1. PERIODO DEL INFORME

PERÍODO A QUE CORRESPONDE EL INFORME	01-02-2025 28-02-2025

2. DATOS DEL SUPERVISOR

NOMBRE DEL SUPERVISOR	VICTOR RAUL BAUTISTA GALINDO Y CARLOS EDUARDO CRUZ GONZALEZ
DEPENDENCIA	Dirección de Tecnología
CARGO	Director de Tecnología (E) y Coordinador de Infraestructura

3. DATOS DEL CONTRATO

OBJETO: Servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el ICETEX	
NÚMERO DE CONTRATO	2022-0792
FECHA DE SUSCRIPCIÓN	30/12/2022
FECHA DE PERFECCIONAMIENTO Y EJECUCIÓN	30/12/2022
CONTRATISTA	INFOTIC S.A.S
CÉDULA DE CIUDADANÍA O NIT	900.068.796-1
VALOR (incluido IVA)	$31.398.996.857,96
PLAZO	39 meses (3 meses de implementación y 36 meses de operación)
FECHA DE INICIO	19/01/2023
FECHA DE FINALIZACIÓN	19/04/2026
ADICIÓN (SI APLICA)	N/A
PRÓRROGA (SI APLICA)	N/A
SUSPENSIÓN (SI APLICA)	N/A

4. SEGUIMIENTO GESTIÓN CONTRACTUAL = NO APLICA

El siguiente cuadro debe ser diligenciado solo para personas naturales:

NÚMERO DE LA OBLIGACIÓN	OBLIGACIÓN ESPECIFICAS (Relacionar obligaciones pactadas en el Contrato)	ASIGNADO PARA EL PERIODO (DE CORTE SEGÚN EL CONTRATO)		Descripción de la gestión realizada para cada actividad durante el periodo	Evidencias (Documentos o links dónde reposa la información)
		Si	No		

Persona jurídica: Adjunta Informe de actividades y soportes: SI ☒ NO ☐

OBSERVACIONES: EL CONTRATISTA ADJUNTA INFORME DE ACTIVIDADES CORRESPONDIENTES AL PERIODO DEL MES DE ENERO DE 2025.

5. PRODUCTOS ENTREGABLES = NO APLICA

NÚMERO DE PRODUCTO	ENTREGABLES (Relacionar los entregables relacionados en el Contrato)	ENTREGADO	NO ENTREGADO
1	El detalle de cada etapa y sus entregables se encuentran resumidos en el Anexo 09 - Gobernabilidad, donde se encuentran descritos los productos mínimos que EL PROVEEDOR DE SERVICIOS debe entregar en cada etapa, para revisión y aprobación por parte del supervisor del contrato asignado por ICETEX. Son de obligatorio cumplimiento los reportes descritos en el Anexo 12 - Reportes Operación.	X	

OBSERVACIONES: (SI A ELLO HUBIERE LUGAR)

Presenta informe de los servicios prestados en periodo de ENERO de 2025, se da continuidad con la concertación de ANS sobre los servicios prestados de acuerdo con el anexo técnico del contrato en el periodo del INFORME ENTREGADO.

6. REPORTE DE DATOS GENERALES Y POSIBLES CONFLICTOS DE INTERÉS CONTRATISTAS (DILIGENCIAR SOLO PERSONA NATURAL) = NO APLICA

En mi calidad de CONTRATISTA, actuando en nombre propio o en calidad de Representante Legal, mediante el presente documento declaro bajo la gravedad de juramento que la información que consigno a la fecha en la que suscribo este documento y relaciono a continuación es real y autorizo para que el Instituto de Crédito Educativo y Estudios en el Exterior "Mariano Ospina Pérez" – ICETEX, bajo cualquier medio legal corrobore la veracidad de la misma:

7. ¿PROCEDE PAGO EN ESTE PERIODO? (Diligenciar el siguiente apartado únicamente para Persona Jurídica)

SI _X___	NO ____

SE ANEXA AL PRESENTE INFORME CERTIFICACIÓN PARA PAGO DE LOS SERVICIOS PRESTADOS DE DICIEMBRE DE 2024. Se procesa el pago correspondiente de la factura FVE-1769 por valor de $ 772.219.902.

Se aplica ANS por valor de $60.923.574 para los servicios de diciembre 2024 de acuerdo con el memorando Radicado 20255110133945-E Id: 559388 en el que se solicita la facturación de los servicios de acuerdo con la aceptación de parte de INFOTIC mediante el comunicado radicado VOP-124-2025.

Los servicios prestados en el periodo de enero de 2025 se encuentran en concertación de ANS.

8. RELACIÓN DE PAGOS A LA SEGURIDAD SOCIAL O CERTIFICACIÓN DE APORTES PARAFISCALES (Diligenciar el siguiente apartado únicamente para Persona Natural) = NO APLICA

Para los fines del presente, el contratista entregó el soporte de pago a la Seguridad Social emitido por el operador XXX, donde indica que ha cumplido con la obligación de pago de los aportes al sistema de seguridad social (pensión, salud y ARL), según lo señalado en el artículo 50 de la Ley 789 de 2002 y el artículo 1° de la Ley 828 de 2003, cuyos pagos se ajustan a los porcentajes establecidos, así:

Mes y año	Número de planilla	Salud	Pensión	ARL
		$	$	$

Persona jurídica: Entrega certificación de Seguridad Social y Aportes Parafiscales. SI ☒ NO ☐

9. ¿EL CONTRATISTA PUBLICÓ LOS DOCUMENTOS DE EJECUCIÓN EN EL SECOP?

SI __X_____	NO _____	NO APLICA _____

SE DEJA CONSTANCIA QUE A LA FIRMA DEL PRESENTE INFORME DE SUPERVISIÓN, EL CONTRATISTA HA CARGADO DENTRO DEL SECOP II LOS INFORMES Y DOCUMENTOS DE EJECUCIÓN CORRESPONDIENTES A LA FECHA Y QUE LA SUPERVISIÓN DEL CONTRATO HA APROBADO LOS MISMOS DENTRO DE LA PLATAFORMA.

10. CUMPLIMIENTO SISTEMA DE GESTION DE SEGURIDAD Y SALUD EN EL TRABAJO - SST

10.1. ¿EL CONTRATISTA ENTREGÓ SOPORTES DE ASISTENCIA A LA INDUCCIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO AL INICIO DEL CONTRATO?

SI _____	**NO** _____	**NO APLICA** _____X_____

NOTA: EL SOPORTE DE ASISTENCIA A LA INDUCCIÓN APLICA SÓLO PARA EL PRIMER PAGO DEL PRESENTE CONTRATO DE PRESTACIÓN DE SERVICIOS PERSONA NATURAL.

10.2 ¿EL CONTRATISTA ENTREGÓ SOPORTES DE ASISTENCIA Y EVALUACIÓN DE MÍNIMO UNA CAPACITACIÓN AL MES DICTADA POR EL ÁREA DE SST?

SI _____	**NO** _____	**NO APLICA** _____X_____

NOTA: SOLO APLICA PARA CONTRATOS PRESTACIÓN DE SERVICIOS PERSONA NATURAL.

SE DEJA CONSTANCIA QUE A LA FIRMA DEL PRESENTE INFORME DE SUPERVISIÓN, EL CONTRATISTA ENTREGÓ AL SUPERVISOR LOS SOPORTES CORRESPONDIENTES, ENUNCIADOS EN EL NUMERAL 10 QUE APLIQUEN, DE CONFORMIDAD CON LO ESTABLECIDO EN EL FORMATO "CARTA DE COMPROMISO DE SEGURIDAD Y SALUD EN EL TRABAJO" (F546), FIRMADA AL INICIO DEL CONTRATO DE PRESTACIÓN DE SERVICIOS. ASÍ CÓMO LOS SOPORTES MENSUALES DE ASISTENCIA Y EVALUACIÓN DE LAS CAPACITACIONES DICTADAS POR EL ÁREA DE SST, DURANTE LA EJECUCIÓN DEL CONTRATO DE PRESTACIÓN DE SERVICIOS PERSONA NATURAL.

OBSERVACIONES: (SI A ELLO HUBIERE LUGAR)

11. EJECUCIÓN PRESUPUESTAL

	VIGENCIA *(AÑO)*
VALOR DEL CONTRATO	$31.398.996.857,96
VALOR ADICIÓN (Si aplica)	$0
VALOR A PAGAR (Si aplica)	$ 772.219.902,00
VALOR EJECUTADO	$ 14.441.737.170,00
VALOR PENDIENTE POR EJECUTAR	$ 16.957.259.687,96

12. ANÁLISIS MATERIALIZACIÓN Y MITIGACIÓN DEL RIESGO:

¿DURANTE LA EJECUCIÓN SE MATERIALIZÓ ALGÚN RIESGO?

SI ☐ **NO** ☒

Si la respuesta es afirmativa, diligencie el número del evento del riesgo radicado en vigía:

13. RECIBO A SATISFACCIÓN:

El DIRECTOR DE TECNOLOGIA (E) VICTOR RAUL BAUTISTA GALINDO Y EL COORDINADOR DE INFRAESTRUCTURA CARLOS EDUARDO CRUZ GONZALEZ en calidad de supervisores, recibieron a satisfacción el cumplimiento de las obligaciones pactadas en el contrato en mención, así como la entrega

de los documentos aquí relacionados, por parte del contratista **INFOTIC S.A.S** identificado(a) con NIT **900.068.796-1** para los servicios prestados en el periodo de DICIEMBRE de 2024.

En virtud de lo anterior se aprueba realizar trámite de pago para la factura No**. FVE-1769** por valor de **SETECIENTOS SETENTA Y DOS MILLONES DOSCIENTOS DIECINUEVE MIL 2NOVECIENTOS DOS PESOS M/CTE ($ 772.219.902)**

En constancia se firma en Bogotá D.C. a los 16 días del mes de mayo de 2025.

Presentó:	**Aprobó:**
 **FIRMA DEL SUPERVISOR** **MONICA MARIA VILLAMIZAR SANCHEZ** **No. CC 26.862.573**	 **FIRMA DEL SUPERVISOR** **VICTOR RAUL BAUTISTA GALINDO** **No. CC 79.352.968**
	 **FIRMA DEL SUPERVISOR** **CARLOS EDUARDO CRUZ GONZALEZ** **No. CC 79.451.906**

Revisó: Raúl Fernando Gutiérrez Tecano- Analista 2 Dirección de Tecnología 

Al contestar cite Radicado 2025000144562-R Id: 5920714 Folios: 1 Fecha: 02-05-2025 05:04:39 Anexos: 1 Remitente: Destinatario:

2 de Mayo de 2025

PARA:

DE: - INFOTIC S.A

ASUNTO:

PDF DEL DOCUMENTO ELECTRÓNICO #FVE1810

Cordialmente,

- INFOTIC S.A
9000687961

No de Contacto: 0
Dirección de Contacto: CL 93B 13 44 PI 2
Correo Electrónico: RECEPCION@INFOTIC.CO

INFOTIC
SOLUCIONES INTELIGENTES

Responsables de IVA - No Somos Autorretenedores
Desde el año 2022 al 2024

7020-1 Actividad Principal 8,66‰ 6202 Otras Actividades 6,9‰

8299 Actividad Secundaria 9,66‰ 6209 Otras Actividades 9,66‰

Sociedad de economia mixta con participacion del 51% de Infimanizales

INFOTIC S.A

Nit: 900068796-1
CL 93B 13 44 PI 2

Tel: 7466000 Fax: 7466000

Bogotá, D.C.

Factura Electrónica De Venta

FVE-1810

Cliente

Nombre: INSTITUTO COLOMBIANO DE CREDITO EDUCATIVO Y ESTUDIOS TECNICOS EN EL EXTERIOR MARIANO OSPINA PEREZ IC
NIT: 899999035
Dirección: CR 3 18 32
Ciudad: Bogotá, D.C.
Teléfono: 4173535
C.C: ICETEX 2022-0792

Fecha: 5/2/2025 4:38:11 PM
Forma de pago: CREDITO 30 DIAS
Moneda: COP
Fecha vcto: 6/2/2025 12:00:00 AM
Medio de pago

Servicio	Descripción	Cant	Valor unitario	Valor bruto	Valor total
VS90900102	SERVICIOS ESPECIALIZADOS EN OUTSOURCING PARA LA CONECTIVIDAD, RED DE COMUNICACIONES, CENTRO DE DATOS Y SERVICIOS CONEXOS CON VALOR AGREGADO PARA EL ICETEX, DURANTE EL MES DE FEBRERO DE 2025. SERVICIOS OPERACIÓN MES DE ENERO DE 2025 (INCLUIDO IVA): $ 833.143.476 (-) DESCUENTOS INCLUIDO IVA: CONECTIVIDAD Y RED DE COMUNICACIONES: -$22.494.688 CENTRO DE DATOS: -$41.127.755 TOTAL DESCUENTO CON IVA: -$63.622.443 OBJETO DEL CONTRATO: SERVICIOS ESPECIALIZADOS EN OUTSOURCING PARA LA CONECTIVIDAD, RED DE COMUNICACIONES, CENTRO DE DATOS Y SERVICIOS CONEXOS CON VALOR AGREGADO PARA EL ICETEX.	1.00	$ 648,562,704.00	$648,562,704.00	$ 771,789,618.00

IMPUESTOS	BASE	TASA	TOTAL
IVA	$648,562,704	19 %	$123,226,914

SETECIENTOS SETENTA Y UN MILLONES SETECIENTOS OCHENTA Y NUEVE MIL SEISCIENTOS DIECIOCHO PESOS M/CTE *****

Notas

facturacion_electronica@icetex.gov.co

RESPONSABLE: MONICA VILLAMIZAR

VALOR BRUTO	$648,562,704.00
DESCUENTO	$0.00
SUBTOTAL	$648,562,704.00
IVA	$123,226,914.00
TOTAL FACTURA	$771,789,618.00

AUTORIZACIÓN NUMERACIÓN DE FACTURACIÓN **Resolución N°:** 18764072568331 **Numeración Desde:** FVE 1356 **Hasta:** FVE 2000
Vigencia Desde: 2024/06/07 **Hasta:** 2025/06/07 **12 Meses**

CUFE e76a83247f1396238b05176a4ccb7c286b487acb5d01fef04ed309ef9341e458284d5788ba4bb4631c41aaec0d3a6aed

FIRMA DIGITAL:

NIvLKowOvfWidDcL0TOIY+gBuQgr0Eyww8kAReQ/6XppV0MDyOpiriHzG84iGIiEvbk0YjgV8464skP/KAmDWXDQ0EwQX/OW1aPHDf37j/naMDY7/GYgRqwzXVm
FIRccyriu9YZYKz5hbLowim6I/DkgDMCJrnGfUVxpgDOVBGmoWz/IIHR3XBsShKqH15XX4XJZmt1FiBqQAA6dMTE1i3rKbP74ekix/PlHS75mvh1Ysh4aOCOob4vew
fbCdCmNy90WLCj1wRfMaGscowEeO7di+sEWSt3CQeZdLQgHWnf37K5OY5oEs5GXtAY3i8uGPYQ5J6nkIJiqFNCN9VJO5g==

FECHA DIAN: 2025-05-02 16:40:20-05:00

Emisor

Nombre Legible y Fecha de Entrega

"SOMOS AGENTES RETENEDORES DE IVA"

Factura generada por software de SISTEMAS DE INFORMACION EMPRESARIAL SA. NIT 890.319.193-3

REIMPRESO

ORIGINAL

INFORME DE ACTIVIDADES

CONTRATO NUMERO 2022-0792

Febrero 01 al 28 de 2025

1. Introducción 7
2. Objetivo del Informe 7
3. Alcance 8
4. AVANCE TÉCNICO 9
4.1. Conectividad Y Red de Comunicaciones 9
4.1.1. Canales instalados en el mes y entregables 9
4.1.1.1. Solicitudes Nuevas Instalación de canales: 10
4.1.2. Pruebas de Saturación Bidireccionales 14
4.2. Centro de Datos 15
4.2.1. Centro de Datos Principal 15
4.2.1.1. Aplicaciones 15
4.2.1.2. Bases de Datos 16
4.2.2. Centro de Datos Alterno 18
4.2.2.1. Hosting Virtual (IaaS) 18
4.2.2.2. Dataguard Bases de Datos Megacenter 21
4.2.2.3. Servicios de Housing – Datacenter Alterno 21
4.2.2.4. Servicios de DRP 22
4.3. Seguridad informática 22
4.3.1. Plataformas Administradas 23
4.3.1.1. FortiGate Triara 23
4.3.1.2. FortiGate Aguas 26
4.3.1.3. FortiGate Medellín 26
4.3.1.4. FortiWeb 2000F 27
4.3.1.5. FortiWeb 2000E 27
4.3.1.6. FortiSandBox 27
4.3.1.7. Sophos EndPoint 28
4.3.2. Estadística de Portales 28
4.3.3. Servicio de centro de Operaciones de Seguridad (SOC) 29
4.3.3.1. Alertas o Incidentes de Seguridad Detectados 31
4.3.3.1.1. Categoría Seguridad 31

4.3.3.1.2. Categoría Disponibilidad 31
4.3.3.1.3. Categoría Rendimiento 32
4.3.3.1.4. Threat Hunting 33
4.3.4. Análisis de Vulnerabilidades ICETEX 33
4.3.4.1. Resumen de Vulnerabilidades 34
4.3.4.2. Conclusiones Vulnerabilidades 34
4.3.5. REPORTE DE IPS 36
5. GESTION FISICA DE LA EJECUCIÓN 37
6. GESTION PRESUPUESTAL 38
7. GESTION ADMINISTRATIVA 39
8. Servicio De Colaboración 41
8.1. Disponibilidad del servicio – sedes Regionales 42
8.2. Disponibilidad del servicio – sedes Bogotá (aguas - ángel) 42
8.3. Gestión de incidencias y requerimientos – sedes regionales 43
8.4. Gestión de incidencias y requerimientos – Bogotá (Aguas - Angel) 43
9. GESTION DE RIESGOS Y PROBLEMAS 47
10. INDICADORES CLAVE DE DESEMPEÑO 48
10.1. ANS por Disponibilidad de canales de comunicaciones: 48
10.1.1. Canal de Replicación (Triara – Megacenter) 51
10.2. ANS por Disponibilidad de servidores: 51
10.2.1. Disponibilidad TRIARA para los servicios de página web 53
10.2.2. Análisis componente Liferay Producción 61
10.2.2. SERVICIO NFS – BACKUP DE NODOS 1 Y 2 DEL PORTAL ICETEX 64
10.2.3. Backup Servidores Triara 68
11. CONTROL DE CAMBIOS 70
12. PLAN DE TRABAJO DE LOS PROXIMOS MESES 70
14. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC 76
14.1. Aumento de la capacidad de Ancho de Banda en algunas de las sedes de la Entidad 76
14.2. Una capacitación al año de seguridad Informática y servicios conexos 78
14.3. TB de capacidad de almacenamiento 78
14.4. Se oferta Ítem de "Wifi" para la gente en 19 sedes 79

15. CONCLUSIONES 80
16. PENDIENTES 81
16.1. Administrador WEB MASTER 81
16.2. Administrador Networking 81
16.3. Administrador Base de datos 81
16.4. Administrador de aplicaciones 81
16.5. Integrador Nube 82
16.6. Seguridad 82
17. ANEXOS 82
17.1. Almacenamiento 82
17.2. Aplicaciones 82
17.3. Bases De Datos 83
17.4. Ejecución Presupuestal 83
17.5. Seguridad 83
17.6. Soporte Y Monitoreo 84
17.7. Data center Alterno: 84
17.8. Data Center Principal: 85

INDICE DE TABLAS

TABLA 1 CASOS NETWORKING ATENDIDOS EN EL MES-FORMATO ICETEX 14
TABLA 2 CASOS ATENDIDOS NETWORKING COMPARATIVO MES ANTERIOR 14
TABLA 3 CANALES PRUEBAS DE SATURACIÓN EJECUTADAS EN EL MES DE FEBRERO 15
TABLA 4 CANALES PENDIENTES PRUEBAS DE SATURACIÓN 15
TABLA 5 CASOS DE ARANDA APLICACIONES 16
TABLA 6 SERVICIOS REPLICADOS – DATACENTER MEGACENTER 19
TABLA 7 TOP 05 MÁQUINAS MAYOR TASA DE TRANSFERENCIA 20
TABLA 8 TOP 05 MÁQUINAS MENOR TASA DE TRANSFERENCIA 20
TABLA 9 FECHAS CON MENOR REPLICACIÓN 20
TABLA 10 DISTRIBUCIÓN TRIMESTRAL DE REPLICACIÓN 21
TABLA 11 DISPONIBILIDAD DE SERVICIOS DE HOUSING – DATA CENTER ALTERNO 22
TABLA 12 TOP 10 DE LOS PORTALES MÁS UTILIZADOS 29
TABLA 13 COMPARATIVO – INDICADORES DE COMPROMISO 30
TABLA 14 COMPARATIVO ALERTAS DE SEGURIDAD 31
TABLA 15 COMPARATIVO ALERTAS DE DISPONIBILIDAD 32
TABLA 16 COMPARATIVO ALERTAS DE RENDIMIENTO 33
TABLA 17 INVENTARIO DE DISPOSITIVOS 34
TABLA 18 GRUPO ESPECIALISTAS 37
TABLA 19 GRUPO ADMINISTRATIVO 37
TABLA 20 ALIADOS PARA EL PROYECTO 38
TABLA 21 EJECUCIÓN PRESUPUESTAL 39
TABLA 22 DISTRIBUCIÓN MÓDULOS DE VIDEOCONFERENCIA POR SEDE 41
TABLA 23 DISTRIBUCIÓN TRIMESTRAL DE REQUERIMIENTOS Y/O INCIDENTES 47
TABLA 24 NIVEL DE RIESGO 48
TABLA 25 GRADO DE RIESGO 48
TABLA 26 DISPONIBILIDAD DE CANALES 50
TABLA 27 DISPONIBILIDAD CANALES “INTERNET PARA LA GENTE” 51
TABLA 28 DISPONIBILIDAD CANALES “SDWAN” 51
TABLA 29 CÓDIGOS RELACIONADOS DISPONIBILIDAD SERVICIOS EN HOUSING – DATACENTER PRINCIPAL 52
TABLA 30 DISPOSITIVOS EN HOUSING – DATACENTER PRINCIPAL 53
TABLA 31 ACTUALIZACIÓN – ANÁLISIS COMPONENTE LIFERAY FEBRERO 64
TABLA 32 SERVICIO NFS– BACKUP DE NODOS 1 Y 2 DEL PORTAL ICETEX 67
TABLA 33 DISTRIBUCIÓN TRIMESTRAL DE ACCESO POR USUARIOS 68
TABLA 34 DISTRIBUCIÓN TRIMESTRAL DE BACKUP EJECUTADOS 69
TABLA 35 DISTRIBUCIÓN TRIMESTRAL DE BACKUP POR SERVICIOS 70
TABLA 36 CONTROLES DE CAMBIO FEBRERO 70
TABLA 37 PLANES DE TRABAJO 72
TABLA 38 CANALES ANCHOS DE BANDA ACTUALES VRS ANCHOS DE BANDA OFRECIDOS 78
TABLA 39 CAPACIDADES DE ALMACENAMIENTO CONTRATADO 79
TABLA 40 CAPACIDADES DE ALMACENAMIENTO APROVISIONADO 79
TABLA 41 WIFI PARA LA GENTE INSTALADOS 80
TABLA 42 WIFI PARA LA GENTE PENDIENTES 80

INFOTIC
SOLUCIONES INTELIGENTES

INDICE DE ILUSTRACIONES

ILUSTRACIÓN 1 DISPONIBILIDAD DE LAS BASES DE DATOS PRINCIPALES ICTXCYC Y APOTEOSY 17
ILUSTRACIÓN 2 CASOS DEL PROYECTO GESTIONADOS ARANDA BASES DE DATOS 17
ILUSTRACIÓN 3 REPORTES DE REPLICACIÓN SRM A SITIO ALTERNO – FEBRERO 19
ILUSTRACIÓN 4 EVIDENCIA DATAGUARD REPLICADO A MEGACENTER BD 21
ILUSTRACIÓN 5 CONSUMO CANAL MPLS 24
ILUSTRACIÓN 6 CONSUMO CANAL INTERNET SEDES 24
ILUSTRACIÓN 7 CONSUMO CANAL INTERNET DATA CENTER 24
ILUSTRACIÓN 8 FILTRADO – WEB – (FORTIGATE – TRIARA) 25
ILUSTRACIÓN 9 INSPECCIÓN – SSL – (FORTIGATE – TRIARA) 25
ILUSTRACIÓN 10 ANTIVIRUS Y ANTIMALWARE – PERIMETRAL (FORTIGATE – TRIARA) 26
ILUSTRACIÓN 11 CONSUMO CANAL MPLS AGUAS 26
ILUSTRACIÓN 12 CONSUMO CANAL MPLS MEDELLÍN 27
ILUSTRACIÓN 13 CONFIGURACIÓN FORTIWEB 27
ILUSTRACIÓN 14 ESTADO SEGURIDAD SOPHOS 28
ILUSTRACIÓN 15 EVIDENCIA GRÁFICA ESTADÍSTICAS DE PORTALES 29
ILUSTRACIÓN 16 TOTAL DE ALERTAS DE SEGURIDAD 31
ILUSTRACIÓN 17 TOTAL DE ALERTAS DE DISPONIBILIDAD 32
ILUSTRACIÓN 18 TOTAL DE ALERTAS DE RENDIMIENTO 32
ILUSTRACIÓN 19 CANTIDAD TOTAL DE HALLAZGOS IDENTIFICADOS 34
ILUSTRACIÓN 20 DISPONIBILIDAD DE SERVICIO VIDEOCONFERENCIA SEDES REGIONALES – FEBRERO 2025 42
ILUSTRACIÓN 21 DISPONIBILIDAD DE SERVICIO VIDEOCONFERENCIA SEDES BOGOTÁ – FEBRERO 2025 43
ILUSTRACIÓN 22 INCIDENTES / REQUERIMIENTOS SEDES REGIONALES – FEBRERO 2025 43
ILUSTRACIÓN 23 LIMPIEZA OPS SALA 8VO PISO PRESIDENCIA – VISITA FEBRERO 2025 44
ILUSTRACIÓN 24 EVIDENCIA MODULO FUNCIONAL SEDE AGUAS 65” PISO 4 - VISITA FEBRERO 2025 45
ILUSTRACIÓN 25 MODULO FUNCIONAL SEDE AGUAS, UBICACIÓN PISO 6 – VISITA FEBRERO 2025 45
ILUSTRACIÓN 26 LIMPIEZA MODULO SEDE AGUAS 65” PISO 2 – VISITA FEBRERO 2025 46
ILUSTRACIÓN 27 MATRIZ DE RIESGOS 47
ILUSTRACIÓN 28 UPTIME – PORTAL WEB WEB.ICETEX.GOV.CO 53
ILUSTRACIÓN 29 MÉTRICA DE VISITANTES PORTAL WEB WEB.ICETEX.GOV.CO 54
ILUSTRACIÓN 30 MÉTRICA DE USUARIO POR PAÍS - PORTAL WEB WEB.ICETEX.GOV.CO 54
ILUSTRACIÓN 31 NODO 1 – VISTA GENERAL – INR0243 55
ILUSTRACIÓN 32 NODO 1 CPU 56
ILUSTRACIÓN 33 NODO 1 MEMORIA 57
ILUSTRACIÓN 34 NODO 1 ALMACENAMIENTO 57
ILUSTRACIÓN 35 NODO 2 – VISTA GENERAL – INR0242 58
ILUSTRACIÓN 36 NODO 2 CPU 58
ILUSTRACIÓN 37 NODO 2 MEMORIA SWAP 59
ILUSTRACIÓN 38 NODO 2 MEMORIA 60
ILUSTRACIÓN 39 NODO 2 ALMACENAMIENTO 60
ILUSTRACIÓN 40 EVIDENCIA BACKUP SERVIDORES RESUMEN BACKUPS Y SU ESTADO 69

RESUMEN EJECUTIVO

1. Introducción

Este informe contiene la información relacionada con las actividades ejecutadas por INFOTIC y sus aliados en el periodo comprendido entre el 01 al 28 de febrero de 2025, para tal fin se cuenta con la información generada por el grupo de 10 especialistas y 3 profesionales administrativos con los cuales 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 63% que representa los 23 meses que lleva dentro de la fase de Operación el proyecto.

El presente informe del mes de febrero 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 28 de febrero 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 hibrido o multi-nube.

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

3. Alcance

El alcance comprende la descripción de las actividades de los servicios especializados durante el periodo del 01 al 28 de febrero del 2025, conforme a los frentes definidos por el ICETEX, así:

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

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

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

otros a fin de fortalecer la seguridad informática de la Entidad.

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

- **Servicios de nube**
  El informe presenta el estado y detalle de los Servicios de Data Center Principal y Alterno los cuales se encuentra bajo la modalidad de Housing y todos los servicios requeridos para nube privada, dejando claro que a través del contrato se busca integrar servicios de nube pública e hibrida.

- **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.

Respecto al canal de Backup que resta por instalar, se encuentra en gestión y seguimiento permanente con el operador su instalación.

Tanto los casos escalados durante el mes, como el estado del canal que falta por instalar, se describe su estado y análisis en el numeral **4.1.1. Canales instalados en el mes y entregables.**

En este mes se retoman las sesiones de seguimiento para la implementación de IPv6 para el año 2025, el avance de los compromisos de igual forma se relaciona en el numeral **12. Plan de trabajo de los próximos meses**.

4.1.1. Canales instalados en el mes y entregables

Durante el presente mes no se realizó la instalación de ningún canal nuevo de comunicaciones, se continúa con la siguiente estadística con respecto a canales:

- De 38 canales MPLS principales contemplados en la línea base, se encuentran instalados 35 canales, de los tres faltantes dos corresponden a sedes donde ICETEX aún no cuenta con Oficinas (Barrancabermeja y San Gil), y uno corresponde a un canal adicional Canal entre Sitio principal e ICETEX - Dirección General – Aguas, el cual fue descartada su instalación por parte de ICETEX.

En conclusión, a la fecha se encuentran instalados el 100% de canales principales de comunicaciones en las sedes contempladas en el contrato.

- De 30 canales de Backups contemplados en la línea base se encuentran instalados 28, de los dos faltantes uno corresponde al Backup de la oficina de Quibdó del cual se ha retrasado su instalación por temas administrativos del centro comercial donde se encuentra la Oficina y el otro corresponde a un canal adicional Canal de Backup entre Sitio principal e ICETEX - Dirección General – Aguas, el cual fue descartada su instalación por parte de ICETEX.

En conclusión, se tiene el 96.55% de los canales Backups instalados y en proceso de instalación un canal restante.

- El servicio de "internet para la gente" se encuentra instalado en las 14 sedes solicitados en el anexo técnico.

En conclusión, se tiene el 100% de los servicios de Internet para la gente contempladas en la línea base.

- Los anchos de banda de acuerdo con las condiciones de servicio ofrecidas se encuentran al 100% cumplidos.

En conclusión, los canales instalados cuentan con el 100% del ancho de banda contratado. A través de la herramienta SolarWinds se realiza el monitoreo mensual de disponibilidad de los canales y se genera el respectivo informe, el cual puede consultarse en el siguiente link: Reporte Mensual Disponibilidad INFOTIC Febrero 2025.pdf

4.1.1.1. Solicitudes Nuevas Instalación de canales:

Se tiene las siguientes solicitudes de instalación de nuevos canales:

- (1) canal de datos principal para una nueva sede en la ciudad de Puerto Carreño -Vichada, INFOTIC remitió a ICETEX la cotización para su revisión y aprobación, una vez se tenga la aceptación se procederá a coordinar la instalación del canal.

- (5) Servicios de Internet para la gente para las sedes de Manizales, Armenia, Cartagena, Sincelejo y Pasto, los cuales se encuentran en proceso se viabilidad por parte del operador para poder tener una oferta comercial.

Los casos atendidos durante el mes están disponibles en la tabla a continuación (en el link Registro Aranda Febrero 2025.xlsx), además se puede acceder a un mayor nivel de detalle a través de la herramienta Aranda:

FECHA Y HORA DEL REPORTE	LUGAR CON LA FALLA	Código de servicio	NÚMERO DE CASO	DURACIÓN HHH:mm:ss
25/02/2025 15:21	Caida de nodo INR0139 / 000333 /SDWAN-MOCOA / PUTUMAYO / CALLE 8 NO. 7-40 at Tuesday, February 25, 2025 10:59 a.m.	INR0139 / 000333	IM-295597-4-82946	04:00:00
25/02/2025 14:49	Descubre lo que sucede en toda la organización.		IM-295584-4-82943	04:00:00
25/02/2025 14:00	Caida de nodo INR0139 / 000333 /SDWAN-MOCOA / PUTUMAYO / CALLE 8 NO. 7-40 at Tuesday, February 25, 2025 9:35 a.m.	INR0139 / 000333	IM-295576-4-82938	04:00:00

25/02/2025 03:19	Caida de nodo INR0139 / 000333 /SDWAN-MOCOA / PUTUMAYO / CALLE 8 NO. 7-40 at Monday, February 24, 2025 10:58 p.m.	INR0139 / 000333	IM-295538-4-82925	04:00:01
25/02/2025 00:12	Caida de nodo INR0144 - APARTADO ICETEX - CARRERA 100 NO. 103ª -2 - PPAL at Monday, February 24, 2025 7:51 p.m.	INR0144	IM-295521-4-82909	04:00:01
24/02/2025 22:12	Caida de nodo INR0144 - APARTADO ICETEX - CARRERA 100 NO. 103ª -2 - PPAL at Monday, February 24, 2025 5:51 p.m.	INR0144	IM-295508-4-82900	04:00:00
24/02/2025 22:12	Caida de nodo INR0264 - BOGOTA ICETEX - DC TRIARA // INTERNET // PPAL at Monday, February 24, 2025 5:51 p.m.	INR0264	IM-295507-4-82899	04:00:00
24/02/2025 22:12	Caida de nodo INR0152 - SANTA MARTA ICETEX- CARRERA 3 NO. 14-16 -BACKUP at Monday, February 24, 2025 5:51 p.m.	INR0152	IM-295506-4-82898	04:00:00
24/02/2025 21:53	Caida de nodo INR0039 - NEIVA ICETEX - CR 5 # 10 - 38 - PPAL at Monday, February 24, 2025 5:27 p.m.	INR0039	IM-295501-4-82897	04:00:00
24/02/2025 21:52	Caida de nodo INR0077 - PEREIRA ICETEX - CALLE 19 NO. 8-34- BACKUP at Monday, February 24, 2025 5:27 p.m.	INR0077	IM-295500-4-82896	04:00:00
20/02/2025 16:22	Caida de nodo INR0000378 // LETICIA -INTERNET - WIFI// Calle 9 # 7-55 59 Local 3 at Thursday, February 20, 2025 12:01 p.m.	INR0000378	IM-295192-4-82826	04:00:00
20/02/2025 16:22	Caida de nodo INR0000374//LETICIA - SDWAN//Calle 9 # 7-55 59 Local 3 at Thursday, February 20, 2025 12:01 p.m.	INR0000374	IM-295191-4-82825	04:00:00
20/02/2025 16:22	Caida de nodo INR0000373 / LETICIA-MPLS // Calle 9 # 7-55 59 Local 3 at Thursday, February 20, 2025 12:01 p.m.	INR0000373	IM-295190-4-82824	04:00:00
19/02/2025 16:42	Caida de nodo INR0077 - PEREIRA ICETEX - CALLE 19 NO. 8-34- BACKUP at Wednesday, February 19, 2025 12:18 p.m.	INR0077	IM-295074-4-82798	04:00:00
19/02/2025 16:34	Caida de nodo INR0039 - NEIVA ICETEX - CR 5 # 10 - 38 - PPAL at Wednesday, February 19, 2025 12:09 p.m.	INR0039	IM-295071-4-82797	04:00:00
19/02/2025 15:43	Caida de nodo INR0034 - BOGOTA ICETEX - Carrera 3 No. 18-32 - Sede Aguas - INTERNET at Wednesday, February 19, 2025 11:21 a.m.	INR0034	IM-295054-4-82788	04:00:00
19/02/2025 15:42	Caida de nodo INR0039 - NEIVA ICETEX - CR 5 # 10 - 38 - PPAL at Wednesday, February 19, 2025 11:21 a.m.	INR0039	IM-295053-4-82787	04:00:00
18/02/2025 14:33	Internet/Redes >> Inc Falla de Conectividad a la Red		IM-294939-4-82759	04:00:00
18/02/2025 14:22	Descubre lo que sucede en toda la organización.		IM-294936-4-82758	04:00:00
17/02/2025 18:31	Caida de nodo INR0000373 / LETICIA-MPLS // Calle 9 # 7-55 59 Local 3 at Monday, February 17, 2025 2:09 p.m.	INR0000373	IM-294862-4-82747	04:00:00
17/02/2025 18:31	Caida de nodo INR0000374//LETICIA - SDWAN//Calle 9 # 7-55 59 Local 3 at Monday, February 17, 2025 2:09 p.m.	INR0000374	IM-294861-4-82746	04:00:00
17/02/2025 18:30	Caida de nodo INR0000378 // LETICIA -INTERNET - WIFI// Calle 9 # 7-55 59 Local 3 at Monday, February 17, 2025 2:09 p.m.	INR0000378	IM-294857-4-82743	04:00:00
17/02/2025 15:00	Active Cisco Spaces para comenzar su recorrido		IM-294829-4-82741	04:00:00
14/02/2025 14:21	Caida de nodo INR0088 - ICETEX MANIZALES - Calle 23 No. 23-16 Piso 3 - Edif. Caja Social de Ahorros - PPAL at Friday, February 14, 2025 9:59 a.m.	INR0088	IM-294707-4-82720	04:00:00
13/02/2025 16:32	Internet/Redes >> Inc Degradación del Servicio 8365		IM-294641-4-82713	04:00:00
13/02/2025 15:03	Internet/Redes >> Inc Degradación del Servicio		IM-294616-4-82710	04:00:00
13/02/2025 14:43	Caida de nodo INR0000373 / LETICIA-MPLS // Calle 9 # 7-55 59 Local 3 at Thursday, February 13, 2025 10:22 a.m.	INR0000373	IM-294612-4-82709	04:00:00

13/02/2025 14:40	Caida de nodo INR0000374//LETICIA - SDWAN//Calle 9 # 7-55 59 Local 3 at Thursday, February 13, 2025 10:19 a.m.	INR0000374	IM-294610-4-82708	04:00:00
13/02/2025 14:39	Caida de nodo INR0000378 // LETICIA -INTERNET - WIFI// Calle 9 # 7-55 59 Local 3 at Thursday, February 13, 2025 10:19 a.m.	INR0000378	IM-294609-4-82707	04:00:00
13/02/2025 05:04	Caida de nodo INR0000378 // LETICIA -INTERNET - WIFI// Calle 9 # 7-55 59 Local 3 at Thursday, February 13, 2025 12:43 a.m.	INR0000378	IM-294592-4-82704	04:00:00
13/02/2025 04:57	Caida de nodo INR0000374//LETICIA - SDWAN//Calle 9 # 7-55 59 Local 3 at Thursday, February 13, 2025 12:37 a.m.	INR0000374	IM-294591-4-82703	04:00:00
12/02/2025 16:57	Caida de nodo INR0000378 // LETICIA -INTERNET - WIFI// Calle 9 # 7-55 59 Local 3 at Wednesday, February 12, 2025 12:35 p.m.	INR0000378	IM-294517-4-82681	04:00:00
12/02/2025 16:57	Caida de nodo INR0000373 / LETICIA-MPLS // Calle 9 # 7-55 59 Local 3 at Wednesday, February 12, 2025 12:35 p.m.	INR0000378	IM-294516-4-82680	04:00:00
12/02/2025 16:55	Caida de nodo INR0000374//LETICIA - SDWAN//Calle 9 # 7-55 59 Local 3 at Wednesday, February 12, 2025 12:32 p.m.	INR0000378	IM-294515-4-82679	04:00:00
12/02/2025 15:41	Inc Falla Conexión al Portal Icetex		IM-294503-4-82678	04:00:00
11/02/2025 14:36	Descubre lo que sucede en toda la organización.		IM-294388-4-82657	04:00:00
11/02/2025 00:40	Caida de nodo INR0147 - TUMACO - Carrera 34 calle 3B Los Pinos at Monday, February 10, 2025 8:19 p.m.	INR0147	IM-294356-4-82648	04:00:01
10/02/2025 21:21	Caida de nodo INR0039 - NEIVA ICETEX - CR 5 # 10 - 38 - PPAL at Monday, February 10, 2025 4:37 p.m.	INR0039	IM-294343-4-82646	04:00:00
10/02/2025 20:58	Caida de nodo INR0041 // NEIVA ICETEX // CR 5 # 10 - 38 - BACKUP at Monday, February 10, 2025 4:37 p.m.	INR0041	IM-294337-4-82643	04:00:00
10/02/2025 20:29	Caida de nodo INR0000374//LETICIA - SDWAN//Calle 9 # 7-55 59 Local 3 at Monday, February 10, 2025 4:07 p.m.	INR0000378	IM-294333-4-82641	04:00:00
10/02/2025 20:28	Caida de nodo INR0000373 / LETICIA-MPLS // Calle 9 # 7-55 59 Local 3 at Monday, February 10, 2025 4:07 p.m.	INR0000378	IM-294332-4-82640	04:00:00
10/02/2025 20:24	Caida de nodo INR0000378 // LETICIA -INTERNET - WIFI// Calle 9 # 7-55 59 Local 3 at Monday, February 10, 2025 4:04 p.m.	INR0000378	IM-294331-4-82639	04:00:00
10/02/2025 15:55	Caida de nodo INR0000378 // LETICIA -INTERNET - WIFI// Calle 9 # 7-55 59 Local 3 at Monday, February 10, 2025 11:31 a.m.	INR0000378	IM-294272-4-82619	04:00:00
10/02/2025 15:01	Internet/Redes >> Inc Falla Conectividad Red WIFI Corporativa-Falla internet CEP Leticia	INR0000378	IM-294237-4-82607	04:00:00
10/02/2025 13:55	Caida de nodo INR0000373 / LETICIA-MPLS // Calle 9 # 7-55 59 Local 3 at Monday, February 10, 2025 9:34 a.m.	INR0000378	IM-294223-4-82604	04:00:00
10/02/2025 13:53	Caida de nodo INR0000378 // LETICIA -INTERNET - WIFI// Calle 9 # 7-55 59 Local 3 at Monday, February 10, 2025 9:31 a.m.	INR0000378	IM-294222-4-82603	04:00:00
10/02/2025 13:51	Caida de nodo INR0000374//LETICIA - SDWAN//Calle 9 # 7-55 59 Local 3 at Monday, February 10, 2025 9:31 a.m.	INR0000378	IM-294221-4-82602	04:00:00
10/02/2025 12:54	Internet/Redes >> Inc Falla Conectividad Red WIFI Corporativa -Sin conexión a internet CEP Sincelejo - Centro	INR0095	IM-294198-4-82594	04:00:00
10/02/2025 09:45	Medellin >> Evento de afectación de servicio.	INR0133	IM-294163-4-82581	04:00:00
10/02/2025 08:43	Caida de nodo INR0000373 / LETICIA-MPLS // Calle 9 # 7-55 59 Local 3 at Monday, February 10, 2025 4:21 a.m.	INR0000378	IM-294162-4-82580	04:00:00

10/02/2025 07:54	Caida de nodo INR0000373 / LETICIA-MPLS // Calle 9 # 7-55 59 Local 3 at Monday, February 10, 2025 3:33 a.m.	INR0000378	IM-294161-4-82579	04:00:00
10/02/2025 07:52	Caida de nodo INR0000378 // LETICIA -INTERNET - WIFI// Calle 9 # 7-55 59 Local 3 at Monday, February 10, 2025 3:30 a.m.	INR0000378	IM-294160-4-82578	04:00:00
10/02/2025 07:51	Caida de nodo INR0000374//LETICIA - SDWAN//Calle 9 # 7-55 59 Local 3 at Monday, February 10, 2025 3:30 a.m.	INR0000378	IM-294159-4-82577	04:00:00
10/02/2025 05:30	Caida de nodo INR0000373 / LETICIA-MPLS // Calle 9 # 7-55 59 Local 3 at Monday, February 10, 2025 1:09 a.m.	INR0000378	IM-294158-4-82576	04:00:00
10/02/2025 05:27	Caida de nodo INR0000374//LETICIA - SDWAN//Calle 9 # 7-55 59 Local 3 at Monday, February 10, 2025 1:06 a.m.	INR0000378	IM-294157-4-82575	04:00:00
10/02/2025 05:27	Caida de nodo INR0000378 // LETICIA -INTERNET - WIFI// Calle 9 # 7-55 59 Local 3 at Monday, February 10, 2025 1:06 a.m.	INR0000378	IM-294156-4-82574	04:00:00
09/02/2025 19:53	Caida de nodo INR0000373 / LETICIA-MPLS // Calle 9 # 7-55 59 Local 3 at Sunday, February 9, 2025 3:33 p.m.	INR0000378	IM-294154-4-82573	04:00:00
09/02/2025 19:53	Caida de nodo INR0000378 // LETICIA -INTERNET - WIFI// Calle 9 # 7-55 59 Local 3 at Sunday, February 9, 2025 3:33 p.m.	INR0000378	IM-294153-4-82572	04:00:00
09/02/2025 19:50	Caida de nodo INR0000374//LETICIA - SDWAN//Calle 9 # 7-55 59 Local 3 at Sunday, February 9, 2025 3:30 p.m.	INR0000378	IM-294152-4-82571	04:00:00
09/02/2025 13:50	Caida de nodo INR0000374//LETICIA - SDWAN//Calle 9 # 7-55 59 Local 3 at Sunday, February 9, 2025 9:29 a.m.	INR0000378	IM-294150-4-82570	04:00:00
09/02/2025 12:14	Caida de nodo INR0000374//LETICIA - SDWAN//Calle 9 # 7-55 59 Local 3 at Sunday, February 9, 2025 7:53 a.m.	INR0000378	IM-294149-4-82569	04:00:00
09/02/2025 07:54	Caida de nodo INR0000378 // LETICIA -INTERNET - WIFI// Calle 9 # 7-55 59 Local 3 at Sunday, February 9, 2025 3:32 a.m.	INR0000378	IM-294148-4-82568	04:00:00
09/02/2025 07:53	Caida de nodo INR0000373 / LETICIA-MPLS // Calle 9 # 7-55 59 Local 3 at Sunday, February 9, 2025 3:32 a.m.	INR0000378	IM-294147-4-82567	04:00:00
09/02/2025 07:51	Caida de nodo INR0000374//LETICIA - SDWAN//Calle 9 # 7-55 59 Local 3 at Sunday, February 9, 2025 3:29 a.m.	INR0000378	IM-294146-4-82566	04:00:00
09/02/2025 01:53	Caida de nodo INR0000373 / LETICIA-MPLS // Calle 9 # 7-55 59 Local 3 at Saturday, February 8, 2025 9:32 p.m.	INR0000378	IM-294145-4-82565	04:00:01
09/02/2025 01:53	Caida de nodo INR0000374//LETICIA - SDWAN//Calle 9 # 7-55 59 Local 3 at Saturday, February 8, 2025 9:32 p.m.	INR0000378	IM-294144-4-82564	04:00:01
09/02/2025 01:53	Caida de nodo INR0000378 // LETICIA -INTERNET - WIFI// Calle 9 # 7-55 59 Local 3 at Saturday, February 8, 2025 9:32 p.m.	INR0000378	IM-294143-4-82563	04:00:01
08/02/2025 07:54	Caida de nodo INR0000373 / LETICIA-MPLS // Calle 9 # 7-55 59 Local 3 at Saturday, February 8, 2025 3:34 a.m.	INR0000378	IM-294141-4-82562	04:00:00
08/02/2025 07:52	Caida de nodo INR0000378 // LETICIA -INTERNET - WIFI// Calle 9 # 7-55 59 Local 3 at Saturday, February 8, 2025 3:31 a.m.	INR0000378	IM-294140-4-82561	04:00:00
08/02/2025 07:52	Caida de nodo INR0000374//LETICIA - SDWAN//Calle 9 # 7-55 59 Local 3 at Saturday, February 8, 2025 3:31 a.m.	INR0000378	IM-294139-4-82560	04:00:00
07/02/2025 23:57	Caida de nodo INR0133 / MEDELLIN ICETEX / Calle 52 #47-42 oficina 1002 piso 10 edificio Coltejer - PPAL at Friday, February 7, 2025 7:37 p.m.	INR0133	IM-294135-4-82559	04:00:00

07/02/2025 23:55	Caida de nodo INR0122 - MEDELLIN ICETEX - Calle 52 #47-42 oficina 1002 piso 10 edificio Coltejer - INTERNET PARA LA GENTE at Friday, February 7, 2025 7:34 p.m.	INR0133	IM-294134-4-82558	04:00:00
07/02/2025 21:18	Caida de nodo INR0144 - APARTADO ICETEX - CARRERA 100 NO. 103ª -2 - PPAL at Friday, February 7, 2025 4:57 p.m.	INR0144	IM-294125-4-82556	04:00:00
07/02/2025 21:18	Caida de nodo INR0140 // APARTADO ICETEX // Carrera 100 No. 103ª -2 - INTERNET at Friday, February 7, 2025 4:57 p.m.	INR0140	IM-294124-4-82555	04:00:00
07/02/2025 20:07	Internet/Redes >> Inc Falla de Conectividad a la Red		IM-294116-4-82553	04:00:00
07/02/2025 19:34	Caida de nodo INR0147 - TUMACO - Carrera 34 calle 3B Los Pinos at Friday, February 7, 2025 3:12 p.m.	INR0147	IM-294108-4-82550	04:00:00
07/02/2025 18:00	Caida de nodo INR0147 - TUMACO - Carrera 34 calle 3B Los Pinos at Friday, February 7, 2025 1:39 p.m.	INR0147	IM-294101-4-82547	04:00:00
07/02/2025 15:57	Caida de nodo INR0147 - TUMACO - Carrera 34 calle 3B Los Pinos at Friday, February 7, 2025 11:36 a.m.	INR0147	IM-294077-4-82542	04:00:00
07/02/2025 15:11	Caida de nodo INR0147 - TUMACO - Carrera 34 calle 3B Los Pinos at Friday, February 7, 2025 10:51 a.m.	INR0147	IM-294068-4-82538	04:00:00
07/02/2025 14:38	Caida de nodo INR0147 - TUMACO - Carrera 34 calle 3B Los Pinos at Friday, February 7, 2025 10:18 a.m.	INR0147	IM-294059-4-82537	04:00:00
07/02/2025 13:41	Caida de nodo INR0147 - TUMACO - Carrera 34 calle 3B Los Pinos at Friday, February 7, 2025 9:21 a.m.	INR0147	IM-294049-4-82535	04:00:00
07/02/2025 13:17	Caida de nodo INR0147 - TUMACO - Carrera 34 calle 3B Los Pinos at Friday, February 7, 2025 8:57 a.m.	INR0147	IM-294041-4-82533	04:00:00
04/02/2025 14:43	Internet/Redes >> Inc Falla de Conectividad a la Red		IM-293718-4-82416	04:00:00
04/02/2025 13:14	Caida de nodo INR0021-QUIBDO-CL30 AVENIDA AEROPUERTO-ICETEX QUIBDO-Internet at Tuesday, February 4, 2025 8:53 a.m.	INR0021	IM-293697-4-82407	04:00:00
04/02/2025 13:14	Caida de nodo INR0014-ICETEX QUIBDO-Calle 30 Avenida Aeropuerto-Icetex Quibdo Canal_Priincipal at Tuesday, February 4, 2025 8:53 a.m.	INR0014	IM-293696-4-82406	04:00:00
02/02/2025 13:50	Caida de nodo INR0081 - MONTERIA ICETEX - CARRERA 31 NO. 4-47PISO 5 - BACKUP at Sunday, February 2, 2025 9:30 a.m.	INR0081	IM-293546-4-82347	04:00:00
02/02/2025 13:49	Caida de nodo INR0080 - MONTERIA ICETEX - CARRERA 31 NO. 4-47PISO 5 - PPAL at Sunday, February 2, 2025 9:27 a.m.	INR0080	IM-293545-4-82346	04:00:00

Tabla 1 Casos Networking atendidos en el mes-Formato ICETEX

Todos los casos fueron gestionados exclusivamente a través de la herramienta Aranda, sin que se registrara atención por otros medios. En comparación con el mes anterior no hubo variación, todos los casos fueron atribuidos a fallos en el servicio por parte del proveedor.

Mes	No. Casos
Febrero 2025	87
Enero 2025	14

Tabla 2 Casos atendidos Networking comparativo mes anterior

4.1.2. Pruebas de Saturación Bidireccionales

Se continua con la realización de las pruebas de saturación bidireccionales, durante el mes de febrero se realizaron dos pruebas de saturación de canales, cuya evidencia se puede consultar en el siguiente link: Prueba de Saturación Febrero

El cronograma de ejecución se continúa enviando semanalmente al ICETEX.

INR	ENLACE	SEDE	Fecha de Saturación	Pruebas de saturación
INR0084	BACKUP	VILLAVICENCIO	12/02/2025	ok
INR0147	PRINCIPAL	TUMACO	12/02/2025	ok
INR0152	BACKUP	SANTA MARTA	12/02/2025	ok
INR0153	BACKUP	CALI	12/02/2025	ok
INR0154	PRINCIPAL	SANTA MARTA	12/02/2025	ok

Tabla 3 Canales pruebas de saturación ejecutadas en el mes de febrero

INR	ENLACE	SEDE
INR0036	BACKUP	AGUAS
INR0037	PRINCIPAL	AGUAS
INR0074	PRINCIPAL	ARMENIA
INR0076	BACKUP	IBAGUE
INR0077	BACKUP	PEREIRA
INR0107	BACKUP	CARTAGENA
INR0273	BACKUP	ANGEL

Tabla 4 Canales pendientes pruebas de saturación

En resumen, se ha alcanzado un **88.88%** de pruebas de saturación hasta el 28 de febrero del 2025.

No se ejecutó el cambio 1116 el 08 de febrero de 2025 (Salida de los portales https://portal.ICETEX.gov.co/portal y www.ICETEX.gov.co) porque se debían realizar unos ajustes previos los cuales realizaron y se debió formalizar mediante un nuevo control de cambios 1128, el cual fue aprobado para ser ejecutado el 15 de marzo del 2025.

4.2. Centro de Datos

4.2.1. Centro de Datos Principal

4.2.1.1. Aplicaciones

En cuanto a la gestión y soporte técnico de las aplicaciones institucionales, se atendieron y solucionaron cinco (5) casos registrados en la herramienta de mesa de servicio Aranda, clasificados en dos categorías: **Gestión de permisos FTP** y **Gestión de incidentes y accesos**.

A continuación, se detalla el alcance y evidencias de los casos atendidos y solucionados en el mes:

#	Fecha	Actividad	Estado	Evidencias
1	03/02/2025	Tarea 515784 Cambio 1120 – Actualización appsetting.json Backend Portal transaccional	Solucionado	Tarea 515784 Cambio 1120 – Actualización appsetting.json Backend Portal transaccional.pdf

2	03/02/2025	Incidente 82366 Falla en descargue del recibo de fondo de garantías	Solucionado	Incidente 82366 Falla en descargue del recibo de fondo de garantias.pdf
3	04/02/2025	Tarea 515961 Cambio 1121 – Actualización Servicio Migración Icetex Integración FSD	Solucionado	Tarea 515961 Cambio 1121 – Actualizacion Servicio Migración Icetex Integración FSD.pdf
4	04/02/2025	Tarea 515962 Cambio 1112 – Actualización Aplicación apisolicitudes	Solucionado	Tarea 515962 Cambio 1112 – Actualización Aplicación apisolicitudes.pdf
5	14/02/2025	Tarea 516477 – Cambio 1123 – Copia de seguridad Archivos Aplicación Subfondo IES prod (Ws WsAdministrativaFondoCovid19)	Solucionado	Tarea 516477 – Cambio 1123 – Copia de seguridad Archivos Aplicación Subfondo IES prod (Ws WsAdministrativaFondoCovid19).pdf
6	14/02/2025	Tarea 516478 – Cambio 1123 – actualización Aplicación Subfondo IES prod (Ws WsAdministrativaFondoCovid19)	Solucionado	Tarea 516478 – Cambio 1123 – Actualizacion Aplicación Subfondo IES prod (Ws WsAdministrativaFondoCovid19) - 14022025.pdf
7	18/02/2025	Tarea 516691 Requerimiento 17396 – Permisos FTP Usuario OCI	Solucionado	Tarea 516691 Requerimiento 17396 – Permisos FTP Usuario OCI.pdf
8	18/02/2025	Tarea 516701 Cambio 17237 – Permisos FTP Usuario OCM	Solucionado	Tarea 516701 Cambio 17237 – Permisos FTP Usuario OCM.pdf
9	19/02/2025	Requerimiento 100996 – Validación Acceso a proyectos pago Anticipado Pruebas	Solucionado	Requerimiento 100996 – Validación Acceso a proyectos pago Anticipado Pruebas.pdf
10	19/02/2025	Requerimiento 101043 – Ajuste del archivo Condiciones2021.asp en Servidor MIRA y C&cetex	Solucionado	Requerimiento 101043 – Ajuste del archivo Condiciones2021.asp en Servidor MIRA y C&cetex.pdf
11	20/02/2025	Tarea 516754 Cambio 1119 – Actualización Backend Aplicación SarlaftApi	Solucionado	Tarea 516754 Cambio 1119 – Actualización Backend Aplicación SarlaftApi.pdf
12	20/02/2025	Tarea 516755 Cambio 1119 – Actualización Aplicación SarlaftFront	Solucionado	Tarea 516755 Cambio 1119 – Actualización Aplicación SarlaftFront.pdf
13	21/02/2025	Incidente 82853 – Caída de C&CETEX Intranet	Solucionado	Incidente 82853 – Caída de C&CETEX Intranet.pdf

Tabla 5 casos de Aranda aplicaciones

Adicional durante el mes, se han llevado a cabo varias actividades, tales como:

1. INFORME DEL ESTADO ACTUAL DE SERVIDORES DE APLICACIÓN ICETEX.pdf
2. FALLA APLICACIÓN TRASUNION.pdf
3. DEPURACION LOGS SERVIDOR ICTXSRVNETCOR01.pdf

4.2.1.2. Bases de Datos

- En cuanto a la atención de solicitudes de usuarios, se resolvieron 456 casos asignados a los administradores de base de datos en febrero de 2025 en los tiempos estipulados por prioridad.

- Los casos atendidos en el mes de febrero disminuyeron en un 14.77% respecto al mes de enero, dicha reducción se presenta a la disminución de las convocatorias que la entidad está ejecutando.
- Disponibilidad del Clusterware BD para el mes de FEBRERO 2025 100% como se evidencia en la siguiente ilustración:

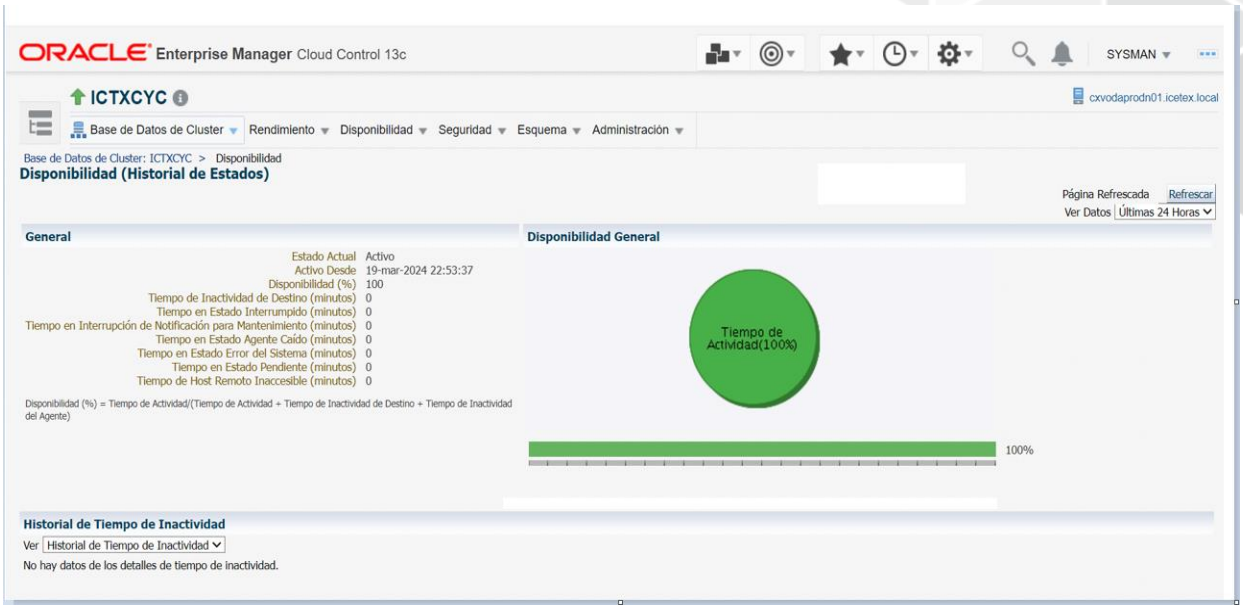


Ilustración 1 Disponibilidad de las Bases de Datos principales ICTXCYC y APOTEOSY

- 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 realizaron ajustes base de datos de sgdea apoteosys pruebas.

- Se generaron los logs de auditoria base de datos core.

- Se solicitó a la gerencia la gestión con el proveedor Claro para generar solicitudes de restauración de backups tanto de los servers de producción donde se alojan las BD's como de las copias de rman que se están tomando a cintas con el fin de dejar claro el procedimiento en caso de contingencia.

Casos del proyecto Gestionados por Bases de datos:

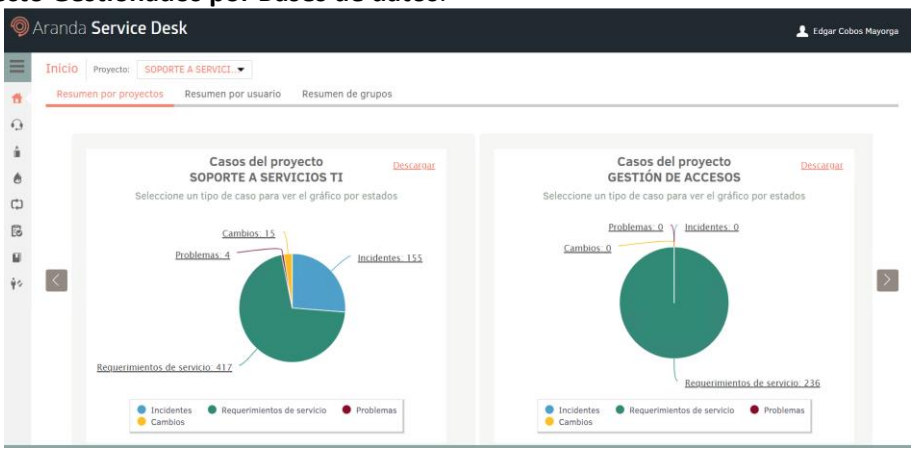


Ilustración 2 Casos del proyecto Gestionados Aranda Bases de datos

Desde Bases de datos se tienen las siguientes recomendaciones:

Almacenamiento:

- 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.

- Se debe aprovisionar más almacenamiento para las bases de datos de producción ya que se encuentra en estado crítico, solo queda disponibles 289G.

Antivirus:

- El antivirus de Symantec en las bases de datos sigue inactivo, hasta no tener claro las parametrizaciones de restricción y los problemas ocasionados de conexión.

Se coordinarán y definirán acciones y responsables para determinar lo requerido para habilitar este antivirus a nivel del server de BD.

Permisos de usuarios en las bases de datos:

- Sigue pendiente retirar permiso de sudo a los usuarios infotic, gawuser y dcscaf con esto usuarios podrían realizar actividades administrativas que no van con su rol.

Se gestionará con ICETEX un trabajo conjunto para que nos definan los roles necesarios y poder realizar los ajustes sobre los mismos.

4.2.2. Centro de Datos Alterno

4.2.2.1. Hosting Virtual (IaaS)

En el transcurso del mes de febrero, se mantuvo en constante replicación las máquinas virtuales configuradas, estos servidores se replicaron desde el origen en data center Triara hasta el data center 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 Febrero 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 **13** replicas

General

Name	Count
OK	12
Not Active	1

Grupo de protección: PG_INFOTIC_7 (1)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0226_INFOTIC_REP	OK	5 of 5	Feb 28, 2025	24.32 MB	5 minutes

Grupo de protección: PG_INFOTIC_6 (2)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0228_INFOTIC_REP	OK	1 of 1	Feb 28, 2025	60.75 MB	1 hour
INR0229_INFOTIC_REP	OK	1 of 1	Feb 28, 2025	92.46 MB	1 hour

Grupo de protección: PG_INFOTIC_1 (2)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0233_INFOTIC_REP	OK	6 of 6	Feb 28, 2025	8.42 MB	30 minutes
INR0262_INFOTIC_REP	OK	1 of 1	Feb 28, 2025	7.4 MB	1 hour

Grupo de protección: PG_INFOTIC_5 (1)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0236_INFOTIC_REP	Not Active	2 of 2	Dec 12, 2024	62.77 MB	2 hours

Grupo de protección: PG_INFOTIC_4 (4)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0237_INFOTIC_REP	OK	2 of 2	Feb 28, 2025	11 MB	5 minutes
INR0238_INFOTIC_REP	OK	2 of 2	Feb 28, 2025	1.78 GB	1 hour
INR0239_INFOTIC_REP	OK	2 of 2	Feb 28, 2025	68.33 MB	1 hour
INR0243_INFOTIC_REP	OK	2 of 2	Feb 28, 2025	443.67 MB	1 hour

Grupo de protección: PG_INFOTIC_3 (2)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO

Ilustración 3 Reportes de replicación SRM a Sitio Alterno – febrero

A continuación, se detallan los servidores con sus correspondientes servicios los cuales están siendo replicados a Megacenter:

No.	INR Replicación	Host name	Servicio	VirtualMachine MEGACENTER
1	INR0204	icetexbogwsmira	Portal Web	INR0226_INFOTIC_REP
2	INR0207	ictxsisgesbd	Sisgestion	INR0228_INFOTIC_REP
3	INR0206	ictxsisgesapp	Sisgestion	INR0229_INFOTIC_REP
4	INR0220	icetexboglxorfeo1	ORFEO	INR0233_INFOTIC_REP
5	INR0219	icetexboglxorfeo2	ORFEO	INR0262_INFOTIC_REP
6	INR0208	ICTXBOGSRVPT1	Portal Transaccional	INR0236_INFOTIC_REP
7	INR0209	icetexbogbalserver1	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	icetexboglxxroad1	XROAD	INR0249_INFOTIC_REP

Tabla 6 Servicios replicados – Datacenter Megacenter

Se tienen las siguientes conclusiones de la replicación para este mes:

- Se presentó el **Not Active** en la maquina **INR0236_INFOTIC_REP** durante todo el mes debido a que la maquina se dejó de replicar porque ICETEX solicitó dar de baja la máquina de producción y redistribuir

sus recursos, pero se debe mantener el pago porque se encuentra aprovisionada.

- No se presenta información de los días 02, 12, 14 y 16 de febrero, esto debido a que la herramienta no generó el reporte, pero se realizó la replicación correspondiente.

- Se realizó la replicación de 12 máquinas virtuales durante todos los días del mes de febrero 2025.

- Para el mes de febrero se tiene el siguiente TOP 5 de las maquinas con mayor tasa de transferencia fueron:

INR	HOSTNAME	MB
INR0238	icetexbogliferaynfs	16765.66
INR0226	icetexbogwsmira	5966.83
INR0243	icetexbogliferayserver1	3805.02
INR0229	ictxsisgesapp	2010.79
INR0228	ictxsisgesbd	1355.1

Tabla 7 TOP 05 máquinas mayor tasa de transferencia

- Se tiene el siguiente TOP 5 de las maquinas con menor tasa de transferencia fueron:

INR	HOSTNAME	MB
INR0249	icetexboglxxroad1	790.46
INR0237	icetexbogbalserver1	391.82
INR0262	icetexboglxorfeo2	266.72
INR0233	icetexboglxorfeo1	225.04
INR0245	icetexboglxdarumasrv2	81.89

Tabla 8 TOP 05 máquinas menor tasa de transferencia

- Los siguientes son las fechas en que se presentó menor replicación de la información a nivel de la replicación que se realiza entre los data center:

Fecha	día	MB
Febrero 13	Lunes	396.69
Febrero 17	Viernes	476.53
Febrero 11	Sábado	529.01
Febrero 9	Jueves	655.91
Febrero 10	Viernes	672.75
Febrero 26	Domingo	745.78
Febrero 3	Viernes	820.31
Febrero 6	Lunes	854.08
Febrero 23	Jueves	996.09
Febrero 21	Martes	1116.91

Tabla 9 Fechas con menor replicación

- Durante el último trimestre la replicación que se realiza entre el data center principal TRIARA y el data center alterno MEGACENTER tuvo un promedio de transferencia de data de 40370 MB y se presenta una disminución de 33.70% entre diciembre y febrero, que equivale a 17123.26 MB.

Mes	MB replicadas
Diciembre	50815.07
Enero	36605.64
Febrero	33691.81

Tabla 10 Distribución trimestral de replicación

4.2.2.2. Dataguard Bases de Datos Megacenter

Durante el mes de febrero 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 INFOTIC_ICETEX - Evidencias Dataguard Megacenter febrero 2025.pdf

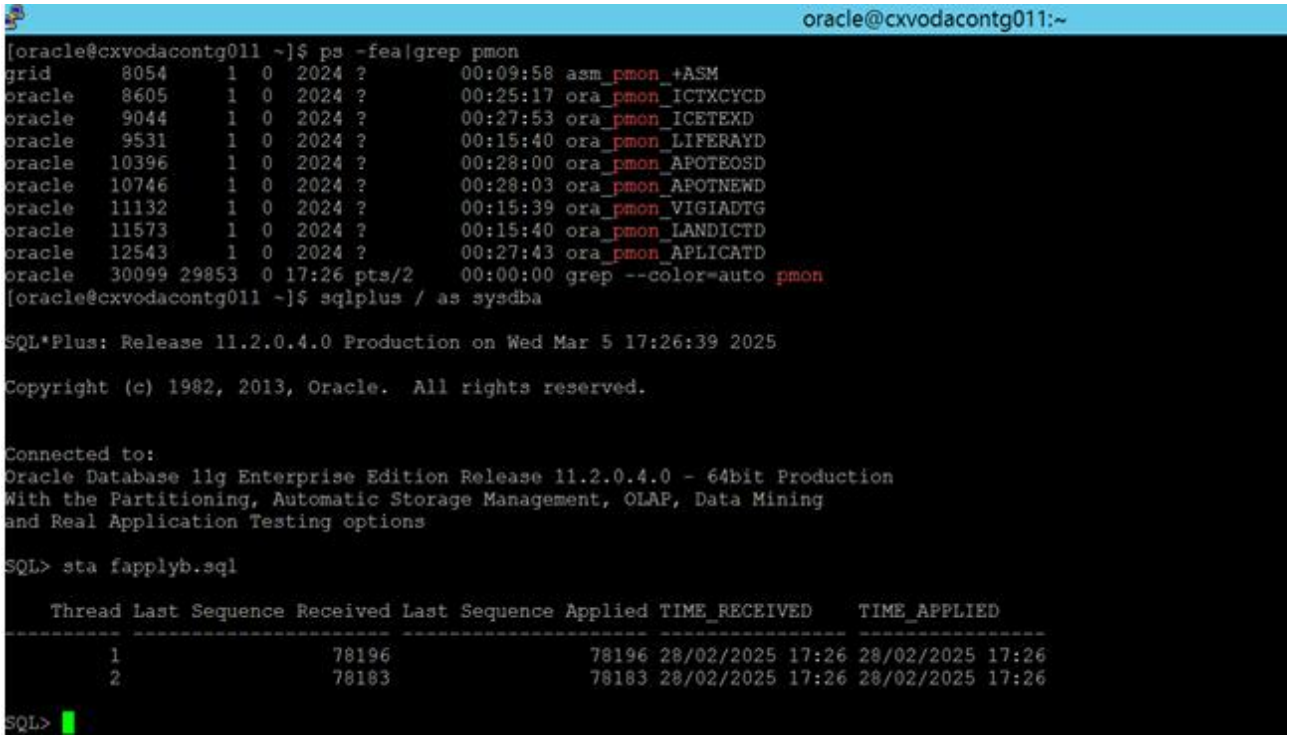


Ilustración 4 Evidencia Dataguard replicado a Megacenter BD

Se generó la consulta de los archives recibidos y aplicados de la base de datos de ICTXCYCD a 28/02/2025 con diferencia cero (0) archives sin aplicar lo que evidencia la sincronización a nivel de Bases de datos Oracle.

4.2.2.3. Servicios de Housing – Datacenter Alterno

A continuación, se presentan las máquinas alojadas en el Datacenter alterno en Medellín, las cuales

estuvieron disponibles todo el mes de febrero 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 11 Disponibilidad de Servicios de Housing – Data Center Alterno

4.2.2.4. Servicios de DRP

De acuerdo con lo establecido para el compromiso del DRP(Plan de recuperación de Desastres), el día 17 de enero se comparte con ICETEX dos opciones para la realización de las pruebas del 2025, las cuales pueden ser modificadas de acuerdo con las necesidades del ICETEX:

- Primer semestre: Domingo 23 de marzo de 2025.
- Segundo semestre: Domingo 17 de agosto de 2025.

Se iniciarán sesiones de trabajo los martes a las 11 am para organizar los puntos que serán analizados dentro de la primera sesión del DRP del 2025, en las sesiones de trabajo entre INFOTIC, CLARO e ICETEX, se definió:

1. Se debe realizar el DRP en ambiente TEST y no se realiza replicación de las acciones realizadas en el datacenter alterno Megacenter al datacenter principal Triara.
2. Se define la ejecución del DRP en un fin de semana que no sea puente.
3. Reducir los tiempos de ejecución de la sesión del DRP
4. Los miembros del grupo de trabajo de INFOTIC estarán de forma presencial en las instalaciones de ICETEX el día de la sesión del DRP
5. Se modifica la fecha de ejecución del DRP para el 27 de abril del 2025
6. Desde INFOTIC se recomienda de las personas de Infraestructura y de riesgos de ICETEX estén de forma presencial en la ejecución del DRP

El documento general con el Plan de Pruebas para el 2025 compartido por el Operador aliado se puede consultar en el Link: Plan de pruebas DRP INFOTIC_ICETEX-2025.pdf

4.3. Seguridad informática

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

- Durante el mes se presentaron eventos de autenticaciones simultaneas de VPN de la misma cuenta desde diferentes ciudades, se valida y se presentaron intentos de conexiones VPN desde otros países e intentando usar nombres de usuarios genéricos que no cumplían el estándar de nombre de usuario que usa la entidad.

- Se bloquearon todas las direcciones IP utilizadas durante estos eventos y se evidencio que estos intentos no fueron exitosos.

- Estas actividades incluyeron la resolución de las alertas de tráfico de la red que genera el SOC, en el FortiSIEM se detectaron durante el mes múltiples eventos relacionados con tráfico permitido desde direcciones IP enmarcadas en listas de amenazas.

- Se revisaron y analizaron los eventos para asegurar que no representaran una amenaza para la seguridad de la red y se tomaron las respectivas acciones para contener posibles amenazas.

- Se implementaron medidas de seguridad adicionales para prevenir accesos no autorizados y se realizó seguimiento continuo.

- Dentro de los alertamientos recibidos durante el mes se presentaron eventos de escaneos e intentos de explotación de vulnerabilidades en las cuales se evidencio que se tomaron las acciones necesarias para prevenir estos escaneos.

Se atienden los casos de Aranda donde se presentaron faltas de acceso a algunas páginas web externas y solicitudes de acceso a nuevos servicios donde se aplican cambios y configuraciones nuevas en los equipos de seguridad perimetral permitiendo estos accesos solicitados. En total se atendieron 19 casos de Aranda durante el mes de febrero los cuales se referencian los cuales se referencian en el ítem 12.2. Gestión de casos Operador de seguridad del Informe Mensual ICETEX FEBRERO.pdf

Para este mes se evidencia una disminución significativa de casos escalados debido a personal en vacaciones y similares.

4.3.1. Plataformas Administradas

Las plataformas administradas por INFOTIC tanto las de propiedad de ICETEX como las de modalidad IaaS son las siguientes:

- FortiWeb
- FortiSandbox
- FortiGate
- Sophos Endpoint
- FortiSIEM

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; actualmente se encuentra en la versión de FortiOS 7.4.7, la cual es una de las versiones reciente más estables.

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

En cuanto a las Interfases, se observa el tráfico hacia la MPLS en promedio 500 G [INR0185 CLARO(MPLS_DC)] en la última semana, tal como se puede ver en la Ilustración.

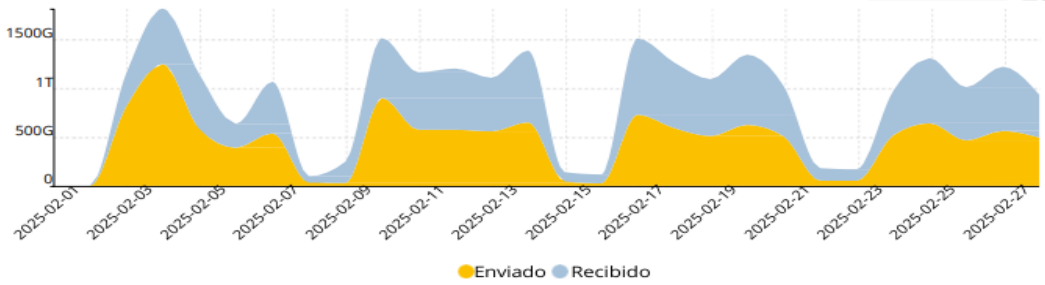


Ilustración 5 Consumo Canal MPLS

Se observa en la Ilustración 6, tráfico hacia la WAN-SEDES-ICETEX [INR0264 (INTE_SEDES_ICTX)] en promedio 600 G en la última semana.

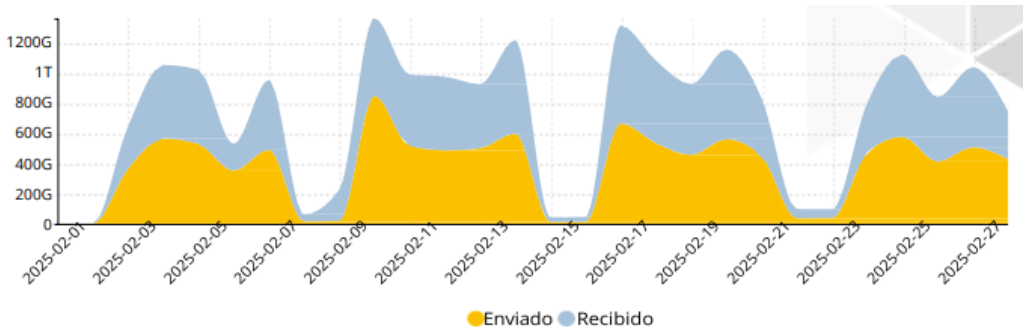


Ilustración 6 Consumo Canal Internet Sedes

En la Ilustración 7, se observa tráfico hacia la INTENET DATACENTER [INTERNET_DC_INR0000320 (Inet_claro)] promedio 450 G en la última semana.

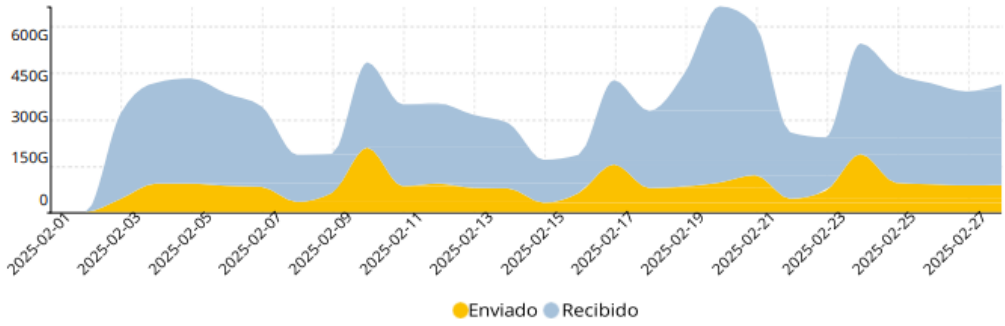


Ilustración 7 Consumo Canal Internet Data Center

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.
default	Perfil con las minimas restricciones	2
Navegacionpcs_Comware	Perfil con restricciones	2
Navegacionpcs_Comware_con_redes	Perfil con restricciones	2
WF-Avanzado	Perfil para FSSO Navegación Avanzada	29
WF-Comunicaciones	Perfil para FSSO comunicaciones	2
WF-General	Perfil para todos	5
WF-General_Sedes	Perfil para todos	1
WF-Sede_Ibague_YT	27022025/InfoTIC/Tarea Aranda 517214 (17458) Se solicita el acceso a youtube	1
WF-Tesoreria	Perfil con restricciones especificas por auditoria	4
WF-VIP	Perfil para FSSO Navegación_VIP	15
WF-wetransfer	Perfil para FSSO Navegación Avanzada	1
wifi-default	Perfil de FULL acceso para pruebas	1

Ilustración 8 Filtrado – WEB – (FortiGate – Triara)

Name	Comments	Ref.
custom-deep-inspection	Customizable deep inspection profile.	0
deep-inspection	Read-only deep inspection profile.	0
certificate-inspection_2780	Read-only SSL handshake inspection profile.	1
Prueba certificate-inspection	Read-only SSL handshake inspection profile.	12
certificate-inspection_ICETEX	SSL para BUS de servicios	29
no-inspection	Read-only profile that does no inspection.	202
certificate-inspection	Read-only SSL handshake inspection profile.	378

Ilustración 9 Inspección – SSL – (FortiGate – Triara)

Name	Comments	Ref.
AV prueba2		60
AV ICETEX		55
AV default	ALL con FSB	42
AV AV-FSB	HTTP,SMTP FULL FSB	39
AV AV-HTTP	HTTP con FSB	26
AV AV-HTTP&CIFS	HTTP,CIFS con FSB	4
AV AV-SMTP	SMTP FULL FSB	1
AV wifi-default	ALL monitoreo sin FSB	1

Ilustración 10 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; actualmente se encuentra en la versión de FortiOS 7.2.9, actualmente se encuentra en la versión de FortiOS 7.4.7, la cual es una de las versiones reciente más estables.

En cuanto a las Interfases, se observa en la Ilustración 11 el tráfico hacia la MPLS de la sede de Aguas con un promedio de 32.54 Mbps (Port7) en la última semana.

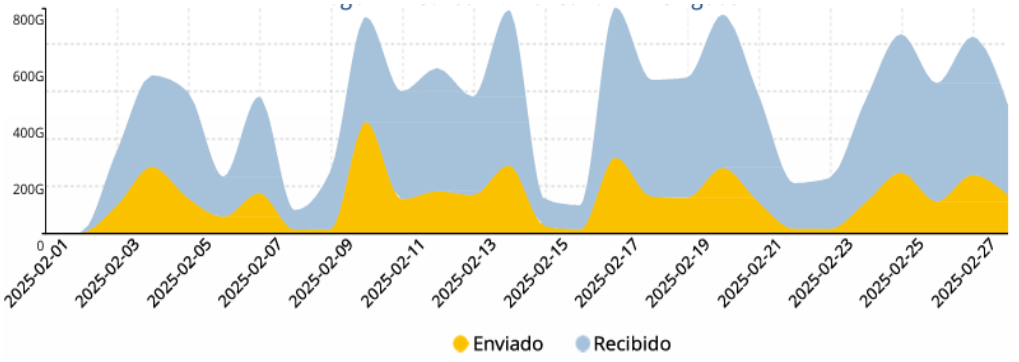


Ilustración 11 Consumo Canal MPLS Aguas

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 7.4.7, la cual es una de las versiones reciente más estables.

Se observa en la Ilustración 12, 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 12 Consumo Canal MPLS Medellín

4.3.1.4. FortiWeb 2000F

A nivel de sistema del FortiWeb en la siguiente ilustración se presenta la configuración actual y su versión de firmware está en la 7.6.2 la cual es una de las versiones actuales más estables.

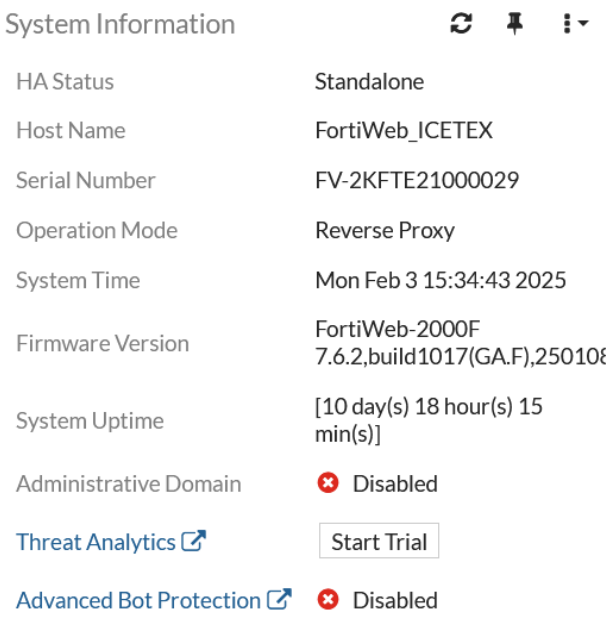


Ilustración 13 Configuración FortiWeb

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 7.6.2 la cual es una de las versiones actuales más estables. Sin embargo, cabe aclarar que, a nivel de licenciamiento, este equipo no tiene un licenciamiento vigente en este momento. Se debe realizar mesa técnica conjunta entre ICETEX e INFOTIC para revisar las alternativas de solución respecto al licenciamiento.

4.3.1.6. FortiSandBox

A nivel de sistema, el Sandbox (FortiSandBox 1000D) muestra su configuración actual y su versión de

firmware que actualmente se encuentra en la 3.2.4 siendo esta la última versión disponible para este dispositivo, ya que está en proceso de EOL (término empleado por el fabricante para describir un producto que pronto será reemplazado por una nueva generación de tecnología).

4.3.1.7. Sophos EndPoint

En la ilustración a continuación, 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.

Se ha informado a ICETEX que en la gestión de la consola de antivirus Sophos se evidenciaba una notificación de caducidad de la licencia de mayor compatibilidad con Windows, en este momento ya se encuentra caducada desde el 30 de agosto de 2024. Esta licencia permite la compatibilidad con versiones del sistema operativo Windows (Server 2008, 2012, Windows 7 y Windows 8, etc.) con el agente de antivirus de Sophos.

Se alertó que la falta de este licenciamiento provoca incompatibilidad y falta de elementos de protección que brinda el agente Sophos a estos sistemas operativos y que representan una brecha de seguridad importante, durante el mes de febrero, se retomaron los comités de pares de seguridad entre ICETEX e INFOTIC revisando los temas pendientes.



Ilustración 14 Estado Seguridad Sophos

4.3.2. Estadística de Portales

Durante el mes de febrero 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 ICETEX FEBRERO.pdf

Como se puede ver en la Ilustración 15, en el periodo de tiempo analizado, se presenta un promedio de 75 GB 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.

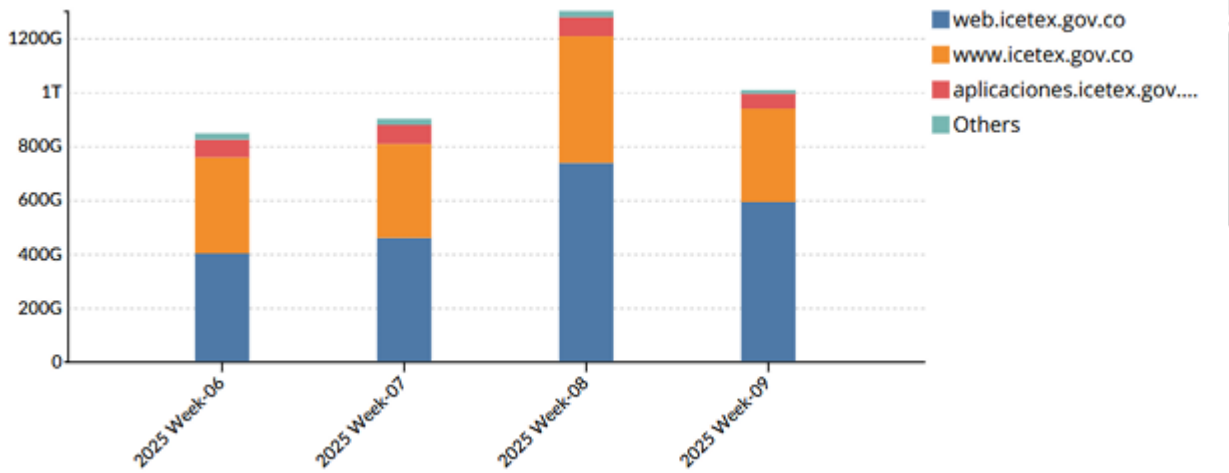


Ilustración 15 Evidencia Gráfica Estadísticas de Portales

Adicional en la Tabla 12, podemos ver los 10 portales más utilizados de acuerdo con la cantidad de solicitudes, siendo para este mes www.icetex.gov.co el primero de este top:

#	HTTP Host	HTTP Request Bytes	HTTP Response Bytes
1	web.icetex.gov.co	170.94 GB	1.99 TB
2	www.icetex.gov.co	31.68 GB	1.38 TB
3	aplicaciones.icetex.gov.co	19.97 GB	243.62 GB
4	portal.icetex.gov.co	1.70 GB	61.45 GB
5	comunidad.icetex.gov.co	220.61 MB	14.24 GB
6	identidad.icetex.gov.co	8.77 MB	100.04 MB
7	186.84.73.155	474.84 KB	88.76 MB
8	186.84.73.157	457.45 KB	85.87 MB
9	186.84.73.131	475.16 KB	84.27 MB
10	186.84.73.158	446.57 KB	83.36 MB

Tabla 12 Top 10 de los Portales más utilizados

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

Este servicio efectúa el monitoreo establecido, acorde con el alcance definido de contrato celebrado entre las partes, para así poder detectar y tomar acciones lo antes posible ante incidentes que puedan afectar la información o infraestructura tecnológica del ICETEX.

Durante el mes de febrero en el ICETEX, el SOC ha continuado en su adaptación y evolución conforme al cambio en las necesidades del ICETEX, por lo cual de manera permanente se mantiene actualizado de acuerdo con la nueva realidad. El detalle se puede ver en el siguiente link Informe Mensual SOC-TH ICETEX Febrero 2025.pdf

El sistema FortiSIEM ofrece más de 100 tableros de monitoreo, incluyendo tableros personalizados que

permiten a ICETEX visualizar en tiempo real las amenazas detectadas, los ataques mitigados y los ataques más frecuentes, lo que mejora significativamente la gestión de la seguridad. Esta capacidad de personalización y seguimiento es fundamental para fortalecer la defensa ante ciberamenazas.

Los tableros de control personalizados para ICETEX se organizan en tres categorías que permiten una visualización clara de las amenazas y ataques, destacando la importancia de la gestión de la seguridad cibernética. Esta estructura facilita la identificación y mitigación de riesgos, así como el análisis de los ataques más frecuentes.

Los tableros de control personalizados para ICETEX se agrupan en tres categorías:

- **AMENAZAS DETECTADAS**
- **ATAQUES MITIGADOS**
- **TOP DE ATAQUES**

Adicional a lo anterior, el SOC implementó más de 70 tableros de control para mejorar el monitoreo y gestión de posibles de amenazas.

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

Indicadores de compromiso (IOC):
Comparativo de los últimos 3 meses que evidencia el incremento en los indicadores mes a mes.

Indicadores de compromiso (IOC)	Febrero 2025	Enero 2025	Diciembre 2024
IOC – Malware DOMINIOS	3.919	3.919	3.897
IOC – Malware IPs	5.278	5.278	5.276
IOC – Malware HASH	1.612	1.612	1.612
IOC – Malware URL	780	780	778

Tabla 13 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 Febrero 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 continuación, se presenta un resumen de cada una de ellas, 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:

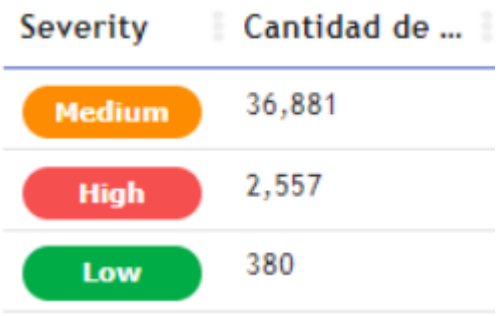


Ilustración 16 Total de alertas de seguridad

Durante el período evaluado se presentaron 352 alertas de seguridad con criticidad ALTA, 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.

Comparativo últimos 3 meses:

Severidad	Alertas de seguridad Febrero 2025	Alertas de Seguridad Enero 2025	Alertas de Seguridad Diciembre 2024
High	352	352	605
Medium	36881	22668	4304
Low	256	256	194

Tabla 14 comparativo Alertas de Seguridad

En el mes de febrero con respecto al mes anterior:

- Las amenazas de seguridad de severidad “Alta” continua igual 00%
- Las amenazas de seguridad de severidad “Media” aumentaron en un 62.70%
- Las amenazas de seguridad de severidad “Baja” continua igual 00%

4.3.3.1.2. Categoría Disponibilidad

A continuación, se relacionan las alertas de disponibilidad presentadas en el periodo analizado, definiendo

el top de los que han tenido mayor concurrencia:

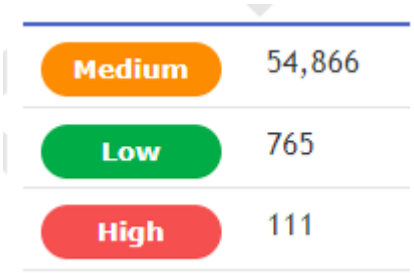


Ilustración 17 Total de alertas de disponibilidad

Durante el período evaluado se presentaron 104 alertas de disponibilidad con criticidad ALTA, 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.

Comparativo últimos 3 meses:

Severidad	Alertas de Disponibilidad Febrero 2025	Alertas de Disponibilidad Enero 2025	Alertas de Disponibilidad Diciembre 2024
High	104	104	84
Medium	54866	56404	67378
Low	765	846	944

Tabla 15 comparativo alertas de disponibilidad

En el mes de febrero con respecto al mes anterior:

- Las amenazas de disponibilidad de severidad “Alta” continua igual 00%
- Las amenazas de disponibilidad de severidad “Media” disminuyeron en un 2.73%
- Las amenazas de disponibilidad de severidad “Baja” disminuyeron en un 9.57%

4.3.3.1.3. Categoría Rendimiento

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



Ilustración 18 Total de alertas de Rendimiento

Durante el período evaluado se presentaron 1239 alertas de rendimiento con criticidad ALTA, 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.

Comparativo últimos 3 meses:

Severidad	Alertas de Rendimiento Febrero 2025	Alertas de Rendimiento Enero 2025	Alertas de Rendimiento Diciembre 2024
High	954	1239	1442
Medium	6417	6417	6324

Tabla 16 comparativo alertas de Rendimiento

En el mes de febrero con respecto al mes anterior:

- Las amenazas de Rendimiento de severidad “Alta” disminuyeron un 23%
- Las amenazas de Rendimiento de severidad “Media” continua igual 00%

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).

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.

4.3.4. Análisis de Vulnerabilidades ICETEX

En el tercer mes de ejecución del análisis de vulnerabilidades, se ha mantenido una cobertura del 100% sobre los activos tecnológicos de la entidad, permitiendo un monitoreo continuo y una identificación más precisa de riesgos. A pesar de que persisten vulnerabilidades críticas sin gestionar, se han observado avances en la mitigación de cifrados débiles y la eliminación de protocolos obsoletos como TLS 1.0 y TLS 1.1.

El análisis ha revelado configuraciones inseguras en servicios clave como SSH, SSL y SMB, lo que refuerza la necesidad de implementar cifrados robustos y fortalecer la seguridad de la red. Además, se ha generado un informe detallado que evalúa la postura de seguridad actual, otorgando un puntaje de riesgo alto debido a la presencia de activos obsoletos, la falta de actualizaciones críticas y debilidades en la configuración de aplicaciones web internas y externas.

Los hallazgos de este período permitirán priorizar acciones correctivas enfocadas en mejorar la seguridad de la infraestructura tecnológica y reducir el nivel de exposición a amenazas.

El ejercicio contempló la realización de análisis de vulnerabilidades y Ethical Hacking, hacia los siguientes activos de la infraestructura tecnológica del ICETEX:

#	Cantidad De IPs Por Activo	Tipo De Activo	Tipo De Dirección (Interna/Externa)
1	142	Servidores	INTERNO
2	34	Dispositivos de Red	INTERNO
3	8	Dispositivos de Seguridad Perimetral	INTERNO
4	113	Aplicaciones WEB	INTERNO Y EXTERNO
5	10	BASES DE DATOS	INTERNO
6	582	EQUIPOS FINALES	INTERNO

Tabla 17 Inventario de dispositivos

A continuación, se provee el consolidado general de vulnerabilidades encontradas en la ejecución de análisis de vulnerabilidades y Ethical Hacking, el detalle de cada vulnerabilidad se puede ver en el INFORME TÉCNICO ANÁLISIS DE VULNERABILIDADES ICETEX (Febrero_2025).pdf

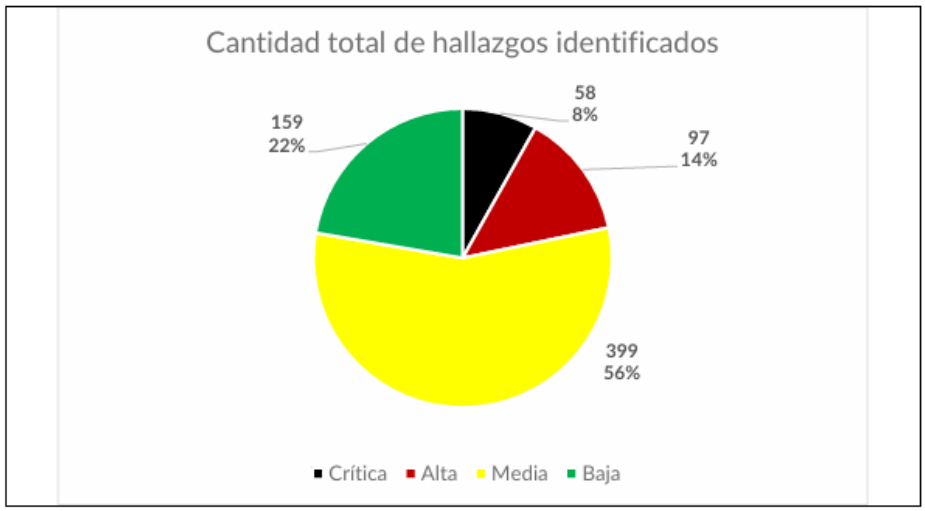


Ilustración 19 Cantidad Total de Hallazgos identificados

4.3.4.1. Resumen de Vulnerabilidades

El estado actual representa un riesgo crítico para la continuidad operativa. Cada día sin acción incrementa exponencialmente la probabilidad de una violación de seguridad con potenciales consecuencias catastróficas: robo de información, interrupción de servicios, y posible colapso de sistemas. La recomendación fundamental es desarrollar e implementar un plan de transformación de seguridad que aborde integralmente estas vulnerabilidades, priorizando la actualización tecnológica, el fortalecimiento de protocolos y la adopción de una cultura de ciberseguridad preventiva. Se debe realizar mesa técnica conjunta entre ICETEX e INFOTIC para revisar las alternativas de solución frente a la gestión de vulnerabilidades.

4.3.4.2. Conclusiones Vulnerabilidades

El análisis de vulnerabilidades realizado en la infraestructura tecnológica de la entidad ha permitido identificar múltiples riesgos críticos que comprometen la confidencialidad, integridad y disponibilidad de los sistemas. Los hallazgos más relevantes incluyen:

- **Uso de software obsoleto y sin soporte:** Se detectaron múltiples versiones sin soporte en servidores web (Apache Tomcat, Microsoft IIS, Oracle Database), bases de datos (Microsoft SQL Server) y sistemas

operativos (Windows Server 2003, versiones antiguas de VMware vCenter). La falta de actualizaciones incrementa la exposición a ataques explotables con RCE (Remote Code Execution).

- **Protocolos de comunicación inseguros:** La presencia de versiones desactualizadas de SSL/TLS (TLS 1.0/1.1, SSL 2/3) y el uso de cifrados débiles (RC4, EXPORT_RSA, EXPORT_DHE) facilitan ataques de interceptación como POODLE, Logjam y FREAK. Además, la ausencia de HSTS en servidores HTTPS deja expuestas las conexiones a ataques de intermediario (MitM).

- **Configuraciones inseguras en servicios clave:** Se encontraron configuraciones deficientes en SMB (SMBv1 activado, falta de firma en SMB), SSH (uso de algoritmos débiles, llaves privadas expuestas) y RDP (falta de autenticación NLA, cifrado insuficiente), lo que incrementa el riesgo de ataques como EternalBlue, BlueKeep y PetitPotam.

- **Aplicaciones web y servidores con vulnerabilidades críticas:** Se detectaron múltiples fallos en aplicaciones web que incluyen ejecución remota de código (Liferay Portal, JBoss, Spring4Shell), inyección SQL, exposición de directorios sensibles y configuraciones por defecto en servidores como Apache Tomcat y IIS.

- **Filtración de información sensible:** Se identificaron servidores y aplicaciones que permiten la transmisión de credenciales en texto plano, divulgación de archivos de configuración sensibles (info.php, phpinfo.php), y errores detallados en IIS que pueden ser utilizados por atacantes para explotar vulnerabilidades específicas.

La combinación de estos factores evidencia una postura de seguridad frágil, que requiere medidas inmediatas para mitigar los riesgos más críticos y reducir la superficie de ataque

Recomendación de Remediación: Para mejorar la postura de seguridad de la entidad y mitigar las vulnerabilidades identificadas, se recomienda:

- **Actualizar y migrar sistemas sin soporte**: Implementar versiones compatibles de servidores, bases de datos y sistemas operativos, eliminando software obsoleto como Windows Server 2003, IIS 6.0, Apache Tomcat versiones antiguas y Microsoft SQL Server sin soporte.

- **Fortalecer los protocolos de comunicación:**
  - Deshabilitar SSL 2.0/3.0, TLS 1.0/1.1 y forzar el uso de TLS 1.2/1.3 con cifrados robustos.
  - Implementar HSTS en servidores HTTPS para evitar ataques de degradación de seguridad.
- **Corregir configuraciones inseguras en servicios críticos:**
  - **SMB:** Deshabilitar SMBv1 y habilitar la firma de SMB.
  - **SSH:** Eliminar el uso de algoritmos débiles y llaves expuestas.
  - **RDP:** Habilitar Network Level Authentication (NLA) y elevar el nivel de cifrado.

- **Mejorar la seguridad de aplicaciones web:** PROCESO DE CONSULTORÍA Formato de informe técnico Código Versión F. Aprobación Página WX-IINFR-06 01 02/06/2023 261 de 261

- Corregir vulnerabilidades de ejecución remota de código en servidores y frameworks como Liferay Portal, JBoss y Spring4Shell.
- Implementar validaciones y controles para prevenir ataques de inyección SQL y XSS.
- Eliminar archivos de configuración expuestos y restringir el acceso a directorios sensibles.

➢ **Mitigar riesgos de filtración de credenciales y autenticación débil:**

- Implementar autenticación multifactor (MFA) en servicios críticos.
- Eliminar la transmisión de credenciales en texto plano y reforzar el cifrado de comunicaciones.
- Deshabilitar métodos HTTP TRACE / TRACK para prevenir ataques de rastreo de sesión.

➢ **Monitorear y gestionar activamente la seguridad:**

- Implementar herramientas de detección y respuesta ante incidentes (SIEM).
- Establecer un plan de gestión de vulnerabilidades con revisiones periódicas y correcciones priorizadas.

La implementación de estas medidas permitirá reducir significativamente la exposición a amenazas, mejorar la seguridad de la infraestructura tecnológica y minimizar el impacto de posibles ataques.

4.3.5. REPORTE DE IPS

Del reporte de IPS se observa que desde las ips 10.1.2.24, 10.1.3.18 y 10.1.6.3 con destino a diversas ips públicas, haciendo match con la siguiente firma TCP.Split.Handshake, se observa en varias repeticiones, por lo tanto se recomienda prevenir este tipo de escaneos adicionalmente se debe aplicar en la vlan 10, vlan 5 y vlan 45 la siguiente recomendación del fabricante: https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-block-the-TCP-split-handshakein-intrusion/ta-p/239186. El equipo de seguridad estará realizando esta actividad en el firewall de Aguas.

En conclusión, como se observa en el Reporte de IPS de febrero_infotic_2025.pdf los eventos de IPs que están siendo solo detectados y no han sido bloqueados ha disminuido considerablemente de acuerdo con las medidas aplicadas en los diferentes equipos de seguridad.

Para mitigar los riesgos asociados, se recomienda implementar las medidas preventivas adecuadas, como la aplicación de la recomendación de Fortinet para bloquear este tipo de tráfico en las VLANs 10, 5 y 45.

El equipo de seguridad procederá a realizar esta configuración en el firewall de Aguas, fortaleciendo así la protección contra potenciales amenazas, es importante considerar el impacto en los recursos de los equipos al implementar estas medidas de seguridad por lo que se ha venido aplicando de forma progresiva evaluando el impacto.

4.4. Servicios de nube

El proceso de integración en la nube se está trabajando en conjunto entre INFOTIC e ICETEX para actualizar los procedimientos para la creación, actualización, mantenimiento, soporte y eliminación de los elementos que se crean en la nube, y todo esto asociarlo a los TAGs que se deben tener en cuenta en el tema de

administración de este tipo de componentes tecnológicos. También se está gestionando la actualización del inventario de aplicaciones para determinar cuáles pueden pasar a la nube para optimizar recursos en el ICETEX.

5. GESTION FISICA DE LA EJECUCIÓN

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.

En el presente informe del mes de febrero del 2025 del proyecto, se encuentra en la fase de operación de los servicios contemplados en el alcance llevando ejecutados 23 meses que equivale al 63% 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.

Los siguientes son los especialistas que estuvieron en el desarrollo de la operación del mes de febrero del 2025:

NOMBRE COMPLETO	ROL RESPONSABLE
Carlos Alberto Roldan Ríos	Administrador de Red
Juan Carlos Martínez Sierra	Administrador Web
Edgar Cobos Mayorga	Administrador DBA
Jose Francisco Escobar Escorcia	Administrador de Soluciones
Davis Alexander Mogollón Fandiño	Administrador de Soluciones
Jose Luis Mantilla Guiza	Integrador de Nube
Jairo Orlando Acevedo Jiménez	Administrador y soporte de seguridad
Jhon Alveiro Pava González	Administrador y soporte de seguridad

Tabla 18 Grupo especialistas

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

NOMBRE COMPLETO	ROL RESPONSABLE
María Victoria Suarez Osorio	Gerente de Servicio
Angie Paola Parra Bustos	Documentadora
Oscar Alberto Viuche Téllez	Gerente de Implementaciones

Tabla 19 Grupo Administrativo

El siguiente es el grupo de aliados estratégicos que estuvo en el desarrollo de la operación del mes de febrero del 2025:

ALIADO	SERVICIOS
	Data center

ALIADO	SERVICIOS
CLARO	Canales de comunicación
	Comunicaciones
	Internet de gente (WIFI)
	Servicios que complementa la arquitectura WAN
	IPv6
	Copias de respaldo
	Hosting
	Portal WEB
	Base de datos
Wexler	SOC
Growdata	Videoconferencia
E&C	Recurso Humano

Tabla 20 Aliados para el proyecto

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 NO EJECUTAD0 2023
	$ 7,849,749,214.53	$5,550,607,398.60	$360,000,000	$0	$ 1,939,141,815.93
	VALOR VIGENCIA 2024	VALOR EJECUTADO 2024	VALOR BOLSA VIGENCIA 2024	VALOR BOLSA EJECUTADO 2024	VALOR NO EJECUTAD0 2024
$ 31.398.996.857,96	$ 10,466,332,286.04	$8,116,163,716.21	$480,000,000	$0	$ 1,870,168,569.83
	VALOR VIGENCIA 2025	VALOR EJECUTADO 2025	VALOR BOLSA VIGENCIA 2025	VALOR BOLSA EJECUTADO 2025	VALOR NO EJECUTAD0 2025
	$ 10,466,332,286.04	$ 1,512,772,003	$480,000,000	$0	$8,953,560,283.21

CONCEPTO						*VALOR*
VALOR TOTAL DEL CONTRATO						***$ 31,398,996,857.96***
VALOR PAGADO						$ 14,441,737,171.00
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	
Pendiente - Pago No. 22 -	mes:	Enero	de	2025	$ 740,982,385.00	
Pendiente - Pago No. 23 -	mes:	Febrero	de	2025	$ 771,789,618.00	
VALOR CAUSADO QUE NO SE HA PAGADO *(valor a pagar factura)* *						$ 771,789,618.00
VALOR TOTAL EJECUTADO *(valor pagado + valor causado no pagado)*						$15,954,509,173.83
SALDO DEL CONTRATO *(valor total del contrato – valor total ejecutado)*						$ 15,444,487,684
PORCENTAJE DE EJECUCIÓN						50.81%
** El valor causado no pagado corresponde a cuentas de cobro o facturas recibidos y aprobados a satisfacción por el supervisor o interventor para su pago**						

Tabla 21 Ejecución Presupuestal

7. GESTION ADMINISTRATIVA

7.1. Profesionales

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

INFORME MENSUAL FEBRERO 2025.pdf

7.1.1. Especialista en Base de Datos DBA

El proyecto cuenta con un DBA y un apoyo al DBA que permiten cubrir y dar solución a los diferentes requerimientos que el ICETEX realiza en marcadas en:

- **Funciones Básicas Especialista Bases de Datos ICETEX:** Se presenta un informe anexo con la información sobre las actividades que realizan en el desarrollo de sus funciones.
- **Informes Requeridos:** Se presentan informes adicionales y de acuerdo con las necesidades del servicio durante cada periodo evaluado teniendo en cuenta la gestión del servicio y la disponibilidad de los servicios que el ICETEX requiere, dentro de estos se tiene las evidencias del DataGuard, Informe de replicación,

- **Tareas de administración:** Mediante herramientas tecnológicas como el "ELASTIC" se tiene configuradas alertas que permiten prevenir indisponibilidades del servicio con consumos elevados realizando acciones administrativas para evitar estos eventos.
- **Gestión operativa.** Manejo de incidentes y problemas: Los dos especialistas reciben mediante Aranda las notificaciones y de la misma forma se retroalimenta sobre las acciones realizadas y los soportes correspondientes.
- **Mejores prácticas en el mantenimiento de bases de datos, enfocada en:** dentro de las acciones de administración y el monitoreo realizadas sobre las bases de datos se aplican las mejores prácticas para el uso y manejo de las bases de datos del ICETEX.

7.1.2. Especialista web máster

El proyecto cuenta con un WEB MÁSTER que permite cubrir y dar solución a los diferentes requerimientos que el ICETEX realiza a nivel del portal WEB:

- **Funciones básicas:** Se presenta un informe anexo con la información sobre las actividades que realizan en el desarrollo de sus funciones.
- **Informes:** Se presentan informes adicionales y de acuerdo con las necesidades del servicio durante cada periodo evaluado teniendo en cuenta la gestión del servicio y la disponibilidad de los servicios que el ICETEX requiere, dentro de esto se tiene reporte de monitoreo, Prueba TEST.

7.1.3. Administrador de Soluciones

El proyecto cuenta con dos especialistas de soluciones que permiten cubrir y dar solución a los diferentes requerimientos que el ICETEX realiza en marcadas en:

- **Funciones básicas:** Se presenta un informe anexo con la información sobre las actividades que realizan en el desarrollo de sus funciones.
- **Informes:** Se presentan informes adicionales y de acuerdo con las necesidades del servicio durante cada periodo evaluado teniendo en cuenta la gestión del servicio y la disponibilidad de los servicios que el ICETEX requiere, dentro de estos se tiene el informe de aplicaciones.

7.1.4. Especialista en Networking

El proyecto cuenta con un especialista de networking que permite cubrir y dar solución a los diferentes requerimientos que el ICETEX realiza en marcadas en:

- **Funciones básicas:** Se presenta un informe anexo con la información sobre las actividades que realizan en el desarrollo de sus funciones.
- **Informes, entregables o productos de la asesoría en networking:** Se presentan informes adicionales y de acuerdo con las necesidades del servicio durante cada periodo evaluado teniendo en cuenta la gestión del servicio y la disponibilidad de los servicios que el ICETEX requiere, dentro de los cuales se tiene pruebas se saturación, informe de disponibilidad, consumo de canales, ANS de canales.

7.1.5. Especialista Integrador de nube

El proyecto cuenta con un especialista en NUBE que permite cubrir y dar solución a los diferentes requerimientos que el ICETEX realiza en marcadas en:

- **Funciones Especialista Integrador de nube:** Se presenta un informe anexo con la información sobre las actividades que realizan en el desarrollo de sus funciones.

7.1.6. Especialista en seguridad

El proyecto cuenta con dos especialistas en plataforma de seguridad informática que permiten cubrir y dar solución a los diferentes requerimientos que el ICETEX realiza en marcadas en:

- **Funciones básicas:** Se presenta un informe anexo con la información sobre las actividades que realizan en el desarrollo de sus funciones.
- **Informes, entregables o productos de la asesoría en seguridad informática:** Se presentan informes adicionales y de acuerdo con las necesidades del servicio durante cada periodo evaluado teniendo en cuenta la gestión del servicio y la disponibilidad de los servicios que el ICETEX requiere, dentro los cuales se tiene, el informe de marca, el informe del SOC, informe de vulnerabilidades, reporte de IPS.

8. Servicio De Colaboración

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

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

Tabla 22 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

8.1. Disponibilidad del servicio – sedes Regionales

En la verificación realizada para el pasado mes de febrero del 2025 sobre la solución de videoconferencia en las sedes regionales, se encontró que la solución completa presentó estado activo para los 28 días del periodo con disponibilidad del 100% para el presente informe, además es importante resaltar que se cuenta con todos los requerimientos realizados en las especificaciones técnicas del contrato.

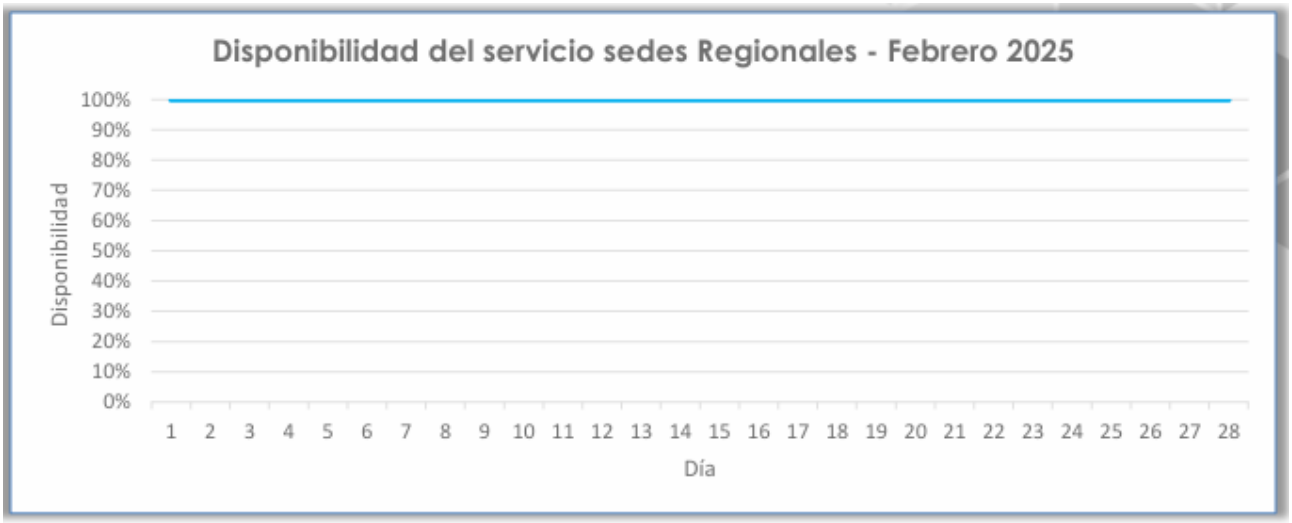


Ilustración 20 Disponibilidad de servicio videoconferencia sedes regionales – febrero 2025

8.2. Disponibilidad del servicio – sedes Bogotá (aguas - ángel)

En la verificación realizada en el mes de febrero del 2025 sobre la solución de videoconferencia distribuida en la ciudad de Bogotá, sedes Aguas y Ángel, la solución completa presentó una disponibilidad del 100% en estado activo para los 28 días del periodo que comprende el presente informe, además es importante resaltar que se cuenta con todos los requerimientos realizados en las especificaciones técnicas del contrato.

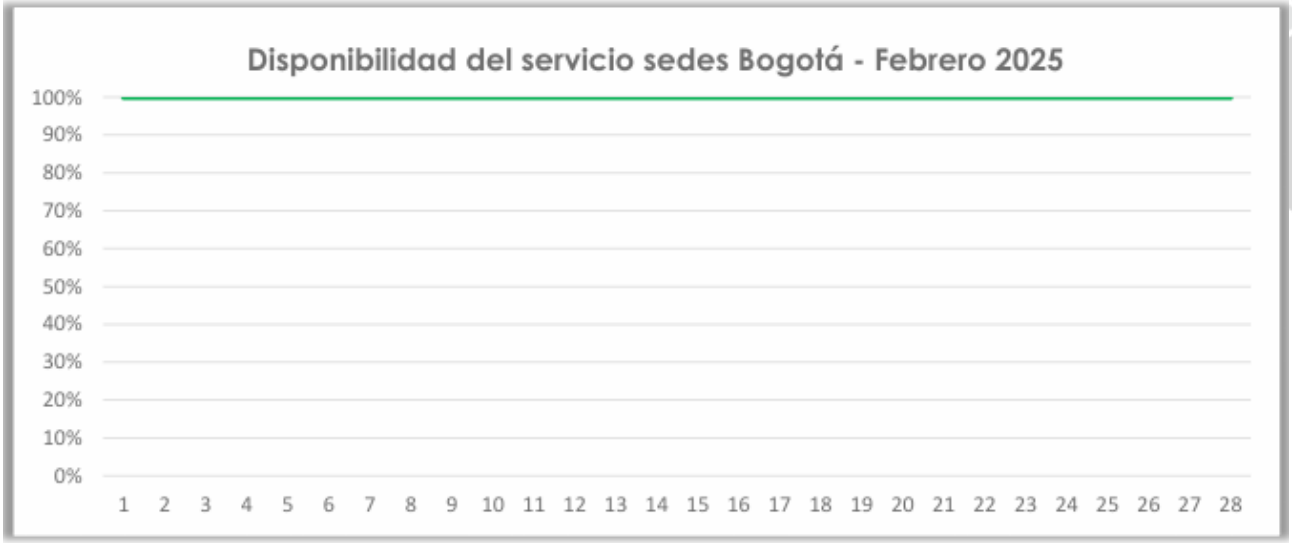


Ilustración 21 Disponibilidad de servicio videoconferencia sedes Bogotá – febrero 2025

8.3. Gestión de incidencias y requerimientos – sedes regionales

Para el periodo de febrero del 2025, comprendido entre el 1 y el 28 del mes, en las sedes Regionales (Cali, Barranquilla, Bucaramanga y Medellín) no se generaron 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, se contó con la disponibilidad para recibir cualquier solicitud de soporte (Incidencia/requerimiento) o apoyo concerniente a la solución de videoconferencia desplegada.



Ilustración 22 Incidentes / Requerimientos sedes regionales – febrero 2025

8.4. Gestión de incidencias y requerimientos – Bogotá (Aguas - Angel)

Para el periodo comprendido entre el 1 y el 28 de febrero del año en curso, para las sedes de Bogotá Aguas y Ángel, no se generaron solicitudes especiales que requirieran gestión y atención del soporte técnico,

tampoco se recibieron requerimientos especiales adicionales para gestión y atención del soporte técnico; No se reportaron incidencias a nivel de indisponibilidad de servicio para estas sedes durante el mes del presente informe, no obstante, 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.

En las visitas del periodo realizada a la sede de Aguas y Ángel, con las personas que apoyan técnicamente de manera frecuente la revisión de los equipos y atención de incidencias/requerimientos, se realizaron las pruebas de verificación de funcionamiento, limpieza superficial de los módulos, inspección y los ajustes requeridos para descartar incidencias en los equipos y poder garantizar continuidad del servicio. En estas revisiones no se encontraron novedades de funcionamiento y los módulos se encuentran prestando el servicio de manera correcta y con la continuidad requerida. La solicitud de ingreso para la visita se realizó mediante el caso RF-293610-8-21884.



Ilustración 23 Limpieza OPS sala 8vo piso presidencia – Visita febrero 2025

Para la OPS del módulo piso 8, se realizó mantenimiento preventivo de limpieza interna, superficial y del ventilador de la OPS para eliminar suciedad en el dispositivo, y se aplica limpia contactos en las partes electrónicas internas, posterior a eso, se realizan las pruebas en el módulo para confirmar el correcto funcionamiento.

Durante la visita realizada para el periodo se realizaron pruebas y el mismo proceso de limpieza en los módulos de los pisos de la sede Aguas que contaron con disponibilidad para revisión, con el fin de validar el funcionamiento normal del servicio con acompañamiento del personal de mesa de ayuda de la entidad, además, de inspección visual de desgaste de elementos y conexiones para garantizar funcionamiento correcto y brindar servicio sin interrupciones, Figura 6. evidencia módulo piso 4 – Aguas. Es importante mencionar que en algunas ocasiones las salas se encuentran en uso, por lo cual no se intervienen, sin embargo, se valida funcionamiento correcto del módulo, y se prioriza la revisión para visitas posteriores.



Ilustración 24 Evidencia modulo funcional sede Aguas 65" piso 4 - Visita febrero 2025



Ilustración 25 Modulo funcional sede aguas, ubicación piso 6 – Visita febrero 2025

Para el módulo ubicado en el auditorio del piso 2 – sede Aguas, se realiza el proceso de mantenimiento

preventivo de limpieza interna y superficial de la OPS para eliminar suciedad, y se valida funcionamiento posterior al mantenimiento realizado al módulo.



Ilustración 26 Limpieza modulo sede aguas 65" piso 2 – visita febrero 2025

Durante el mes de febrero, como se realiza en los periodos anteriores, se garantizó la continuidad del servicio de módulos de videoconferencia en las diferentes sedes de la entidad prestando el servicio con normalidad sin presentar interrupciones. En las visitas de revisión del periodo se realizaron pruebas de verificación de funcionamiento, inspección de los módulos y limpieza interna y externa de los equipos, principalmente en las OPS, que se encuentran instalados en las sedes de Bogotá, además, se corroboró el funcionamiento correcto de cada uno, con apoyo técnico encargado para este fin, y acompañamiento de personal de la mesa de ayuda de la entidad.

Con el fin de prevenir fallas y garantizar un rendimiento óptimo, además, prolongar la vida útil de los equipos que componen los módulos de videoconferencia y poder garantizar la continuidad del servicio en las sedes, se proyecta continuar con las visitas frecuentes para las sedes de Bogotá para validación de funcionamiento y actividades de limpieza de equipos. Para las sedes regionales de ICETEX, durante la vigencia 2025, se encuentran proyectados los mantenimientos preventivos de acuerdo con la regularidad requerida por uso y funcionamiento de los equipos, con el fin de inspeccionar desgaste de piezas que se puedan presentar en los componentes que integran los módulos y demás incidencias que se puedan presentar por el uso frecuente de los equipos.

Durante el mes de febrero 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 principalmente de las OPS de los módulos instalados en la sede Aguas de la ciudad de Bogotá, para garantizar la prestación continua del servicio y validar que no se estén presentado novedades y/o incidencias.

- Informe mensual febrero 2025 de operación y seguimiento a la prestación del servicio.

Las evidencias se pueden encontrar en el siguiente link: Informe actividades Módulos videoconferencia ICETEX Febrero 2025.pdf

Durante los últimos 3 meses se presentaron los siguientes requerimientos y/o incidentes durante la prestación del servicio de videoconferencia:

	Diciembre 2024	Enero 2024	Febrero 2025
Requerimiento	0	0	0
Incidentes	0	0	0

Tabla 23 Distribución trimestral de requerimientos y/o incidentes

Para el mes de febrero 2025 no se presentaron afectaciones en el servicio de videoconferencia en las sedes del ICETEX.

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	Evaluacion del riesgo			Medidas de control a implementar	Responsable
					Severidad (S)	Probalidad (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	Perdida 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 corpartida	INFOTIC
2	Instalación de agente de antivirus en los servidores de ICETEX	Sufrir ataques que pueden 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 ultima versión de parches actualizada	3	6	18	Verificación con los fabricantes sobre la ultima versión libera y funcionando comparada con la instala actualmente en los servidores	INFOTIC
4	Actualiación 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 ewquipos	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 27 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:

- **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 24 Nivel de riesgo

- Tabla de grado de riesgo

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

Tabla 25 Grado de riesgo

10. INDICADORES CLAVE DE DESEMPEÑO

10.1. ANS por Disponibilidad de canales de comunicaciones:

Durante el mes de febrero 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 tienen los reportes:

Reporte Mensual Disponibilidad INFOTIC Febrero 2025.pdf
Informe Mensual ALLOT febrero 2025 (1).pdf

También se puede consultar en el repositorio un documento en Excel con el análisis del comportamiento de los canales para el mes de febrero ANS_Febrero_2025_NEW.xlsx

Sede	Categoría	INR	% Mes
BOGOTA D.C.	Principal / FO (Sede Aguas)	INR0037	99.99%
	Backup / FO (Sede Aguas)	INR0036	99.69%
	Principal / IPVPN (Sede Chapinero)	INR0022	100.00%
	Backup / IPVPN (Sede chapinero)	INR0020	100.00%
	Principal / IPVPN (Angel)	INR0272	99.64%
	Backup / IPVPN (Angel)	INR0273	100.00%
IBAGUE	Principal / IPVPN	INR0073	100.00%
	Backup / IPVPN	INR0076	99.97%
LETICIA	Principal / Satelital	INR0000373	95.79%
NEIVA	Principal / IPVPN	INR0039	91.05%
	Backup / IPVPN	INR0041	92.27%
TUNJA	Principal / IPVPN	INR0104	99.95%
	Backup / IPVPN	INR0106	99.94%
VILLAVICENCIO	Principal / IPVPN	INR0085	99.93%
	Backup / IPVPN	INR0084	99.39%
ARMENIA	Principal / IPVPN	INR0074	100.00%
	Backup / IPVPN	INR0072	99.90%
MANIZALES	Principal / IPVPN	INR0088	99.86%
	Backup / IPVPN	INR0087	99.99%
MEDELLIN	Principal / IPVPN	INR0133	85.88%
	Backup / IPVPN	INR0132	99.48%
APARTADO	Principal / IPVPN	INR0144	98.38%
PEREIRA	Principal / IPVPN	INR0079	100.00%
	Backup / IPVPN	INR0077	98.55%
QUIBDO	Principal / IPVPN	INR0014	85.17%
	Backup / IPVPN		0.00%
BARRANQUILLA	Principal / IPVPN	INR0103	100.00%
	Backup / IPVPN	INR0100	100.00%
CARTAGENA	Principal / IPVPN	INR0109	99.61%
	Backup / IPVPN	INR0107	99.95%
MONTERIA	Principal / IPVPN	INR0080	95.09%
	Backup / IPVPN	INR0081	96.61%
RIOHACHA	Principal / IPVPN	INR0164	100.00%
	Backup / IPVPN	INR0162	99.99%
SANTA MARTA	Principal / IPVPN	INR0154	99.55%
	Backup / IPVPN	INR0152	98.19%
SINCELEJO	Principal / IPVPN	INR0095	100.00%
	Backup / IPVPN	INR0097	99.53%
SAN ANDRES	Principal / IPVPN	INR000036 INR0000369	99.67%
BARRANCABERMEJA	Principal / IPVPN		0.00%
SAN GIL	Principal / IPVPN		0.00%
BUCARAMANGA	Principal / IPVPN	INR0062	99.83%
	Backup / IPVPN	INR0061	99.80%
CUCUTA	Principal / IPVPN	INR0044	99.98%
	Backup / IPVPN	INR0047	99.44%
VALLEDUPAR	Principal / IPVPN	INR0091	100.00%
	Backup / IPVPN	INR0090	100.00%
YOPAL	Principal / IPVPN	INR0121	99.74%
	Backup / IPVPN	INR0123	99.45%
ARAUCA	Principal / IPVPN	INR0110	90.66%
CALI	Principal / IPVPN	INR0151	100.00%

	Backup / IPVPN	INR0153	99.96%
BUENAVENTURA	Principal / IPVPN	INR0051	99.23%
MOCOA	Principal / IPVPN	INR0135	100.00%
	Backup / Satelital	INR0136	100.00%
PASTO	Principal / IPVPN	INR0130	99.96%
	Backup / IPVPN	INR0131	99.47%
POPAYAN	Principal / IPVPN	INR0035	99.96%
	Backup / IPVPN	INR0032	99.97%
TUMACO	Principal / IPVPN	INR0147	84.74%
DC TRIARA	MPLS PP	INR0266	100.00%
	MPLS Backup	INR0171	100%
DC TRIARA	INTERNET BK	INR0221	100%
	INTERNET PP	INR0264	98.43%
DC TRIARA	NOC claro dedidcado (DWDM) 2G Traira megacentro	INR0224	
Canal entre Sitio principal e Icetex - Dirección General - Aguas	Principal /IPVPN		0.00%
	Backup / IPVPN		0.00%
BOGOTA D.C.	Internet (Sede Aguas)	INR0034	98.36%
DC Megacentro	MEGACENTER MPLS BACKUP MEDELLIN	INR0177	99.42%
DC TRIARA	Internet Principal	INR0230	99.96%
DC Megacentro	Internet Backup	INR0268	99.96%
Banco de la Republica hasta Edificio Dirección General ICETEX	Ubicado en Datacenter Principal. interconectado a traves de red MPLS	INR0000289	99.68%
DECEVAL hasta Edificio de ICETEX Dirección General.	Ubicado en Datacenter Principal. interconectado a traves de red MPLS	INR0000317	99.98%
DECEVAL hasta Edificio de ICETEX Dirección General.	Ubicado en Datacenter Principal. interconectado a traves de red MPLS (Backup)	INR0000318	99.61%
Salidadelportaleshttps://portal.icetex.gov.co/portalywww.icetex.gov.cohaciainternet en centro de cómputo principal TRIARA	InternetReversoparaPortales	INR0000320	
Salida del portales https://portal.icetex.gov.co/portal y www.icetex.gov.co hacia internet en centro de cómputo de contingencia	Internet Reverso para Portales	INR0274	
DC TRIARA	allot entralizado 800M triara	INR0270	
BARRANQUILLA	INTERNET PARA LA GENTE	INR0094	99.99%
BUCARAMANGA	INTERNET PARA LA GENTE	INR0057	99.83%
CALI	INTERNET PARA LA GENTE	INR0160	99.91%
AGUAS	INTERNET PARA LA GENTE	INR0029	100.00%
CHAPINERO	INTERNET PARA LA GENTE	INR0015	100.00%
MEDELLIN	INTERNET PARA LA GENTE	INR0122	85.90%
APARTADO	INTERNET PARA LA GENTE	INR0140	99.74%
ARAUCA	INTERNET PARA LA GENTE	INR0115	91.19%
LETICIA	INTERNET PARA LA GENTE	INR0000378	95.59%
QUIBDO	INTERNET PARA LA GENTE	INR0021	84.72%
RIOHACHA	INTERNET PARA LA GENTE	INR0159	99.56%
SAN ANDRES	INTERNET PARA LA GENTE	INR0000368	99.66%
YOPAL	INTERNET PARA LA GENTE	INR0127	99.75%
MOCOA	INTERNET PARA LA GENTE	INR0141	100.00%
SD WAN AGUAS	SD WAN	INR0033 / 00 0334	100.00%
SD WAN MOCOA	SD WAN	INR0139 / 000333	98.79%
SD WAN LETICIA	SD WAN	INR0000374	95.37%
SDWAN SANANDRES	SDWAN	INR0000371	99.93%

Tabla 26 Disponibilidad de Canales

Durante el mes de febrero 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	93.25%
AGUAS	INTERNET PARA LA GENTE	INR0029	100.00%
CHAPINERO	INTERNET PARA LA GENTE	INR0015	100.00%
MEDELLIN	INTERNET PARA LA GENTE	INR0122	96.58%
APARTADO	INTERNET PARA LA GENTE	INR0140	99.89%
ARAUCA	INTERNET PARA LA GENTE	INR0115	30.30%
LETICIA	INTERNET PARA LA GENTE	INR0000378	95.93%
QUIBDO	INTERNET PARA LA GENTE	INR0021	100.00%
RIOHACHA	INTERNET PARA LA GENTE	INR0159	100.00%
SAN ANDRES	INTERNET PARA LA GENTE	INR0000368	97.61%
YOPAL	INTERNET PARA LA GENTE	INR0127	99.37%
MOCOA	INTERNET PARA LA GENTE	INR0141	99.97%

Tabla 27 Disponibilidad canales "Internet para la gente"

Durante el mes de febrero, los canales SD WAN definidos estuvieron disponibles sin interrupciones como se ve en la siguiente tabla sus porcentajes de disponibilidad:

Sede	Categoría	INR	% Mes
SD WAN AGUAS	SD WAN	INR0033 / 000334	100.00%
SD WAN MOCOA	SD WAN	INR0139 / 000333	99.98%
SD WAN LETICIA	SD WAN	INR0000374	95.88%
SD WAN SANANDRES	SDWAN	INR0000371	98.22%

Tabla 28 Disponibilidad Canales "SDWAN"

10.1.1. Canal de Replicación (Triara – Megacenter)

El proyecto tiene asignado dos (2) canales 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 febrero continúa su funcionamiento correctamente sin novedades que afectaran la prestación del servicio.

La evidencia se encuentra en el Informe mensual replicacion Febrero 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 el documento Reporte Monitoreo ICETEX Febrero 2025-ELK.pdf

Desde diciembre, el operador CLARO ha iniciado un proceso de migración hacia una nueva versión de la herramienta, específicamente la versión 8.15.2 de ELK. Actualmente, la migración de todos los servidores a esta nueva versión no se ha completado, por lo que para verificar la disponibilidad de los servidores que aún no han sido migrados, es necesario consultar un segundo informe, el cual se encuentra en Reporte Monitoreo ICETEX Febrero 2025-ELK.pdf, que corresponde a la versión 8.14.3 de la herramienta.

Una vez que se complete la migración, se procederá con la actualización a ICETEX y la entrega oficial.

Cod Servicio	Hostname	Disponibilidad
INR0228	ictxsisgesbd	100%
INR0229	ictxsisgesapp	100%
INR0233	icetexboglxorfeo1	100%
INR0234	ictxprusisgapp	100%
INR0237	icetexbogbalserver1-r	100%
INR0238	icetexbogliferaynfs	100%
INR0239	icetexbogelasticserver1	100%
INR0241	icetexbogelasticserver3	99,98%
INR0242	icetexbogliferayserver2	99,92%
INR0243	icetexbogliferayserver1	87,50%
INR0244	icetexboglxdarumasrv1	100%
INR0245	icetexboglxdarumasrv2	100%
INR0246	icetebоglxdarumatest	100%
INR0247	preprodsec-icetexboglxxroad2n	100%
INR0248	icetexboglxxroad3	100%
INR0249	xroadsec-icetexboglxxroad1	100%
INR0250	qasec-icetexboglxxroadtest	100%
INR0262	icetexboglxorfeo2	100%
INR0276	cxvodaprodn011	100%
INR0277	cxvodaprodn021	100%
INR0278	cxvodacontn011	99,94%
INR0240	icetexbogelasticserver2	100%
INR0260	icetexbogosbognfs1	100%
INR0252	icetexbogosbognfs2	99,93%
INR0236**	ictxbogsrvpt1	100%
INR0235**	ictxbogsrvpt2	100%
INR0000322	ictxcontroldoc	100%
INR0226	mira	100%
INR0253*	bastion	99,97%
INR251	Openshift	41,07%
INR254	Openshift	41,07%
INR255	Openshift	41,07%
INR256	Openshift	41,07%
INR257	Openshift	41,07%
INR258*	Openshift	100%
INR259	Openshift	41,07%

Tabla 29 Códigos relacionados Disponibilidad Servicios en Housing – Datacenter Principal

**Estos dos servidores (ictxbogsrvpt1 y ictxbogsrvpt2) en el mes de diciembre se solicitó por parte del ICETEX dar de baja y distribuir sus recursos en los servidores de OPENSHIFT, dicha solicitud quedo aplicada la cierre del mes de diciembre, por lo tanto no se visualiza en el Reporte de disponibilidad ELK Reporte Monitoreo ICETEX Febrero 2025-ELK.pdf, 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 de Openshift (Master) INR258 se encuentra actualmente en proceso de reinstalación por parte de ICETEX, lo que provoca que no esté visible en el sistema de monitoreo. De igual manera, el servidor bastion también del cluster de Openshift no está siendo visible en el monitoreo. Una vez que ICETEX finalice este proceso, se reactivará el monitoreo correspondiente.

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 30 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 presento en el mes de febrero un **UPTIME del [99,94%]** tal como se evidencia en la gráfica a continuación.

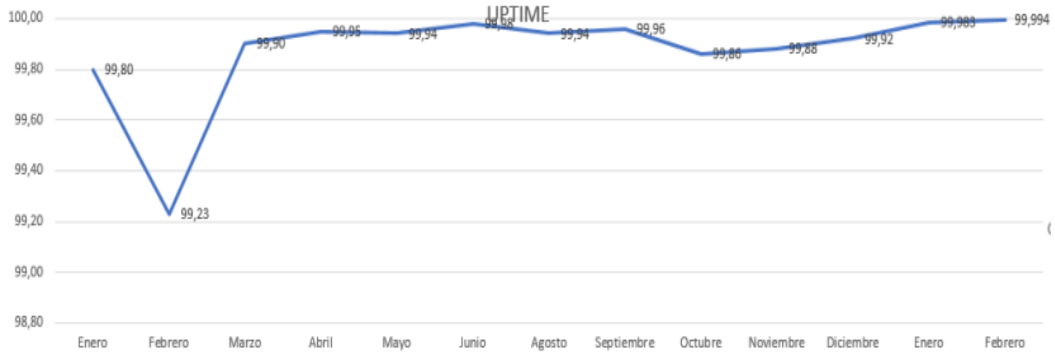


Ilustración 28 UPTIME – Portal WEB web.ICETEX.gov.co

Durante el mes de febrero se evidenció un comportamiento estable del portal WEB institucional y se cumplió con el porcentaje de disponibilidad de este con un porcentaje del **99,94%,** en este informe mensual se incluyen métricas e indicadores que contribuyen al entendimiento y al comportamiento del servicio, tales como número de visitantes donde se evidencia que el portal WEB cuenta para este mes con un total de 558 mil usuarios, con 291 mil usuarios nuevos. El tiempo de interacción medio es de 1 minutos 59 segundos, señalando el interés de la audiencia en las diferentes páginas del portal web.ICETEX.gov.co.

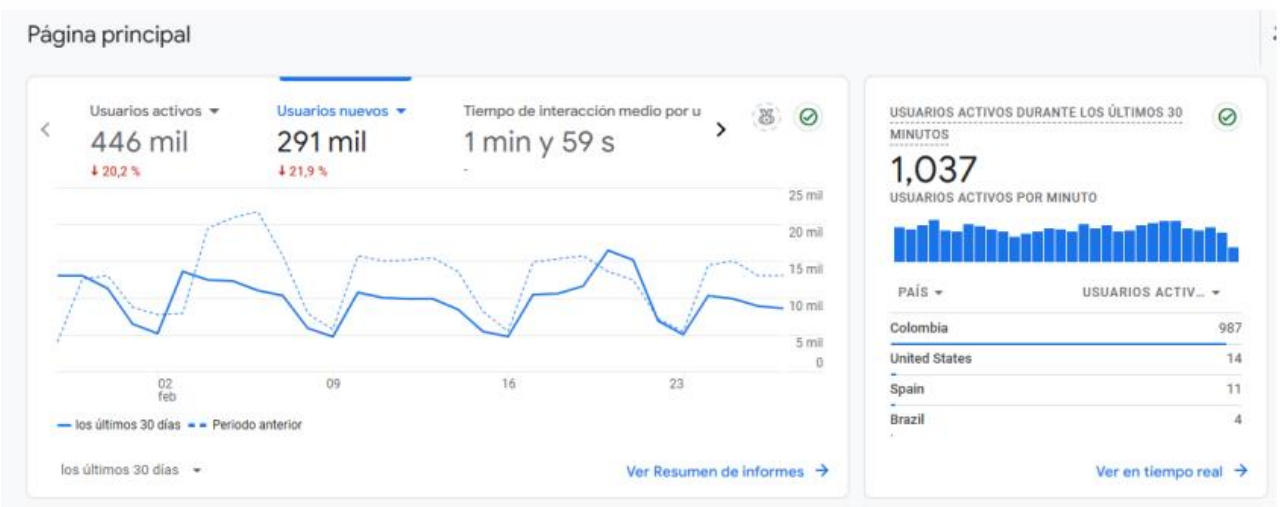


Ilustración 29 Métrica de visitantes Portal WEB web.ICETEX.gov.co

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

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 Medellín.

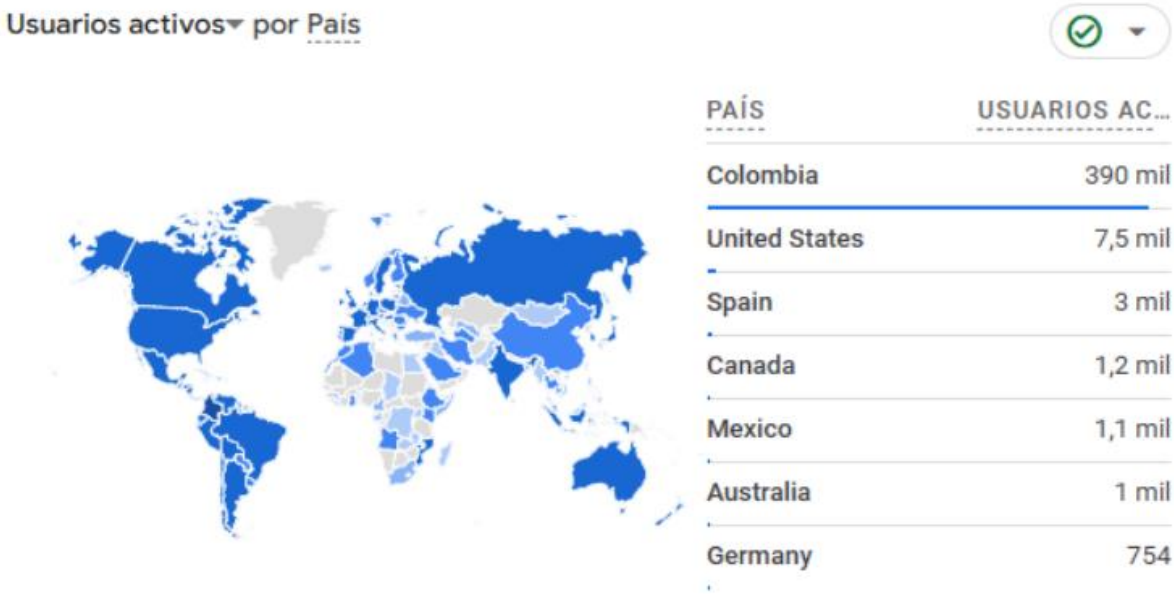


Ilustración 30 Métrica de usuario por país - Portal WEB web.ICETEX.gov.co

Métricas por tecnologías de acceso: El sistema operativo con el que más se acceso el portal web es Windows seguido de Android, así como el navegador web más usado es Chrome seguido por Safari. También podemos evidenciar que los dispositivos móviles se imponen frente a los computadores.

A continuación, se muestran las gráficas referentes a memoria RAM y almacenamiento en los nodos 1 y 2 del portal ICETEX desde el sábado 1 de febrero desde las 0:00 am hasta las 11:59 am del viernes 28 de febrero de 2.025.

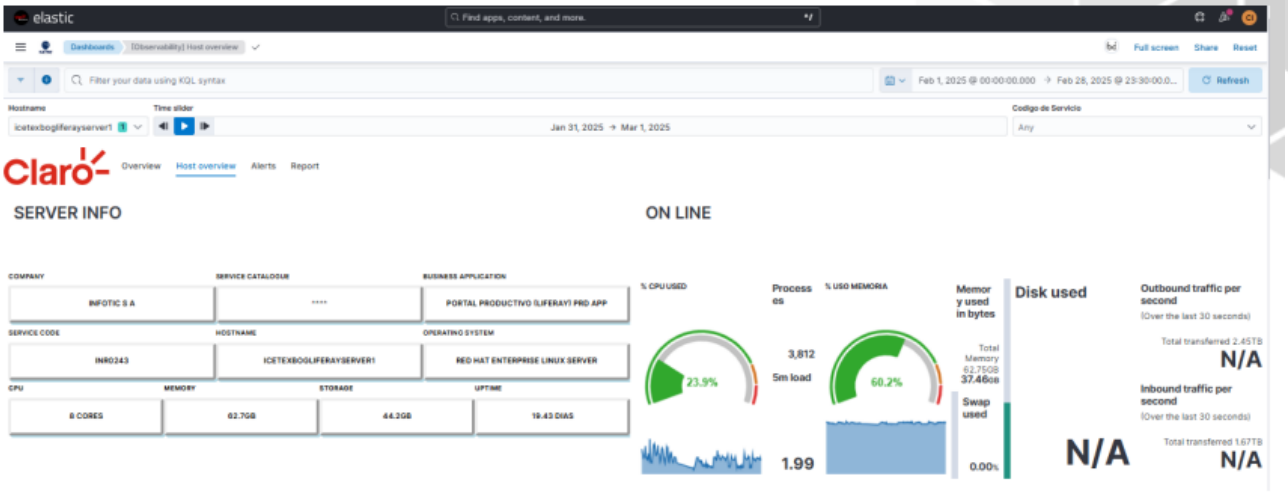


Ilustración 31 NODO 1 – Vista General – INR0243

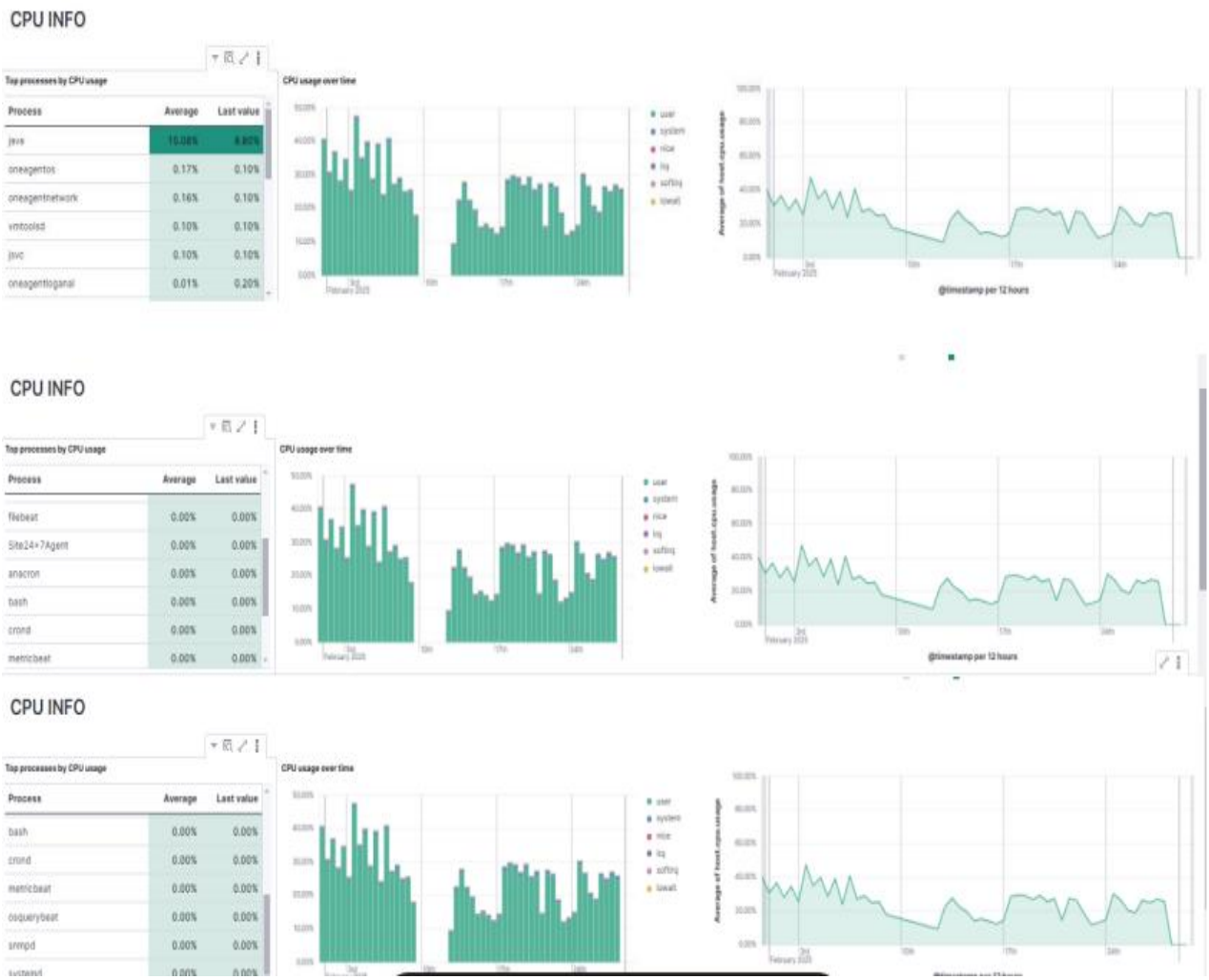


Ilustración 32 NODO 1 CPU

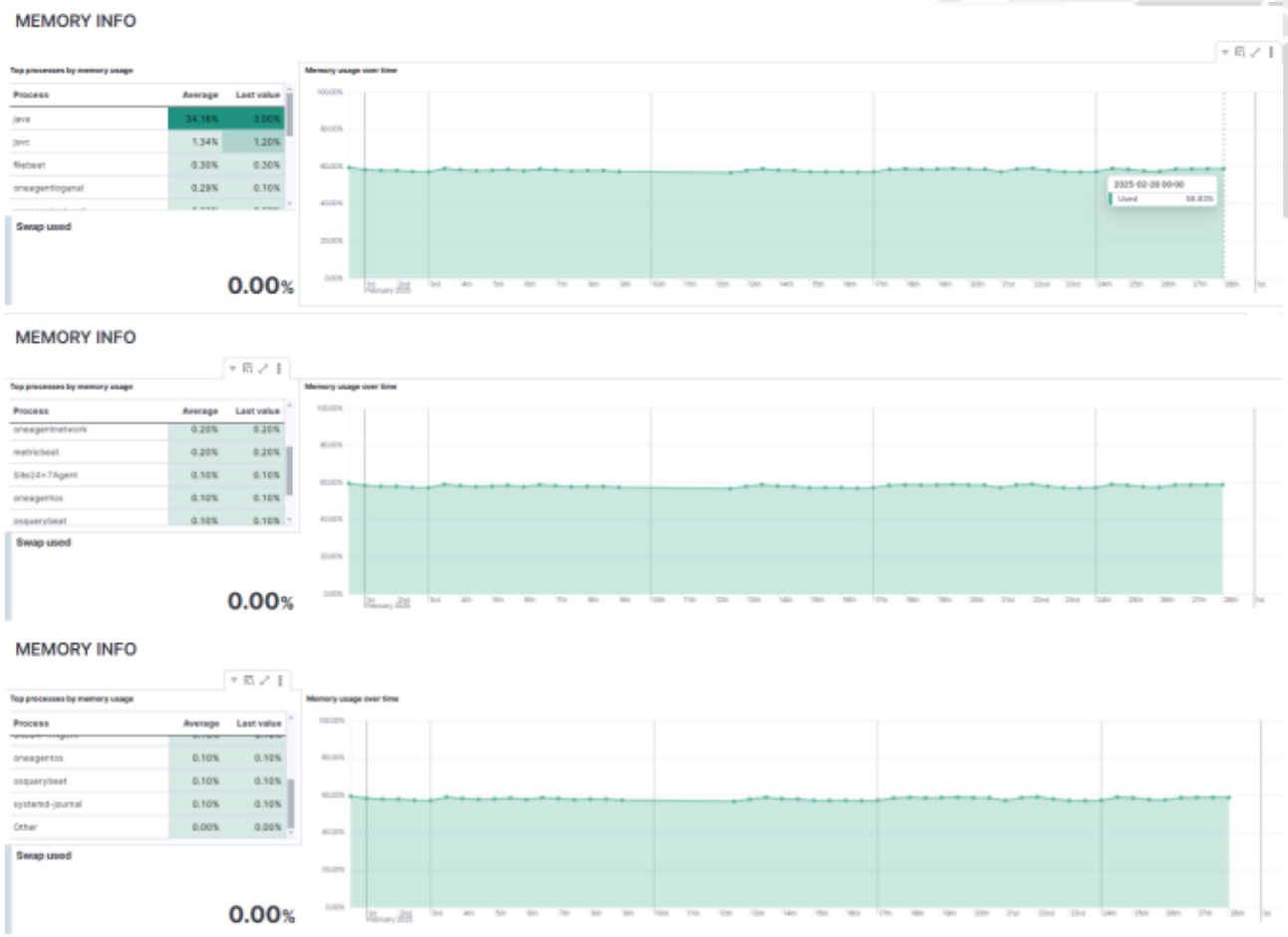


Ilustración 33 NODO 1 Memoria



Ilustración 34 NODO 1 Almacenamiento



Ilustración 35 NODO 2 – Vista General – INR0242

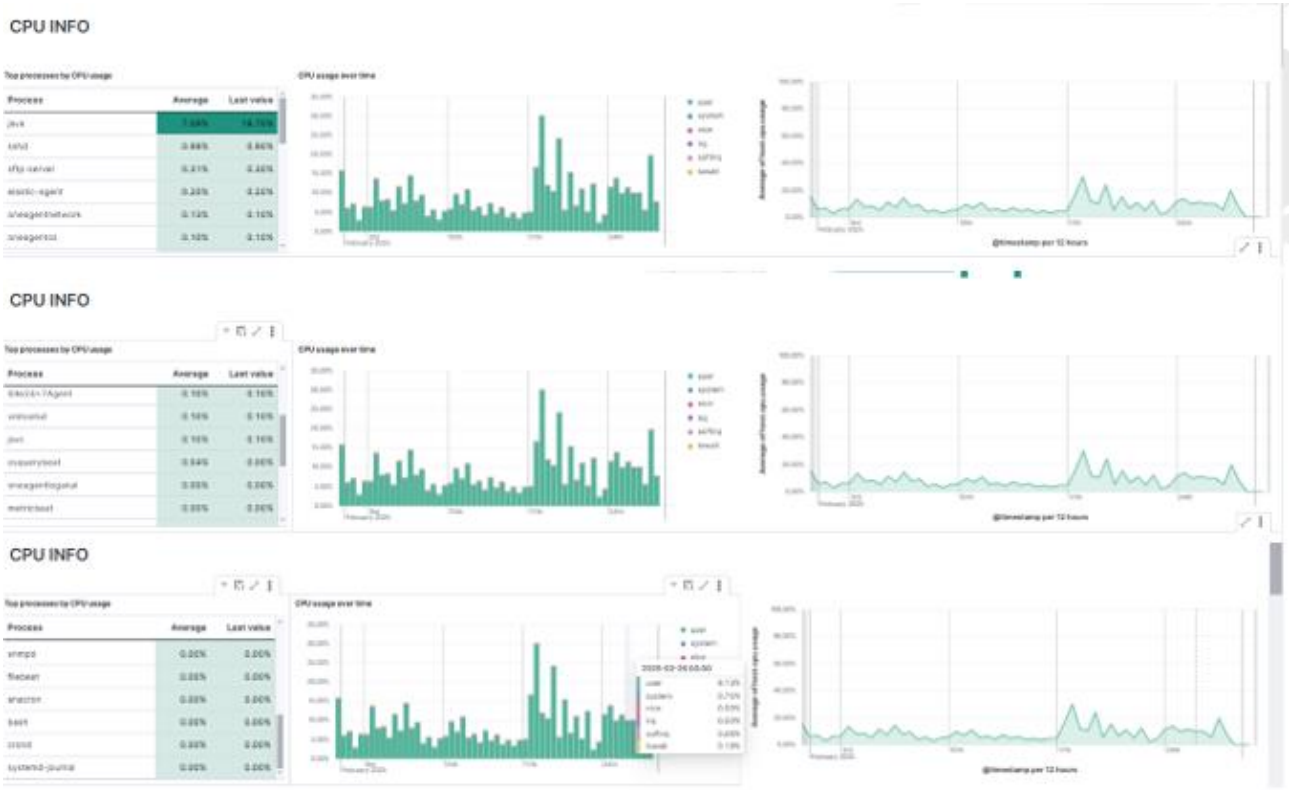


Ilustración 36 NODO 2 CPU

Durante el periodo comprendido entre el 1 y el 28 de febrero, el nodo 2 no experimentó un uso excesivo de memoria SWAP, gracias a la ejecución diaria de un código Groovy recomendado por el soporte de Liferay, correspondiente al caso **N° 125259**. Esta implementación ha permitido que el consumo de memoria SWAP en el nodo 2 se mantenga en niveles moderados. Así, al 28 de febrero de 2025 a las 9:32 a.m., el porcentaje de SWAP disponible es del 82.9%, como se puede observar en la captura de pantalla adjunta. Por lo tanto, el

aliado Claro no ha enviado más alertas por correo electrónico relacionadas con un alto consumo de SWAP en el nodo 2.

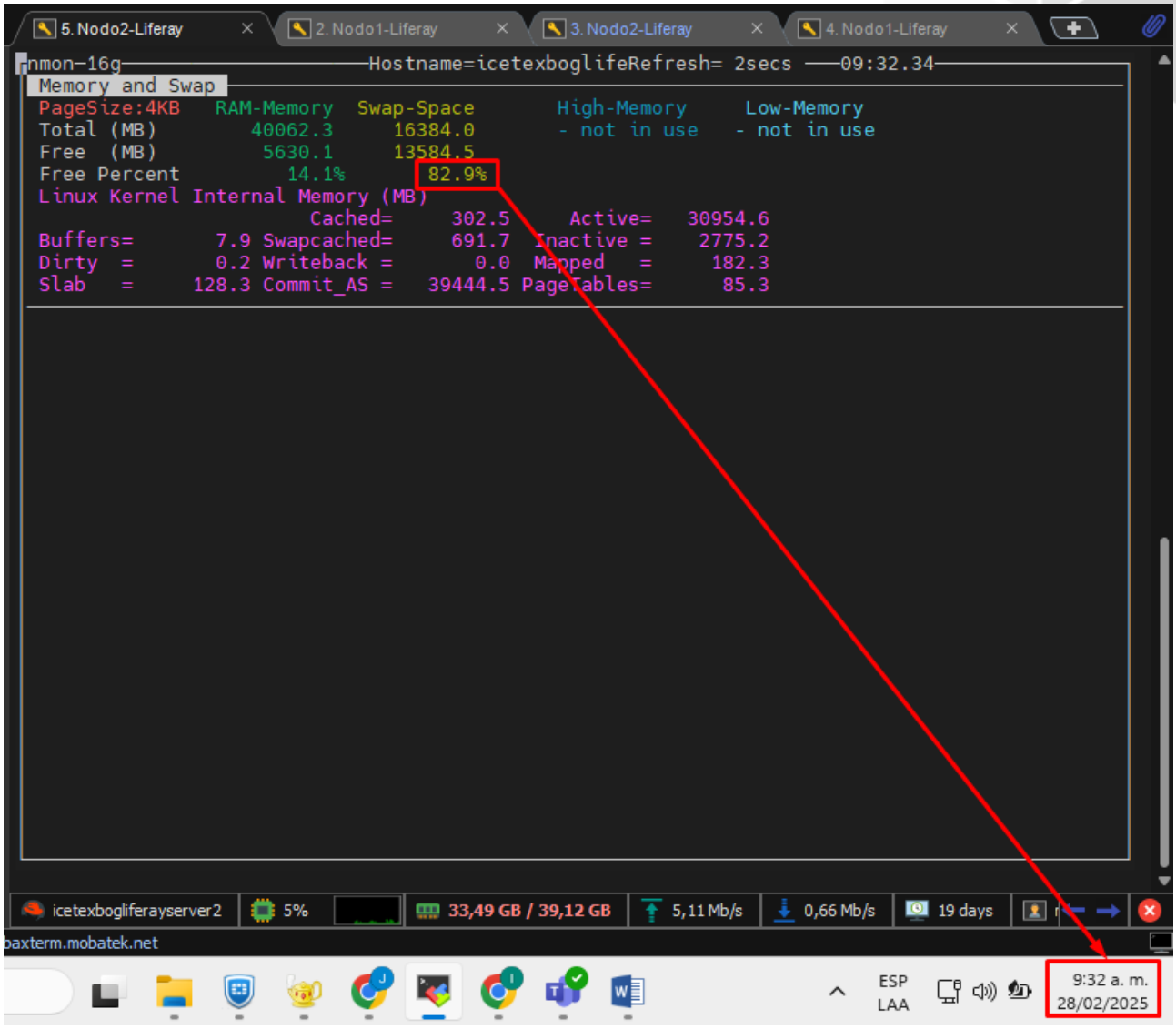


Ilustración 37 NODO 2 memoria SWAP



Ilustración 38 NODO 2 Memoria

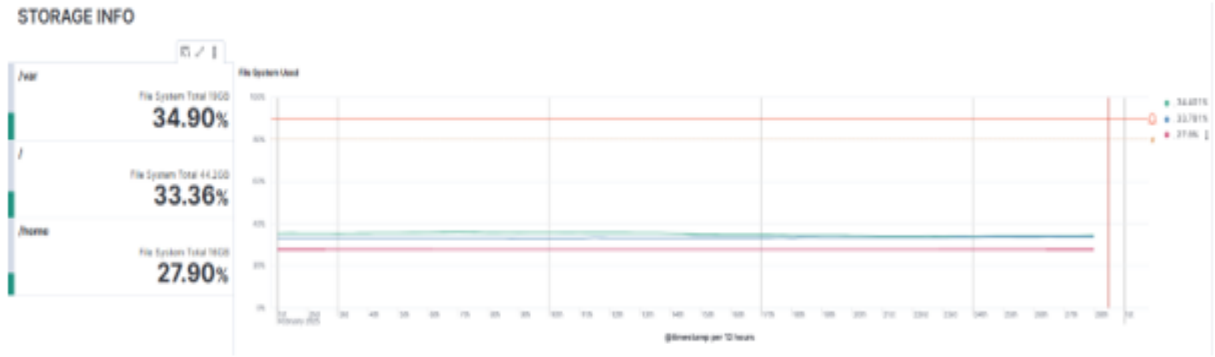


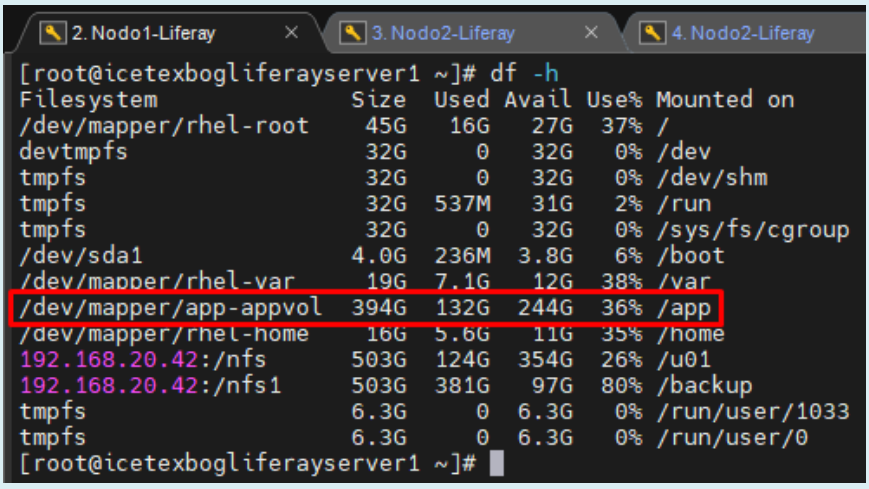
Ilustración 39 NODO 2 Almacenamiento

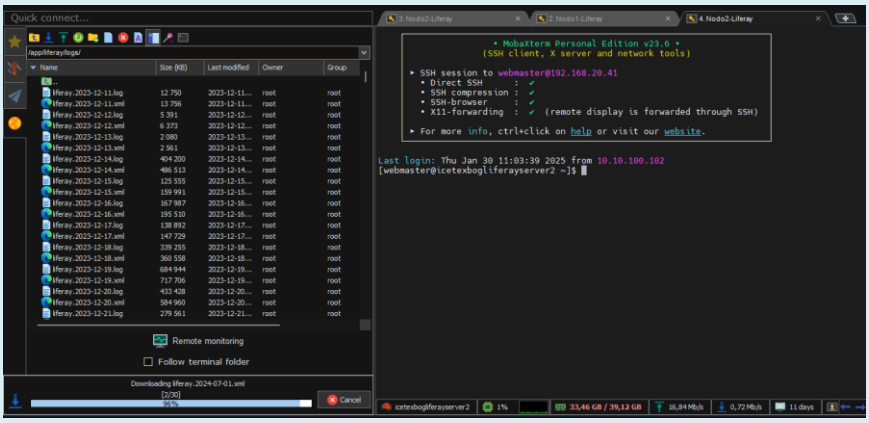
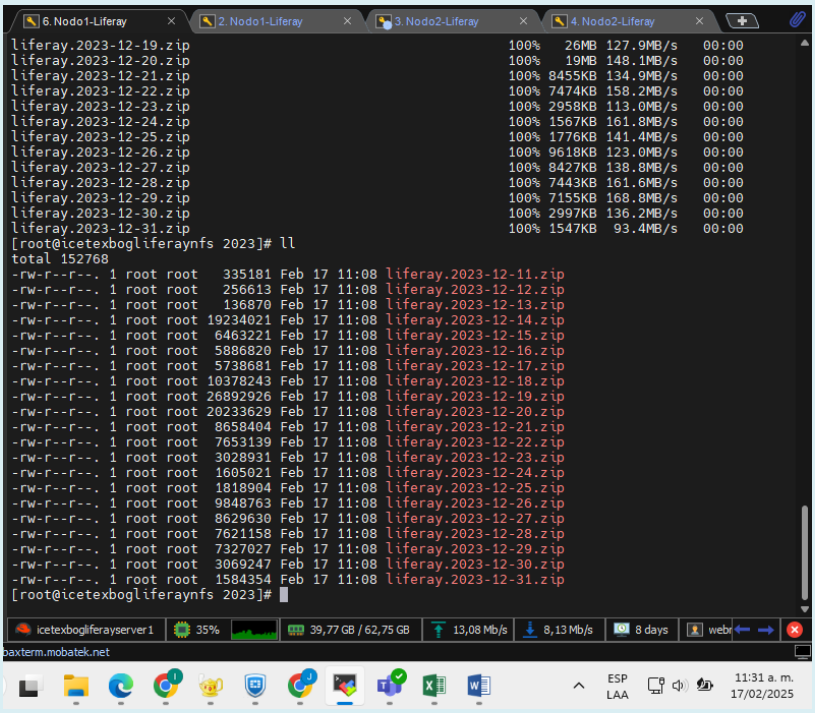
Los recursos del sistema de los servidores nodo 1 y 2, no presentaron indisponibilidad durante los 28 días del mes.

10.2.2. Análisis componente Liferay Producción

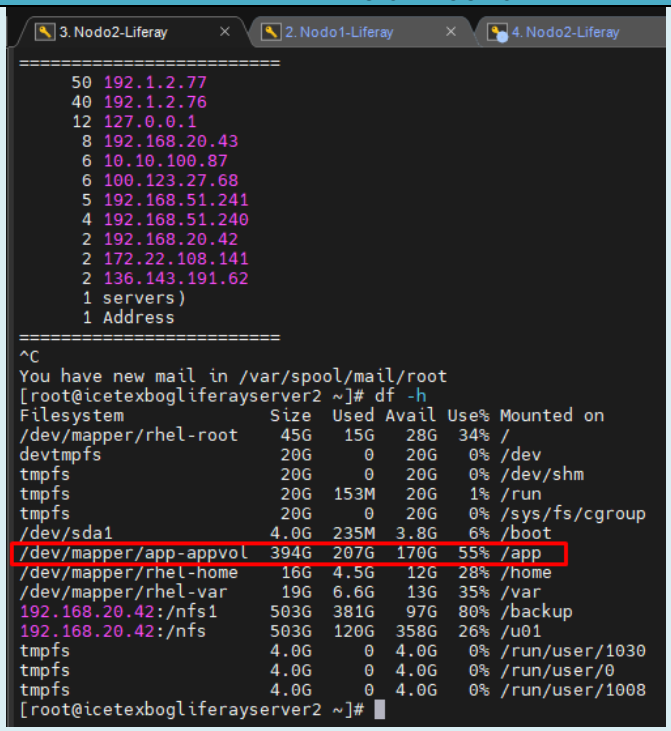
Como parte de las actividades desarrolladas por el Web máster se realiza una revisión de la infraestructura tecnológica y el entorno de software del portal Liferay, abordando aspectos fundamentales para su óptimo rendimiento y seguridad los Hallazgos encontrados en los nodos 1 y 2 del portal Liferay 7.3.10 GA1.

A continuación, se presenta un cuadro con la actualización para el presente mes con los hallazgos y observaciones:

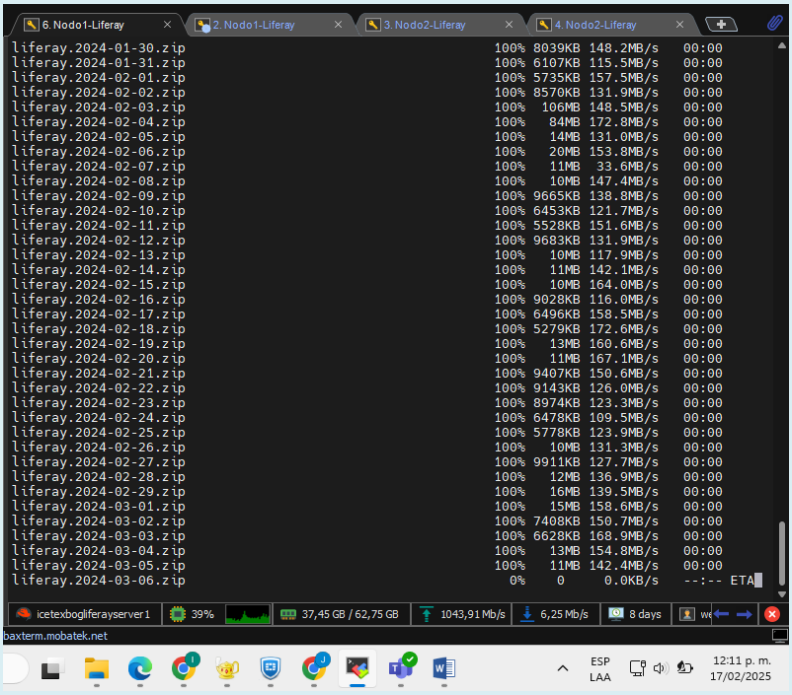
UNIDAD	HALLAZGO	OBSERVACIONES
MEMORIA RAM	**Nodo 1** total de memoria RAM – 65.79 GB. **Nodo 2** total de memoria RAM – 41.02 GB	En espera de **la autorización** para disponer y configurar la memoria necesaria para que los dos nodos queden iguales.
SISTEMA OPERATIVO	La última versión del UPDATE **del Sistema Operativo Red Hat Enterprise 7.2**, donde está alojada el servidor de Liferay 7.3.10 GA1	Está pendiente de programarse la actividad en el mes de febrero. Se tiene previsto realizar la actividad de actualización de sistema operativo Linux Red Hat 7.9 de acuerdo con el N° de Caso Claro **1116300** con el minutograma compartido por Claro. Los servicios pendientes por actualizar son los siguientes: Nodo 1 – Portal ICETEX - INR0243, Nodo 2 – Portal ICETEX - INR0242, Nodo 1 – Elasticsearch - INR0239, Nodo 2 – Elasticsearch - INR0240, Nodo 3 – Elasticsearch - INR0241 Posterior a esta actividad de actualización, un recurso de migración de realizar el cambio de Liferay 7.3 a la versión 7.4 DXP o 7.4 Quarter Released.
DISCO DURO	El espacio en disco utilizado por el CMS Liferay en el **nodo 1 es 132 GB**. El espacio disponible es de 244 GB.	**NODO 1** Comportamiento normal. Con el proceso de eliminación de logs en el nodo 1 del portal ICETEX realizado el 23 de enero por parte de los ingenieros de Claro, se cuenta con un espacio disponible de **244 GB**.  **NODO 2**

UNIDAD	HALLAZGO	OBSERVACIONES
	El espacio en disco utilizado por el CMS Liferay en el **nodo 2 es 207 GB**. El espacio disponible es de 170 GB. Cabe destacar que este indicador es antes de la eliminación de logs 10:03 a.m del 27/02/2025.	Se realizó la exportación de los logs del nodo 2 al servicio NFS, a continuación, se detalla el proceso:  Se realizó copia de los logs (.xml y .log por fecha) del año 2023 comprimidos en formato .zip a la ruta **/nfs/nodo2logs/2023/** 

UNIDAD	HALLAZGO	OBSERVACIONES



Se realiza copia de los logs (.xml y .log por fecha) del año 2024 comprimidos en formato .zip a la ruta **/nfs/nodo2logs/2024/**



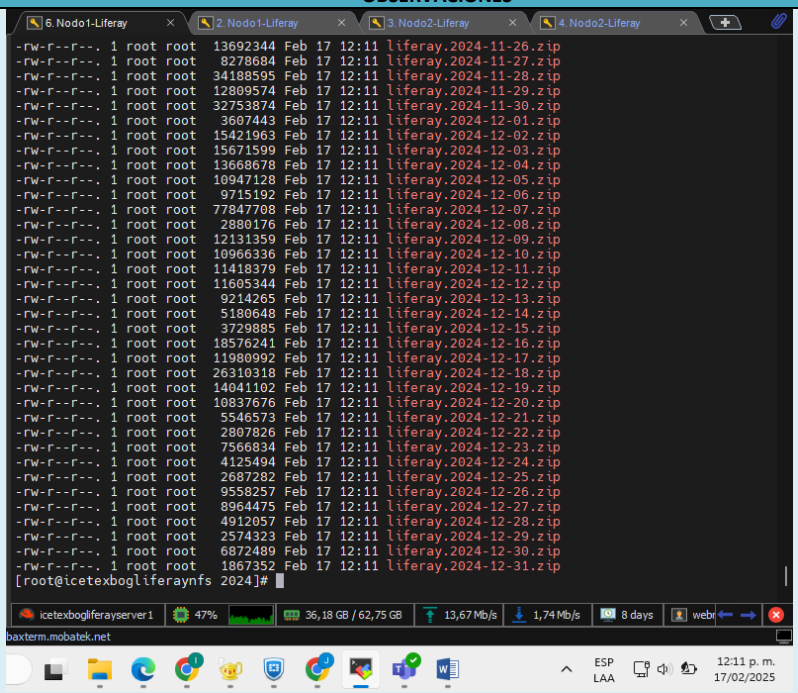
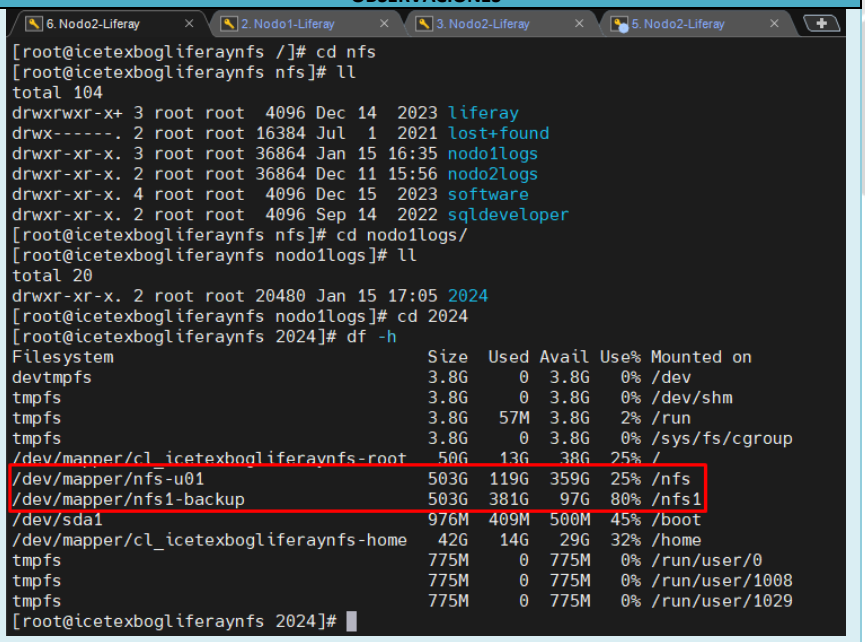
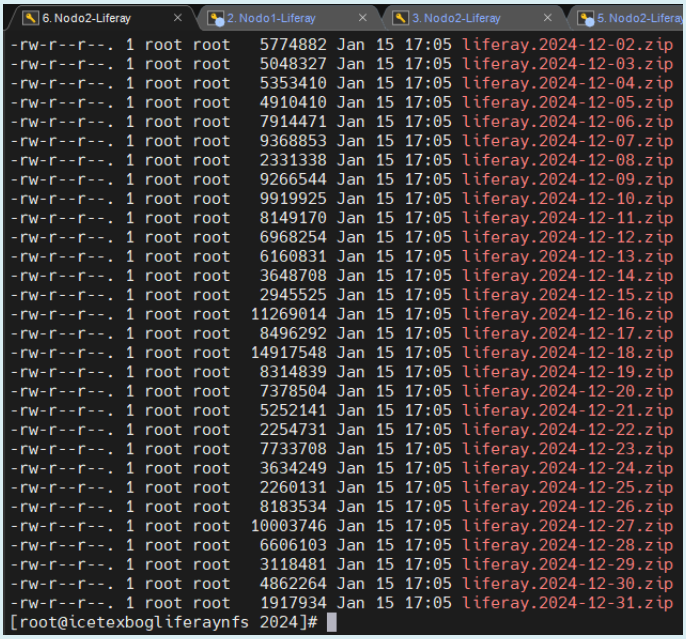
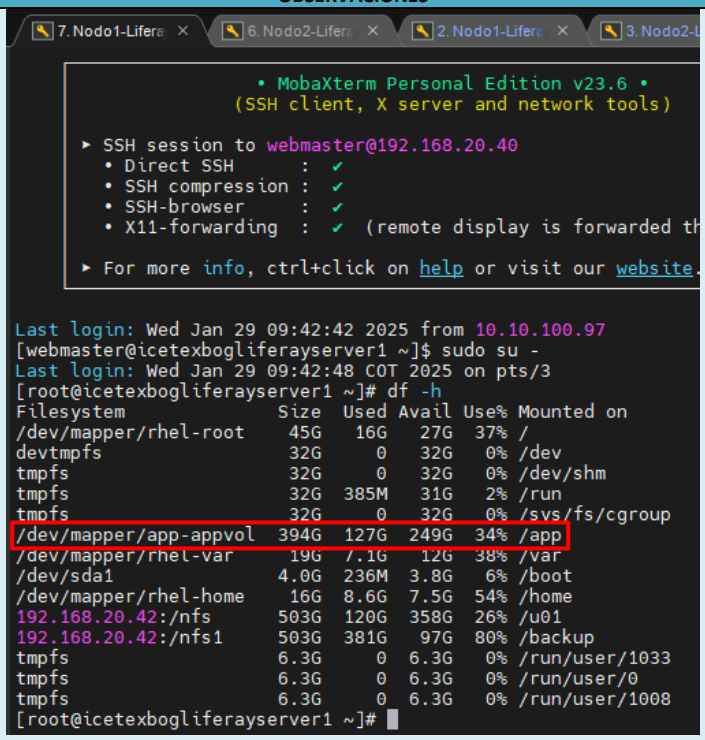
UNIDAD	HALLAZGO	OBSERVACIONES
		
FILE SYSTEM	El espacio en disco utilizado por el CMS Liferay en el **nodo 1 es 430 MB.** El espacio en disco utilizado por el CMS Liferay en el **nodo 2 es 681 MB.**	El viernes 28 de febrero a las 11:11 a.m se realizó eliminación de logs de los años 2023 y 2024 en icetexbogliferayserver2 - Nodo 2 INR0242 - 192.168.20.41 ruta **/app/liferay/logs/** con el acompañamiento del Ingeniero Carlos Javier Casanova Castillo de parte de Claro.
PARCHES DE SEGURIDAD	**Nodo 1** - activation-key-dxpproduction-7.3-icetex-publicportal 40.xml activation-key-dxpproduction-7.3-icetex-publicportal - icetexbogliferayserver1.xml **Nodo 2** - activation-key-dxpproduction-7.3-icetex-publicportal - icetexbogliferayserver2.xml	Pendiente de aprobación por parte del cliente de la renovación de soporte Liferay. Con la renovación se garantiza que el recurso que realice la actividad de migración obtenga del fabricante el instalador de Liferay 7.4 DXP para WildFly y sus parches de seguridad.
VOLUMEN DE LOGS	Registro de logs entre finales de noviembre comienzos de diciembre.	No se registran errores de logs en los nodos 1 y 2 del portal ICETEX. Está pendiente una reunión con los ingenieros de Claro para que ellos realicen la eliminación de los logs del nodo 2 desde el 11 de diciembre de 2023 hasta el 31 de diciembre de 2024.

Tabla 31 Actualización – Análisis componente LIFERAY febrero

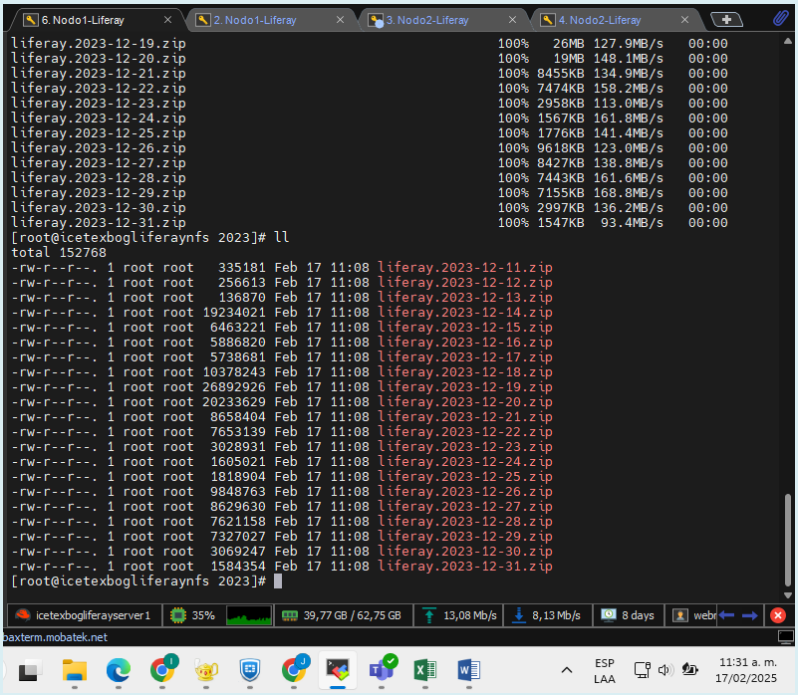
10.2.2. SERVICIO NFS – BACKUP DE NODOS 1 Y 2 DEL PORTAL ICETEX

UNIDAD	HALLAZGO	OBSERVACIONES
DISCO DURO	**Partición NFS** total de espacio en disco – 503 GB, espacio usado 119 GB, espacio disponible 359 GB y porcentaje usado 25%. **Partición NFS1** total de espacio en disco – 503 GB, espacio usado 381 GB, espacio disponible 97 GB y porcentaje usado 80%.	 Se realizó la copia de los archivos logs comprimidos en formato .zip del nodo 1 del portal ICETEX (.xml y .log por fecha) a la carpeta **/nfs/nodo1logs/2024/** del servicio NFS.  Posterior a este proceso, se realizó reunión el 23/01/2025 con el partner Claro para eliminar los logs del nodo 1 del portal ICETEX, que corresponden desde el 1 de enero hasta el 31 de diciembre de 2024, con el acompañamiento del Ing. de Claro Silder Mauricio Quiñones Sánchez, quedando el nodo 1 del portal ICETEX con un espacio disponible de **249 GB**.

UNIDAD	HALLAZGO	OBSERVACIONES



Se realiza copia de los logs (.xml y log por fecha) del año 2023 en la ruta **/nfs/nodo2logs/2023/**



Se realiza copia de los logs (.xml y .log por fecha) del año 2024 comprimidos en formato .zip a la ruta **/nfs/nodo2logs/2024/**

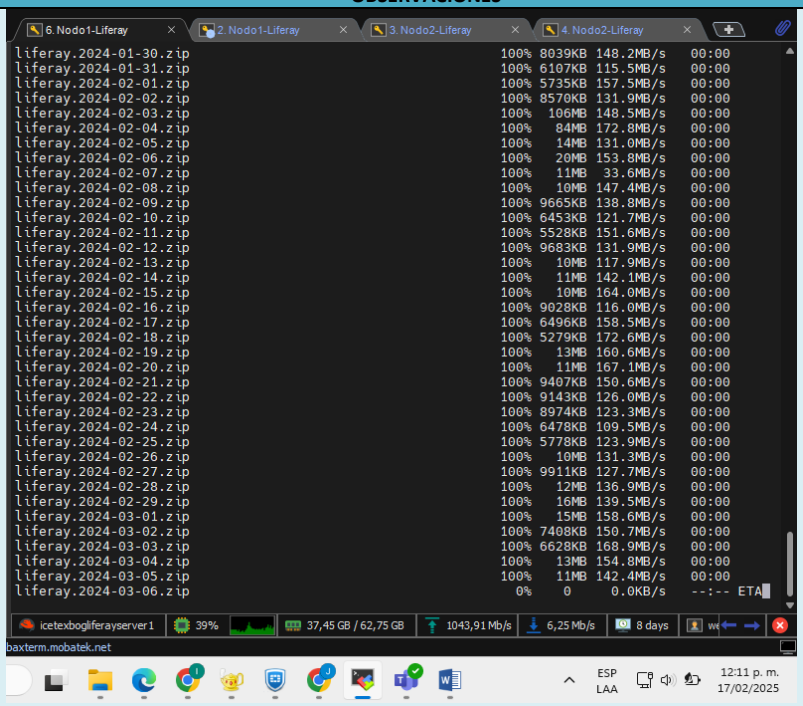
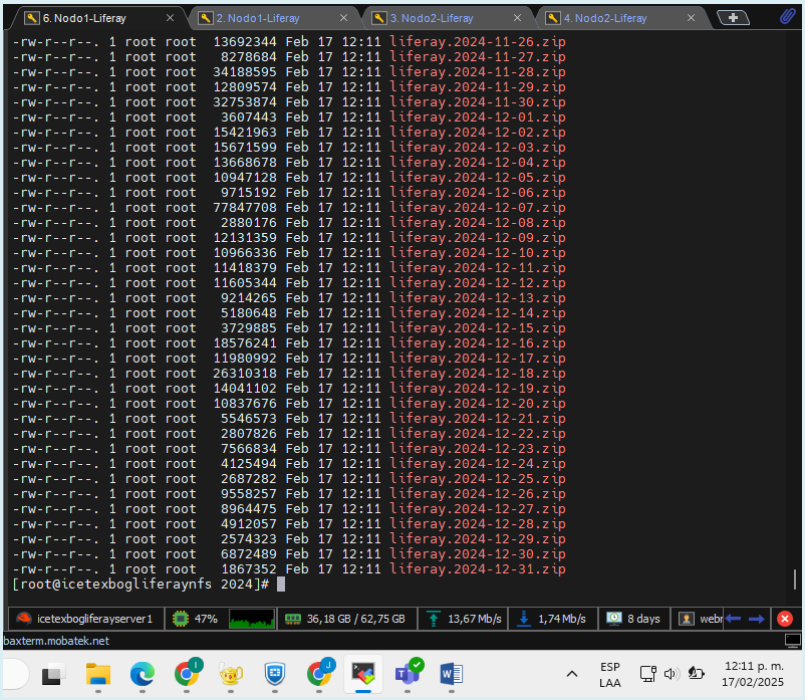
UNIDAD	HALLAZGO	OBSERVACIONES
		  El viernes 28 de febrero a las 11:11 a.m se realizó eliminación de logs de los años 2023 y 2024 en icetexbogliferayserver2 - Nodo 2 INR0242 - 192.168.20.41 ruta **/app/liferay/logs/** con el acompañamiento del Ingeniero Carlos Javier Casanova Castillo de parte de Claro.

Tabla 32 servicio NFS– backup de nodos 1 y 2 del portal ICETEX

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

	Diciembre	Enero 2025	Febrero 2025
Usuarios mes	676000	558000	446000
Usuarios nuevos	459000	373000	291000
Tiempo acceso (seg)	146	137	119

Tabla 33 Distribución trimestral de acceso por usuarios

Durante el último trimestre, el portal web recibió un promedio de 560.000 usuarios, lo que refleja un interés significativo en los servicios y contenidos ofrecidos por la entidad. Sin embargo, al analizar los datos correspondientes al mes de febrero, se observó una disminución del 20.10% en el número de usuarios que accedieron a la página. Esta caída representa aproximadamente 112,000 usuarios menos.

Durante el último trimestre, se ha observado que, en promedio, 374.333 nuevos usuarios accedieron a la página. Sin embargo, es importante destacar una tendencia negativa en relación con los accesos nuevos en febrero, la cifra de usuarios nuevos experimentó una disminución del 21.98%, lo que representa un total de 82,000 usuarios.

Las siguientes Url´s están siendo monitoreadas desde la herramienta ELK y en el mes de febrero tuvieron la disponibilidad del 99.98%:

- http://www.icetex.gov.co
- http://web.icetex.gov.co
- www.icetex.gov.co

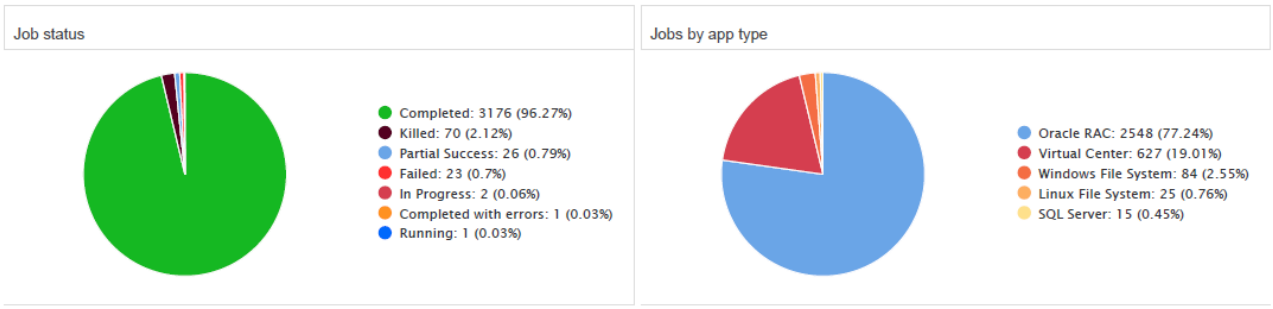
10.2.3. Backup Servidores Triara

Durante el periodo de febrero se realizaron los Backups de acuerdo con las políticas definida por el ICETEX, las cuales desde su inicio se implementaron en el Datacenter. Se puede verificar en el documento, Informe Backups mes de febrero 2025.pdf que se genera con el análisis del comportamiento de los backups durante el mes y se adjunta el reporte de los backups que se genera automáticamente desde la herramienta que se utiliza para realizar los backups.

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 Backup que se encuentra actualizada con la operación actual.

Politica Backup Icetex.xlsx

Para el mes de febrero el resultado de la ejecución de los Backups fue:



Summary

Job status	Total Jobs	Size of Application	Media Size	Protected Objects	Failed Objects	Failed Folders
Completed	3176	206.61 TB	31.46 TB	98802821	8305	33
Killed	70	0.00 BYTES	0.00 BYTES	0	0	0
Partial Success	26	1.47 TB	26.16 GB	0	26	0
Failed	23	0.00 BYTES	0.00 BYTES	0	40	0
In Progress	2	572.25 GB	1.21 GB	0	2	0
Completed with errors	1	18.81 GB	8.05 GB	1	0	0
Running	1	2.90 TB	13.74 GB	4304318	0	0

1 - 7 of 7 items

Ilustración 40 Evidencia Backup servidores resumen Backups y su estado

En el caso de los Backups que no fueron exitosos o que presentan algún tipo de problema son reportados a las áreas correspondientes para gestionar las sesiones de trabajo con el operador CLARO para solucionar la falla y proceder a la toma de la copia de respaldo de acuerdo con lo estipulado.

El total del tamaño de la información respalda en cintas de Backups para el mes de febrero corresponde a 214.61 TB, donde 96.27% se completó en el primer lanzamiento del robot con un total de 206.61 TB de información.

El 77.24% está representado en el respaldo dado a la información del Oracle RAC.

Se realiza el comparativo del último trimestre con respecto a la toma de backup con el siguiente resultado:

Tareas	Diciembre	Enero 2025	Febrero 2025
Completado	98.62%	97.89%	96.27%
Fallido	0.59%	0.78%	0.7%
Cancelados	0.5%	0.78%	2.12%
Terminados parcialmente	0.23%	0.47%	0.79%
Completado con errores	0.03%	0.04%	0.06%
En Proceso	0.03%	0.02%	0.06%
Tamaño	**562.01 TB**	**341.45 TB**	**214.61 TB**

Tabla 34 Distribución trimestral de Backup ejecutados

El promedio de los Backups completado del último trimestre en el primer lanzamiento del robot fue de 97.59%, donde el mes con mayor nivel de ejecución fue diciembre con 98.62%, el 2.41% corresponde a los siguientes parámetros: Fallido, Cancelados, Terminados parcialmente, Completado con errores y En Proceso.

El promedio de toma Backups Fallido durante el último trimestre corresponde a 0.69%, el mes donde más se presentó un mayor porcentaje de fallas fue enero con el 0.78%

	Diciembre	Enero 2025	Febrero 2025
Oracle RAC	93.36%	86.52%	77.24%
Virtual Center	5.51%	11.87%	19.01%
Windows File System	0.79%	1.47%	2.55%
Linux File System	0.22%	0.45%	0.76%
SQL Server	0.12%	0.18%	0.45%

Tabla 35 Distribución trimestral de Backup por servicios

- El servicio que ocupo el mayor porcentaje en la toma de backup fue el ORACLE RAC.
- El promedio del último trimestre del respaldo de Oracle RAC fue de 85.71% donde el mes con mayor tamaño de información respaldada fue diciembre con el 93.36%

NOTA 1: En el caso de los Backups que no fueron exitosos o que presentan algún tipo de problema son revisados de forma interna por parte de CLARO, subsanados y nuevamente tomados por el área correspondiente, para el caso de los que no se pueden solucionar se escalan con el cliente para que se revise la falla y se proceda a ejecutarlos nuevamente.

NOTA 2: la evidencia se genera diariamente en el reporte que se entrega de forma automática por parte del operador tecnológico a los correos que el ICETEX solicito y en el informe mensual se anexan todas 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 Backup Informe de Backup

11. CONTROL DE CAMBIOS

Durante el mes de febrero 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
1116	Saturación del canal INR0000320	22/01/2025	8/02/2025	No ejecutado	Se crea el cambio 1128

Tabla 36 Controles de cambio febrero

12. PLAN DE TRABAJO DE LOS PROXIMOS MESES

Se adjunta la tabla del plan de trabajo:

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
Se debe realizar mesa técnica conjunta entre ICETEX e INFOTIC para revisar las alternativas de solución respecto al licenciamiento de las herramientas de seguridad (perimetral y antivirus)	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se inicio la revisión del tema en los comités de pares que se inició el 13/02/2025 donde Se recomendó por parte de los especialistas de seguridad de INFOTIC a Icetex, la renovación de FortiSandbox en la nube y del WAF en la

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
				nube, con el fin de evitar el pago de años anteriores. Teniendo en cuenta que FortiSandbox ya no recibe actualizaciones. En cuanto al antivirus de Sophos, se encuentra pendiente la renovación para Windows 7 y Windows 2008, y se comentó por ICETEX que están considerando alternativas. Soporte de la sesión ver el acta: Acta pares de seguridad 12 13-02-2025.docx
Se debe realizar mesa técnica conjunta entre ICETEX e INFOTIC para revisar las lecciones aprendidas del último DRP y generar los planes de trabajo correspondientes antes de programar el próximo DRP debido a que la Oficina de Riesgos de ICETEX no dio por aceptado el segundo DRP realizado el 4 de noviembre de 2024.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se tiene pendiente la definición del alcance del próximo DRP, se define con ICETEX generar sesión ICETEX-INFOTIC-OPERADOR CLARO para retomar el tema con la opción del WAF virtual expuesto por INFOTIC y de Icetex incluir al ing. Carlos cruz quien es el supervisor encargado. Soporte de la sesión ver el acta: Acta pares de seguridad 12 13-02-2025.docx
Se debe realizar mesa técnica conjunta entre ICETEX e INFOTIC para revisar las alternativas de solución frente a la gestión de vulnerabilidades.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Con respecto a las vulnerabilidades de los Portales y seguridades a nivel de cabeceras está pendiente la respuesta a los especialistas de seguridad de INFOTIC del correo: de asunto: seguridades aplicadas desde el WAF—ambiente de pruebas. El ingeniero Jhon Pava reenviara el correo a ICETEX para retomar el tema e involucrar a los interesados. Soporte de la sesión ver el acta: Acta pares de seguridad 12 13-02-2025.docx
Se debe realizar mesa técnica conjunta entre ICETEX e INFOTIC para revisar los informes de Backup, su forma de presentación frente a las necesidades de ICETEX, los resultados periódicos de las pruebas de restauración y en caso de requerirse, realizar los planes de trabajo correspondientes.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Está pendiente coordinar la sesión con los especialistas de ICETEX, se realizará 12/03/2025
Actualización el sistema operativo LINUX de la versión 7.2 a la versión 7.9	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se está preparando propuesta comercial para presentar a ICETEX de la infraestructura paralela para la realización de las actualizaciones de S.O. y pruebas de sobre los servidores del Portal de ICETEX.
Actualización de Liferay de la versión 7.3 a la 7.4	INFOTIC - ICETEX	01-dic-24	28-mar-25	Depende del numeral anterior y la actualización del soporte de liferay.
Verificar la configuración de los equipos de LAN y WAN que hace falta para el funcionamiento de IPv6.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se está haciendo seguimiento a estos temas de implementación de IPV6 en las sesiones señales que se comenzaron en febrero.
Traslado de los equipos de servicio de internet para la nueva sede de Arauca	INFOTIC - ICETEX	01-dic-24	28-feb-25	En el mes de febrero quedo culminado el traslado del canal de Arauca.
Instalación del canal Backup de Quibdó	INFOTIC - ICETEX	01-dic-24	28-feb-25	El canal de Backup de Quibdó, ya quedó instalado en el cuarto de comunicaciones del centro comercial el 27/02/2025, para habilitar el servicio en el local es necesario que Icetex solicite a la administración del CC Airplan la Cross-conexión desde el cuarto de equipos del CC hasta el cuarto de equipos de la agencia de Icetex. Ese cableado es exclusivo del CC. Se envía correo con esta solicitud a Icetex 24/02/2025 y 27/02/2025,
Instalación del canal principal de Puerto Carreño	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se envía el 11/02/2025 la OFERTA PV-594-1 ICETEX - INFOTIC: instalación recursos tecnológicos sede Puerto Carreño.
Nueva configuración de SD WAN en	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se está trabajando en el tema hay que enviar

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
triara				una información y se acuerda que estos temas se van a trabajar en conjunto Networking y seguridad, es una mejora en la solución instalada. Soporte de la sesión ver el acta: Acta pares de seguridad 12 13-02-2025.docx
Gestión de la administración Azure nube	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se coordinará la sesión el con ICETEX y el integrador de NUBE para definir las acciones a implementar. Fecha propuesta : 17/03/2025
Políticas e inventarios de las creaciones en la nube	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se coordinará la sesión el con ICETEX y el integrador de NUBE para definir las acciones a implementar. Fecha propuesta : 17/03/2025
Seguimiento a la adquisición de los Takedown por parte de ICETEX	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se envió un correo el 29 de noviembre 2024 notificando a ICETEX que no hay más Takedown disponibles, se espera respuesta de ICETEX. Claudia de Wexler envía a INFOTIC las alternativas para reportar estas páginas desde el ICETEX. Soporte de la sesión ver el acta: Acta pares de seguridad 12 13-02-2025.docx
Capacitación en seguridad al grupo de especialistas de seguridad del ICETEX	INFOTIC - ICETEX	01-dic-24	28-mar-25	El tema se revisará con INFOTIC para coordinar con Icetex las capacitaciones de valor agregado. Soporte de la sesión ver el acta: Acta pares de seguridad 12 13-02-2025.docx
Monitoreo de los diferentes servicios realizados por el SOC. Revisión conjunta entre ICETEX – INFOTIC	INFOTIC - ICETEX	01-dic-24	28-mar-25	Realizar una revisión conjunta para determinar si los dispositivos se están monitoreando. Soporte de la sesión ver el acta: Acta pares de seguridad 12 13-02-2025.docx
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-dic-24	28-mar-25	Se coordinará la sesión con los ingenieros de CLARO, INFOTIC e ICETEX para revisar y generar la solución, se mueve la fecha de la sesión para el mes de marzo por porque se presentaron actividades prioritarias de la operación por parte del DBA.
Realizar mesa técnica entre ICETEX e INFOTIC para la revisión del alcance de Antivirus.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Perfiles de navegación se enviaron a Icetex y está pendiente de que confirmen si se van a aplicar. Jairo Acevedo INFOTIC, enviará el correo para retomar. Soporte de la sesión ver el acta: Acta pares de seguridad 12 13-02-2025.docx
Reunión técnica de aclaraciones del diagrama de red para la realización del DRP Link Minutograma tecnico DRP Noviembre actualizado.xlsx pestaña diagrama.	INFOTIC - ICETEX	01-dic-24	28-feb-25	Depende del nuevo alcance que se defina del DRP. Soporte de la sesión ver el acta: Acta pares de seguridad 12 13-02-2025.docx
Realizar mesa de trabajo técnica en la cual se exponga claramente el cumplimiento de la implementación del canal DWDM de acuerdo con el anexo 2.1 punto 19 a satisfacción de ICETEX.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se realizó una sesión el 27/02/2025 personal de preventa de CLARO y Especialista de Networking de ICETEX donde se aclaran dudas frente al cumplimiento del canal de replicación frente al requerimiento contractual.
Solicitud de instalación de (5) Internet para la gente en las Oficinas ICETEX de Manizales, Armenia, Cartagena, Sincelejo y Pasto.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se encuentra del lado comercial de INFOTIC la propuesta, una vez se tenga se enviará a ICETEX.
Solicitud de Monitoreo de la LAN de todas las sedes	INFOTIC -ICETEX	01-dic-24	28-mar-25	Se realizó el requerimiento al aliado de CLARO para dar respuesta a solicitud de ICETEX .

Tabla 37 Planes de trabajo

13. RECOMENDACIONES DEL CONTRATISTA AL ICETEX

Las siguientes son las recomendaciones para el mes de febrero que desde cada servicio de especialistas asignados al proyecto ICETEX realizan para mejorar los diferentes ámbitos, se llevará a cabo una colaboración entre INFOTIC y el ICETEX para implementar las recomendaciones, asegurando que cada uno contribuya desde su ámbito de acción.

13.1. Administrador WEB MASTER

- La renovación del soporte de Liferay, que se mantuvo activo hasta el 31 de enero de 2025, es esencial para garantizar la colaboración del fabricante en varios procesos. Esto incluye la obtención de nuevos instaladores, parches de seguridad, claves de licencia para el entorno productivo, así como para pruebas y desarrollo en localhost. Además, es fundamental para llevar a cabo la migración a la nueva versión Liferay 7.4 GA125

13.2. Administrador 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: Durante este mes, se reportó un daño en uno de los equipos en la sede de San Andrés, el cual fue reemplazado por otro dispositivo del ICETEX. Sin embargo, se debe notificar a ICETEX que actualmente no hay disponibilidad de equipos adicionales para reemplazos futuros en caso de que surjan nuevos daños.

- Cableado estructurado: Se sugiere cambiar el cableado estructurado de todas las sedes ya que se está cristalizando, llevando a daños de físicos presentando intermitencias a los usuarios

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

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

13.4. Administrador de 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.

- El antivirus de symatec en las bases de datos siguen inactivos hasta no tener claro las parametrizaciones de restricción y los problemas ocasionados de conexión.

- Sigue pendiente retirar permiso de sudo a los usuarios infotic, gawuser y dcscaf con esto usuarios podrían realizar actividades administrativas que no van con su role.

- Se debe aprovisionar más almacenamiento para las bases de datos de producción ya que se encuentra en estado crítico, solo queda disponibles 289G.

13.5. Administrador de aplicaciones

- Se aconseja a los usuarios finales que, aunque se presta atención a todas las solicitudes, estas deben ser gestionadas a través de la mesa de servicio de Aranda, dado que aún hay casos que se manejan sin un registro adecuado.

- Las aplicaciones desarrolladas en Framework .Net Classic deben ser migradas a un Framework actual y con soporte.

- Asimismo, se sugiere que las aplicaciones que operan en sistemas operativos obsoletos sean trasladadas a servidores que utilicen versiones actuales y con soporte vigente de Microsoft.

- Finalmente, se recomienda que cada aplicación web disponga de su propio servidor.

13.6. Integrador Nube

- Contratar persona delegada y/o responsable de la nube que pueda escalar necesidades a nivel interno en la entidad o en su defecto, continuar con la ingeniería con la que se trabajó durante el 2024 para mantener continuidad.

- Definir procedimientos y cronograma para la creación de futuros recursos masivos, en este caso, VMs si es el caso.

- Continuar con la remediación de hallazgos, en el correo se respondieron algunas dudas, pero falta la implementación de los tags solicitados para tener un mayor seguimiento sobre los recursos y su monitoreo.

- Levantar la información pendiente para comprender las necesidades, solicitantes, aprobadores y finalmente, justificaciones de lo existente, la entidad debe contar con una documentación e inventario de todo lo que existe en la nube como también, aplicaciones de la entidad.

- Los tags en las Nubes son indispensables para llevar a cabo seguimiento y ejecución en políticas de eliminación de recursos, en otras palabras, es necesario contactar al responsable de cada recurso para confirmar su eliminación, muchas veces las personas rotan y los recursos se quedan creados, es normal solicitar la creación de recursos, pero no su eliminación, por lo que esto incluye monitoreo como tarea de administración.

- Evitar que los administradores del office 365 utilicen cuentas de administradores en la nube haciendo uso de todos los poderes y permisos administrativos sin regulación ni aprobación previa, se necesita identificar el usuario para poder escalar, sería como que un usuario siempre use el usuario root en los linux evitando su identificación.

- Se espera poder contar con un equipo de trabajo y que la entidad siga o aplique mis recomendaciones, también es vital contar con los perfiles necesarios previamente explicados en reuniones para apoyar y destrabar aplicaciones, automatizaciones, despliegues, entre otros, como también, aplicar innovación a bajo coste en la nube donde incluso se pueda contemplar la migración de OpenShift a Azure.

13.7. Seguridad

- 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 una tecnología 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.

- 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

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.

CIUDAD	Enlace - Tipo medio	INR	BW- Mínimo Requerido (MBPS)	Ancho de Banda actual	Ancho de Banda Ofrecido según Anexo 2.1
BOGOTA D.C.	Principal / FO (Sede Aguas)	INR0037	370	400	400
	Backup / FO (Sede Aguas)	INR0036	160	200	200
	Principal / IPVPN (Sede Chapinero)	INR0022	38	40	40
	Backup / IPVPN (Sede chapinero)	INR0020	22	25	25
	Principal / IPVPN (Angel)	INR0272	205	205	205
	Backup / IPVPN (Angel)	INR0273	205	205	205
IBAGUE	Principal / IPVPN	INR0073	18	20	20
	Backup / IPVPN	INR0076	8	10	10
LETICIA	Principal / Satelital	INR0000373	8	8	8
NEIVA	Principal / IPVPN	INR0039	18	20	20
	Backup / IPVPN	INR0041	8	10	10
TUNJA	Principal / IPVPN	INR0104	18	20	10
	Backup / IPVPN	INR0106	5	5	5
VILLAVICENCIO	Principal / IPVPN	INR0085	18	20	20
	Backup / IPVPN	INR0084	8	10	10
ARMENIA	Principal / IPVPN	INR0074	15	20	20
	Backup / IPVPN	INR0072	8	10	10
MANIZALES	Principal / IPVPN	INR0088	18	20	20
	Backup / IPVPN	INR0087	8	10	10
MEDELLIN	Principal / IPVPN	INR0133	63	100	100
	Backup / IPVPN	INR0132	15	20	20
APARTADO	Principal / IPVPN	INR0144	15	20	20
PEREIRA	Backup / IPVPN	INR0079	18	20	20
	Principal / IPVPN	INR0077	8	10	10
QUIBDO	Principal / IPVPN	INR0014	18	20	20
	Backup / IPVPN	0	8		
BARRANQUILLA	Principal / IPVPN	INR0103	63	100	100
	Backup / IPVPN	INR0100	15	20	20
CARTAGENA	Principal / IPVPN	INR0109	18	20	20
	Backup / IPVPN	INR0107	8	10	10
MONTERIA	Principal / IPVPN	INR0080	18	20	20

CIUDAD	Enlace - Tipo medio	INR	BW- Mínimo Requerido (MBPS)	Ancho de Banda actual	Ancho de Banda Ofrecido según Anexo 2.1
	Backup / IPVPN	INR0081	8	10	10
RIOHACHA	Principal / IPVPN	INR0164	18	20	20
	Backup / IPVPN	INR0162	8	10	10
SANTA MARTA	Principal / IPVPN	INR0154	18	20	20
	Backup / IPVPN	INR0152	8	10	10
SINCELEJO	Principal / IPVPN	INR0095	15	20	20
	Backup / IPVPN	INR0097	5	5	5
SAN ANDRES	Principal / IPVPN	INR0000367 INR0000369	8	8	8
BARRANCABERMEJA	Principal / IPVPN	0	18		20
SAN GIL	Principal / IPVPN	0	10		10
BUCARAMANGA	Principal / IPVPN	INR0062	26	30	30
	Backup / IPVPN	INR0061	12	20	20
CUCUTA	Principal / IPVPN	INR0044	18	20	20
	Backup / IPVPN	INR0047	8	10	10
VALLEDUPAR	Principal / IPVPN	INR0091	18	20	20
	Backup / IPVPN	INR0090	8	10	10
YOPAL	Principal / IPVPN	INR0121	18	20	20
	Backup / IPVPN	INR0123	8	10	8
ARAUCA	Principal / IPVPN	INR0110	15	20	15
CALI	Principal / IPVPN	INR0151	63	100	100
	Backup / IPVPN	INR0153	15	20	20
BUENAVENTURA	Principal / IPVPN	INR0051	10	10	10
MOCOA	Principal / IPVPN	INR0135	10	10	10
	Backup / Satelital	INR0136	5	5	5
PASTO	Principal / IPVPN	INR0130	18	20	20
	Backup / IPVPN	INR0131	8	10	10
POPAYAN	Principal / IPVPN	INR0035	20	20	20
	Backup / IPVPN	INR0032	5	5	5
TUMACO	Principal / IPVPN	INR0147	18	20	
WAN general (concentrador total red)	Principal /IPVPN	INR0266	1000	1000	1024
	Backup / IPVPN	INR0171	1000	1000	1024
Conectividad dedicada a funciones de réplica para eventos de DRP.	DWDM	INR0224	2000	2000	2048
Canal entre Sitio principal e ICETEX - Dirección General - Aguas	Principal /IPVPN	0	1000		1024
	Backup / IPVPN	0	600		600
BOGOTA ICETEX - Carrera 3 No. 18-32 - Sede Aguas - INTERNET bk	BOGOTA ICETEX - Carrera 3 No. 18-32 - Sede Aguas - INTERNET	INR0034	70	70	70
MEGACENTER MPLS BACKUP MEDELLIN	Conectividad brindada a través de la red MPLS, con acceso a los dos Datacenter	INR0177	500	500	500
Salida a Internet para toda la WAN desde Bogotá EN CENTRO DE COMPUTO principal	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0230	500	500	500
Internet Dedicado Navegación centralizada Megacenter	Internet Backup	INR0268	400	400	400
Banco de la Republica hasta Edificio Dirección General ICETEX	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0000289	40	40	40

CIUDAD	Enlace - Tipo medio	INR	BW- Mínimo Requerido (MBPS)	Ancho de Banda actual	Ancho de Banda Ofrecido según Anexo 2.1
DECEVAL hasta Edificio de ICETEX Dirección General.	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0000317	40	40	40
DECEVAL hasta Edificio de ICETEX Dirección General.	Ubicado en Datacenter Principal, interconectado a través de red MPLS (Backup)	INR0000318	15	15	15
Salida de los portales https://portal.ICETEX.gov.co/portal y www.ICETEX.gov.co hacia internet en centro de cómputo principal	Internet Reverso para Portales	INR0000320	1024	800	1024
Salida de los portales https://portal.ICETEX.gov.co/portal y www.ICETEX.gov.co hacia internet en centro de cómputo de contingencia	Internet Reverso para Portales	INR0274	800	800	800
BARRANQUILLA	Internet para la gente	INR0094	10	10	10
BUCARAMANGA	Internet para la gente	INR0057	10	10	10
CALI	Internet para la gente	INR0160	10	10	10
AGUAS	Internet para la gente	INR0029	20	20	20
CHAPINERO	Internet para la gente	INR0015	20	20	20
MEDELLIN	Internet para la gente	INR0122	10	10	10
APARTADO	Internet para la gente	INR0140	10	10	10
ARAUCA	Internet para la gente	INR0115	10	10	10
LETICIA	Internet para la gente	INR0000378	10	10	10
QUIBDO	Internet para la gente	INR0021	10	10	10
RIOHACHA	Internet para la gente	INR0159	10	10	10
SAN ANDRES	Internet para la gente	INR0000368	10	10	10
YOPAL	Internet para la gente	INR0127	10	10	10
MOCOA	Internet para la gente	INR0141	10	10	10

Tabla 38 Canales anchos de Banda actuales VrS anchos de banda ofrecidos

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

Se encuentran pendientes y en proceso de coordinación para enviar a ICETEX las opciones de capacitación, fechas y asistentes para la respectiva programación.

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 39 Capacidades de almacenamiento contratado

Aprovisionado se tienen las siguientes capacidades instaladas:

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

Tabla 40 Capacidades de almacenamiento aprovisionado

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

14.4. Se oferta Ítem de “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.

INFOTIC se encuentra actualmente en la elaboración de la propuesta comercial para ICETEX, en respuesta a la solicitud de instalación de cinco puntos de Internet para las sedes de Manizales, Armenia, Cartagena, Sincelejo y Pasto.

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 41 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 42 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. PENDIENTES

16.1. Administrador WEB MASTER

- Solicitud de renovación de soporte Liferay, que estaba vigente hasta el 31 de enero de 2025. Es necesario actualizar el soporte para poder tener una colaboración de parte del fabricante en diversos procesos como por ejemplo los nuevos instaladores, parches de seguridad, key de licencias de ambiente productivo, pruebas y desarrollo (localhost) y posteriormente realizar la migración a la nueva versión Liferay 7.4 GA125.

16.2. Administrador Networking

- Coordinación con ICETEX para revisar y definir el plan de trabajo de la configuración de IPv6 para las sedes que tienen router de voz.

- Traslado del SD WAN de aguas a Triara, a la fecha se encuentra en proceso por parte del proveedor tecnológico.
- Instalación del canal de Backup de Quibdó.
- Traslado del canal de Arauca.

16.3. Administrador Base de datos

- Creación base de datos LANDICTX 19C en ambiente de calidad

16.4. Administrador de aplicaciones

- En general, al finalizar el mes en la administración de servidores, se registran las actividades completadas, a menos que existan tareas que, por su naturaleza, requieran ser trabajadas en múltiples sesiones y se extiendan de un mes a otro. En esta ocasión, no hay temas pendientes.

16.5. Integrador Nube

- Implementación de TAGs a los recursos creados y existentes, paso que se debatirá posterior al análisis solicitado y entregado, se espera empezar en Agosto del 2024 dicho análisis.

- Espera de decisiones y socialización por parte de la entidad ICETEX.

- 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, hace 2 informes atrás manifesté que sólo es soportada la versión .Net 8 y la entidad aún cuenta con versiones .Net 6 en sus datacenters, aún cuando mi 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 datacenters de la entidad.

16.6. Seguridad

- Se continúa con la depuración de políticas en el Firewall de Aguas, se ha realizado borrado de políticas con cantidad de tráfico en 0 y algunas que se encontraban repetidas. Para este mes se tiene un total de 602, esto debido a tareas realizadas que no han permitido continuar con la depuración durante este mes. Se continuará evaluando si existen otras que se puedan agrupar e ir depurando. Adicionalmente, se han ido eliminando objetos duplicados en el firewall de Aguas como parte de la administración y mejora sobre estos dispositivos para optimizar su rendimiento.

- Se continua con el mejoramiento del informe mensual conforme han surgido observaciones por parte de la entidad, en evaluación continua por parte de esta, para aceptación de los cambios que se realizan. Se ha actualizado el formato de informe mensual según las solicitudes realizadas por parte de la Entidad.

17. ANEXOS

17.1. Almacenamiento

Backups Diarios:

- Backups diarios febrero (28 reportes) Backup Diario

Informe de Backups:

- Consolidado mensual Backup febrero Consolidado Diario Backup Febrero 2025.pdf

- Informe Backup febrero Informe Backups mes de febrero 2025.pdf

17.2. Aplicaciones

- Informe actividades Módulos videoconferencia ICETEX febrero

Informe actividades Módulos videoconferencia ICETEX Febrero 2025.pdf

- Informe mensual Administrador de Soluciones febrero
  Formato Informe Mensual InfoTIC Administrador de Soluciones Febrero 2025.pdf

- Informe mensual Administrador Web Master febrero
  Informe Mensual InfoTIC Webmaster Febrero 2025.pdf

- Informe mensual Integrador Nube febrero
  Informe Mensual InfoTIC IntegradordeNube Febrero 2025.pdf

17.3. Bases De Datos

- Informe de evidencias Dataguard Megacenter febrero
  INFOTIC_ICETEX - Evidencias Dataguard Megacenter febrero 2025.pdf

- Informe mensual Administrador de Bases de datos febrero
  Informe Mensual InfoTIC DBA Febrero 2025.pdf

17.4. Ejecución Presupuestal

- Conciliación febrero
  Conciliación febrero.xlsx

- Consolidado informe mensual especialistas febrero
  INFORME MENSUAL FEBRERO 2025.pdf

- Informe de Gestión Servicio febrero 2025
  Informe de Gestion Servicio febrero 2025 V3.docx

17.5. Seguridad

- Informe Mensual MARCA-OSINT ICETEX febrero
  Informe Mensual MARCA-OSINT ICETEX Febrero 2025.pdf

- Informe Mensual Seguridad febrero
  Informe Mensual ICETEX FEBRERO.pdf

- Informe Mensual SOC - ICETEX febrero
  Informe Mensual SOC-TH ICETEX Febrero 2025.pdf

- Informe técnico análisis de vulnerabilidades ICETEX febrero

INFORME TÉCNICO ANÁLISIS DE VULNERABILIDADES ICETEX (Febrero_2025).pdf

- Reporte de IPS febrero
  Reporte de IPS de febrero_infotic_2025.pdf

Reporte total ataques recibidos-SIEM:

- Denegados febrero 01 al 12
  Denegados febrero 1-12.pdf

- Denegados febrero 13 al 28
  Denegados febrero 13-28.pdf

17.6. Soporte Y Monitoreo

Canales

- ANS febrero
  ANS_Febrero_2025_NEW.xlsx

- Informe mensual Administrador de Networking febrero
  Informe Mensual InfoTIC Administrador Redes Febrero 2025.pdf

- Informe Mensual Disponibilidad febrero
  Reporte Mensual Disponibilidad INFOTIC Febrero 2025.pdf

Graficas de consumo:

- Informe Mensual ALLOT febrero
  Reporte Mensual Disponibilidad INFOTIC Febrero 2025.pdf

- Pruebas Nuevas de Saturación Canales febrero
  Prueba de Saturación Febrero

17.7. Data center Alterno:

Replicación

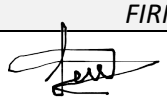
- Informe mensual replicación febrero
  Informe mensual replicacion Febrero 2025.pdf

- Reportes diarios febrero (25 reportes)
  Data Center Alterno

17.8. Data Center Principal:

- Reporte Monitoreo ICETEX febrero
  Reporte Monitoreo ICETEX Febrero 2025-ELK.pdf

Revisión técnica

REVISÓ	*FIRMAS*
SANDRA MILENA GARCIA HERNANDEZ CONTRATISTA GRUPO DE INFRAESTRUCTURA	
RAUL FERNANDO GUTIERREZ TECANO ANALISTA 2	