



INFORME DE ACTIVIDADES DEL CONTRATO

**CONTRATO NUMERO
2022-0792**

Noviembre 01 al 30 de 2025

versión	Observaciones	Fecha	Responsable
1.0	Versión Inicial	01/12/2025	Francisco Javier Pulido
1.2	Ajustes solicitados ICETEX	5/12/2025	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. Canales instalados en el mes y entregables	14
4.1. Despliegue de direcciones IP V6	15
4.2. Implementación canales SDWAN	16
4.3. Centro de Datos Principal	17
4.3.1.1. Aplicaciones	17
4.3.1.2. Bases de Datos	20
4.3.1.3. Sitio Web	24
4.3. Centro de Datos Alterno	27
4.3.2.1. Hosting Virtual (IaaS)	27
4.3.2.2. DataGuard Bases de Datos Megacenter	29
4.3.2.3. Servicios de Housing – Datacenter Alterno	30
4.3.2.4. Servicios de DRP	30
4.4. Seguridad informática	31
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	43
4.3.3.1. Alertas o Incidentes de Seguridad Detectados	47
4.3.3.1.1. Categoría Seguridad	47

4.3.3.1.2. Categoría Disponibilidad	49
4.3.3.1.2. Amenazas de Ciberseguridad	51
4.3.4.2. Gestión de Vulnerabilidades	57
4.3.5. Actividades de PENTEST	60
4.3.6. Reporte De IPS	62
4.3.7. Arquitectura de Seguridad	62
4.3.8. Plan de Continuidad	65
5. GESTION DE LA EJECUCIÓN CONTRACTUAL	68
6. GESTION PRESUPUESTAL	69
7. GESTION ADMINISTRATIVA	72
7.1. Profesionales	72
8. SERVICIO DE COLABORACIÓN	73
9. GESTION DE RIESGOS Y PROBLEMAS	75
10. INDICADORES CLAVE DE DESEMPEÑO	76
10.1. ANS por Disponibilidad de canales de comunicaciones:	76
10.1.1. Canal de Replicación (Triara – Megacenter)	79
10.2.1. Disponibilidad TRIARA para los servicios de página web	81
10.2.2. Análisis componente Liferay Producción	86
10.2.3. Backup Servidores Triara	87
11. CONTROL DE CAMBIOS	89
12. PLAN DE TRABAJO DE LOS PROXIMOS MESES	91
13. RECOMENDACIONES DEL CONTRATISTA AL ICETEX	92
13.1. Networking	92
13.2. Aplicaciones	93
13.3. Seguridad	94
13.4. Bases De Datos	95
13.5. Integrador De Nube	95
14. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC	96
14.1. Aumento de la capacidad de Ancho de Banda en algunas de las sedes de la Entidad	96
14.2. Una capacitación al año de seguridad Informática y servicios conexos	96

14.3. TB de capacidad de almacenamiento	96
14.4. “Wifi” para la gente en 19 sedes	97
15. CONCLUSIONES	98
16. ANEXOS	99

TABLA 1 NORMALIZACIÓN DE DIRECCIONES	13
TABLA 2 PRUEBAS DE CONECTIVIDAD IPV6	14
TABLA 3 CASOS ATENDIDOS NETWORKING COMPARATIVO MES ANTERIOR.....	15
TABLA 4 LISTADO DE DIRECCIONES IP V6 ASIGNADAS A LAS OFICINAS.....	15
TABLA 5 VIGENCIA DE LOS CERTIFICADOS DIGITALES.....	19
TABLA 6 INVENTARIO PRINCIPALES SERVIDORES PRODUCCIÓN	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 SERVICIOS REPLICADOS – DATACENTER MEGACENTER	28
TABLA 11 TOP 5 MÁQUINAS MAYOR TASA DE TRANSFERENCIA.....	28
TABLA 12 TOP 4 MÁQUINAS MENOR TASA DE TRANSFERENCIA.....	28
TABLA 13 DISPONIBILIDAD DE SERVICIOS DE HOUSING – DATA CENTER ALTERNO.....	30
TABLA 14 DETALLE PLATAFORMAS SEGURIDAD ADMINISTRADAS INFOTIC.....	35
TABLA 15 LICENCIAMIENTO FORTIGATE	35
TABLA 16 LICENCIAMIENTO FORTIWEB	40
TABLA 17 CONFIGURACIÓN FORTISANDBOX 1000D	42
TABLA 18 RECOMENDACIONES DE SEGURIDAD	45
TABLA 19 COMPARATIVO – INDICADORES DE COMPROMISO	47
TABLA 20 COMPARATIVO ALERTAS DE SEGURIDAD	48
TABLA 21 PLANES Y PROYECTOS PARA LOGRAR LA ARQUITECTURA OBJETIVO.....	65
TABLA 22 PLAN DE TRABAJO MICROSOFT AZURE – ICETEX.....	68
TABLA 23 EJECUCIÓN PRESUPUESTAL	71
TABLA 24 PERFILES Y ACTIVIDADES	73
TABLA 25 GRUPO ADMINISTRATIVO.....	73
TABLA 26 DISTRIBUCIÓN MÓDULOS DE VIDEOCONFERENCIA POR SEDE.....	74
TABLA 27 NIVEL DE RIESGO	76
TABLA 28 GRADO DE RIESGO	76
TABLA 29 DISPONIBILIDAD DE CANALES.....	79
TABLA 30 DISPONIBILIDAD CANALES “INTERNET PARA LA GENTE”.....	79
TABLA 31 CÓDIGOS RELACIONADOS DISPONIBILIDAD SERVICIOS EN HOUSING – DATACENTER PRINCIPAL.....	80
TABLA 32 DISPOSITIVOS EN HOUSING – DATACENTER PRINCIPAL.....	81
TABLA 33 DISTRIBUCIÓN TRIMESTRAL DE ACCESO POR USUARIOS	82
TABLA 34 CINTAS BACKUPS ICETEX.....	87
TABLA 35 CONTROLES DE CAMBIO NOVIEMBRE	91
TABLA 36 PLANES DE TRABAJO	92
TABLA 37 CAPACIDADES DE ALMACENAMIENTO CONTRATADO	96
TABLA 38 CAPACIDADES DE ALMACENAMIENTO APROVISIONADO.....	97
TABLA 39 PRUEBAS DE RESTAURACIONES DE BACKUPS DE NOVIEMBRE	97
TABLA 40 WIFI PARA LA GENTE INSTALADOS	98
TABLA 41 WIFI PARA LA GENTE PENDIENTES	98
TABLA 42 ANEXOS.....	101

ILUSTRACIÓN 1 TOPOLOGÍA APROBADA SDWAN	16
ILUSTRACIÓN 2 PLAN DE TRABAJO REIMPLEMENTACIÓN SDWAN	17
ILUSTRACIÓN 3 DISPONIBILIDAD DEL CLUSTER	22
ILUSTRACIÓN 4 DISPONIBILIDAD DE LAS BASES DE DATOS PRINCIPALES ICTXCYC Y APOTEOSYS	22
ILUSTRACIÓN 5 CASOS DEL PROYECTO GESTIONADOS ARANDA BASES DE DATOS	23
ILUSTRACIÓN 6 UPTIME: PORTAL WEB WEB.ICETEX.GOV.CO [99,879%]	25
ILUSTRACIÓN 7 TRÁFICO GENERAL DE LOS PORTALES	26
ILUSTRACIÓN 8 REPORTES DE REPLICACIÓN SRM A SITIO ALTERNO – NOVIEMBRE 2025	27
ILUSTRACIÓN 9 FECHAS CON MAYOR REPLICACIÓN	29
ILUSTRACIÓN 10 EVIDENCIA DATAGUARD REPLICADO A MEGACENTER BD	30
ILUSTRACIÓN 11 DIAGRAMA DE LA ARQUITECTURA DE SEGURIDAD.....	31
ILUSTRACIÓN 12 TOPOLOGÍA DE WAF CLOUD USADO EN PORTALES DE MEDELLÍN	32
ILUSTRACIÓN 13 CONSUMO CANAL MPLS - PROMEDIO 1200G [INR0185 CLARO(MPLS_DC)]	35
ILUSTRACIÓN 14 CONSUMO CANAL INTERNET SEDES - PROMEDIO 1100 GB WAN-SEDES-ICETEX [INR0264 (INTE_SEDES_ICTX)]	36
ILUSTRACIÓN 15 CONSUMO CANAL INTERNET DATA CENTER- INTERNET DATACENTER [INTERNET_DC_INR0000320 (INET_CLARO)].....	36
ILUSTRACIÓN 16 FILTRADO – WEB – (FORTIGATE – TRIARA).....	37
ILUSTRACIÓN 17 INSPECCIÓN – SSL – (FORTIGATE – TRIARA)	37
ILUSTRACIÓN 18 ANTIVIRUS Y ANTIMALWARE – PERIMETRAL (FORTIGATE – TRIARA)	38
ILUSTRACIÓN 19 CONSUMO CANAL MPLS AGUAS - PROMEDIO 800 GB	38
ILUSTRACIÓN 20 FILTRADO-WEB-(FORTIGATE-AGUAS).....	39
ILUSTRACIÓN 21 INSPECCIÓN-SSL-(FORTIGATE-AGUAS)	39
ILUSTRACIÓN 22 ANTIVIRUS Y ANTIMALWARE-PERIMETRAL-(FORTIGATE-AGUAS)	39
ILUSTRACIÓN 23 CONSUMO CANAL MPLS MEDELLÍN	40
ILUSTRACIÓN 24 TRÁFICO GENERAL DE LOS PORTALES	41
ILUSTRACIÓN 25 TRÁFICO GENERAL DE LOS PORTALES	41
ILUSTRACIÓN 26 DESEMPEÑO POR PROCESOS	43
ILUSTRACIÓN 27 ESTADO SEGURIDAD SOPHOS	43
ILUSTRACIÓN 28 TOTAL DE ALERTAS DE SEGURIDAD	48
ILUSTRACIÓN 29 TOP 5 DE ALERTAS DE SEGURIDAD ALTAS	49
ILUSTRACIÓN 30 TOP 5 DE ALERTAS DE SEGURIDAD MEDIAS	49
ILUSTRACIÓN 31 TOP 10 DE ALERTAS DE DISPONIBILIDAD ALTAS	50
ILUSTRACIÓN 32 ATAQUES IPS PERMITIDOS	51
ILUSTRACIÓN 33 ATAQUES IPS DENEGADOS	51
ILUSTRACIÓN 34 PUERTOS ENTRANTES DE PÚBLICO A PRIVADO (PERMITIDOS).....	52
ILUSTRACIÓN 35 TOP DE ACCESOS FALLIDOS PLATAFORMA WINDOWS	53
ILUSTRACIÓN 36 CUENTAS BLOQUEADOS.....	54
ILUSTRACIÓN 37 INCIDENTES POR TIPO DE AMENAZA	55
ILUSTRACIÓN 38 ESTADO DE REMEDIACIÓN AMENAZAS-CLON SERVIDOR MIRA.....	57
ILUSTRACIÓN 39 RESULTADO ESCaneo VULNERABILIDADES URL'S.....	60
ILUSTRACIÓN 40 RESULTADO ESCaneo VULNERABILIDADES SERVIDORES	61
ILUSTRACIÓN 41 MATRIZ DE RIESGOS	75
ILUSTRACIÓN 42 UPTIME – PORTAL WEB WEB.ICETEX.GOV.CO	82
ILUSTRACIÓN 43 MÉTRICA DE VISITANTES PORTAL WEB WEB.ICETEX.GOV.CO.....	82
ILUSTRACIÓN 44 MÉTRICA ADQUISICIÓN USUARIOS PORTAL WEB WEB.ICETEX.GOV.CO	83
ILUSTRACIÓN 45 MÉTRICA DE USUARIO POR PAÍS - PORTAL WEB WEB.ICETEX.GOV.CO	83
ILUSTRACIÓN 46 MÉTRICA DE CIUDADES DE COLOMBIA- PORTAL WEB WEB.ICETEX.GOV.CO	84
ILUSTRACIÓN 47 NODO 1 CPU	85
ILUSTRACIÓN 48 NODO 1 MEMORIA	86

ILUSTRACIÓN 49 NODO 1 ALMACENAMIENTO.....	86
ILUSTRACIÓN 50 EVIDENCIA BACKUP SERVIDORES RESUMEN GENERAL BACKUPS	88
ILUSTRACIÓN 51 EVIDENCIA BACKUP SERVIDORES RESUMEN BACKUPS Y SU ESTADO	88
ILUSTRACIÓN 52 HISTÓRICO CONSOLIDADO USO DE DISCOS SERVIDOR ICTXSRVNETCOR01	94

1. INTRODUCCIÓN

Este informe contiene la información relacionada con las actividades ejecutadas por INFOTIC con ocasión de la celebración del contrato 2022-0792, durante el periodo comprendido entre el 01 al 30 de noviembre de 2025. 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 88.8 % que representa los 32 meses que lleva dentro de la fase de Operación el proyecto.

El presente informe, correspondiente al mes de noviembre del 2025, describe los servicios realizados durante el periodo por el equipo de profesionales y las herramientas tecnológicas asignadas y dispuestas por INFOTIC para desempeñar las funciones y atender los requerimientos del ICETEX según lo establecido en el contrato.

2. OBJETIVO DEL INFORME

Presentar las actividades ejecutadas por INFOTIC durante el periodo del 01 al 30 de noviembre de 2025, 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 30 de noviembre 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 Alterno los cuales se encuentra bajo la modalidad de Housing y todos los servicios requeridos para nube privada, dejando claro que a través del contrato se busca integrar servicios de nube pública e híbrida. A la fecha todos los recursos actuales se están usando sin sobre dimensionamientos.

➤ **Servicios conexos**

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

4. AVANCE TÉCNICO

4.1. Conectividad y Red de Comunicaciones

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

Durante el presente periodo y a fin de destacar se atendieron un total de 16 solicitudes, con respecto al mes anterior hubo un incremento de 8 casos ya que se atendieron 8 solicitudes en el mes anterior.

[Registro Aranda Noviembre 2025.xlsx](#)

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:

[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>

Con el fin de garantizar conectividad con el protocolo IPV6, hemos adelantado un plan de trabajo, cuyo estado a la fecha se presenta a continuación:

SEDE	Segmento IPv4	Segmento IPv6
Aguas	10.255.0.0/24	2801:192:6:E0::/64
Chapinero Bogotá	10.255.1.0/24	2801:192:6:E1::/64
Ángel Bogotá	10.255.2.0/24	2801:192:6:E2::/64
Cali	10.255.3.0/24	2801:192:6:E3::/64
Medellín	10.255.4.0/24	2801:192:6:E4::/64
Buenaventura	10.255.5.0/24	2801:192:6:E5::/64
Quibdó	10.255.6.0/24	2801:192:6:E6::/64
Riohacha	10.255.7.0/24	2801:192:6:E7::/64
Montería	10.255.8.0/24	2801:192:6:E8::/64
Pereira	10.255.9.0/24	2801:192:6:E9::/64
Bucaramanga	10.255.10.0/24	2801:192:6:EA::/64
Popayán	10.255.11.0/24	2801:192:6:EB::/64
Valledupar	10.255.12.0/24	2801:192:6:EC::/64
Santa Marta	10.255.13.0/24	2801:192:6:ED::/64
Barranquilla	10.255.14.0/24	2801:192:6:EE::/64
Sincelejo	10.255.15.0/24	2801:192:6:EF::/64
Tumaco	10.255.16.0/24	2801:192:6:F0::/64
Cúcuta	10.255.17.0/24	2801:192:6:F1::/64
Villavicencio	10.255.18.0/24	2801:192:6:F2::/64
Tunja	10.255.19.0/24	2801:192:6:F3::/64
Cartagena	10.255.20.0/24	2801:192:6:F4::/64

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	Segmento IPv4	Segmento IPv6
Aguas	10.255.0.0/24	2801:192:6:E0::/64
San Andrés	10.255.21.0/24	2801:192:6:F5::/64
Armenia	10.255.22.0/24	2801:192:6:F6::/64
Arauca	10.255.23.0/24	2801:192:6:F7::/64
Pasto	10.255.24.0/24	2801:192:6:F8::/64
Ibagué	10.255.25.0/24	2801:192:6:F9::/64
Apartado	10.255.26.0/24	2801:192:6:FA::/64
Mocoa	10.255.27.0/24	2801:192:6:FB::/64
Yopal	10.255.28.0/24	2801:192:6:FC::/64
Manizales	10.255.29.0/24	2801:192:6:FD::/64
Neiva	10.255.30.0/24	2801:192:6:FE::/64
Angel	10.255.31.0/24	
Leticia	10.255.32.0/24	2801:192:6:FF::/64
Mocoa SD WAN	10.255.61.0/24	
Aguas SD_WAN		
Leticia SD_WAN	10.255.70.0/24	

Tabla 1 Normalización de direcciones

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.

Hasta la fecha, las sedes que se han realizado pruebas de conectada IPv6 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	09:00 - 11:00	Realizadas
4	Medellín	2/10/2025	09:00 - 11:00	Realizadas
5	Buenaventura	3/10/2025	09:00 - 11:00	Realizadas
6	Quibdó	7/10/2025	09:00 - 11:00	Realizadas
7	Riohacha	9/10/2025	09:00 - 11:00	Realizadas
8	Montería	10/10/2025	16:00 - 17:00	Realizadas
9	Bucaramanga	16/10/2025	09:00 - 11:00	Realizadas
10	Popayán	17/10/2025	09:00 - 11:00	Realizadas
11	Pereira	20/10/2025	09:00 - 11:00	Realizadas
12	Valledupar	21/10/2025	09:00 - 11:00	Realizadas

Consecutivo	Sede	Pruebas seguridad	Horario	Observación
13	Santa Marta	23/10/2025	09:00 - 11:00	Realizadas
14	Barranquilla	24/10/2025	09:00 - 11:00	Realizadas
15	Sincelejo	28/10/2025	09:00 - 11:00	Realizadas
16	Tumaco	30/10/2025	09:00 - 11:00	Realizadas
17	Cúcuta	4/11/2025	09:00 - 11:00	Realizadas

Tabla 2 Pruebas de conectividad IPv6

4.1. 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 Noviembre 2025.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 noviembre.

Los casos atendidos durante el mes están disponibles en el siguiente enlace:
[Registro Aranda Noviembre 2025.xlsx](#)

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

Mes	No. Casos
Septiembre	43
Octubre	8
Noviembre	16

Tabla 3 Casos atendidos Networking comparativo mes anterior

4.1. 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	09:00 - 11:00	Realizadas
4	Medellín	2/10/2025	09:00 - 11:00	Realizadas
5	Buenaventura	3/10/2025	09:00 - 11:00	Realizadas
6	Quibdó	7/10/2025	09:00 - 11:00	Realizadas
7	Riohacha	9/10/2025	09:00 - 11:00	Realizadas
8	Montería	10/10/2025	16:00 - 17:00	Realizadas
9	Bucaramanga	16/10/2025	09:00 - 11:00	Realizadas
10	Popayán	17/10/2025	09:00 - 11:00	Realizadas
11	Pereira	20/10/2025	09:00 - 11:00	Realizadas
12	Valledupar	21/10/2025	09:00 - 11:00	Realizadas
13	Santa Marta	23/10/2025	09:00 - 11:00	Realizadas
14	Barranquilla	24/10/2025	09:00 - 11:00	Realizadas
15	Sincelejo	28/10/2025	09:00 - 11:00	Realizadas
16	Tumaco	30/10/2025	09:00 - 11:00	Realizadas
17	Cúcuta	4/11/2025	09:00 - 11:00	Realizadas

Tabla 4 Listado de direcciones IP V6 asignadas a las oficinas

4.2. Implementación canales SDWAN

La topología, aprobada, para la solución de SD-WAN en la que se traslada el punto central a Triara es la siguiente:

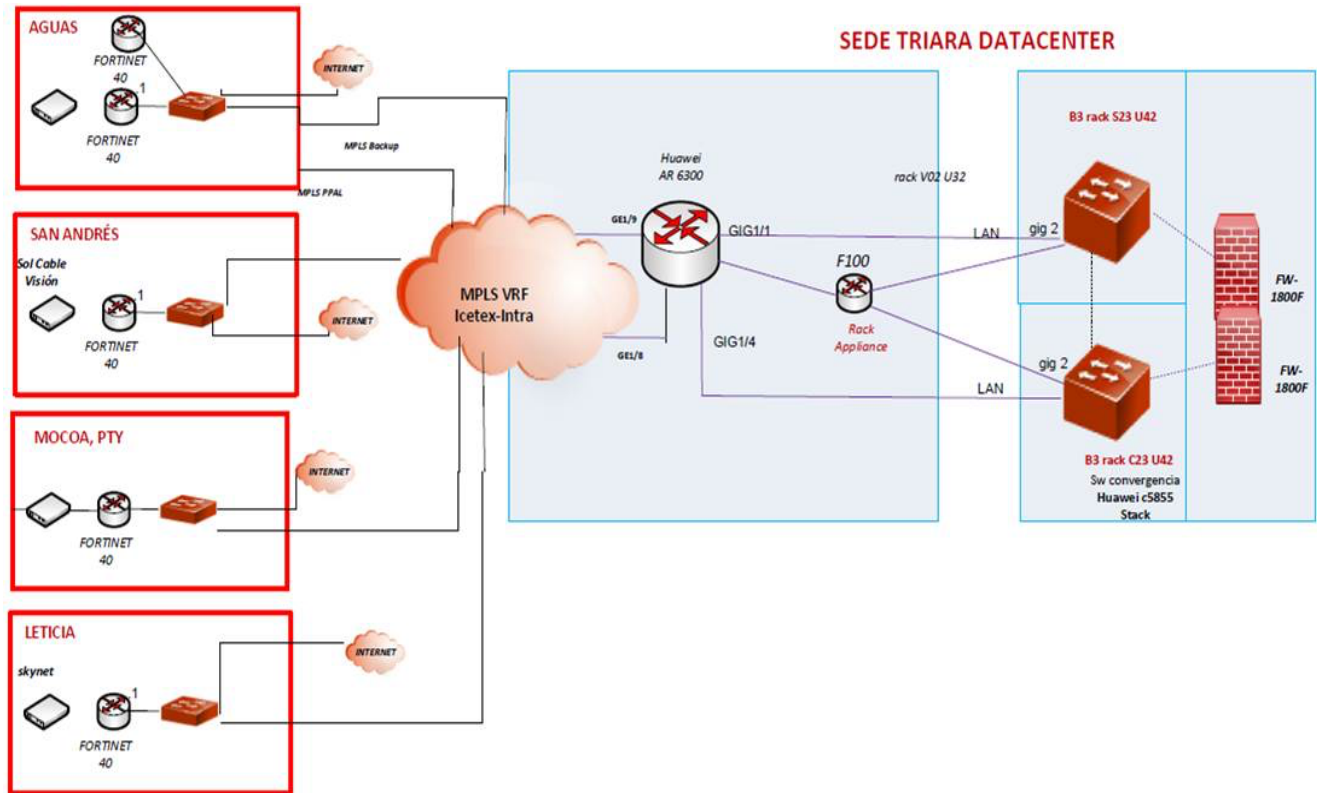


Ilustración 1 Topología aprobada SDWAN

En este escenario se conserva la topología de las 4 sedes:

- Aguas
- San Andrés
- Mocoa
- Leticia

A continuación, se presenta el estado actual del 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

Gerente del proyecto:		Arley Vargas					
Inicio del proyecto:		23-oct-25					
Nombre del proyecto:		INFOTIC					
		Semana Inicio:					
#	Actividad	Asignado a	Inicio	Fin	Duración	Estado	% Ejecutado
1	KickOff con Cliente	Claro - Infotíc	23-oct-25	23-oct-25	1	Terminada	100%
2	Adquisición de Equipos	Proyectos - Compras	23-oct-25	28-oct-25	4	Terminada	100%
3	Levantamiento de información Técnica	Claro - Infotíc	28-oct-25	28-oct-25	1	Terminada	100%
4	Elaboración Plan técnico / Sow	Líder Técnico	28-oct-25	12-nov-25	12	Terminada	100%
5	Presentación Plan técnico/ Sow	Líder Técnico	24-nov-25	24-nov-25	1	En curso	50%
6	Solicitud espacio y carga	Claro	31-oct-25	14-nov-25	11	Terminada	100%
7	Instalación Equipos Triara	Claro	26-nov-25	26-nov-25	1	Asiganda	0%
8	Cxc en Triara	Claro	27-nov-25	5-dic-25	7	Asiganda	0%
9	Definición de estrategia plan de migración	Claro - Infotíc	24-nov-25	1-dic-25	6	En curso	10%
10	Pruebas finales y estabilización Triara	Claro	8-dic-25	12-dic-25	5	Asiganda	0%
11	Instalación y pruebas sedes remotas	Claro	15-dic-25	19-dic-25	5	Asiganda	0%
12	Pruebas finales y estabilización	Claro	22-dic-25	26-dic-25	5	Asiganda	0%
13	Paso a operación	Claro	29-dic-25	31-dic-25	3	Asiganda	0%
14	Cierre	Gerente de Proyecto	31-dic-25	31-dic-25	1	Asiganda	0%

Ilustración 2 Plan de trabajo reimplementación SDWAN

4.3. Centro de Datos

4.3. Centro de Datos Principal

4.3.1.1. Aplicaciones

Durante el mes de noviembre de 2025, se atendieron un total de un total de 23 solicitudes, todas documentadas con sus respectivas evidencias. A continuación, se presenta el detalle de estas:

- **Actualización de archivos en servidores C&CTEX y MIRA**
Se realizaron cuatro intervenciones orientadas a la modificación y ajuste de archivos ASP, garantizando la continuidad y el correcto funcionamiento de las aplicaciones institucionales.
- **Optimización de la integración PSE (recaptcha)**
Se ejecutaron tareas tanto en el **FrontEnd** como en el **BackEnd** del sistema de pagos, fortaleciendo los mecanismos de validación y seguridad para los usuarios.
- **Acceso a servidores de pruebas**
Se habilitaron accesos a distintos servidores (10.1.18.65 y 10.1.18.124), asegurando la disponibilidad de entornos de validación y pruebas para el equipo de desarrollo.
- **Desarrollo y actualización de aplicaciones institucionales**
 - Creación e implementación de la aplicación Simulador de Crédito Educativo, junto con su posterior actualización.
 - Copia y actualización de plantillas asociadas a la aplicación WsDesembolsos, garantizando su alineación con los procesos operativos.

- **Gestión de accesos y permisos FTP**

Se configuraron y ajustaron permisos para usuarios VF y OCM, asegurando un control adecuado en la transferencia de archivos y la gestión de información.

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 1218 y 1219 con el fin de proceder a efectuar las actualizaciones respectivas.

Los servidores administrados se encuentran en estado estable, sin eventos críticos, únicamente registros informativos normales. El detalle de los consumos de los principales recursos puede ser consultado en el informe de especialistas de soluciones.

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 Noviembre2025.xlsx](#)

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

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

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

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, en donde destacan vencimiento de dos certificados en el mes de noviembre:

No	Sitio Web	Subdominio (icetex.gov.co)	Fecha creación	Fecha revocación	Tipo SSL Asignado
1	Colección de Aplicaciones	aplicaciones.icetex.gov.co	4/12/2024	4/12/2025	Secure Site Pro EV SSL
2	Portal Institucional	web.icetex.gov.co	4/12/2024	4/12/2025	Secure Site Pro EV SSL
3	Portal DECEVAL - Pagaré	pagare.icetex.gov.co	3/12/2024	3/12/2025	Secure Site Pro SSL
4	Portal C&CETEX	www.icetex.gov.co	4/12/2024	4/12/2025	Secure Site Pro EV SSL
5	Colección de Web Services Internos	appwebservices.icetex.gov.co	3/12/2024	3/12/2025	Secure Site Pro SSL
6	Pasareladepagos	webhook.icetex.gov.co	16/10/2025	25/10/2026	RapidSSL
7	Web Service RNEC	mec.icetex.gov.co	16/10/2025	25/10/2026	RapidSSL
8	Wildcard	*.icetex.gov.co	17/11/2024	17/11/2025	Wildcard Rapid SSL RSA CA

Tabla 5 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.

Para el presente mes se tuvo dificultades en la operación con el certificado que se emplea para la interacción con la registraduría nacional del estado civil. Es imperativo que el ICETEX asegure la provisión de los certificados próximos a vencer de forma oportuna para evitar incidentes en la operación.

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

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

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

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

Tabla 6 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.

4.3.1.2. Bases de Datos

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

BASES DE DATOS	VERSION	TAMAÑO
ASMn user grid	19.13.0.0.0	GB
ICTXCYC	11.0.2.0.4	4,925
ICETEX	11.0.2.0.4	207
APLICATI	11.0.2.0.4	243
APOTEOSY	11.0.2.0.4	481
VIGIAPRD	19.16.0.0	178
LIFERAY LIFERAYPDB	19.16.0.0	8.20

BASES DE DATOS	VERSION	TAMAÑO
LANDICTX	19.16.0.0	554
SGDEA	19.16.0.0	143

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 valido 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 noviembre 2025 fue del 100% como se evidencia en la siguiente ilustración:

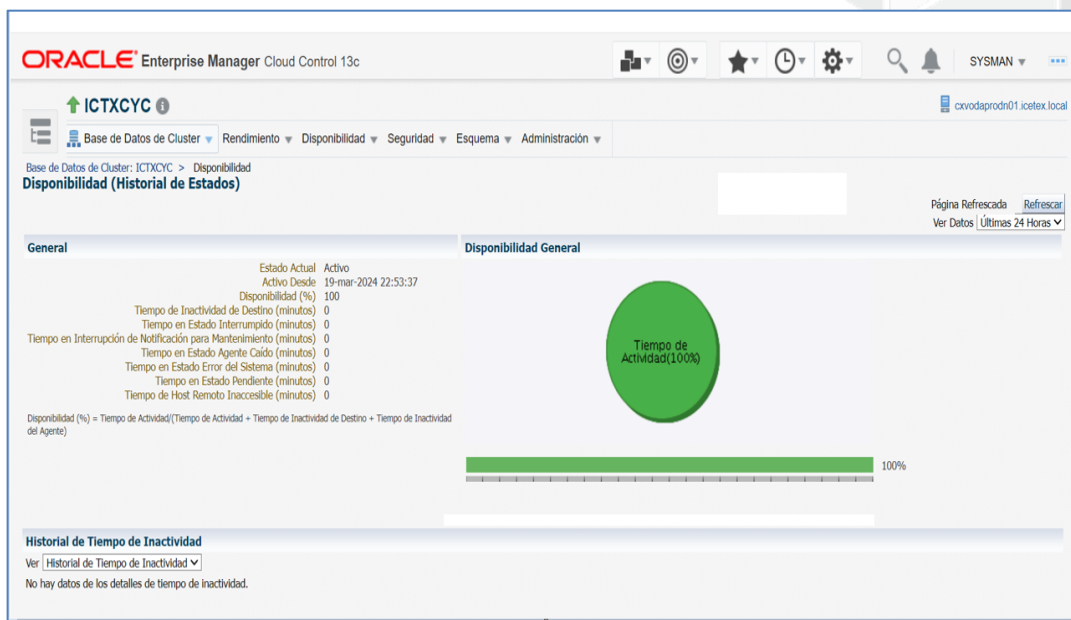


Ilustración 3 Disponibilidad del cluster

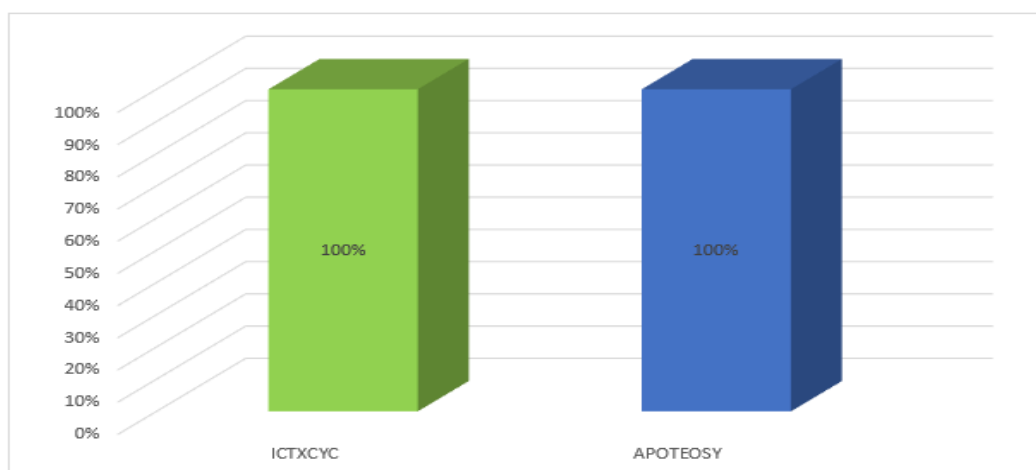


Ilustración 4 Disponibilidad de las Bases de Datos principales ICTXYC y APOTEOSY

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.

En periodos pasados se elaboró una propuesta para el control de accesos a nivel de BD, sin tener respuesta por parte del ICETEX. A la fecha se tiene evidencia, por medio de consultas a la auditoría, que hay usuarios realizando DML's y DDL's en la BD empleando usuarios de aplicación sin ningún tipo de solicitud o control de cambio.

Se migró la base de datos de ICTXCYC producción versión 11G a versión de pruebas 19C

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.

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

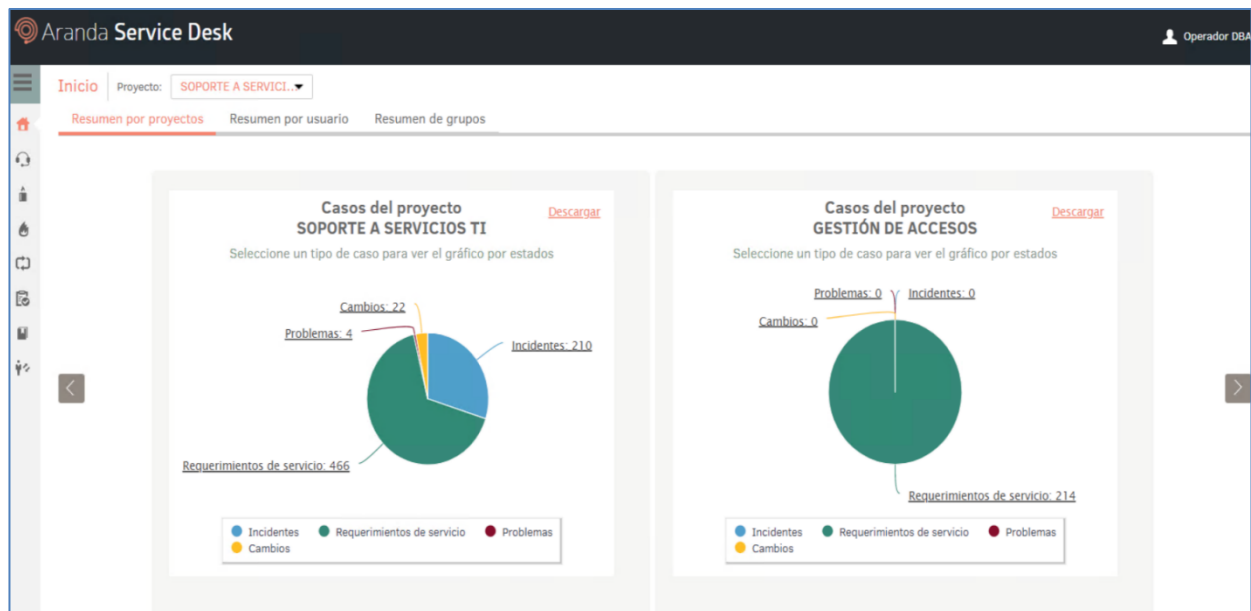


Ilustración 5 Casos del proyecto Gestionados Aranda Bases de datos

Desde Bases de datos se tienen las siguientes recomendaciones:

Almacenamiento:

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

BASE DE DATOS	ABRIL 2025	MAYO 2025	JUNIO 2025	JULIO 2025	AGO 2025	SEPT 2025	OCT-2025	NOV 2025
ICTXCYC	4,652	4,590	4,641	4,683	4,766	4,774	4,923	4,925
ICETEX	204	202	203	206	206	206	206	207
APLICATI	247	243	243	243	243	243	243	243
APOTEOSY	485	458	459	460	460	480	481	481
VIGIAPRD	120	133	137	143	143	166	175	178
LIFERAY LIFERAYPDB	8.20	8.20	8	8	8	8	8	8
LANDICTX	533.5	529	529	529	529	529	529	554
SGDEA	108	112	120	124	124	136	140	143
TOTAL==>	6357.7	6,274.90	6,340.20	6,396.00	6,479.00	6,542.00	6,705.00	6,738.56

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

- Se aumentó el espacio del área de recuperación de las bases de datos productivas de 1TB a 2TB para tener una retención de 10 días o más.

Virus:

- Se iniciaron las acciones para el cambio del antivirus en las bases de datos.

Permisos de usuarios en las bases de datos:

- Se bloquearon los usuarios INFOTIC Y DCSCAF.
- Se finalizó la actividad de restringir a los usuarios de desarrollo a las bases de datos de producción y se les otorgaron permisos de consulta al ambiente replicado emn el centro de datos alterno.

Replicación

- Durante el mes de noviembre de 2025 se continuo con la replicación permanente de las BD Oracle al Datacenter alterno de acuerdo con las políticas establecidas, utilizando el Oracle Active Data Guard el cual garantiza una alta disponibilidad, protección de datos y recuperación ante desastres.

4.3.1.3. Sitio Web

Durante el mes de noviembre 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 noviembre2025.pdf](#)

En cuanto a la disponibilidad del portal web de la entidad se presentan unos uptime superiores al 99.018% como se evidencia en la siguiente gráfica:

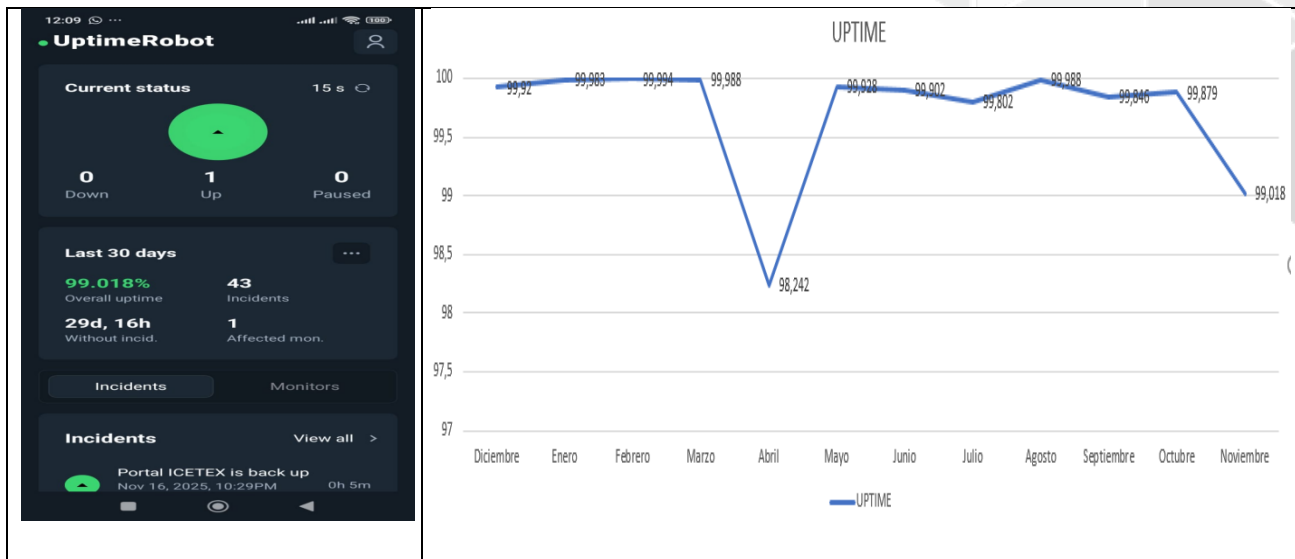


Ilustración 6 UPTIME: Portal WEB web.icetex.gov.co [99,879%]

En relación con los requerimientos, aumentó en un 50%, debido a que se brindó apoyo a la OCM en ocultar una información en la parte superior de tres contenidos web y se reporta un caso escalado por error.

Por consiguiente, se brindó apoyo a la OCM con la republicación de contenidos, atendiendo 31 casos de Aranda, terminando todo el proceso con un total de 66 casos atendidos.

Los incidentes disminuyeron en un 36,36%, los casos reportados corresponden a caídas del servicio Elasticsearch, se reportan 4 casos escalados por error.

En cuanto a los casos de gestión de cambios disminuyeron en un 50%, debido a solo se ejecutó el caso correspondiente a la implementación de IPv6 en los servicios del portal ICETEX.

Por último, los casos SD Claro disminuyeron en 50%, los casos que se reportaron fueron de acompañamiento para ventanas de mantenimiento por caída del portal y redireccionamiento de URLs por parte de la OCM.

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

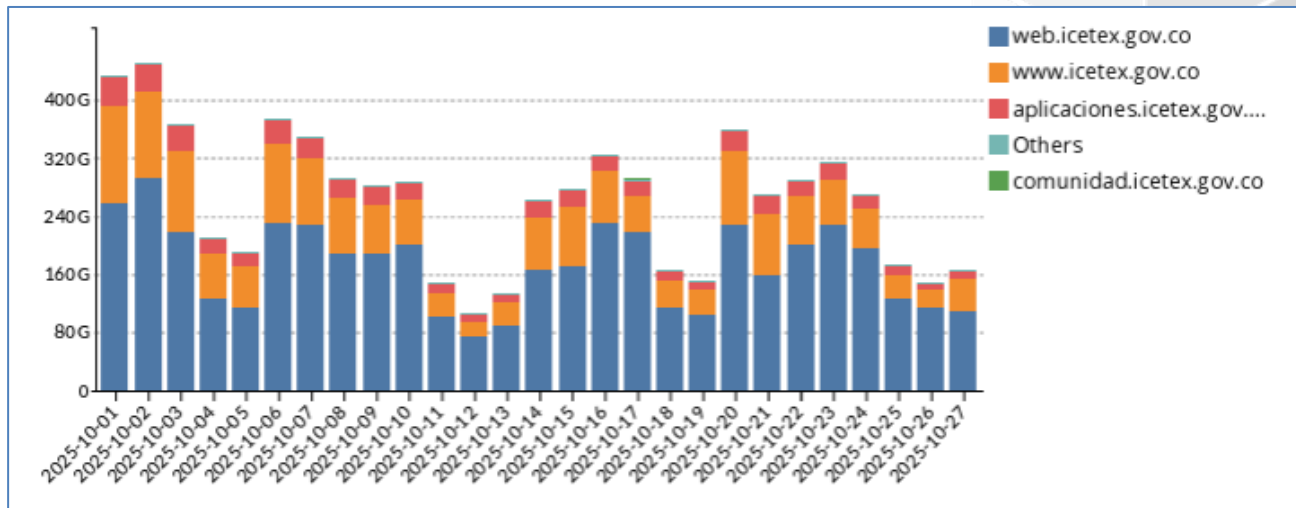


Ilustración 7 Tráfico General De Los Portales

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

#	HTTP Host	HTTP Request Bytes	HTTP Response Bytes
1	web.icetex.gov.co	386.47 GB	4.28 TB
2	www.icetex.gov.co	29.34 GB	1.62 TB
3	aplicaciones.icetex.gov.co	78.37 GB	522.76 GB
4	comunidad.icetex.gov.co	402.78 MB	22.62 GB
5	comunidad.icetex.gov.co:443	3.40 MB	474.54 MB
6	web.icetex.gov.co:443	5.72 MB	378.48 MB
7	cina.icetex.gov.co:443	2.97 MB	343.08 MB
8	comunidad.icetex.gov.co:80	1.96 MB	268.00 MB
9	transaccional.icetex.gov.co:80	2.19 MB	263.37 MB
10	identidad.icetex.gov.co	11.01 MB	101.55 MB

Tabla 9 Top 10 Portales más utilizados

El estado del licenciamiento es el siguiente:

- Liferay 7.3 vence el 18 de noviembre de 2026.
- Elasticsearch vence el 30 de noviembre de 2026.

4.3. Centro de Datos Alterno

4.3.2.1. Hosting Virtual (IaaS)

En el transcurso del mes de noviembre, 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 Noviembre 2025.pdf](#) cuyo reporte refleja el consolidado de los informes mensuales y que se están entregando periódicamente, a continuación se puede ver el último reporte diario del mes.

Site Recovery Manager - Estado Replicas INFOTIC

Actualmente el SRM (vcsatriara-ext.datacenterdhs.local -> vcmegacenter.datacenterdhs.local) cuenta con 9 replicas

General					
Name			Count		
OK			9		
Grupo de protección: PG_INFOTIC_7 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0226_INFOTIC_REP	OK	5 of 5	Nov 30, 2025	143.38 MB	5 minutes
Grupo de protección: PG_INFOTIC_6 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0228_INFOTIC_REP	OK	1 of 1	Nov 30, 2025	46.69 MB	1 hour
INR0229_INFOTIC_REP	OK	1 of 1	Nov 30, 2025	101.51 MB	1 hour
Grupo de protección: PG_INFOTIC_4 (3)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0238_INFOTIC_REP	OK	2 of 2	Nov 30, 2025	51.24 MB	1 hour
INR0239_INFOTIC_REP	OK	2 of 2	Nov 30, 2025	33.7 MB	1 hour
INR0243_INFOTIC_REP	OK	2 of 2	Nov 30, 2025	125.38 MB	1 hour
Grupo de protección: PG_INFOTIC_3 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0244_INFOTIC_REP	OK	1 of 1	Nov 30, 2025	81.07 MB	1 hour
INR0245_INFOTIC_REP	OK	1 of 1	Nov 30, 2025	9.49 MB	5 minutes
Grupo de protección: PG_INFOTIC_2 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0249_INFOTIC_REP	OK	2 of 2	Nov 30, 2025	13.09 MB	5 minutes

Ilustración 8 Reportes de replicación SRM a Sitio Alterno – Noviembre 2025

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

#	INR Replicación	Host Name	Servicio	Virtual Machine 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	INR0209 **	icetexboglobserver1	Portal productivo (liferay)	INR0237_INFOTIC_REP
8	INR0210	icetexbogliferaynfs	Portal productivo (liferay)	INR0238_INFOTIC_REP
9	INR0217	icetexbogelasticserver1	Portal productivo (liferay)	INR0239_INFOTIC_REP
10	INR0218	icetexbogliferayserver1	Portal productivo (liferay)	INR0243_INFOTIC_REP
11	INR0215	icetexboglxdarumasrv1	DARUMA	INR0244_INFOTIC_REP
12	INR0213	icetexboglxdarumasrv2	DARUMA	INR0245_INFOTIC_REP
13	INR0214	icetexboglxroad1	XROAD	INR0249_INFOTIC_REP

Tabla 10 Servicios replicados – Datacenter Megacenter

*Se detiene la replicación identificada con el código INR0208 que replica la máquina INR0236- ICTXBOGSRVPT1. Los recursos de esta última se distribuyen, en el centro de datos TRIARA, entre los servidores OPENSIFT identificados con los códigos de servicio INR0259, INR0258 e INR0251.

** Se detiene la replicación INR0209 que replica la máquina virtual INR0237- icetexboglobserver1, corresponde al antiguo balanceador, NGIX, que fue deshabilitado en TRIARA

***Por solicitud de ICETEX se detiene la replicación INR0219 y INR0220 que replica las máquinas virtuales INR0233 e INR0262 icetexboglxorfeo1 y icetexboglxorfeo2 respectivamente, las máquinas virtuales siguen en producción en TRIARA.

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

INR	HOSTNAME	MB
INR0243	icetexbogliferayserver1	56332,23
INR0228	ictxisgesbd	9814,6
INR0229	ictxisgesapp	7128,61
INR0226	icetexbogwsmira	6874,52
INR0238	icetexbogliferaynfs	5872,17

Tabla 11 TOP 5 máquinas mayor tasa de transferencia

INR	HOSTNAME	MB
INR0245	icetexboglxdarumasrv2	205,12
INR0249	icetexboglxroad1	581,06
INR0239	icetexbogelasticserver1	1793,15
INR0244	icetexboglxdarumasrv1	2214,35

Tabla 12 TOP 4 máquinas menor tasa de transferencia

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

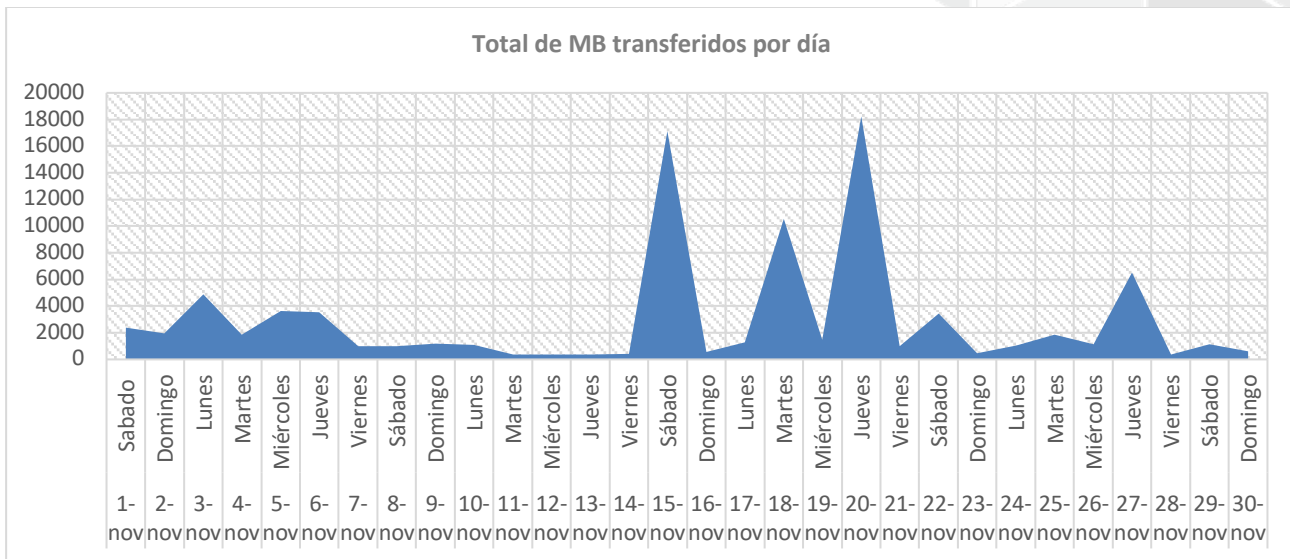


Ilustración 9 Fechas con mayor replicación

La transferencia de datos está altamente concentrada en la máquina virtual INR0243, esta VM representa aproximadamente el **62%** del total de datos replicados en noviembre que fue aproximadamente 90.81 GB

El volumen de 90,815MB aproximadamente 90.8 GB en noviembre es más de cuatro veces (315.53%) más que el mes anterior.

Se observa una tendencia a tener picos de transferencia significativos concentrados en días específicos, particularmente los fines de semana (sábados 14-nov y 22-nov, Domingos 15-nov) o viernes (20-nov).

Las semanas 2 y 3 con 471 GB y 502 GB muestran una transferencia más constante.

- El día con más tráfico: jueves 20 de noviembre con 18.23 GB
- El día con menos tráfico: jueves 13 de noviembre con 346.78 MB

Los datos muestran que el proceso de replicación incremental está funcionando correctamente. Las variaciones en las cantidades de datos transferidos en las semanas posteriores reflejan la cantidad de cambios (nuevos datos o modificaciones) que se produjeron en el entorno de las máquinas virtuales durante esos períodos.

4.3.2.2. DataGuard Bases de Datos Megacenter

Durante el mes de noviembre de 2025 se continuo con la replicación permanente de las BD Oracle al Datacenter alterno de acuerdo con las políticas establecidas, utilizando el Oracle Active DataGuard el cual garantiza una alta disponibilidad, protección de datos y recuperación ante desastres. Ver las evidencias en el documento [Informe Mensual InfoTIC DBA Noviembre2025.pdf](#)

```

10.1.18.120 - Conexión a Escritorio remoto
oracle@covodacontg011:~$ ps -ef | grep pmon
oracle 3828 1 0 Aug22 T 00:00:00 ora_pmon_SMON0
grid 7987 1 0 Aug22 T 00:13:56 asm_pmon_ASM
oracle 7998 1 0 Aug22 T 00:13:56 ora_pmon_ICMT0
oracle 9638 1 0 Aug22 T 00:13:56 ora_pmon_ML000
oracle 10288 1 0 Aug22 T 00:14:01 ora_pmon_MF000
oracle 10592 1 0 Aug22 T 00:14:18 ora_pmon_ML001
oracle 10998 1 0 Aug22 T 00:14:18 ora_pmon_LAND0
oracle 15527 1 0 Aug22 T 00:14:18 ora_pmon_MF000
oracle 21343 26/5 0 1A:2A pts/0 00:00:00 grep --color=auto pmon
oracle 22385 1 0 Aug22 T 00:00:00 ora_pmon_L11000
oracle 27315 1 0 Aug22 T 00:00:00 ora_pmon_ICT000
[oracle@covodacontg011 ~]$ sqlplus / as sysdba
SQL*Plus: Release 11.2.0.4.0 Production on Mon Dec 1 14:24:16 2025
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 apply

  Thread Last Sequence Received Last Sequence Applied TIME RECEIVED TIME APPLIED
-----
1 153345 01/12/2025 14:22 01/12/2025 14:22
2 187289 01/12/2025 14:22 01/12/2025 14:22

SQL> sta apply

  Thread Last Sequence Received Last Sequence Applied Difference
-----
1 153345 01/12/2025 14:22 01/12/2025 14:22 0
2 187289 01/12/2025 14:22 01/12/2025 14:22 0

SQL>
  
```

Ilustración 10 Evidencia DataGuard replicado a Megacenter BD

Se generó la consulta de los archivos recibidos y aplicados de la base de datos de ICTXCYCD a 01/12/2025 con diferencia cero(0) archivos sin aplicar, lo anterior indica que las BD y su replicación se encuentran sincronizadas.

4.3.2.3. 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 noviembre al 100%:

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

Tabla 13 Disponibilidad de Servicios de Housing – Data Center Alterno

4.3.2.4. Servicios de DRP

El 29 de noviembre se ejecutó, la actividad programada, del DRP.

- **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.
- **Objetivos:**
 - 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:

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

- Asegurar la disponibilidad de los recursos de infraestructura tecnológica que soportan los servidores de PORTAL PRODUCTIVO (LIFERAY) y servidor de aplicaciones MIRA de ICETEX de modo Aislado en Megacenter.
- Ejecutar validaciones técnicas, conectividad y pruebas funcionales formulario “Renovación de crédito” de modo Aislado en el sitio alternativo
- **Escenario seleccionado:** Falla de Conectividad de Red
- **Acción:** Simular una interrupción de la red que aísla el Datacenter principal y se levanta el alternativo de forma paralela.
- **Minutograma y formularios de Pruebas compartidos por correo con Icetex.**

El ejercicio tuvo una demora de una 1 hora y media, debido a que el funcionario Mauricio morales, funcionario del ICETEX, retardó las pruebas sin ninguna justificación técnica.

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

4.4. Seguridad informática

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

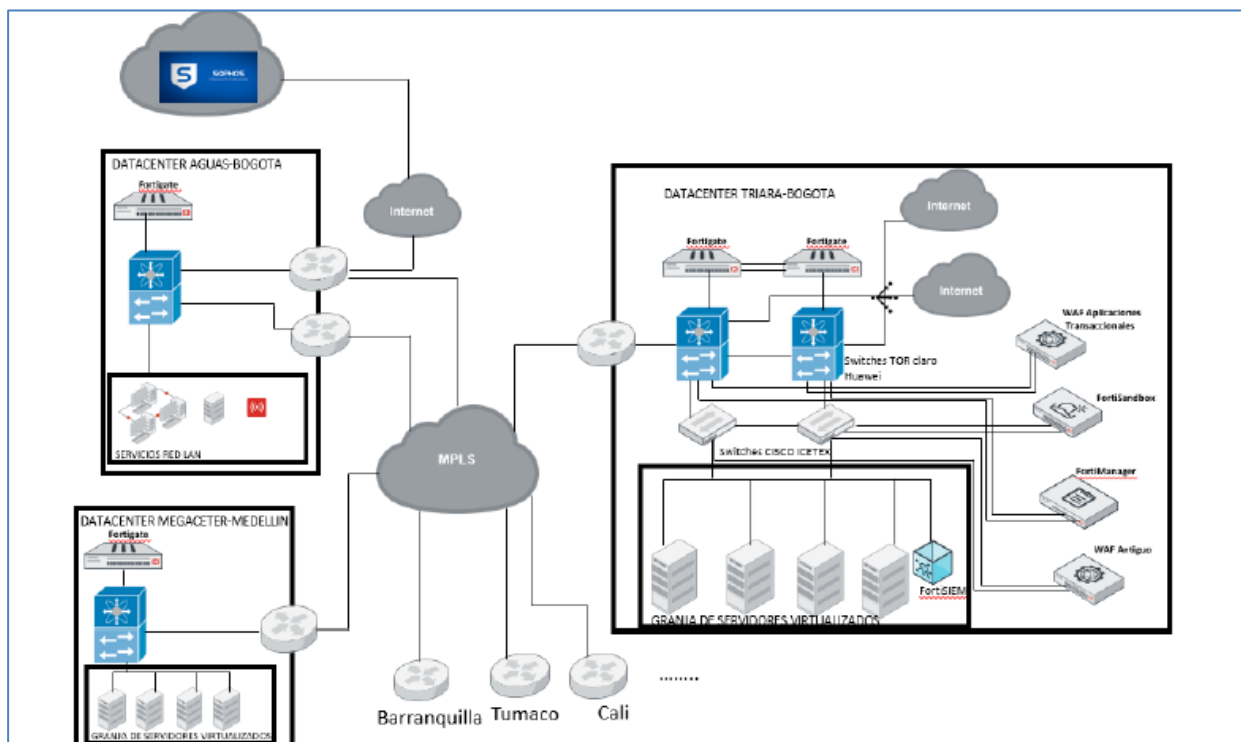


Ilustración 11 Diagrama de la Arquitectura de Seguridad

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

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

En la ilustración 12, se observa la implementación del WAF Cloud donde se utilizaron dos aplicaciones web para el DRP los cuales tienen como dominios: webdrp.icetex.gov.co y drp.icetex.gov.co.

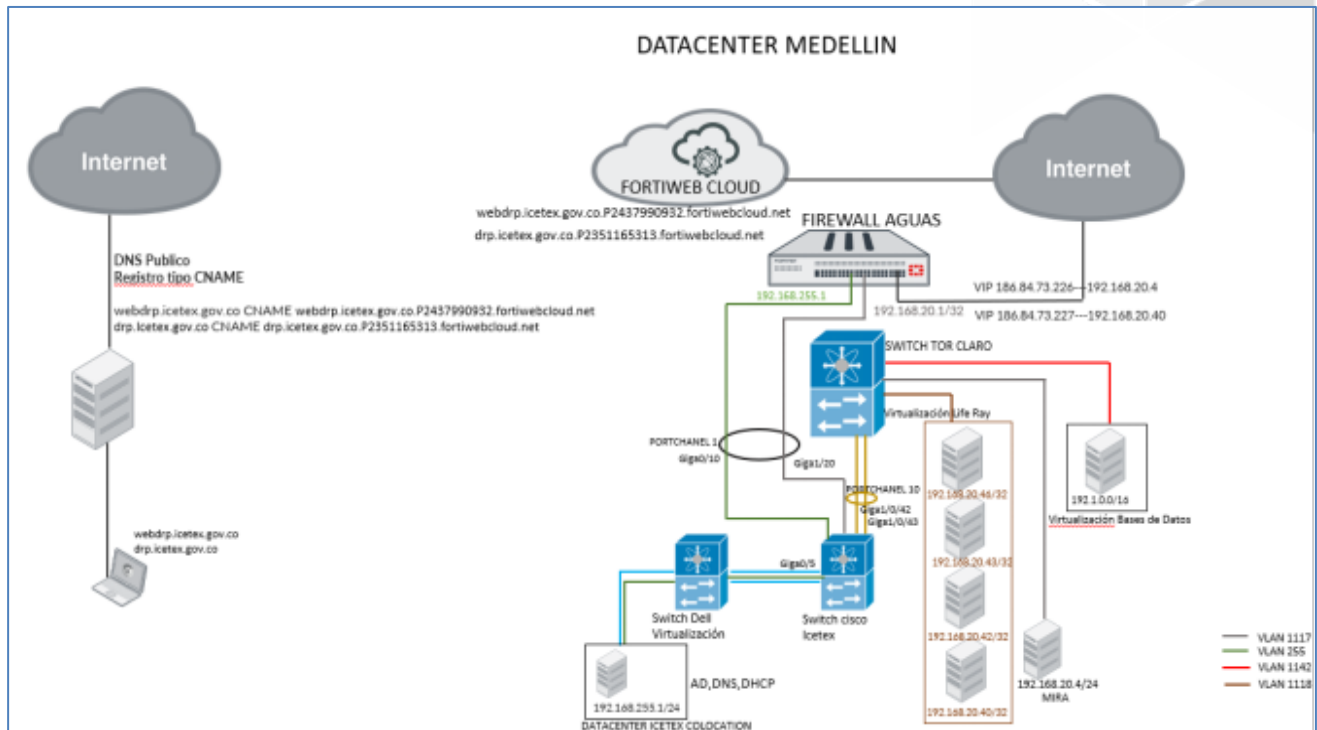


Ilustración 12 Topología de WAF Cloud usado en portales de Medellín

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 Infotíc.

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

Se realizó 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 noviembre, link: [Informe Mensual InfoTIC Seguridad noviembre2025.pdf](#)

Durante el mes de noviembre de 2025 se realizaron las actividades relacionadas con la administración y gestión de la seguridad perimetral:

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

Durante el mes de Noviembre de 2025, se llevaron a cabo diversas actividades relacionadas con la administración y gestión de la seguridad perimetral de la entidad.

Se atendieron y resolvieron múltiples eventos de seguridad, dentro de los cuales se incluyeron intentos de acceso no autorizado a los servicios institucionales, detectados por el SOC. A través de FortiSIEM se identificaron diversas direcciones IP maliciosas que intentaron establecer conexiones hacia los servicios web desde diferentes puertos.

Renovación de los certificados en el waf.

Ajuste permisos bases de datos producción.

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 apoyó en los inconvenientes presentados en la caída del portal web.icetex.gov.co.

Se realizó prueba de Drp el día 29 de noviembre.

- **Monitoreo de seguridad y respuesta ante incidentes**

- **Detección Oportuna de Amenazas**

Se identificaron múltiples eventos de seguridad como intentos de acceso no autorizado a través de VPNs desde el extranjero, tráfico hacia indicadores de compromiso (IoC) y ataques de denegación de servicio (DoS). La oportuna intervención del equipo permitió contener las amenazas, minimizar el riesgo y ajustar las configuraciones para prevenir eventos futuros.

- **Ajustes y Afinamientos en Políticas de Seguridad**

Se realizaron labores de depuración y optimización en las reglas de firewall, eliminando políticas obsoletas, duplicadas o sin tráfico, especialmente en el firewall de Aguas, mejorando la eficiencia y mantenibilidad de las reglas. También se fortalecieron las configuraciones IPv6.

- **Plataformas Actualizadas y con Buen Rendimiento**

Los dispositivos FortiGate, FortiWeb y FortiSandbox se encuentran operativos con versiones estables de firmware y dentro de los parámetros normales de rendimiento (uso de CPU, memoria y sesiones). No obstante, se detectaron dispositivos con licenciamiento vencido o en etapa de fin de vida útil, como el FortiWeb 2000E y el FortiSandbox 1000D, lo cual requiere acciones próximas.

- **Cobertura y Contención con Sophos Endpoint**

Se bloquearon múltiples amenazas, en su mayoría variantes de malware HTML y troyanos, desde diversas fuentes, especialmente del dominio “crearfuturo.co” y sitios externos maliciosos. A pesar de la buena cobertura, se identificaron equipos sin conexión al sistema de protección durante más de 9 meses, recomendándose su revisión y eventual retiro.

- **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 brindó acompañamiento a diversas áreas de la organización en la atención de requerimientos específicos, incluyendo publicaciones en IPv6, configuración de certificados, bloqueos por parte del waf otros.

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

SERIAL	MODELO	UBICACIÓN FÍSICA	OBSERVACIONES
FAC1KD3A17000020	FortiAuthenticat or 1000D	Data Center Triara	Funciona para autenticación y CA de certificados - Propiedad de Icetex
FAC1KD3A17000036	FortiAuthenticat or 1000D	Data Center Triara	Propiedad de Icetex

Tabla 14 Detalle plataformas Seguridad administradas INFOTIC

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

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

Tabla 15 Licenciamiento FortiGate

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; se adelantó la actualización a la versión de FortiOS 7.4.9.

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

A continuación se presentan los consumos en el presente mes:

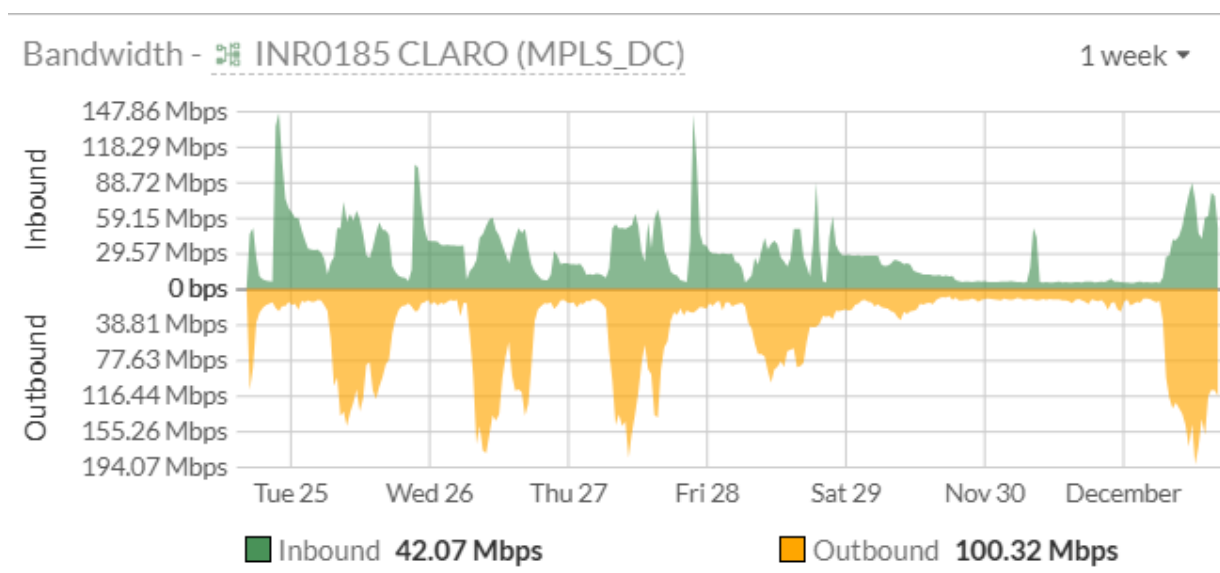


Ilustración 13 Consumo canal MPLS - promedio 1200G [INR0185 CLARO(MPLS_DC)]

Bandwidth - INR0264 (INTE_SEDES ICTX)

1 week ▾

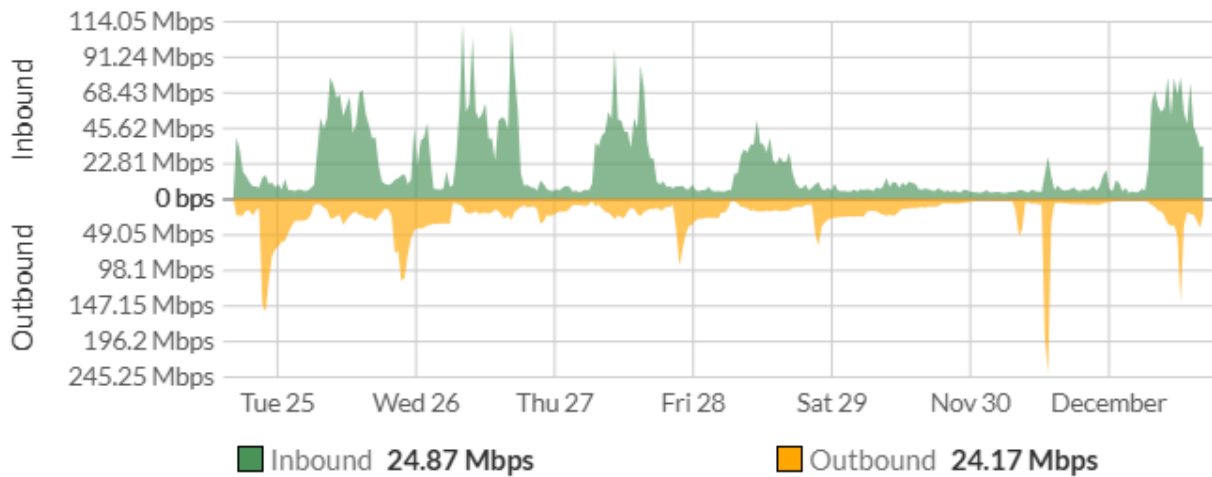


Ilustración 14 Consumo canal Internet Sedes - Promedio 1100 GB WAN-SEDES-ICETEX [INR0264 (INTE_SEDES ICTX)]

Bandwidth - INTERNET_DC_INR0000320 (Inet_claro)

1 week ▾

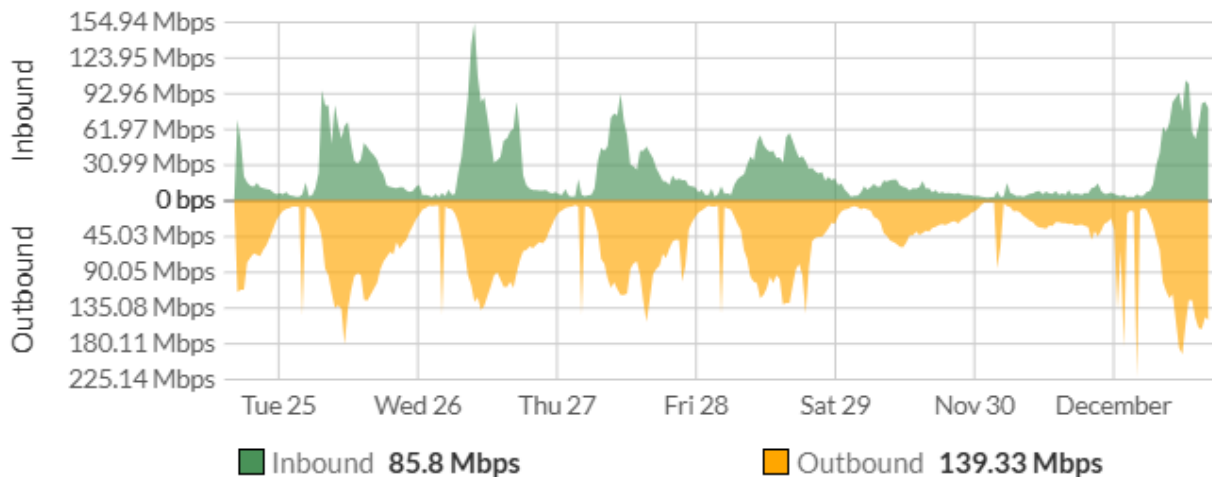


Ilustración 15 Consumo Canal Internet Data Center- INTERNET DATACENTER [INTERNET_DC_INR0000320 (Inet_claro)]

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:

	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 específicas por auditoría.	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 16 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 17 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 18 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; Para el presente mes, se efectuó la actualización a la versión de FortiOS 7.4.8.

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

A continuación se presentan los consumos en el presente mes:

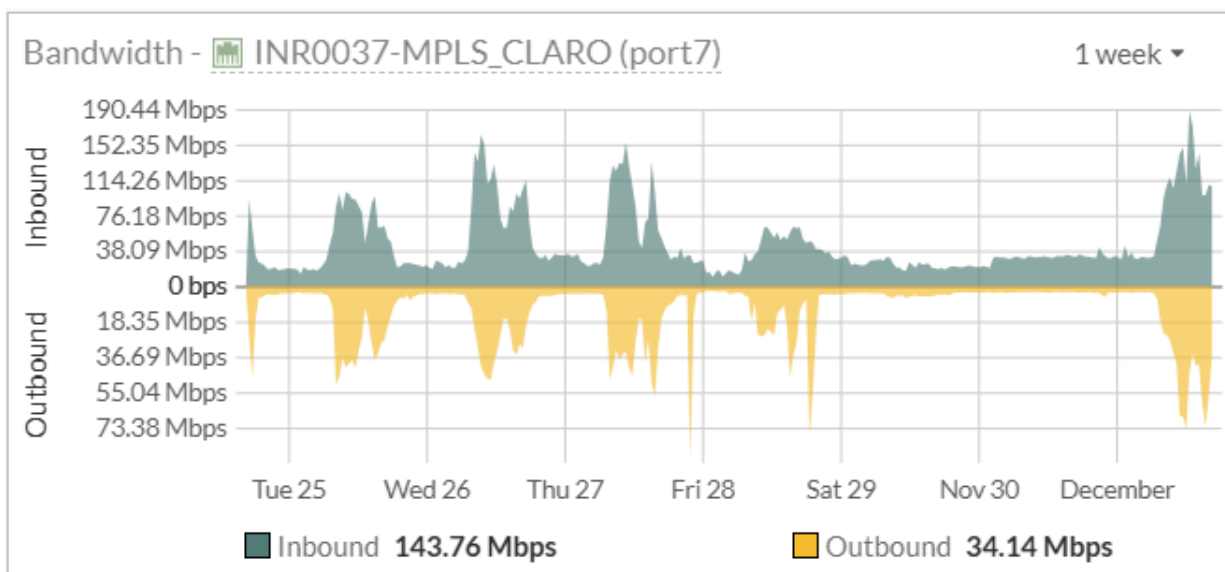


Ilustración 19 Consumo Canal MPLS Aguas - promedio 800 GB

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

	Name	Comments	Ref.
WEB	default	Default web filtering.	0
WEB	General_Icetex		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 20 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 21 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 22 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 7.4.8.

Se observa en la Ilustración 24, que la interfaz de la MPLS del Data Center de Medellín no presenta tráfico debido a que este se tiene como Data Center Alterno.

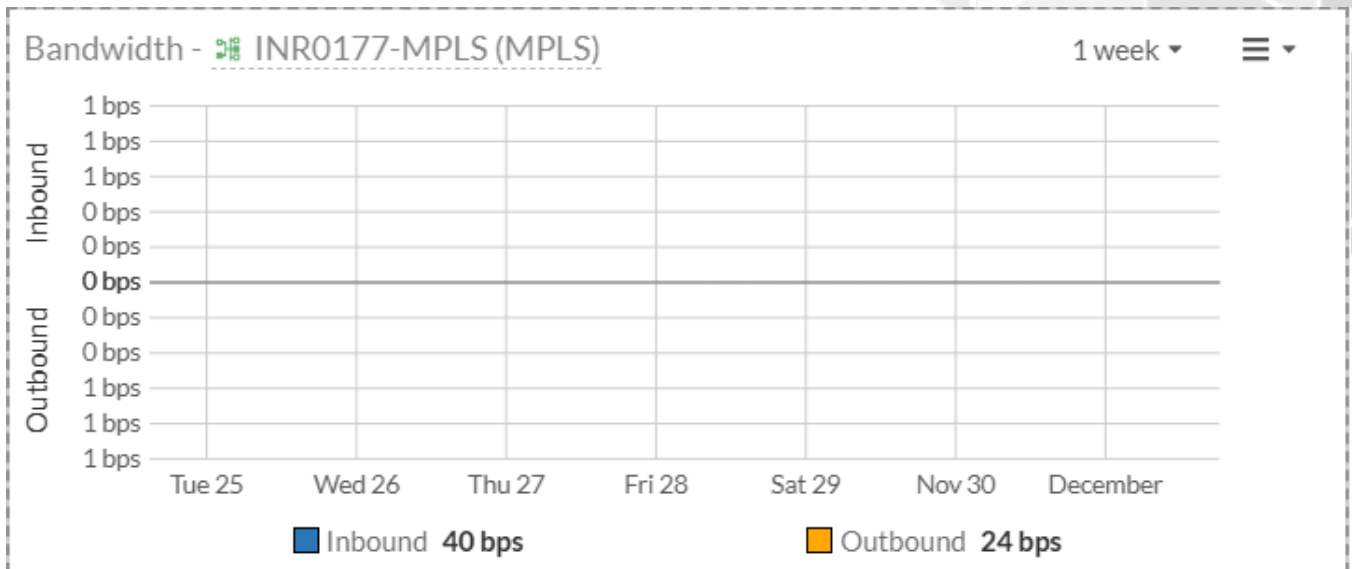


Ilustración 23 Consumo Canal MPLS Medellín

4.3.1.4. FortiWeb 2000F

A nivel de sistema del FortiWeb su versión de firmware está en la 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 que actualmente se encuentra en la 7.6.4 Sin embargo, cabe aclarar que, a nivel de licenciamiento, los equipos no tienen un licenciamiento vigente en este momento.

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

Tabla 16 Licenciamiento FortiWeb

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

2.2.Top Hosts per Response Bytes

#	HTTP Host	HTTP Request Bytes	HTTP Response Bytes
1	web.icetex.gov.co	509.91 GB	7.49 TB
2	www.icetex.gov.co	34.61 GB	1.75 TB
3	aplicaciones.icetex.gov.co	85.92 GB	626.20 GB
4	appwebsites.icetex.gov.co	549.93 MB	184.50 GB
5	comunidad.icetex.gov.co	604.64 MB	34.81 GB
6	web.icetex.gov.co:443	4.53 MB	225.98 MB
7	webhook.icetex.gov.co	631.43 MB	129.77 MB
8	186.84.73.174	436.04 KB	82.78 MB
9	186.84.73.163	361.92 KB	69.24 MB
10	186.84.73.155	350.33 KB	65.69 MB

Ilustración 24 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.

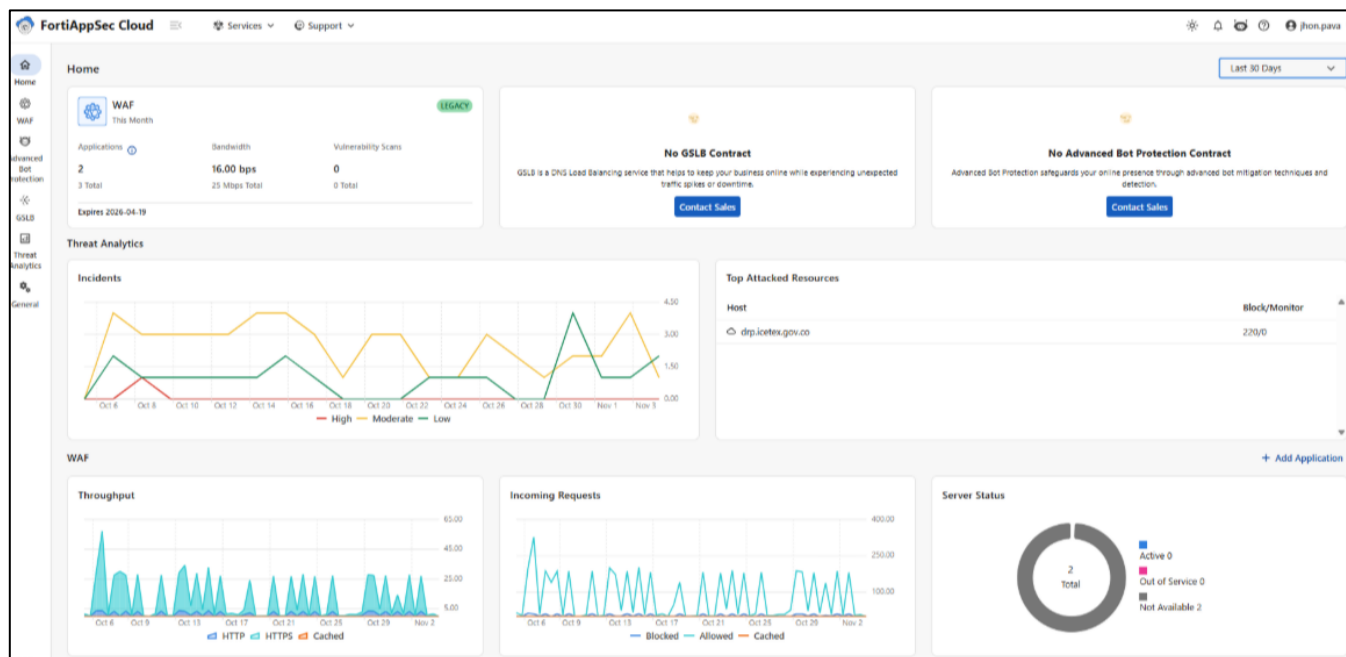


Ilustración 25 Tráfico General de los portales

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 este dispositivo, ya

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

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

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

Tabla 17 Configuración FortiSandBox 1000D

4.3.1.8. FortiSIEM

Debido a problemas de rendimiento en la plataforma FortiSIEM ocasionados principalmente por la falta de recursos de hardware, en particular de CPU, la cual se ha mantenido con un uso sostenido del 100% por más de 7 días y que ha sido reportada en reiteradas ocasiones por el SOC , se presentan inconvenientes para consultar información sobre este dispositivo. Se reitera la necesidad de renovar el soporte y las capacidades de este dispositivo, aspectos que se encuentran a cargo del ICETEX.

Resultado de esta situación, no ha sido posible realizar las siguientes acciones esenciales para el funcionamiento del SOC:

- Generación del informe mensual: No es posible generar el informe de manera completa debido a los errores continuos en la plataforma, lo que impide procesar adecuadamente la información necesaria para su elaboración.
- Monitoreo diario de eventos: La incapacidad para procesar los eventos en tiempo real afecta la visibilidad de las alertas y eventos críticos, limitando la capacidad de monitoreo y respuesta oportuna.

Es importante señalar que esta situación está afectando gravemente la calidad y disponibilidad del servicio de monitoreo.

A continuación, se presenta el desempeño por procesos:

Cloud Health Collector Health Agent Health Replication Health

Process health for FORTISIM_ICTX (192.1.1.100)

Columns Search... Summary Mode

Process Name	Owner	Status	Uptime	CPU	Memory	Resident Memory	Disk Read Rate	Disk Write Rate	SharedStore Type
AppSvr	admin	Up	77d 11h	19%	14%	4.34 GB	OKBps	OKBps	
phParser	admin	Up	73d 4h	11%	6.30%	1.95 GB	OKBps	OKBps	writer
phPerfMonitor	admin	Up	73d 4h	11%	2.80%	890 MB	OKBps	OKBps	
phReportWorker	admin	Up	73d 4h	5%	2.30%	745 MB	OKBps	OKBps	reader
phDataManager	admin	Up	73d 4h	2%	11.90%	3.71 GB	OKBps	OKBps	reader
phQueryMaster	admin	Up	73d 4h	0%	0.90%	277 MB	OKBps	OKBps	
phRuleMaster	admin	Up	12d 7h	0%	7.60%	2.37 GB	OKBps	OKBps	
phRuleWorker	admin	Up	73d 4h	0%	3.80%	1.19 GB	OKBps	OKBps	reader
phQueryWorker	admin	Up	73d 4h	0%	2.40%	761 MB	OKBps	OKBps	reader
phDiscover	admin	Up	73d 4h	0%	0.10%	26 MB	OKBps	OKBps	
phReportMaster	admin	Up	73d 4h	0%	0.40%	118 MB	OKBps	OKBps	
phIdentityWorker	admin	Up	73d 4h	0%	1.90%	605 MB	OKBps	OKBps	reader
phIdentityMaster	admin	Up	73d 4h	0%	0.10%	29 MB	OKBps	OKBps	
phAgentManager	admin	Up	73d 4h	0%	0.20%	66 MB	OKBps	OKBps	
phDataPurger	admin	Up	73d 4h	0%	0.20%	60 MB	OKBps	OKBps	
phEventForwarder	admin	Up	73d 4h	0%	0.10%	21 MB	OKBps	OKBps	
phMonitor	admin	Up	77d 11h	0%	0.40%	118 MB	OKBps	OKBps	

Ilustración 26 Desempeño por procesos

4.3.1.9. Sophos EndPoint

En la ilustración 27, se observa un resumen del estado de Seguridad del Endpoint donde actualmente se están cumpliendo en un 100% los puntos de seguridad de la plataforma de Sophos indicando protección de equipos, políticas y exclusiones.



Ilustración 27 Estado Seguridad Sophos

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

Los cuatro equipos de la ilustración 41, que se encuentran no protegido son: BOGARRIENDO88, BOGIMAC01, BOGVFAPC502, COWORKING11 y llevan más de 9 meses en algunos casos de no conectarse, recomendamos que la mesa de servicio revise los equipos.

En la sección 6.6.1 del informe de seguridad [Informe Mensual InfoTIC Seguridad noviembre2025.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 usuarios y claves dentro de las aplicaciones de ICETEX.	En evaluación por parte de ICETEX.	Alta	N/A	N/A	N/A
Adquirir un equipo Firewall para correo para prevenir brechas de seguridad asociadas al uso del correo electrónico y que este es susceptible a muchos tipos de amenazas.	En evaluación por parte de ICETEX.	Alta	Informes Mensuales - sesiones	Reunión de pares de seguridad	Grupo Coordinación de Infraestructura Tecnológica / Grupo Coordinación de Infraestructura Tecnológica
Validar a nivel de punto final, los equipos que se han visto involucrados con comportamiento malicioso.	Se evalúa por parte de ICETEX. Se hace seguimiento por parte del SOC quien reporta comportamiento malicioso. Sin embargo, es necesario establecer	Critica	Informes Mensuales	N/A	N/A

Recomendación	Estado	Criticidad	Fuente	Asunto	Personal de ICETEX a quien se notificó
	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.				
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 de 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 de Coordinación de Infraestructura Tecnológica / Profesional de tecnología

Tabla 18 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 2.989 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 noviembre 2025.pdf](#)

Para **THREAT HUNTING** específicamente son tres componentes: **Casos de Uso Seguridad, Indicadores de Compromiso y Tableros de control (20)**

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

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

otros CSIRT, e Inteligencia y Caza Amenazas.

Indicadores de compromiso (IOC)	Noviembre	Septiembre	Agosto
IOC – Malware DOMINIOS	6.047	6.047	6.047
IOC – Malware IPs	11.119	11.121	11.189
IOC – Malware HASH	1.627	1.627	1.627
IOC – Malware URL	4.564	4.564	4.564

Tabla 19 Comparativo – Indicadores de Compromiso

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

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

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

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

4.3.3.1. Alertas o Incidentes de Seguridad Detectados

En el documento [Informe Mensual SOC-TH ICETEX noviembre 2025.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.

4.3.3.1.1. Categoría Seguridad

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



Ilustración 28 Total de alertas de seguridad

Durante el período evaluado de 178.911 alertas de seguridad identificadas, se presentaron con criticidad ALTA un total de 1.862 equivalentes al 1,01% 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 5 meses, se presenta a continuación:

Severidad	Alertas de Seguridad Noviembre	Alertas de Seguridad Octubre	Alertas de Seguridad Septiembre	Alertas de Seguridad Agosto	Alertas de Seguridad Julio	Alertas de Seguridad junio
High	1.862	2.599	4.450	3.949	1.536	825
Medium	178.911	250.034	312.033	199.433	9.711	12.459
Low	1.076	2.556	3.310	2.224	193	174

Tabla 20 comparativo Alertas de Seguridad

Durante el período evaluado se presentaron 1.862 alertas de seguridad con criticidad MEDIA, un disminuyó con relación a periodos anteriores. En el documento [Informe Mensual SOC-TH ICETEX noviembre 2025.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 4 se presenta a continuación:

Chart	Criticidad	Event Name	Criticidad	Tactica	Cantidad de Alertas
☒	High	Concurrent Failed Authentications To Same Account From Multiple Countries	9	Credential Access	1,269
☒	High	Critical large Outbound Transfer To Outside My Country ICETEX - WX N3	9		231
☒	High	Brute Force Host Login Success CUSTOM 8/10/2021	9		101
☒	High	Repeated Multiple Logon Failures: Server	9	Credential Access	52
☒	High	Denegacion de Servicios desde Internet - WX Nivel3	9	Impact	32

Ilustración 29 Top 5 de Alertas de Seguridad Altas

Durante el período evaluado se presentaron 178.911 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	Event Name	Criticidad	Criticidad	Tactica	Cantidad de Alertas
☒	Alerta Domain Controller Hora Oficina	Medium	8		2,001
☒	Large Inbound Transfer From Outside My Country	Medium	8	Command And Control	1,799
☒	Large Outbound Transfer To Outside My Country ICETEX	Medium	8		892
☒	Large Outbound Transfer	Medium	8	Exfiltration	680
☒	Account Locked: Server	Medium	8	Credential Access	344

Ilustración 30 Top 5 de Alertas de Seguridad Medias

4.3.3.1.2. Categoría Disponibilidad

Durante el período evaluado se presentaron 355 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	Event Name	Criticidad	Criticidad	Tactica	Cantidad de Alertas
☒	Network Device Down: no ping response - WX N3	High	10	Impact	112
☒	Server Down: No Ping Response ICETEX	High	10		8
☒	FortiSIEM EventDB event store failed	High	10		7
☒	WMI or OMI Service Unavailable	High	9	Impact	117
☒	SNMP Service Unavailable	High	9	Impact	43
☐	Network Device Hardware Critical	High	9		16
☐	EventDB: Event Retention Policy Violation	High	9		12
☐	Excessive Clock Skew Between Collector and Supervisor nodes	High	9		8
☐	FortiSIEM Agent Operational Error WXN2	High	9		6
☐	System Collector is down	High	9		6
☐	No logs from a device in 8 hours - WX N3	High	9		5
☐	Scheduled Report Send Error	High	9		5
☐	FortiSIEM EPS License Exceeded	High	9		4
☐	Windows Cluster Service Startup Error	High	9		4
☐	Windows Cluster Service Quorum Error	High	9		2

Gráfica: Línea de tiempo y top de alertas de disponibilidad criticidad alta
 Ilustración 31 Top 10 de Alertas de Disponibilidad Altas

A continuación, se presentan los análisis efectuados:

- “FortiSIEM EventDB Event store failed” – Esta alerta se genera cuando se detecta que el módulo DataManager no puede crear un directorio en NFS para escribir archivos de eventos, incluso después de varios reintentos. Se perderán los datos. Es decir que el sistema intentó guardar eventos en el almacenamiento de red (NFS), pero no tiene permisos, espacio o conectividad para hacerlo. Como no pudo crear la carpeta necesaria, los eventos que deberían guardarse ahí no se van a conservar.
- “WMI or OMI Service Unavailable” – Esta alerta se genera cuando Detecta que el servicio WMI u OMI no está disponible. Nota: Se recomienda verificar el estado de los protocolos WMI de los dispositivos relacionados, los cuales se utilizan para enviar eventos de seguridad al SIEM; de lo contrario informar al SOC si el dispositivo se encuentra fuera de servicio con el fin de depurar y actualizar la base de datos del FortiSIEM – CMDB.
- “Excessive Clock Skew Between Collector and Supervisor nodes” – Esta alerta se genera cuando detecta un desfase de reloj de más de 2 minutos entre el colector y el supervisor; esto provocará que las reglas en tiempo real no se activen para los eventos recibidos de ese recopilador.
- “EventDB: Event Retention Policy Violation” – Esta alerta se genera cuando Detecta violaciones de la política de retención de eventos. Esto podría indicar que se están eliminando, modificando o reteniendo logs de manera parcial, incumpliendo las políticas definidas por la entidad.

- “Excessive External Event Dropped By License” – Esta alerta se genera cuando detecta que los eventos se descartan debido a una licencia inadecuada.
- “FortiSIEM EPS License Exceeded” – Esta alerta se genera cuando detecta que se excede la licencia global de EPS incluso con una redistribución elástica de EPS. Los eventos se eliminarán a menos que se actualice la licencia.

4.3.3.1.2. 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.

Reporting Device	Attack Name	Signature Id	Severity	Firewall Action	COUNT(Match...
90 DC_FG_MST_ICETEX	DNS PTR Records Scan	51391	Low	detected	18,137
90 DCAGUAS_FG_MST_ICETEX	DNS PTR Records Scan	51391	Low	detected	38

Ilustración 32 ataques IPS permitidos

Reporting Device	Attack Name	Signature Id	Severity	Firewall Action	COUNT
90 DC_FG_MST_ICETEX	Nmap Script Scanner	45360	Medium	dropped	1,142
90 DC_FG_MST_ICETEX	ZGrab Scanner	48805	Medium	dropped	577
90 DC_FG_MST_ICETEX	PHPUnit Eval stdio PHP Remote Code ...	45765	Medium	dropped	317
90 DCAGUAS_FG_MST_ICETEX	TCP Split Handshake	26339	Medium	dropped	306
90 DC_FG_MST_ICETEX	HTTP URI SQL Injection	15621	Medium	dropped	209
90 DC_FG_MST_ICETEX	Censys.io Scanner	50899	Medium	dropped	195
90 DC_FG_MST_ICETEX	ALFA TEaM Web Shell	53229	Medium	dropped	102
90 DC_FG_MST_ICETEX	Spring Boot Actuator Unauthorized Ac...	49620	Medium	dropped	99
90 DC_FG_MST_ICETEX	Kubernetes Ingress NGINX Controller ...	57679	Medium	dropped	94
90 DC_FG_MST_ICETEX	Telerik Web UI RadAsyncUpload Handl...	48789	Medium	dropped	88
90 DC_FG_MST_ICETEX	MS.IIS.ShortName Vulnerability Scanner	47145	Medium	dropped	86
90 DC_FG_MST_ICETEX	Apache HTTP Server cgi-bin Path Trav...	50825	Medium	dropped	85
90 DC_FG_MST_ICETEX	Apache Log4j Error Log Remote Code ...	51006	Medium	dropped	77
90 DC_FG_MST_ICETEX	WordPress REST API Username Enumer...	48072	Medium	dropped	72
90 DCAGUAS_FG_MST_ICETEX	HTTP Headers End With LF CR CRLF	43399	Medium	dropped	56

Ilustración 33 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).

Source IP	Destination IP	IP Protocol	Destination TCP/UDP Port	COUNT(Matched Events)	SUM(Sent Bytes64)	SUM(Received Bytes64)	SUM(Total Bytes64)
2801:192:2:18::10:65	2801:192:2:51::65	17 (UDP)	53 (DOMAIN)	794,034	18.55 GB	23.9 GB	42.46 GB
190.60.81.39	192.168.91.18	6 (TCP)	443 (HTTPS)	38,468	30.46 MB	89.53 MB	120 MB
190.60.81.39	192.168.91.15	6 (TCP)	443 (HTTPS)	27,824	1.49 GB	20.84 GB	22.34 GB
2801:192:6:e6:d543:8d94:bddf:c9db	2603:1030:40c:e::	6 (TCP)	443 (HTTPS)	19,995	36.49 MB	57.51 MB	94 MB
2801:192:6:e6:d543:8d94:bddf:c9db	2603:1030:40c:e::2	6 (TCP)	443 (HTTPS)	18,758	34.24 MB	53.98 MB	88.23 MB
2801:192:6:e2:b530:1362:8747:cdef	2620:149:a41:580::2:b	6 (TCP)	443 (HTTPS)	18,463	0B	0B	0B
66.102.8.171	192.168.91.17	6 (TCP)	443 (HTTPS)	18,031	678.74 MB	15.77 GB	16.44 GB
2801:192:6:e2:b530:1362:8747:cdef	2620:149:a41:580::2:4	6 (TCP)	443 (HTTPS)	17,889	0B	0B	0B
66.102.8.170	192.168.91.17	6 (TCP)	443 (HTTPS)	17,872	700.02 MB	15.77 GB	16.45 GB
66.102.8.172	192.168.91.17	6 (TCP)	443 (HTTPS)	17,737	636.56 MB	14.93 GB	15.15 GB
2801:192:6:e2:b530:1362:8747:cdef	2620:149:a41:580::2:9	6 (TCP)	443 (HTTPS)	17,361	0B	0B	0B
2801:192:2:18::16	2801:192:2:51::65	17 (UDP)	53 (DOMAIN)	16,729	1.38 MB	2.5 MB	3.89 MB
190.157.218.113	192.168.91.15	6 (TCP)	443 (HTTPS)	16,155	1.3 GB	14.22 GB	15.52 GB
66.249.72.33	192.168.91.15	6 (TCP)	443 (HTTPS)	15,009	8.85 GB	88.66 GB	97.51 GB
66.249.72.34	192.168.91.15	6 (TCP)	443 (HTTPS)	14,991	8.51 GB	85.68 GB	94.2 GB
66.249.72.35	192.168.91.15	6 (TCP)	443 (HTTPS)	14,378	7.55 GB	75.48 GB	83.04 GB
2801:192:6:e6:d543:8d94:bddf:c9db	2603:1030:40c:e::1	6 (TCP)	443 (HTTPS)	14,373	26.3 MB	41.42 MB	67.73 MB
2801:192:6:e2:b530:1362:8747:cdef	2620:149:a41:580::2:2	6 (TCP)	443 (HTTPS)	14,316	0B	0B	0B
2800:484:4271:e800:792f:1006:cccc:435c	2801:192:d:13::123	6 (TCP)	443 (HTTPS)	14,192	523.35 GB	275.69 GB	799.05 GB
2801:192:6:e2:b530:1362:8747:cdef	2620:149:a41:580::2:7	6 (TCP)	443 (HTTPS)	13,411	0B	0B	0B
66.249.72.36	192.168.91.15	6 (TCP)	443 (HTTPS)	13,075	6.31 GB	60.87 GB	67.19 GB
2801:192:6:e2:d57a:32a1:a279:d4b	2620:149:a41:580::2:2	6 (TCP)	443 (HTTPS)	12,581	0B	0B	0B
2801:192:6:e2:b530:1362:8747:cdef	2620:149:a41:580::2:8	6 (TCP)	443 (HTTPS)	12,282	0B	0B	0B

Ilustración 34 Puertos entrantes de público a privado (Permitidos)

Se recomienda verificar si es necesario mantener expuestos a internet de los siguientes puertos conocidos como el 53 (DOMAIN), 123 (NTP) los cual comúnmente son autorizados como puertos de salida y no de entrada, así mismo confirmar otros puertos conocidos como el 440 (SGCP), 458 (APPLEQTC), 547 (DHCP), 389 (LDAP) los cuales en su mayoría son utilizados en entornos LAN o privados.

Puertos salientes de público a privado (Permitidos): Debido a las limitantes de recursos de la herramienta FortiSIEM no se puede realizar la extracción de información de este componente.

Failed Windows Login

Last

Source IP	User	Server	COUNT
90 192.168.20.29	51 gestiondoc	90 ICTXSRVAD001.icet...	2,940
90 192.168.20.29	rfgutierrez	90 ICTXSRVAD001.icet...	996
77 172.16.224.24	70 asotoc	90 ictxsrvfs.icetex.loc...	804
10.2.254.8	66 jpforero	90 ictxsrvfs.icetex.loc...	576
70 10.2.254.2	66 jpforero	90 ictxsrvfs.icetex.loc...	573
70 10.2.254.4	66 jpforero	90 ictxsrvfs.icetex.loc...	568
70 10.10.101.8	66 USER	90 ictxsrvfs.icetex.loc...	492
70 10.2.254.4	90 wrozo	90 ictxsrvfs.icetex.loc...	435
10.2.254.123	39 jcperez	90 ictxsrvfs.icetex.loc...	406
89 10.200.176.33	81 Administrador	90 ICTXSRVAD000.icet...	353
89 10.200.176.33	81 Administrador	90 ICTXSRVAD001.icet...	342
10.2.254.216	39 jalberson	90 ictxsrvfs.icetex.loc...	310
58 10.2.254.6	66 jpforero	90 ictxsrvfs.icetex.loc...	244
59 192.168.61.1	aleimbachi	90 MIRA	244
172.16.224.114	66 jpforero	90 ictxsrvfs.icetex.loc...	171

Ilustración 35 Top de Accesos Fallidos plataforma Windows

Server	User	COUNT(
90 ICTXSRVAD001.icetex.local	90 larrieta	986
90 ICTXSRVAD001.icetex.local	90 mmedina	743
90 ICTXSRVAD001.icetex.local	90 dileshe	404
90 ICTXSRVAD001.icetex.local	90 mmedinamon	348
90 ICTXSRVAD001.icetex.local	90 jbarrera	270
90 ICTXSRVAD001.icetex.local	90 mriascos	252
90 ICTXSRVAD001.icetex.local	90 22823906	248
90 ICTXSRVAD001.icetex.local	79 mcruz	229
90 ICTXSRVAD000.icetex.local	90 mmedina	178
90 ICTXSRVAD000.icetex.local	90 larrieta	143
90 ICTXSRVAD001.icetex.local	90 Administrator	128
90 ICTXSRVAD001.icetex.local	61 Idiaza	120
90 ICTXSRVAD003.icetex.local	90 larrieta	120
90 ICTXSRVAD001.icetex.local	85 jvillalbam	82
90 ICTXSRVAD003.icetex.local	90 mmedinamon	65

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.

4.3.3.1.4. 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 noviembre 2025.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 documento [Informe Mensual SOC-TH ICETEX noviembre 2025.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.

Todo el tráfico fue bloqueado, sin embargo, se recomienda la verificación de los equipos con las direcciones IP origen privada. A continuación, Información de la amenaza o reportes negativos en plataformas de CTI.

4.3.3.1.4. ANALISIS MARCA OSINT

Durante el periodo evaluado, la plataforma de monitoreo de protección de marca y OSINT – AXUR, reporta un total de 1,7k posibles amenazas de las 63,8k que fueron encontradas y analizadas automáticamente por la plataforma de monitoreo. A estas 1,7k posibles amenazas se les realizó una revisión y análisis interno, de sus características, datos e información.

Durante el periodo evaluado se detectó 18 incidentes de los cuales 13 están relacionados con Otros datos confidenciales y 05 con Perfil falso en red social.



Ilustración 37 Incidentes por Tipo de Amenaza

En cuanto a casos relacionados a Fraudes digitales y fuga de información, estos se encuentran detallados en el anexo Informe Mensual MARCA-OSINT ICETEX Noviembre 2025.PDF.

4.3.4. Análisis de Vulnerabilidades ICETEX

Durante noviembre de 2025 se ejecutó satisfactoriamente el análisis de vulnerabilidades correspondiente a la Fase 8 del plan de trabajo. En esta etapa se evaluaron 77 activos: 76 equipos de usuario final (en línea con la planificación mensual) y 1 equipos adicional atendidos por requerimiento para verificación de remediación de vulnerabilidades. 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 — noviembre) el enfoque operó por segmentos mensuales, con un diseño que estima una cobertura parcial cercana al 50 % del parque en cada bloque mensual.

El balance de toda esta fase se resume a continuación:

- Mayo: Se ejecutaron pruebas sobre 76 servidores.
- Junio: Se evaluaron 65 servidores adicionales y 11 dispositivos de red (switches).
- Julio: Se evaluaron 23 dispositivos de red (switches), 8 dispositivos de seguridad perimetral, 43 aplicaciones o portales web internos y 2 bases de datos Oracle.
- Agosto: Se evaluaron 28 bases de datos y 48 equipos de usuario final
- Septiembre: 76 equipos de usuario final y 3 servidores (requerimiento adicional).
- Noviembre. 76 equipos de usuario final y re-test de 3 servidores (requerimiento adicional para verificación de remediación de vulnerabilidades).

Entre los hallazgos más relevantes se encuentran:

Para el equipo identificado con la IP 192.168.20.57 (Clon de MIRA), el estado de remediación de vulnerabilidades fue el siguiente:

Severidad	Vulnerabilidad	Dispositivos afectados	Estado de remediación
Medium	Strict-Transport-Security Header Not Set	192.168.20.57	Sin remediar
Medium	Conjuntos de cifrado SSL de intensidad media compatibles (SWEET32)	192.168.20.57	Remediada
Medium	Conjuntos de cifrado SSL RC4 compatibles (Bar Mitzvah)	192.168.20.57	Remediada
Medium	Detección del protocolo SSL versión SSLv2 y SSLv3	192.168.20.57	Remediada
Medium	TLS Version 1.1 Deprecated Protocol	192.168.20.57	Remediada
Medium	Conjuntos de cifrado SSL débiles		Remediada
Low	X-Content-Type-Options Header Missing	192.168.20.57	Sin remediar

Ilustración 38 Estado de Remediación amenazas-Clon Servidor Mira

conclusión: las actividades de remediación sobre el servidor disminuyeron el grado de explotación de vulnerabilidades que hubieren derivado en un compromiso del servidor; siendo la intervención oportuna y el parcheo/migración completada para las vulnerabilidades detectada en la fortaleza de cifrados SSL, TLS y conjunto de cifrados débiles.

Durante el análisis no se identificaron vulnerabilidades críticas; sin embargo, se reportaron hallazgos de severidad media y baja, principalmente asociados a configuraciones criptográficas inseguras, tales como:

Configuraciones criptográficas Inseguras

- **Protocolos inseguros expuestos en servicios críticos**, incluyendo soporte de **TELNET**, **TLS 1.0** y **TLS 1.1**, obsoletos y sin soporte oficial desde 2020.
- **Cifrados de mediana y baja fortaleza habilitados**, entre ellos **SHA1** y **CBC**, lo que expone los servicios a ataques criptográficos conocidos.

Gestión Deficiente de Protocolos y Cifrado

- Soporte de protocolos criptográficos obsoletos y vulnerables, con impacto en la confidencialidad e integridad de la información transmitida en servicios TELNET (TCP/21) y SSH (TCP/22).
- Uso de certificados SSL internos sin validaciones adecuadas, lo que incrementa la superficie de riesgo frente a ataques de intermediario (MITM).

4.3.4.2. Gestión de Vulnerabilidades

El pasado jueves 13 de noviembre, se realizó la primera sesión de gestión de vulnerabilidades. En dicha reunión se evidenció que el ng. Víctor Raúl bautista, asignado para esta actividad. Se determinó, junto con el Ing. Víctor Bautista, que se priorizará la gestión de las vulnerabilidades de corto y mediano plazo en aquellos servidores que actualmente son administrados por los especialistas de ICETEX. Esta decisión se toma debido

a que aún no se cuenta con un inventario actualizado de los dispositivos de la entidad, lo que ha impedido identificar a los responsables de los servidores que presentan vulnerabilidades. Dicho inventario se encuentra en proceso de construcción, y su disponibilidad será fundamental para asignar responsables, coordinar acciones de remediación y mejorar la eficiencia en la gestión de vulnerabilidades.

En sesión del 28 de noviembre la sesión de seguimiento de gestión de vulnerabilidades de ICETEX, en la cual se presentaron los siguientes puntos:

1. Se validaron las vulnerabilidades de los servidores ICTXSRVCRMB1, ICTXSRVCRMB2 y 10.1.18.135 que están relacionados con el CRM que maneja la entidad.
2. Se va a realizar la deshabilitación de los protocolos TLS/SSL inseguro de los servidores, para que estos cambios aplique se debe realizar el reinicio.

Resultado de esta gestión se consolidó, con el reporte del ICETEX, la remediación correspondiente a la vulnerabilidad SWEET32 (CVE-2016-2183) ha sido ejecutada exitosamente en los servidores Windows Server que operan como backend de Dynamics CRM Customer Services On-Premise.

Para efectos de validar la efectividad de las labores ejecutadas, el equipo del SOC, a la fecha del presente informe, se encuentra efectuando un nuevo escaneo sobre dicho servidor.

Nuestro equipo de especialistas gestionó la clonación de la máquina 192.168.20.57 (MIRA) con el fin de efectuar la remediación correspondiente a **WINDOWS SERVER 2008 R2. Las acciones adelantadas fueron:**

1. Des habilitación de protocolos inseguros. Se deshabilitaron los protocolos obsoletos:

- **SSL 2.0**
- **SSL 3.0**

Estos protocolos son vulnerables a ataques como POODLE y ya no se consideran seguros.

✓ Comunicaciones seguras ahora requieren **TLS 1.0/1.1/1.2**

(Dependiendo compatibilidad de aplicaciones internas; idealmente TLS 1.2 habilitado y priorizado)

2. Eliminación de cifrados débiles / vulnerables. Se deshabilitaron cipher suites basados en:

- **RC4** (ataque Bar Mitzvah / RC4 bias)
- **3DES / DES** (vulnerabilidad SWEET32)
- **MD5** (hash criptográfico roto)
- **RC2** y otros cifrados débiles heredados

✓ Solo permanecen cifrados seguros basados en **AES-CBC / AES-GCM**

✓ Intercambio de claves mediante **RSA / DHE / ECDHE** según compatibilidad

3. Configuración manual de Cipher Suite Seguros. Se configuró manualmente la lista de cipher suites permitidos en:

HKLM\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002

dejando únicamente algoritmos fuertes compatibles con Windows Server 2008 R2.

4. Limpieza de valores débiles en SCHANNEL. Se agregaron claves específicas para forzar des habilitación criptográfica:

Triple DES 168/168 = Disabled

DES 56/56 = Disabled

RC2 40/128 = Disabled

RC2 56/128 = Disabled

RC4 128/128 = Disabled

RC4 64/128 = Disabled

RC4 56/128 = Disabled

RC4 40/128 = Disabled

5. Instalación de actualizaciones pendientes. Se instalaron actualizaciones de seguridad acumuladas y de compatibilidad criptográfica necesarias para mitigar vulnerabilidades en TLS y mejorar compatibilidad de cifrados modernos.

Actualizaciones aplicadas:

windows6.1-kb4099950-x64

windows6.1-kb4345459-ia64

windows6.1-kb4345459-x64

windows6.1-kb4517297-x64

windows6.1-kb4539602-x64

Dentro de la gestión de vulnerabilidades realizada durante el mes de noviembre, la efectividad presentó resultados negativos debido al incremento de nuevas vulnerabilidades derivadas de los escaneos programados para este periodo, así como de los hallazgos adicionales proporcionados.

A esto se suma el bajo avance en las actividades de remediación, lo que en conjunto genera un aumento en el volumen total de vulnerabilidades pendientes por gestionar

Las vulnerabilidades gestionadas durante el mes de noviembre están relacionadas principalmente con aspectos de seguridad en certificados digitales. Estas vulnerabilidades suelen indicar configuraciones inseguras, uso de certificados caducados o algoritmos criptográficos débiles, lo que puede comprometer la confidencialidad e integridad de las comunicaciones, facilitar ataques de interceptación (MITM) y afectar la confianza de los servicios expuestos. Por lo tanto, su adecuada revisión y actualización es fundamental para garantizar la protección de los canales cifrados y mantener la robustez del entorno tecnológico.

4.3.5. Actividades de PENTEST

Nuestro equipo de especialistas gestionó la clonación de la máquina 192.168.20.57 (MIRA) con el fin de efectuar la remediación correspondiente a

Durante el presente periodo, de acuerdo con el otro sí No 3 suscrito, se efectuaron los ejercicios con los siguientes resultados:

4.3.5.1. Actividades de PENTEST WEB

El análisis general de hallazgos [Informe Pentesting URLs ICETEX Noviembre.pdf](#) presenta una visión consolidada de las vulnerabilidades identificadas durante el proceso de pruebas de penetración. En esta sección se agrupan los resultados más relevantes, clasificándolos según su nivel de criticidad y el impacto potencial sobre la confidencialidad, integridad y disponibilidad de la información.

Las URL's, evaluadas, fueron:

- <https://aplicaciones.icetex.gov.co/WebSitePortalTransaccional/crearusuario>
- <https://aplicaciones.icetex.gov.co/CuentasInactivasFront/login>
- <https://aplicaciones.icetex.gov.co/CuentasAbandonadas/login>

El escaneo de vulnerabilidades realizada a las URLs detectó un total de 30 vulnerabilidades: 4 de severidad media y 26 de severidad baja. A continuación, se detallan las vulnerabilidades por URLs.

URL	Criticas	Altas	Medias	Baja
WebSitePortalTransaccional/crearusuario	0	0	1	10
CuentasInactivasFront/login	0	0	2	8
CuentasAbandonadas/login	0	0	1	8

Ilustración 39 Resultado Escaneo Vulnerabilidades URL's

El balance de estos hallazgos se resume a continuación:

- Los portales de autenticación no tienen una limitación en los intentos de acceso, lo que permite a un atacante probar un número ilimitado de combinaciones de usuario y contraseña en un corto periodo de tiempo.
- Software y complementos desactualizados.
- En los portales de inicio de sesión se identificó que no están sanitizado correctamente las entradas.
- Ausencia de cabeceras de seguridad.
- Pese a que se cuenta con cookies de sesión, estas no están complementadas con atributos como HttpOnly o Secure.

4.3.5.1. Actividades de PENTEST SERVIDORES

En lo que concierne a ejercicios de PENTEST de servidores se concertaron con el ICETEX, el ataque a los servidores con las siguientes IP's:

192.168.51.161

192.168.51.163

192.168.53.38

192.168.53.39

10.1.18.134

Antes de iniciar el análisis, se llevó a cabo una fase de reconocimiento para mapear la superficie de los servidores, centrándose en la recopilación de información para identificar tecnologías, servicios y posibles vectores de ataque y puertos abiertos.

Destacan patrones comunes en la exposición de riesgos, posibles vectores de ataque recurrentes y áreas de mayor atención dentro de la infraestructura evaluada. Este análisis permite priorizar esfuerzos de mitigación y sirve como base para la toma de decisiones estratégicas en materia de seguridad de la información.

URL	Criticas	Altas	Medias	Baja	Informativa
192.168.51.161	0	1	5	1	35
192.168.51.163	0	1	5	1	35
192.168.53.38	0	0	8	2	40
192.168.53.39	0	0	8	2	41
10.1.18.134	0	1	6	1	36

Ilustración 40 Resultado Escaneo Vulnerabilidades Servidores

Los resultados se presentan a continuación:

- Los servidores evaluados durante el mes de noviembre no presentaron vulnerabilidades críticas, y las vulnerabilidades de severidad alta fueron pocas. La mayor parte de los hallazgos correspondió a vulnerabilidades de severidad media y baja, lo que indica que, aunque no existen riesgos extremos, aún es necesario fortalecer la postura de seguridad para reducir la exposición a amenazas aprovechables.
- Dentro de los servidores evaluados durante el mes de noviembre se evidenció que varios de ellos operan con un sistema operativo obsoleto y, además, tienen habilitado el servicio Microsoft IIS httpd 10.0. Esta combinación incrementa el nivel de riesgo, ya que, aunque IIS 10.0 continúa teniendo soporte cuando se ejecuta sobre sistemas operativos vigentes, al estar instalado sobre plataformas sin soporte, deja de recibir actualizaciones de seguridad y se expone a vulnerabilidades que no pueden ser corregidas mediante parches oficiales.
- Dentro del reconocimiento realizado a los servidores se identificó que cuentan con una nomenclatura adecuada, lo cual facilita su clasificación, la identificación de sus funciones y la detección del rol que desempeña cada uno. Sin embargo, es importante considerar que, si estos servidores se encuentran visibles o expuestos en la red sin los debidos controles de seguridad, esta información puede ser utilizada por un atacante para obtener inteligencia del entorno y orientar posibles acciones maliciosas.

En el anexo [Informe Pentesting Servidores ICETEX Noviembre.pdf](#) se puede consultar con mayor detalle los hallazgos aquí descritos.

4.3.6. Reporte De IPS

Se recomienda realizar una validación de las firmas detectadas durante el escaneo con el fin de determinar su origen, criticidad y posible impacto sobre la infraestructura de red. Adicionalmente, se sugiere implementar y habilitar las políticas del sistema de prevención de intrusiones (IPS) en el firewall, con el objetivo de fortalecer la detección y mitigación de posibles intentos de intrusión. En caso de confirmarse la presencia de firmas asociadas a amenazas conocidas, se aconseja aplicar medidas de bloqueo directamente desde el IPS, considerando que este punto de control se encuentra más cercano a la fuente del tráfico.

Asimismo, se recomienda habilitar la funcionalidad de Deep Inspection mediante el despliegue del certificado correspondiente, lo que permitirá realizar un análisis más profundo del tráfico cifrado y detectar posibles amenazas ocultas en las comunicaciones SSL/TLS. Finalmente, se sugiere mantener un monitoreo continuo del tráfico de red y de las alertas generadas por el IPS/IDS, así como garantizar la actualización permanente de las bases de datos de firmas y de las políticas de seguridad, con el propósito de asegurar la protección frente a vulnerabilidades y amenazas emergentes.

4.3.7. Arquitectura de Seguridad

Durante el presente periodo, se adelantaron varias sesiones con la Oficina de Riesgos del ICETEX, validando los aspectos metodológicos y los instrumentos existentes.

Además, de acuerdo con el plan de trabajo previsto, se efectuó la definición de la arquitectura objetivo (TO BE) tomando como referencia la guía general metodológica emitida por el MINTIC MAE.G.AS - DOMINIO DE

ARQUITECTURA DE SEGURIDAD¹, la cual está basada en SABSA (Sherwood Applied Business Security Architecture). Se trata de un marco de arquitectura de dominio optimizado para la seguridad, que proporciona técnicas y métodos detallados para proteger la información del ICETEX.

En el documento se incluye los planes y proyectos para poder lograr la arquitectura objetivo:

Dominio SABSA	DESCRIPCION	SERVICIOS, MECANISMOS, PRODUCTOS, HERRAMIENTAS.
1. Arquitectura de Seguridad Contextual (Negocio)	Definir la visión estratégica y los objetivos del ICETEX que sirvan de base para la implementación de procedimientos automatizados, soluciones tecnológicas, programas de sensibilización y cultura organizacional, asegurando que la seguridad de la información se mantenga alineada con la gobernanza corporativa, la gestión integral del riesgo y el cumplimiento normativo del sector.	6.1. Alineación de los Objetivos Estratégicos con la Seguridad de la Información 6.2. Necesidades Institucionales Del ICETEX 6.3. Partes Interesadas 6.4. Alcance del Gobierno, Riesgo y Cumplimiento en el ICETEX como entidad financiera y pública 6.5. Requisitos del ICETEX.
2. Arquitectura de Seguridad Conceptual	La arquitectura de seguridad conceptual permite al ICETEX como entidad financiera y pública, aplicar los principios de la seguridad de la información y alinear la gestión estratégica con el control de riesgos y el cumplimiento normativo.	7.1. Principios de Arquitectura de Seguridad de la Información 7.2. Modelo Conceptual del Gobierno, Riesgo y Cumplimiento 7.3. Capacidades de Seguridad (TO-BE) 7.4. Indicadores Clave de Desempeño (KPIs)
3.Arquitectura de Seguridad Lógica	Protección de los activos digitales, el cumplimiento normativo y la confianza institucional en el ICETEX. Su aplicación permite garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de la información que soporta los procesos misionales, operativos y de servicio a los ciudadanos.	8.1. Lineamientos para implementar el modelo de Zero Trust Network Access (ZTNA) 8.2. Protección de Infraestructura Tecnológica 8.3. Lineamientos de Seguridad para componentes de la Infraestructura Tecnológica 8.3.1. Lineamientos de Seguridad para Windows Server 8.3.2. Lineamientos de Seguridad para Sistemas Unix/Linux 8.3.3. Lineamientos de Seguridad para Sistemas IBM AS/400 (IBM) 8.3.4. Lineamientos de Seguridad para Office 365 8.3.5. Lineamientos de Seguridad para Bases de Datos Oracle 8.4. Desarrollo Seguro 8.5. Lineamientos Técnicos para la Protección y Gestión Segura de la Información 8.6. Seguridad en la nube 8.7. Detección y Respuesta 8.8. Continuidad y Resiliencia 8.9. Gestión de Vulnerabilidades / Ethical

¹ https://www.mintic.gov.co/arquitecturaempresarial/630/w3-propertyvalue-385293.html?__noredirect=1

DOMINIO SABSA	DESCRIPCION	SERVICIOS, MECANISMOS, PRODUCTOS, HERRAMIENTAS.
		Hacking
4.Arquitectura de Seguridad Física	Protección integral al salvaguardar las instalaciones, los activos tecnológicos, los documentos y al personal que desarrolla las operaciones institucionales.	9.1. Controles de acceso físico 9.2. Monitoreo y vigilancia 9.3. Protección ambiental y energética 9.4. Protección de equipos y activos 9.5. Continuidad y contingencia
5.Componentes de Arquitectura de Seguridad (Tecnología)	En este dominio se identifican, seleccionan e implementan las herramientas y tecnologías de seguridad que soportan las políticas, procesos y requerimientos establecidos a nivel lógico y conceptual. Garantizando que la infraestructura tecnológica disponga de componentes interoperables, actualizados y alineados con los objetivos de protección del ICETEX, asegurando una cobertura efectiva frente a las amenazas y vulnerabilidades identificadas, obteniendo una gobernanza tecnología y garantizando que cada solución de seguridad contribuya de forma medible a la gestión integral del riesgo.	10.1. Gobernanza, el riesgo y el cumplimiento (GRC) 10.2. Gestión de Identidades y Accesos (IAM) 10.3. Realizar detección y respuesta extendida XDR, agentes XDR en todos los endpoints. 10.4. Gestión de Acceso Privilegiado (PAM), Herramienta de protección, gestión y supervisión del acceso a las cuentas y credenciales privilegiadas 10.5. Secure Access Service Edge (SASE) 10.6. Prevención de Perdida de Información (DLP) 10.7. Mobile Device Management (MDM) 10.8. WAF 10.9. Ciframiento de datos 10.10. Gestión de vulnerabilidades 10.11. NGFW con inspección TLS en perímetro y datacenter. 10.12. Sensores IDS/IPS en red interna crítica. 10.13. Análisis de Código Estático y Dinámico (SAST y DAST) 10.14. SANDBOX 10.15. SIEM

DOMINIO SABSA	DESCRIPCION	SERVICIOS, MECANISMOS, PRODUCTOS, HERRAMIENTAS.
6.Arquitectura de Seguridad Operacional	Dominio encargado de mantener la seguridad activa y sostenible en el tiempo, asegurando que los controles, procesos y tecnologías implementados en los dominios anteriores del modelo SABSA funcionen de manera efectiva, coordinada y alineada con los objetivos de la Organización.	11.1. Security Operations Center (SOC) 11.2. Gestión de cambios: Controlada por CAB-Comité asesor de cambios con revisiones de seguridad. 11.3. Pruebas y auditorías: Pentesting semestral, auditoría interna anual. 11.4. Gestión continua de riesgos: Revisiones trimestrales. 11.5. Concientización y Cultura 11.6. Simulaciones de phishing periódicas 11.7. Métricas de efectividad en cultura de seguridad

Tabla 21 Planes y proyectos para lograr la Arquitectura objetivo

Dichos entregables se encuentran en el siguiente anexo:

[Arquitectura Seguridad TOBE para el ICETEX 1.4.pdf](#)
[Presentación Infotíc consultoría ARQ TOBE 1.0.pptx](#)

4.3.8. Plan de Continuidad

Durante el presente periodo, se adelantaron las fases I y II del plan previsto.

Fase I. En esta fase se establecieron los elementos estratégicos y de referencia necesarios para la actualización del Sistema de Gestión de Continuidad de Negocio (SGCN) del ICETEX, a partir del entendimiento del entorno institucional, regulatorio y sectorial en el que opera la entidad.

Principales desarrollos realizados:

Documento de Contexto del ICETEX en materia de continuidad

- Se elaboró un análisis situacional que consideró el rol de la entidad dentro del sector educativo y financiero, su marco normativo, las expectativas de los grupos de interés y su nivel de dependencia tecnológica y operativa.
- Este análisis permitió identificar los factores internos y externos que impactan la continuidad de los servicios institucionales.

Declaración de Alcance del SGCN y formulación de la Política de Continuidad

- Se definió el alcance formal del sistema, delimitando los servicios esenciales, las sedes, los procesos incluidos y las exclusiones justificadas.
- Se generó la versión actualizada de la Política de Continuidad, alineada con los principios de gestión de riesgos, resiliencia organizacional y las exigencias de la norma ISO 22301.

Matriz de procesos críticos a evaluar

- Se identificaron y priorizaron los procesos críticos mediante criterios de impacto, dependencia tecnológica, afectación al usuario y exigencias regulatorias.

Metodología de uso, instrumentos de gestión y plantillas operativas

- Se diseñó y documentó la metodología de trabajo del SGCN, incluyendo lineamientos, fases, responsables e integración con otros sistemas de gestión institucionales.
- Se desarrollaron los formatos, matrices y herramientas que serán utilizados en las siguientes etapas (BIA, análisis de riesgos, planes, tableros de control, etc.).

Fase II. En esta fase se realizó la evaluación formal de los riesgos que afectan la continuidad operativa del ICETEX y se consolidaron los resultados del Análisis de Impacto al Negocio (BIA), con el fin de priorizar los procesos críticos y definir los parámetros de recuperación requeridos para la entidad. Los principales desarrollos realizados:

Metodología de Evaluación de Riesgos y Matriz Consolidada

- Se diseñó y aplicó la metodología para la valoración de riesgos asociados a la continuidad de los servicios institucionales.
- Se consolidó la matriz de riesgos de los procesos priorizados para el SGCN, identificando niveles inherentes, residuales y controles existentes.

Metodología BIA e Informe Consolidado

- Se aplicó la metodología de Análisis de Impacto al Negocio (BIA), obteniendo los valores de RTO, RPO y los tiempos máximos tolerables de interrupción para cada proceso evaluado.
- El informe permitió validar los procesos críticos que requieren planes de continuidad y recuperación prioritaria.

Matriz de Interdependencia de Procesos

- Se elaboró la matriz que evidencia las relaciones funcionales, tecnológicas y operativas entre los procesos críticos, identificando dependencias internas y externas clave para la operación.
- Informe de Impactos Potenciales a Corto Plazo
- Se debe identificar la infraestructura tecnológica transversal que habilita la recuperación de los sistemas de información: site alternativo comunicación y seguridad, Directorio Activo, BUS, Accesos

Información más detallada de cada uno de los entregables se encuentra en los siguientes anexos:

Fase1_Entregables.zip

Fase2_Entregables.zip

Se adelantaron sesiones con el equipo de apoyo a la supervisión, así como con personal de la oficina de riesgos, presentando los resultados aquí expuestos, sin recibir observaciones a la fecha.

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

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

4.4. Servicios de nube

Durante el mes de NOVIEMBRE de 2025, se desarrollaron actividades orientadas al fortalecimiento, optimización y documentación de la infraestructura Microsoft Azure – ICETEX, avanzando en la ejecución de acciones estratégicas derivadas del Assessment de Infraestructura Azure y en la implementación de nuevos recursos dentro del entorno productivo. El periodo se caracterizó por el despliegue de componentes clave, la depuración de recursos obsoletos y la consolidación de prácticas de gobernanza y monitoreo, asegurando la continuidad y estabilidad de los servicios alojados en la nube institucional. En materia de planificación y gestión, se elaboró el Plan de Trabajo – Assessment Azure, que establece los frentes de acción, responsables, tiempos y prioridades para la ejecución de actividades de mejora, consolidando una hoja de ruta técnica para las siguientes fases del proyecto. Se avanzó en la optimización de la infraestructura mediante la depuración de recursos huérfanos (NSG, NIC e IP públicas), reduciendo costos innecesarios y mejorando el control administrativo del entorno. Asimismo, se realizaron despliegues exitosos de infraestructura productiva, destacando la implementación de la máquina virtual vm-devops-agent, destinada a la ejecución de pipelines CI/CD, y el despliegue del grupo de recursos rg-ori-qas, configurado a través de un template ARM que integra servicios de aplicación, almacenamiento y análisis cognitivo. En el componente de monitoreo y trazabilidad, se completó la implementación del entorno de grabaciones, que incluyó la creación de la Storage Account recordingicetex y el Log Analytics Workspace log-workspace-recordings-prd, integrando auditoría y monitoreo en tiempo real de operaciones de almacenamiento bajo estándares de seguridad y cumplimiento. Adicionalmente, se elaboró y validó la Guía de conexión mediante Azure Storage Explorer, documento técnico que estandariza el procedimiento de acceso al almacenamiento recordingicetex mediante token SAS, fortaleciendo la gestión controlada de accesos al entorno productivo. En el ámbito de seguridad y gobernanza, se avanzó en el Assessment integral de la suscripción Azure ICETEX Producción y en el análisis de roles y asignaciones RBAC, identificando cuentas con privilegios elevados y oportunidades de mejora en el control de accesos, actualmente en fase de evaluación. Finalmente, se consolidó la documentación técnica del periodo, integrando los informes de actividades, planes de trabajo, registros de despliegue y validaciones realizadas, garantizando trazabilidad operativa y soporte documental para auditorías o revisiones posteriores. En conjunto, las actividades desarrolladas durante noviembre permitieron fortalecer la arquitectura operativa, mejorar la trazabilidad de los servicios, optimizar recursos y avanzar en la madurez de gobernanza cloud del ICETEX, estableciendo bases sólidas para las fases de implementación y seguimiento que continuarán en el próximo periodo. Un extracto de dicho plan se presenta a continuación:

Acción	Esfuerzo (S/M/L)	Impacto (H/M/L)	Dependencias
Validación de la conectividad de los usuarios hacia las máquinas con exposición al rango 0.0.0.0/0.	S	H	Validar accesos operativos; ventana de cambio
Identificación de los puertos utilizados, tipo de conectividad y origen de los accesos a la máquina.	M	H	Revisión de puertos requeridos por AVD
Depurar NSG huérfanos tras confirmar cero dependencias	S	M	Revisar scripts/terraform históricos

Eliminación de NIC huérfanos, validando previamente que no estén asociados a máquinas virtuales activas o recursos en uso. Además, revisar etiquetas, direcciones IP públicas o privadas, y grupos de seguridad (NSG) asociados antes de su eliminación.	S	M	Verificar IPs públicas asociadas
Validar las IP públicas desasignadas de algún recurso, identificando a qué aplicación pertenecieron. (botatereqjud2-ip, net-avd-bck, vm-rpa-prd2-vnet-ip)	S	M	Confirmar historial y no-dependencia
Migrar IPs a SKU Standard (pip-ti-hub-01), La dirección IP pública pertenece a la conexión Site-to-Site entre ICETEX y Azure, asociada al VPN Gateway. La migración puede tardar entre 10 y 20 minutos, por lo que se requiere una ventana de mantenimiento.	M	H	Compatibilidad con LB/NIC, ventana de cambio
Rediseñar el direccionamiento y las subredes (10.4.0.0/24) para la red vm-app-home-vnet como parte del plan de migración. Se identificó que las redes botatereqjud2-vnet y vm-rpa-prd2-vnet se encuentran huérfanas, sin recursos conectados actualmente y están mal dimensionadas.	L	M	Inventario IP, peerings, VPN/ER

Tabla 22 Plan de trabajo Microsoft Azure – ICETEX

En el presente periodo se han adelantado las siguientes actividades:

- Eliminación de interfaces de red huérfanas en Azure
- Eliminación de direcciones IP públicas huérfanas en Azure
- Eliminación y redimensionamiento de redes virtuales en Azure
- Creación de reserva de capacidad para máquina virtual – SKU Standard_D16s_v5
- Redireccionamiento de redes virtuales – Optimización del espacio IP en Azure
- Eliminación de grupos de recursos huérfanos
- Eliminación de grupos de recursos sin dependencias en Azure

5. GESTION DE LA EJECUCIÓN CONTRACTUAL

El contrato 2022-0792 con fecha de perfeccionamiento del acta de inicio del 30 de diciembre 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 enero 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.

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

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

En el presente informe del mes de noviembre del 2025 del proyecto, se encuentra en la fase de operación de los servicios contemplados en el alcance llevando ejecutados 31 meses que equivale al 86,11% 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	\$ 9.322.124.020	\$480,000,000	\$420,000,000	\$60,000,000	\$3.915.152.986,12
	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	0	\$120,000,000	0		0
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		
	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 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	
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	
Pendiente - Pago No. 30 -	mes:	Septiembre	de	2025	\$ 769,683,313.00	
						Contrato Inicial*

Pendiente - Pago No. 30 -	mes:	Septiembre	de	2025	\$420,000,000		Bolsa
Pendiente - Pago No. 1 -	mes:	Septiembre	de	2025	\$120,882,259.89		OTROSI-Adición Servicios
Pendiente - Pago No. 31 -	mes:	Octubre	de	2025	\$782,805,080.00		Contrato Inicial*
Pendiente - Pago No. 2 -	mes:	Octubre	de	2025	\$120,882,259.89		OTROSI-Adición Servicios**
Pendiente - Pago No. 32 -	mes:	Noviembre	de	2025	\$ 779.487.583		Contrato Inicial*
Pendiente - Pago No. 3 -	mes:	Noviembre	de	2025	\$594.225.142		OTROSI-Adición Servicios**
VALOR CAUSADO QUE NO SE HA PAGADO (valor a pagar factura) *							\$784,142,167.57
VALOR CAUSADO QUE NO SE HA PAGADO (valor a pagar factura) **							\$594.225.142
VALOR TOTAL EJECUTADO (valor pagado + valor causado no pagado)							\$ 23.763.861.191
SALDO DEL CONTRATO (valor total del contrato – valor total ejecutado)							\$ 10.396.616.037
PORCENTAJE DE EJECUCIÓN							69.57%
* 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 23 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 Noviembre2025.pdf
Especialista Web Máster	Juan Carlos Martinez	Informe Mensual InfoTIC Webmaster Noviembre 2025.pdf
Especialista Integrador de nube	Carlos Barrera	Informe Mensual InfoTIC Integrador de Nube Noviembre 2025.pdf
Especialistas de Seguridad	Jhon Alveiro Pava González Edwin Morales	Informe Mensual InfoTIC Seguridad noviembre2025.pdf
Especialistas de soluciones	Jose Francisco Escobar Escorcía Davis Alexander Mogollón Fandiño	Informe Mensual InfoTIC Administrador de Soluciones Noviembre 2025.pdf
Especialista de Networking	Carlos Alberto Roldan Ríos Victor Manuel Castiblanco Sanchez - Apoyo Networking	Informe Mensual InfoTIC Administrador de Redes Noviembre 2025.pdf
Líder Red Team	Luis Alfonso Rodriguez	Informe Pentesting URLs ICETEX Noviembre.pdf Informe Pentesting Servidores ICETEX Noviembre.pdf Plan de Remediación Vulnerabilidades ICETEX V7.pdf Matriz Remediación de Vulnerabilidades ICETEX V2.xlsx
Consultoría Arquitectura de Seguridad	Sonia Constanza Villamil	Arquitectura Seguridad TOBE para

Perfiles	Especialistas	Anexo
		el ICETEX 1.4.pdf Presentación Infotíc consultoría ARQ TOBE 1.0.pptx
Consultoría BCP	Mario Cifuentes Zarta	Matriz Escenarios de alternativas de Continuidad para procesos priorizados y evaluados.xlsx Plan de continuidad de negocio BCP para los procesos evaluados.docx Informe de recomendación de estrategia de continuidad.docx 2. Plan de recuperacion de TI - DRP.docx 3. Documento de la estrategia seleccionada por ICETEX.docx 3. Protocolo de Gestion de Crisis.docx 4. Procedimientos Recuperación.docx 4.. Procedimientos Recuperacion.docx

Tabla 24 Perfiles y Actividades

El siguiente es el grupo administrativo que estuvo en el desarrollo de la operación del mes de Noviembre del 2025:

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

Tabla 25 Grupo Administrativo

8. SERVICIO DE COLABORACIÓN

Durante el mes de noviembre, 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:

ÍTEM	SERVICIO	CIUDAD	DIRECCIÓN	CANTIDAD
1	Sala de video conferencia o	Bogotá – Aguas	Carrera 3 No. 18-32 Piso 2,	3

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

	sala virtual (Tamaño 65")		4 y 6	
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 26 Distribución módulos de videoconferencia por sede

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

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

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

- Visita en sitio en sedes de Bogotá, para realizar pruebas de funcionamiento, 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 Regionales, el cual se puede consultar en el link [Informe actividades Módulos videoconferencia ICETEX Noviembre2025.pdf](#)

Para el periodo de noviembre del presente año, comprendido entre el 1 y el 30 del mes, en las sedes Regionales (Cali, Barranquilla, Bucaramanga, Medellín y Chapinero) no se recibieron solicitudes especiales que requirieran atención y gestión de soporte técnico, tampoco se reportaron incidencias a nivel del servicio para estas sedes durante el periodo, sin embargo, como en cada periodo, se contó con la disponibilidad para recibir cualquier solicitud de soporte (Incidencia/requerimiento) o apoyo concerniente a la solución de videoconferencia desplegada y puesta en funcionamiento.

Para el periodo comprendido entre el 1 y el 30 de noviembre, para las sedes de Bogotá Aguas y Ángel, No se recibieron requerimientos para gestión y atención del soporte técnico; tampoco fueron reportadas incidencias a nivel del servicio para estas sedes durante el mes del presente informe, no obstante, como cada periodo, se contó con la disponibilidad técnica para recibir cualquier requerimiento de soporte o solicitud de apoyo en lo concerniente a la solución de videoconferencia desplegada. La solicitud de gestión interna de ingreso a la entidad para la visita técnica frecuente se realizó mediante el caso RF-320775-8-24861.

9. GESTION DE RIESGOS Y PROBLEMAS

Se construyó una tabla de nivel riesgo que contiene los factores a analizar cómo son severidad y probabilidad otorgando un rango de valor que representa cada uno de los niveles de ocurrencia, con los cuales se determina el nivel de riesgo. Cabe destacar que la determinación de estos valores no sigue una regla estricta, y puede ser ajustada de acuerdo con las necesidades del proyecto.

➤ Matriz de riesgos

Se adjunta la matriz de riesgo y de deja la evidencia del documento generado.

No.	Actividad	Peligro	Consecuencia Riesgo	Medidas de control	Evaluación del riesgo			Medidas de control a implementar	Responsable
					Severidad (S)	Probabilidad (P)	S x P		
1	Sin acceso a los servidores con los usuarios y contraseñas entregados	No poder gestionar los servicios requeridos por el ICETEX	Pérdida de tiempo y dinero	Realizar pruebas mensualmente para confirmar el acceso a los servidores	3	8	24	Verificar con CLARO los cambios que realicen a nivel de la gestión corporativa	INFOTIC
2	Instalación de agente de antivirus en los servidores de ICETEX	Sufrir ataques que puedan dañar la información o no permitir el desarrollo de los servicios instalados en los equipos	Fallas de seguridad	Inventario de los servidores identificando cuales tienen instalado y actualizado la versión del antivirus	2	6	12	Mensualmente revisar los servidores asignados al proyecto revisando el estado del antivirus	INFOTIC
3	Parches de actualización de los sistemas operativos de los servidores del ICETEX	Se presentan vulnerabilidades a nivel de los servidores	Fallas de seguridad	Inventario de los servidores identificando la última versión de parches actualizada	3	6	18	Verificación con los fabricantes sobre la última versión liberada y funcionando comparada con la instalada actualmente en los servidores	INFOTIC
4	Actualización de servidores que son 2008 y 2012	Se presentan vulnerabilidades a nivel de los servidores	Fallas de seguridad	Inventario de los servidores	4	8	32	Verificación semanal del estado de los servidores	ICETEX - INFOTIC
		Fallas en el funcionamiento de las aplicaciones instaladas en estos equipos	Reprocesos y altos costos ya que estos equipos no tienen soporte de fabricante	Inventario de las aplicaciones				Verificación semanal del estado de las aplicaciones	ICETEX - INFOTIC

Ilustración 41 Matriz de riesgos

Matriz de riesgos ICETEX.xlsx

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.

Durante la ejecución de un proyecto, existen una gran cantidad de factores que pueden determinar el nivel de riesgo, por lo que es importante diferenciar dos tipos:

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

- **Factores internos:** son aquellos que hacen parte esencial del desarrollo de la operación que se realiza en ICETEX y que tienen que ver con el alcance del proyecto, como lo pueden ser los servidores, aplicaciones, canales de comunicaciones, data center principal y externo.
- **Factores externos:** son aquellos que se encuentran fuera del alcance de la empresa, y son de difícil identificación, tales como los fenómenos naturales o fenómenos económicos.

Para lo cual, se tiene:

- Tabla de nivel de riesgo

		PROBABILIDAD				
		IMPROBABLE	POSIBLE	OCASIONAL	MODERADA	CONSTANTE
SEVERIDAD		2	4	6	8	10
INSIGNIFICANTE	1	2	4	6	8	10
MENOR	2	4	8	12	16	20
MODERADO	3	6	12	18	24	30
CRITICO	4	8	16	24	32	40
CATASTROFICO	5	10	20	30	40	50

Tabla 27 Nivel de Riesgo

- Tabla de grado de riesgo

COLOR	NIVEL DE RIESGOS
	Riesgo Aceptable
	Riesgo Tolerable
	Riesgo Alto
	Riesgo Extremo

Tabla 28 Grado de riesgo

10. INDICADORES CLAVE DE DESEMPEÑO

10.1. ANS por Disponibilidad de canales de comunicaciones:

Durante el mes de Noviembre de 2025, 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 Noviembre 2025.pdf](#)

También se puede consultar en el repositorio un documento en Excel con el análisis del comportamiento de los canales para el mes de Noviembre [ANS Noviembre 2025.xlsx](#)

Sede	Categoría	INR	%MES
BOGOTAD.C.	Principal/FO (Sede Aguas)	INR0037	99,99%
	Backup /FO (Sede Aguas)	INR0036	99,76%
	Principal/IPVPN (Sede Chapinero)	INR0022	100,00%
	Backup /IPVPN (Sede chapinero)	INR0020	99,99%
	Principal/IPVPN (Angel)	INR0272	100,00%
	Backup /IPVPN (Angel)	INR0273	100,00%
IBAGUE	Principal/IPVPN	INR0073	100,00%
	Backup/IPVPN	INR0076	99,63%
LETICIA	Principal/Satelital	INR0000373	96,29%
NEIVA	Principal/IPVPN	INR0039	100,00%
	Backup/IPVPN	INR0041	100,00%
TUNJA	Principal/IPVPN	INR0104	100,00%
	Backup/IPVPN	INR0106	99,56%
VILLAVICENCIO	Principal/IPVPN	INR0085	100,00%
	Backup/IPVPN	INR0084	99,90%
ARMENIA	Principal/IPVPN	INR0074	100,00%
	Backup/IPVPN	INR0072	99,87%
MANIZALES	Principal/IPVPN	INR0088	99,96%
	Backup/IPVPN	INR0087	99,82%
MEDELLIN	Principal/IPVPN	INR0133	99,78%
	Backup/IPVPN	INR0132	99,79%
APARTADO	Principal/IPVPN	INR0144	99,55%
PEREIRA	Principal/IPVPN	INR0079	100,00%
	Backup/IPVPN	INR0077	100,00%
QUIBDO	Principal/IPVPN	INR0014	99,35%
	Backup/IPVPN		0
BARRANQUILLA	Principal/IPVPN	INR0103	100,00%
	Backup/IPVPN	INR0100	99,83%
CARTAGENA	Principal/IPVPN	INR0109	99,98%
	Backup/IPVPN	INR0107	99,99%
MONTERIA	Principal/IPVPN	INR0080	99,85%
	Backup/IPVPN	INR0081	99,85%
RIOHACHA	Principal/IPVPN	INR0164	98,63%
	Backup/IPVPN	INR0162	97,84%
SANTAMARTA	Principal/IPVPN	INR0154	97,00%
	Backup/IPVPN	INR0152	99,90%
SINCELEJO	Principal/IPVPN	INR0095	100,00%
	Backup/IPVPN	INR0097	99,89%
SAN ANDRES	Principal/IPVPN	INR0000367 INR0000369	88,37%
BARRANCABERMEJA	Principal/IPVPN		0

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	%MES
SANGIL	Principal/IPVPN		0
BUCARAMANGA	Principal/IPVPN	INR0062	100,00%
	Backup/IPVPN	INR0061	100,00%
CUCUTA	Principal/IPVPN	INR0044	100,00%
	Backup/IPVPN	INR0047	99,99%
VALLEDUPAR	Principal/IPVPN	INR0091	100,00%
	Backup/IPVPN	INR0090	100,00%
YOPAL	Principal/IPVPN	INR0121	98,16%
	Backup/IPVPN	INR0123	98,16%
ARAUCA	Principal/IPVPN	INR0110	100,00%
CALI	Principal/IPVPN	INR0151	100,00%
	Backup/IPVPN	INR0153	99,40%
BUENAVENTURA	Principal/IPVPN	INR0051	96,26%
MOCOA	Principal/IPVPN	INR0135	100,00%
	Backup/Satelital	INR0136	100,00%
PASTO	Principal/IPVPN	INR0130	100,00%
	Backup/IPVPN	INR0131	100,00%
POPAYAN	Principal/IPVPN	INR0035	100,00%
	Backup/IPVPN	INR0032	99,96%
TUMACO	Principal/IPVPN	INR0147	86,61%
DCTRIARA	MPLSPP	INR0266	100,00%
	MPLS Backup	INR0171	100,00%
DCTRIARA	INTERNET BK	INR0221	0
	INTERNET PP	INR0264	100,00%
DCTRIARA	NOC claro de dedicado (DWDM)2GTriaramegacentro	INR0224	100,00%
Canal entre Sitio principal Icetex-Dirección General-Aguas	Principal/IPVPN		0
	Backup/IPVPN		0
BOGOTAD.C.	Internet (Sede Aguas)	INR0034	100,00%
DC Megacentro	DCMEGACENTER–CONTIGENCIA–MPLSPPAL	INR0177	100,00%
DCTRIARA	DCMEGACENTER–CONTIGENCIA–MPLS BK	INR0230	100,00%
DC Megacentro	Internet	INR0268	100,00%
Banco de la Republica hasta Edificio Dirección General ICETEX	Ubicado en Data center Principal. Interconectado a través de red MPLS	INR0000289	100,00%
DECEVAL hasta Edificio de ICETEX Dirección General	Ubicado en Data center Principal. Interconectado a través de red MPLS	INR0000317	99,99%
DECEVAL hasta Edificio de ICETEX Dirección General	Ubicado en Data center Principal. Interconectado a través de red MPLS (Backup)	INR0000318	100,00%

Sede	Categoría	INR	%MES
Salidadelportaleshttps://portal.icetex.gov.co/portalywww.icetex.gov.cohaciainternetencentrod ecómputoprincipal	Internet Reverso para Portales	INR0000320	100,00 %
Salidadelportaleshttps://portal.icetex.gov.co/portalywww.icetex.gov.cohaciainternetencentrod ecómputodecontingencia	Internet Reverso para Portales	INR0274	0 %
DCTRIARA	Allot Centralizado 800M Triara(equipo)	INR0270	100,00 %

Tabla 29 Disponibilidad de Canales

Durante el mes de noviembre de 2025 el servicio de Internet para la gente se prestó sin interrupciones en todas las catorce sedes contratadas donde ICETEX cuenta con oficina, las cuales se relacionan a continuación:

Sede	Categoría	INR	% Mes
BARRANQUILLA	INTERNET PARA LA GENTE	INR0094	100,00%
BUCARAMANGA	INTERNET PARA LA GENTE	INR0057	100,00%
CALI	INTERNET PARA LA GENTE	INR0160	100,00%
AGUAS	INTERNET PARA LA GENTE	INR0029	99,99%
CHAPINERO	INTERNET PARA LA GENTE	INR0015	100,00%
MEDELLIN	INTERNET PARA LA GENTE	INR0122	99,79%
APARTADO	INTERNET PARA LA GENTE	INR0140	99,55%
ARAUCA	INTERNET PARA LA GENTE	INR0115	88,91%
LETICIA	INTERNET PARA LA GENTE	INR0000378	96,29%
QUIBDO	INTERNET PARA LA GENTE	INR0021	99,35%
RIOHACHA	INTERNET PARA LA GENTE	INR0159	98,64%
SAN ANDRES	INTERNET PARA LA GENTE	INR0000368	88,38%
YOPAL	INTERNET PARA LA GENTE	INR0127	100,00%
MOCOA	INTERNET PARA LA GENTE	INR0141	99,99%

Tabla 30 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 noviembre continúa su funcionamiento correctamente sin novedades que afectaran la prestación del servicio. La evidencia se encuentra en el [Informe mensual replicacion Noviembre 2025.pdf](#)

10.2. ANS por Disponibilidad de servidores:

La herramienta utilizada para el monitoreo de la disponibilidad de servidores es ELK, y el informe correspondiente permite la revisión de los ANS en los documentos [Disponibilidad Server ELK Noviembre 2025.xlsx](#) y [Disponibilidad Server ELK Noviembre 2025.xlsx](#)

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

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

No	COD.	Etiquetas de fila	Disponibilidad
1	INR0000322	ictsrvctrldoc	100,00%
2	INR0226	mira	99,95%
3	INR0228	ictxisgesbd	100,00%
4	INR0229	ictxisgesapp	99,98%
5	INR0233	icetexboglخورفو1.localdomain	100,00%
6	INR0234	ictxprusisgapp	99,97%
7	INR0235	ictxbogsrvpt2 **	100,00%
8	INR0236	ictxbogsrvpt1**	100,00%
9	INR0237	icetexbogbalsever1-r*	100,00%
10	INR0238	icetexbogliferaynfs	96,37%
11	INR0239	icetexbogelasticserver1	100,00%
12	INR0240	icetexbogelasticserver2	100,00%
13	INR0241	icetexbogelasticserver3	100,00%
14	INR0242	icetexbogliferayserver2	99,97%
15	INR0243	icetexbogliferayserver1	99,95%
16	INR0244	icetexboglxdarumasrv1	100,00%
17	INR0245	icetexboglxdarumasrv2	100,00%
18	INR0246	icetexboglxdarumatest	100,00%
19	INR0247	preprodsec	100,00%
20	INR0248	icetexboglxroad3	100,00%
21	INR0249	xroadsec	100,00%
22	INR0250	qasec	100,00%
23	INR0251	INR0251_INFOTIC	99,99%
24	INR0252	icetexosbognfs2	100,00%
25	INR0253	bastion.localdomain	100,00%
26	INR0254	INR0254_INFOTIC	100,00%
27	INR0255	INR0255_INFOTIC	99,99%
28	INR0256	INR0256_INFOTIC	100,00%
29	INR0257	INR0257_INFOTIC	100,00%
30	INR0258	INR0258_INFOTIC	99,95%
31	INR0259	INR0259_INFOTIC	99,98%
32	INR0260	icetexosbognfs1	100,00%
33	INR0262	icetexboglخورفو2.localdomain	100,00%
34	INR0276	cxvodaprodn011	100,00%
35	INR0277	cxvodaprodn021	100,00%
36	INR0278	cxvodacontg011	100,00%

Tabla 31 Códigos relacionados Disponibilidad Servicios en Housing – Datacenter Principal

**Los servidores (ictxbogsrvpt1 y ictxbogsrvpt2) en el mes de diciembre 2024 se solicitó por parte del ICETEX dar de baja y distribuir sus recursos en los servidores de OPENSIFT, dicha solicitud quedó aplicada la cierre

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

del mes de diciembre, por lo tanto no se visualizarán a partir del mes de enero de 2025 en el Reporte de disponibilidad, sin embargo para efectos de facturación se continúan teniendo en cuenta tal como se acordó, evidencia de la solicitud en el documento: [Baja de servidores - Actualización OpenShift incremento de RAM.pdf](#)

El servidor *icetexboglobserver1-r, que corresponde al antiguo balanceador de carga, fue deshabilitado a principios del mes de julio. Esta acción se llevó a cabo debido a la puesta en producción de un nuevo balanceador en el mes de junio.

Como resultado de esta medida, este servidor dejó de aparecer en el Reporte de Disponibilidad a partir de agosto, no obstante, el servidor sigue facturándose. En el mes de Noviembre se asignaron los recursos de memoria en el servidor Nodo 2 de Portal Icetex.

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

#	Dispositivo	Marca	Modelo
1	FORTIWEB01	Fortinet	2000E
2	FORTIWEB02	Fortinet	2000E
3	FORTIAUTH01	Fortinet	1000D
4	FORTIAUTH02	Fortinet	1000D
5	FORTISANDBOX	Fortinet	1000D
6	Cisco 3650X	Cisco	WS-C3650-48TQ
7	Cisco 3560X SW	Cisco	WS-C3650-48TQ
8	Switch DELL Networking	Dell	N4032 24 ports
9	Controladora SAN Dell Compellent	Dell	SC8000
10	Controladora SAN Dell Compellent	Dell	SC8000
11	Enclosure Discos SAN	Dell	EN-SC200
12	Enclosure Discos SAN	Dell	EN-SC220
13	Enclosure Discos SAN	Dell	EN-SC200
14	Enclosure Discos SAN	Dell	EN-SC220
15	Enclosure Discos SAN	Dell	EN-SC220
16	Enclosure Discos SAN	Dell	EN-SC200
17	Enclosure Dell Blade – Principal 5 Servidor – Blade M1000, 6 IOM Slot B2 -Tarjeta Enclosure - M1000	Dell	M1000E

Tabla 32 Dispositivos en Housing – Datacenter Principal

10.2.1. Disponibilidad TRIARA para los servicios de página web

A continuación, se evidencia que la disponibilidad del Portal Web institucional web.ICETEX.gov.co, el cual presentó en el mes de Noviembre un **UPTIME del [99.018%]** tal como se evidencia en la gráfica a continuación.



Ilustración 42 UPTIME – Portal WEB web.ICETEX.gov.co

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

	Agosto	Septiembre	Octubre	Noviembre
Usuarios activos mes	457000	526.000	422.000	408000
Usuarios nuevos	314000	408.000	291.000	283000
Tiempo de interacción (seg)	139	91	65	62

Tabla 33 Distribución trimestral de acceso por usuarios

El portal WEB cuenta con un total de 408 mil usuarios, con 283 mil usuarios nuevos. El tiempo de interacción medio es de 2 minuto2 y 2 segundos, señalando el interés de la audiencia en las diferentes páginas del portal web.icetex.gov.co.

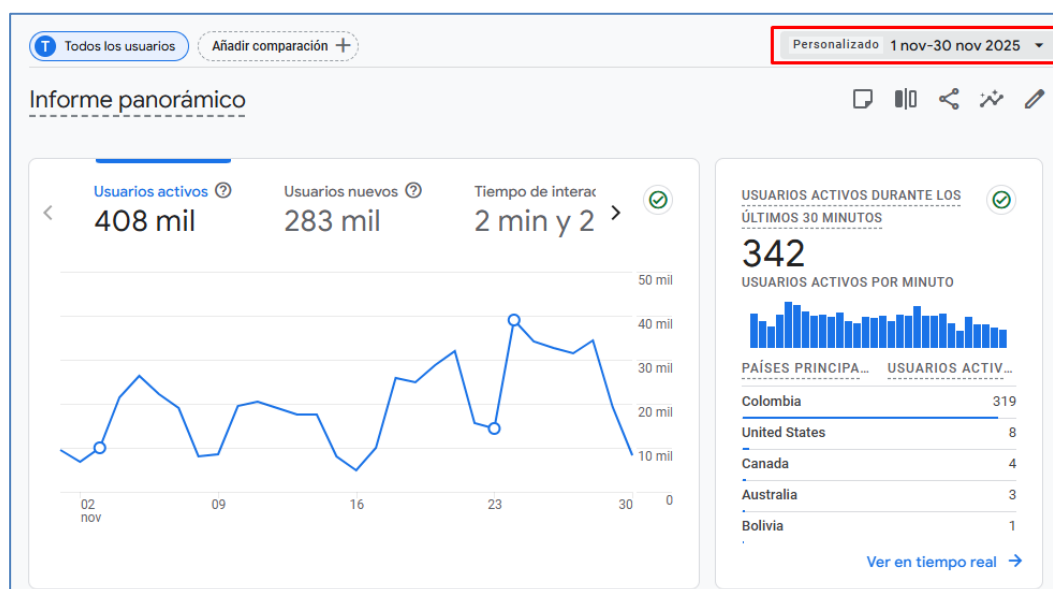


Ilustración 43 Métrica de visitantes Portal WEB web.ICETEX.gov.co

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

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

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:

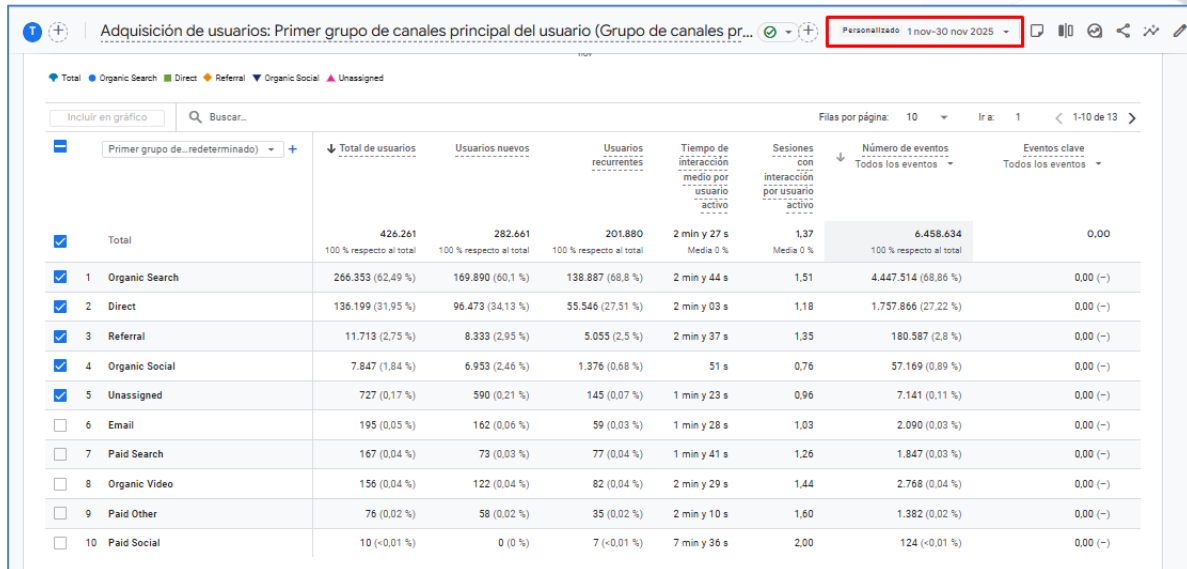


Ilustración 44 Métrica adquisición usuarios Portal WEB web.ICETEX.gov.co

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.

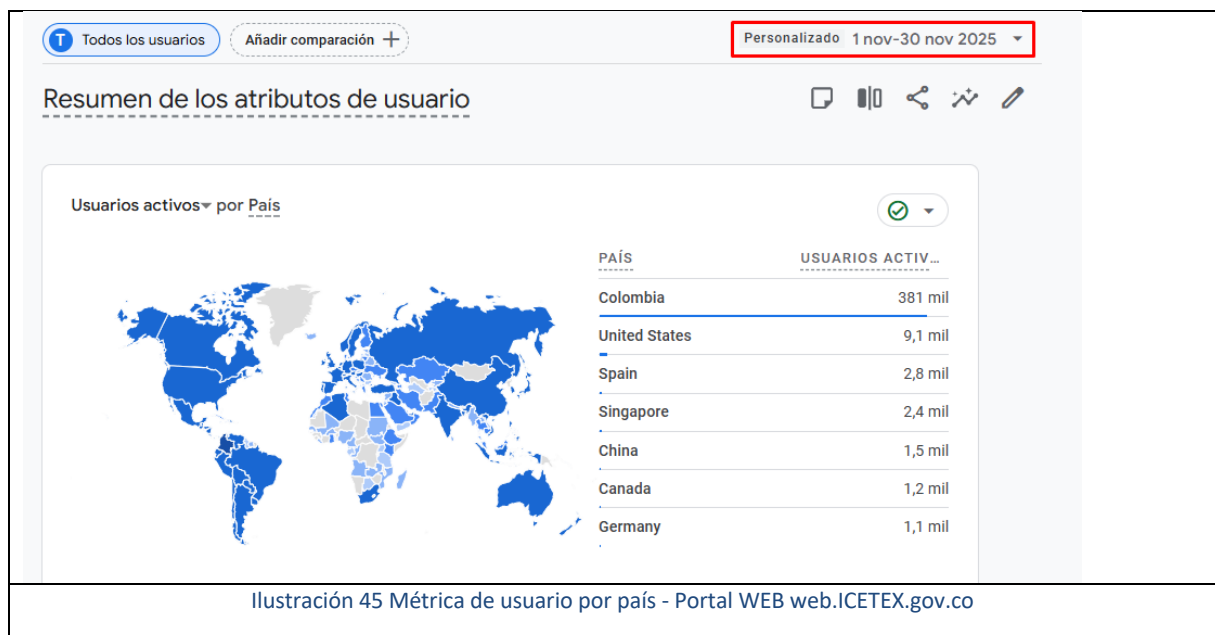
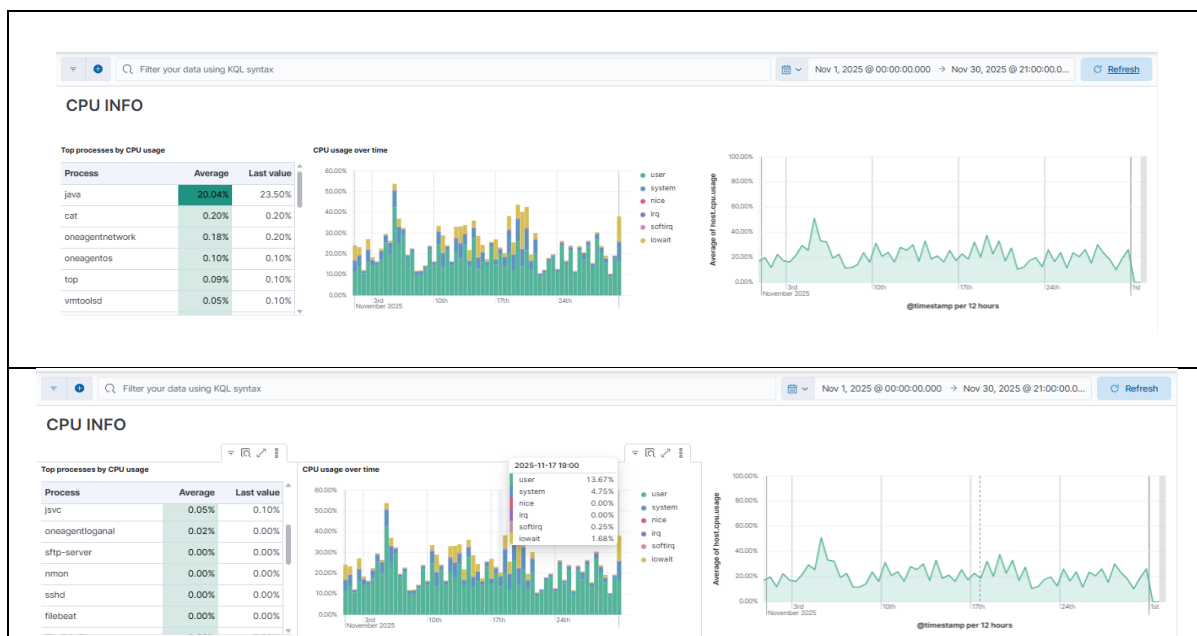


Ilustración 45 Métrica de usuario por país - Portal WEB web.ICETEX.gov.co



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 NOVIEMBRE desde las 00:00 horas hasta las 23:59 horas del 30 de noviembre de 2.025



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

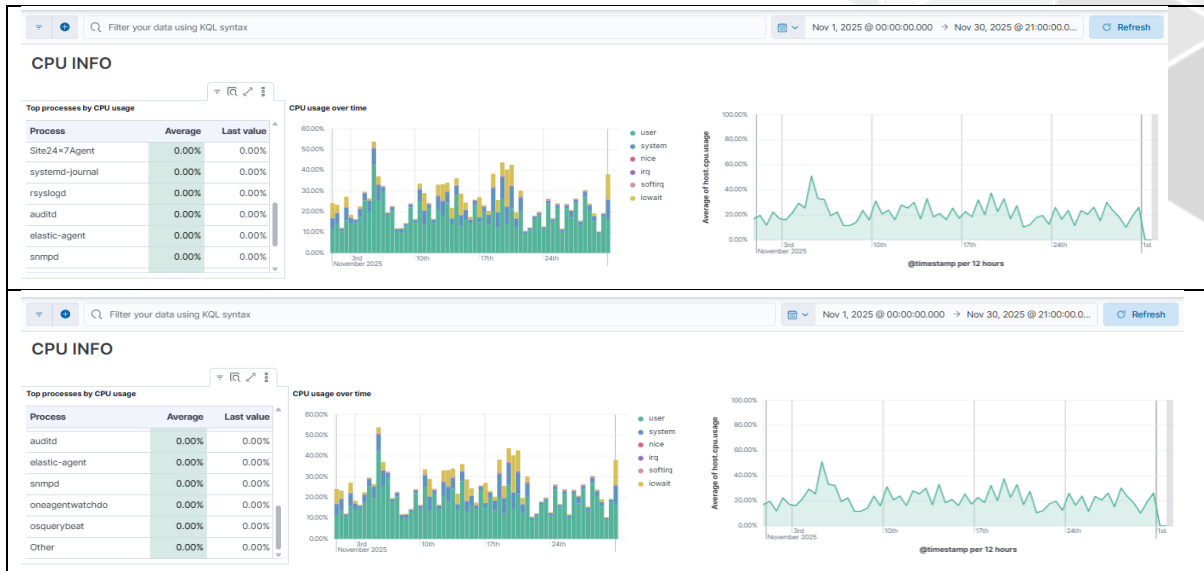
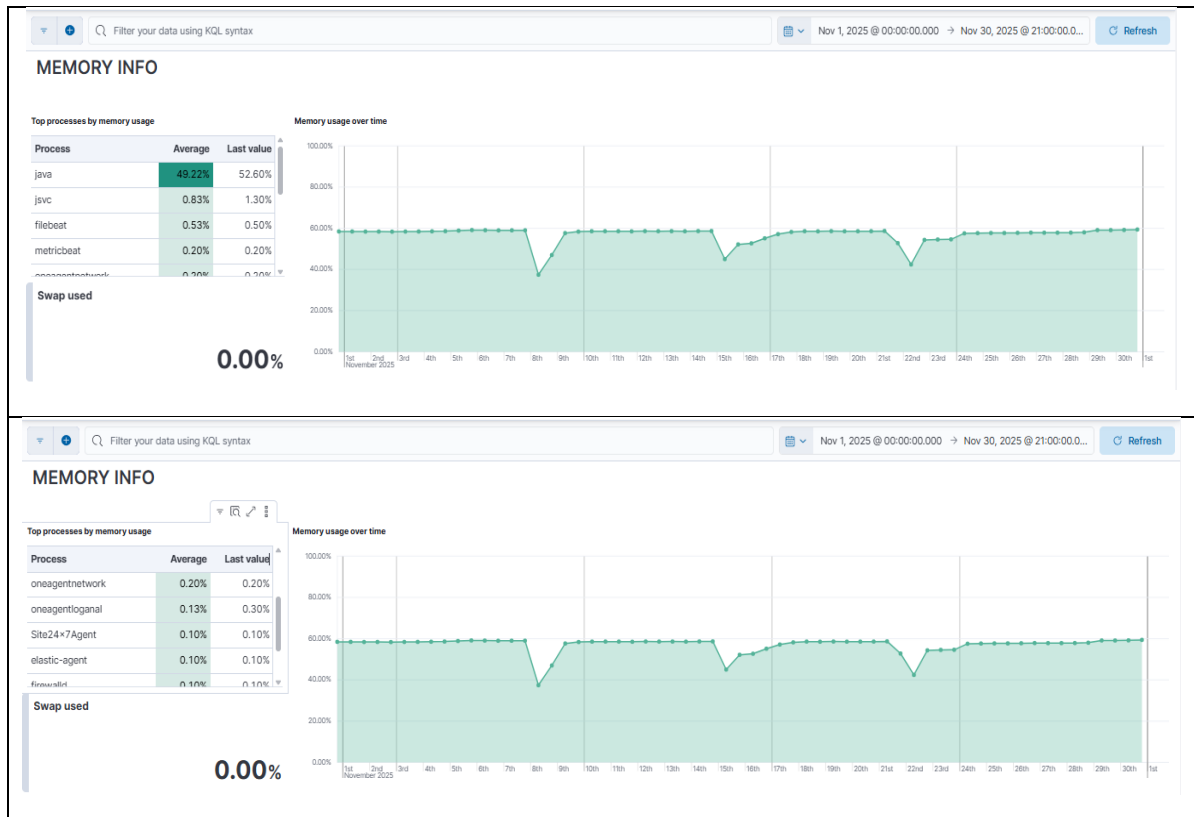
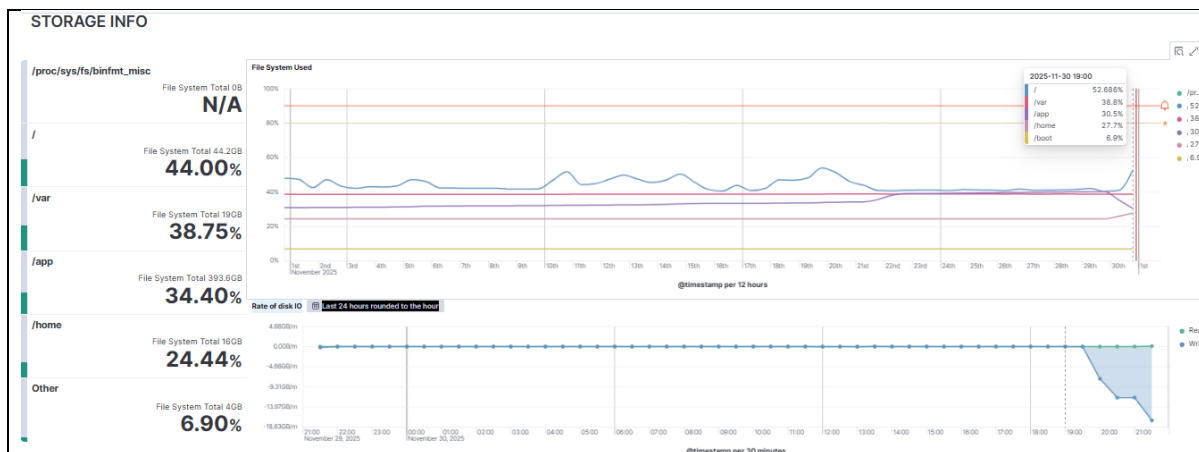


Ilustración 47 NODO 1 CPU





Estos mismos recursos, para el nodo 2 se monitorean de igual manera. El detalle de los consumos y sus umbrales puede ser consultado en el informe de nuestro especialista web master [Informe Mensual InfoTIC Webmaster Noviembre 2025.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.

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

10.2.3. Backup Servidores Triara

Durante el periodo de noviembre se realizaron los Backups de acuerdo con las políticas definidas por el ICETEX, las cuales desde su inicio se implementaron en el Datacenter. Se puede verificar en el documento [Informe Backups mes de Noviembre 2025.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 noviembre 2025.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 V2.xlsx](#)

Actualmente, se cuenta con la custodia externa de 294 cintas en las instalaciones de VISE, correspondientes a la información histórica entregada a partir del 23 de agosto de 2023.

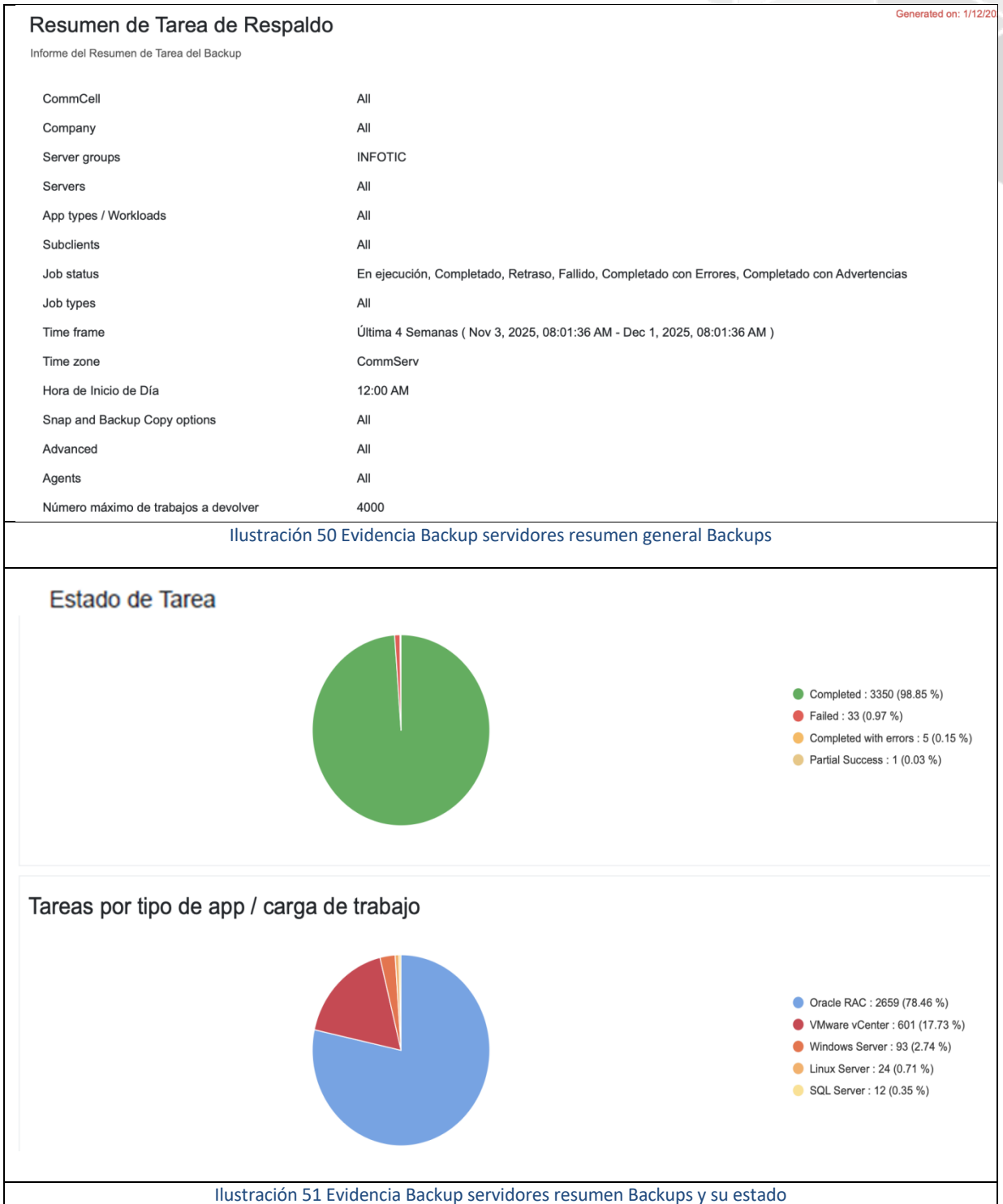
A la fecha, el ICETEX, no ha entregado las cintas de backup necesarias para llevar a cabo el almacenamiento y traslado a custodia externa, lo que permitiría devolver todas las cintas que actualmente se encuentran en calidad de préstamo.

El consolidado de las cintas utilizadas hasta la fecha son las siguientes:

Ubicación	Cantidad de Cintas ICETEX
Custodia Vise	303
Librería	32
Nuevo Custodia	60
Total	395 cintas

Tabla 34 Cintas Backups ICETEX

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



El total del tamaño de la información respalda para el mes de noviembre corresponde a 197.87 TB, donde 98.85% se completó en el primer lanzamiento del robot con un total de 197.8 TB de información.

El 78.46% está representado en el respaldo dado a la información del Oracle RAC.

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

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

De un total de 3389 trabajos analizados, el 99% se completó con éxito (incluyendo los que tuvieron errores menores). El 98.85% de todos los trabajos se completaron sin ningún error.

- Tasa de éxito: 99 % (trabajos completados o completados con errores)
- Tasa de fracaso: 0.97% (trabajos fallidos o cancelados)
- Oracle RAC: El 78.46% de los trabajos de respaldo corresponden a este tipo de servidor, con un total de 2659 trabajos.
- VMware vCenter: El 17.73% de los trabajos pertenecen a este entorno, con 601 trabajos.
- Otros Servidores: Los trabajos de Windows Server, Linux Server y SQL Server representan el 2.71%, 0.71% y 0.35% 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](#)

A la fecha ICETEX no ha realizado la entrega de las cintas de Backup para devolver las cintas que se están usando en calidad de préstamo para realizar el almacenamiento y traslado a custodia externa.

11. CONTROL DE CAMBIOS

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

No. Cambio	Alcance	Fecha De Creación	Fecha De Ejecución	Resultado	Observaciones
1218	Actualizaciones de parches de seguridad para Servidores Windows: El cambio aplica a los siguientes servidores: • ICTXSRVMOODLE (192.168.51.82): aloja la aplicación Comunidad ICETEX, publicada en internet y accedida por usuarios externos. • ICTXSRVAPPMIX3 (192.168.51.139): aloja el servicio	12/11/2025	16/11/2025	Exitoso	N/A

No. Cambio	Alcance	Fecha De Creación	Fecha De Ejecución	Resultado	Observaciones
	CustomWindowsServiceNovacion, 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.				
1219	Actualizaciones de parches de seguridad para Servidores Windows: El cambio aplica a los siguientes servidores en entorno de producción: • ICTXSRVAPPMIX1 (192.168.51.134): aloja las aplicaciones PSE, Cargue Archivos, Cuentas Abandonadas, Cuentas Inactivas, Portal Transaccional y Transunion, las cuales están publicadas en internet y accedidas por usuarios externos. • ICTXSRVNETCOR01 (192.168.51.165): aloja las aplicaciones internas Desembolsos, Reporteador, Servicios de Integración MEN, Censo Indígena, Sisben, 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. Los tres servidores serán actualizados con los últimos parches de seguridad y estabilidad del sistema operativo Windows. No se verán afectadas otras máquinas ni servicios fuera de estos entornos.	12/11/2025	16/11/2025	Exitoso	N/A
1217	Ejecución Pruebas DRP segundo Semestre 2025	11/11/2025	29/11/2025	Exitoso	N/A

No. Cambio	Alcance	Fecha De Creación	Fecha De Ejecución	Resultado	Observaciones
1216	Actualización del Clúster físico de los Servidores de Base de Datos de Oracle INR0276 e INR0277	11/11/2025	21/11/2025	Exitoso	N/A

Tabla 35 Controles de cambio noviembre

12. PLAN DE TRABAJO DE LOS PROXIMOS MESES

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

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
Revisar las alternativas de solución respecto al licenciamiento de las herramientas de seguridad (perimetral y antivirus)	ICETEX	01-06-2025	31-12-2025	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.	INFOTIC - ICETEX	01-12-2024	31-12-2025	Se está haciendo seguimiento a estos temas de implementación de IPV6 en las sesiones semanales. Ver avances en la última acta de seguimiento del mes de noviembre.
Capacitación en seguridad al grupo de especialistas de seguridad del ICETEX	INFOTIC - ICETEX	01-12-2024	31-12-2025	Se realizó la segunda capacitación de temas de ciberseguridad al ICETEX el 28/11/2025.
Monitoreo de los diferentes servicios realizados por el SOC. Revisión conjunta entre ICETEX – INFOTIC	INFOTIC - ICETEX	01-12-2024	31-12-2025	Se envió el mes pasado al ICETEX un informe sobre los dispositivos que están siendo monitoreados por el SOC, con el fin de que sean validados por dicha entidad. Actualmente, estamos a la

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
				espera de su respuesta. El correo tiene como asunto: Dispositivos monitoreados FortiSIEM.
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	31-12-2025	Se debió bajar el agente de Symantec porque generó bloqueos en la BD de Oracle, el aliado nos indica una alternativa con otro antivirus por lo tanto se realizará mesa de trabajo de los DBA con los especialistas del aliado para revisar la viabilidad de instalar el antivirus Falcon.

Tabla 36 Planes de trabajo

13. RECOMENDACIONES DEL CONTRATISTA AL ICETEX

13.1. Networking

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

Reemplazo de Equipos Dañados: Luego del daño del equipo en la sede de San Andrés, 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.

13.2. Aplicaciones

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

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

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

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

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, correspondiente a los meses de agosto, septiembre y noviembre de 2025, seguido de observaciones y recomendaciones:

Disco	Métrica	jul-25	ago-25	sep-25	Observaciones	Recomendaciones
C:	Espacio usado	65% (66.6 GiB)	58% (58.1 GiB)	69% (68.97 GiB)	Se incrementó el uso en almacenamiento en comparación con el mes anterior en aproximadamente 11 GiB.	Considerar mover archivos no esenciales a otro volumen que dispongan desde el lado de infraestructura hacia almacenamiento secundario.
	Espacio libre	33.3 GiB	41.4 GiB	30.54 GiB		
F:	Espacio usado	92% (1.74 TiB)	95% (1.80 TiB)	96% (1.90 TiB)	Altísima ocupación constante (>90%), aunque mejora en septiembre debido al aumento del almacenamiento en 100GB	Urgente implementar políticas de depuración de archivos antiguos o inactivos. 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 52 Histórico consolidado uso de discos servidor ICTXSRVNETCOR01

13.3. Seguridad

En cuanto a la gestión de las bases de datos se recomienda retirar permiso de SUDO a los usuarios INFOTIC, GAWUSER y DCSCAF pues, con esto usuarios, podrían realizar actividades administrativas que no van con su rol. Para ello se debe analizar la razón de estos privilegios con los equipos que realizan mantenimientos a las aplicaciones y verificar el cambio a un rol más apropiado a sus labores.

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

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

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

- Se debe trabajar en el perfilamiento de la navegación de acuerdo con lo entregado por ICETEX.
- Validar la autenticación de doble factor para todas las plataformas misionales del ICETEX.
- Realizar autenticación a través del LDAPS, para la gestión de las plataformas de seguridad.
- Realizar la contención automática de equipos que se identifiquen en la red como maliciosos.
- Realizar el aumento de recursos a la plataforma de FortiSIEM (CPU, Memoria y disco) y hacer un cambio de arquitectura con el objetivo de mejorar.
- Se debe realizar la integración de los activos críticos de la compañía a la plataforma de SIEM, no se ha podido lograr por la falta de recursos de este.
- Adquirir un equipo Firewall para correo para prevenir brechas de seguridad asociadas al uso del correo electrónico y que este es susceptible a muchos tipos de amenazas.
- Integrar los servidores de Directorio Activo con el SIEM.
- Garantizar la segmentación de la red que permita claramente definir qué servicios deben ser alcanzados por cada usuario.
- Se recomienda, que el ICETEX, adquiera una herramienta que permita realizar análisis de tráfico de la red (NTA- Network Traffic Analysis).

- Se recomienda una tecnología que permita la gestión o validación de privilegios de accesos (IAM). Evitar configurar usuarios y claves dentro de las aplicaciones de ICETEX.
- Validar a nivel de punto final, los equipos que se han visto involucrados con comportamiento malicioso.
- Integrar los equipos que hacen parte del proceso de pagos con el SIEM.
- Evaluar los riesgos sobre las plataformas en la nube y considerar aplicar plataformas de seguridad para los ambientes Cloud que cuenta la entidad ya que estos contienen servicios críticos para la misma.

13.4. Bases De Datos

Se deben aumentar los espacios del área de recuperación de las bases de datos productivas de 1TB a 5TB para tener una retención de 10 días o más, con el TB de almacenamiento aprovisionado solo se puede mantener 2 días por BD.

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

13.5. Integrador De Nube

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

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

14. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC

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

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

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

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

Para el periodo de reporte se reporta, la ejecución de la segunda capacitación de seguridad el pasado **28 de noviembre de 2025**, correspondiente al segundo año del contrato.

Se continuará con la programación de la capacitación correspondiente al año 3 del contrato de acuerdo con la disponibilidad de agenda de los equipos de trabajo del ICETEX, aspecto que se concertará con la supervisión del contrato.

14.3. 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	
INR0192	MEGACENTER	Almacenamiento Centralizado 15 TB Tier 2	25
INR0191	MEGACENTER	Almacenamiento Centralizado 10 TB Tier 2.5	
			60

Tabla 37 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

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

Almacenamiento MVs replicación VMware	19,4	RVTools
Almacenamiento MVs KVM (BD)	10,9	RF1700669
TOTAL	30,3	
TOTAL, ALMACENAMIENTO APROVISIONADO	90,8	

Tabla 38 Capacidades de almacenamiento provisionado

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

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

Código de Servicio	Hostname	Tipo de restauración	Fecha backup restaurado	Fecha prueba restauración	Resultado	Evidencia
INR0238	icetexbogliferafnfs	full backup	22/11/2025	25/12/2025	Exitoso	INR0238

Tabla 39 Pruebas de Restauraciones de Backups de Noviembre

14.4. “Wifi” para la gente en 19 sedes

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

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

Tabla 40 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 41 WIFI para la gente pendientes

15. CONCLUSIONES

- El uso de autenticación de doble factor en las conexiones VPN de los funcionarios ayudaría a proteger mejor la información sensible y evitar accesos no autorizados.
- Administrar adecuadamente las contraseñas y permisos garantiza que solo las personas autorizadas accedan a información importante, reduciendo riesgos de seguridad.
- Configurar controles de acceso a la red basados en los servidores de la entidad permite restringir el acceso a ciertas áreas, evitando que los usuarios lleguen a sitios peligrosos.
- Optimizar los recursos del FortiSIEM facilitaría el monitoreo de sistemas clave como bases de datos, aplicaciones internas y equipos, permitiendo detectar problemas rápidamente y responder de forma oportuna.
- Ajustar las reglas de seguridad en la red ha permitido un mejor control sobre los recursos clave,

asegurando que solo lo necesario esté disponible y fortaleciendo la protección.

- Implementar soluciones para gestionar quién puede conectarse a la red mejoraría la seguridad y reduciría el impacto de posibles incidentes.
- Los reportes del SOC han sido clave para detectar y corregir vulnerabilidades, evitando que amenazas afecten la infraestructura crítica de la entidad.
- 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.

16. ANEXOS

Tema	SubTema	Anexo
Almacenamiento	Backups Diarios	Backups diarios noviembre 2025 (30 reportes) Backup Diario
	Informe de Backups	Consolidado mensual Backups noviembre 2025 Consolidado Mensual de Backups noviembre 2025.pdf Informe Backups mes de Noviembre 2025.pdf Politica Backup Icetex V2.xlsx
Aplicaciones	Informes de actividades	Informe actividades Módulos videoconferencia ICETEX noviembre 2025 Informe actividades Módulos videoconferencia ICETEX Noviembre2025.pdf Informe mensual Administrador de Soluciones noviembre 2025 Informe Mensual InfoTIC Administrador de Soluciones Noviembre 2025.pdf Informe mensual Administrador Web Master noviembre 2025 Informe Mensual InfoTIC Webmaster Noviembre 2025.pdf Informe mensual Integrador Nube noviembre 2025 Informe Mensual InfoTIC Integrador de Nube Noviembre 2025.pdf
Arquitectura de Seguridad		Informe de Arquitectura AS-IS de Seguridad de la Información V. 1.4 Arquitectura Seguridad TOBE para el ICETEX 1.4.pdf Presentación Infotíc consultoría_ARQ_TOBE_1.0

Tema	SubTema	Anexo
		Presentación Infotíc consultoría ARQ TOBE 1.0.pptx
Bases De Datos		Informe mensual Administrador de Bases de datos noviembre 2025 Informe Mensual InfoTIC DBA Noviembre2025.pdf
Ejecución Presupuestal		Conciliación noviembre consolidado Conciliación Noviembre consolidado.xlsx Informe de Gestión Servicio noviembre2025 Informe de Gestion Servicio Noviembre 2025.pdf Informe de Gestion Servicio Noviembre 2025.docx
Informe Pentest		Informe Pentest Informe Pentesting URLs ICETEX Noviembre.pdf Informe Pentesting Servidores ICETEX Noviembre.pdf Plan de Remediación Vulnerabilidades ICETEX V7.pdf Matriz Remediacion de Vulnerabilidades ICETEX V2.xlsx
Informes Plan de Continuidad		Informes Plan de Continuidad Matriz Escenarios de alternativas de Continuidad para procesos priorizados y evaluados.xlsx Plan de continuidad de negocio BCP para los procesos evaluados.docx Informe de recomendación de estrategia de continuidad.docx 2. Plan de recuperacion de TI - DRP.docx 3. Documento de la estrategia seleccionada por ICETEX.docx 3. Protocolo de Gestion de Crisis.docx 4. Procedimientos Recuperación.docx 4.. Procedimientos Recuperacion.docx
Seguridad		Informe Mensual MARCA-OSINT ICETEX noviembre Informe Mensual MARCA-OSINT ICETEX Noviembre 2025.pdf Informe Mensual Seguridad noviembre 2025 Informe Mensual InfoTIC Seguridad noviembre2025.pdf Informe Mensual SOC - ICETEX noviembre 2025 Informe Mensual SOC-TH ICETEX noviembre 2025.pdf Informe técnico análisis de vulnerabilidades ICETEX noviembre 2025 WX INFORME TECNICO AV ICETEX Noviembre.pdf WX Matriz de Vulnerabilidades ICETEX Noviembre.xlsx

Tema	SubTema	Anexo
		Reporte de IPS noviembre 2025 Reporte de IPS de noviembre infotic 2025.docx
Soporte Y Monitoreo	Canales	ANS noviembre 2025 ANS Noviembre 2025.xlsx Informe mensual Administrador de Networking noviembre 2025 Informe Mensual InfoTIC Administrador de Redes Noviembre 2025.pdf Informe Mensual Disponibilidad Noviembre 2025 Reporte Mensual Disponibilidad INFOTIC Noviembre 2025.pdf
	Gráficas de consumo	Informe Mensual ALLOT Noviembre 2025 Graficas de consumo Noviembre 2025 – ALLOT INFOTIC.xls Consumo general mensual 1.12.25 6.00 AM.pdf
Data center Alterno	Replicación	Informe mensual replicación Noviembre 2025 Informe mensual replicacion Noviembre 2025.pdf Reportes diarios Noviembre 2025 (30 reportes) Replicación
Data Center Principal		Reporte Monitoreo ICETEX noviembre 2025-ELK Reporte Monitoreo ICETEX Noviembre 2025-ELK.pdf Data ELK Disponibilidad Server_ELK_Noviembre_2025.xlsx

Tabla 42 Anexos

Revisión técnica

REVISÓ	FIRMAS
SANDRA MILENA GARCIA HERNANDEZ Contratista Grupo De Infraestructura	
JOAO DO NELSON DUCUARA Contratista Grupo De VOT	
GERMAN MANUEL DIAZ Contratista Grupo De VOT	
NELSON JAVIER CASALLAS BELTRAN Contratista Grupo De VOT	
GERMAN AUGUSTO MEJIA CARDONA Coordinador Grupo de Infraestructura Tecnológica	