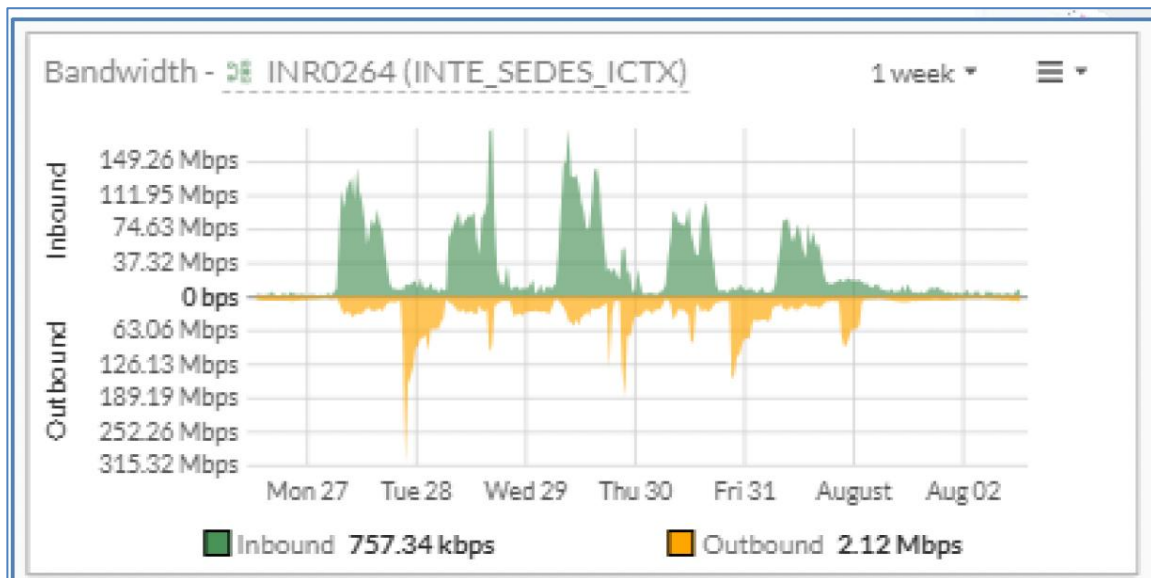


Ilustración 13 Consumo canal Internet Sedes - Prom 120 MBPS WAN-SEDES-ICETEX [INR0264 (INTE_SEDES ICTX)]

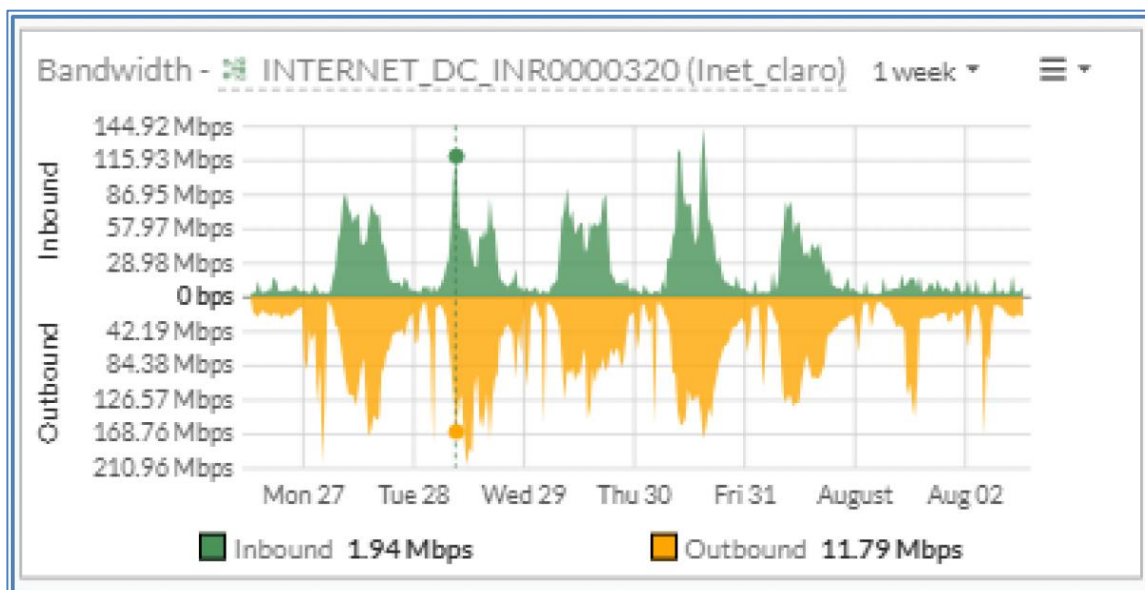


Ilustración 14 Consumo Canal INTERNET DATACENTER [INTERNET_DC_INR0000320 (Inet_claro)]

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

Name	Comments	Ref.
WEB default	Perfil con las mínimas restricciones	0
WEB Mesa_de_Ayuda	Mesa_de_Ayuda	1
WEB Navegacionpcs_Comware	Perfil con restricciones	5
WEB Navegacionpcs_Comware_con_redes	Perfil con restricciones	2
WEB WF-Avanzado	Perfil para FSSO Navegación Avanzada	35
WEB WF-Comunicaciones	Perfil para FSSO comunicaciones	4
WEB WF-General	Perfil para todos	6
WEB WF-General_Sedes	Perfil para todos	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 15 Filtrado – WEB – (FortiGate – Triara)

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 16 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 17 Antivirus y Antimalware – Perimetral (FortiGate – Triara)

4.3.4.2. FortiGate Aguas

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

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

A continuación se presentan los consumos en el presente mes:

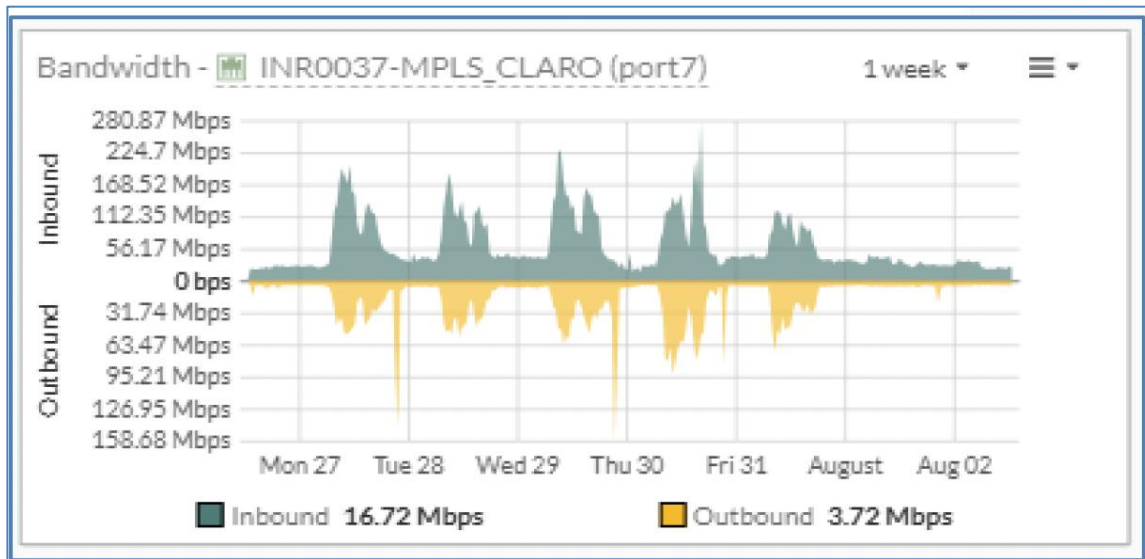


Ilustración 18 Consumo Canal MPLS Aguas - promedio 41.37 MBPS

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

Name	Comments	Ref.
WEB default	Default web filtering.	0
WEB General_Icetex		89
WEB Mesa_de_Ayuda	Mesa_de_Ayuda	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 19 Filtrado-Web-(FortiGate-Aguas)

Para el para el periodo del 01 al 31 de julio de 2026 y de acuerdo con el reporte enviado por el SOC, es necesario realizar las actualizaciones de Firmware de los equipos de Seguridad Perimetral.

Fortinet publicó 7 nuevos avisos de seguridad que abordan vulnerabilidades con distintos niveles de severidad, desde fallos de inyección de cabeceras de baja gravedad hasta desbordamientos de búfer de severidad media, incluyendo una exposición crítica por acceso VNC no autenticado. Los productos afectados corresponden a FortiOS, FortiSanbox, FortiPAM, FortiProxu. Lo indicado se detalla en los CVE-2025-62826, CVE-2025-62675, CVE-2026-59837, CVE-2026-23573, CVE-2026-59839, CVE-2025-43892 y CVE-2026-59835.

Al revisar cada uno de los CVEs, es necesario realizar la actualización del firmware de los equipos de Seguridad Perimetral de la entidad, para ello, se debe seguir la siguiente ruta de actualización de acuerdo con lo estipulado en la URL "<https://docs.fortinet.com/upgrade-tool/fortigate>":

4.3.4.3. FortiGate Medellín

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

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

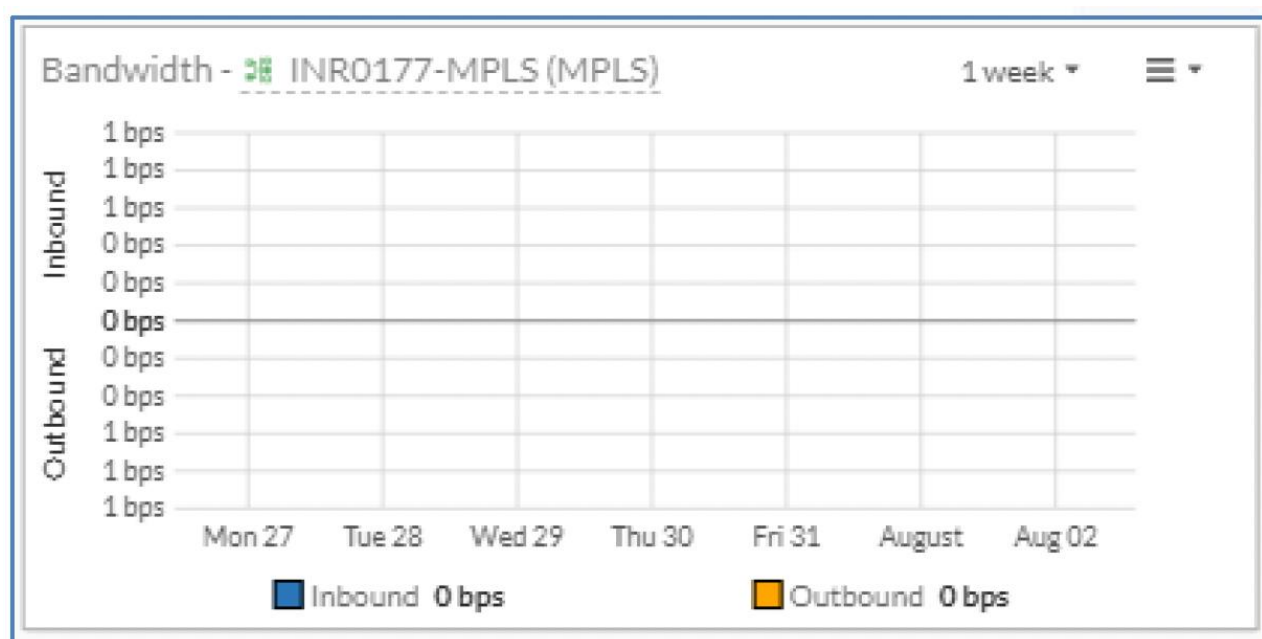


Ilustración 20 Consumo Canal MPLS Medellín

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.

4.3.4.5. FortiWeb 2000E

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

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

Tabla 16 Licenciamiento FortiWeb

Se identifica una situación que requiere atención prioritaria respecto de la plataforma de protección de aplicaciones web (WAF). Los dispositivos FortiWeb 2000E de propiedad del ICETEX presentan el licenciamiento vencido desde el 20 de junio de 2023 y, adicionalmente, alcanzaron la fecha de Last Service Extension el 13 de enero de 2026, manteniéndose únicamente con soporte hasta el 13 de enero de 2027. Esta condición limita el acceso a actualizaciones, firmas de seguridad, nuevas funcionalidades y soporte especializado, incrementando el riesgo operativo y de ciberseguridad para los servicios publicados.

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.

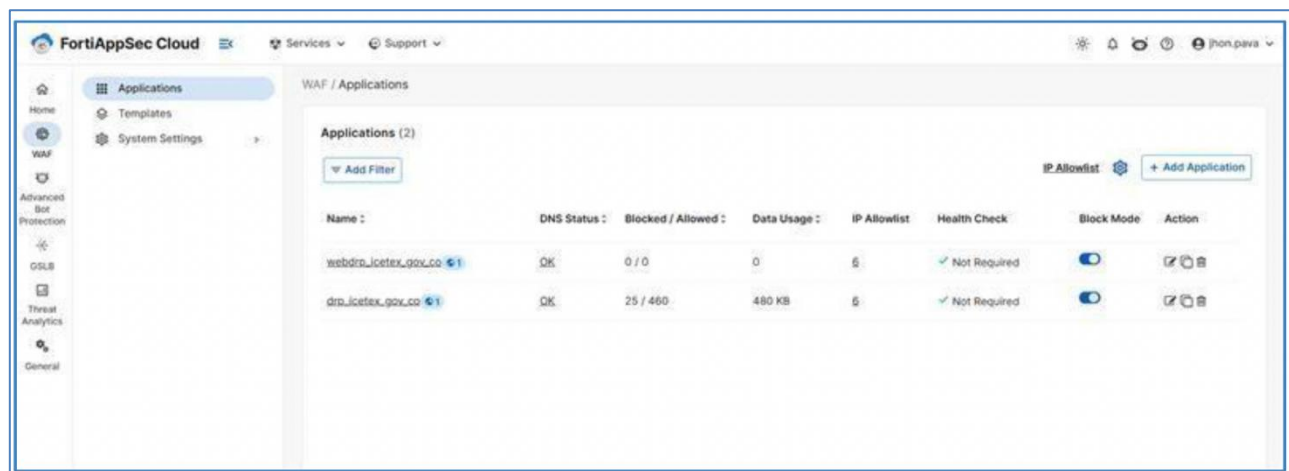


Ilustración 21 Tráfico General de los portales

4.3.4.7. FortiSandBox

A nivel de sistema, el Sandbox (FortiSandBox 1000D) muestra su configuración actual y su versión de firmware que actualmente se encuentra en la 3.2.4 siendo esta la última versión disponible para

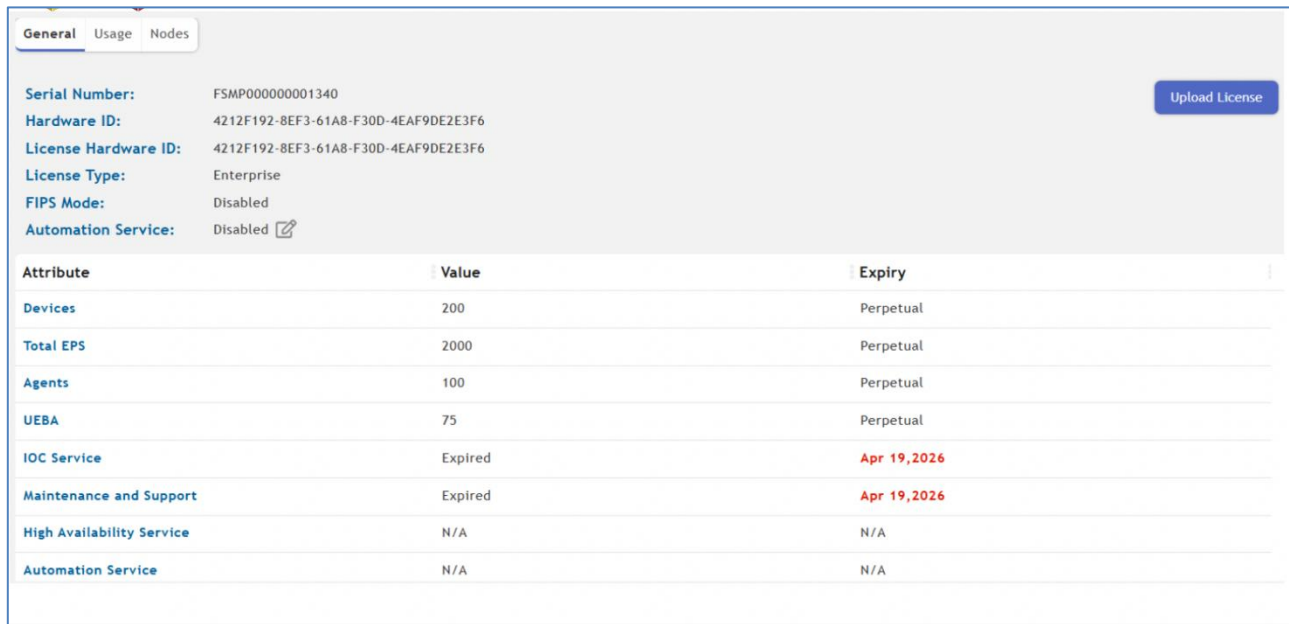
este dispositivo, ya que está en EOL (término empleado por el fabricante para describir un producto que pronto será reemplazado por una nueva generación de tecnología).

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

Tabla 17 Configuración FortiSandBox 1000D

4.3.4.8. FortiSIEM

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



The screenshot shows the FortiSIEM license management interface. It includes tabs for General, Usage, and Nodes. The General tab is active, displaying the following information:

- Serial Number:** FSMPO00000001340
- Hardware ID:** 4212F192-8EF3-61A8-F30D-4EAF9DE2E3F6
- License Hardware ID:** 4212F192-8EF3-61A8-F30D-4EAF9DE2E3F6
- License Type:** Enterprise
- FIPS Mode:** Disabled
- Automation Service:** Disabled

There is an "Upload License" button in the top right corner. Below this information is a table showing the license details:

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 22 licenciamiento FortiSIEM

A continuación, se presenta el desempeño por procesos:

Process health for FORTISIEM_ICTX (192.1.1.100)

Columns Search... Summary Mode 1/1 30

Process Name	Owner	Status	Uptime	CPU	Memory	Resident Memory	Disk Read Rate
AppSvr	admin	Up	1 hr 19 min 9 sec	10%	19%	5.74 GB	0KBps
phParser	admin	Up	1 hr 13 min 36 sec	2%	6%	1.92 GB	0KBps
phQueryMaster	admin	Up	1 hr 13 min 36 sec	0%	1%	220 MB	0KBps
phRuleMaster	admin	Up	1 hr 13 min 36 sec	0%	6%	1.82 GB	0KBps
phRuleWorker	admin	Up	1 hr 13 min 36 sec	0%	3%	897 MB	0KBps
phQueryWorker	admin	Up	1 hr 13 min 36 sec	0%	2%	625 MB	0KBps
phDataManager	admin	Up	1 hr 13 min 36 sec	0%	6%	1.89 GB	0KBps
phDiscover	admin	Up	1 hr 13 min 35 sec	0%	0%	117 MB	0KBps
phReportWorker	admin	Up	1 hr 13 min 36 sec	0%	2%	769 MB	0KBps
phReportMaster	admin	Up	1 hr 13 min 36 sec	0%	0%	131 MB	0KBps
phIdentityWorker	admin	Up	1 hr 13 min 35 sec	0%	2%	615 MB	0KBps
phIdentityMaster	admin	Up	1 hr 13 min 35 sec	0%	0%	78 MB	0KBps
phAgentManager	admin	Up	1 hr 13 min 35 sec	0%	1%	150 MB	0KBps
phPerfMonitor	admin	Up	1 hr 13 min 35 sec	0%	1%	245 MB	0KBps

Ilustración 23 FortiSIEM Performance por procesos

Se reportan riesgos asociados a FortiSIEM y almacenamiento, pero no se observa un plan formal de cierre o mitigación definitiva por parte del ICETEX.

4.3.4.9. Sophos EndPoint

Hemos efectuado revisión de los aspectos que permitan efectuar un afinamiento para un uso mas eficiente de la solución SOPHOS.

Se efectuó una verificación de las configuraciones actuales de la herramienta, con el propósito de evaluar su estado de implementación, validar los parámetros configurados e identificar posibles oportunidades de ajuste u optimización. Como resultado de esta revisión, se obtuvo un diagnóstico preliminar que servirá como base para las actividades de afinamiento y fortalecimiento de la solución, de acuerdo con las necesidades y mejores prácticas aplicables, las cuales anexamos a esta comunicación.

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 la ilustración 26, se observa un resumen del estado de Seguridad del Endpoint donde actualmente se están cumpliendo en un 55% los puntos de seguridad de la plataforma de Sophos indicando protección de equipos, políticas y exclusiones.



Ilustración 24 Estado Seguridad Sophos

En términos de políticas, Tamper protection (amenazas), exclusiones y agentes, la plataforma refleja un estado de salud óptimo.

En la sección 6.6.1 del informe de seguridad [Informe Mensual InfoTIC Seguridad Julio2026.pdf](#) se detallan las amenazas contenidas por la herramienta el Sophos instalado en los equipos ordenadores y servidores.

4.3.4.10. SIEM

La ilustración refleja la alarma correspondiente a capacidad de disco duro, cuyo porcentaje de utilización se encuentra por encima del 85%.

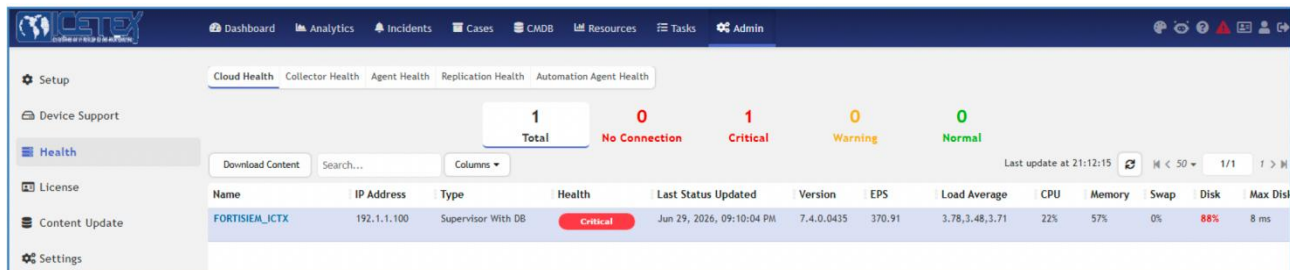


Ilustración 25 Estado Plataforma SIEM

Nuestros especialistas realizaron una serie de tareas controladas orientadas a restablecer la operación del sistema, la cual incluyó:

- Identificación del componente con mayor consumo de almacenamiento

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

- Depuración técnica de datos históricos no críticos
- Liberación progresiva de capacidad en el volumen afectado
- Validación de integridad del sistema y recuperación de servicios

Como resultado, se evidenció lo siguiente:

- Se redujo el uso del almacenamiento de 100% a 80%
- Se liberaron aproximadamente 500–600 GB de espacio
- Se restableció el comportamiento normal de la plataforma
- Se normalizaron los tiempos de procesamiento y análisis de eventos

Actualmente el sistema opera en condiciones estables y dentro de parámetros recomendados.

Con el propósito de apoyar al ICETEX en el uso y administración de la plataforma SIEM, se diseñó y presentó un plan de depuración del espacio ocupado por los registros (logs), orientado a optimizar el almacenamiento, mejorar el desempeño de la solución y garantizar una adecuada gestión de la información. La propuesta fue estructurada para que su ejecución sea técnicamente viable, auditable y alineada con las capacidades, restricciones y mejores prácticas de FortiSIEM, permitiendo establecer criterios claros para la retención, depuración y conservación de los eventos de seguridad, en concordancia con las necesidades operativas y de cumplimiento de la Entidad.

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	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

Recomendación	Estado	Criticidad	Fuente	Asunto	Personal de ICETEX a quien se notificó
susceptible a muchos tipos de amenazas.					
Validar a nivel de punto final, los equipos que se han visto involucrados con comportamiento malicioso.	Se evalúa por parte de ICETEX. Se hace seguimiento por parte del SOC quien reporta comportamiento malicioso. Sin embargo, es necesario establecer políticas de conexión de equipos externos BYOD debido a que muchos de los casos reportados por el SOC vienen de equipos personales que no hacen parte de la Entidad.	Critica	Informes Mensuales	N/A	N/A
Integrar los equipos que hacen parte del proceso de pagos con el SIEM.	Se debe evaluar la capacidad del SIEM, se espera plan de mejora.	Media	Informes Mensuales - sesiones	Recursos de FORTISIEM CPU, Memoria y disco / Recomendaciones de arquitectura de FortiSIEM Icetex	Líder infraestructura / Especialista Desarrollo / Especialista de seguridad / Especialista de seguridad / Grupo Coordinación de Infraestructura Tecnológica / Profesional de tecnología
Evaluar los riesgos sobre las plataformas en la nube y considerar aplicar plataformas de seguridad para los ambientes cloud que cuenta la entidad ya que estos contienen servicios críticos para la misma.	En evaluación por parte de ICETEX.	Alta	N/A	N/A	N/A
Se debe realizar la integración de los activos críticos de la compañía a la plataforma de SIEM, no se ha podido lograr por la falta de recursos de este.	En evaluación por parte de ICETEX.	Alta	Informes Mensuales - sesiones	Recursos de FORTISIEM CPU, Memoria y disco / Recomendaciones de arquitectura de FortiSIEM Icetex	Líder infraestructura / Especialista Desarrollo / Especialista de seguridad / Especialista de seguridad / Grupo Coordinación de Infraestructura Tecnológica / Profesional de tecnología

Tabla 18 Recomendaciones de Seguridad

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

De acuerdo con las conexiones y las reglas configuradas sobre la herramienta de monitoreo SOC FortiSIEM, el cual analiza las alertas en busca de patrones de comportamiento inusuales; estas reglas estudian y conectan las alertas para evaluar su prioridad y confiabilidad. Actualmente el motor de búsqueda de amenazas está distribuido en cuatro criterios de búsqueda y correlación, los cuales son: compromiso del sistema, explotación e instalación de agentes maliciosos, entrega y ataque, reconocimiento y sondeo y finalmente advertencia ambiental o 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
- Alertas de acceso permitido a páginas web maliciosas o de baja reputación

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

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

Para cualquier detalle relacionado con las reglas puede consultarse en el siguiente [Informe Mensual SOC-TH ICETEX Julio 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)	Julio	Junio	Mayo	Abril	Marzo	Febrero
IOC – Malware DOMINIOS	6.047	6.047	6.047	6.047	6.047	6.047
IOC – Malware IPs	11.276	11.167	11.167	11.167	11.167	11.119
IOC – Malware HASH	1.627	1.627	1.627	1.627	1.627	1.627
IOC – Malware URL	4.564	4.564	4.564	4.564	4.564	4.564

Tabla 19 Comparativo – Indicadores de Compromiso

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

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

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

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

4.3.6.2. Alertas o Incidentes de Seguridad Detectados

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

4.3.6.2.1. Categoría Seguridad

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

4.3.6.2.2. Categoría Disponibilidad

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

4.3.6.2.3. Amenazas de Ciberseguridad

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

4.3.6.3. Threat Hunting

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

4.3.6.4. Análisis de Marca OSINT

Durante el periodo evaluado, la plataforma de monitoreo de protección de marca y OSINT– AXUR, reporta un total de 611 posibles amenazas de las 35k que fueron encontradas y analizadas automáticamente por la plataforma de monitoreo. A estas 611 posibles amenazas se les realizó una revisión y análisis interno, de sus características, datos e información.

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

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

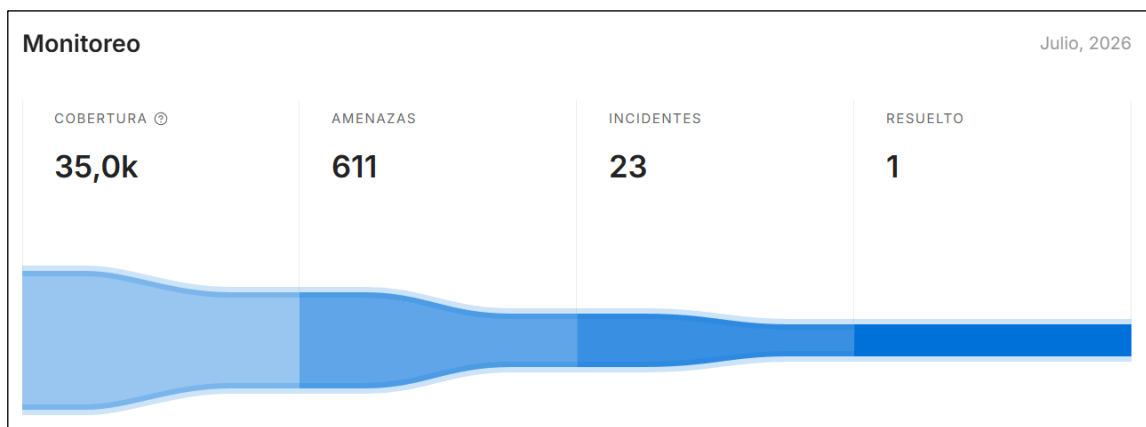


Ilustración 26 Incidentes por Tipo de Amenaza

Durante el periodo evaluado se detectó 23 incidentes de los cuales, 18 están relacionados con Perfil falso en red social, 4 relacionados con Otros datos confidenciales y 1 con Phishing.



Ilustración 27 Incidentes por Fraudes Digitales

En cuanto a fuga de datos, durante el periodo evaluado, se presentaron 566 casos, de los cuales 562 fueron clasificados como falsos positivos y posteriormente descartados, debido a una configuración implementada en los bots de búsqueda para repositorios que incrementó el número de alertas generadas sin representar un riesgo real para la entidad, los cuatro 4 casos restantes fueron validados, reportados oportunamente a la entidad y actualmente se encuentran en proceso de tratamiento por parte del Icetex.

A continuación por distribución de tipo de amenaza:

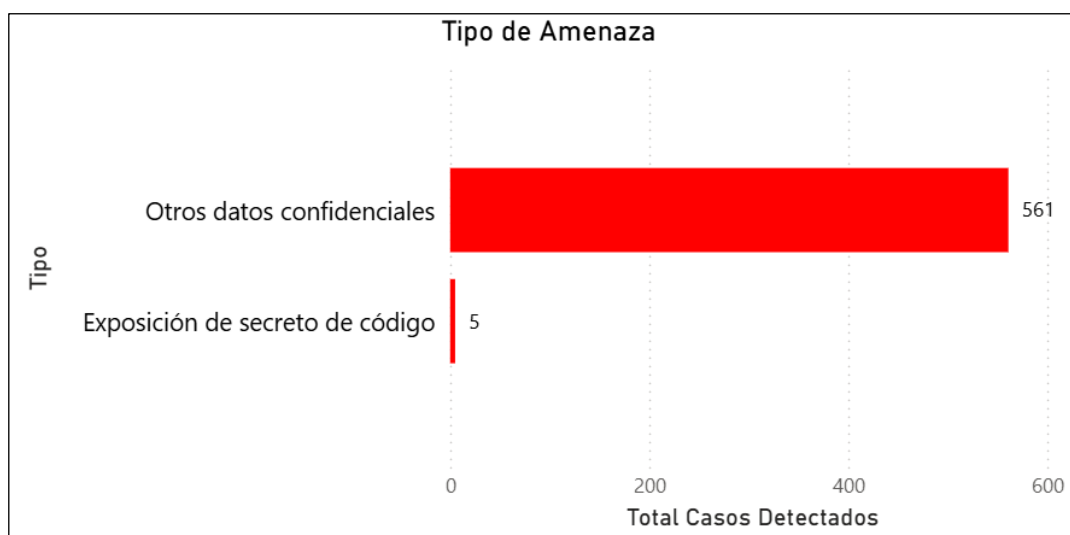


Ilustración 28 Incidentes por Fuga de Datos

Casos Relacionados con el módulo Piratería on Line. Durante el período evaluado se identificó 02 caso. Tras el análisis realizado, fue descartado, debido a que la publicación solo se mencionaba la marca sin presentar un riesgo para la entidad.

Casos relacionados con la Dark Web, Durante el periodo evaluado se registraron 4 casos los cuales corresponden a la misma fuente de información (URL) asociada a un repositorio de logs stealer previamente reportado a la entidad. En todos los casos se evidencian las mismas menciones de dominios institucionales, sin identificarse nuevos indicadores adicionales de compromiso o cambios que representen un incremento en el nivel de riesgo respecto al evento inicialmente reportado. Dado que los registros corresponden a información repetitiva del mismo hallazgo y no aportan nuevos elementos de análisis, los casos se documentan únicamente para fines de control y trazabilidad, procediendo con su cierre. A continuación, se presenta la tipología de amenazas identificadas en este módulo.

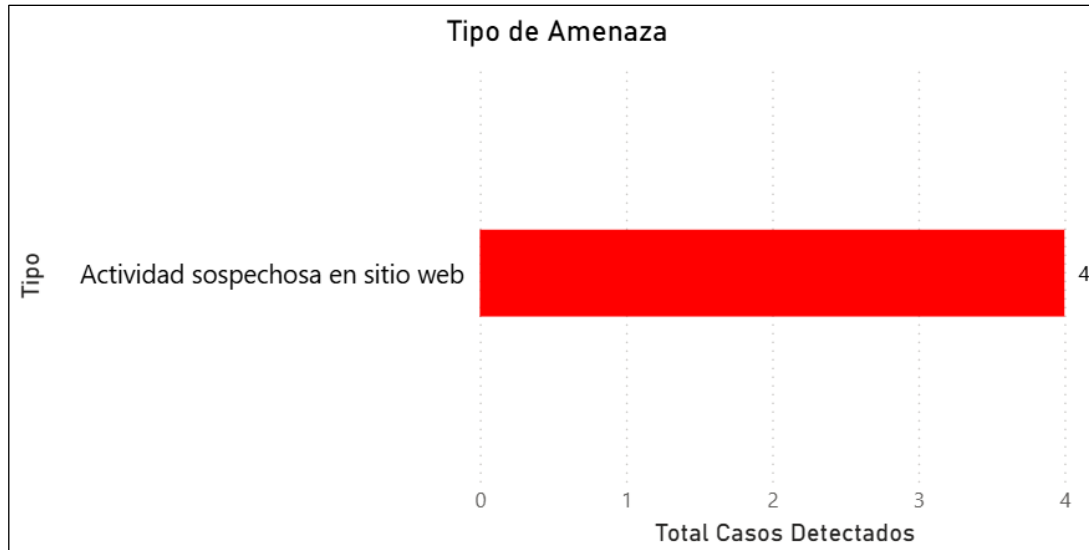


Ilustración 29 Incidentes módulo Deep & Dark Web

Los casos se encuentran detallados en el [Anexo Informe Mensual MARCA-OSINT ICETEX Julio 2026.xlsx](#)

Durante el periodo evaluado se realizó el análisis a 600 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	19	6	0	26
FUGA DE DATOS	0	0	4	562	0	566
DEEP & DARK WEB	0	0	0	4	0	4
CTI	0	0	2	0	0	2
PIRATERÍA ONLINE	0	0	0	2	0	2
TOTAL GENERAL	1	0	25	574	0	600

Tabla 20 Total de Casos gestionados SOC

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.

Con respecto a los casos de Fuga de Datos – Otros Datos Confidenciales - recordar las medidas a considerar:

- Verifique y confirme si la información publicada realmente es de carácter confidencial y no debería estar expuesta públicamente.
- En caso de que el contenido publicado corresponda a información de carácter privado, se recomienda que el área legal del ICETEX contacte al administrador o webmaster del portal para solicitar su retiro.
- No obstante, es importante contar con certeza absoluta de que se trata de una suplantación, ya que, una vez realizada la solicitud, esta acción podría no ser reversible.
- Determinar finalmente si la información publicada no representa ningún riesgo para la entidad.

4.3.7. Análisis de Vulnerabilidades ICETEX

Durante el mes de Julio de 2026, se ejecutó satisfactoriamente el análisis de vulnerabilidades correspondiente a la Fase 2 del plan de trabajo, abordando el segundo bloque de activos planificados para este ciclo. En esta etapa se evaluaron 38 activos (37 Servers, 1 URL), en línea con la planificación mensual de Julio establecida para avanzar progresivamente en la cobertura del entorno completo; además se adicionan 7 activos pendientes de análisis de los meses de abril y mayo, que fueron reportados a la entidad y por lo tanto se ejecutaron en el presente mes de Julio sumando un total de 45 activos analizados.

En el mes de julio se incluyen los siete (7) activos informados de los que no se tenía alcance inicialmente para el cronograma de pruebas del mes de abril-mayo:

No	ACTIVO	TIPO	OBSERVACIONES
1	https://comunidad.icetex.gov.co/login/index.php	EXTERNA	La página existe es respuesta de un servidor PHP, el subdominio esta registrado en el DNS y tiene su resolución a la ip local 192.168.91.11
2	https://web.icetex.gov.co/creditos/preinscribete-y-recibe-asesoria	EXTERNA	Página del portal de ICETEX, existe y funciona normalmente.
3	https://aplicaciones.icetex.gov.co	INTERNA	la página funciona normalmente sin error, pero al invocarla se denota vacía, el subdominio esta registrado en el DNS y tiene su resolución la ip local 192.168.51.165
4	https://aplicaciones.icetex.gov.co/WsPortalTransaccional/api/externalservice/factura	INTERNA	la página funciona normalmente sin error, pero al invocarla se denota vacía, el subdominio esta registrado en el DNS y tiene su resolución la ip local 192.168.51.165
5	10.0.0.30	INTERNA	Regla de firewall des habilitada
6	10.0.0.53	INTERNA	Regla de firewall des habilitada
7	192.168.51.206	INTERNA	Regla de firewall des habilitada

Tabla 21 Activos Faltantes

Durante el análisis se identificaron diez (10) vulnerabilidad críticas; principalmente asociados a uso de componentes con vulnerabilidades conocidas, o sin parches de actualización disponibles por llegar al fin de su vida útil, tales como:

4.3.7.1. Uso de servicios con versiones vulnerables conocidas

- **Unsupported Windows OS (remote), y Unsupported Web Server Detection:** El dispositivo remoto cuenta con un sistema operativo Windows que ha superado su fecha de fin de soporte extendido. Al carecer de actualizaciones de seguridad, cualquier fallo crítico descubierto con posterioridad quedará sin remedio.
- **OpenSSH < 9.6 Multiple Vulnerabilities:** Esta designación agrupa múltiples fallos de seguridad en versiones de OpenSSH anteriores a la 9.6. Entre ellas destaca la vulnerabilidad conocida como "Terrapin" (CVE-2023-48795), que permite a un atacante en medio (MITM) degradar la integridad de la conexión SSH durante el intercambio de claves inicial, pudiendo deshabilitar ciertas características de seguridad como la protección contra ataques de temporización
- **Microsoft IIS ISM.DLL HTR Request Remote Overflow:** Esta vulnerabilidad crítica, identificada como CVE-1999-0874, es un desbordamiento de búfer que afecta al componente ISAPI ISM.DLL de los servidores Microsoft IIS 4.0 y 5.0.

A continuación, se presenta el balance de los hallazgos efectuados:

Severidad	Vulnerabilidades
CRÍTICA	10
ALTA	2
MEDIA	38
BAJA	13
TOTAL	63

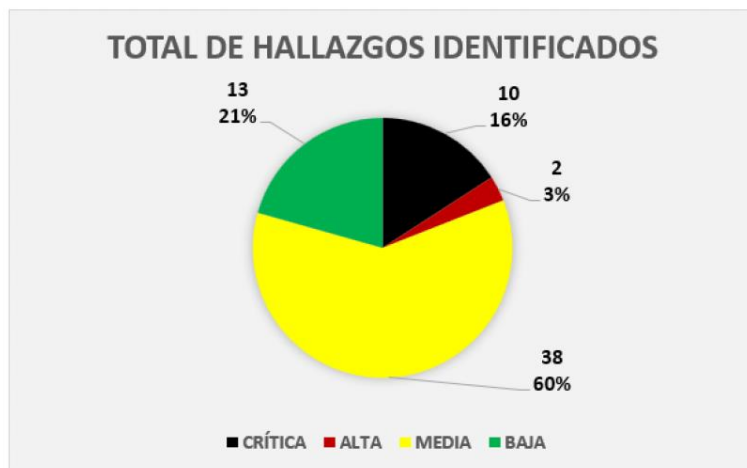


Ilustración 30 Total Hallazgos Análisis de Vulnerabilidades

4.3.7.2. Recomendaciones Derivadas

- Migrar todos los servicios afectados a protocolos modernos (TLS 1.2 y TLS 1.3) y deshabilitar protocolos obsoletos.
- Actualizar servidores con versiones de OpenSSH ≥ 9.6 y aplicar parches de seguridad vigentes.
- Endurecer la configuración de SSH, eliminando cifrados inseguros (CBC, 3DES) y algoritmos débiles de intercambio de claves.
- Implementar controles de monitoreo y endurecimiento en servicios expuestos (RDP y SSH), junto con revisiones periódicas de configuración criptográfica.

4.3.7.3. 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.

4.3.7.4. Recomendaciones

- Evaluar y ampliar los recursos de FortiSIEM (CPU, almacenamiento y capacidad de procesamiento), dado que se están generando alertas críticas por falta de espacio para logs y sobrecarga de CPU, lo que afecta la generación de reportes mensuales y provoca pérdida visual de alertas en la plataforma, comprometiendo la visibilidad y efectividad del monitoreo de seguridad.
- Verificar el estado de los dispositivos monitoreados y realizar depuración de equipos que no se encuentren en operación.

4.4. Servicios de nube

Durante julio de 2026 la gestión del entorno Azure se orientó a la optimización financiera ante el vencimiento del Enterprise Agreement, el fortalecimiento de la ciberseguridad y la modernización de servicios. El gasto total ascendió a USD 12,902.73, con una previsión de cierre de USD 13,753.49, ubicándose por debajo del presupuesto mensual de USD 20,300 y con una reducción del 59.0 % frente a junio, tras normalizarse el consumo extraordinario del mes anterior.

Concepto	Junio 2026	Julio 2026	Variación
Costo total (USD)	31,490.18	12,902.73	-18,587.45 (-59.0%)
Previsión de cierre (USD)	33,116.37	13,753.49	-19,362.88 (-58.5%)
Presupuesto mensual (USD)	20,300.00	20,300.00	Dentro del presupuesto

Tabla 22 Comportamiento de costos (junio - Julio) 2026

Servicio	Junio (USD)	Julio (USD)	Var.	Lectura ejecutiva
Storage	6,678.23	6,028.98	-9.7%	US East 2 concentra >92% del gasto.
Virtual Machines	21,065.48	3,262.63	-84.5%	Storage pasa a ser el 1er componente (~47%).
Microsoft Defender	740.93	730.17	-1.5%	Defender, Backup y GitHub estables.
Backup	663.54	655.45	-1.2%	Caída impulsada por VM (-84.5%).
GitHub	408.91	382.36	-6.5%	Consumo controlado bajo presupuesto.
Total	31,490.18	12,902.73	-59.0%	Fuente: Azure Cost Management.

Tabla 23 Comportamiento de costos por Servicio (junio - Julio) 2026

4.4.1. Principales actividades y logros del mes

- Activación de Microsoft Sentinel: entorno operativo de monitoreo y detección con 50 reglas analíticas, 5 automatizaciones y UEBA (hallazgos MON-SEN-01/02).
- Optimización de costos y Enterprise Agreement: ahorro recurrente anual estimado ~USD 30,118 (desinstalación de recursos, Azure Hybrid Benefit y Reserved Instances); saldo del EA ~USD 113,169.
- Migración del correo a Azure Communication Services: cierre de la transición (>14,000 envíos) y cancelación de Twilio SendGrid; ahorro ~USD 3,000–5,000 anual.
- Tablero de monitoreo diario de ACS: Azure Workbook automatizado (7:00 a. m.), con costo inferior a USD 1 mensual y visibilidad operativa y financiera.
- Ampliación de Microsoft Defender for Cloud: Defender for Servers Plan 2 con MDE en 53 VMs y protección de contenedores; Defender for API a Free (hallazgos SEC-DEF-01/NSG-04/05).
- Propuestas de robustecimiento (Portal Pruebas y AKS WSO2): redimensionamiento y reservas con ahorros estimados de ~60 % (~USD 11,800) y ~62 % (~USD 11,100).
- Preparación del ambiente para la migración del Portal ICETEX: validación de infraestructura, conectividad Hub and Spoke, Bastion y VPN, con 3 VMs validadas.

4.4.2. Conclusiones

Las estrategias de optimización aplicadas normalizaron el consumo del mes, que retornó por debajo del presupuesto, con un ahorro recurrente anual estimado cercano a USD 30,118.

Se fortaleció de forma significativa la ciberseguridad de la suscripción, con Microsoft Sentinel operativo y Microsoft Defender for Cloud ampliado sobre las 53 máquinas virtuales.

Se modernizó el correo transaccional mediante la migración a Azure Communication Services y la baja de Twilio SendGrid, eliminando la dependencia de un proveedor externo.

Persisten decisiones que requieren gestión oportuna, asociadas al vencimiento del Enterprise Agreement (31/07/2026) y a riesgos operativos abiertos (saturación del disco F: del servidor ICTXSRVNETCOR01 y estabilidad del desbloqueo en listas negras).

4.4.3. Recomendaciones

- Mitigar la saturación del disco F: del servidor ICTXSRVNETCOR01 (1,6 % libre) migrando a Azure Files o Blob Storage mediante el procedimiento seguro documentado.
- Completar la implementación de Microsoft Sentinel (Content Hub, conectores, Watchlists y Playbooks) y definir su modelo operativo, con seguimiento al volumen de ingesta.
- Finalizar el endurecimiento con Defender for Cloud (onboarding a MDE, Just-in-Time VM Access y File Integrity Monitoring) y migrar las cuentas de Basic Auth SMTP a OAuth 2.0.
- Confirmar con Claro la causa raíz del bloqueo en listas negras y definir el requerimiento de GitHub Copilot para el próximo Enterprise Agreement.

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 julio 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	\$6.282.040.244	\$ 855.603.847	\$15.206.400	\$840.397.447	\$4.978.024.979,76
OTROS13-Adición Servicios	ITEM1 Arquitectura de Seguridad	ITEM2 Gestion de Vulnerabilidades	ITEM3 Pruebas de Pentesting	ITEM4 Continuidad		
\$ 2.761.480.370	\$ 762.253.015	\$275.243.152	\$208.285.884	\$1.515.698.319		Valores Totales
CONCEPTO					VALOR	
VALOR TOTAL DEL CONTRATO Inicial					\$ 31,398,996,857.96	
OTROS13-Adición Servicios					\$ 2.761.480.370	
OTROS14-Continuidad de Servicios por 8 meses					\$ 8.641.116.065	
VALOR TOTAL DEL CONTRATO					\$ 42.801.593.293	
VALOR PAGADO					\$ 20,628,979,988.10	

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

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	
Pago No. 36 -	mes:	Marzo	de	2026	\$ 792.559.106	
Pago No. 37 -	mes:	Abril 1-18	de	2026	\$ 470.362.652	Contrato Inicial*
Pago No. 1	mes:	Abril 19-30	de	2026	\$ 397.242.170	OTROSI4-Continuidad de Servicios por 8 meses
Pago No. 2	mes:	Mayo	de	2026	\$ 1.024.142.866	OTROSI4-Continuidad de Servicios por 8 meses
Pago No. 2	mes:	Mayo	de	2026	\$ 15.206.400	Bolsa
Pendiente- Pago No. 3	mes:	Junio	de	2026	\$ 1.020.170.794	OTROSI4-Continuidad de Servicios por 8 meses
Pendiente- Pago No. 4	mes:	Julio	de	2026	\$ 1.022.533.727	OTROSI4-Continuidad de Servicios por 8 meses
VALOR CAUSADO QUE NO SE HA PAGADO (valor a pagar factura)						\$ 1.022.533.727
VALOR TOTAL EJECUTADO (valor pagado + valor causado no pagado)						\$ 32.127.062.660
SALDO DEL CONTRATO (valor total del contrato – valor total ejecutado)						\$ 10.674.530.633
PORCENTAJE DE EJECUCIÓN						75,06%
* El valor causado no pagado corresponde a cuentas de cobro o facturas recibidos y aprobados a satisfacción por el supervisor o interventor para su pago*						

Tabla 24 Ejecución Presupuestal

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

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 Morales– Apoyo DBA	Informe Mensual InfoTIC DBA Julio2026.pdf
Especialista Web Máster	Juan Carlos Martinez Sierra	Informe Mensual InfoTIC Webmaster Julio2026.pdf
Especialista Integrador de nube	Carlos Fernando Barrera Narvaez	Informe Mensual InfoTIC Integrador de Nube Julio2026.pdf
Especialistas de Seguridad	Juan Carlos Quiroga Varila Hector Manuel Rojas Ibanez	Informe Mensual InfoTIC Seguridad Julio2026.pdf
Especialistas de soluciones	Jose Francisco Escobar Escorcia Davis Alexander Mogollón Fandiño	Informe Mensual InfoTIC Administrador de Soluciones Julio2026.pdf
Especialista de Networking	Carlos Alberto Roldan Ríos Walter Eduardo Pinilla Tenorio - Apoyo Networking	Informe Mensual InfoTIC Administrador de Redes Julio2026.pdf

Tabla 25 Perfiles y Actividades

El siguiente es el grupo administrativo que estuvo en el desarrollo de la operación del mes de Julio 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 26 Grupo Administrativo

* La gerente de servicios salió a vacaciones desde el 21 de julio y se reincorporó, a la operación el 1o de agosto.

8. SERVICIO DE COLABORACIÓN

Durante el mes de Julio, 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.

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

ÍTEMS	SERVICIO	CIUDAD	DIRECCIÓN	CANTIDAD
1	Sala de video conferencia o sala virtual (Tamaño 65")	Bogotá – Aguas	Carrera 3 No. 18-32 Piso 2, 4 y 6	3
2	Sala de video conferencia o sala virtual (Tamaño 65")	Bogotá – Ángel	Cl. 19 #6-68 piso 17	1
3	Sala de video conferencia o sala virtual (Tamaño 55")	Bogotá – Aguas	Carrera 3 No. 18-32 es una unidad 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 27 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 Ictetex.

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

- Visita en sitio en sedes de Bogotá, para realizar pruebas de funcionamiento, verificación de actualizaciones pendientes, inspección de los módulos y posterior limpieza interna y externa de los componentes de cada módulo que se encuentra en la sede Aguas, Ángel y chapinero, para garantizar la prestación continua del servicio y validar que no se estén presentado novedades y/o incidencias.
- Se realizó actualización del sistema operativo de tres (3) OPS de los módulos de la sede Aguas, Windows 10 a Windows 11.

- Disponibilidad de atención a requerimientos que surjan para revisión de novedades presentadas.
- Informe mensual de operación del servicio y reporte técnico de visitas a sedes, el cual se puede consultar en el link [Informe actividades Módulos videoconferencia ICETEX Julio 2026.pdf](#)

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

9. GESTION DE RIESGOS Y PROBLEMAS

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

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

10. INDICADORES CLAVE DE DESEMPEÑO

10.1. ANS por Disponibilidad de canales de comunicaciones

Durante el mes de Julio 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 mensual del comportamient : [Reporte Mensual Disponibilidad INFOTIC Julio 2026.pdf](#)

También se puede consultar en el repositorio un documento en Excel con las disponibilidades promedio de los canales para el mes de Julio: [ANS Julio 2026.xlsx](#)

Durante el mes de julio de 2026 el servicio de Internet para la gente se prestó sin interrupciones en todas las catorce sedes contratadas donde ICETEX cuenta con oficina, dichas disponibilidades pueden ser consultas en el archivo mencionado en el párrafo anterior.

10.1.1. Canal de Replicación (Triara – Megacenter)

El proyecto tiene asignado un canal de comunicación con un ancho de banda de 2 Gbps, el cual se comunica en forma bidireccional entre los data centers de Triara y Megacenter, permitiendo generar la replicación de la información de los equipos de ICETEX, para el mes de Julio continúa su funcionamiento correctamente sin novedades que afectaran la prestación del servicio. La evidencia se encuentra en el [Informe mensual replicacion Julio 2026.pdf](#).

10.2. ANS por Disponibilidad de servidores

La herramienta utilizada para el monitoreo de la disponibilidad de servidores es ELK y el informe correspondiente que permite la revisión de los ANS es el [Reporte Monitoreo ICETEX Julio ELK.pdf](#) y [Disponibilidad Server ELK Julio 2026.xlsx](#)

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 28 Dispositivos en Housing – Datacenter Principal

10.2.1. Disponibilidad TRIARA para los servicios de página web 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

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

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

	Mayo	Junio	Julio
Usuarios activos mes	495000	571000	663000
Usuarios nuevos	314000	365000	442000
Tiempo de interacción (seg)	121	136	117

Tabla 29 Distribución trimestral de acceso por usuarios

El portal WEB cuenta con un total de 663 mil usuarios, con 442 mil usuarios nuevos. El tiempo de interacción medio es de 1 minutos y 57 segundos, señalando el interés de la audiencia en las diferentes páginas del portal web.icetex.gov.co.

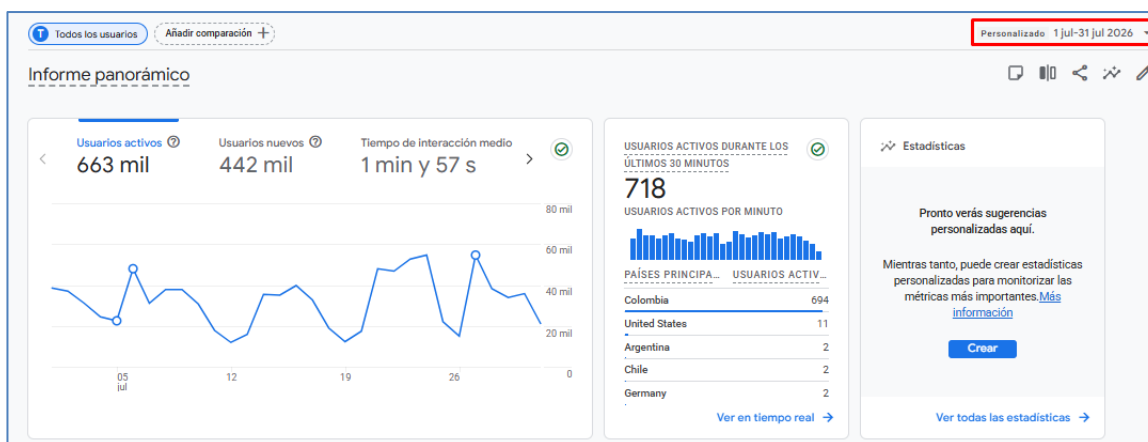


Ilustración 31 Métrica de visitantes Portal WEB web.ICETEX.gov.co

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 usuario (...)

Personalizado 1 jul-31 jul 2026

Filas por página: 10 Ir a: 1-10 de 13

	↓ Total de usuarios	Usuarios nuevos	Usuarios recurrentes	Tiempo de interacción medio por usuario activo	Sesiones con interacción por usuario activo	Número de eventos Todos los eventos
☒ Total	691.621 100 % respecto al total	442.246 100 % respecto al total	331.014 100 % respecto al total	1 min y 57 s Media 0 %	1,29 Media 0 %	9.383.359 100 % respecto al total
☒ 1 Organic Search	414.100 (59,87 %)	232.112 (52,48 %)	238.614 (72,09 %)	2 min y 24 s	1,57	6.506.497 (69,34 %)
☒ 2 Direct	252.082 (36,45 %)	184.386 (41,69 %)	83.802 (25,32 %)	1 min y 09 s	0,94	2.546.649 (27,14 %)
☒ 3 Referral	13.650 (1,97 %)	9.746 (2,2 %)	5.362 (1,62 %)	2 min y 23 s	1,25	176.327 (1,88 %)
☒ 4 Organic Social	13.275 (1,92 %)	11.664 (2,64 %)	2.374 (0,72 %)	48 s	0,74	97.853 (1,04 %)
☒ 5 AI Assistant	4.677 (0,68 %)	4.124 (0,93 %)	1.216 (0,37 %)	5 min y 16 s	1,00	50.134 (0,53 %)
☐ 6 Paid Other	115 (0,02 %)	71 (0,02 %)	64 (0,02 %)	1 min y 30 s	1,39	1.881 (0,02 %)
☐ 7 Unassigned	106 (0,02 %)	42 (<0,01 %)	42 (0,01 %)	1 min y 02 s	0,92	890 (<0,01 %)
☐ 8 Email	97 (0,01 %)	49 (0,01 %)	47 (0,01 %)	2 min y 39 s	1,70	1.438 (0,02 %)
☐ 9 Organic Video	85 (0,01 %)	49 (0,01 %)	40 (0,01 %)	2 min y 33 s	1,39	1.073 (0,01 %)
☐ 10 Paid Search	32 (<0,01 %)	1 (<0,01 %)	24 (<0,01 %)	2 min y 15 s	2,58	502 (<0,01 %)

Ilustración 32 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.

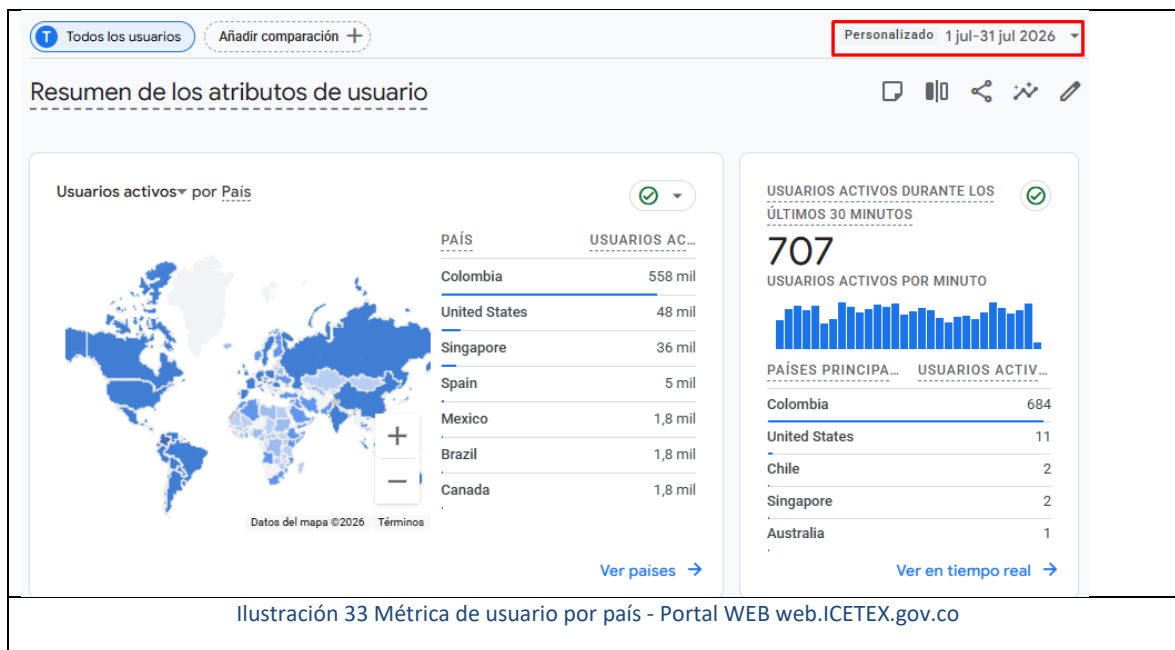


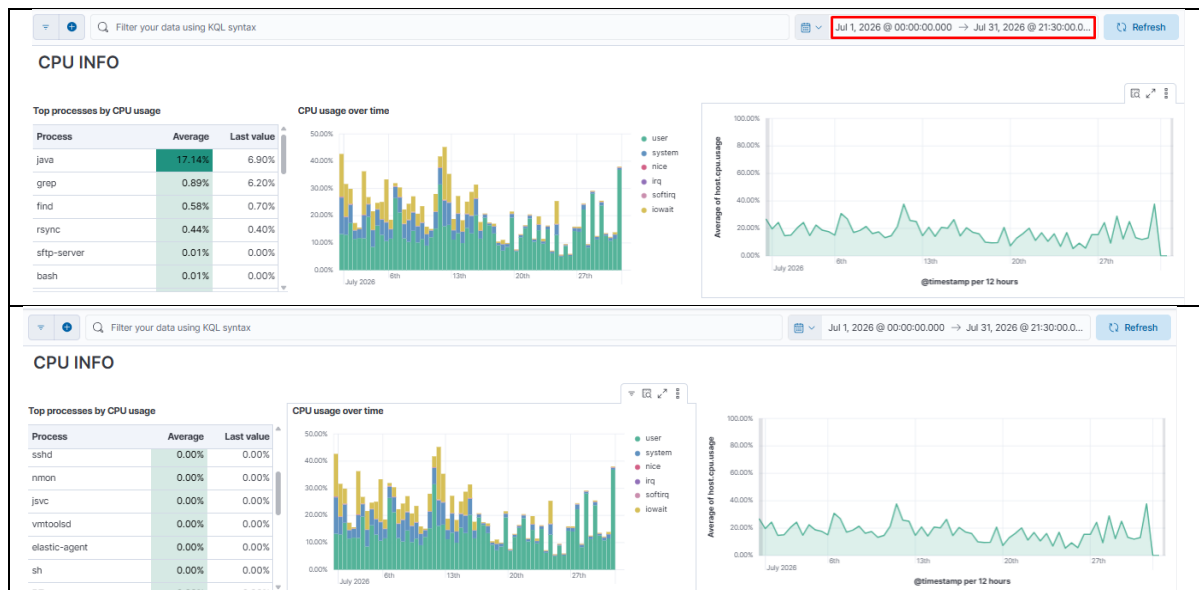
Ilustración 33 Métrica de usuario por país - Portal WEB web.ICETEX.gov.co

Detalles demográficos: Ciudad Personalizado 1 jul-31 jul 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 Todos los eventos
☒ Total	663.364 100 % respecto al total	442.334 100 % respecto al total	858.530 100 % respecto al total	54,6 % Media 0 %	1,29 Media 0 %	1 min y 57 s	9.385.502 100 % respecto al total
☒ 1 Bogotá	209.523 (31,58 %)	127.572 (28,84 %)	294.832 (34,34 %)	57,1 %	1,41	2 min y 00 s	3.186.053 (33,95 %)
☒ 2 Medellín	57.200 (8,62 %)	30.047 (6,79 %)	64.191 (7,48 %)	54,47 %	1,12	1 min y 19 s	634.754 (6,76 %)
☒ 3 Barranquilla	53.076 (8 %)	25.469 (5,76 %)	74.034 (8,62 %)	55,02 %	1,39	1 min y 40 s	706.826 (7,53 %)
4 (not set)	51.725 (7,8 %)	33.063 (7,47 %)	58.092 (6,77 %)	55,99 %	1,12	1 min y 36 s	588.519 (6,27 %)
☒ 5 Cali	47.994 (7,23 %)	24.814 (5,61 %)	57.821 (6,73 %)	57,41 %	1,20	1 min y 46 s	581.652 (6,2 %)
☐ 6 Singapore	34.918 (5,26 %)	34.634 (7,83 %)	2.023 (0,24 %)	5,92 %	0,06	0 s	123.629 (1,32 %)
☐ 7 Cartagena	24.606 (3,71 %)	11.517 (2,6 %)	35.409 (4,12 %)	60,24 %	1,44	2 min y 09 s	341.547 (3,64 %)
☐ 8 Montería	12.940 (1,95 %)	5.983 (1,35 %)	18.550 (2,16 %)	57,89 %	1,43	1 min y 57 s	181.140 (1,93 %)
☐ 9 Sincelejo	10.197 (1,54 %)	4.909 (1,11 %)	19.161 (2,23 %)	59,5 %	1,88	2 min y 40 s	181.225 (1,93 %)
☐ 10 Bucaramanga	9.577 (1,44 %)	4.961 (1,12 %)	11.871 (1,38 %)	59,13 %	1,24	1 min y 40 s	116.838 (1,24 %)

Ilustración 34 Métrica de ciudades de Colombia- Portal WEB web.ICETEX.gov.co

A continuación, se muestran las gráficas referentes a CPU, memoria RAM y almacenamiento en el nodo 1 del portal ICETEX desde el 1 de Julio desde las 00:00 horas hasta las 23:59 horas del 31 de Julio de 2026.



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

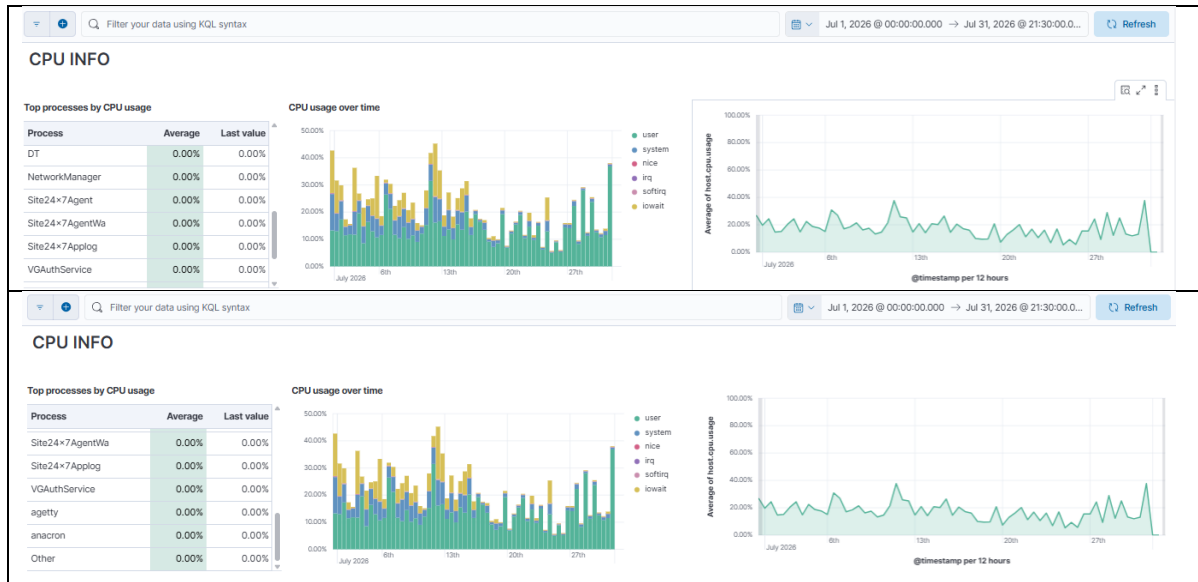
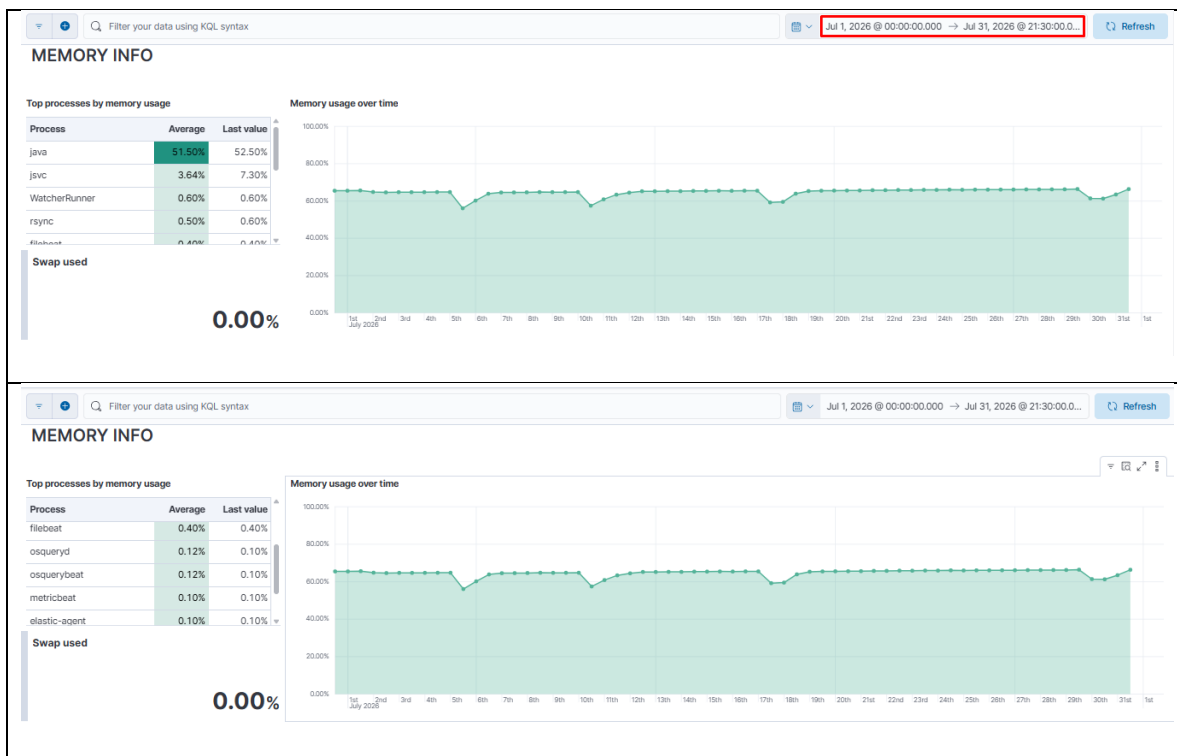
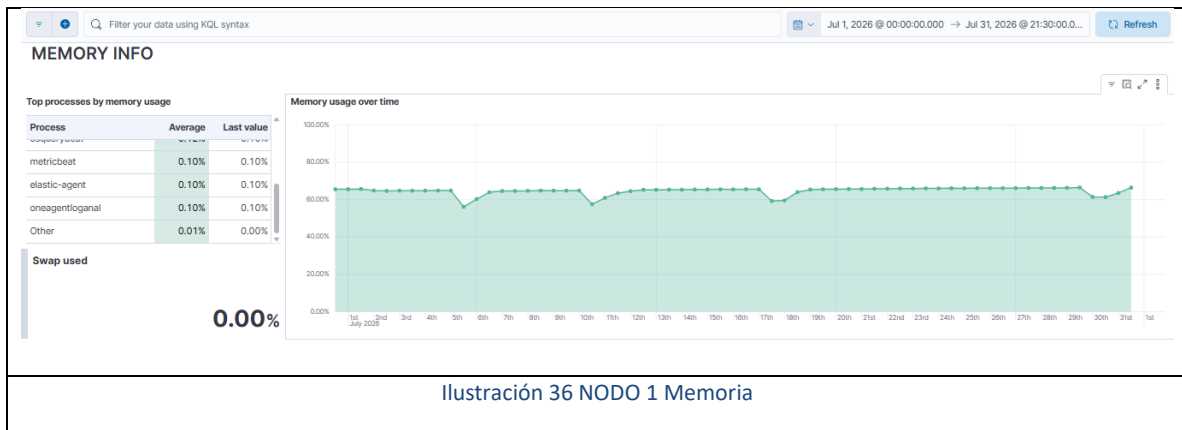


Ilustración 35 NODO 1 CPU



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



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 Julio2026.pdf](#)

10.2.2. Análisis componente Liferay Producción

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

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

10.2.3. Backup Servidores Triara

Durante el periodo de julio 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 Julio 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 Backup julio 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 Julio el resultado de la ejecución de los Backups fue el siguiente:

Generated on: Aug 1, 2026, 0:39 am

Backup job summary	
Backup job summary report	
CommCell	CS02-CAP-TRIARA
Company	All
Server groups	INFOTIC
Servers	All
App types / Workloads	All
Subclients	All
Job status	Running, Completed, Delayed, Failed, Killed, Completed with Errors, Completed with Warnings, Committed
Job types	All
Time frame	Last 4 Weeks (Jul 4, 2026, 08:39:21 AM - Aug 1, 2026, 08:39:21 AM)
Time zone	CommServ
Day start time	12:00 AM
Snap and Backup Copy options	All
Advanced	All
Agents	All
Max number of jobs to return	4000

Ilustración 38 Evidencia Backup servidores resumen general Backups



La infraestructura gestionó de manera correcta un volumen crítico de datos, consolidando un total de 232.38 TB de información respaldada durante el mes.

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

- Se alcanzó una tasa de éxito sobresaliente del **99.04%** sobre un universo de **3,759 trabajos analizados**. Esto demuestra la estabilidad de la plataforma Commvault y la madurez de las políticas de retención y respaldo actuales.
- La tasa de fallo o cancelación es marginal (**0.96%**). El proceso interno garantiza la resiliencia operativa, ya que los incidentes identificados son mitigados, corregidos y reejecutados de forma proactiva por el equipo técnico para evitar brechas en la pérdida de datos.
- Los servidores Oracle RAC representan el núcleo crítico de la operación, concentrando el 76.59% de la actividad total (2,879 trabajos).
- Los entornos de **VMware vCenter** constituyen el segundo pilar operativo con el **16.89%** de los trabajos (635 respaldos).
- Los servidores tradicionales y específicos (Windows Server, Linux Server y SQL Server) mantienen una participación menor y distribuida, sumando en conjunto el 6.52% restante de la carga de trabajo.

Métrica Clave	Resultado	Estado
Volumen Total Respaldado	232.38 TB	Óptimo
Trabajos Evaluados	3,759	Completo
Efectividad	99.04%	Excelente
Tasa de Falla / Cancelación	0.96%	Controlado e Intervenido
Componente Crítico	Oracle RAC (76.59%)	Foco Principal

Tabla 30 Resumen comportamiento de Backups Julio

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](#)

La estrategia de respaldo y continuidad operativa es uno de los componentes más maduros y estables del servicio.

11. CONTROL DE CAMBIOS

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

No. Cambio	Alcance	Fecha De Creación	Fecha De Ejecución	Resultado	Observaciones
39865	Actualización del sistema operativo Oracle Linux en los servidores de bases de datos. Actualización Sistema Operativo – Productivos Nodos -INR0276 INR0277 – Servidor de Contingencia-INR0278	07/07/2025	10/07/2026	Exitoso	Versión Final: Nodos Producción: INR0276_CXVODAPRODN011 OS: RedHat7.9 Kernel: 5.4.17-2136.357.3.1.el7uek.x86_64 IP: 100.66.24.133 Uptime: 0 días, 0 horas, 1 minutos INR0276_CXVODAPRODN011 OS: RedHat7.9 Kernel: 5.4.17-2136.357.3.1.el7uek.x86_64 IP: 100.66.24.133 Uptime: 0 días, 0 horas, 1 minutos Contingencia INR0278_CXVODACONTG011 OS: RedHat7.9 Kernel: 5.4.17-2136.357.3.1.el7uek.x86_64 IP: 172.20.77.1 Uptime: 0 días, 0 horas, 2 minutos

Tabla 31 Controles de cambio enero

Quedamos atentos a la disponibilidad de los recursos de virtualización (colocation) por parte del ICETEX para dar continuidad a las actualizaciones de sistema operativo. Con esto, retomaremos la programación y ejecución habitual de los controles de cambios mensuales sobre los servidores detallados a continuación:

- ICTXSRVNETCOR01(192.168.51.165): servidor que 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): servidore que aloja la aplicacionPSE
- ICTXSRVDCVAL01(192.168.51.170): servidor que 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 las alternativas de solución respecto al licenciamiento de las herramientas de seguridad (perimetral y antivirus)	ICETEX	01-08-2025	19-12-2026	Esta situación implica riesgos críticos tanto a nivel de seguridad como de continuidad operativa, entre los que se destacan: - Falta de actualizaciones de seguridad críticas. - Mayor exposición a vulnerabilidades y ataques cibernéticos. - Incompatibilidad con software y hardware actualizado. - Ausencia de soporte oficial por parte del fabricante.
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	01-08-2024	19-12-2026	Se programará la desinstalación de Symantec y la migración al antivirus Falcon, conforme a las ventanas de mantenimiento y disponibilidad que defina el ICETEX.

Tabla 32 Planes de trabajo

13. RECOMENDACIONES DEL CONTRATISTA AL ICETEX

13.1. 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.

13.2. 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.

13.3. Seguridad

Continuar con las respectivas socializaciones para realizar remediaciones tempranas y poder socializar o en su defecto, crear políticas cuando se detecten sus necesidades, por lo que se requiere un análisis y levantamiento de información previa de lo cual para saber dónde se necesita y en qué procedimientos.

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

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

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

13.4. Bases De Datos

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

Las versiones disponibles del sistema manejador de base de datos ORACLE son Oracle Database 23 ai, Oracle Database 21c y Oracle Database 19c. No obstante que se dio inicio, al plan de migración de las bases de datos que se encuentran en versiones anteriores, se recomienda al ICETEX, que analice la posibilidad de efectuar la migración sobre versiones más recientes con el fin de evitar ejecutar planes de migración con demasiada frecuencia.

13.5. Integrador De Nube

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

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

14. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC

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

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

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

14.2. TB de capacidad de almacenamiento

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

CONTRATADO			
Cod Servicio	CIUDAD	ALCANCE	CAPACIDAD (TB)
INR0194	TRIARA	Almacenamiento Centralizado 23 TB Tier 2	35
INR0193	TRIARA	Almacenamiento Centralizado 12 TB Tier 2.5	

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

INR0192	MEGACENTER	Almacenamiento Centralizado 15 TB Tier 2	25
INR0191	MEGACENTER	Almacenamiento Centralizado 10 TB Tier 2.5	
			60

Tabla 33 Capacidades de almacenamiento contratado

Aprovisionado se tienen las siguientes capacidades instaladas:

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

Tabla 34 Capacidades de almacenamiento aprovisionado

Se implementaron los 60 TB contemplados contractualmente. Adicionalmente, se dispone de 30 TB en calidad de préstamo en el Data Center Triara, utilizados por máquinas virtuales clonadas, restauradas, apagadas o en espera de actualización, las cuales actualmente consumen capacidad de almacenamiento. Es importante precisar que este espacio adicional se ha asignado de manera temporal y no genera compromisos contractuales ni obligaciones legales para el ICETEX.

En el almacenamiento aprovisionaron 3 TB como valor agregado de INFOTIC para realizar la prueba de restauración de Backups, la solicitud de restauración recibida desde Icetex en julio sigue pendiente. Se debe liberar espacio de almacenamiento en el servidor destino (colocation de Icetex), pues la capacidad actual es insuficiente para completar el proceso. El ticket es el RS-SoporteTI-42780 y el formato de solicitud se encuentra en el repositorio link: [Restauraciones](#)

14.3. “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 35 WIFI para la gente instalados

15. 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.

16. ANEXOS

Tema	SubTema	Anexo
Almacenamiento	Backups Diarios	Backups diarios Julio 2026 Backup Diario
	Informe de Backups	Consolidado mensual Backups Julio 2026 Consolidado mensual de Backup julio 2026.pdf Informe Backups mes de Julio 2026.pdf Politica Backup Icetex V7.xlsx ReporteMensualCintasInfotc_2026-07-29.html Restauraciones
Aplicaciones	Informes de actividades	Informe actividades Módulos videoconferencia ICETEX Julio 2026 Informe actividades Módulos videoconferencia ICETEX Julio 2026.pdf Informe mensual Administrador de Soluciones Julio 2026 Informe Mensual InfoTIC Administrador de Soluciones Julio2026.pdf Informe mensual Administrador Web Master Julio 2026 Informe Mensual InfoTIC Webmaster Julio2026.pdf Informe mensual Integrador Nube Julio 2026 Informe Mensual InfoTIC Integrador de Nube Julio2026.pdf
Bases De Datos		Informe mensual Administrador de Bases de datos Julio 2026 Informe Mensual InfoTIC DBA Julio2026.pdf
Ejecución Presupuestal		Conciliación Julio consolidado Conciliación Julio consolidado 2026.xlsx Informe de Gestión Servicio Julio 2026 Informe de Gestion Servicio Julio 2026.pdf Informe de Gestion Servicio Julio 2026.docx
Seguridad		Informe Mensual MARCA-OSINT ICETEX Julio 2026 Anexo Informe Mensual MARCA-OSINT ICETEX Julio 2026.xlsx Anexo Informe Mensual MARCA-OSINT ICETEX Julio 2026.xlsx Informe Mensual Seguridad Julio 2026 Informe Mensual InfoTIC Seguridad Julio2026.pdf Informe Mensual SOC - ICETEX Julio 2026 Informe Mensual SOC-TH ICETEX Julio 2026.pdf Informe Técnico Análisis de Vulnerabilidades Julio 2026 INFORME TÉCNICO ANÁLISIS DE VULNERABILIDADES ICETEX (Julio 2026).pdf
Soporte Y Monitoreo	Canales	ANS Julio 2026

Tema	SubTema	Anexo
		ANS Julio 2026.xlsx Informe mensual Administrador de Networking Julio 2026 Informe Mensual InfoTIC Administrador de Redes Julio2026.pdf Informe Mensual Disponibilidad Julio 2026 Reporte Mensual Disponibilidad INFOTIC Julio 2026.pdf
	Gráficas de consumo	Informe Mensual ALLOT Julio 2026 Graficas de consumo Julio 2026 – ALLOT INFOTIC.xls
Data center Alterno	Replicación	Informe mensual replicación Julio 2026 Informe mensual replicacion Julio 2026.pdf Reportes diarios Julio 2026 Replicaciones
Data Center Principal		Reporte Monitoreo ICETEX Julio 2026-ELK Reporte Monitoreo ICETEX Julio ELK.pdf Data ELK Disponibilidad Server ELK Julio 2026.xlsx

Tabla 36 Anexos

Revisión técnica

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	