



INFORME DE ACTIVIDADES DEL CONTRATO

**CONTRATO NUMERO
2022-0792**

Marzo 01 al 31 de 2026

versión	Observaciones	Fecha	Responsable
1.0	Versión Inicial	01/04/2026	Francisco Javier Pulido

Tabla de contenido

1.	INTRODUCCIÓN	9
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.	Despliegue de direcciones IP V6.....	14
4.1.3.	Implementación canales SDWAN.....	15
4.1.4.	Recomendaciones.....	15
4.2.	Centro de Datos	16
4.2.1.	Centro de Datos Principal	16
4.2.1.1.	Aplicaciones	16
4.2.1.2.	Bases de Datos	20
4.2.1.3.	Sitio Web.....	24
4.2.1.4.	Servicios de DRP	27
4.2.2.	Centro de Datos Alterno	28
4.2.2.1.	Hosting Virtual (IaaS).....	28
4.2.2.2.	DataGuard Bases de Datos Megacenter	30
4.2.2.3.	Servicios de Housing – Datacenter Alterno	31
4.3.	Seguridad informática	31
4.3.1.	Plataformas Administradas	34
4.3.1.1.	FortiGate Triara	35
4.3.1.2.	FortiGate Aguas.....	38
4.3.1.3.	FortiGate Medellín.....	39
4.3.1.4.	FortiWeb 2000F	40
4.3.1.5.	FortiWeb 2000E	40
4.3.1.6.	FortiWebCloud DRP.....	41
4.3.1.7.	FortiSandBox	41

4.3.1.8.	FortiSIEM	42
4.3.1.9.	Sophos EndPoint	42
4.3.2.	Recomendaciones de Seguridad para el ICETEX.	43
4.3.3.	Servicio de centro de Operaciones de Seguridad (SOC).....	44
4.3.3.1.	Indicadores de compromiso (Thread Hunting):.....	45
4.3.3.2.	Alertas o Incidentes de Seguridad Detectados.....	46
4.3.3.2.1.	Categoría Seguridad.....	46
4.3.3.2.2.	Categoría Disponibilidad	48
4.3.3.2.3.	Amenazas de Ciberseguridad.....	49
4.3.3.3.	Threat Hunting	52
4.3.3.4.	Análisis de Marca OSINT	52
4.3.4.	Análisis de Vulnerabilidades ICETEX	55
4.3.5.	Reporte De IPS	55
4.4.	Servicios de nube	56
5.	GESTION DE LA EJECUCIÓN CONTRACTUAL	57
6.	GESTION PRESUPUESTAL	58
7.	GESTION ADMINISTRATIVA.....	60
7.1.	Profesionales	60
8.	SERVICIO DE COLABORACIÓN.....	61
9.	GESTION DE RIESGOS Y PROBLEMAS.....	62
10.	INDICADORES CLAVE DE DESEMPEÑO	62
10.1.	ANS por Disponibilidad de canales de comunicaciones.....	62
10.1.1.	Canal de Replicación (Triara – Megacenter)	65
10.2.	ANS por Disponibilidad de servidores.....	65
10.2.1.	Disponibilidad TRIARA para los servicios de página web.....	67
10.2.2.	Análisis componente Liferay Producción	72
10.2.3.	Backup Servidores Triara	72
11.	CONTROL DE CAMBIOS	74
12.	PLAN DE TRABAJO DE LOS PROXIMOS MESES	75
13.	PLAN DE ENTREGA	76

14.	RECOMENDACIONES DEL CONTRATISTA AL ICETEX.....	79
14.1.	Networking	79
14.2.	Aplicaciones	80
14.3.	Seguridad.....	81
14.4.	Bases De Datos.....	82
14.5.	Integrador De Nube.....	82
15.	EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC.....	83
15.1.	Aumento de la capacidad de Ancho de Banda en algunas de las sedes de la Entidad	83
15.2.	Una capacitación al año de seguridad Informática y servicios conexos	83
15.3.	TB de capacidad de almacenamiento	83
15.4.	“Wifi” para la gente en 19 sedes	84
16.	CONCLUSIONES.....	85
17.	ANEXOS	87

TABLA 1 CASOS ATENDIDOS NETWORKING COMPARATIVO MES ANTERIOR.....	14
TABLA 2 LISTADO DE DIRECCIONES IP V6 ASIGNADAS A LAS OFICINAS.....	15
TABLA 3 VIGENCIA DE LOS CERTIFICADOS DIGITALES.....	18
TABLA 4 INVENTARIO PRINCIPALES SERVIDORES PRODUCCIÓN	19
TABLA 5 PARÁMETROS DE SISTEMA OPERATIVO- COMPONENTE DE SEGURIDAD WINDOWS DEFENDER FIREWALL	20
TABLA 6 SERVIDORES Y SCHEMAS ADMINISTRADOS.....	20
TABLA 7 ESTADO BD ORACLE	21
TABLA 8 CRECIMIENTO DE LAS BASES DE DATOS EN LOS ÚLTIMOS 7 MESES.....	24
TABLA 9 TOP 10 PORTALES MÁS UTILIZADOS.....	26
TABLA 10 ESTADO LICENCIAMIENTO PORTAL WEB ICETEX	27
TABLA 11 SERVICIOS REPLICADOS – DATACENTER ALTERNO-MEGACENTER	29
TABLA 12 TOP 5 MÁQUINAS MAYOR TASA DE TRANSFERENCIA	29
TABLA 13 TOP 5 MÁQUINAS MENOR TASA DE TRANSFERENCIA.....	29
TABLA 14 DISPONIBILIDAD DE SERVICIOS DE HOUSING – DATA CENTER ALTERNO	31
TABLA 15 DETALLE PLATAFORMAS SEGURIDAD ADMINISTRADAS INFOTIC.....	35
TABLA 16 LICENCIAMIENTO FORTIGATE	35
TABLA 17 LICENCIAMIENTO FORTIWEB	40
TABLA 18 CONFIGURACIÓN FORTISANDBOX 1000D.....	42
TABLA 19 RECOMENDACIONES DE SEGURIDAD	44
TABLA 20 COMPARATIVO – INDICADORES DE COMPROMISO.....	46
TABLA 21 COMPARATIVO ALERTAS DE SEGURIDAD	47
TABLA 22 EJECUCIÓN PRESUPUESTAL.....	60
TABLA 23 PERFILES Y ACTIVIDADES.....	60
TABLA 24 GRUPO ADMINISTRATIVO	61
TABLA 25 DISTRIBUCIÓN MÓDULOS DE VIDEOCONFERENCIA POR SEDE.....	61
TABLA 26 DISPONIBILIDAD DE CANALES.....	65
TABLA 27 DISPONIBILIDAD CANALES “INTERNET PARA LA GENTE”	65
TABLA 28 CÓDIGOS RELACIONADOS DISPONIBILIDAD SERVICIOS EN HOUSING – DATACENTER PRINCIPAL.....	66
TABLA 29 DISPOSITIVOS EN HOUSING – DATACENTER PRINCIPAL	67
TABLA 30 DISTRIBUCIÓN TRIMESTRAL DE ACCESO POR USUARIOS	67
TABLA 31 CONTROLES DE CAMBIO MARZO.....	75
TABLA 32 PLANES DE TRABAJO	76
TABLA 33 SESIONES DE PRESENTACIÓN LISTAS DE CHEQUEO ENTREGA DE SERVICIOS.....	78
TABLA 34 CAPACIDADES DE ALMACENAMIENTO CONTRATADO	84
TABLA 35 CAPACIDADES DE ALMACENAMIENTO APROVISIONADO	84
TABLA 36 PRUEBAS DE RESTAURACIONES DE BACKUPS DE MARZO	84
TABLA 37 WIFI PARA LA GENTE INSTALADOS	85
TABLA 38 WIFI PARA LA GENTE PENDIENTES.....	85
TABLA 39 ANEXOS.....	88

ILUSTRACIÓN 1 DISPONIBILIDAD DEL CLÚSTER	12
ILUSTRACIÓN 2 DISPONIBILIDAD DEL CLUSTER	22
ILUSTRACIÓN 3 DISPONIBILIDAD DE LAS BASES DE DATOS PRINCIPALES ICTXCYC Y APOTEOSYS	22
ILUSTRACIÓN 4 CASOS DEL PROYECTO GESTIONADOS ARANDA BASES DE DATOS	23
ILUSTRACIÓN 5 UPTIME: PORTAL WEB WEB.ICETEX.GOV.CO [98,609%]	25
ILUSTRACIÓN 6 TRÁFICO GENERAL DE LOS PORTALES	26
ILUSTRACIÓN 7 REPORTES DE REPLICACIÓN SRM A SITIO ALTERNO – MARZO 2026	28
ILUSTRACIÓN 8 FECHAS CON MAYOR REPLICACIÓN.....	30
ILUSTRACIÓN 9 EVIDENCIA DATAGUARD REPLICADO A MEGACENTER BD	31
ILUSTRACIÓN 10 DIAGRAMA DE LA ARQUITECTURA DE SEGURIDAD.....	32
ILUSTRACIÓN 11 TOPOLOGÍA DE WAF CLOUD USADO EN PORTALES DE MEDELLÍN	33
ILUSTRACIÓN 12 CONSUMO CANAL MPLS - PROMEDIO 84.23 MPPSG [INR0185 CLARO(MPLS_DC)]	36
ILUSTRACIÓN 13 CONSUMO CANAL INTERNET SEDES - PROMEDIO 133.49 MBPS WAN-SEDES-ICETEX [INR0264 (INTE_SEDES_ICTX)].....	36
ILUSTRACIÓN 14 CONSUMO CANAL INTERNET DATA CENTER- INTERNET DATACENTER [INTERNET_DC_INR0000320 (INET_CLARO)].....	36
ILUSTRACIÓN 15 FILTRADO – WEB – (FORTIGATE – TRIARA).....	37
ILUSTRACIÓN 16 INSPECCIÓN – SSL – (FORTIGATE – TRIARA)	37
ILUSTRACIÓN 17 ANTIVIRUS Y ANTIMALWARE – PERIMETRAL (FORTIGATE – TRIARA)	38
ILUSTRACIÓN 18 CONSUMO CANAL MPLS AGUAS - PROMEDIO 44.72 MBPS.....	38
ILUSTRACIÓN 19 FILTRADO-WEB-(FORTIGATE-AGUAS).....	39
ILUSTRACIÓN 20 INSPECCIÓN-SSL-(FORTIGATE-AGUAS)	39
ILUSTRACIÓN 21 ANTIVIRUS Y ANTIMALWARE-PERIMETRAL-(FORTIGATE-AGUAS)	39
ILUSTRACIÓN 22 CONSUMO CANAL MPLS MEDELLÍN	40
ILUSTRACIÓN 23 TRÁFICO GENERAL DE LOS PORTALES	41
ILUSTRACIÓN 24 TRÁFICO GENERAL DE LOS PORTALES	41
ILUSTRACIÓN 25 DESEMPEÑO POR PROCESOS.....	42
ILUSTRACIÓN 26 ESTADO SEGURIDAD SOPHOS.....	43
ILUSTRACIÓN 27 CANTIDAD DE ORDENADORES CON AGENTE	43
ILUSTRACIÓN 28 CANTIDAD SERVIDORES CON AGENTE.....	43
ILUSTRACIÓN 29 TOTAL DE ALERTAS DE SEGURIDAD	47
ILUSTRACIÓN 30 TOP 5 DE ALERTAS DE SEGURIDAD ALTAS	48
ILUSTRACIÓN 31 TOP 5 DE ALERTAS DE SEGURIDAD MEDIAS	48
ILUSTRACIÓN 32 TOP 5 DE ALERTAS DE DISPONIBILIDAD ALTAS.....	48
ILUSTRACIÓN 33 ATAQUES IPS PERMITIDOS	50
ILUSTRACIÓN 34 ATAQUES IPS DENEGADOS	50
ILUSTRACIÓN 35 TOP DE ACCESOS FALLIDOS PLATAFORMA WINDOWS	51
ILUSTRACIÓN 36 CUENTAS BLOQUEADOS.....	51
ILUSTRACIÓN 37 INCIDENTES POR TIPO DE AMENAZA.....	53
ILUSTRACIÓN 38 INCIDENTES POR FRAUDES DIGITALES	53
ILUSTRACIÓN 39 INCIDENTES POR FUGA DE DATOS.....	53
ILUSTRACIÓN 40 MÉTRICA DE VISITANTES PORTAL WEB WEB.ICETEX.GOV.CO.....	68
ILUSTRACIÓN 41 MÉTRICA ADQUISICIÓN USUARIOS PORTAL WEB WEB.ICETEX.GOV.CO.....	68
ILUSTRACIÓN 42 MÉTRICA DE USUARIO POR PAÍS - PORTAL WEB WEB.ICETEX.GOV.CO	69
ILUSTRACIÓN 43 MÉTRICA DE CIUDADES DE COLOMBIA- PORTAL WEB WEB.ICETEX.GOV.CO	69
ILUSTRACIÓN 44 NODO 1 CPU	70
ILUSTRACIÓN 45 NODO 1 MEMORIA	71
ILUSTRACIÓN 46 NODO 1 ALMACENAMIENTO.....	72
ILUSTRACIÓN 47 EVIDENCIA BACKUP SERVIDORES RESUMEN GENERAL BACKUPS	73

ILUSTRACIÓN 48 EVIDENCIA BACKUP SERVIDORES RESUMEN BACKUPS Y SU ESTADO	73
ILUSTRACIÓN 49 HISTÓRICO CONSOLIDADO USO DE DISCOS SERVIDOR ICTXSRVNETCOR01	81

1. INTRODUCCIÓN

Este informe contiene la información relacionada con las actividades ejecutadas por INFOTIC con ocasión de la celebración del contrato 2022-0792, durante el periodo comprendido entre el 01 al 31 de MARZO 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. Inició desde el 1 de abril de 2023, cuenta con un avance en la ejecución del 97,2 % que representa los 35 meses que lleva dentro de la fase de Operación el proyecto.

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

2. OBJETIVO DEL INFORME

Presentar las actividades ejecutadas por INFOTIC durante el periodo del 01 al 31 de marzo de 2026, con el fin de determinar el estado, la gestión, evolución y la disponibilidad de los servicios especializados prestados al ICETEX en virtud de la ejecución del contrato, para lo cual se han considerado la recolección de mediciones desde las herramientas de monitoreo, el análisis y la

producción de informes y reportes periódicos sobre cada una de las gestiones y demás informes especiales sobre los servicios prestados.

El presente informe comprende:

- **Administración de Seguridad, Redes y Telecomunicaciones:**
Descripción de las acciones ejecutadas en la gestión de redes y telecomunicaciones, con énfasis en la estabilidad, disponibilidad y optimización de la infraestructura.
Reporte de incidentes de seguridad, su impacto y las medidas correctivas implementadas.
- **Conectividad y Red de comunicaciones:**
Estado de las redes LAN/WAN, su desempeño y disponibilidad.
Indicadores de tráfico, calidad de servicio (QoS) y balanceo de cargas.
- **Centro de Datos:**
Estado de operación de los centros de datos, incluyendo disponibilidad, desempeño de servidores, almacenamiento y virtualización.
Acciones de mantenimiento preventivo y correctivo realizadas.
- **Seguridad Informática:**
Medidas implementadas para proteger la información y la infraestructura, como monitoreo, control de acceso, actualizaciones y parches de seguridad.
- **Servicios de Nube:**
Reporte de uso de servicios en la nube, desempeño y cumplimiento de niveles de servicio (SLA).
Descripción de servicios implementados o integrados en el entorno híbrido o multi-nube.
- **Servicios Conexos:**
Detalle de actividades complementarias relacionadas con la infraestructura tecnológica, como soporte técnico de los componentes anteriormente descritos, gestión de incidentes con el seguimiento del servicio de SOC y herramientas Threat Hunting y continuidad del servicio en el marco del componente DRP.

3. ALCANCE

El alcance comprende la descripción de las actividades de los servicios especializados durante el periodo del 01 al 31 de marzo conforme a los frentes definidos por el ICETEX, así:

- **Conectividad y red de comunicaciones**
Este informe presenta el estado del servicio que comprende los componentes exigidos de la arquitectura de conectividad, comunicaciones, software, hardware y dispositivos de seguridad informática, mínimos necesarios para la operación de los servicios establecidos en el contrato 2022-0792.

➤ **Centro de datos**

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

➤ **Seguridad informática**

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

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

➤ **Servicios de nube**

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

➤ **Servicios conexos**

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

4. AVANCE TÉCNICO

4.1. Conectividad y Red de Comunicaciones

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 8 solicitudes, con respecto al mes anterior hubo reducción de 8 casos ya que se atendieron 16 solicitudes en el mes anterior.

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

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

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

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

[inventario de equipos.xlsx](#)

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

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

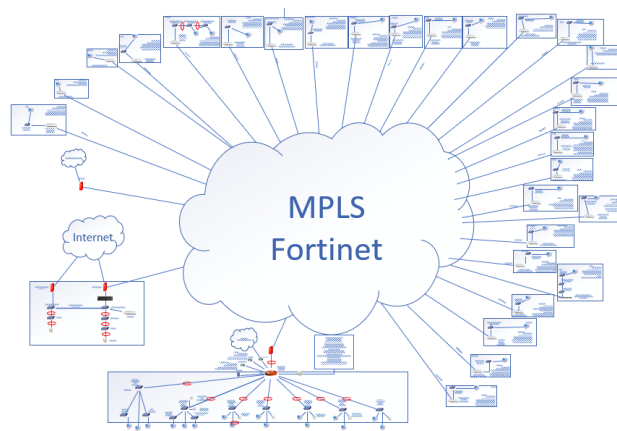


Ilustración 1 Disponibilidad del clúster

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

TOPOLOGIAS DE AGUAS

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

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

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

4.1.1. Canales instalados en el mes y entregables

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

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

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

Canales de Backup. De los 32 canales de Backups previstos en la línea base, se han instalado 30, lo que representa un avance del 96,55%. Actualmente, queda pendiente la instalación del canal de Backup para la oficina en Quibdó, así como un canal entre el sitio principal e ICETEX - Dirección General - Aguas, cuya instalación ya fue descartada por ICETEX.

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

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

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

Los casos atendidos durante el mes están disponibles en el siguiente enlace:

[Registro Aranda Marzo 2026.xlsx](#)

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

Mes	No. Casos
Enero	7
Febrero	16
marzo	8

Tabla 1 Casos atendidos Networking comparativo mes anterior

4.1.2. Despliegue de direcciones IP V6

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

Consecutivo	Sede	Pruebas seguridad	Horario	Observación
1	Aguas	27/08/2025	0:00	Realizadas
2	Chapinero Bogotá	9/09/2025	0:00	Realizadas
3	Cali Prueba 2	29/09/2025	0:00	Realizadas
4	Medellín	2/10/2025	0:00	Realizadas
5	Buenaventura	3/10/2025	0:00	Realizadas
6	Quibdó	7/10/2025	0:00	Realizadas
7	Riohacha	9/10/2025	0:00	Realizadas
8	Montería	10/10/2025	0:00	Realizadas
9	Bucaramanga	16/10/2025	0:00	Realizadas
10	Popayán	17/10/2025	0:00	Realizadas
11	Pereira	20/10/2025	0:00	Realizadas
12	Valledupar	21/10/2025	0:00	Realizadas
13	Santa Marta	23/10/2025	0:00	Realizadas
14	Barranquilla	24/10/2025	0:00	Realizadas
15	Sincelejo	28/10/2025	0:00	Realizadas
16	Tumaco	30/10/2025	0:00	Realizadas
17	Cúcuta	4/11/2025	0:00	Realizadas
18	Villavicencio	6/11/2025	0:00	Realizadas

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

Consecutivo	Sede	Pruebas seguridad	Horario	Observación
19	Tunja	7/11/2025	0:00	Realizadas
20	Cartagena	11/11/2025	0:00	Realizadas
21	Armenia	13/11/2025	0:00	Realizadas
22	Arauca	14/11/2025	0:00	Realizadas
23	Pasto	18/11/2025	0:00	Realizadas
24	Ibagué	20/11/2025	0:00	Realizadas
25	Apartado	21/11/2025	0:00	Realizadas
26	Mocoa	24/11/2025	0:00	Realizadas
27	Yopal	26/11/2025	0:00	Realizadas
28	Manizales	1/12/2025	0:00	Realizadas
29	Neiva	1/12/2025	0:00	Realizadas
30	Ocaña	3/12/2025	0:00	No realizar pruebas de ipv6
31	Puerto Inírida	3/12/2025	0:00	No realizar pruebas de ipv6
32	Puerto Carreño	3/12/2025	0:00	No realizar pruebas de ipv6
33	Florencia	5/12/2025	0:00	No realizar pruebas de ipv6
34	Leticia	5/12/2025	0:00	No realizar pruebas de ipv6
35	Sincelejo	5/12/2025	0:00	Realizadas
36	San Andrés	No se realizará	0:00	No realizar pruebas de ipv6
37	Ángel Bogotá	Pendiente	0:00	Realizadas

Tabla 2 Listado de direcciones IP V6 asignadas a las oficinas

4.1.3. Implementación canales SDWAN

Durante el presente mes, el ICETEX formalizó la recepción de los canales SDWAN, según consta en el acta del link: [Acta de Entrega Canales SD-WAN .pdf](#)

4.1.4. Recomendaciones

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

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

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

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

4.2. Centro de Datos

4.2.1. Centro de Datos Principal

4.2.1.1. Aplicaciones

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

Las actividades desarrolladas estuvieron enfocadas principalmente en:

- **Despliegues y actualizaciones en producción:** Se realizaron actualizaciones de archivos productivos como `udplegalizar`, `condiciones2021.asp`, `loggingestion.asp` y el archivo `Cronograma_Cierre_Contable_2026.xlsx`, asegurando la correcta implementación de cambios solicitados y la disponibilidad de información actualizada para los procesos institucionales.
- **Atención de incidentes:** Se gestionó el incidente relacionado con el botón de pago PSE, el cual fue atendido y solucionado de manera oportuna, restableciendo la operación normal del servicio afectado.
- **Gestión de accesos y permisos:** Se atendieron múltiples solicitudes de asignación de permisos FTP para usuarios institucionales, garantizando accesos controlados y seguros 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 durante el mes se presentaron dos controles de cambio, el 20824 y 20830, los cuales fueron ejecutados exitosamente.

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

políticas de respaldo sobre esa información, si se están ejecutando y alternativas para optimizar dicho espacio.

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

Se continua con la actualización del inventario de los servidores con los servicios que allí se prestan, el cual puede ser consultado en el siguiente enlace [Revision IIS Marzo2026.xlsx](#)

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

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

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

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

Además, con base a los registros de los últimos tres meses (enero a marzo 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	pasarelapagos.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.

Proveedor	Sitio Web	App Pool	Estado	Parent(s)	Certificado SSL	Seguridad (Readers)	Logging	Framework	Reciclaje	Actualización / Año	Worker Processes Máximo
ICTS/INFORMACION (192.168.51.165)	AhorroMedioAmbiente	AhorroMedioAmbienteApp	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20%	Última act. 13/02/2025	1
	AplicacionesMódulo	AplicacionesMódulo	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20%	Última act. 13/02/2025	1
	AplicacionesMasivo	AplicacionesMasivo	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20%	Última act. 30/03/2025	1
	AplicacionesNCA	AplicacionesNCA	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20%	Última act. 13/02/2025	1
	CargasArduas	ICTEXX_CargasArduas	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20%	Última act. 13/02/2025	1
	CondicionesCIE	WebCondicionesCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20%	Última act. 19/06/2024	1
	CondicionesCIE	WebCondicionesCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20%	Última act. 13/02/2025	1
	CondicionesCIEVFA	WebSiteCondicionesCIEVFA	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 40.00 AM	sin cambios	1
	ConsultaPlanBeneficios	ConsultaPlanBeneficios	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 40.00 AM	sin cambios	1
	ConsultaPlanBeneficiosCIE	ConsultaPlanBeneficiosCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 40.00 AM	sin cambios	1
	CuentasAbandonadas	WebSiteCuentasAbandonadas	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	sin cambios	1
	CuentasAbandonadas	WebSiteCuentasAbandonadas	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	sin cambios	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
	CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/2025	1	
CuentasActivasPreCIEAPI	CIAPIPreCIE	Active	443	Valido 4/12/2025	X-Frame-Options: Strict-Transport-Security	SI	NET 4.0	Si 20.00 AM	Última act. 19/03/20		

Tabla 4 Inventario principales servidores producción

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

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

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

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

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. 53^a-26 Arboleda
Alta.
NIT: 900.068.796-1
Teléfono: (+606) 88612612

En el presente mes se ajustaron las configuraciones de los siguientes parámetros:

Nombre del parámetro	Configuración gpedit.msc	Configuración secpol.msc	rsop	Configuración recomendada	Descripción	Recomendación para IIS
Devices: Allowed to format and eject removable media	No Defined	No Defined	Not Defined	Administrators	Controla quién puede formatear/expulsar medios.	✓ Aplicar
Interactive logon: Do not display last user name	Disabled	No Defined	Not Defined	Enabled	Ocultar último usuario autenticado en logon.	✓ Aplicar
Interactive logon: Require CTRL+ALT+DEL	Disabled	Disabled	Disabled	Enabled	Obliga Ctrl+Alt+Del al iniciar sesión.	✓ Aplicar
Microsoft network server: Digitally sign communications (always)	Disabled	Disabled	Enable	Enabled	Firma comunicaciones SMB entrantes obligatoriamente.	✓ Aplicar
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	Disabled	Not Defined	Enabled	Evita listar recursos y usuarios de forma anónima.	✓ Aplicar
User Account Control: Admin Approval Mode for the Built-in Administrator account	No Defined	No Defined	Not Defined	Enabled	Habilita UAC para cuenta Admin integrada.	✓ Aplicar

Tabla 5 Parámetros de sistema Operativo- componente de seguridad Windows Defender Firewall

El resto de las configuraciones, así como su recomendación pueden ser consultadas en el siguiente enlace:

Anexo: [Ajustes de hardening en políticas de seguridad.pdf](#)

4.2.1.2. Bases de Datos

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

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

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

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

OEM		BASES DE DATOS		VERSION	
10.1.4.96		EMCLOUD	12.2.0.1.0		

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

BASES DE DATOS	VERSION	TAMAÑO
ASMn user grid	19.29.0.0.0	GB
ICTXCYC	11.0.2.0.4	5.647
ICETEX	11.0.2.0.4	209
APLICATI	11.0.2.0.4	245
APOTEOSY	11.0.2.0.4	483
VIGIAPRD	19.29.0.0	217
LIFERAY LIFERAYPDB	19.29.0.0	24
LANDICTX	19.29.0.0	615
SGDEA	19.29.0.0	159

Tabla 7 Estado BD Oracle

Resultado del proceso de administración se destacan las siguientes actividades:

- 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.
- Se resolvieron los casos asignados a los administradores de base de datos en los tiempos estipulados por prioridad.
- Se atendieron todas las reuniones solicitadas por el ICETEX.
- Se realizaron los mantenimientos de los espacios de los filesystem /oracle /grid /opt /DATOS de las maquinas donde se encuentran alojadas las bases de datos para su correcto funcionamiento.
- Se validaron los respaldos de las bases de datos de los archive log, 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.
- Se realizaron actividades de tuning base de datos SGDEA (Control Doc)
- Se realizaron los mantenimientos de los espacios de los filesystem /oracle /grid /opt /DATOS de las maquinas donde se encuentran alojadas las bases de datos para su correcto funcionamiento.
- La disponibilidad del Clusterware BD para el mes de marzo de 2026 fue del 100% como se evidencia en la siguiente ilustración:

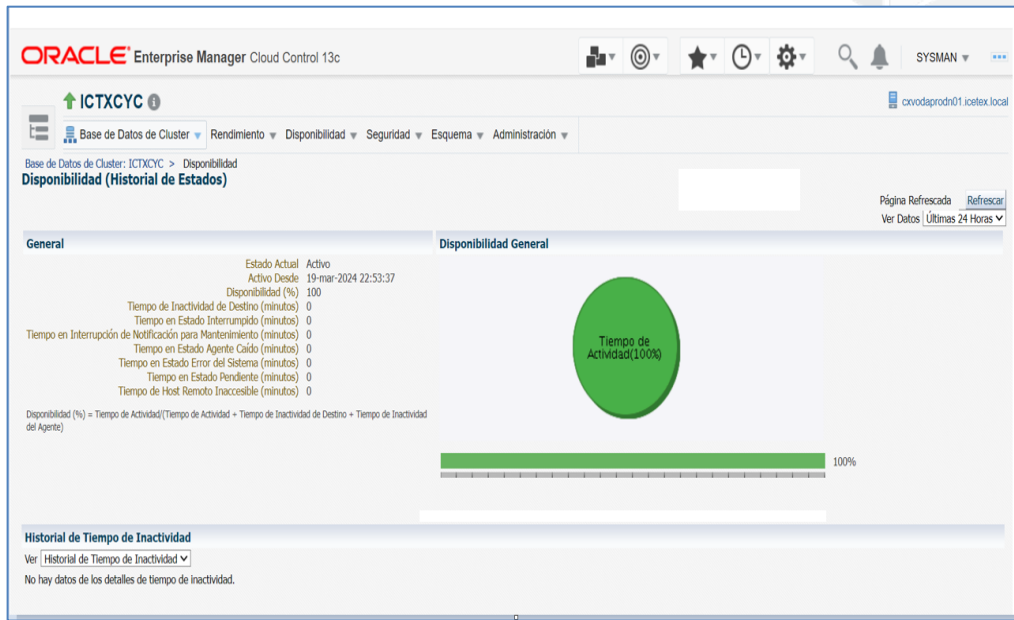


Ilustración 2 Disponibilidad del cluster

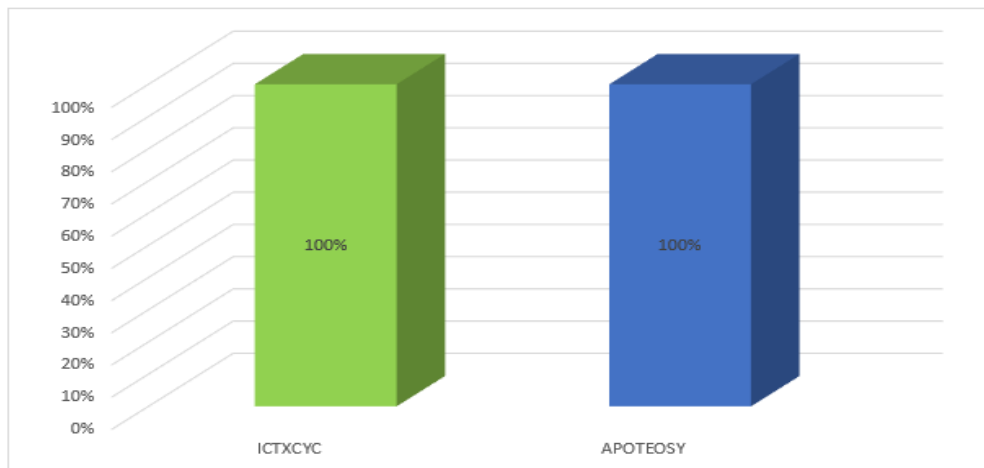


Ilustración 3 Disponibilidad de las Bases de Datos principales ICTXCYC y APOTEOSY

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

La versión de base de datos 11 G ya no tiene soporte por Oracle la versión que en este momento tiene soporte es 19C y, en la actualidad, se cuentan con 5 base de datos operando en esta versión. Se ha brindado soporte, al equipo de sistemas de información del ICETEX, en el proceso de

migración a la versión 19c, siendo la base de datos con la que se dio inicio APOTEOSYS en el mes de agosto y hemos apoyado en las tareas que se adelantan con respecto a CICETEX.

Se adelantó la ventana de mantenimiento, para finalizar el parchado a la versión 19.29 sobre el home de oracle y grid en cada nodo del rac, en particular el elemento que quedo faltando de las actividades adelantadas en el mes de febrero. Nos referimos al parchado de DATAGUARD.

Procederemos a programar una nueva ventana para llevarla a la versión correspondiente

➤ **Casos del proyecto Gestionados por Bases de datos:**

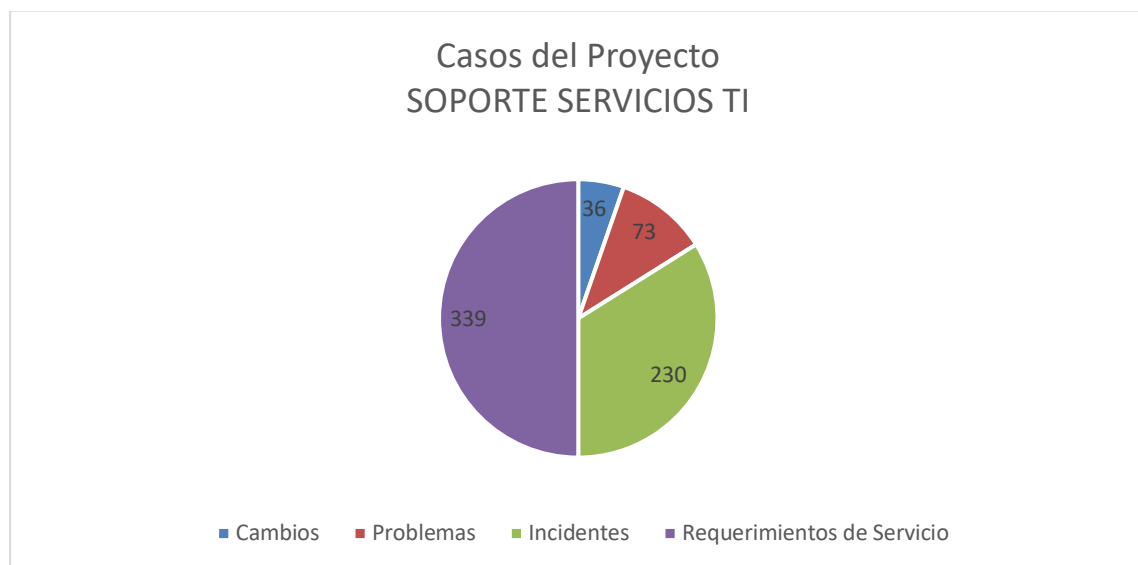


Ilustración 4 Casos del proyecto Gestionados Aranda Bases de datos

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.

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

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

BASE DE DATOS	"AGO 2025"	"SEPT 2025"	"OCT-2025"	"NOV 2025"	"DICIEMBRE 2025"	ENERO 2026	FEBRERO 2026	"MARZO 2026"
ICTXCYC	4,766	4,774	4,923	4,925	4,996	5,259	5,445	5,647
ICETEX	206	206	206	207	207	209	209	209
APLICATI	243	243	243	243	244	244	245	245
APOTEOSY	460	480	481	481	481	482	483	483
VIGIAPRD	143	166	175	178	188	200	211	217
LIFERAY LIFERAYPDB	8	8	8	8	8	23	23	24
LANDICTX	529	529	529	554	584	596	612	615
SGDEA	124	136	140	143	147	151	155	159
TOTAL==>	6,479.00	6,542.00	6,705.00	6,738.56	6,855.06	7,164.44	7,383.57	7,599.00
CRECIMIENTO		63.00	163.00	33.56	116.50	309.38	219.13	215.43

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

Replicación

Durante el mes de marzo 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

Durante el mes de marzo se continuo con el monitoreo permanente a los portales sobre los que opera el ICETEX, manteniendo, las alertas y reportes a tiempo en caso de que se presentara algún evento que pudiera ocasionar una interrupción en la prestación de los servicios que se ofrecen a través de los portales, este informe se encuentra detallado en el documento [Informe Mensual InfoTIC Seguridad Marzo2026.pdf](#)

En cuanto a la disponibilidad del portal web de la entidad se presentan unos uptime superiores al 98.609% como se evidencia en la siguiente gráfica:



Ilustración 5 UPTIME: Portal WEB web.icetex.gov.co [98,609%]

Durante en el mes de marzo no se escalaron requerimientos en la mesa de servicios.

Los incidentes disminuyeron en un 50%, los 2 incidentes fueron escalados por error por la mesa de servicios.

Los casos internos (Claro) aumentaron en un 37.5%, debido al caso de acompañamiento con los especialistas para las dos ventanas de mantenimiento de actualización del kernel y optimización de los tres nodos de Elasticsearch. También los tres casos de redireccionamiento que solicitó la OCM, los casos de llenado de caché en la partición / nodo 1 y 2 de Liferay, acompañamiento de los especialistas para validar información en el diagrama físico y el reinicio de la máquina INR0243 - 192.168.20.40 realizado el 22 de marzo a las 21:04 horas.

El sábado 14 de marzo a las 10:00 p.m, se llevó a cabo la actualización del kernel del servicio NFS - 192.168.20.42, a versión 4.18.0-348.7.1.el8_5.x86_64, terminando la ventana de mantenimiento el domingo 15 de marzo a las 2:00 a.m, con el objetivo de mantener el sistema operativo actualizado, reduciendo exposición a vulnerabilidades, mejorando estabilidad bajo carga, optimizando el rendimiento de I/O como la comunicación en red, garantizar la compatibilidad con drivers y controladores del entorno.

En el mes, se presenta un promedio de 750GB 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.

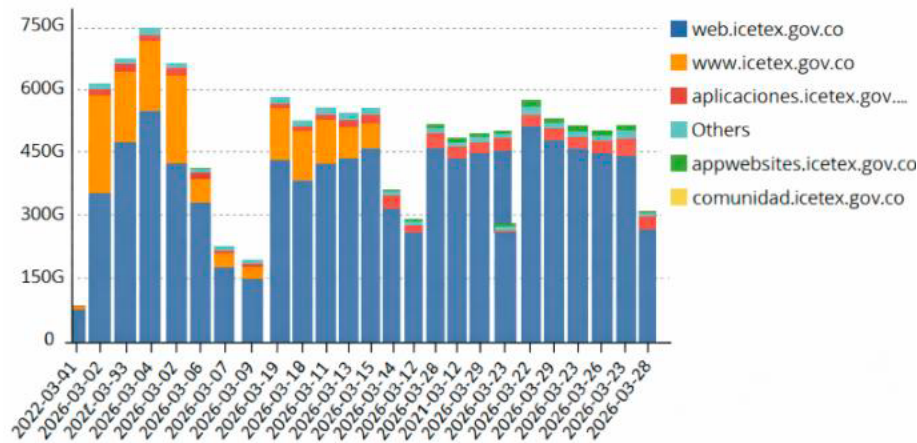


Ilustración 6 Tráfico General De Los Portales

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	119,094	83.24%
2	aplicaciones.icetex.gov.co	13,314	9.31%
3	www.icetex.gov.co	5,353	3.74%
4	crmweb.icetex.gov.co:777	2,636	1.84%
5	pasareladepagos.icetex.gov.co	1,748	1.22%
6	gestordeservicios.icetex.gov.co	517	0.36%
7	webhook.icetex.gov.co	242	0.17%
8	appwebsites.icetex.gov.co	120	0.08%
9	comunidad.icetex.gov.co	34	0.02%
10	www.icetex.gov.co:443	13	0.01%
Total		143,071	100.00%

Tabla 9 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

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

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

4.2.1.4. Servicios de DRP

[InformeGerencial_Icetex_PruebaAislada_20260323.pdf](#)

El 23 de marzo se ejecutó, la actividad programada, del DRP, los informes de resultado de la actividad se pueden consultar en el siguientes link: [DRP](#)

4.2.1.4.1. Alcance

Probar la integridad, confidencialidad y disponibilidad de la información del portal web en contingencia y estimar el tiempo que tomaría disponibilizar este portal y acceder a secciones para realizar todas las actividades por medio de las cuales se evidencie su funcionamiento.

4.2.1.4.2. Objetivo

Principal: Probar el Portal Web ICETEX de manera Aislada en Megacenter; con el fin de probar las aplicaciones en ambiente controlado sin afectar la operación de producción.

Específicos:

- Asegurar la disponibilidad de los recursos de infraestructura tecnológica que soportan los servidores de Portal Web Icetex Productivo (LIFERAY) y servidor de aplicaciones MIRA de ICETEX de modo Aislado en el sitio alterno(Megacenter).
- Ejecutar validaciones técnicas, conectividad y pruebas funcionales formulario “Renovación de crédito” de modo Aislado en el sitio alterno(Megacenter).

4.2.1.4.3. Escenario seleccionado

Falla de Conectividad de Red

4.2.1.4.4. Acción

Simular una interrupción de la red que aísla el Datacenter principal y se levanta el alterno de forma paralela.

La prueba culminó de forma satisfactoria y el balance y recomendaciones se entregarán en la 2da semana del mes de abril.

4.2.2. Centro de Datos Alterno

4.2.2.1. Hosting Virtual (IaaS)

En el transcurso del mes de marzo, 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 Marzo 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 -> vmegacenter.datacenterdhs.local) cuenta con **10** replicas

General					
Name			Count		
OK			9		
Incremental Sync			1		
Grupo de protección: PG_INFOTIC_7 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0226_INFOTIC_REP	OK	5 of 5	Mar 31, 2026	15.44 MB	5 minutes
Grupo de protección: PG_INFOTIC_6 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0228_INFOTIC_REP	OK	1 of 1	Mar 31, 2026	99.54 MB	1 hour
INR0229_INFOTIC_REP	OK	1 of 1	Mar 31, 2026	60.15 MB	1 hour
Grupo de protección: PG_INFOTIC_1 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0233_INFOTIC_REP	OK	3 of 3	Mar 31, 2026	35.02 MB	1 hour
Grupo de protección: PG_INFOTIC_4 (3)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0238_INFOTIC_REP	OK	2 of 2	Mar 31, 2026	31.03 MB	1 hour
INR0239_INFOTIC_REP	OK	2 of 2	Mar 31, 2026	48.98 MB	1 hour
INR0243_INFOTIC_REP	Incremental Sync	2 of 2	Mar 31, 2026	24.28 GB	1 hour
Grupo de protección: PG_INFOTIC_3 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0244_INFOTIC_REP	OK	1 of 1	Mar 31, 2026	82.48 MB	1 hour
INR0245_INFOTIC_REP	OK	1 of 1	Mar 31, 2026	6.45 MB	5 minutes
Grupo de protección: PG_INFOTIC_2 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0249_INFOTIC_REP	OK	2 of 2	Mar 31, 2026	11.39 MB	5 minutes

Ilustración 7 Reportes de replicación SRM a Sitio Alterno – marzo 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	icetexbogwsmira	Portal Web	INR0226_INFOTIC_REP
2	INR0207	ictxisgesbd	Sisgestion	INR0228_INFOTIC_REP
3	INR0206	ictxisgesapp	Sisgestion	INR0229_INFOTIC_REP
4	INR0220	icetexboglxorfeo1	ORFEO	INR0233_INFOTIC_REP
5	INR0219 **	icetexboglxorfeo2	ORFEO	INR0262_INFOTIC_REP
6	INR0208 *	ICTXBOGSRVPT1	Portal Transaccional	INR0236_INFOTIC_REP
7	INR0210	icetexbogliferaynfs	Portal productivo (liferay)	INR0238_INFOTIC_REP
8	INR0217	icetexbogelasticserver1	Portal productivo (liferay)	INR0239_INFOTIC_REP
9	INR0218	icetexbogliferayserver1	Portal productivo (liferay)	INR0243_INFOTIC_REP
10	INR0215	icetexboglxdarumasrv1	DARUMA	INR0244_INFOTIC_REP
11	INR0213	icetexboglxdarumasrv2	DARUMA	INR0245_INFOTIC_REP
12	INR0214	icetexboglxroad1	XROAD	INR0249_INFOTIC_REP

Tabla 11 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 -icetexboglxorfeo2

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

INR	HOSTNAME	GB
INR0243	icetexbogliferayserver1	166,0
INR0249	icetexboglxroad1	23,9
INR0226	icetexbogwsmira	5,2
INR0228	ictxisgesbd	4,7
INR0239	icetexbogelasticserver1	3,2

Tabla 12 TOP 5 máquinas mayor tasa de transferencia

INR	HOSTNAME	GB
INR0233	icetexboglxorfeo1	2,8
INR0244	icetexboglxdarumasrv1	1,8
INR0229	ictxisgesapp	1,5
INR0238	icetexbogliferaynfs	1,3
INR0245	icetexboglxdarumasrv2	0,2

Tabla 13 TOP 5 máquinas menor tasa de transferencia

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

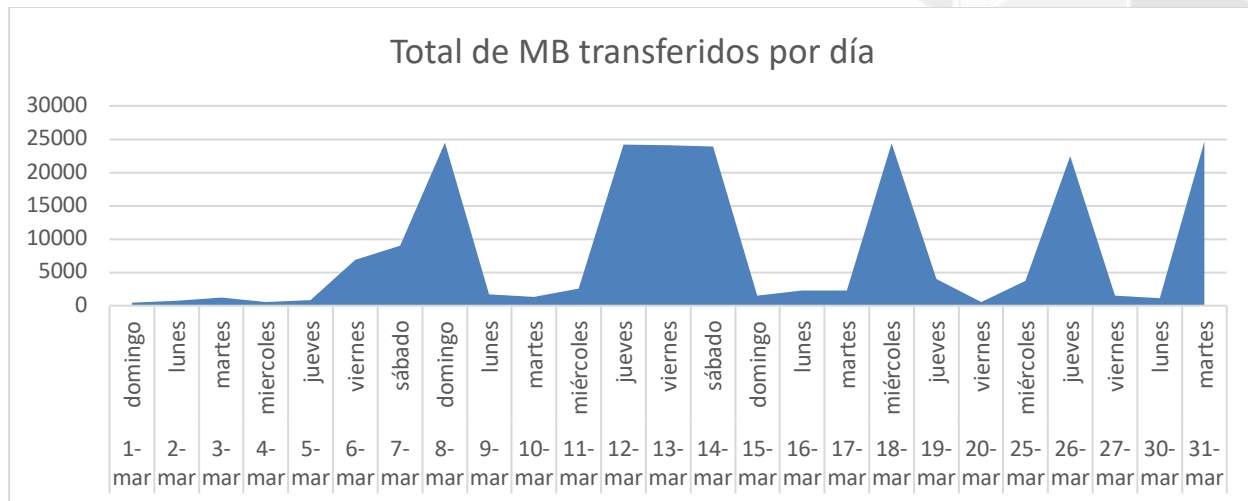


Ilustración 8 Fechas con mayor replicación

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

- La transferencia de datos está altamente concentrada en la máquina virtual INR0243, esta VM representa aproximadamente el **78.8% del tráfico total** del mes que fue **165,996.54 MB** (aprox. **166 GB**)
- El tráfico total de replicación en marzo fue de 210,441.4 MB (210.44 GB).
- El salto registrado entre diciembre y enero (213 GB) tuvo una réplica casi idéntica en marzo (210 GB), tras una caída del 51% en febrero (102 GB). Esta tendencia indica que, además de los cierres de año fiscal, existen procesos trimestrales o de cierre de ciclo que generan una carga de escritura en disco significativamente mayor.
- La infraestructura ha dejado de mostrar la "estabilización" observada en febrero para retornar a un estado de alta demanda.
- **El día de mayor tráfico** fue el **31 de marzo**, con un acumulado total de **24,655.04 MB** (principalmente por INR0243 la cual cerró con el pico individual más alto para la VM INR0243 (**24,280 MB**), confirmando que los cierres de mes disparan la tasa de cambio de datos.
- El **13 de marzo** se registró un evento inusual en la VM **INR0249** correspondiente a icetexboglxroad1 con **23,410 MB**, lo cual es un comportamiento atípico para ese servidor (que promedia sólo aproximadamente 10 MB diariamente).

4.2.2.2. DataGuard Bases de Datos Megacenter

Durante el mes de marzo 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 marzo2026.pdf](#)

```

oracle@cxvodacontg011:~$ ps -fea |grep pmon
oracle 502 1 0 Feb28 ? 00:12:40 ora_pmon DBP1VOT
oracle 12290 32219 0 19:29 pts/1 00:00:00 grep --color=auto pmon
oracle 16690 1 0 Mar23 ? 00:03:57 ora_pmon LIFERAYD
grid 21929 1 0 Feb28 ? 00:07:49 asm_pmon +ASM
oracle 25656 1 0 Mar25 ? 00:04:30 ora_pmon ICTXCYCD
oracle 26070 1 0 Feb28 ? 00:14:11 ora_pmon APOTEOSD
oracle 27395 1 0 Feb28 ? 00:10:00 ora_pmon LANDICTD
oracle 28275 1 0 Feb28 ? 00:08:31 ora_pmon SGDEAD
oracle 28527 1 0 Feb28 ? 00:09:35 ora_pmon VIGIADTG

[oracle@cxvodacontg011 ~]$ . oraenv
ORACLE_SID = [ICTXCYCD] ?
ORACLE_BASE environment variable is not being set since this
information is not available for the current user ID oracle.
You can set ORACLE_BASE manually if it is required.
Resetting ORACLE_BASE to its previous value or ORACLE_HOME
The Oracle base remains unchanged with value /oracle/app/oracle/product/product/11.2.0/dbhome_1
[oracle@cxvodacontg011 ~]$ cat fapfly.sqlplu^C1
[oracle@cxvodacontg011 ~]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.4.0 Production on Mon Apr 6 19:30:02 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 fapfly

  Thread Last Sequence Received Last Sequence Applied TIME_RECEIVED TIME_APPLIED
  -----
1          258054          258054 06/04/2026 19:27 06/04/2026 19:27
2          205294          205294 06/04/2026 19:27 06/04/2026 19:27

SQL> sta uapfly

  Thread Last Sequence Received Last Sequence Applied Difference
  -----
1          258054          258054          0
2          205294          205294          0
  
```

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 alternativo en Medellín, las cuales estuvieron disponibles todo el mes de marzo 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 14 Disponibilidad de Servicios de Housing – Data Center Alterno

4.3. Seguridad informática

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

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

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

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

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

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

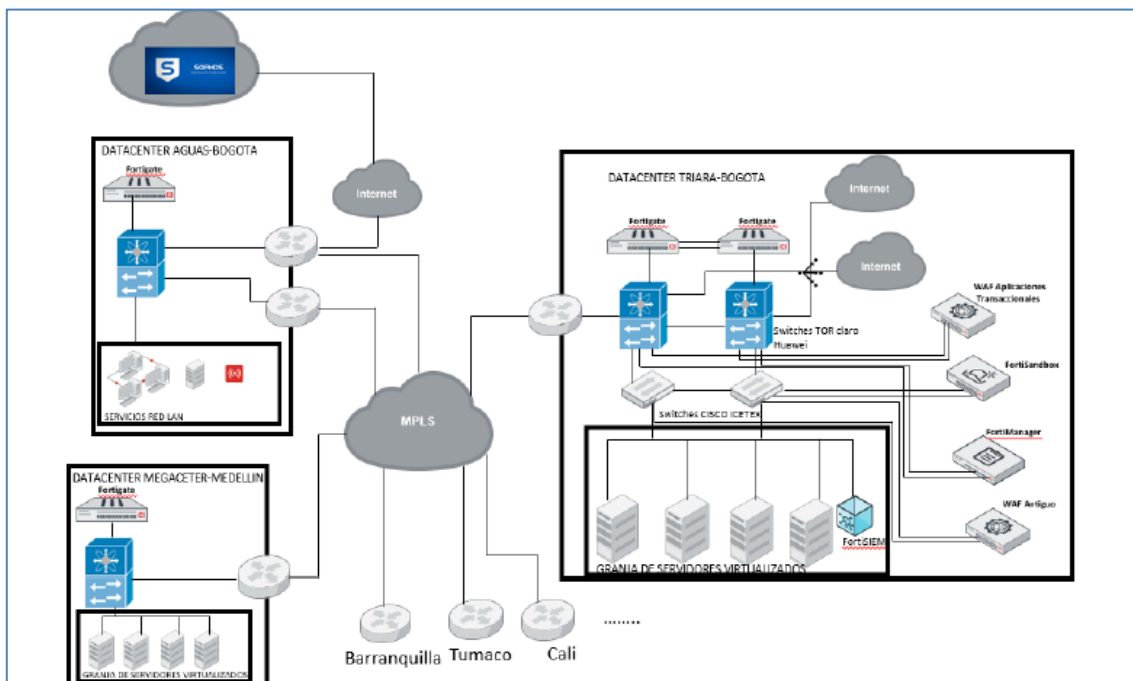


Ilustración 10 Diagrama de la Arquitectura de Seguridad

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

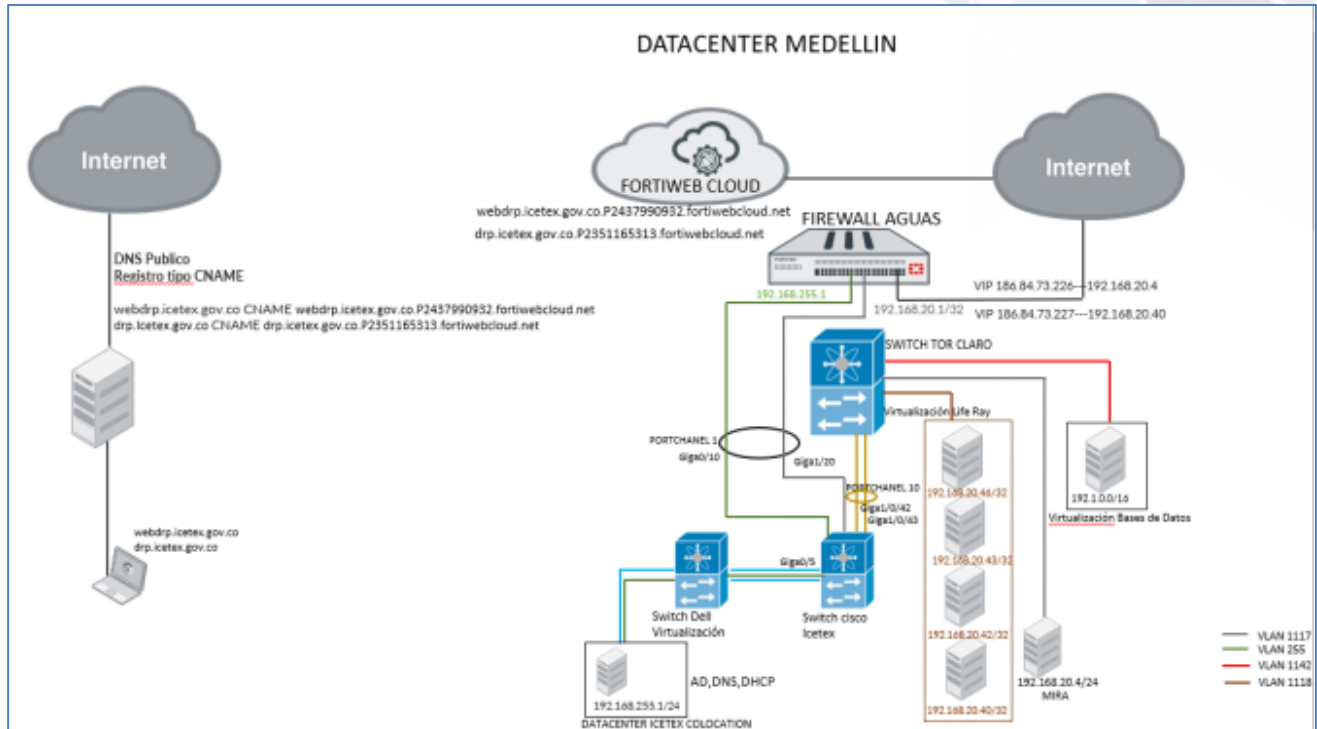


Ilustración 11 Topología de WAF Cloud usado en portales de Medellín

En el ámbito de la gestión de políticas de seguridad, se realizaron configuraciones sobre IPv6, permitiendo el tráfico para la prueba de las sedes.

Se realizó la configuración de VPN Site To Site para el análisis de vulnerabilidades InfotIC.

Se realiza configuración de VPN SSL para ayudar a la conexión del web máster a el ambiente de pruebas.

Se realiza el ajuste a nivel del CPU para el FortiSIEM.

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

Las evidencias de esta gestión fueron incluidas en el numeral 6.2 del informe mensual de especialistas de seguridad del mes de febrero, link: [Informe Mensual InfoTIC Seguridad Marzo2026.pdf](#)

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

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

- **Gestión y fortalecimiento de la seguridad perimetral.**

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

- Se realizó la actualización de las plataformas de seguridad.
- Se realizó los ajustes de los permisos requeridos para las bases de datos de producción.

- **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 identificados como falsos positivos, con el fin de apoyar los ajustes y afinamientos necesarios.

- **Gestión Operativa y soporte de seguridad**

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

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

4.3.1. 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 infotíc
FG180FTK22901087	FortiGate 1800F	Data Center Triara	Funciona como Firewall - Prestación como servicio infotíc
FG180FTK22901182	FortiGate 1800F	Backup Data Center Triara	Funciona como Firewall - Prestación como servicio infotíc
FG6H0FTB22902086	FortiGate 600F	Data Center Megacenter Medellín	Funciona como Firewall - Prestación como servicio infotíc
FV-2KFTE21000029	FortiWeb 2000F	Data Center Triara	Función como WAF - Prestación como servicio infotíc

SERIAL	MODELO	UBICACIÓN FÍSICA	OBSERVACIONES
FMG2HGTA22000550	FortiManager 200G	Data Center Triara	Prestación como servicio infotíc
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 15 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

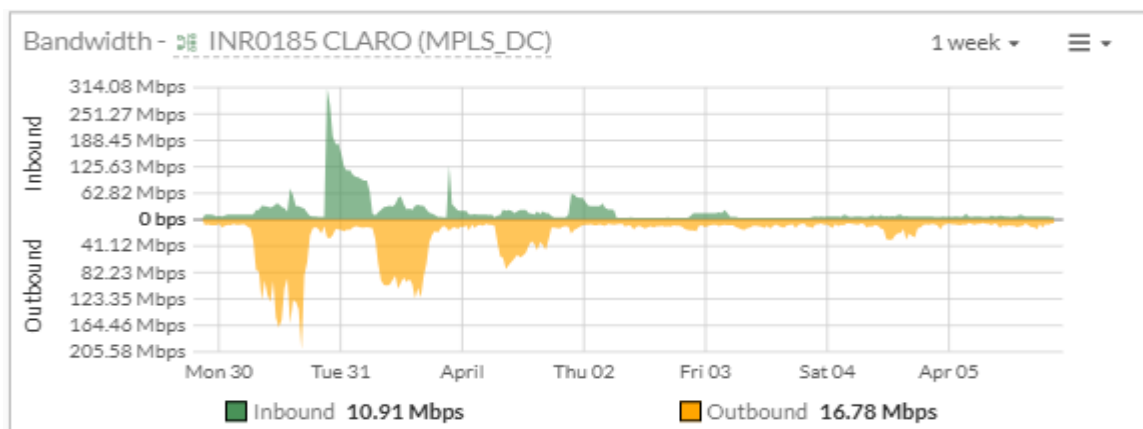
Tabla 16 Licenciamiento FortiGate

4.3.1.1. 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:



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

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

Ilustración 12 Consumo canal MPLS - promedio 84.23 MPPSG [INR0185 CLARO(MPLS_DC)]

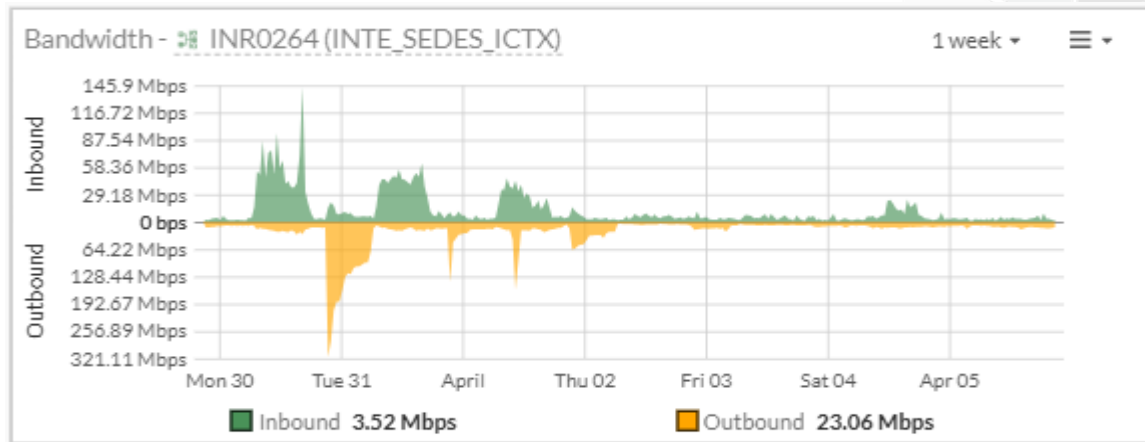


Ilustración 13 Consumo canal Internet Sedes - Promedio 133.49 MBPS WAN-SEDES-ICETEX [INR0264 (INTE_SEDES_ICTX)]

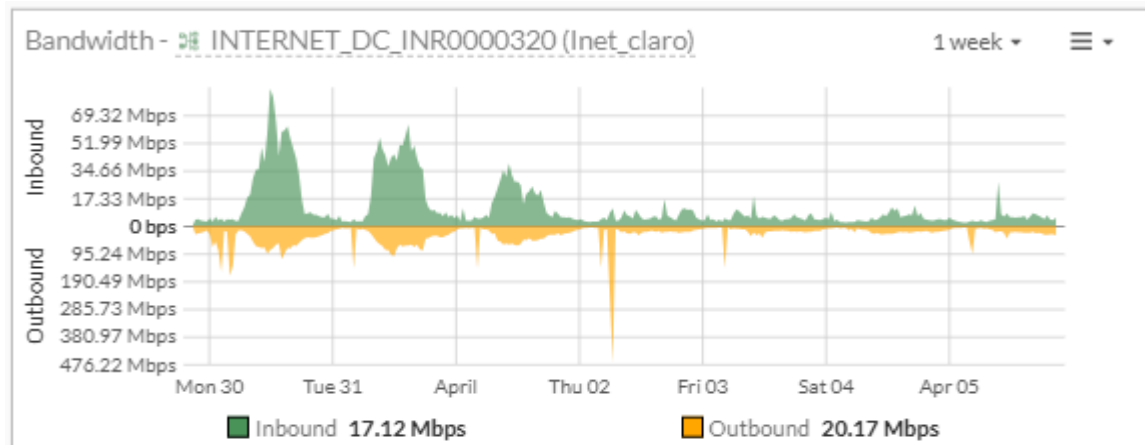


Ilustración 14 Consumo Canal Internet Data Center- INTERNET DATACENTER [INTERNET_DC_INR0000320 (Inet_claro)]

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:

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

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

	Name	Comments	Ref.
WEB	default	Perfil con las mínimas restricciones	0
WEB	Navegacionpcs_Comware	Perfil con restricciones	2
WEB	Navegacionpcs_Comware_con_redes	Perfil con restricciones	1
WEB	WF-Avanzado	Perfil para FSSO Navegación Avanzada	31
WEB	WF-Comunicaciones	Perfil para FSSO comunicaciones	2
WEB	WF-General	Perfil para todos	5
WEB	WF-General_Sedes	Perfil para todos	1
WEB	WF-Sede_Ibague_YT	27022025/InfoTIC/Tarea Aranda 517214 (17458) Se solicita el acc...	1
WEB	WF-Tesoreria	Perfil con restricciones especificas por auditoria.	4
WEB	WF-VIP	Perfil para FSSO Navegación_VIP	16
WEB	WF-wetransfer	Perfil para FSSO Navegación Avanzada	1
WEB	wifi-default	Perfil de FULL acceso para pruebas	1

Ilustración 15 Filtrado – WEB – (FortiGate – Triara)

	Name	Comments	Ref.
SSL	custom-deep-inspection	Customizable deep inspection profile.	0
SSL	deep-inspection	Read-only deep inspection profile.	0
SSL	certificate-inspection_2780	Read-only SSL handshake inspection profile.	1
SSL	certificate-inspection_IPv6	Read-only SSL handshake inspection profile.	1
SSL	Prueba certificate-inspection	Read-only SSL handshake inspection profile.	12
SSL	certificate-inspection_ICETEX	SSL para BUS de servicios	31
SSL	no-inspection	Read-only profile that does no inspection.	230
SSL	certificate-inspection	Read-only SSL handshake inspection profile.	400

Ilustración 16 Inspección – SSL – (FortiGate – Triara)

	Name	Comments	Ref.
AV	AV-FSB	HTTP,SMTP FULL FSB	73
AV	AV-HTTP	HTTP con FSB	25
AV	AV-HTTP&CIFS	HTTP,CIFS con FSB	4
AV	AV-SMTP	SMTP FULL FSB	1
AV	default	ALL con FSB	40
AV	ICETEX		65
AV	prueba2		57
AV	wifi-default	ALL monitoreo sin FSB	1

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

4.3.1.2. FortiGate Aguas

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

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

A continuación se presentan los consumos en el presente mes:

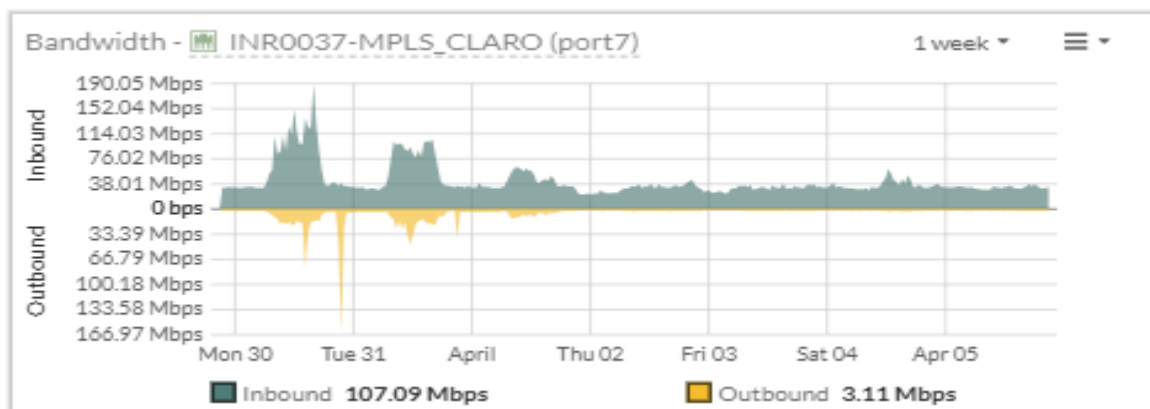


Ilustración 18 Consumo Canal MPLS Aguas - promedio 44.72 MBPS

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

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

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

	Name	Comments	Ref.
WEB	default	Default web filtering.	0
WEB	General_Icetex		51
WEB	monitor-all	Monitor and log all visited URLs, flow-based.	0
WEB	VIP_FUNCIONARIOS		3
WEB	wifi-default	Default configuration for offloading WiFi traffic.	1

Ilustración 19 Filtrado-Web-(FortiGate-Aguas)

	Name	Comments	Ref.
SSL	certificate-inspection	Read-only SSL handshake inspection profile.	275
SSL	certificate-inspection_WX	Read-only SSL handshake inspection profile.	2
SSL	custom-deep-inspection	Customizable deep inspection profile.	0
SSL	custom-deep-inspection_icetex	Customizable deep inspection profile.	0
SSL	deep-inspection	Read-only deep inspection profile.	0
SSL	no-inspection	Read-only profile that does no inspection.	239

Ilustración 20 Inspección-SSL-(FortiGate-Aguas)

	Name	Comments	Ref.
AV	AV-ICETEX		242
AV	default	Scan files and block viruses.	4
AV	wifi-default	Default configuration for offloading WiFi traffic.	1

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

4.3.1.3. FortiGate Medellín

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

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

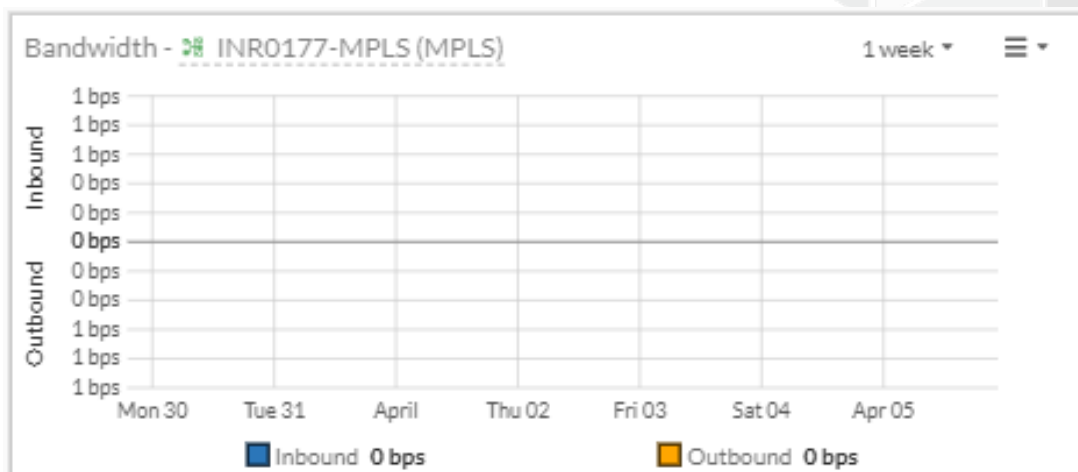


Ilustración 22 Consumo Canal MPLS Medellín

4.3.1.4. FortiWeb 2000F

A nivel de sistema del FortiWeb su versión de firmware se encuentra actualizada a la versión 7.6.5 la cual es una de las versiones actuales más estables.

4.3.1.5. FortiWeb 2000E

A nivel de sistema, el FortiWeb presenta su configuración actual y su versión de Firmware fue actualizada a la 7.6.7. Sin embargo, cabe aclarar que, a nivel de licenciamiento, los equipos no tienen un licenciamiento vigente en este momento.

Dispositivo	IP	Propiedad Ictex	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 17 Licenciamiento FortiWeb

En el mes, se presenta un promedio de 750GB de tráfico general hacia los portales protegidos por el FortiWeb donde el portal de web.ictex.gov.co y www.ictex.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.

#	HTTP Host	Hits	% of Total
1	web.icetex.gov.co	119,094	83.24%
2	aplicaciones.icetex.gov.co	13,314	9.31%
3	www.icetex.gov.co	5,353	3.74%
4	crmweb.icetex.gov.co:777	2,636	1.84%
5	pasareladepagos.icetex.gov.co	1,748	1.22%
6	gestordeservicios.icetex.gov.co	517	0.36%
7	webhook.icetex.gov.co	242	0.17%
8	appwebsites.icetex.gov.co	120	0.08%
9	comunidad.icetex.gov.co	34	0.02%
10	www.icetex.gov.co:443	13	0.01%
Total		143,071	100.00%

Ilustración 23 Tráfico General de los portales

4.3.1.6. FortiWebCloud DRP

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

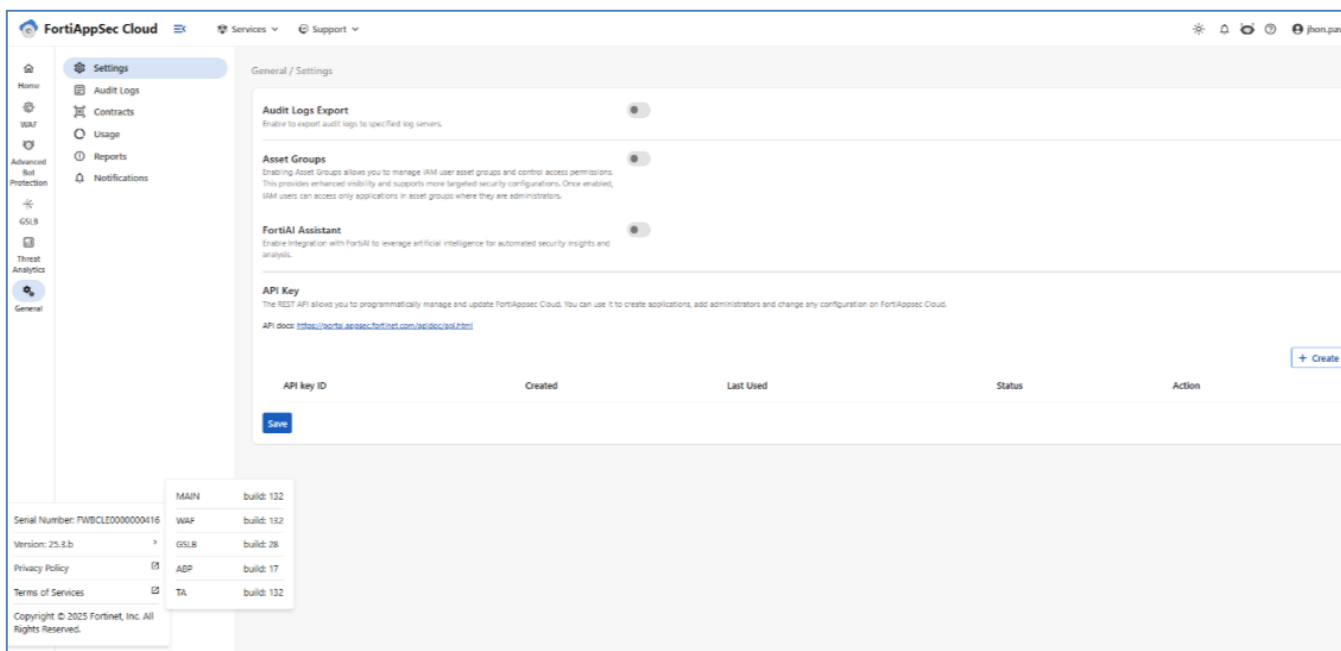


Ilustración 24 Tráfico General de los portales

4.3.1.7. 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

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

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

este 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 18 Configuración FortiSandBox 1000D

4.3.1.8. FortiSIEM

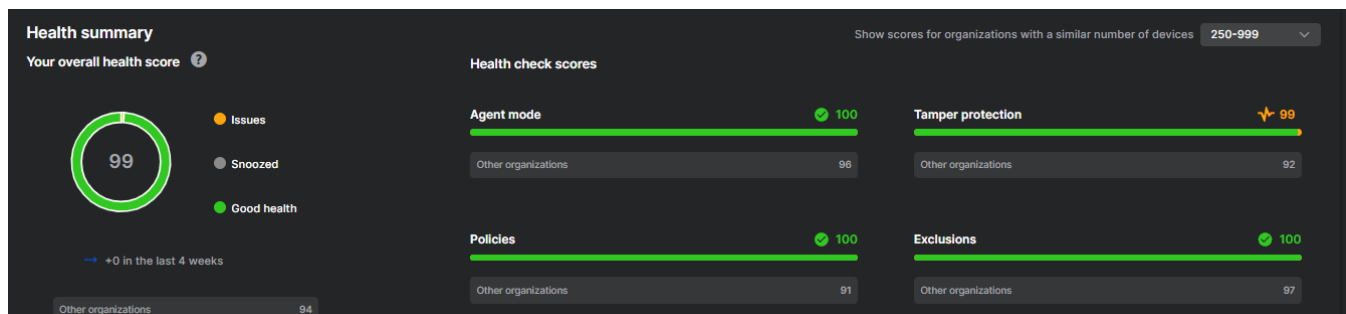
A continuación, se presenta el desempeño por procesos:

General Usage Nodes			Upload License	
Serial Number:	FSMP000000001340			
Hardware ID:	4212F192-8EF3-61A8-F30D-4EAF9DE2E3F6			
License Hardware ID:	4212F192-8EF3-61A8-F30D-4EAF9DE2E3F6			
License Type:	Enterprise			
FIPS Mode:	Disabled			
Attribute	Value	Expiry		
Devices	200	Perpetual		
Total EPS	2000	Perpetual		
Agents	100	Perpetual		
UEBA	75	Perpetual		
IOC Service	Valid	Apr 19, 2026		
Maintenance and Support	Valid	Apr 19, 2026		
High Availability Service	N/A	N/A		

Ilustración 25 Desempeño por procesos

4.3.1.9. Sophos EndPoint

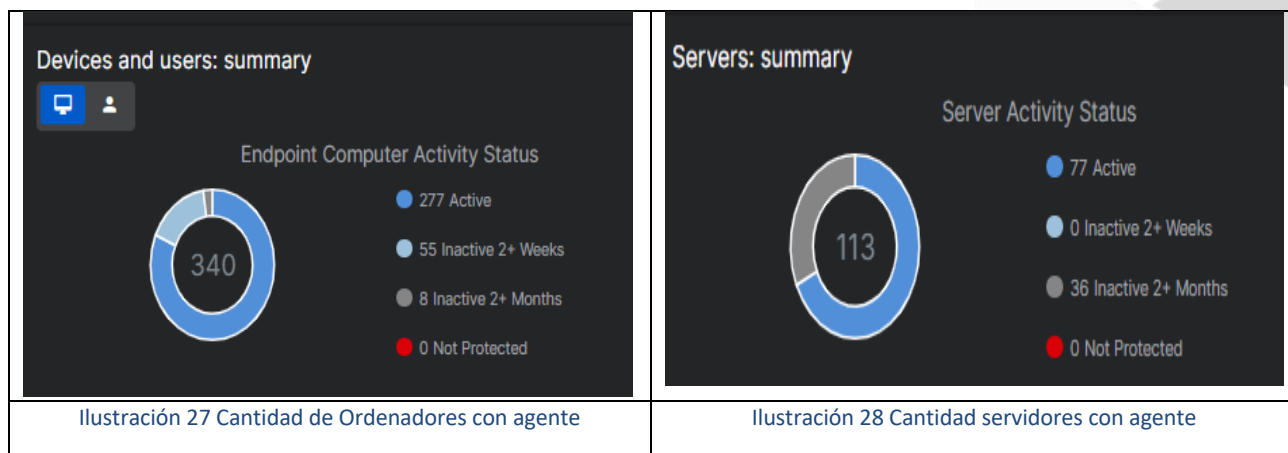
En la ilustración 26, se observa un resumen del estado de Seguridad del Endpoint donde actualmente se están cumpliendo en un 100% los puntos de seguridad de la plataforma de Sophos indicando protección de equipos, políticas y exclusiones.



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 cuanto al licenciamiento se cuenta con una vigencia hasta el 26 de junio de 2026.



Los cuatro equipos que se encuentran no protegidos son: BOGARRIENDO88, BOGIMAC01, BOGVFAPC502 y COWORKING11, los cuales tienen más de 9 meses en algunos casos de no conectarse, recomendamos que la mesa de servicio revise dichos equipos.

En la sección 6.6.1 del informe de seguridad [Informe Mensual InfoTIC Seguridad Marzo2026.pdf](#) se detallan las amenazas contenidas por la herramienta el Sophos instalado en los equipos ordenadores y servidores.

4.3.2. 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	En evaluación por parte de ICETEX.	Alta	N/A	N/A	N/A

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

Recomendación	Estado	Criticidad	Fuente	Asunto	Personal de ICETEX a quien se notificó
usuarios y claves dentro de las aplicaciones de ICETEX.					
Adquirir un equipo Firewall para correo para prevenir brechas de seguridad asociadas al uso del correo electrónico y que este es susceptible a muchos tipos de amenazas.	En evaluación por parte de ICETEX.	Alta	Informes Mensuales - sesiones	Reunión de pares de seguridad	Grupo Coordinación de Infraestructura Tecnológica / Grupo Coordinación de Infraestructura Tecnológica
Validar a nivel de punto final, los equipos que se han visto involucrados con comportamiento malicioso.	Se evalúa por parte de ICETEX. Se hace seguimiento por parte del SOC quien reporta comportamiento malicioso. Sin embargo, es necesario establecer políticas de conexión de equipos externos BYOD debido a que muchos de los casos reportados por el SOC vienen de equipos personales que no hacen parte de la Entidad.	Crítica	Informes Mensuales	N/A	N/A
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 19 Recomendaciones de Seguridad

4.3.3. 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 marzo 2026.pdf](#)

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

4.3.3.1. 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)	Marzo	Febrero	Enero	Diciembre
IOC – Malware DOMINIOS	6.047	6.047	6.047	6.047
IOC – Malware IPs	11.167	11.119	11.119	11.076
IOC – Malware HASH	1.627	1.627	1.627	1.627
IOC – Malware URL	4.564	4.564	4.564	4.564

Tabla 20 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)

4.3.3.2. Alertas o Incidentes de Seguridad Detectados

En el documento [Informe Mensual SOC-TH ICETEX marzo2026.pdf](#) se ven las alertas generadas a lo largo del periodo monitoreado, dichas alertas se clasifican en 3 categorías principales de monitoreo, las cuales corresponden a Seguridad, Disponibilidad y Rendimiento, a partir de este informe se presenta un resumen de las alertas de seguridad y se incluye amenazas cibernéticas, sin embargo, el detalle del tratamiento que se realizó a cada uno de los casos se debe revisar en el Informe mencionado anteriormente.

4.3.3.2.1. Categoría Seguridad

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

Severity : Cantidad de Alertas

Medium	92,076
High	1,565
Low	756

Ilustración 29 Total de alertas de seguridad

Durante el período evaluado de 94.397 alertas de seguridad identificadas, se presentaron con criticidad ALTA un total de 1.565 equivalentes al 1,6% del periodo. En el informe mensual del SOC, se puede observar la cantidad según el tipo de alerta y se realiza una descripción de los tipos de alertas que mayor cantidad de registros o que requieran una indagación más exacta. El comparativo, en los últimos 6 meses, se presenta a continuación:

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

Tabla 21 comparativo Alertas de Seguridad

Durante el período evaluado se presentaron 1.565 alertas de seguridad con criticidad ALTA, un disminuyó con relación a periodos anteriores. En el documento [Informe Mensual SOC-TH ICETEX marzo 2026.pdf](#) se presenta la cantidad según el tipo de alerta y se realiza una descripción de los tipos de alertas que mayor cantidad de registros o que requieran una indagación más exacta.

En cuanto a las alertas altas, el top 5 se presenta a continuación:

Tipo de Alerta	Severidad	Táctica	Cantidad de Alertas
Concurrent Failed Authentications To Same Account From Multiple Countries	9		863
Critical large Outbound Transfer To Outside My Country ICETEX-WX N3	9		167
System Exploit Detected by Network IPS	9		130
Trafico_Permitido_o_Denegado_Hacia_IoC_Maliciosas_WX_Nivel3	9		118
Brute_Force_Host_Login_Success_CUSTOMISADA_8_10_2021	9	Credential Access	56

Ilustración 30 Top 5 de Alertas de Seguridad Altas

Durante el período evaluado se presentaron 92.076 alertas de seguridad con criticidad MEDIA, a continuación, se puede observar la cantidad según el tipo de alerta y se realiza una descripción de los tipos de alertas que mayor cantidad de registros o que requieran una indagación más exacta.

Chart	Criticidad de las alertas	Event Name	Attack Tactic	Criticidad de las alertas	Cantidad de Alertas
☒	Medium	Windows successful file access	Impact, Collection	5	75,765
☒	Medium	Group Policy Object Modified	Privilege Escalation, Defense Evasion	7	5,864
☒	Medium	Windows: AD User Enumeration	Discovery	5	2,241
☒	Medium	Sudden User Login Pattern Change ICETEX		7	1,578
☒	Medium	Large Inbound Transfer From Outside My Country	Command And Control	8	1,377

Ilustración 31 Top 5 de Alertas de Seguridad Medias

4.3.3.2.2. Categoría Disponibilidad

Durante el período evaluado se presentaron 187 alertas de disponibilidad con criticidad ALTA, a continuación, se puede observar la cantidad según el tipo de alerta y se realiza una descripción de los tipos de alertas que mayor cantidad de registros presentaron y se realiza una descripción de los tipos de alertas que mayor cantidad de registros presentaron:

Chart	Criticidad	Event Name	Attack Tactic	Criticidad	Cantidad de alertas
☒	High	Network Device Down: no ping response - WX N3	Impact	10	79
☒	High	SNMP Service Unavailable	Impact	9	29
☒	High	WMI or OMI Service Unavailable	Impact	9	24
☒	High	Network Device Hardware Critical		9	13
☒	High	No logs from a device in 8 hours - WX N3		9	8

Ilustración 32 Top 5 de Alertas de Disponibilidad Altas

A continuación, se presentan los análisis efectuados:

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

- “SNMP Service Unavailable” Esta alerta indica que el servicio SNMP de un dispositivo no está disponible, lo que impide la recolección de métricas, monitoreo y gestión remota, y puede deberse a una caída del servicio, cambios de configuración, problemas de red o incluso actividad maliciosa que intenta evadir la visibilidad; se recomienda verificar si el dispositivo está accesible por otros medios (SSH, web), confirmar que el servicio SNMP esté activo y correctamente configurado, revisar cambios o mantenimientos, validar conectividad de red entre el monitor y el dispositivo, y, si no es esperado, revisar logs para identificar la causa, restaurar el servicio y reforzar controles de monitoreo para evitar pérdida de visibilidad
- “WMI or OMI Service Unavailable” Se presenta cuando el servicio de administración remota como WMI (Windows Management Instrumentation) u OMI (Open Management Infrastructure) no está disponible, lo que puede afectar la supervisión, ejecución remota de comandos y recolección de información, y puede deberse a fallas del servicio, problemas de red, cambios de configuración o incluso intentos de evasión por parte de un atacante; se recomienda verificar si el host está accesible por otros medios, confirmar que los servicios estén activos y configurados correctamente, revisar puertos y reglas de firewall asociados, validar credenciales y permisos, analizar cambios recientes o mantenimientos, y, si la indisponibilidad no es esperada, restaurar el servicio y reforzar monitoreo para evitar pérdida de visibilidad o posibles actividades sospechosas.
- “Network Device Hardware Critical” Esta alerta indica que un dispositivo de red ha reportado una condición crítica de hardware (como fallas en CPU, memoria, temperatura, ventiladores o fuentes de poder), lo cual puede comprometer seriamente su funcionamiento y la disponibilidad de la red; se recomienda verificar el estado del equipo a través de sus interfaces de gestión, validar condiciones físicas (energía, ventilación, ambiente), y si es necesario, aplicar medidas como reducción de carga, failover a equipos redundantes o reemplazo de hardware; además, es clave escalar al proveedor o soporte técnico, asegurar respaldos de configuración y mantener monitoreo continuo para prevenir una caída total del servicio.

4.3.3.2.3. Amenazas de Ciberseguridad

A continuación, se relacionan los Top de ciberataques en tres categorías Ataques IPS, Perímetro y acceso fallidos:

- **Top Ataques IPS:** Se representa el Top de los ataques IPS permitidos por los dispositivos de ciberseguridad perimetral. Se recomienda el bloqueo de los ataques de severidad alta detectados por el IPS y verificar los eventos o alertas de severidad media.

3.1.1 FortiGate: Top IPS Ataques Permitidos - WX						Last 1 mon 
Reporting Device	Attack Name	Signature Id	Severity	Firewall Action	COUNT(Matched Events)	
90 DC_FG_MST_ICETEX	DNS_PTR.Records.Scan	51391	Low	detected	24	
90 DC_FG_MST_ICETEX	SSL.Anonymous.Ciphers.Negotiation	43544	Low	detected	13	

Ilustración 33 ataques IPS permitidos

3.1.1 FortiGate: Top IPS Ataques Denegados - WX						Last 1 mon 
Reporting Device	Attack Name	Signature Id	Severity	Firewall Action	COUNT(Matched Events)	
90 DC_FG_MST_ICETEX	Apache.Log4j.Error.Log.Remote.Code.Execution	51006	Medium	dropped	8,811	
90 DC_FG_MST_ICETEX	Nmap.Script.Scanner	45360	Medium	dropped	2,619	
90 DC_FG_MST_ICETEX	Kubernetes.Ingress.NGINX.Controller.Remote.Code.Execution	57679	Medium	dropped	993	
90 DC_FG_MST_ICETEX	MS.IIS.ShortName.Vulnerability.Scanner	47145	Medium	dropped	827	
90 DC_FG_MST_ICETEX	ZGrab.Scanner	48805	Medium	dropped	534	
90 DC_FG_MST_ICETEX	ALFA.TEaM.Web.Shell	53229	Medium	dropped	513	
90 DC_FG_MST_ICETEX	Mirai.Botnet	43191	Medium	dropped	498	
90 DC_FG_MST_ICETEX	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	48789	Medium	dropped	222	
90 DC_FG_MST_ICETEX	Linksys.Devices.Administrative.Console.Authentication.Bypass	44582	Medium	dropped	213	
90 DC_FG_MST_ICETEX	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	45765	Medium	dropped	192	
90 DC_FG_MST_ICETEX	Linux.Kernel.TCP.SACK.Panic.DoS	48103	Medium	dropped	186	
90 DC_FG_MST_ICETEX	Censys.io.Scanner	50899	Medium	dropped	178	
90 DC_FG_MST_ICETEX	Java.Debug.Wire.Protocol.Insecure.Configuration	44187	Medium	dropped	148	
90 DC_FG_MST_ICETEX	Apache.HTTP.Server.cgi-bin.Path.Traversal	50825	Medium	dropped	125	
90 DC_FG_MST_ICETEX	Hikvision.Products.SDK.WebLanguage.Tag.Command.Injection	50872	Medium	dropped	88	

Ilustración 34 ataques IPS denegados

➤ **Top Perímetro:** A continuación se presentan el TOP de los eventos o tráfico de red organizado por los puertos TCP/UDP que más recibieron o enviaron bytes hacia Internet. Principales Puertos Entrantes por Conexiones (Tráfico Permitido).

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

Source IP	User	Server	COUNT(Matched Events)
10.10.101.46	63 ibohorquezs	90 ictxsrvfs.icetex.local	1,886
49 10.2.254.5	70 jpforero	90 ictxsrvfs.icetex.local	1,799
64 10.2.254.3	70 jpforero	90 ictxsrvfs.icetex.local	1,654
64 10.2.254.4	70 jpforero	90 ictxsrvfs.icetex.local	1,533
63 10.10.101.8	90 mlopeza	90 ictxsrvfs.icetex.local	1,342
90 192.168.20.29	62 gestiondoc	90 ICTXSRVAD001.icetex.local	1,327
49 10.2.254.2	70 jpforero	90 ictxsrvfs.icetex.local	936
64 10.2.254.6	70 jpforero	90 ictxsrvfs.icetex.local	893
10.2.254.107	90 enino	90 ictxsrvfs.icetex.local	883
75 172.16.224.210	51 lsaenzr	90 ictxsrvfs.icetex.local	864
192.168.53.10	90 goanywhere	90 ICTXSRVAD001.icetex.local	750
64 10.2.254.6	50 mzambrano	90 ictxsrvfs.icetex.local	689

Ilustración 35 Top de Accesos Fallidos plataforma Windows

Server	User	COUNT(Matched Events)
90 ICTXSRVAD001.icetex.local	90 22823906	1,279
90 ICTXSRVAD001.icetex.local	90 mmedina	748
90 ICTXSRVAD001.icetex.local	90 mmedinamon	477
90 ICTXSRVAD001.icetex.local	90 kagudelo	431
90 ICTXSRVAD001.icetex.local	90 dileshe	368
90 ICTXSRVAD001.icetex.local	90 cgarciab	326
90 ICTXSRVAD001.icetex.local	90 yrojasm	242
90 ICTXSRVAD000.icetex.local	90 mmedina	203
90 ICTXSRVAD001.icetex.local	mriascos	199
90 ICTXSRVAD001.icetex.local	36 epuertasv	176
90 ICTXSRVAD001.icetex.local	90 ldíaza	157
90 ICTXSRVAD001.icetex.local	90 caucique	153
90 ICTXSRVAD001.icetex.local	90 jdelgadoc	138
90 ICTXSRVAD000.icetex.local	90 yrojasm	136
90 ICTXSRVAD003.icetex.local	90 mmedinamon	135

Tabla: Cuentas bloqueados

Ilustración 36 Cuentas bloqueados

Debido a las limitantes de recursos de la herramienta FortiSIEM no se puede realizar la extracción de información de los intentos de logon fallidos de sesión VPN y de Inicio de sesión Unix.

4.3.3.3. Threat Hunting

Se lleva a cabo el proceso de "Threat Hunting" de manera proactiva mediante la realización de boletines de ciber amenazas y la utilización de la plataforma MISP (Malware Information Sharon Platform) del First (Forum of Incident Response Team), los boletines pueden ser consultado en el numeral 4.4 Boletines del [Informe Mensual SOC-TH ICETEX marzo 2026.pdf](#)

En este procedimiento, se realiza una búsqueda activa de Indicadores de Compromiso (IoC) asociados a las principales amenazas que tienen relevancia a nivel mundial. Estos IoC son posteriormente cargados en el Sistema de Gestión de Eventos e Información de Seguridad (SIEM) para llevar a cabo la correlación con los registros de actividad (logs) de la entidad ICETEX.

El objetivo fundamental es detectar y mitigar posibles amenazas antes de que se materialice un incidente de seguridad. Los resultados obtenidos durante el periodo de monitoreo con relación al tráfico detectado proveniente de la entidad en interacción con estos actores maliciosos y se relacionan en el informe mensual.

Los indicadores de compromiso - IoC fueron recopilados por intercambio de información con algunas instituciones del Estado Colombiano, inteligencia de amenazas en plataformas públicas o privadas, como el FIRST, CISA, CSIRT'S y caza de amenazas en plataformas de ciberseguridad. Los análisis de dichos indicadores, así como sus recomendaciones se encuentran consignados en el [Informe Mensual SOC-TH ICETEX marzo 2026.pdf](#), **es importante resaltar que todo el tráfico fue bloqueado**, sin embargo, se recomienda la verificación de los equipos con las direcciones IP origen privada.

4.3.3.4. Análisis de Marca OSINT

Durante el periodo evaluado, la plataforma de monitoreo de protección de marca y OSINT – AXUR, reporta un total de 12 posibles amenazas de las 34,3k que fueron encontradas y analizadas automáticamente por la plataforma de monitoreo. A estas 12 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

Durante el periodo evaluado se detectó 7 incidentes de los cuales 4 están relacionados con Exposición de secreto en código, 2 con Perfil falso en red social y 1 con Uso fraudulento de marca.



Ilustración 37 Incidentes por Tipo de Amenaza

Durante el periodo evaluado, en cuanto a fraudes digitales, se presentó un total de 06 casos, de los cuales 03 casos fueron descartados, teniendo en cuenta que algunos no tenía relación y otros solo mencionaban la marca, 03 casos fueron reportados a la entidad y se encuentra en estado de tratamiento.

KEY	FECHA DE DETECCIÓN	ESTATUS	TIPO	ESTADO	RESOLUCIÓN	FECHA DE CIERRE
V8NRNK	18/03/2026 12:30	En tratamiento	Uso fraudulento de marca	Abierto	Ninguna	
JS287G	11/03/2026 18:08	En tratamiento	Perfil falso en red social	Abierto	Ninguna	
DVLJ50	25/03/2026 23:19	En tratamiento	Perfil falso en red social	Abierto	Ninguna	
TZHKQX	18/03/2026 3:37	Cerrado	Perfil falso en red social	Cerrado	Descartada	18/03/2026 9:37
J8CWLZ	8/03/2026 21:09	Cerrado	Perfil falso en red social	Cerrado	Descartada	9/03/2026 14:43
8TWC3M	18/03/2026 3:37	Cerrado	Perfil falso en red social	Cerrado	Descartada	18/03/2026 9:37

Ilustración 38 Incidentes por Fraudes Digitales

Aspectos relacionados con la **fuga de datos** Durante el periodo evaluado, se presentaron 06 casos, de los cuales 03 casos fueron descartados, teniendo en cuenta que algunos no tenían relación con la entidad o solo se mencionaba la marca, 03 casos fueron reportados a la entidad y se encuentran en tratamiento.

KEY	FECHA DE DETECCIÓN	ESTATUS	TIPO	ESTADO	RESOLUCIÓN	FECHA DE CIERRE
L00RQR	9/03/2026 3:20	En tratamiento	Exposición de secreto de código	Abierto	Ninguna	
F8UVZU	21/03/2026 3:56	En tratamiento	Exposición de secreto de código	Abierto	Ninguna	
73P3ZD	3/03/2026 3:21	En tratamiento	Exposición de secreto de código	Abierto	Ninguna	
O2MB24	14/03/2026 3:26	Cerrado	Exposición de secreto de código	Cerrado	Descartada	17/03/2026 11:59
K34TLK	27/03/2026 9:51	Cerrado	Otros datos confidenciales	Cerrado	Descartada	27/03/2026 10:44
2YVKZ4	27/03/2026 9:51	Cerrado	Otros datos confidenciales	Cerrado	Descartada	27/03/2026 10:44

Ilustración 39 Incidentes por Fuga de Datos

Durante el periodo evaluado no se identificaron casos relacionados con actividades de piratería. Esto indica que, en el marco del monitoreo realizado, no se evidenció la distribución no autorizada de

contenido, uso indebido de la marca en material pirateado ni afectaciones asociadas a este tipo de riesgo.

Durante el periodo evaluado no se identificaron casos asociados al módulo de deep y dark web. Esto indica que, en el marco del monitoreo realizado, no se evidenciaron menciones, filtraciones o actividades que representaran un riesgo directo para la entidad en este tipo de fuentes.

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

Los casos se encuentran detallados en el [Informe Mensual SOC-TH ICETEX marzo 2026.pdf](#)

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

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

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

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

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

4.3.4. Análisis de Vulnerabilidades ICETEX

Durante marzo de 2026 se ejecutó satisfactoriamente el análisis de vulnerabilidades correspondiente a la **Fase 12** del plan de trabajo. En esta etapa se evaluaron **76 activos de usuario final** (en línea con la planificación mensual). Esta actividad forma parte del avance progresivo definido para cubrir el entorno completo por bloques, manteniendo la continuidad con las fases anteriores.

Cabe recordar que la Fase 5 (abril) cubrió el 100 % de los activos inicialmente definidos y sirvió como línea base. A partir de la Fase 7 (mayo 2025 — marzo 2026) el enfoque operó por segmentos mensuales, con un diseño que estima una cobertura parcial cercana al 50 % del parque en cada bloque mensual.

Durante el análisis se identificaron:

- Servicios con configuración de cifrados débiles: Se identificó un (1) equipo con uso de criptografía débil en seguridad de conexiones.
- Problemas de uso de versiones inseguras de conexión remota: se identificaron que al menos tres (3) dispositivos mantienen uso de protocolos de comunicación con vulnerabilidades conocidas.
- No se identificaron vulnerabilidades críticas y altas.
- Se identificaron cinco (5) vulnerabilidad medias; principalmente asociados a configuraciones por defecto y uso de protocolos con vulnerabilidades conocidas, tales como:
- TLS Version 1.0 - Version 1.1 Protocol Detection: Uso de versiones antiguas e inseguras de TLS (1.0 y 1.1) que contienen vulnerabilidades conocidas como POODLE y BEAST, susceptibles a ataques de descifrado y pérdida de confidencialidad.
- Terminal Services Doesn't Use Network Level Authentication (NLA) Only: Servicios de Terminal (RDP) configurados sin exigir autenticación a nivel de red, permitiendo posibles ataques de fuerza bruta directos y exposición de credenciales antes del establecimiento del túnel cifrado.

4.3.5. Reporte De IPS

En el análisis del informe se identifican dos firmas críticas: `SSL.Anonymous.Ciphers.Negotiation` y `React.Server.Components.react-flight.Remote.Code.Execution`. La primera se observa desde diferentes direcciones IP, pero las asociadas no presentan otros indicadores ni reportes adicionales, lo que podría sugerir un falso positivo.

Se recomienda realizar una verificación del servidor con IP 192.168.51.73 para confirmar si los servicios implementados requieren el uso de cifrados anónimos. En caso de que no sean necesarios, se debe bloquear la firma siguiendo las directrices del fabricante (si se desea bloquear seguir el siguiente documento del fabricante:

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

<https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-SSL-Anonymous-Ciphers-Negotiation-in-IPS-log/ta-p/317987>).

Esta validación es fundamental para evitar vulnerabilidades relacionadas con cifrados débiles que podrían comprometer la confidencialidad de las comunicaciones.

Por otro lado, la firma `React.Server.Components.react-flight.Remote.Code.Execution` presenta un riesgo alto, está asociada al CVE-2025-55182 (para más información: <https://www.cve.org/CVERecord?id=CVE-2025-55182>) y afecta componentes de React Server que permiten ejecución remota de código. El informe relaciona tres IP públicas (151.115.91.13, 38.54.13.232 y 203.145.44.183) que, aunque muestran indicadores de compromiso negativos, deben ser tratadas como potencialmente maliciosas debido a la criticidad de la vulnerabilidad. Se recomienda validar las publicaciones y servicios expuestos que interactúan con estas IP, y posteriormente bloquearlas en los controles perimetrales. Adicionalmente, se debe aplicar la firma en los perfiles IPS para robustecer la detección y bloqueo de intentos de explotación. Para más detalles sobre la firma: <https://www.fortiguard.com/encyclopedia/ips/59644>.

4.4. Servicios de nube

Durante el mes de marzo de 2026, se ejecutó un conjunto integral de actividades orientadas al fortalecimiento, optimización y evolución del entorno tecnológico en Microsoft Azure para ICETEX, abordando de manera estructurada componentes clave como almacenamiento, redes, gobierno, seguridad, integración de servicios, plataformas colaborativas y procesos de migración hacia la nube.

En el componente de almacenamiento, se destaca la migración exitosa de cuentas críticas hacia esquemas de redundancia zonal (ZRS), lo cual permitió mejorar significativamente la disponibilidad y resiliencia de la información, garantizando la continuidad operativa ante posibles fallas en zonas de la región principal. Esta implementación se encuentra alineada con las mejores prácticas del fabricante y fortalece la capacidad de respuesta del entorno ante escenarios de contingencia.

A nivel de arquitectura de red, se llevó a cabo la estandarización del direccionamiento IP bajo el bloque 172.16/12 conforme a la RFC 1918, logrando una segmentación ordenada, eficiente y libre de conflictos con la infraestructura on-premise. Esta actividad permitió establecer una base sólida para el crecimiento del entorno, mejorando la trazabilidad, el control y la escalabilidad de las redes virtuales en Azure.

En el ámbito de plataformas colaborativas, se realizó un análisis detallado del entorno SharePoint Online, evidenciando oportunidades de mejora en la asignación de cuotas de almacenamiento y en el modelo de gobierno del tenant. Se identificaron escenarios de sobredimensionamiento en un número significativo de sitios, lo cual abre la posibilidad de optimizar el uso de la capacidad disponible, así como implementar controles de ciclo de vida que permitan una gestión más eficiente de la información.

En materia de integración tecnológica, se evaluaron los mecanismos de autenticación requeridos para la conexión con Power BI Service, identificando limitaciones en el uso de permisos de tipo aplicación (Application Permissions). A partir de este análisis, se definió como alternativa viable el uso de permisos delegados, asegurando la continuidad de las integraciones bajo un modelo alineado con las capacidades técnicas del servicio y las mejores prácticas de Microsoft.

Adicionalmente, se fortaleció el componente de infraestructura mediante el despliegue de una máquina virtual con capacidades de virtualización (Hyper-V) en Azure, permitiendo la habilitación de entornos de prueba para cargas legacy. Esto incluyó la clonación y puesta en marcha de servidores, garantizando un entorno controlado para validaciones técnicas. Paralelamente, se avanzó en la estrategia de migración hacia la nube mediante la preparación del appliance de Azure Migrate, dejando habilitada la fase de descubrimiento de cargas de trabajo desde entornos VMware.

Como parte del proceso de gestión integral, se llevó a cabo la consolidación del informe de assessment de infraestructura Azure, el cual recopila 25 actividades ejecutadas durante el periodo, organizadas en dominios estratégicos como seguridad, gobernanza, costos, arquitectura y resiliencia. Este documento constituye una base fundamental para la toma de decisiones, el seguimiento de iniciativas y la mejora continua del entorno tecnológico.

Desde el punto de vista financiero, el comportamiento del consumo en Azure refleja una evolución en el uso de la plataforma, evidenciada en la incorporación de nuevas capacidades, especialmente en servicios de analítica avanzada como Microsoft Fabric. Este comportamiento indica una transición hacia escenarios de mayor aprovechamiento de la nube, alineados con necesidades de procesamiento, integración y análisis de información.

De manera transversal, las actividades ejecutadas permitieron fortalecer la postura de seguridad del entorno, reducir riesgos asociados a configuraciones inadecuadas, mejorar la gobernanza de los recursos y optimizar la arquitectura tecnológica, consolidando un entorno más robusto, controlado y alineado con estándares internacionales y buenas prácticas del fabricante.

En conclusión, el entorno Azure de ICETEX evidencia un avance significativo en su nivel de madurez, destacándose mejoras en disponibilidad, resiliencia, seguridad, gobierno y eficiencia operativa. Asimismo, se encuentra preparado para afrontar procesos de modernización, analítica avanzada y crecimiento de manera estructurada, controlada y alineada con las estrategias tecnológicas de la entidad.

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 el 1 de abril de 2024, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato, es de aclarar que la fase de transición no es facturable.

En el presente informe del mes de marzo del 2025 del proyecto, se encuentra en la fase de operación de los servicios contemplados en el alcance llevando ejecutados 35 meses que equivale al 97,22% de avance, 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
	\$2,618,949,159.00	\$ 2.347.588.035	\$120,000,000	0	\$120,000,000	\$ 271.361.124
OTROSI-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
	Fase1: \$85.079.733	\$68.810.788	\$52.071.471	Fase 0: \$79.796.152		
	Fase 2: \$287.192.343			Fase 1: \$94.418.303		

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

	Fase 3: \$253.506.908			Fase 2: \$ 299.128.428		
	Fase 4: \$85.079.733			Fase 3: \$ 269.884.125		
	Fase 5: \$51.394.298			Fase 4: \$ 240.639.821		
				Fase 5: \$211.395.517		
				Fase 6: \$167.529.063		
				Fase 7: \$152.906.910		
Licenciamiento Liferay	\$420.000.000					Mes de septiembre 2025
CONCEPTO						
VALOR						VALOR
VALOR TOTAL DEL CONTRATO Inicial						\$ 31,398,996,857.96
OTROSI-Adición Servicios						\$ 2.761.480.370
VALOR TOTAL DEL CONTRATO						\$ 34,160,477,227.96
VALOR PAGADO						
Pago No. 1 -	mes:	Abril	de	2023	\$ 537.090.736,00	\$ 20,628,979,988.10
Pago No. 2 -	mes:	Mayo	de	2023	\$ 544.104.546,00	
Pago No. 3 -	mes:	Junio	de	2023	\$ 596.978.314,00	
Pago No. 4 -	mes:	Julio	de	2023	\$ 624.431.841,60	
Pago No. 5 -	mes:	Agosto	de	2023	\$ 650.825.466,00	
Pago No. 6 -	mes:	Septiembre	de	2023	\$ 661.959.450,00	
Pago No. 7 -	mes:	Octubre	de	2023	\$ 641.792.285,00	
Pago No. 8 -	mes:	Noviembre	de	2023	\$ 633,094,717.00	
Pago No. 9 -	mes:	Diciembre	de	2023	\$ 663.076.196,00	
Pago No. 10 -	mes:	Enero	de	2024	\$ 681.934.328,00	
Pago No. 11 -	mes:	Febrero	de	2024	\$ 732,950,102.00	
Pago No. 12 -	mes:	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**

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. 4 -	mes:	Diciembre	de	2025	\$1.305.083.859		OTROSI-Adición Servicios**
Pago No.33 -	mes:	Diciembre	de	2025	\$ 779,550,507		<i>Contrato Inicial*</i>
Pago No.34 -	mes:	Enero	de	2026	\$ 780.630.928		
Pago No.35	mes:	Febrero	de	2026	\$ 783.420.281		
Pendiente- Pago No.36	mes:	Marzo	de	2026	\$ 783.536.826		
VALOR CAUSADO QUE NO SE HA PAGADO (valor a pagar factura)							\$ 783.536.826
VALOR TOTAL EJECUTADO (valor pagado + valor causado no pagado)							\$ 28.192.610.451
SALDO DEL CONTRATO (valor total del contrato – valor total ejecutado)							\$ 5.967.866.777
PORCENTAJE DE EJECUCIÓN							82,53%
* 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 22 Ejecución Presupuestal

7. GESTION ADMINISTRATIVA

7.1. Profesionales

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

Perfiles	Especialistas	Anexo
Especialista Bases de datos DBA	Edgar Cobos Mayorga Johan Cardozo – Apoyo DBA	Informe Mensual InfoTIC DBA marzo2026.pdf
Especialista Web Máster	Juan Carlos Martinez	Informe Mensual InfoTIC Webmaster marzo2026.pdf
Especialista Integrador de nube	Carlos Barrera	Informe Mensual InfoTIC Integrador de Nube marzo2026.pdf
Especialistas de Seguridad	Jhon Alveiro Pava González Edwin Morales	Informe Mensual InfoTIC Seguridad Marzo2026.pdf
Especialistas de soluciones	Jose Francisco Escobar Escorcía Davis Alexander Mogollón Fandiño	Informe Mensual InfoTIC Administrador de Soluciones marzo2026.pdf
Especialista de Networking	Carlos Alberto Roldan Ríos Victor Manuel Castiblanco Sanchez - Apoyo Networking	Informe Mensual InfoTIC Administrador de Redes marzo2026.pdf

Tabla 23 Perfiles y Actividades

El siguiente es el grupo administrativo que estuvo en el desarrollo de la operación del mes de marzo del 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

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

Tabla 24 Grupo Administrativo

8. SERVICIO DE COLABORACIÓN

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

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

ÍTEMS	SERVICIO	CIUDAD	DIRECCIÓN	CANTIDAD
1	Sala de video conferencia o sala virtual (Tamaño 65")	Bogotá – Aguas	Carrera 3 No. 18-32 Piso 2, 4 y 6	3
2	Sala de video conferencia o sala virtual (Tamaño 65")	Bogotá – Ángel	Cl. 19 #6-68 piso 17	1
3	Sala de video conferencia o sala virtual (Tamaño 55")	Bogotá – Aguas	Carrera 3 No. 18-32 es una unidad 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 25 Distribución módulos de videoconferencia por sede

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

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

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

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

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

- Visita en sitio en sedes de Bogotá, para realizar pruebas de funcionamiento, verificación de actualizaciones pendientes, inspección de los módulos y posterior limpieza interna y externa de los componentes de cada módulo que se encuentra en la sede Aguas, Ángel y chapinero, para garantizar la prestación continua del servicio y validar que no se estén presentado novedades y/o incidencias.
- Disponibilidad de atención 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 marzo 2026.pdf](#)

Durante el mes de marzo, 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-19115.

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 marzo de 2026, los canales principales y Backup instalados operaron de manera normal, se realizó monitoreo del servicio de los canales mediante la herramienta SolarWinds, el informe de disponibilidad es el que permite la revisión de los ANS y se tiene la línea base de los canales instalados con sus anchos de banda iniciales la cual se actualizando con las ampliaciones de

las canales acordadas contractualmente, se tiene el reporte: [Reporte Mensual Disponibilidad INFOTIC Marzo 2026.pdf](#)

También se puede consultar en el repositorio un documento en Excel con el análisis del comportamiento de los canales para el mes de febrero: [ANS Marzo 2026.xlsx](#)

Sede	Categoría	INR	BW	%MES
BOGOTAD.C.	Principal/FO(SedeAguas)	INR0037	400MB	100,00%
	Backup /FO(SedeAguas)	INR0036	200MB	100,00%
	Principal/IPVPN(SedeChapinero)	INR0022	40MB	100,00%
	Backup /IPVPN(SedeChapinero)	INR0020	25MB	100,00%
	Principal/IPVPN(Angel)	INR0272	200MB	100,00%
	Backup /IPVPN(Angel)	INR0273	200MB	100,00%
IBAGUE	Principal/IPVPN	INR0073	20MB	100,00%
	Backup/IPVPN	INR0076	20MB	100,00%
LETICIA	Principal/Satelital	INR0000373	8MB	99,72%
NEIVA	Principal/IPVPN	INR0039	20MB	100,00%
	Backup/IPVPN	INR0041	10MB	100,00%
TUNJA	Principal/IPVPN	INR0104	20MB	98,70%
	Backup/IPVPN	INR0106	5MB	100,00%
VILLAVICENCIO	Principal/IPVPN	INR0085	20MB	99,86%
	Backup/IPVPN	INR0084	10MB	96,70%
ARMENIA	Principal/IPVPN	INR0074	20MB	100,00%
	Backup/IPVPN	INR0072	10MB	99,97%
MANIZALES	Principal/IPVPN	INR0088	20MB	100,00%
	Backup/IPVPN	INR0087	10MB	100,00%
MEDELLIN	Principal/IPVPN	INR0133	100MB	100,00%
	Backup/IPVPN	INR0132	30MB	100,00%
APARTADO	Principal/IPVPN	INR0144	20MB	100,00%
PEREIRA	Principal/IPVPN	INR0079	20MB	100,00%
	Backup/IPVPN	INR0077	20MB	100,00%
QUIBDO	Principal/IPVPN	INR0014	20MB	91,42%
	Backup/IPVPN			
BARRANQUILLA	Principal/IPVPN	INR0103	100MB	100,00%
	Backup/IPVPN	INR0100	20MB	100,00%
CARTAGENA	Principal/IPVPN	INR0109	20MB	100,00%
	Backup/IPVPN	INR0107	10MB	100,00%
MONTERIA	Principal/IPVPN	INR0080	20MB	99,99%
	Backup/IPVPN	INR0081	10MB	99,97%
RIOHACHA	Principal/IPVPN	INR0164	20MB	99,39%
	Backup/IPVPN	INR0162	10MB	99,96%

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

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

Sede	Categoría	INR	BW	%MES
SANTAMARTA	Principal/IPVPN	INR0154	20MB	99,87%
	Backup/IPVPN	INR0152	10MB	99,88%
SINCELEJO	Principal/IPVPN	INR0095	20MB	100,00%
	Backup/IPVPN	INR0097	5MB	100,00%
SANANDRES	Principal/IPVPN	INR0000367 INR0000369	8MB	97,22%
BUCARAMANGA	Principal/IPVPN	INR0062	30MB	100,00%
	Backup/IPVPN	INR0061	20MB	100,00%
CUCUTA	Principal/IPVPN	INR0044	20MB	100,00%
	Backup/IPVPN	INR0047	10MB	99,86%
VALLEDUPAR	Principal/IPVPN	INR0091	20MB	99,52%
	Backup/IPVPN	INR0090	10MB	99,39%
YOPAL	Principal/IPVPN	INR0121	20MB	95,38%
	Backup/IPVPN	INR0123	10MB	99,99%
ARAUCA	Principal/IPVPN	INR0110	20MB	99,83%
CALI	Principal/IPVPN	INR0151	100MB	99,67%
	Backup/IPVPN	INR0153	150MB	100,00%
BUENAVENTURA	Principal/IPVPN	INR0051	10MB	96,25%
MOCOA	Principal/IPVPN	INR0135	10MB	100,00%
	Backup/Satelital	INR0136	5MB	97,86%
PASTO	Principal/IPVPN	INR0130	20MB	99,42%
	Backup/IPVPN	INR0131	10MB	100,00%
POPAYAN	Principal/IPVPN	INR0035	20MB	99,62%
	Backup/IPVPN	INR0032	5MB	99,37%
TUMACO	Principal/IPVPN	INR0147	20MB	99,87%
DCTRIARA	MPLS PP	INR0266	1GB	100,00%
	MPLS BK	INR0171	1GB	100,00%
DCTRIARA	INTERNET BK	INR0221	800MB	0%
	INTERNET PP	INR0264	800MB	100,00%
DCTRIARA	NOCclarodedidcado(DWDM)2GTriaram egacentro	INR0224	2GB	100,00%
BOGOTAD.C.	Internet(SedeAguas)	INR0034	70MB	100,00%
DCMegacentro	DCMEGACENTER–CONTIGENCIA– MPLSPPAL	INR0177	500MB	100,00%
	DCMEGACENTER–CONTIGENCIA– MPLSBK	INR0230	500MB	100,00%
	Internet	INR0268	400MB	100,00%
BancodelaRepublicaha staEdificioDirecciónGe neralICETEX	UbicadoenDatacenterPrincipal.intercon ectadoatravesderedMPLS	INR0000289	40MB	100,00%
DECEVALhastaEdificiod elICETEXDirecciónGene ral.	UbicadoenDatacenterPrincipal.intercon ectadoatravesderedMPLS	INR0000317	40MB	100,00%

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

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

Sede	Categoría	INR	BW	%MES
DECEVALhastaEdificio de ICETEX Dirección General.	Ubicado en Datacenter Principal. Interconectado a través de red MPLS (Backup)	INR0000318	15MB	99,94%

Tabla 26 Disponibilidad de Canales

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

Sede	Categoría	INR	% Mes
BARRANQUILLA	INTERNET PARA LA GENTE	INR0094	100.00%
BUCARAMANGA	INTERNET PARA LA GENTE	INR0057	100.00%
CALI	INTERNET PARA LA GENTE	INR0160	99.64%
AGUAS	INTERNET PARA LA GENTE	INR0029	100.00%
CHAPINERO	INTERNET PARA LA GENTE	INR0015	88.32%
MEDELLIN	INTERNET PARA LA GENTE	INR0122	93.68%
APARTADO	INTERNET PARA LA GENTE	INR0140	100.00%
ARAUCA	INTERNET PARA LA GENTE	INR0115	99.73%
LETICIA	INTERNET PARA LA GENTE	INR0000378	98.81%
QUIBDO	INTERNET PARA LA GENTE	INR0021	91.43%
RIOHACHA	INTERNET PARA LA GENTE	INR0159	99.42%
SAN ANDRES	INTERNET PARA LA GENTE	INR0000368	98.80%
YOPAL	INTERNET PARA LA GENTE	INR0127	94.80%
MOCOA	INTERNET PARA LA GENTE	INR0141	100.00%

Tabla 27 Disponibilidad canales "Internet para la gente"

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 marzo continúa su funcionamiento correctamente sin novedades que afectaran la prestación del servicio. La evidencia se encuentra en el [Reporte Monitoreo ICETEX Marzo_2026-ELK.pdf](#) y en el archivo de [Disponibilidad Server ELK Marzo 2026.xlsx](#)

10.2. ANS por Disponibilidad de servidores

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

No	COD.	Etiquetas de fila	Disponibilidad
1	INR0278	cxvodacontg011	99,60%
2	INR0277	cxvodaprodn021	100%

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	COD.	Etiquetas de fila	Disponibilidad
3	INR0276	cxvodaprodn011	100%
4	INR0262	icetexboglخورفو2.localdomain	100%
5	INR0260	icetexosbognfs1	100%
6	INR0259	INR0259_INFOTIC	99,99%
7	INR0258	INR0258_INFOTIC	0%
8	INR0257	INR0257_INFOTIC	100%
9	INR0256	INR0256_INFOTIC	100%
10	INR0255	INR0255_INFOTIC	100%
11	INR0254	INR0254_INFOTIC	100%
12	INR0253	bastion.localdomain	100%
13	INR0252	icetexosbognfs2	100%
14	INR0251	INR0251_INFOTIC	100%
15	INR0250	qasec	100%
16	INR0249	xroadsec	100%
17	INR0248	icetexboglxxroad3	100%
18	INR0247	preprodsec	100%
19	INR0246	icetexboglxdarumatest	100%
20	INR0245	icetexboglxdarumasrv2	100%
21	INR0244	icetexboglxdarumasrv1	100%
22	INR0243	icetexbogliferaerver1	100%
23	INR0242	icetexbogliferaerver2	100%
24	INR0241	icetexbogelasticserver3	100%
25	INR0240	icetexbogelasticserver2	100%
26	INR0239	icetexbogelasticserver1	100%
27	INR0238	icetexbogliferaynfs	100%
28	INR0237	icetexbogbalserver1-r	0%
29	INR0236**	ictxbogsvrpt1	100%
30	INR0235**	ictxbogsvrpt2	100%
31	INR0234	ictxprusisgapp	100%
32	INR0233	icetexboglخورفو1.localdomain	100%
33	INR0229	ictxisisgesapp	100%
34	INR0228	ictxisisgesbd	100%
35	INR0226	mira	100%
36	INR0000322	ictxsrvtctrlidoc	100%
Balanceador Nodo 1	INR0197	TFM1412	100%
Balanceador Nodo 1	INR0197	TFM1407	100%

Tabla 28 Códigos relacionados Disponibilidad Servicios en Housing – Datacenter Principal

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

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

#	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 29 Dispositivos en Housing – Datacenter Principal

10.2.1. Disponibilidad TRIARA para los servicios de página web

La disponibilidad del Portal Web institucional web.ICETEX.gov.co, en el mes de marzo presentó un **UPTIME del [99.823%]** tal como se evidencia en el numeral 4.2.1.3 Sitio Web.

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

	Enero	Febrero	Marzo
Usuarios activos mes	528000	613000	600000
Usuarios nuevos	361000	425000	382000
Tiempo de interacción (seg)	133	101	97

Tabla 30 Distribución trimestral de acceso por usuarios

El portal WEB cuenta con un total de 600 mil usuarios, con 382 mil usuarios nuevos. El tiempo de interacción medio es de 1 minutos y 37 segundos, señalando el interés de la audiencia en las diferentes páginas del portal web.icetex.gov.co.

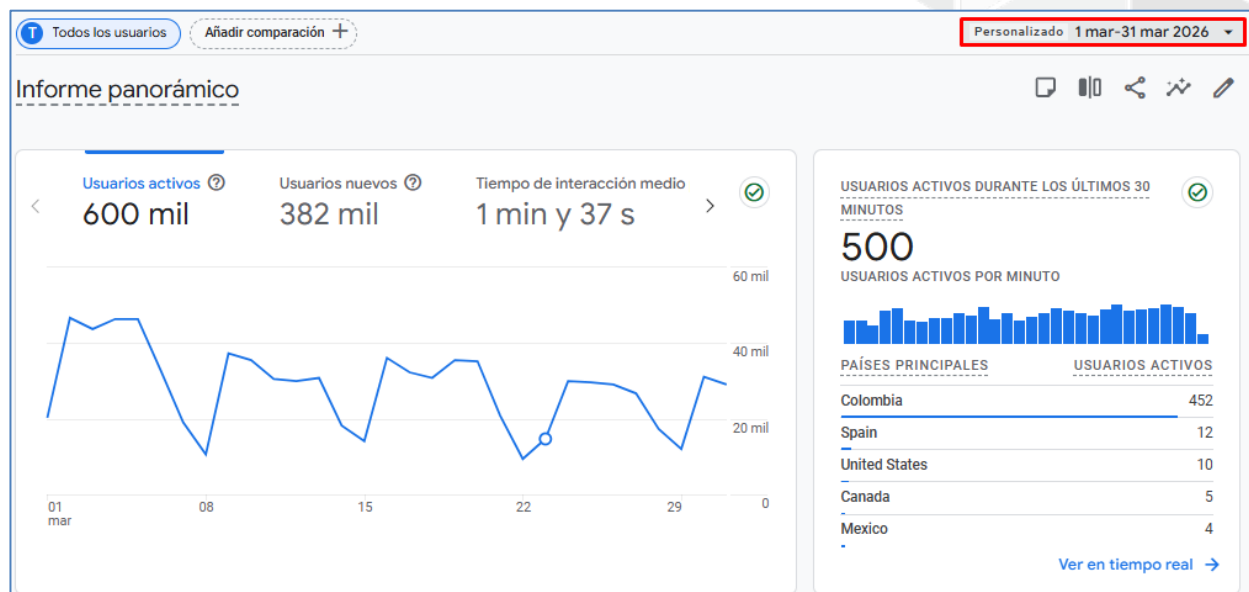
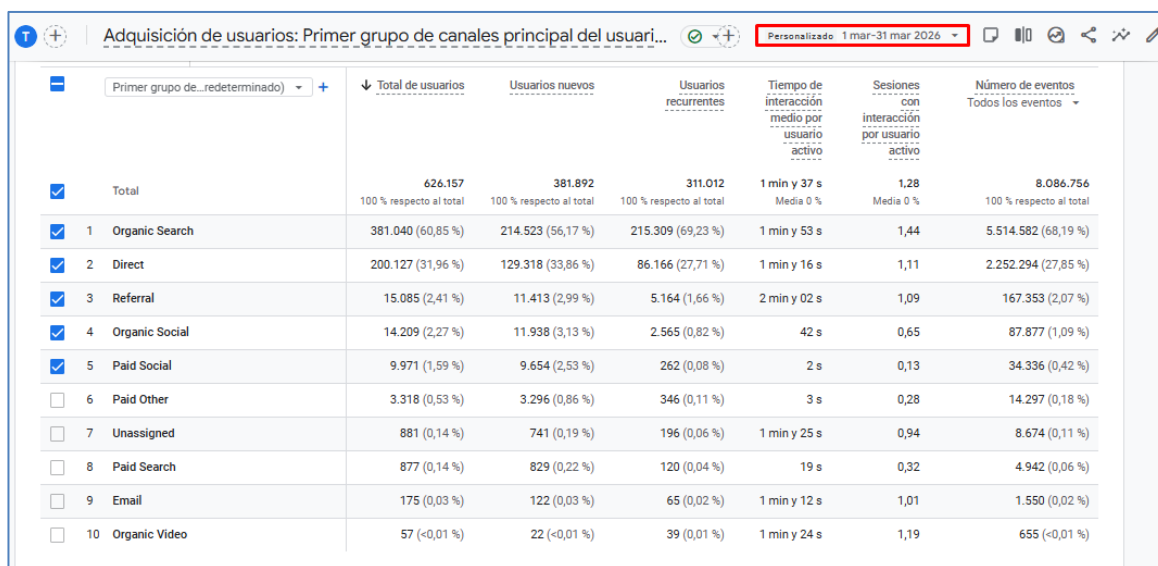


Ilustración 40 Métrica de visitantes Portal WEB web.ICETEX.gov.co

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



Adquisición de usuarios: Primer grupo de canales principal del usuari...

Personalizado 1 mar-31 mar 2026

	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	626.157 100 % respecto al total	381.892 100 % respecto al total	311.012 100 % respecto al total	1 min y 37 s Media 0 %	1,28 Media 0 %	8.086.756 100 % respecto al total
☒ 1 Organic Search	381.040 (60,85 %)	214.523 (56,17 %)	215.309 (69,23 %)	1 min y 53 s	1,44	5.514.582 (68,19 %)
☒ 2 Direct	200.127 (31,96 %)	129.318 (33,86 %)	86.166 (27,71 %)	1 min y 16 s	1,11	2.252.294 (27,85 %)
☒ 3 Referral	15.085 (2,41 %)	11.413 (2,99 %)	5.164 (1,66 %)	2 min y 02 s	1,09	167.353 (2,07 %)
☒ 4 Organic Social	14.209 (2,27 %)	11.938 (3,13 %)	2.565 (0,82 %)	42 s	0,65	87.877 (1,09 %)
☒ 5 Paid Social	9.971 (1,59 %)	9.654 (2,53 %)	262 (0,08 %)	2 s	0,13	34.336 (0,42 %)
☐ 6 Paid Other	3.318 (0,53 %)	3.296 (0,86 %)	346 (0,11 %)	3 s	0,28	14.297 (0,18 %)
☐ 7 Unassigned	881 (0,14 %)	741 (0,19 %)	196 (0,06 %)	1 min y 25 s	0,94	8.674 (0,11 %)
☐ 8 Paid Search	877 (0,14 %)	829 (0,22 %)	120 (0,04 %)	19 s	0,32	4.942 (0,06 %)
☐ 9 Email	175 (0,03 %)	122 (0,03 %)	65 (0,02 %)	1 min y 12 s	1,01	1.550 (0,02 %)
☐ 10 Organic Video	57 (<0,01 %)	22 (<0,01 %)	39 (0,01 %)	1 min y 24 s	1,19	655 (<0,01 %)

Ilustración 41 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.

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

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

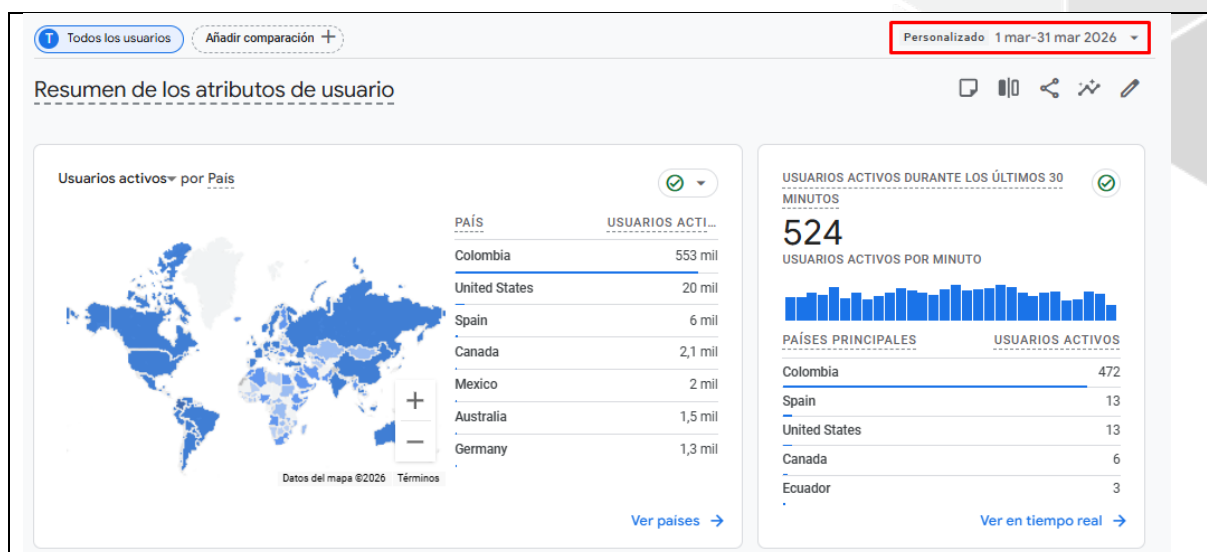


Ilustración 42 Métrica de usuario por país - Portal WEB web.ICETEX.gov.co

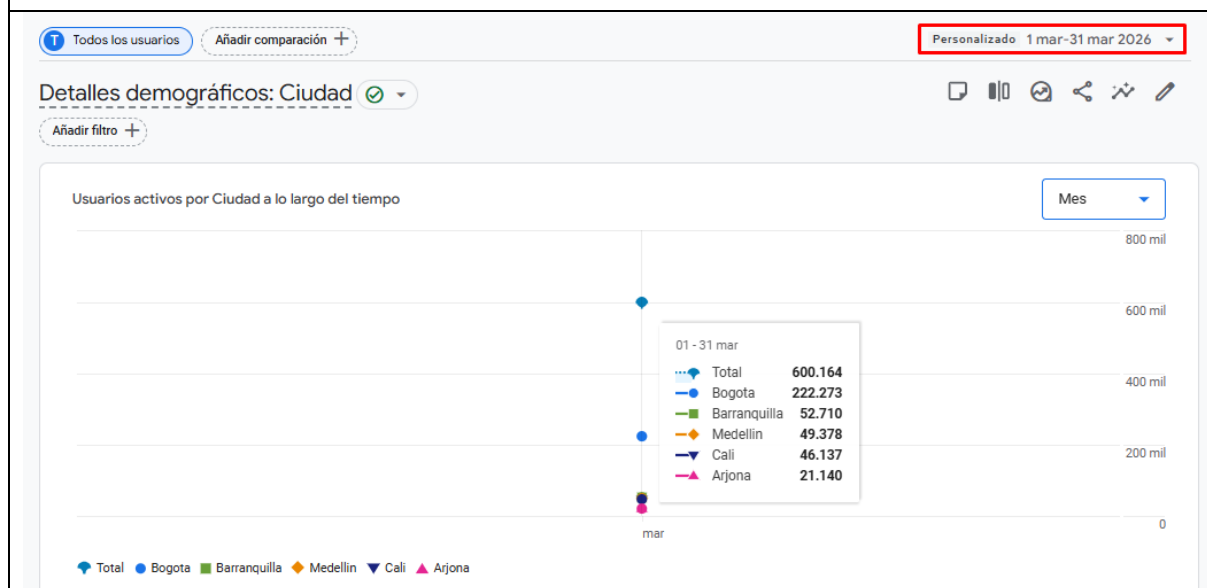


Ilustración 43 Métrica de ciudades de Colombia- Portal WEB web.ICETEX.gov.co

A continuación, se muestran las gráficas referentes a memoria RAM y almacenamiento en los nodos 1 y 2 del portal ICETEX desde el 1 de marzo desde las 00:00 horas hasta las 23:59 horas del 31 de marzo de 2026

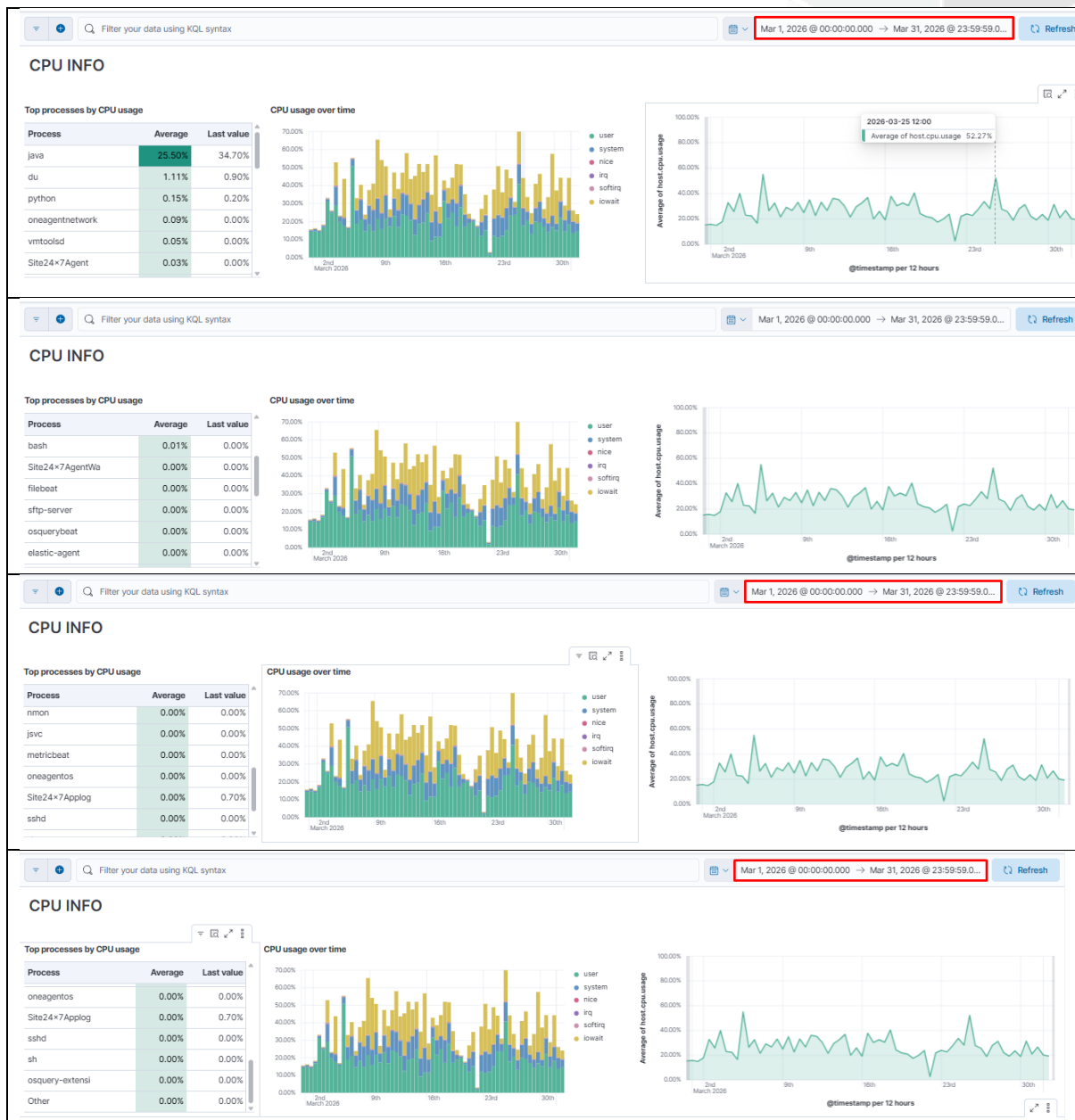
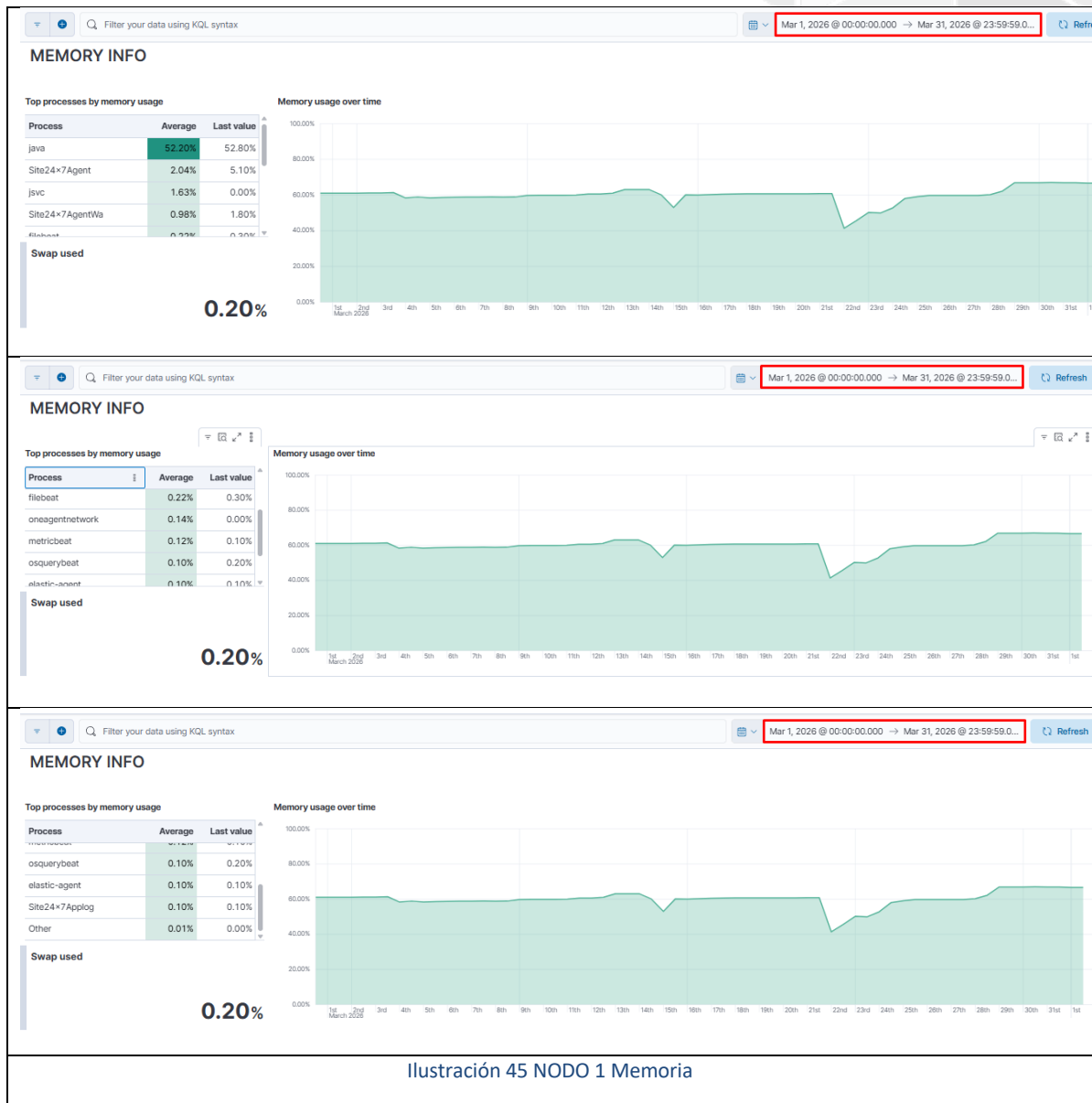


Ilustración 44 NODO 1 CPU

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



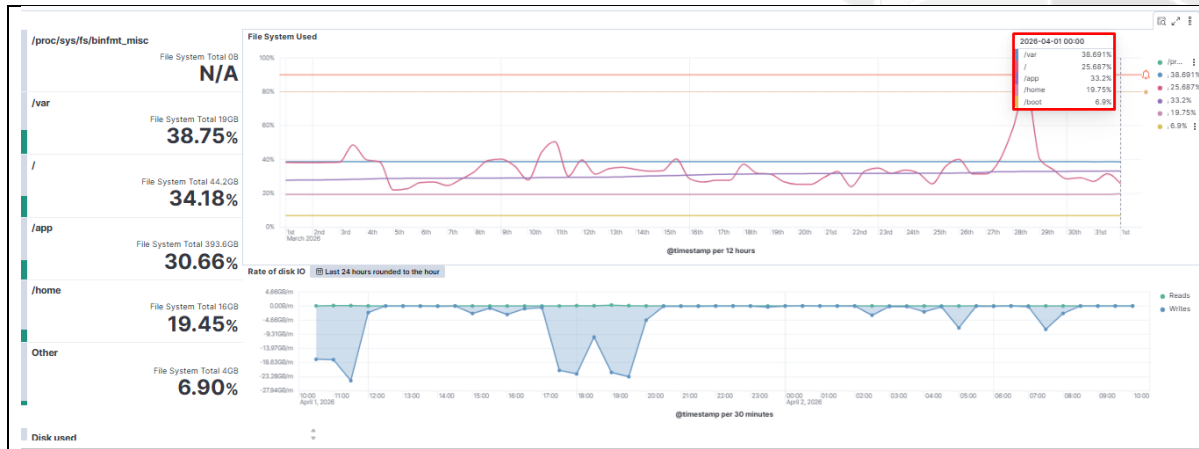


Ilustración 46 NODO 1 Almacenamiento

Estos mismos recursos, para el nodo 2 se monitorean de igual manera. El detalle de los consumos y sus umbrales puede ser consultado en el informe de nuestro especialista web master [Informe Mensual InfoTIC Webmaster marzo2026.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 febreros 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 Marzo 2026.pdf](#) que se genera con la guía de los diferentes reportes de Backups disponibles durante el mes y se adjunta el reporte de los backups que se genera automáticamente desde la herramienta de Backups [Consolidado Mensual de Backups Marzo 2026.pdf](#)

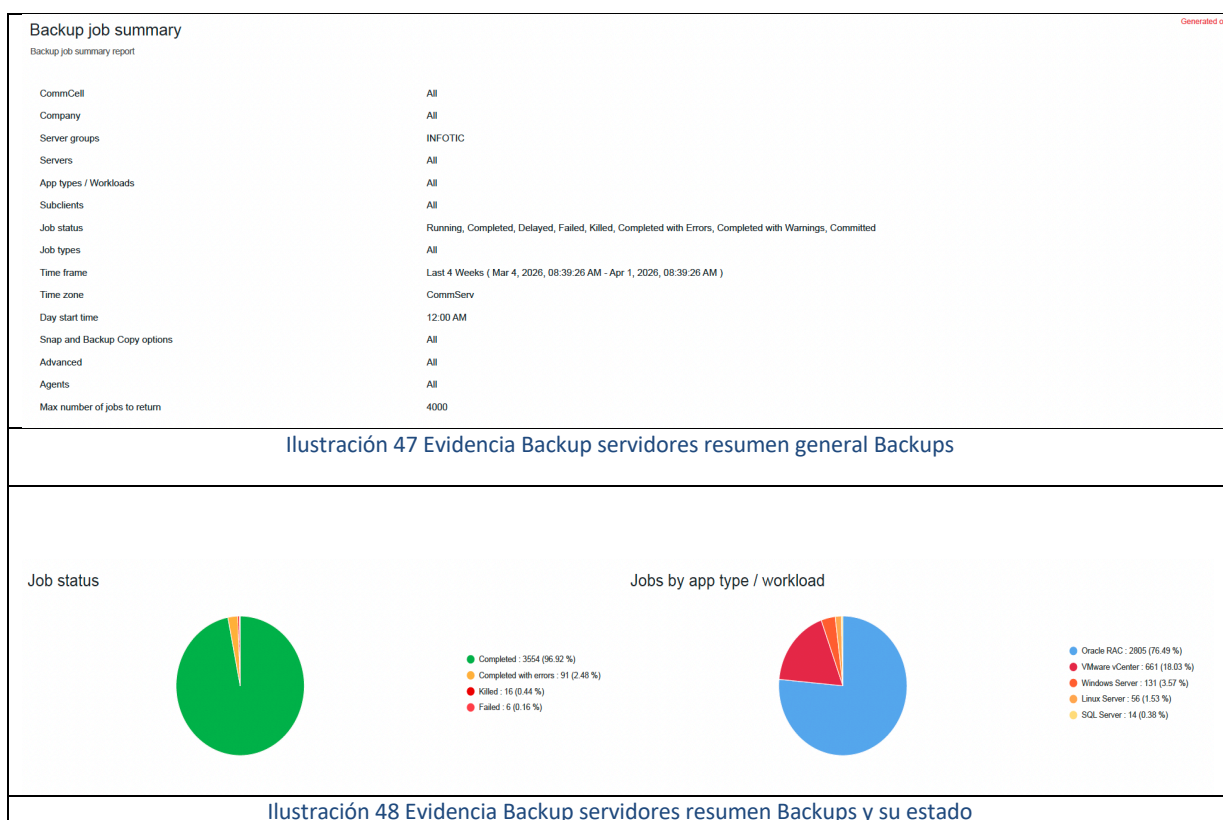
Dentro de las actividades del proyecto de servicios tecnológicos para ICETEX, se tiene la toma de copias de respaldo de la información creada, actualizada, reutilizada y procesada dentro de las diferentes actividades de la entidad la cual requiere para el desarrollo de sus actividades diarias,

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 V5.xlsx](#)

Respecto a la gestión de medios, en este periodo se inició 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.

El avance de esta migración de Backups a corte del mes se puede consultar en el reporte: [ReporteMensualCintasInfotic 2026-03-29.html](#)

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



El total del tamaño de la información respalda para el mes de marzo corresponde a 224.04 TB, donde 96.92% se completó en el primer lanzamiento del robot con un total de 223.98 TB de información.

El 75.49% está representado en el respaldo dado a la información del Oracle RAC.

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

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

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

De un total de 3667 trabajos analizados, el 99,4% se completó con éxito (incluyendo los que tuvieron errores menores). El 96.92% de todos los trabajos se completaron sin ningún error.

- Tasa de éxito: 96.92 % (trabajos completados o completados con errores)
- Tasa de fracaso: 0.6% (trabajos fallidos o cancelados)
- Oracle RAC: El 76.49% de los trabajos de respaldo corresponden a este tipo de servidor, con un total de 2805 trabajos.
- VMware vCenter: El 18.03% de los trabajos pertenecen a este entorno, con 661 trabajos.
- Otros Servidores: Los trabajos de Windows Server, Linux Server y SQL Server representan el 3.57%, 1.53% y 0.38% respectivamente.

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

Desde el punto de vista administrativo, se incorporaron todos los ajustes solicitados al manual de operación de *backups*. La versión definitiva fue remitida a mediados de marzo y puede consultarse en el siguiente enlace: [Manual Backups 1.3-20260316.pdf](#)

11. CONTROL DE CAMBIOS

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

No. Cambio	Alcance	Fecha De Creación o Aprobación	Fecha De Ejecución	Resultado	Observaciones
13284	Instalación y configuración del parche liberado por el proveedor oracle para el home de oracle ,grid del rac de produccion oda-prod y del servidor de contingencias(Megacenter)	13/02/2026	01/03/2026	Exitoso	Se realizó la instalación y configuración del parche 38291812 proporcionado por el proveedor para actualizar a la versión 19.29. El procedimiento se ejecutó sobre el Oracle Home y Grid Infrastructure de cada nodo del RAC; en el servidor de contingencia, se aplicó una actualización secuencial

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. Cambio	Alcance	Fecha De Creación o Aprobación	Fecha De Ejecución	Resultado	Observaciones
					de la versión 19.28 a la 19.29.
15801	PRUEBA DRP PRIMER SEMESTRE 2026	25/02/2026	23/03/2026	Exitoso	
16845	ejecutar la actualización del kernel del servidor NFS para mantener el sistema operativo alineado con buenas prácticas de mantenimiento, reduciendo exposición a vulnerabilidades, mejorando estabilidad bajo carga y optimizando el rendimiento de I/O y comunicación en red, garantizando además compatibilidad con drivers y controladores del entorno.	27/02/2026	14/03/2026	Exitoso	Se actualizó el kernel del servicio NFS a la versión 4.18.0-348.7.1.el8_5.x86_64.
20824	El cambio aplica a los siguientes servidores que tienen instalado Windows Server 2019 Standard: ICTXSRVMOODLE (192.168.51.82): aloja la aplicación ComunidadICETEX (https://comunidad.icetex.gov.co/ComunidadIcetexFront/inicio), publicada en internet y accedida por usuarios externos. ICTXSRVAPPMIX3 (192.168.51.139): aloja el servicio CustomWindowsS erviceNovacion, crítico para procesos internos. Ambos servidores serán actualizados con los últimos parches de seguridad y estabilidad de Windows. No se verán afectadas otras máquinas o servicios fuera de estos entornos.	19/03/2026	28/03/2026	Exitoso	2026-03 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5078752)
20830	El cambio aplica a los siguientes servidores en entorno de producción: • ICTXSRVNETCOR01 (192.168.51.165) aloja las aplicaciones PSE, Cargue Archivos, Cuentas Abandonadas, Cuentas Inactivas, PortalTransaccional y Transunion, las cuales están publicadas en internet y accedidas por usuarios externos. • ICTXSRVAPPMIX1 (192.168.51.134) : aloja las aplicaciones internas Desembolsos, Reporteador, Servicios de Integración MEN, Censo Indígena, Sisbén, Vigía e Icfes, utilizadas para procesos institucionales críticos. • ICTXSRVDCVAL01 (192.168.51.170): aloja la aplicación Deceval, esencial para la integración con servicios financieros externos.	19/03/2026	29/03/2026	Exitoso	2026-03 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5078752) 2026-03 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5078938).
21183	Optimizar el servicio Elasticsearch en los tres nodos - 192.168.20.43, 192.168.20.44 y 192.168.20.45.	20/03/2026	28/03/2026	Exitoso	

Tabla 31 Controles de cambio Marzo

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:

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

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

Tabla 32 Planes de trabajo

13. PLAN DE ENTREGA

Por parte del ICETEX no se ha efectuado la designación formal de los líderes técnicos para el acuerdo de las listas de chequeo y de los cronogramas de entrega.

Por parte de INFOTIC, se elaboró una propuesta de listas de chequeo para algunos servicios, así como otros insumos orientados a facilitar el proceso de verificación y control durante la entrega, las cuales fueron remitidas mediante oficio al ICETEX.

De igual manera, se propuso una estructura documental para el repositorio destinado al almacenamiento de las evidencias de la entrega. La estructura fue revisada y aprobada por el ICETEX, y se presenta a continuación:

- └— 00_Gobierno_y_Transversal
- └— 01_Conectividad_y_Comunicaciones
- └— 02_Centro_de_Datos
- └— 03_Seguridad_Informatica
- └— 04_Servicios_de_Nube
- └— 05_Servicios_Conexos

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

 00_Gobierno_y_Transversal.

(Información común a todos los servicios)

- |— 01_Contrato_y_Anexos
- |— 02_Modelo_de_Operacion
- |— 03_Gestion_de_Riesgos
- |— 04_Informes
- |— 05_Comunicaciones_Oficiales

 01_Conectividad_y_Comunicaciones

- |— 01_Arquitectura_de_Red
 - | |— Diagramas
 - | |— Topologias
 - | |— Inventario_de_Red
- |— 02_Configuraciones
 - | |— Routers
 - | |— Switches
 - | |— Otros_Dispositivos
- |— 03_Monitoreo_y_Disponibilidad
- |— 04_IPV6

 02_Centro_de_Datos

- |— 01_Arquitectura_DC
 - | |— Principal
 - | |— Alterno
- |— 02_Housing_y_Hosting
- |— 03_Inventario_de_Equipos
- |— 04_Continuidad_y_DRP
- |— 05_Aplicaciones
- |— 08_Base de datos
- |— 09_Sitio web

 03_Seguridad_Informatica

- |— 01_Modelo_de_Seguridad
- |— 02_Gestion_de_Vulnerabilidades

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

- └─ 03_Monitoreo_y_SOC
- └─ 04_Incidentes_de_Seguridad
- └─ 05_Configuraciones de las Herramientas

04_Servicios_de_Nube

- └─ 01_Arquitectura_Cloud |
- └─ 02_Provisionamiento
- └─ 03_Gestion_de_Recursos
- └─ 04_Seguridad_en_la_Nube
- └─ 05_Backup_y_Recuperacion
- └─ 06_Monitoreo_y_Costos

05_Servicios_Conexos.

Para efectos de avanzar en este plan se concertaron sesiones de presentación de dichas listas, de las cuales se enuncian las celebradas:

Fecha	Tema	Participantes
2023-03-17	General	Gerencia INFOTIC - Supervisión y apoyo a la supervisión
2026-03-18	Aplicaciones	Especialistas de soluciones - Apoyo supervisión ICETEX
2026-03-18	Seguridad-SIEM	Especialistas de Seguridad - Apoyo supervisión Seguridad ICETEX
2026-03-24	General	Gerencia INFOTIC - Supervisión y apoyo a la supervisión
2026-03-25	Aplicaciones	Especialistas de soluciones - Apoyo supervisión ICETEX
2026-03-26	Base de datos	Especialistas de soluciones - Apoyo supervisión ICETEX
2026-03-26	Sitio Web	Web master - Apoyo supervisión ICETEX
2026-03-25	Aplicaciones	Especialistas de soluciones - Apoyo supervisión ICETEX
2026-03-25	Seguridad	Especialistas de Seguridad - Apoyo supervisión Seguridad ICETEX
2026-03-27	DataCenter - Hosting - Collocation	Gerente de Servicios - Apoyo supervisión Seguridad ICETEX

Tabla 33 Sesiones de presentación Listas de Chequeo entrega de servicios

Existen algunas líneas de servicio cuya característica es prestación de servicios en todo su alcance y para lo cual se proponen entregas vinculadas a los informes , como se presenta a continuación:

Monitoreo Marca OSINT. Como propuesta de cierre de este servicio y dado que AXUR es un servicio bajo modalidad SaaS (Software as a Service), por lo que toda la infraestructura se encuentra alojada y gestionada directamente por parte de INFOTIC, se llevará a cabo una desactivación gradual de todas las configuraciones implementadas durante la operación del servicio, en el siguiente orden:

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

- Eliminación de palabras clave: se eliminan todas las bibliotecas y conjuntos de términos utilizados por la plataforma para detectar menciones relacionadas con la organización, con el fin de detener cualquier tipo de rastreo o correlación automática.
- Eliminación de reglas de búsqueda: una vez eliminadas las palabras clave, se procede a deshabilitar y eliminar todas las reglas de búsqueda personalizadas configuradas a lo largo del servicio, evitando que la plataforma continúe realizando búsquedas automatizadas vinculadas a la organización.
- Eliminación de usuarios: finalmente, se revocan los accesos de todos los usuarios creados para la operación del servicio y se eliminan sus cuentas, asegurando que no exista ninguna credencial activa con permisos de ingreso a la plataforma. Este proceso permite garantizar que no se conserve información relacionada con la organización dentro del entorno de AXUR. La eliminación completa de toda la configuración puede tardar hasta 30 días en reflejarse por completo dentro de la plataforma.

Análisis de vulnerabilidades. En el marco del plan de entrega, socializado el pasado mes de febrero, les informamos que, para el servicio de análisis de vulnerabilidades, como ítem de entrega, será remitido un resumen ejecutivo consolidado, en el cual se presentará el balance de las actividades desarrolladas, los principales resultados obtenidos y el estado a la fecha.

Este documento complementa los informes mensuales que se han venido generando y remitiendo de manera periódica durante la ejecución del contrato, y tiene como propósito ofrecer una visión integral y ejecutiva del servicio prestado.

14. RECOMENDACIONES DEL CONTRATISTA AL ICETEX

14.1. Networking

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

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

Renovación y Certificación de Cableado: Se recomienda realizar una renovación o sustitución del cableado en diversos puntos de la entidad, dado que la infraestructura de cableado es muy antigua.

Se sugiere también llevar a cabo una certificación del nuevo cableado para garantizar su calidad y desempeño.

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

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

14.2. Aplicaciones

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

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

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

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

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

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

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

Disco	Métrica	Jul-25	ago-25	sep-25	Observaciones	Recomendaciones
C:	Espacio usado	65% (56.6 GiB)	58% (58.1 GiB)	69% (68.97 GiB)	Se incrementó el uso en almacenamiento en comparación con el mes anterior en aproximadamente 11 GiB.	Considerar mover archivos no esenciales a otro volumen que dispongan desde el lado de infraestructura hacia almacenamiento secundario.
	Espacio libre	33.3 GiB	41.4 GiB	30.54 GiB		
F:	Espacio usado	92% (1.74 TiB)	95% (1.80 TiB)	96% (1.90 TiB)	Altísima ocupación constante (>90%), aunque mejora en septiembre debido al aumento del almacenamiento en 100GB	Urgente implementar políticas de depuración de archivos antiguos o inactivos. Considerar expansión del volumen o migración de datos a almacenamiento secundario.
	Espacio libre	146 GiB	89.4 GiB	72.91 GiB		
E:	Espacio usado	79% (51.7 GiB)	65% (42.5 GiB)	88% (57.08 GiB)	Aún se mantiene en zona de riesgo por encima del 80%.	Considerar mover archivos no esenciales a otro volumen que dispongan desde el lado de infraestructura hacia almacenamiento secundario. Considerar expansión del volumen si requieren almacenar por mucho más tiempo los logs de las aplicaciones
	Espacio libre	13.3 GiB	22.4 GiB	7.92 GiB		

Ilustración 49 Histórico consolidado uso de discos servidor ICTXSRVNETCOR01

14.3. Seguridad

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

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

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

- Se debe trabajar en el perfilamiento de la navegación de acuerdo con lo entregado por ICETEX.
- Validar la autenticación de doble factor para todas las plataformas misionales del ICETEX.
- Realizar autenticación a través del LDAPS, para la gestión de las plataformas de seguridad.
- Realizar la contención automática de equipos que se identifiquen en la red como maliciosos.
- Realizar el aumento de recursos a la plataforma de FortiSIEM (CPU, Memoria y disco) y hacer un cambio de arquitectura con el objetivo de mejorar.

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

14.4. Bases De Datos

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

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

14.5. Integrador De Nube

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

- Se lograron avances sólidos en la optimización, ordenamiento y fortalecimiento de la infraestructura Microsoft Azure – ICETEX, consolidando un entorno productivo más organizado, seguro y alineado con buenas prácticas Cloud.
- Las actividades ejecutadas fortalecieron la gobernanza mediante la depuración de redes y grupos de recursos huérfanos, el ajuste de reglas NSG y el redimensionamiento de la VNet vm-app-home-vnet.

- La instrumentación de alertas preventivas y el aprovisionamiento de almacenamiento especializado mejoraron la observabilidad, permitiendo monitoreo oportuno de servicios críticos.
- La Reserva de Instancia aplicada a la VM vm-devops-agent representa un avance clave en eficiencia financiera, asegurando ahorros relevantes en el horizonte operativo.
- La documentación técnica consolidada para Datafondos refuerza la trazabilidad y asegura continuidad operativa bajo estándares de seguridad.
- La Solicitud Especial – Microsoft – ÁBACOS marca el inicio formal de la etapa de diseño y dimensionamiento del micrositio y plataforma educativa a migrar hacia ICETEX.
- El mes de marzo representó un progreso importante hacia la madurez operativa y de gobernanza del entorno Azure institucional, sentando bases para fases futuras de automatización, control de costos y consolidación arquitectónica.

15. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC

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

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

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

15.2. Una capacitación al año de seguridad Informática y servicios conexos

El pasado 25 de marzo, a las 3:00 p. m., se impartió la tercera capacitación titulada: 'Cómo protegernos ante amenazas cibernéticas y la Inteligencia Artificial (IA)'. Esta jornada tuvo como objetivo fortalecer las buenas prácticas de seguridad digital y la concientización sobre los riesgos tecnológicos emergentes. Con esta sesión, se da cumplimiento total al valor agregado contractual, el cual contemplaba una capacitación anual en Seguridad Informática y servicios conexos durante los tres años de vigencia del contrato.

15.3. 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 34 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 35 Capacidades de almacenamiento aprovisionado

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

En el almacenamiento aprovisionaron 3 TB como valor agregado de INFOTIC para realizar la prueba de restauración de Backups, durante el mes de marzo se realizaron las siguientes pruebas de restauración:

Código de Servicio	Hostname	Tipo de restauración	Fecha Solicitud de Restauración	Resultado	Evidencia
INR0000290	ICTXSRVFS	Granular	17/03/2025	Exitoso	RS-SoporteTI-19214 FormatoRestauraciones 13_03_2026.xlsx RE_RS-SoporteTI-19214.pdf
INR0000290	ICTXSRVFS	Granular	20/03/2025	Exitoso	FormatoRestauraciones 20_03_2026.xlsx

Tabla 36 Pruebas de Restauraciones de Backups de marzo

15.4. “Wifi” para la gente en 19 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

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 37 WIFI para la gente instalados

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

Tabla 38 WIFI para la gente pendientes

16. CONCLUSIONES

- El uso de autenticación de doble factor en las conexiones VPN de los funcionarios ayudaría a proteger mejor la información sensible y evitar accesos no autorizados.
- Administrar adecuadamente las contraseñas y permisos garantiza que solo las personas autorizadas accedan a información importante, reduciendo riesgos de seguridad.
- Configurar controles de acceso a la red basados en los servidores de la entidad permite restringir el acceso a ciertas áreas, evitando que los usuarios lleguen a sitios peligrosos.

- Optimizar los recursos del FortiSIEM facilitaría el monitoreo de sistemas clave como bases de datos, aplicaciones internas y equipos, permitiendo detectar problemas rápidamente y responder de forma oportuna.
- Ajustar las reglas de seguridad en la red ha permitido un mejor control sobre los recursos clave, asegurando que solo lo necesario esté disponible y fortaleciendo la protección.
- Implementar soluciones para gestionar quién puede conectarse a la red mejoraría la seguridad y reduciría el impacto de posibles incidentes.
- Los reportes del SOC han sido clave para detectar y corregir vulnerabilidades, evitando que amenazas afecten la infraestructura crítica de la entidad.
- Es fundamental contar con una persona desde ICETEX en temas de nube que pueda auditar y revisar autorizaciones, ya que su apoyo es crucial para abordar y resolver los hallazgos reportados, lo que permitirá avanzar en los proyectos relacionados con recursos en la nube. La falta de un responsable limita la capacidad de gestión y solución de problemas en este ámbito.

17. ANEXOS

Tema	SubTema	Anexo
Almacenamiento	Backups Diarios	Backups diarios Marzo 2026 (31 reportes) Backup Diario
	Informe de Backups	Consolidado mensual Backups Marzo 2026 Consolidado Mensual de Backups Marzo 2026.pdf Informe Backups mes de Marzo 2026.pdf Manual Backups 1.3-20260316.pdf Politica Backup Icetex V5.xlsx
Aplicaciones	Informes de actividades	Informe actividades Módulos videoconferencia ICETEX Marzo 2026 Informe actividades Módulos videoconferencia ICETEX marzo 2026.pdf Informe mensual Administrador de Soluciones marzo 2026 Informe Mensual InfoTIC Administrador de Soluciones marzo2026.pdf Informe mensual Administrador Web Master marzo 2026 Informe Mensual InfoTIC Webmaster marzo2026.pdf Informe mensual Integrador Nube marzo 2026 Informe Mensual InfoTIC Integrador de Nube marzo2026.pdf
Bases De Datos		Informe mensual Administrador de Bases de datos marzo 2026 Informe Mensual InfoTIC DBA marzo2026.pdf
Ejecución Presupuestal		Conciliación marzo consolidado Conciliación marzo consolidado 2026.xlsx Informe de Gestión Servicio marzo 2026 Informe de Gestion Servicio Marzo 2026.pdf Informe de Gestion Servicio Marzo 2026.docx
Seguridad		Informe Mensual MARCA-OSINT ICETEX marzo 2026 Informe Mensual MARCA-OSINT ICETEX Marzo 2026.pdf Anexo Informe Mensual MARCA-OSINT ICETEX Marzo 2026.xlsx Informe Mensual Seguridad marzo 2026 Informe Mensual InfoTIC Seguridad Marzo2026.pdf Informe Mensual SOC - ICETEX marzo 2026 Informe Mensual SOC-TH ICETEX marzo 2026.pdf Informe técnico análisis de vulnerabilidades ICETEX marzo 2026 WX INFORME TECNICO AV ICETEX Marzo 2026 v1.pdf

Tema	SubTema	Anexo
		WX Matriz de Vulnerabilidades ICETEX MARZO 2026.xlsx
Soporte Y Monitoreo	Canales	ANS marzo 2026 ANS Marzo 2026.xlsx Informe mensual Administrador de Networking marzo 2026 Informe Mensual InfoTIC Administrador de Redes marzo2026.pdf Informe Mensual Disponibilidad marzo2026 Reporte Mensual Disponibilidad INFOTIC Marzo 2026.pdf
	Gráficas de consumo	Informe Mensual ALLOT marzo 2026 Graficas de consumo Marzo 2026 – ALLOT INFOTIC.xls
Data center Alterno	Replicación	Informe mensual replicación febrero2026 Informe mensual replicacion Marzo 2026.pdf Reportes diarios marzo 2026 (31 reportes) Replicaciones
	DRP	Informes Resultado DRP: InformeGerencial Icetex PruebaAislada 20260323.pdf Informe prueba Aislada DRP Icetex 20260323.pdf Anexo1 Evidencias InformePruebaDRPIcetex 20260323.pdf
Data Center Principal		Reporte Monitoreo ICETEX Marzo 2026-ELK Reporte Monitoreo ICETEX Marzo 2026-ELK.pdf Data ELK Disponibilidad Server_ELK Marzo 2026.xlsx

Tabla 39 Anexos

Revisión técnica

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

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

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



INFOTIC
SOLUCIONES INTELIGENTES

REVISÓ	FIRMAS
CONTRATISTA GRUPO DE INFRAESTRUCTURA	

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

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