1. PERIODO DEL INFORME

PERÍODO A QUE CORRESPONDE EL INFORME	01-01-2025 A 31-01-2025

2. DATOS DEL SUPERVISOR

NOMBRE DEL SUPERVISOR	VICTOR RAUL BAUTISTA GALINDO
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 PRESENTA EL INFORME DE ACTIVIDADES CORRESPONDIENTES AL PERIODO DEL MES DE DICIEMBRE DE 2024

5. PRODUCTOS ENTREGABLES

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 DICIEMBRE de 2024, se da continuidad con la concertación de ANS sobre los servicios prestados de acuerdo con el anexo técnico del contrato.

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 ____	NO __X__
En virtud que no se ha concerta aplicación de ANS en los servicios prestados en el periodo de diciembre de 2024, no generando pago.	

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)

Presenta informes de los servicios prestados en diciembre de 2024, No se genera pago en el periodo supervisado, se adelanta aplicación de ANS sobre los servicios prestados.

11. EJECUCIÓN PRESUPUESTAL

	VIGENCIA *(AÑO)*
VALOR DEL CONTRATO	$31.398.996.857,96
VALOR ADICIÓN (Si aplica)	$0
VALOR A PAGAR (Si aplica)	$0
VALOR EJECUTADO	$ 13.669.517.268,00
VALOR PENDIENTE POR EJECUTAR	$ 17.729.479.589,96

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:

En el periodo supervisado no se genera pago por no concluir concertación de aplicación de ANS de los servicios prestados en el periodo de diciembre de 2024.

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

Presentó:	Aprobó:
	
FIRMA DEL SUPERVISOR INFOTIC **MONICA MARIA VILLAMIZAR SANCHEZ** **No. CC 26.862.573**	**FIRMA DEL SUPERVISOR** **VICTOR RAUL BAUTISTA GALINDO** **No. CC 79.352.968**

Revisó: Raúl Fernando Gutiérrez Tecano- Analista 2 Coordinación de infraestructura – DT Raul Gutierrez Tecano

Al contestar cite Radicado 2025000145445-R Id: 5922844 Folios: 1 Fecha: 05-05-2025 09:56:04 Anexos: 1 Remitente: Destinatario:

5 de Mayo de 2025

PARA:

DE: - INFOTIC S.A

ASUNTO:

PDF DEL DOCUMENTO ELECTRÓNICO #FVE1811

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-1811

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: 5/5/2025 9:40:29 AM
Forma de pago: CREDITO 30 DIAS
Moneda: COP
Fecha vcto: 6/5/2025 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 ENERO DE 2025. SERVICIOS OPERACIÓN MES DE ENERO DE 2025 (INCLUIDO IVA): $ 833.143.476 (-) DESCUENTOS INCLUIDO IVA: ONECTIVIDAD Y RED DE COMUNICACIONES: -$27.193.986 CENTRO DE DATOS: -$64.967.105 TOTAL DESCUENTO CON IVA: -$92.161.091 . 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	$ 622,674,273.00	$622,674,273.00	$ 740,982,385.00

IMPUESTOS	BASE	TASA	TOTAL
IVA	$622,674,273	19 %	$118,308,112

SETECIENTOS CUARENTA MILLONES NOVECIENTOS OCHENTA Y DOS MIL TRESCIENTOS OCHENTA Y CINCO PESOS M/CTE *****

Notas

facturacion_electronica@icetex.gov.co

RESPONSABLE: MONICA VILLAMIZAR

VALOR BRUTO	$622,674,273.00
DESCUENTO	$0.00
SUBTOTAL	$622,674,273.00
IVA	$118,308,112.00
TOTAL FACTURA	$740,982,385.00

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 39ab6f097a7822c9426499d18063e5918156042aa1685510d29425319b7fa6dc942df755a76173c31d6f983b8de1111d

FIRMA DIGITAL:

R+ZKOOmDS39fX6eK/ihqYOWNsOUEqZROV/g30TfYVESk3uReDdi5vm4z+GmEFvYQM89a+EI30Z4OkZPn/LQ1xT1QUncX3rQm6M5+tr0ItPIMwZnV8xK76ytMnwE
7huG6JEenGnSETy5aKdBswMB7qHt1i83snRoigmAsHMnuQVPO1d7ZL0nkJkk+KfmEdMAXyuPaNONH2Qe0Q9RK07F5Kuyk5kD0evfaLLw7zVCjgoFDVCo9lELhuYJ7Q
apXdTHv9Za3wk5HU+gfDPqrxGDj1gl4SrgcXTXtYkVSKvtGmFV8LRYna4CFzk+77B+W/Cgki3/kiL56/ylVL9gpRQe1Kw==

FECHA DIAN: 2025-05-05 09:42:28-05:00

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

Enero 01 al 31 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 12
4.2. Centro de Datos 13
4.2.1. Centro de Datos Principal 13
4.2.1.1. Aplicaciones 13
4.2.1.2. Bases de Datos 13
4.2.2. Centro de Datos Alterno 16
4.2.2.1. Hosting Virtual (IaaS) 16
4.2.2.2. Dataguard Bases de Datos Megacenter 18
4.2.2.3. Servicios de Housing – Datacenter Alterno 19
4.2.2.4. Servicios de DRP 19
4.3. Seguridad informática 20
4.3.1. Plataformas Administradas 21
4.3.1.1. FortiGate Triara 21
4.3.1.2. FortiGate Aguas 24
4.3.1.3. FortiGate Medellín 25
4.3.1.4. FortiWeb 2000F 25
4.3.1.5. FortiWeb 2000E 26
4.3.1.6. FortiSandBox 26
4.3.1.7. Sophos EndPoint 27
4.3.2. Estadística de Portales 27
4.3.3. Servicio de centro de Operaciones de Seguridad (SOC) 29
4.3.3.1. Alertas o Incidentes de Seguridad Detectados 30

4.3.3.1.1. Categoría Seguridad 30
4.3.3.1.2. Categoría Disponibilidad 31
4.3.3.1.3. Categoría Rendimiento 32
4.3.3.1.4. Threat Hunting 32
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 41
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) 44
9. GESTION DE RIESGOS Y PROBLEMAS 49
10. INDICADORES CLAVE DE DESEMPEÑO 50
10.1. ANS por Disponibilidad de canales de comunicaciones: 50
10.1.1. Canal de Replicación (Triara – Megacenter) 54
10.2. ANS por Disponibilidad de servidores: 54
10.2.1. Disponibilidad TRIARA para los servicios de página web 56
10.2.2. Análisis componente Liferay Producción 64
10.2.2. SERVICIO NFS – BACKUP DE NODOS 1 Y 2 DEL PORTAL ICETEX 66
10.2.3. Backup Servidores Triara 69
11. CONTROL DE CAMBIOS 71
12. PLAN DE TRABAJO DE LOS PROXIMOS MESES 72
14. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC 78
14.1. Aumento de la capacidad de Ancho de Banda en algunas de las sedes de la Entidad 78
14.2. Una capacitación al año de seguridad Informática y servicios conexos 81
14.3. TB de capacidad de almacenamiento 81

14.4. Se oferta Ítem de "Wifi" para la gente en 19 sedes 82
15. CONCLUSIONES 83
16. PENDIENTES 84
16.1. Administrador WEB MASTER 84
16.2. Administrador Networking 84
16.3. Administrador Base de datos 84
16.4. Administrador de aplicaciones 84
16.5. Integrador Nube 85
16.6. Seguridad 85
17. ANEXOS 86
17.1. Almacenamiento 86
17.2. Aplicaciones 86
17.3. Bases De Datos 86
17.4. Ejecución Presupuestal 86
17.5. Seguridad 87
17.6. Soporte Y Monitoreo 87
17.7. Data center Alterno: 88
17.8. Data Center Principal: 88

INDICE DE TABLAS

TABLA 1 CASOS NETWORKING ATENDIDOS EN EL MES-FORMATO ICETEX 11
TABLA 2 CASOS ATENDIDOS NETWORKING COMPARATIVO MES ANTERIOR 11
TABLA 3 CANALES PRUEBAS DE SATURACIÓN EJECUTADAS EN EL MES DE ENERO 2025 12
TABLA 4 CANALES PENDIENTES PRUEBAS DE SATURACIÓN 12
TABLA 5 CASOS DE ARANDA APLICACIONES 13
TABLA 6 SERVICIOS REPLICADOS – DATACENTER MEGACENTER 17
TABLA 7 TOP 05 MÁQUINAS MAYOR TASA DE TRANSFERENCIA 17
TABLA 8 TOP 05 MÁQUINAS MENOR TASA DE TRANSFERENCIA 18
TABLA 9 FECHAS CON MENOR REPLICACIÓN 18
TABLA 10 DISTRIBUCIÓN TRIMESTRAL DE REPLICACIÓN 18
TABLA 11 DISPONIBILIDAD DE SERVICIOS DE HOUSING – DATA CENTER ALTERNO 19
TABLA 12 TOP 10 DE LOS PORTALES MÁS UTILIZADOS 28
TABLA 13 COMPARATIVO – INDICADORES DE COMPROMISO 29
TABLA 14 COMPARATIVO ALERTAS DE SEGURIDAD 30
TABLA 15 COMPARATIVO ALERTAS DE DISPONIBILIDAD 31
TABLA 16 COMPARATIVO ALERTAS DE RENDIMIENTO 32
TABLA 17 INVENTARIO DE DISPOSITIVOS 33
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 49
TABLA 24 NIVEL DE RIESGO 50
TABLA 25 GRADO DE RIESGO 50
TABLA 26 DISPONIBILIDAD DE CANALES 53
TABLA 27 DISPONIBILIDAD CANALES “INTERNET PARA LA GENTE” 53
TABLA 28 DISPONIBILIDAD CANALES “SDWAN” 54
TABLA 29 CÓDIGOS RELACIONADOS DISPONIBILIDAD SERVICIOS EN HOUSING – DATACENTER PRINCIPAL 55
TABLA 30 DISPOSITIVOS EN HOUSING – DATACENTER PRINCIPAL 56
TABLA 31 ACTUALIZACIÓN – ANÁLISIS COMPONENTE LIFERAY ENERO 66
TABLA 32 SERVICIO NFS– BACKUP DE NODOS 1 Y 2 DEL PORTAL ICETEX 68
TABLA 33 DISTRIBUCIÓN TRIMESTRAL DE ACCESO POR USUARIOS 68
TABLA 34 DISTRIBUCIÓN TRIMESTRAL DE BACKUP EJECUTADOS 71
TABLA 35 DISTRIBUCIÓN TRIMESTRAL DE BACKUP POR SERVICIOS 71
TABLA 36 CONTROLES DE CAMBIO ENERO 71
TABLA 37 PLANES DE TRABAJO 75
TABLA 38 CANALES ANCHOS DE BANDA ACTUALES VRS ANCHOS DE BANDA OFRECIDOS 81
TABLA 39 CAPACIDADES DE ALMACENAMIENTO CONTRATADO 82
TABLA 40 CAPACIDADES DE ALMACENAMIENTO APROVISIONADO 82
TABLA 41 WIFI PARA LA GENTE INSTALADOS 83
TABLA 42 WIFI PARA LA GENTE PENDIENTES 83

INFOTIC
SOLUCIONES INTELIGENTES

INDICE DE ILUSTRACIONES

ILUSTRACIÓN 1 DISPONIBILIDAD DE LAS BASES DE DATOS PRINCIPALES ICTXCYC Y APOTEOSY 14
ILUSTRACIÓN 2 CASOS DEL PROYECTO GESTIONADOS ARANDA BASES DE DATOS 15
ILUSTRACIÓN 3 REPORTES DE REPLICACIÓN SRM A SITIO ALTERNO – ENERO 2025 16
ILUSTRACIÓN 4 EVIDENCIA DATAGUARD REPLICADO A MEGACENTER BD 19
ILUSTRACIÓN 5 CONSUMO CANAL MPLS 21
ILUSTRACIÓN 6 CONSUMO CANAL INTERNET SEDES 22
ILUSTRACIÓN 7 CONSUMO CANAL INTERNET DATA CENTER 22
ILUSTRACIÓN 8 FILTRADO – WEB – (FORTIGATE – TRIARA) 23
ILUSTRACIÓN 9 INSPECCIÓN – SSL – (FORTIGATE – TRIARA) 23
ILUSTRACIÓN 10 ANTIVIRUS Y ANTIMALWARE – PERIMETRAL (FORTIGATE – TRIARA) 24
ILUSTRACIÓN 11 CONSUMO CANAL MPLS AGUAS 25
ILUSTRACIÓN 12 CONSUMO CANAL MPLS MEDELLÍN 25
ILUSTRACIÓN 13 CONFIGURACIÓN FORTIWEB 26
ILUSTRACIÓN 14 ESTADO SEGURIDAD SOPHOS 27
ILUSTRACIÓN 15 EVIDENCIA GRÁFICA ESTADÍSTICAS DE PORTALES 28
ILUSTRACIÓN 16 TOTAL DE ALERTAS DE SEGURIDAD 30
ILUSTRACIÓN 17 TOTAL DE ALERTAS DE DISPONIBILIDAD 31
ILUSTRACIÓN 18 TOTAL DE ALERTAS DE RENDIMIENTO 32
ILUSTRACIÓN 19 CANTIDAD TOTAL DE HALLAZGOS IDENTIFICADOS 34
ILUSTRACIÓN 20 DISPONIBILIDAD DE SERVICIO VIDEOCONFERENCIA SEDES REGIONALES – ENERO 2025 42
ILUSTRACIÓN 21 DISPONIBILIDAD DE SERVICIO VIDEOCONFERENCIA SEDES BOGOTÁ – ENERO 2025 43
ILUSTRACIÓN 22 INCIDENTES / REQUERIMIENTOS SEDES REGIONALES – ENERO 2025 43
ILUSTRACIÓN 23 PRUEBA DE FUNCIONAMIENTO VISITA SEDE CHAPINERO – ENERO 2025 44
ILUSTRACIÓN 24 MÓDULO FUNCIONAL SALA 8VO PISO PRESIDENCIA – VISITA ENERO 2025 45
ILUSTRACIÓN 25 EVIDENCIA MÓDULO FUNCIONAL SEDE AGUAS 65, PISO 4 - VISITA ENERO 2025 46
ILUSTRACIÓN 26 EVIDENCIA MÓDULO FUNCIONAL SEDE AGUAS, UBICACIÓN PISO 6 – VISITA ENERO 2025 46
ILUSTRACIÓN 27 EVIDENCIA MÓDULO FUNCIONAL SEDE AGUAS PISO 2 – VISITA ENERO 2025 47
ILUSTRACIÓN 28 VERIFICACIÓN MÓDULO VISITA SEDE ÁNGEL - ENERO 2025 48
ILUSTRACIÓN 29 MATRIZ DE RIESGOS 49
ILUSTRACIÓN 30 UPTIME – PORTAL WEB WEB.ICETEX.GOV.CO 57
ILUSTRACIÓN 31 MÉTRICA DE VISITANTES PORTAL WEB WEB.ICETEX.GOV.CO 57
ILUSTRACIÓN 32 MÉTRICA DE USUARIO POR PAÍS - PORTAL WEB WEB.ICETEX.GOV.CO 58
ILUSTRACIÓN 33 NODO 1 – VISTA GENERAL – INR0243 58
ILUSTRACIÓN 34 NODO 1 CPU 59
ILUSTRACIÓN 35 NODO 1 MEMORIA 60
ILUSTRACIÓN 36 NODO 1 ALMACENAMIENTO 60
ILUSTRACIÓN 37 NODO 2 – VISTA GENERAL – INR0242 61
ILUSTRACIÓN 38 NODO 2 CPU 61
ILUSTRACIÓN 39 NODO 2 MEMORIA SWAP 62
ILUSTRACIÓN 40 NODO 2 MEMORIA 63
ILUSTRACIÓN 41 NODO 2 ALMACENAMIENTO 63
ILUSTRACIÓN 42 EVIDENCIA BACKUP SERVIDORES RESUMEN BACKUPS Y SU ESTADO 70

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 31 de enero 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 61.11 % que representa los 22 meses que lleva dentro de la fase de Operación el proyecto.

El presente informe del mes de enero 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 31 de enero 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 31 de enero 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.**

Teniendo en cuenta que en enero aún no se contaba con personal de Networking y seguridad contratada en Icetex, se acuerda que la reunión conjunta propuesta en la cual se establezcan las actividades de implementación de IPv6 para el año 2025 se reprograme para el siguiente mes, 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 100.00% de los servicios de Internet para la gente.

- 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 Enero 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 y backup para una nueva sede en la ciudad de Puerto Carreño -Vichada, la cual se encuentra en gestión desde INFOTIC para proceder a enviar el costo de los canales y de esta forma llegar a un acuerdo comercial con ICETEX y si es viable proceder con la instalación.

- (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 https://icetex.sharepoint.com/:f:/r/sites/Infraestructura/Documentos%20compartidos/NETWORKING%202023/casos%20aranda%20por%20mes?csf=1&web=1&e=PWNYBS), 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 hh:mm:ss
27/01/2025	Cali >> Evento de afectación de servicio.	INR0151	IM-292852-4-82092	
23/01/2025	Villavicencio >> Evento de afectación de servicio.	INR0085	IM-292596-4-82031	
16/01/2025	Internet/Redes >> Inc Falla de Conectividad a la Red		IM-292033-4-81861	
16/01/2025	- Página Web Icetex >> Inc Caída de la Página (intermitencia del internet de la sede de Yopal)		IM-291937-4-81836	
15/01/2025	Tumaco >> Evento de afectación de servicio.	INR0147	IM-291915-4-81825	
15/01/2025	Internet/Redes >> Inc Falla de Navegación		IM-291858-4-81814	
14/01/2025	Tumaco >> Evento de afectación de servicio	INR0147	IM-291666-4-81762	
13/01/2025	Internet/Redes >> Inc Falla de Navegación		IM-291636-4-81750	
13/01/2025	Internet/Redes >> Inc Falla de Conectividad a la Red		IM-291620-4-81743	
13/01/2025	Buenaventura >> Evento de afectación de servicio.	INR0051	IM-291614-4-81742	
9/01/2025	INCIDENTE FALLA - CASO RECUERRENCIA IMPRESORA A COLOR PRESIDENCIA (tema de velocidad de negociación de la impresora se colocó a 1 GB)		IM-291362-4-81660	
7/01/2025	Internet/Redes >> Inc Falla de Conectividad a la Red		IM-291145-4-81573	
3/01/2025	Internet/Redes >> Inc Falla de Conectividad a la Red		IM-291078-4-81545	
3/01/2025	Internet/Redes >> Inc Falla de Conectividad a la Red		IM-291063-4-81539	

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
Enero 2025	14
Diciembre 2024	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 enero se realizaron dos pruebas de saturación de canales, cuya evidencia se puede consultar en el siguiente link: Pruebas de Saturación Enero

El cronograma de ejecución se continúa enviando semanalmente al ICETEX.

CIUDAD	Enlace - Tipo medio	Código Servicio	Fecha de Saturación
SAN ANDRES	SDWAN	INR0000371	13/01/2025
PEREIRA	Backup/ IPVPN	INR0077	29/01/2025

Tabla 3 Canales pruebas de saturación ejecutadas en el mes de enero 2025

CIUDAD	Enlace - Tipo medio	Código Servicio
BOGOTA(AGUAS)	**Principal / IPVPN**	**INR0036**
BOGOTA(AGUAS)	**Backup/ IPVPN**	**INR0037**
BUENAVENTURA	**Principal / IPVPN**	**INR0051**
ARMENIA	**Backup/ IPVPN**	**INR0072**
ARMENIA	**Principal / IPVPN**	**INR0074**
IBAGUE	**Backup/ IPVPN**	**INR0076**
VILLAVICENCIO	**Backup/ IPVPN**	**INR0084**
CARTAGENA	**Backup/ IPVPN**	**INR0107**
TUMACO	**Principal / IPVPN**	**INR0147**
SANTA MARTA	**Backup/ IPVPN**	**INR0152**
CALI	**Backup/ IPVPN**	**INR0153**
SANTA MARTA	**Principal / IPVPN**	**INR0154**
BOGOTA(ANGEL)	**Principal / IPVPN**	**INR0273**
LETICIA	**SDWAN**	**INR0000374**
Triara*	**Principal**	**INR0000320**

Tabla 4 Canales pendientes pruebas de saturación

En resumen, se ha alcanzado un **76%** de pruebas de saturación hasta el 31 de enero de 2025.

Se tiene programada la ejecución del control de cambios para la prueba de saturación del canal denominado *Internet Reverso para Portales (Salida de los portales https://portal.ICETEX.gov.co/portal y www.ICETEX.gov.co hacia internet en centro de cómputo principal), cuyo cambio CHG-292535-4-1116 fue aprobada su ejecución en el comité de control de cambios del día 30 de enero para el 8 de febrero 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	Evidencias
1	06/01/2025	Tarea 513893 Cambio 16844 – Permisos FTP Usuarios OCM **Solución:** Se otorgaron permisos FTP a usuarios de OCM.	Tarea 513893 Cambio 16844 – Permisos FTP Usuarios OCM.pdf
2	07/01/2025	Incidente 81596 – Error Aplicación Cargue Archivos **Solución:** Se resolvió un error en la aplicación de Cargue de Archivos, asegurando su correcto funcionamiento.	Incidente 81596 – Error Aplicación Cargue Archivos.pdf
3	15/01/2025	Tarea 514589 Requerimiento 16986 - Acceso al servidor de pruebas 10.1.18.124 **Solución:** Se gestionó el acceso al servidor de pruebas 10.1.18.124 para cumplir con un requerimiento técnico.	Tarea 514589 Requerimiento 16986 - Acceso al servidor de pruebas 10.1.18.124.pdf
4	20/01/2025	Tarea 514990 Cambio 17042 – Permisos FTP Usuarios Operaciones **Solución:** Se asignaron permisos FTP a usuarios del área de Operaciones	Tarea 514990 Cambio 17042 – Permisos FTP Usuarios Operaciones.pdf
5	29/01/2025	Tarea 515611 Cambio 17156 – Permisos FTP Usuarios Operaciones. **Solución:** Se realizó un ajuste adicional en los permisos FTP para usuarios de Operaciones	Tarea 515611 Cambio 17156 – Permisos FTP Usuarios Operaciones.pdf

Tabla 5 casos de Aranda aplicaciones

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

- DEPURACION LOGS SERVIDOR ICTXSRVNETCOR01 ENERO 17 DE 2024.pdf
- DEPURACION LOGS SERVIDOR MIRA ENERO 28 DE 2024.pdf
- Publicacion de TrasnunionApi Enero 8 de 2025.pdf
- Publicacion 2 de TrasnunionApi Enero 9 de 2025.pdf

4.2.1.2. Bases de Datos

- En cuanta a atención de solicitudes de usuarios, se resolvieron 535 casos asignados a los administradores de base de datos en enero de 2025 en los tiempos estipulados por prioridad.

- Los casos atendidos en el mes de enero aumentaron en un 1% respecto al mes de diciembre de 2024, dicho aumento aunque no fue significativo obedeció a las nuevas convocatorias que debieron ser atendidas por el

cliente.

- Se realizó la depuración de Filesystems de S.O (/grid /oracle) alertados de manera proactiva por consumo por encima del 80%.

- Disponibilidad del Clusterware BD para el mes de ENERO 2025 100% como se evidencia en la siguiente ilustración:

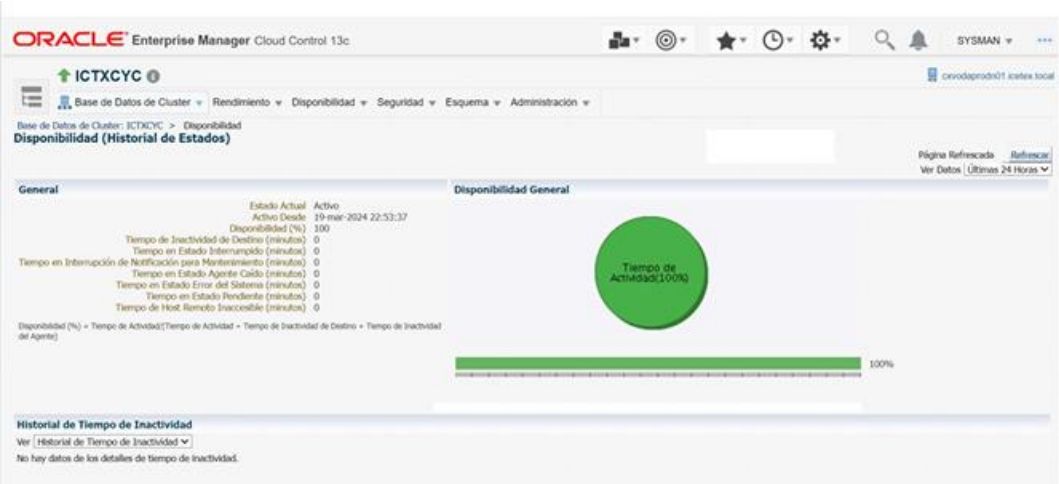


Ilustración 1 Disponibilidad de las Bases de Datos principales ICTXCYC y APOTEOSY

- Se realizaron ajustes a los querys de las aplicaciones de consultas que reportaban como lentas en la base de datos.

- Se realizaron ajustes base de datos de sgdea apoteosys pruebas.

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

- Se generaron restauraciones solicitadas con éxito.

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 329G.

El 27 de enero se presentó ante el ICETEX un memorando con el asunto: Respuesta a los comunicados: 20245110860175-E Id: 252870, Fecha: 2024-11-26 y 20245110879625-E Id 5282615 Fecha: 2024-12-05. Este documento, con radicado VOP-099-2025, incluye una propuesta de INFOTIC que podría contribuir a resolver esta necesidad.

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 enero, se mantuvo en constante replicación las máquinas virtuales configuradas, estos servidores se replicaron desde el origen en Triara hasta Megacenter usando la herramienta nativa de VMware, Site Recovery Manager (SRM) el detalle de las máquinas virtuales replicadas se puede evidenciar en el Informe mensual replicacion Enero 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.

Claro

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	Jan 31, 2025	630.23 MB	5 minutes

Grupo de protección: PG_INFOTIC_6 (2)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0228_INFOTIC_REP	OK	1 of 1	Jan 31, 2025	60.38 MB	1 hour
INR0229_INFOTIC_REP	OK	1 of 1	Jan 31, 2025	325.03 MB	1 hour

Grupo de protección: PG_INFOTIC_1 (2)

Ilustración 3 Reportes de replicación SRM a Sitio Alterno – enero 2025

A continuación, se detallan los servidores con sus correspondientes servicios los cuales están siendo

replicados a Megacenter:

#	INR Replicación	Host Name	Servicio	Virtual Machine 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	INR0209	ICETEXbogbalserver1	Portal productivo (liferay)	INR0237_INFOTIC_REP
7	INR0210	ICETEXbogliferaynfs	Portal productivo (liferay)	INR0238_INFOTIC_REP
8	INR0217	ICETEXbogelasticserver1	Portal productivo (liferay)	INR0239_INFOTIC_REP
9	INR0218	ICETEXbogliferayserver1	Portal productivo (liferay)	INR0243_INFOTIC_REP
10	INR0215	ICETEXboglxdarumasrv1	DARUMA	INR0244_INFOTIC_REP
11	INR0213	ICETEXboglxdarumasrv2	DARUMA	INR0245_INFOTIC_REP
12	INR0214	ICETEXboglxxroad1	XROAD	INR0249_INFOTIC_REP

Tabla 6 Servicios replicados – Datacenter Megacenter

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

- Durante el mes de enero del 2025: 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 21, 22, 25, 26 y 28 de enero, esto debido a que la herramienta no genero el reporte, pero se realizó la replicación correspondiente.

- Se realizaron las replicaciones de los 12 equipos durante todos los días del mes de enero 2025.

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

Top	INR	HOST NAME	MB
1	INR0238	icetexbogliferaynfs	21850.61
2	INR0243	icetexbogliferayserver1	4154.49
3	INR0226	icetexbogwsmira	3134.12
4	INR0229	ictxsisgesapp	2194.22
5	INR0228	ictxsisgesbd	1999.13

Tabla 7 TOP 05 máquinas mayor tasa de transferencia

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

Top	INR	HOST NAME	MB
1	INR0237	icetexbogbalserver1	340.7

Top	INR	HOST NAME	MB
2	INR0233	icetexboglxorfeo1	252.37
3	INR0262	icetexboglxorfeo2	215.29
4	INR0249	icetexboglxxroad1	147.37
5	INR0245	icetexboglxdarumasrv2	91.5

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	Dia	MB
10-ene	Viernes	363.37
06-ene	Lunes	426.76
07-ene	Martes	477.99
20-ene	Lunes	504.44
15-ene	Miércoles	547.6
05-ene	Domingo	652.37
08-ene	Miércoles	735.34
13-ene	Lunes	754.38
24-ene	Viernes	910.63
12-ene	Domingo	982.26

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 34466.55 MB y se presenta un aumento de 27.96% entre diciembre y enero, que equivale a 14209.43 MB.

Mes	MB replicadas
Noviembre	21280.29
Diciembre	50815.07
Enero	36605.64

Tabla 10 Distribución trimestral de replicación

4.2.2.2. Dataguard Bases de Datos Megacenter

Durante el mes de enero 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 Enero 2025.pdf

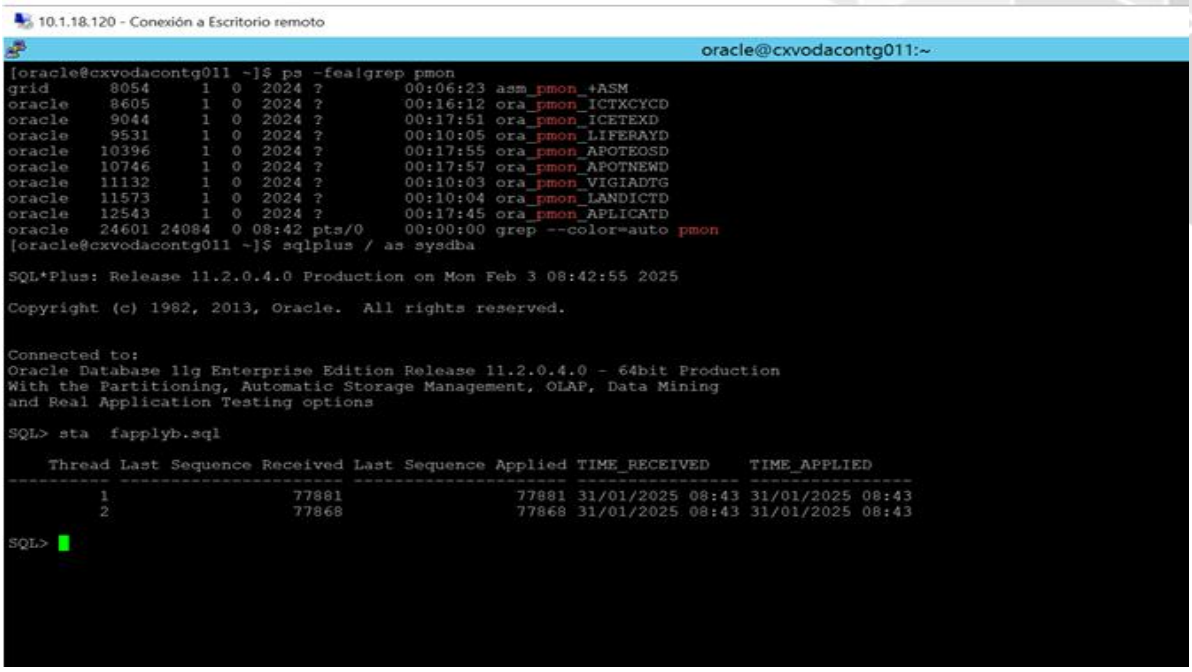


Ilustración 4 Evidencia Dataguard replicado a Megacenter BD

Se generó la consulta de los archives recibidos y aplicados de la base de datos de ICTXCYCD a 31/01/2025 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 enero 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 para organizar los puntos que serán analizados en cada escenario, al cierre del mes aún no se tiene respuesta para organizar con el ICETEX y los demás aliados la ejecución de las pruebas correspondientes, por lo tanto el próximo mes se iniciaran las sesiones correspondientes para ir avanzando con este tema.

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 enero 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 enero los cuales se referencian los cuales se referencian en el ítem 12.2. Gestión de casos Operador de seguridad del Reporte Mensual ICETEX_v2- ENERO.pdf

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

En el mes de enero, se actualizaron los firmwares de los equipos de seguridad perimetral del fabricante Fortinet (FortiGate, FortiManager, FortiWeb y FortiSIEM). Se actualizan a las últimas versiones estables que ofrece el fabricante como parte de los servicios de mantenimiento que se hace sobre estos dispositivos y con el fin de corregir posibles vulnerabilidades que se puedan estar presentando en las versiones anteriores. Dicha actualización se realizó el día 24 de enero de 2025 con el cambio # 1115 expuesto al comité de cambios explicando el proceso de actualización.

4.3.1. Plataformas Administradas

Las plataformas administradas por INFOTIC tanto las la 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 25.33 Mbps [INR0185 CLARO(MPLS_DC)] en la última semana, tal como se puede ver en la Ilustración.

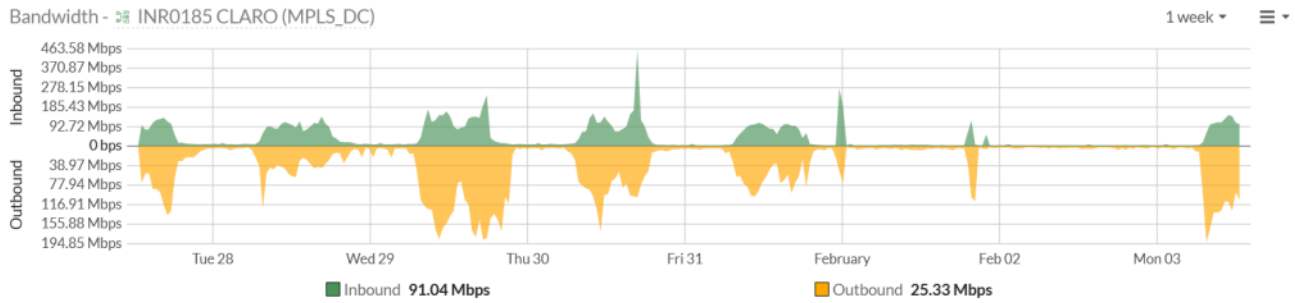


Ilustración 5 Consumo Canal MPLS

Se observa en la Ilustración 6, tráfico hacia la WAN-SEDES-ICETEX [INR0264 (INTE_SEDES_ICTX)] en promedio 54.25 Mbps en la última semana.

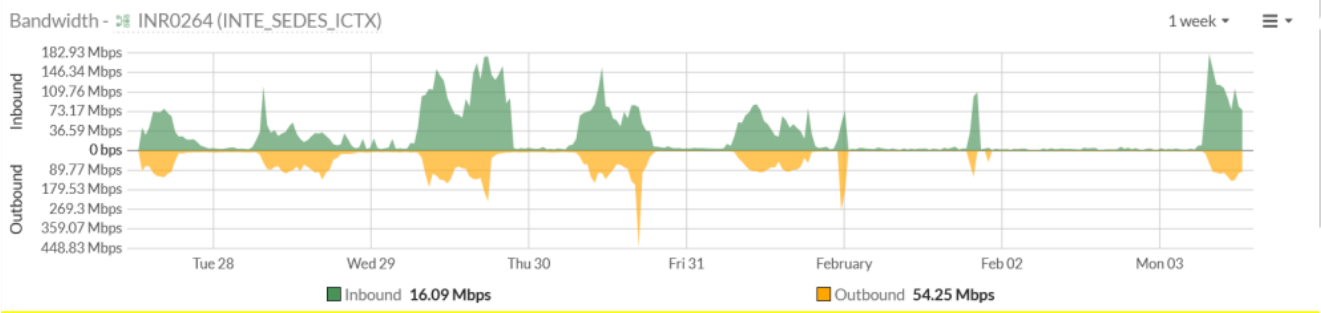


Ilustración 6 Consumo Canal Internet Sedes

En la Ilustración 7, se observa tráfico hacia la INTENET DATACENTER [INTERNET_DC_INR0000320 (Inet_claro)] promedio 44.36 Mbps en la última semana.

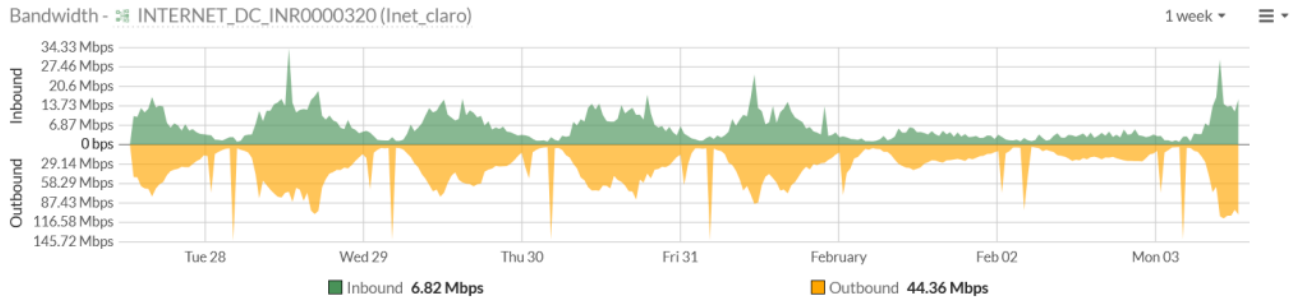


Ilustración 7 Consumo Canal Internet Data Center

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.
WEB default	Perfil con las mínimas restricciones	2
WEB Navegacionpcs_Comware	Perfil con restricciones	2
WEB Navegacionpcs_Comware_con_redes	Perfil con restricciones	2
WEB WF-Aereolineas	RF-186510-7-9612 24/03/2022	0
WEB WF-Avanzado	Perfil para FSSO Navegación Avanzada	30
WEB WF-Comunicaciones	Perfil para FSSO comunicaciones	2
WEB WF-General	Perfil para todos	4
WEB WF-General_Sedes	Perfil para todos	1
WEB WF-Redessociales	Perfil para FSSO Navegación Avanzada	0
WEB WF-Tesoreria	Perfil con restricciones especificas por auditoria.	4
WEB WF-Tesoreria_Sala_Segura	Permisos para equipos de Sala Segura de Tesoreria	0
WEB WF-VIP	Perfil para FSSO Navegación_VIP	15
WEB WF-wetransfer	Perfil para FSSO Navegación Avanzada	1
WEB wifi-default	Perfil de FULL acceso para pruebas	1

Ilustración 8 Filtrado – WEB – (FortiGate – Triara)

Name	Comments	Ref
SSL Pruebas liferay		0
SSL custom-deep-inspection	Customizable deep inspection profile.	0
SSL deep-inspection	Read-only deep inspection profile.	0
SSL certificate-inspection_2780	Read-only SSL handshake inspection profile.	1
SSL Prueba certificate-inspection	Read-only SSL handshake inspection profile.	13
SSL certificate-inspection_ICETEX	SSL para BUS de servicios	29
SSL no-inspection	Read-only profile that does no inspection.	201
SSL certificate-inspection	Read-only SSL handshake inspection profile.	373

Ilustración 9 Inspección – SSL – (FortiGate – Triara)

Name	Comments	Ref.
AV AV-FSB	HTTP,SMTP FULL FSB	38
AV AV-FTP	FTP FULL FSB	0
AV AV-HTTP	HTTP con FSB	26
AV AV-HTTP_Mobile	HTTP, mobile con FSB	0
AV AV-HTTP&CIFS	HTTP,CIFS con FSB	4
AV AV-SMTP	SMTP FULL FSB	1
AV default	ALL con FSB	43
AV ICETEX		50
AV Prueba	ALL con FSB	0
AV prueba2		60
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.

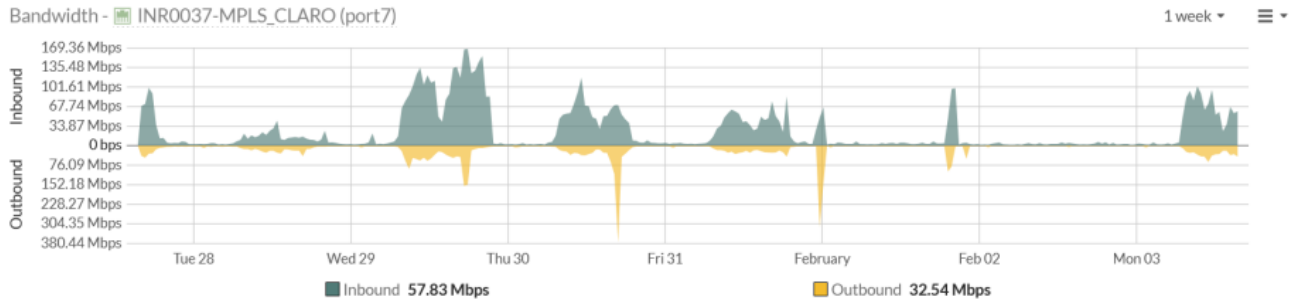


Ilustración 11 Consumo Canal MPLS Aguas

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.

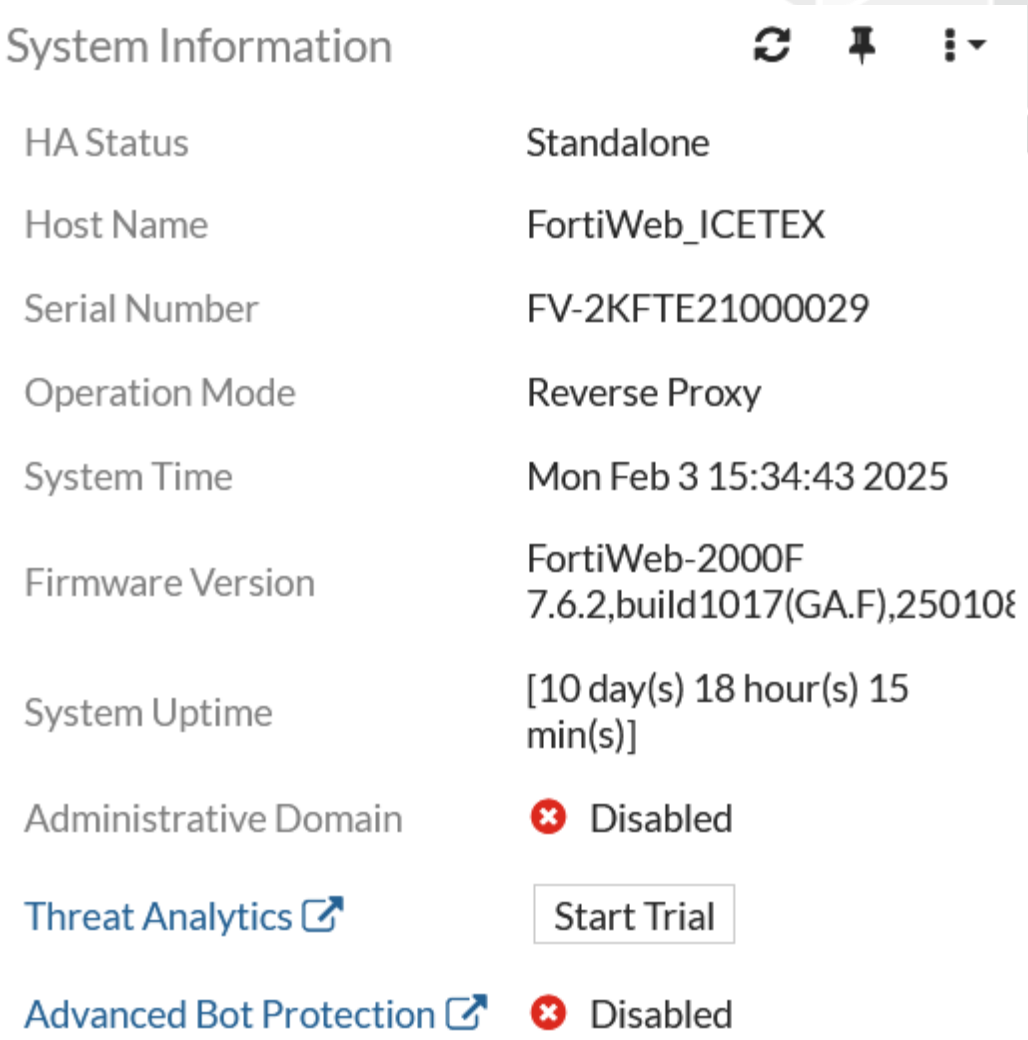


Ilustración 13 Configuración FortiWeb

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 enero, por la falta de los especialistas de seguridad del lado del ICETEX no se realizaron los comités de pares donde se revisan estos temas por lo tanto este tema se encuentran en gestión del proceso de la renovación de este componente tal como nos habían informado en el último comité del mes de diciembre de 2024. Se acordó con el ICETEX retomar estos comités con el personal disponible y allí en conjunto entre ICETEX e INFOTIC se revisarán nuevamente estos temas pendientes.



Ilustración 14 Estado Seguridad Sophos

4.3.2. Estadística de Portales

Durante el mes de enero 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 Reporte Mensual ICETEX_v2- ENERO.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.

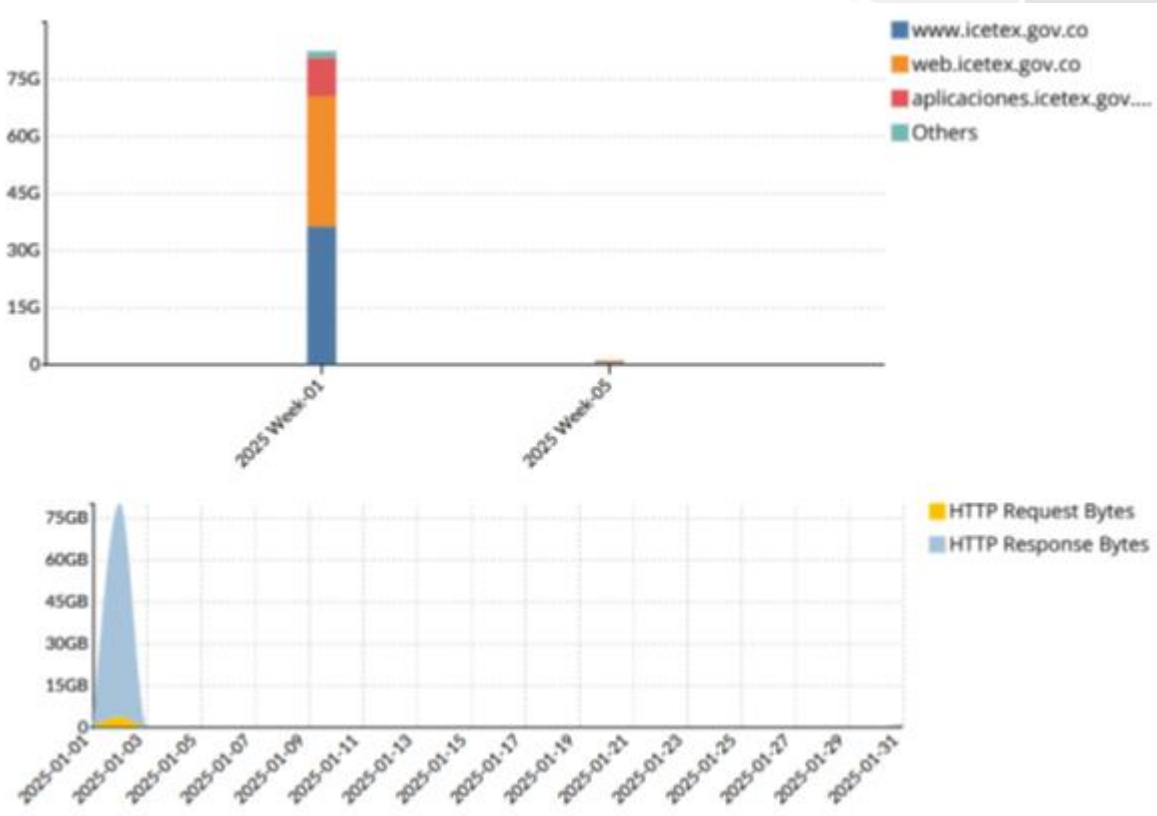


Ilustración 15 Evidencia Gráfica Estadísticas de Portales

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	www.icetex.gov.co	571.24 MB	33.96 GB
2	web.icetex.gov.co	1.85 GB	32.33 GB
3	aplicaciones.icetex.gov.co	1.15 GB	9.46 GB
4	portal.icetex.gov.co	38.49 MB	1.35 GB
5	comunidad.icetex.gov.co	4.57 MB	310.18 MB
6	web.icetex.gov.co:443	30.48 KB	1.71 MB
7	(186.84.73.154) web.icetex.gov.co	6.52 KB	1.06 MB
8	(186.84.73.155) transaccional.icetex.gov.co	2.19 KB	382.83 KB
9	www.icetex.gov.co:443	43.54 KB	274.61 KB
10	(186.84.73.163) cina.icetex.gov.co	939 B	233.64 KB

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 enero 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 250201 Informe Mensual SOC-TH ICETEX Enero 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)	Enero 2025	Diciembre 2024	Noviembre 2024
IOC – Malware DOMINIOS	3.919	3.897	3.897
IOC – Malware IPs	5.278	5.276	5.253
IOC – Malware HASH	1.612	1.612	1.606
IOC – Malware URL	780	778	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 250201 Informe Mensual SOC-TH ICETEX Enero 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:

Severity	Cantidad de ...
Medium	22,668
High	352
Low	256

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 Enero 2025	Alertas de Seguridad Diciembre 2024	Alertas de Seguridad Noviembre 2024
High	352	605	272
Medium	22668	4304	3862
Low	256	194	348

Tabla 14 comparativo Alertas de Seguridad

En el mes de enero con respecto al mes anterior:

- Las amenazas de seguridad de severidad “Alta” disminuyeron en un 42%
- Las amenazas de seguridad de severidad “Media” aumentaron en un 427%
- Las amenazas de seguridad de severidad “Baja” aumentaron en un 32%

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:

Severity	Cantidad de ...
Medium	56,404
Low	846
High	104

Ilustración 17 Total de alertas de disponibilidad

Durante el período evaluado se presentaron 106 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 Enero 2025	Alertas de Disponibilidad Diciembre 2024	Alertas de Disponibilidad Noviembre 2024
High	104	84	74
Medium	56404	67378	94505
Low	846	944	645

Tabla 15 comparativo alertas de disponibilidad

En el mes de enero con respecto al mes anterior:

- Las amenazas de disponibilidad de severidad “Alta” aumentaron en un 24%
- Las amenazas de disponibilidad de severidad “Media” disminuyeron en un 16%
- Las amenazas de disponibilidad de severidad “Baja” disminuyeron en un 10%

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:

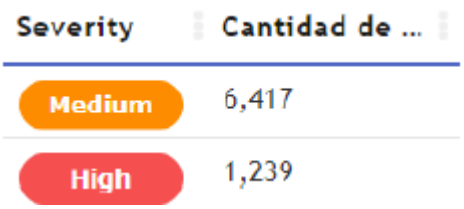


Ilustración 18 Total de alertas de Rendimiento

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 Enero 2025	Alertas de Rendimiento Diciembre 2024	Alertas de Rendimiento Noviembre 2024
High	1239	1442	1389
Medium	6417	6324	5976

Tabla 16 comparativo alertas de Rendimiento

En el mes de enero con respecto al mes anterior:

- Las amenazas de Rendimiento de severidad “Alta” disminuyeron un 14%
- Las amenazas de Rendimiento de severidad “Media” aumentaron en un 1%

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 Enero2025).pdf

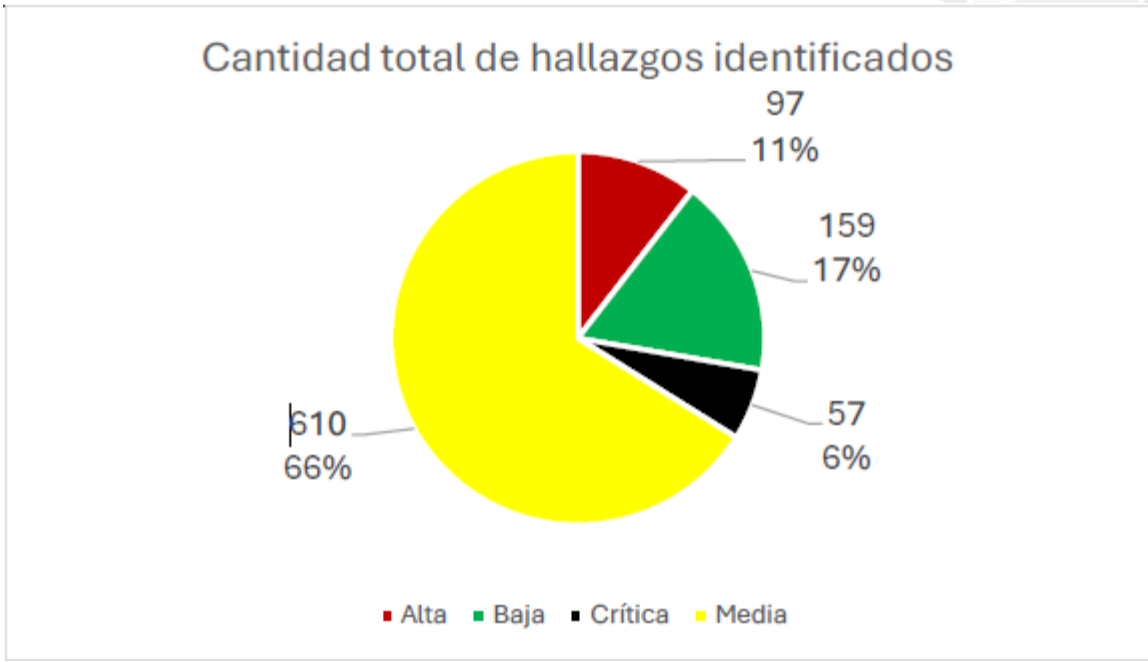


Ilustración 19 Cantidad Total de Hallazgos identificados

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 Enero_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 enero del 2025 del proyecto, se encuentra en la fase de operación de los servicios contemplados en el alcance llevando ejecutados 22 meses que equivale al 61.11% de avance, para lo cual INFOTIC presenta:

- Informes de cada uno de los especialistas.
- Reportes e informes generados por cada uno de los aliados estratégicos sobre la gestión realizada.
- Las evidencias sobre las situaciones y acciones realizadas sobre eventos presentados en la operación de INFOTIC sobre la infraestructura del ICETEX.

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

NOMBRE COMPLETO	ROL RESPONSABLE
Carlos Alberto Roldan Ríos	Administrador de Red
Juan Carlos Martínez Sierra	Administrador Web
Edgar Cobos Mayorga	Administrador DBA
Jairo Ever Prada Murcia	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 enero 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 enero del 2025:

ALIADO	SERVICIOS
	Data center
	Canales de comunicación
	Comunicaciones
	Internet de gente (WIFI)

ALIADO	SERVICIOS
CLARO	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**
$ 31.398.996.857,96	$ 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**
	$ 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		$480,000,000		

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	$ 803,086,052.43	
VALOR CAUSADO QUE NO SE HA PAGADO *(valor a pagar factura)* *						$ 803,086,052.43
VALOR TOTAL EJECUTADO *(valor pagado + valor causado no pagado)*						$ 15,244,823,223
SALDO DEL CONTRATO *(valor total del contrato – valor total ejecutado)*						$ 16,154,173,635
PORCENTAJE DE EJECUCIÓN						48.55%
** 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 ENERO 2025.pdf
Reporte Mensual ICETEX_v2- ENERO.pdf

7.1.1. Especialista en Base de Datos DBA

El proyecto cuenta con dos 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 dos especialistas de networking 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 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 enero del 2025 sobre la solución de videoconferencia en las sedes regionales, se encontró que la solución completa presentó estado activo para los 31 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.

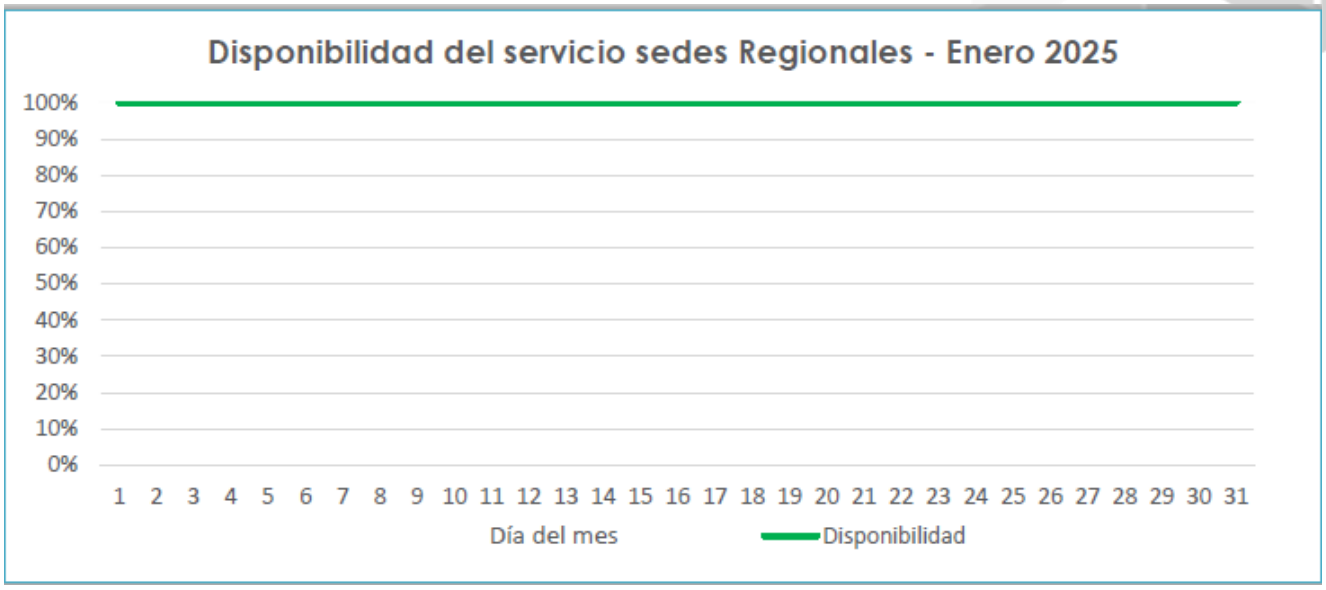


Ilustración 20 Disponibilidad de servicio videoconferencia sedes regionales – enero 2025

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

En la verificación realizada en el mes de enero 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 31 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.

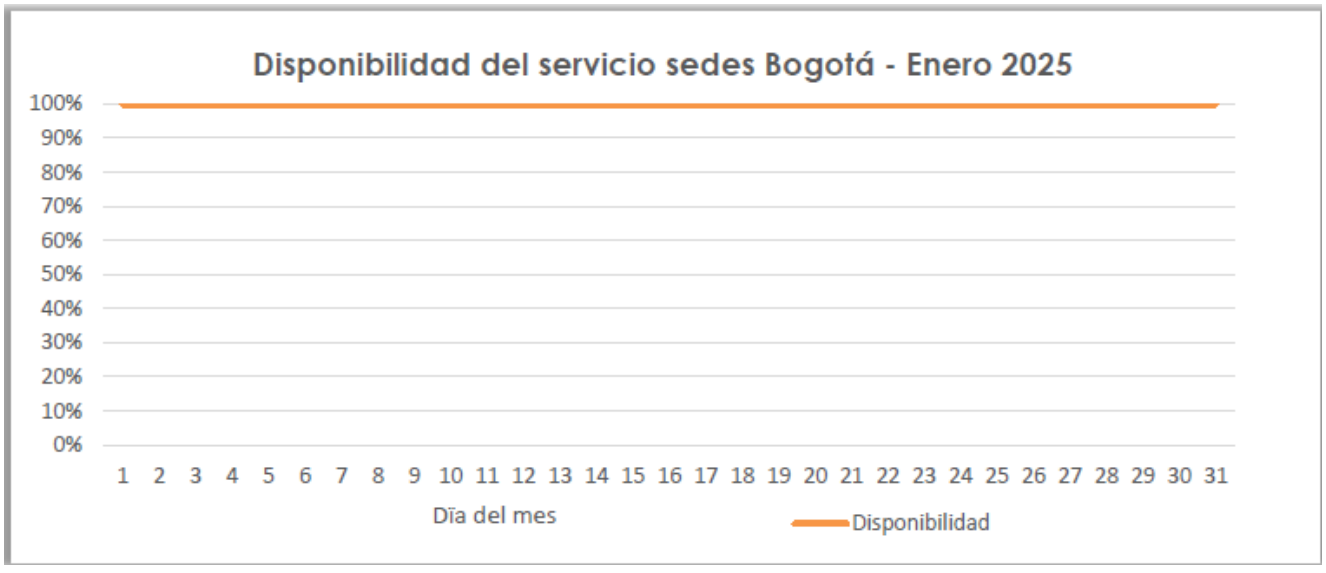


Ilustración 21 Disponibilidad de servicio videoconferencia sedes Bogotá – enero 2025

8.3. Gestión de incidencias y requerimientos – sedes regionales

Para el periodo de enero del 2025, comprendido entre el 1 y el 31 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.

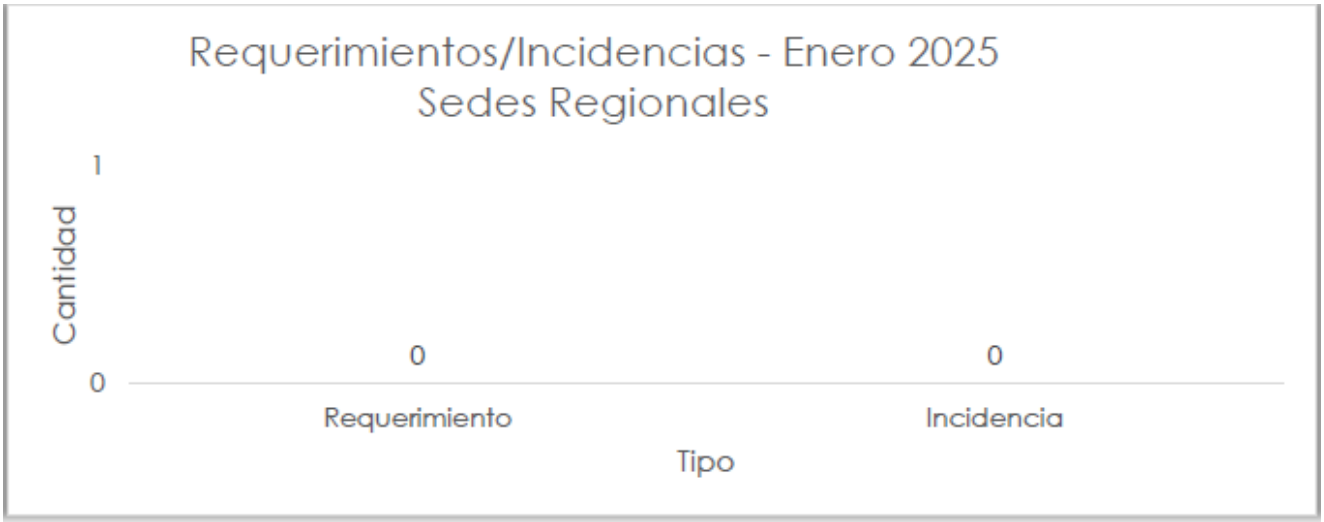


Ilustración 22 Incidentes / Requerimientos sedes regionales – enero 2025

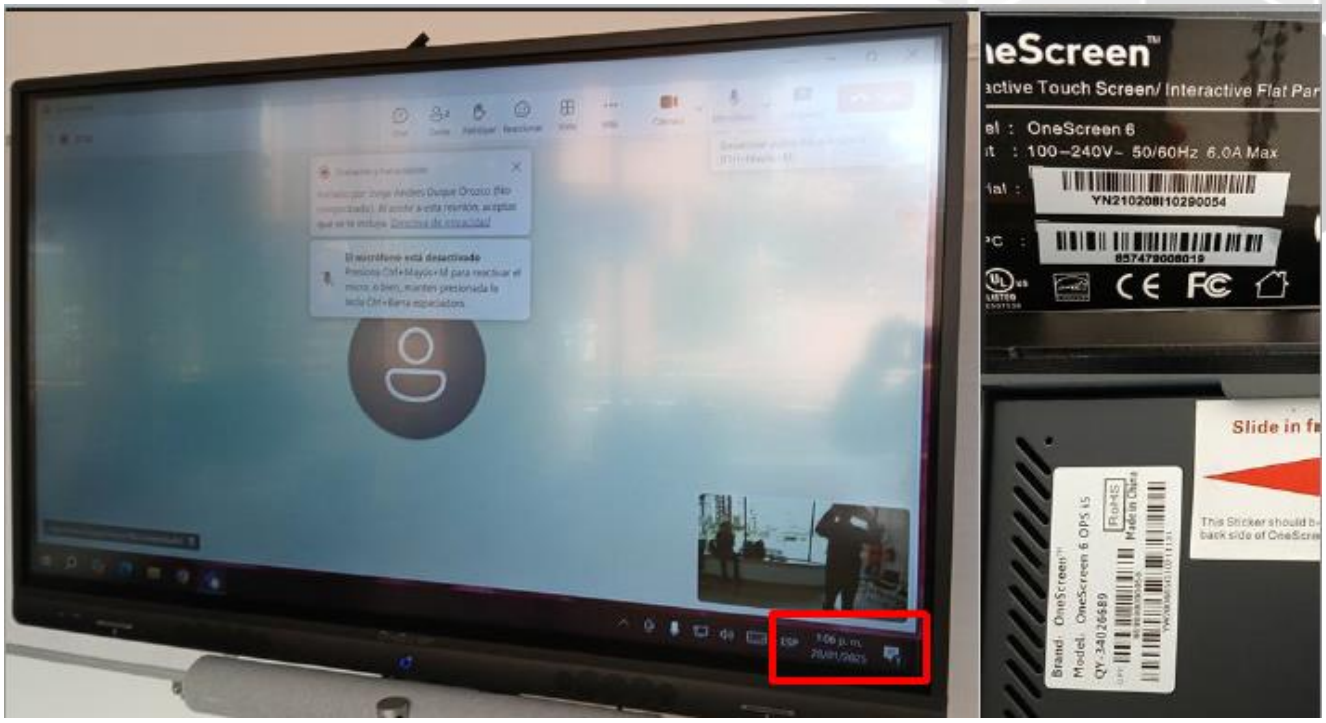


Ilustración 23 Prueba de funcionamiento visita sede chapinero – enero 2025

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

Para el periodo comprendido entre el 1 y el 31 de enero 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-292884-8-21810.

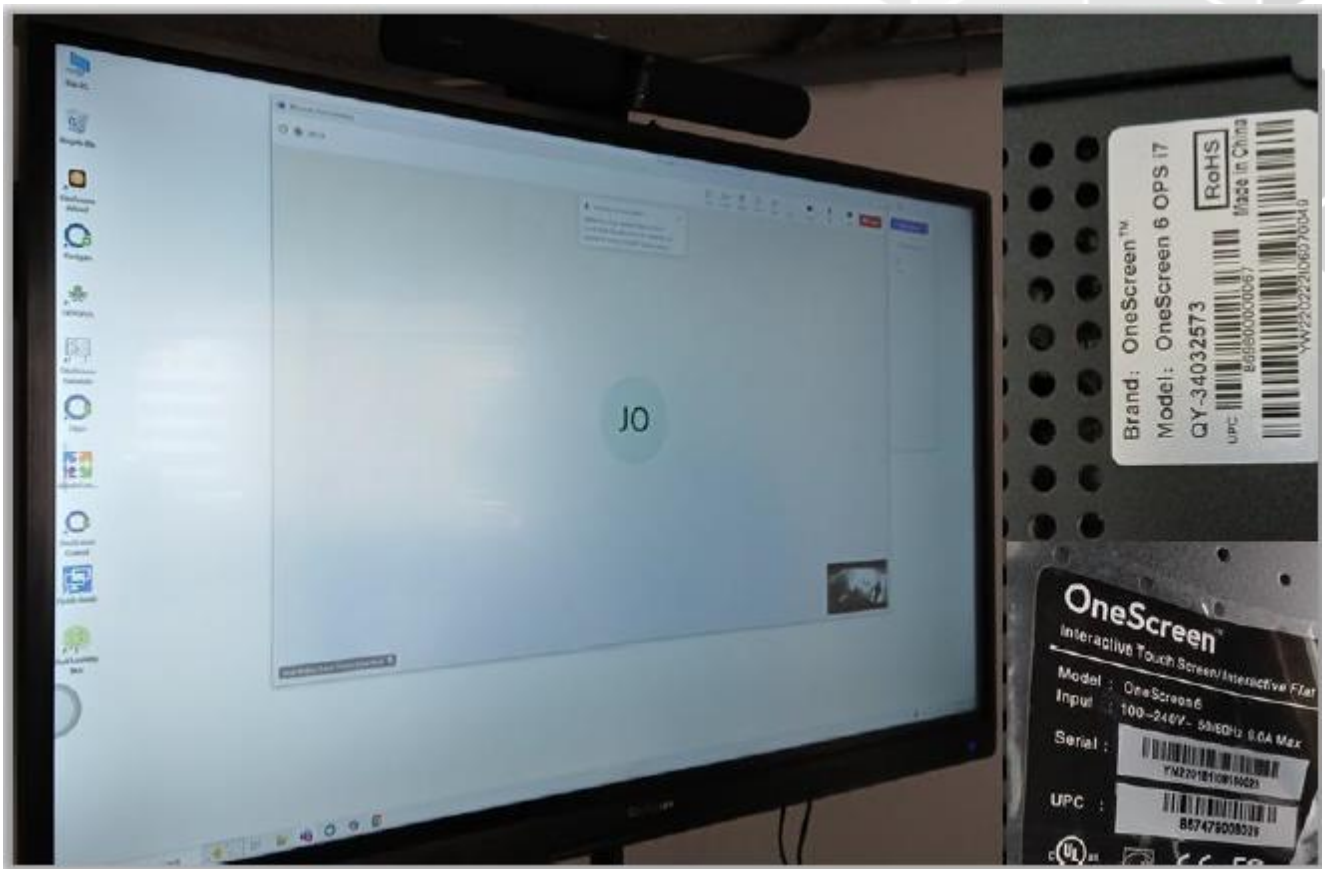


Ilustración 24 Módulo funcional sala 8vo piso Presidencia – Visita enero 2025

Para la OPS del módulo piso 8, se proyecta realizar inicialmente en una próxima visita mantenimiento preventivo de limpieza interna de la OPS para eliminar suciedad en el dispositivo.

Durante la visita realizada para el periodo se realizaron pruebas en los módulos de cada piso de la sede Aguas para 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, en la imagen a continuación se encuentra la evidencia del correcto funcionamiento del módulo piso 4 – Aguas.



Ilustración 25 Evidencia módulo funcional sede Aguas 65, piso 4 - Visita enero 2025

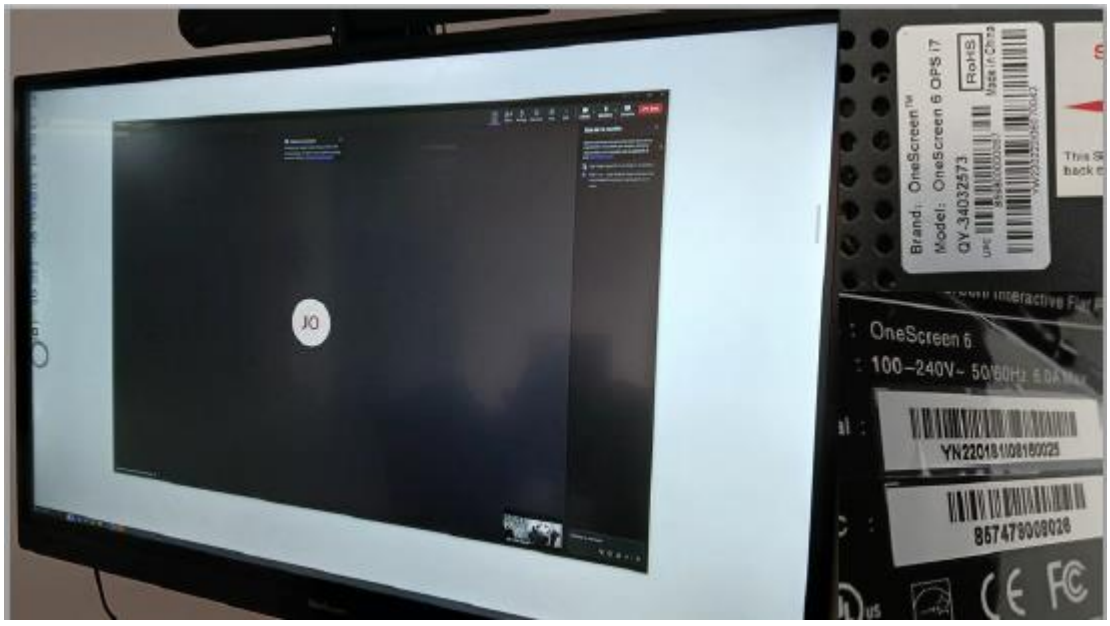


Ilustración 26 Evidencia módulo funcional sede Aguas, ubicación piso 6 – Visita enero 2025

Para el módulo ubicado en el auditorio del piso 2 – sede Aguas, se encontró que la antena de la tarjeta de red inalámbrica se encuentra rota la base plástica posiblemente por una mala manipulación de elemento.

Adicional, se configuró la aplicación de TEAMS del módulo en el modo de visualización con la pantalla externa (TV extendida), debido a que cuando se iniciaba una sesión virtual o reunión, el contenido del módulo se visualizaba en la pantalla externa o extendida y no permitía manipular la pantalla interactiva del módulo, por lo cual se deja en los valores estándar y retoma, con funcionamiento normal.

Se desconoce si la configuración que tenía el módulo fue aplicada por algún usuario o personal de soporte técnico de la entidad, sin embargo, se corrige la novedad encontrada como se visualiza en la imagen a continuación.



Ilustración 27 Evidencia módulo funcional sede Aguas Piso 2 – Visita enero 2025

En la figura siguiente se evidencia la revisión realizada del módulo de la sede Ángel, el cual se encuentra funcionando con normalidad sin presentar incidencias, para el cual se proyecta en una próxima visita inicialmente realizar mantenimiento preventivo de limpieza interna de la OPS para eliminar suciedad en el dispositivo.



Ilustración 28 Verificación módulo visita sede Ángel - enero 2025

Durante el mes de enero, al igual que 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 externa de los equipos que se encuentran instalados en las sedes de Bogotá, con lo cual 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 y funcionarios en las sedes regionales.

Para prevenir fallas y garantizar un rendimiento óptimo, además con el fin de 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 y realizar nuevamente en la vigencia 2025 con la regularidad requerida los mantenimientos preventivos en las sedes regionales de Icetex, con lo cual se busca 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 enero se realizaron las siguientes actividades relacionadas al servicio de módulos de videoconferencia:

- Visita en sitio recurrente del periodo para pruebas de funcionamiento, inspección de los módulos y posterior limpieza externa módulos instalados en la ciudad de Bogotá, Aguas, Ángel y Chapinero, para garantizar la prestación continua del servicio y validar que no se estén presentado novedades y/o incidencias.

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

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

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

	Noviembre 2024	Diciembre 2024	Enero 2025
Requerimiento	4	0	0
Incidentes	0	0	0

Tabla 23 Distribución trimestral de requerimientos y/o incidentes

Para el mes de enero 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 29 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 enero 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 Enero 2025.pdf
Informe Mensual ALLOT Enero 2025.pdf

También se puede consultar en el repositorio un documento en Excel con el análisis del comportamiento de los canales para el mes de enero ANS_Enero_2025.xlsx

Sede	Categoría	INR	%MES
BOGOTAD.C.	Principal/FO (Sede Aguas)	INR0037	100.00%
	Backup /FO (Sede Aguas)	INR0036	100.00%
	Principal/IPVPN (Sede Chapinero)	INR0022	100.00%
	Backup /IPVPN (Sede chapinero)	INR0020	100.00%
	Principal/IPVPN (Angel)	INR0272	100.00%
	Backup /IPVPN (Angel)	INR0273	100.00%
IBAGUE	Principal/IPVPN	INR0073	100.00%
	Backup/IPVPN	INR0076	100.00%
LETICIA	Principal/Satelital	INR0000373	95.93%
NEIVA	Principal/IPVPN	INR0039	99.98%
	Backup/IPVPN	INR0041	100.00%
TUNJA	Principal/IPVPN	INR0104	99.92%
	Backup/IPVPN	INR0106	100.00%
VILLAVICENCIO	Principal/IPVPN	INR0085	97.36%
	Backup/IPVPN	INR0084	85.17%
ARMENIA	Principal/IPVPN	INR0074	100.00%
	Backup/IPVPN	INR0072	99.93%
MANIZALES	Principal/IPVPN	INR0088	99.48%
	Backup/IPVPN	INR0087	100.00%
MEDELLIN	Principal/IPVPN	INR0133	96.59%
	Backup/IPVPN	INR0132	96.68%
APARTADO	Principal/IPVPN	INR0144	99.88%
PEREIRA	Principal/IPVPN	INR0079	99.89%
	Backup/IPVPN	INR0077	100.00%
QUIBDO	Principal/IPVPN	INR0014	100.00%
	Backup/IPVPN		0%
BARRANQUILLA	Principal/IPVPN	INR0103	100.00%
	Backup/IPVPN	INR0100	100.00%
CARTAGENA	Principal/IPVPN	INR0109	95.36%
	Backup/IPVPN	INR0107	99.25%
MONTERIA	Principal/IPVPN	INR0080	100.00%
	Backup/IPVPN	INR0081	100.00%
RIOHACHA	Principal/IPVPN	INR0164	100.00%
	Backup/IPVPN	INR0162	99.93%
SANTAMARTA	Principal/IPVPN	INR0154	99.81%
	Backup/IPVPN	INR0152	99.92%

Sede	Categoría	INR	%MES
SINCELEJO	Principal/IPVPN	INR0095	99.89%
	Backup/IPVPN	INR0097	99.89%
SANANDRES	Principal/IPVPN	INR0000367 INR0000369	97.61%
BARRANCABERMEJA	Principal/IPVPN		0%
SANGIL	Principal/IPVPN		0%
BUCARAMANGA	Principal/IPVPN	INR0062	100.00%
	Backup/IPVPN	INR0061	100.00%
CUCUTA	Principal/IPVPN	INR0044	100.00%
	Backup/IPVPN	INR0047	100.00%
VALLEDUPAR	Principal/IPVPN	INR0091	100.00%
	Backup/IPVPN	INR0090	99.66%
YOPAL	Principal/IPVPN	INR0121	99.37%
	Backup/IPVPN	INR0123	100.00%
ARAUCA	Principal/IPVPN	INR0110	30.30%
CALI	Principal/IPVPN	INR0151	93.22%
	Backup/IPVPN	INR0153	100.00%
BUENAVENTURA	Principal/IPVPN	INR0051	99.38%
MOCOA	Principal/IPVPN	INR0135	99.97%
	Backup/Satelital	INR0136	98.96%
PASTO	Principal/IPVPN	INR0130	100.00%
	Backup/IPVPN	INR0131	100.00%
POPAYAN	Principal/IPVPN	INR0035	99.93%
	Backup/IPVPN	INR0032	99.93%
TUMACO	Principal/IPVPN	INR0147	78.85%
DCTRIARA	MPLSPP	INR0266	100.00%
	MPLS Backup	INR0171	100.00%
DCTRIARA	NOC claro de dedicado (DWDM)2GTriaramegacentro	INR0224	100.00%
Canal entre Sitio principal Icetex-Dirección General-Aguas	Principal/IPVPN		0%
	Backup/IPVPN		0%
BOGOTAD.C.	Internet (Sede Aguas)	INR0034	100.00%
DC Megacentro	DCMEGACENTER–CONTIGENCIA–MPLSPPAL	INR0177	99.99%
DCTRIARA	DCMEGACENTER–CONTIGENCIA–MPLSBK	INR0230	99.99%
DC Megacentro	Internet	INR0268	100.00%
Banco de la Republica hasta Edificio Dirección General ICETEX	Ubicado en Data center Principal. Interconectado a través de red MPLS	INR0000289	100.00%

Sede	Categoría	INR	%MES
DECEVAL hasta Edificio de ICETEX Dirección General	Ubicado en Data center Principal. Interconectado a través de red MPLS	INR0000317	100.00%
DECEVAL hasta Edificio de ICETEX Dirección General	UbicadoenDatacenterPrincipal.interconectadoatravesderedMPLS(Backup)	INR0000318	100.00%
Salidadelportaleshttps://portal.icetex.gov.co/portalywww.icetex.gov.cohaciainternetencentrodecómputoprincipal	Internet Reverso para Portales	INR0000320	100.00%
Salidadelportaleshttps://portal.icetex.gov.co/portalywww.icetex.gov.cohaciainternetencentrodecómputodecontingencia	Internet Reverso para Portales	INR0274	100.00%
DCTRIARA	allotentralizado800Mtriara(equipo)	INR0270	100.00%

Tabla 26 Disponibilidad de Canales

Durante el mes de enero 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 enero, 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%

Sede	Categoría	INR	% Mes
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 enero continúa su funcionamiento correctamente sin novedades que afectaran la prestación del servicio.

La evidencia se encuentra en el Informe mensual replicacion Enero 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 Enero 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 Enero 2025-ELK_2.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. Se estima que esta migración concluirá en el mes de febrero.

Durante el mes de Enero algunas máquinas virtuales dejaron de reportar en la herramienta ELK , los datos faltantes en dicha herramienta se pudieron observar en la herramienta SITESCOPE porque todavía conservaban dicho monitoreo, se puede evidenciar en el link: Reporte Monitoreo ICETEX Enero 2025-SITESCOPE.pdf

Se encontraron hallazgos que afectaron el reporte de disponibilidad de los servidores reportados, aclarando que los servidores no presentaron incidencia todo se debió al proceso de migración de la herramienta de monitoreo ELK .

Lo cual arrojo la siguiente disponibilidad al promediar la información registrada en ELK y SITESCOPE:

Cod Servicio	Hostname	Disponibilidad
INR0228	ictxsisgesbd	72.58%
INR0229	ictxsisgesapp	99.98%
INR0233	icetexboglxorfeo1	72.58%
INR0234	ictxprusisgapp	99.82%
INR0237	icetexbogbalserver1-r	100%
INR0238	icetexbogliferaynfs	99.93%

Cod Servicio	Hostname	Disponibilidad
INR0239	icetexbogelasticserver1	100%
INR0241	icetexbogelasticserver3	100%
INR0242	icetexbogliferayserver2	100%
INR0243	icetexbogliferayserver1	100%
INR0244	icetexboglxdarumasrv1	99.96%
INR0245	icetexboglxdarumasrv2	100%
INR0246	icetebоglxdarumatest	72.58%
INR0247	preprodsec-icetexboglxxroad2n	72.58%
INR0248	icetexboglxxroad3	99.86%
INR0249	xroadsec-icetexboglxxroad1	72.58%
INR0250	qasec-icetexboglxxroadtest	72.58%
INR0262	icetexboglxorfeo2	100%
INR0276	cxvodaprodn011	100%
INR0277	cxvodaprodn021	100%
INR0278	cxvodacontn011	100%
INR0240	icetexbogelasticserver2	100%
INR0260	icetexbogosbognfs1	100%
INR0252	icetexbogosbognfs2	100%
INR0236**	ictxbogsrvpt1	100%
INR0235**	ictxbogsrvpt2	100%
INR0000322	ictxcontroldoc	0%
INR0226	mira	72.58%
INR0253*	bastion	0%
INR251	Openshift	100%
INR254	Openshift	100%
INR255	Openshift	100%
INR256	Openshift	100%
INR257	Openshift	100%
INR258*	Openshift	100%
INR259	Openshift	100%

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 visualizaran a partir del mes de enero de 2025 en el Reporte de disponibilidad ELK Reporte Monitoreo ICETEX Enero 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 enero un **UPTIME del [99,983%]** tal como se evidencia en la gráfica a continuación.

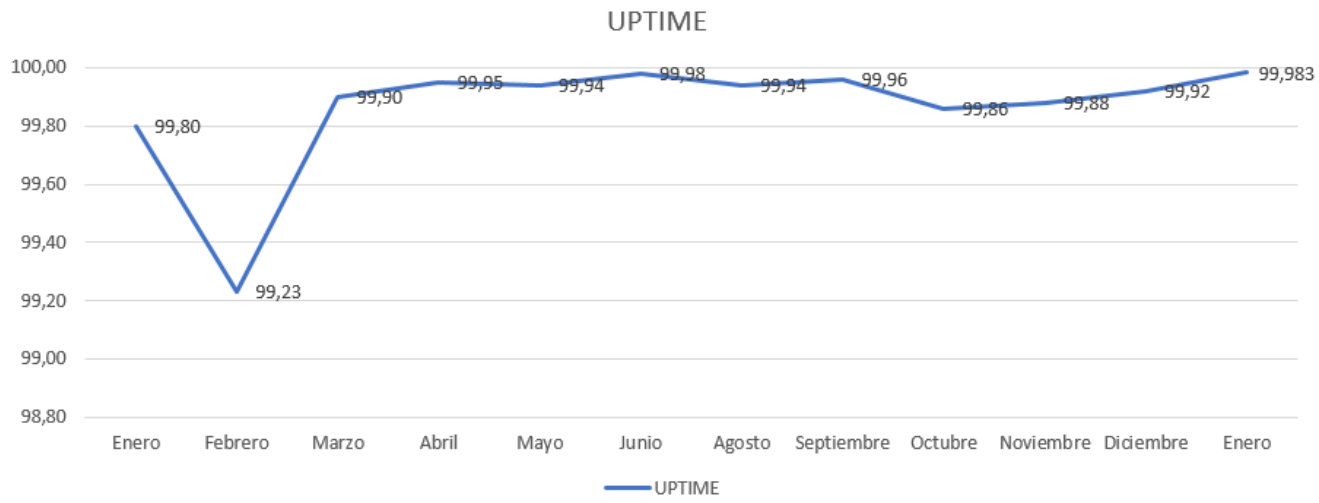


Ilustración 30 UPTIME – Portal WEB web.ICETEX.gov.co

Durante el mes de enero se evidenció un comportamiento estable del portal WEB institucional y se cumplió con el porcentaje de disponibilidad de este con un porcentaje del **99,983%,** 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 373 mil usuarios nuevos. El tiempo de interacción medio es de 2 minutos 17 segundos, señalando el interés de la audiencia en las diferentes páginas del portal web.ICETEX.gov.co.

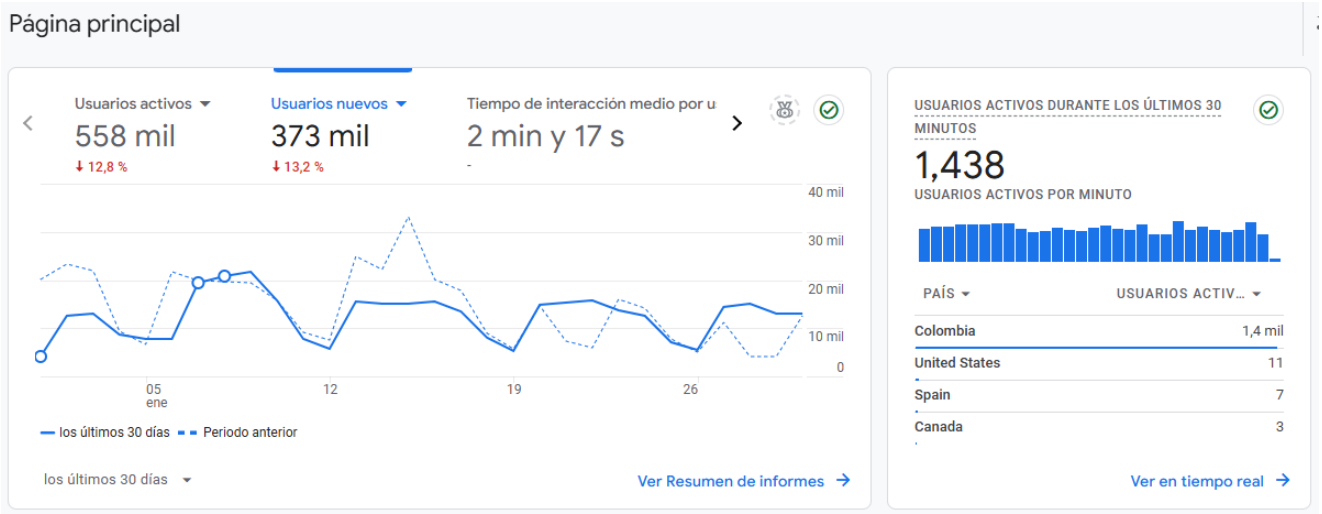


Ilustración 31 Métrica de visitantes Portal WEB web.ICETEX.gov.co

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

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 32 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 miércoles 1 de enero desde las 0:00 am hasta las 11:59 am del viernes 31 de enero de 2.025.

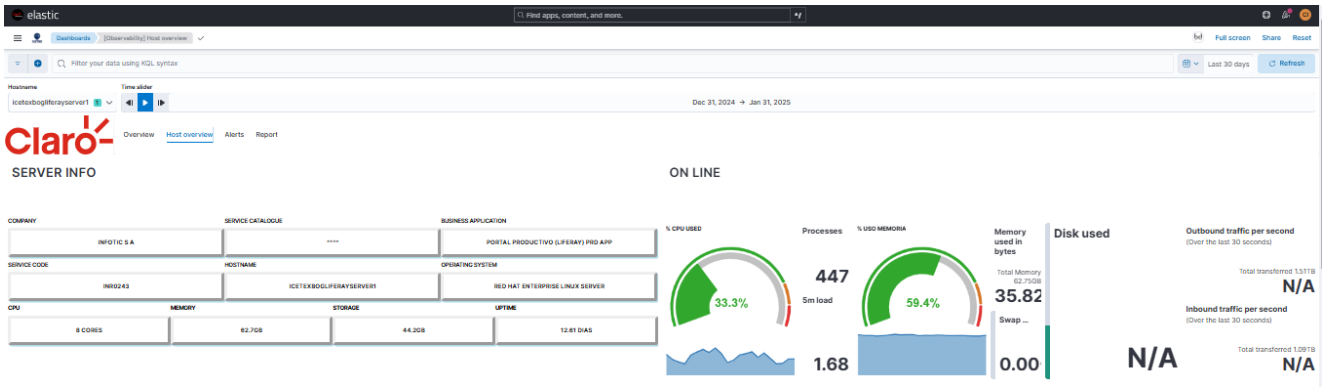


Ilustración 33 NODO 1 – Vista General – INR0243

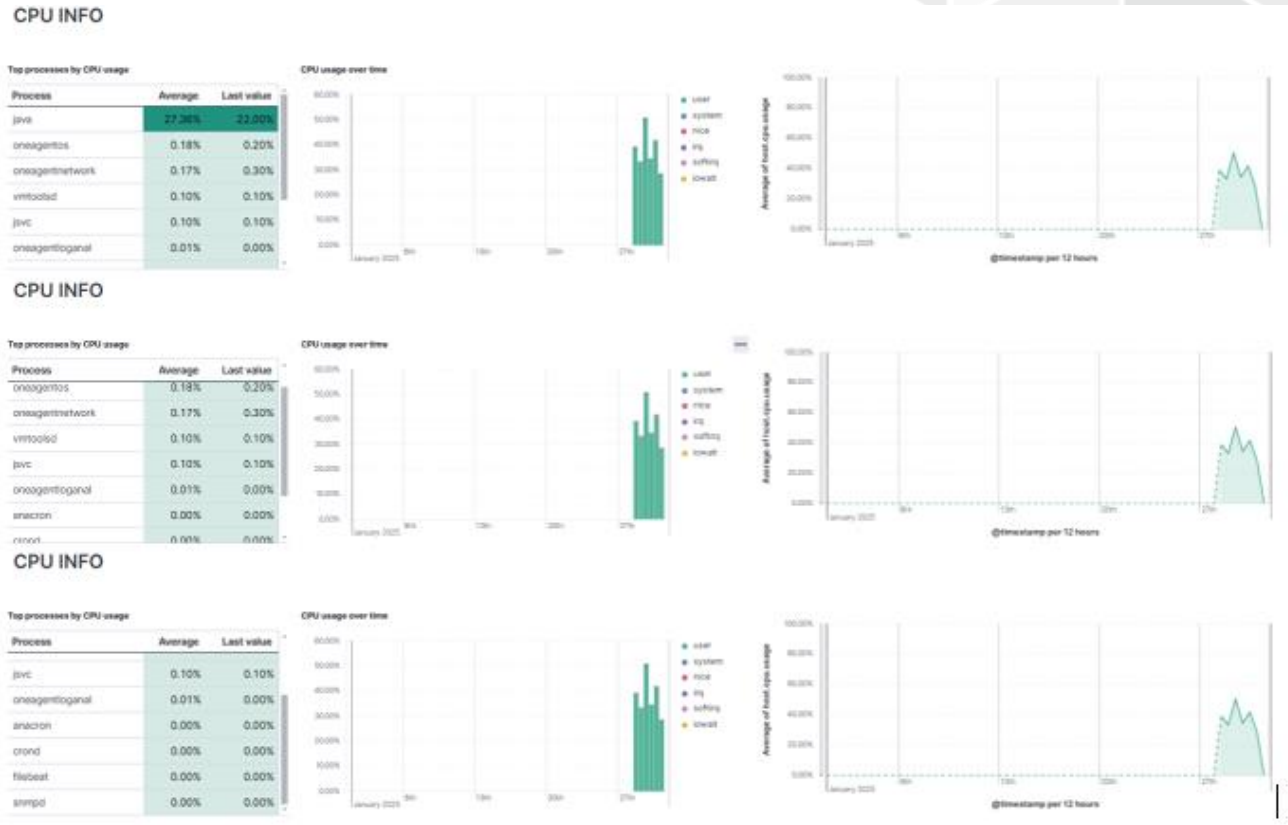


Ilustración 34 NODO 1 CPU

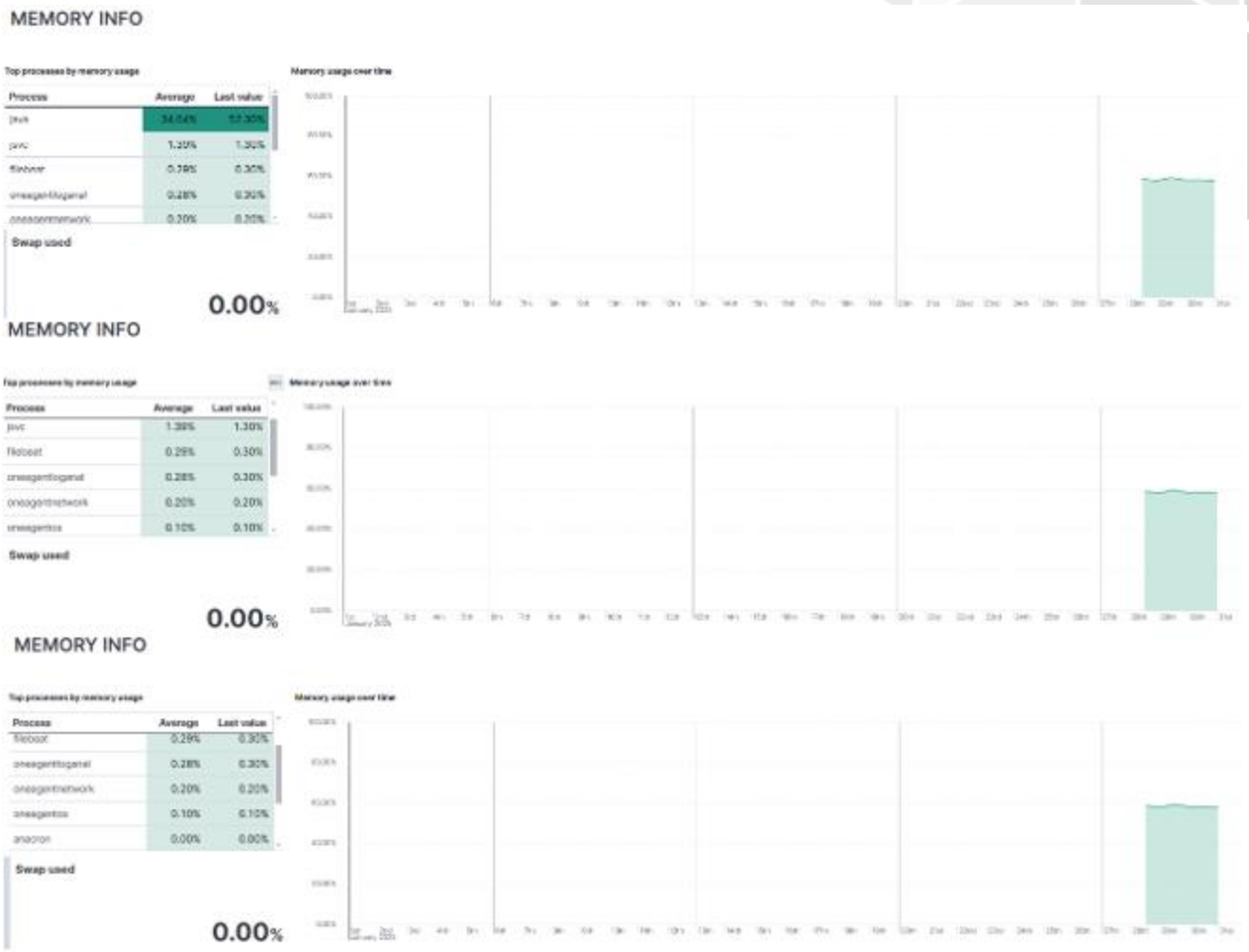


Ilustración 35 NODO 1 Memoria

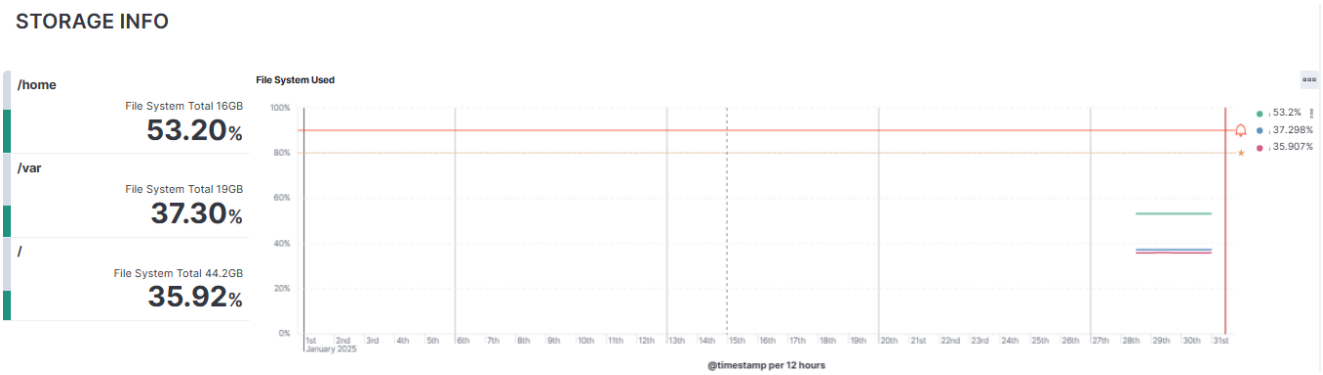


Ilustración 36 NODO 1 Almacenamiento

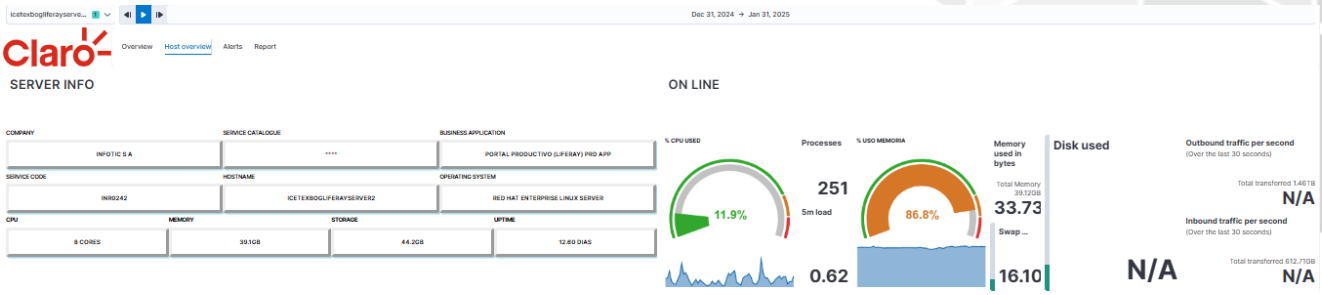


Ilustración 37 NODO 2 – Vista General – INR0242

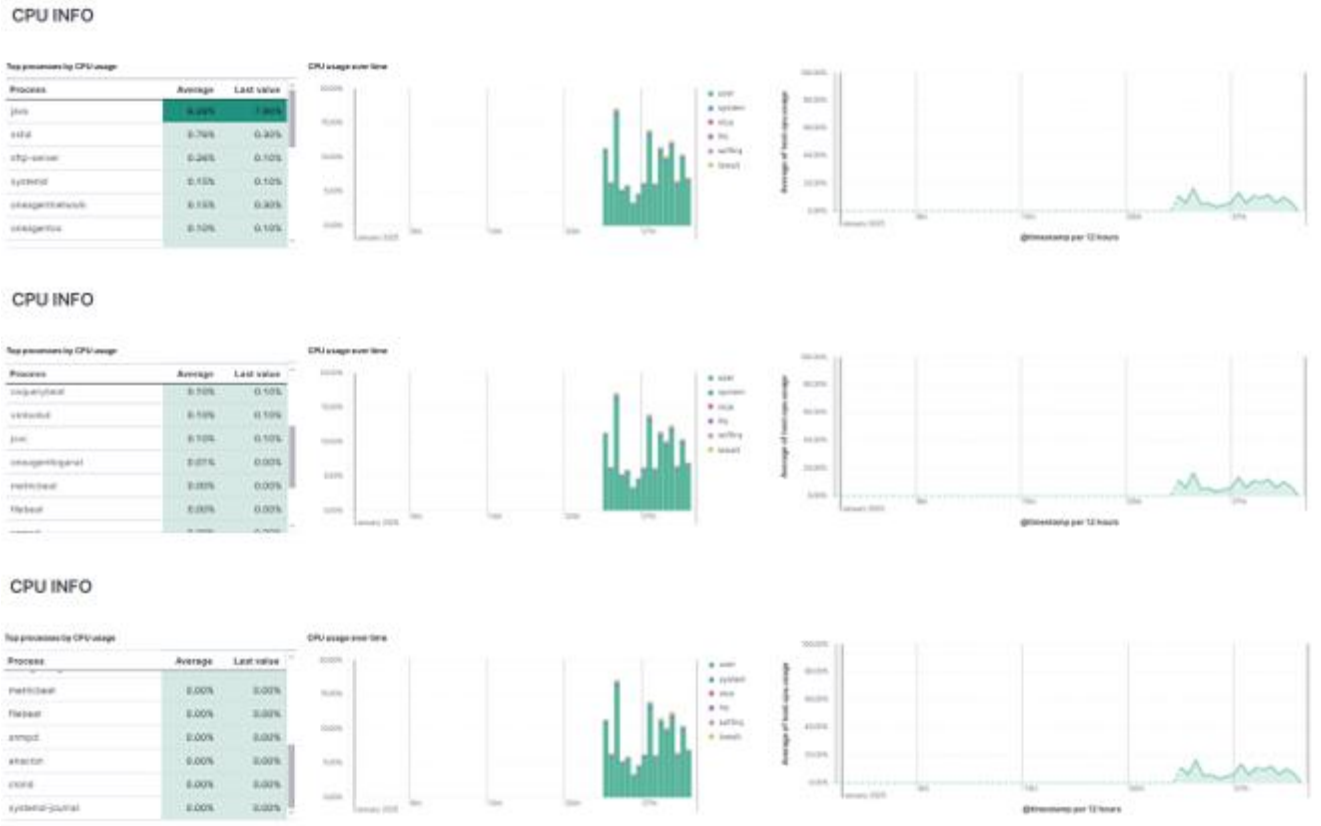


Ilustración 38 NODO 2 CPU

Entre el 1 y el 31 de enero, no hubo consumo desmedido de memoria SWAP en el nodo 2, debido a que se ejecutó a diario un código Groovy sugerido por soporte Liferay **caso N° 125259**. Con la ejecución del script el consumo de memoria SWAP en nodo 2 ha sido moderado, se adjunta imagen. Por consiguiente, el partner Claro no volvió a emitir alarmas de alto consumo de SWAP en nodo 2.

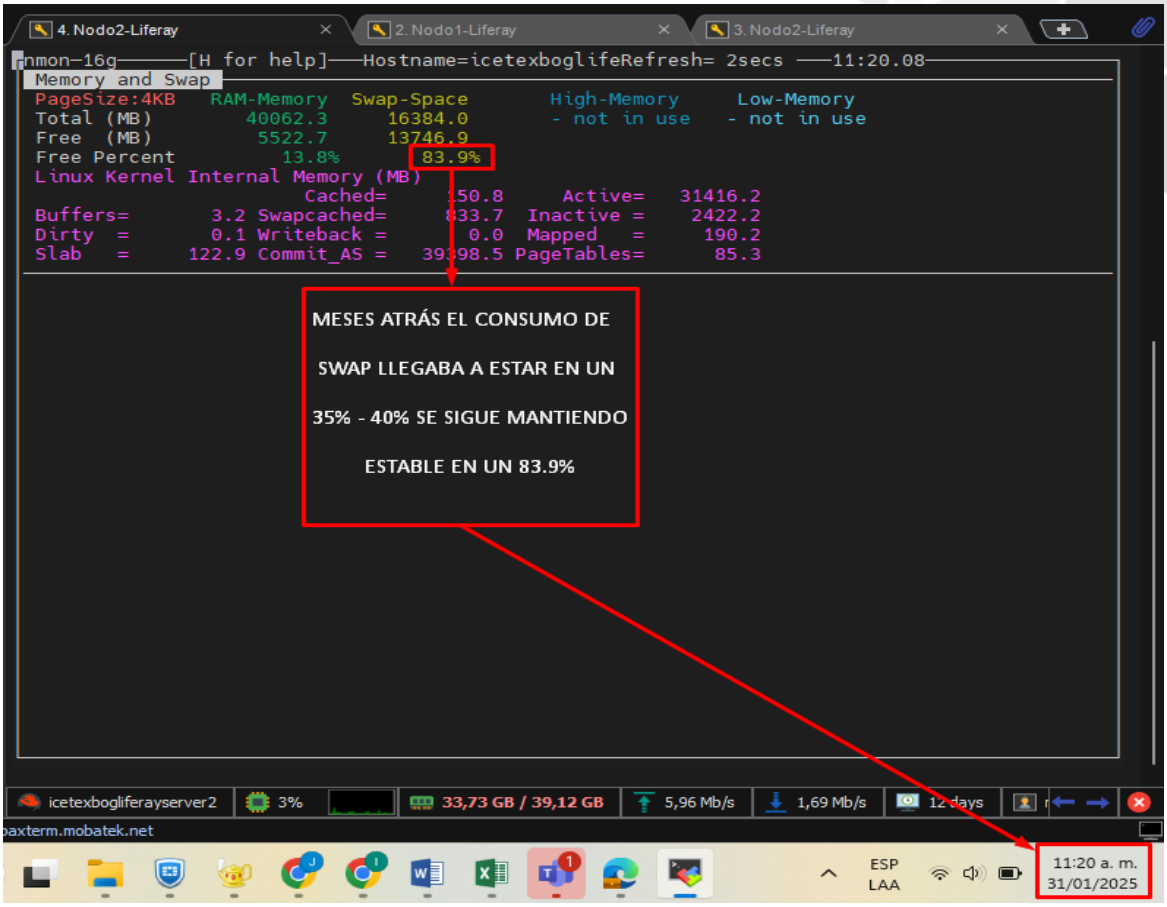


Ilustración 39 NODO 2 memoria SWAP



Ilustración 40 NODO 2 Memoria

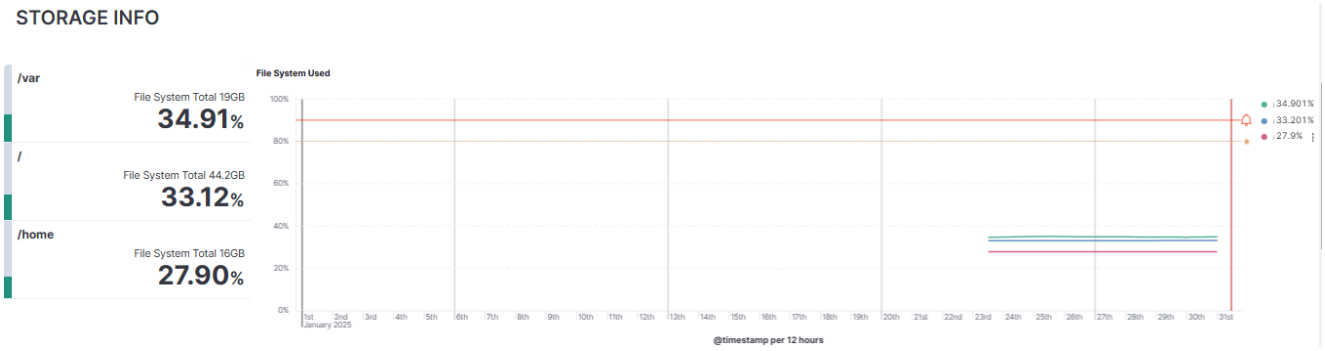


Ilustración 41 NODO 2 Almacenamiento

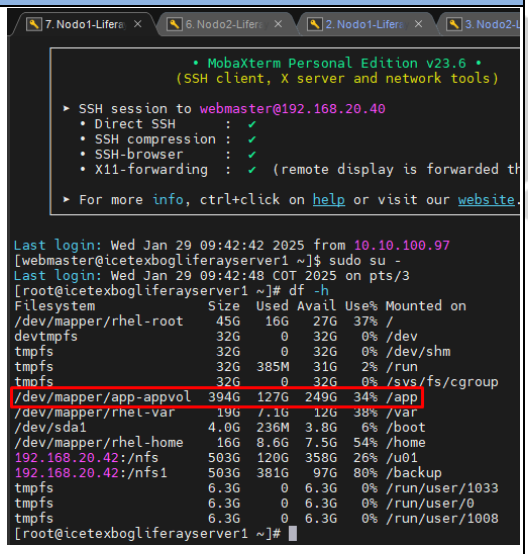
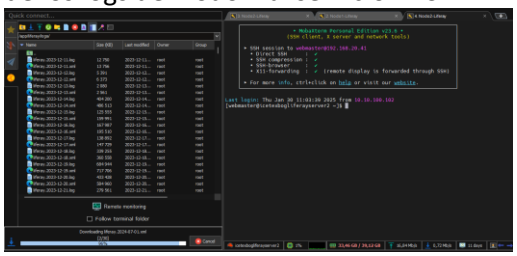
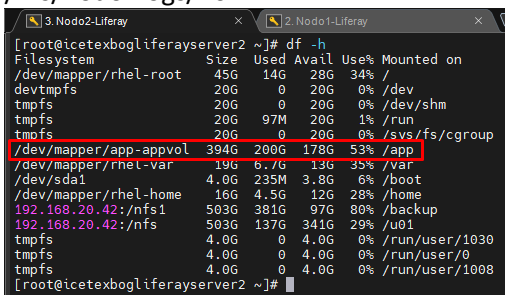
Los recursos del sistema de los servidores nodo 1 y 2, no presentaron indisponibilidad durante los 31 días del mes.

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:

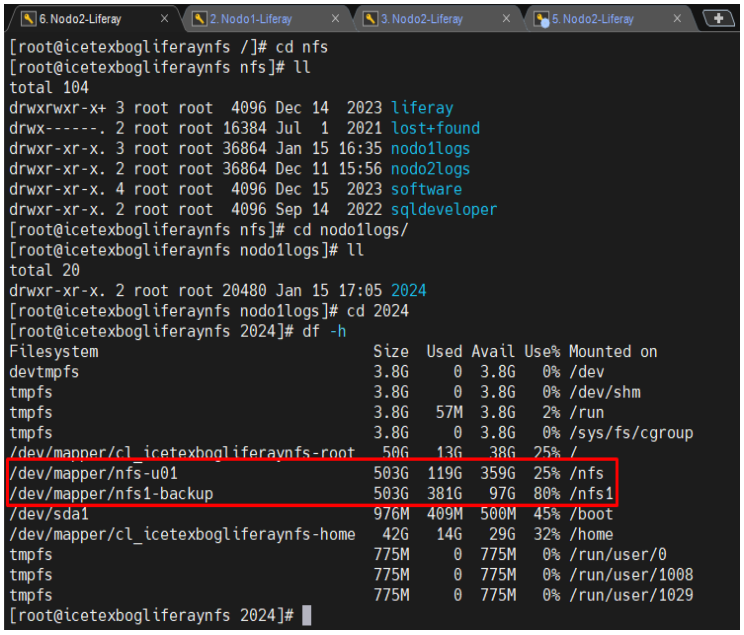
UNIDAD	HALLAZGO	OBSERVACIONES
MEMORIA RAM	**Nodo 1** total de memoria RAM – 65.79 GB. **Nodo 2** total de memoria RAM – 41.02 GB	En espera de **la autorización** para disponer y configurar la memoria necesaria para que los dos nodos queden iguales.
SISTEMA OPERATIVO	La última versión del UPDATE **del 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 291 GB**. El espacio disponible es de 86 GB.	Comportamiento normal. Se realizó la exportación de logs comprimidos en formato .zip al servicio NFS, ruta: /nfs/nodo1logs/2024 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 **249 GB**.

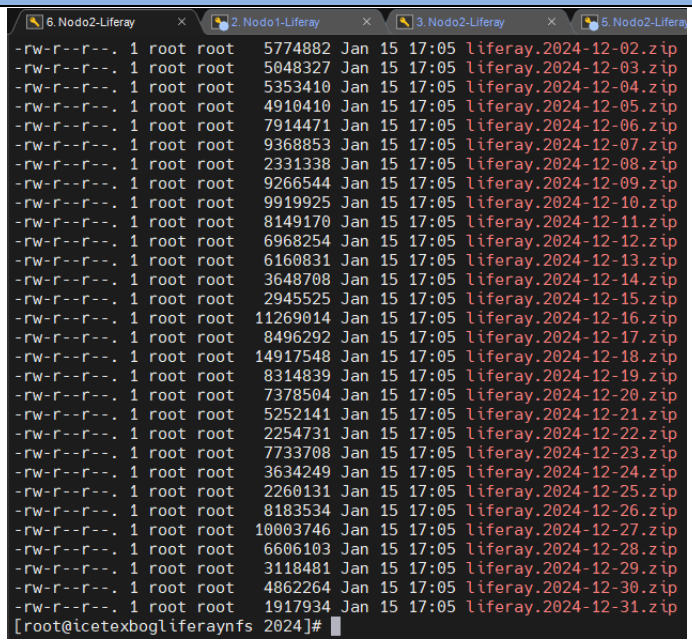
UNIDAD	HALLAZGO	OBSERVACIONES
	El espacio en disco utilizado por el CMS Liferay en el **nodo 2 es 200 GB**. El espacio disponible es de 194 GB.	 Actualmente, se trabaja en la exportación de los logs del nodo 2 al servicio NFS: 
FILE SYSTEM	El espacio en disco utilizado por el CMS Liferay en el **nodo 1 es 428 MB.** El espacio en disco utilizado por el CMS Liferay en el **nodo 2 es 679 MB.**	Posteriormente se copian los logs (.xml y .log por fecha) a la ruta /nfs/nodo2logs/2024 
PARCHES DE SEGURIDAD	**Nodo 1** - activation-key-dxpproduction-7.3-icetex-publicportal 40.xml activation-key-dxpproduction-7.3-icetex-publicportal - icetexbogliferayserver1.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.

UNIDAD	HALLAZGO	OBSERVACIONES
	Nodo 2 - activation-key-dxpproduction-7.3-icetex-publicportal - icetexbogliferayserver2.xml	
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. El 23 de enero, los ingenieros de Claro realizaron la eliminación de los logs del nodo 1 desde el 1 de enero de 2024 hasta el 31 de diciembre de 2024.

Tabla 31 Actualización – Análisis componente LIFERAY Enero

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%.	 6. Nodo2-Liferay | 2. Nodo1-Liferay | 3. Nodo2-Liferay | 5. Nodo2-Liferay [root@icetexbogliferaynfs /]# cd nfs [root@icetexbogliferaynfs nfs]# ll total 104 drwxrwxr-x+ 3 root root 4096 Dec 14 2023 liferay drwx------. 2 root root 16384 Jul 1 2021 lost+found drwxr-xr-x. 3 root root 36864 Jan 15 16:35 nodo1logs drwxr-xr-x. 2 root root 36864 Dec 11 15:56 nodo2logs drwxr-xr-x. 4 root root 4096 Dec 15 2023 software drwxr-xr-x. 2 root root 4096 Sep 14 2022 sqldeveloper [root@icetexbogliferaynfs nfs]# cd nodo1logs/ [root@icetexbogliferaynfs nodo1logs]# ll total 20 drwxr-xr-x. 2 root root 20480 Jan 15 17:05 2024 [root@icetexbogliferaynfs nodo1logs]# cd 2024 [root@icetexbogliferaynfs 2024]# df -h Filesystem Size Used Avail Use% Mounted on devtmpfs 3.8G 0 3.8G 0% /dev tmpfs 3.8G 0 3.8G 0% /dev/shm tmpfs 3.8G 57M 3.8G 2% /run tmpfs 3.8G 0 3.8G 0% /sys/fs/cgroup /dev/mapper/cl_icetexbogliferaynfs-root 50G 13G 38G 25% / /dev/mapper/nfs-u01 503G 119G 359G 25% /nfs /dev/mapper/nfs1-backup 503G 381G 97G 80% /nfs1 /dev/sda1 976M 409M 500M 45% /boot /dev/mapper/cl_icetexbogliferaynfs-home 42G 14G 29G 32% /home tmpfs 775M 0 775M 0% /run/user/0 tmpfs 775M 0 775M 0% /run/user/1008 tmpfs 775M 0 775M 0% /run/user/1029 [root@icetexbogliferaynfs 2024]# 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.

UNIDAD	HALLAZGO	OBSERVACIONES
		

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**.

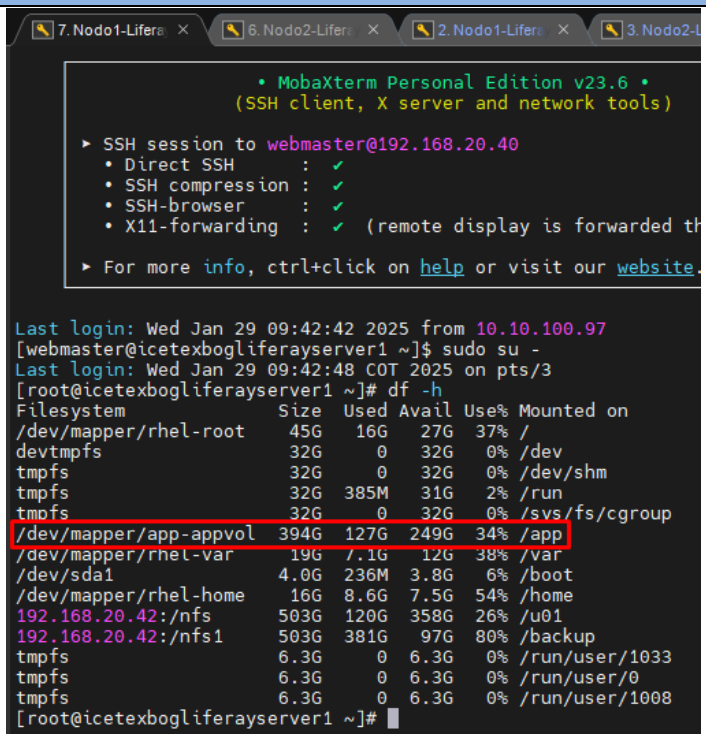
UNIDAD	HALLAZGO	OBSERVACIONES
		 Se trabaja en la compresión de los archivos logs (.xml y log por fecha) del nodo 2 para posteriormente copiarlos a la carpeta del servicio NFS **/nfs/nodo2logs/2024/** El paso siguiente, es programar reunión con el partner Claro para que apoyen con la eliminación de los logs del nodo 2 del portal ICETEX que comprende desde el 11 de diciembre de 2023 al 31 de diciembre de 2024.

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:

	Noviembre	Diciembre	Enero 2025
Usuarios mes	487000	676000	558000
Usuarios nuevos	263000	459000	373000
Tiempo acceso (seg)	147	146	137

Tabla 33 Distribución trimestral de acceso por usuarios

Durante el último trimestre, el portal web recibió un promedio de 573,667 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 enero, se observó una disminución del 17.5% en el número de usuarios que accedieron a la página. Esta caída representa aproximadamente 118,000 usuarios menos.

Durante el último trimestre, se ha observado que, en promedio, 365,000 nuevos usuarios accedieron a la página.

Sin embargo, es importante destacar una tendencia negativa en relación con los accesos nuevos en enero, la cifra de usuarios nuevos experimentó una disminución del 18.7%, lo que representa un total de 86,000 usuarios.

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

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

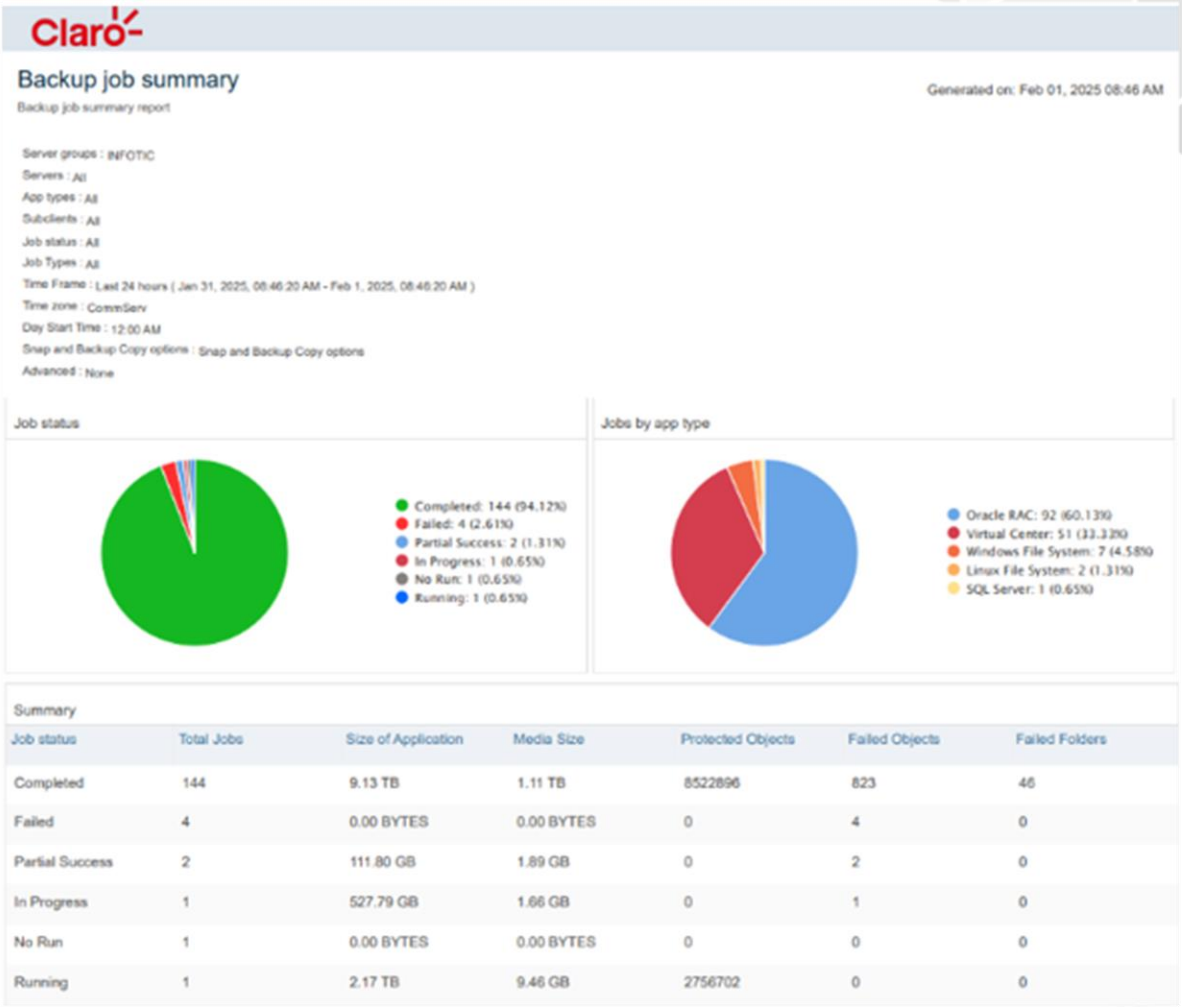
10.2.3. Backup Servidores Triara

Durante el periodo de enero 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 enero 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 enero el resultado de la ejecución de los Backups fue:



Claro

Backup job summary

Backup job summary report

Generated on: Feb 01, 2025 08:46 AM

Server groups : INFOTIC
Servers : All
App types : All
Subclients : All
Job status : All
Job Types : All
Time Frame : Last 24 hours (Jan 31, 2025, 08:46:20 AM - Feb 1, 2025, 08:46:20 AM)
Time zone : CommServ
Day Start Time : 12:00 AM
Snap and Backup Copy options : Snap and Backup Copy options
Advanced : None

Job status

Completed: 144 (94.12%)
Failed: 4 (2.61%)
Partial Success: 2 (1.31%)
In Progress: 1 (0.65%)
No Run: 1 (0.65%)
Running: 1 (0.65%)

Jobs by app type

Oracle RAC: 92 (60.13%)
Virtual Center: 51 (33.33%)
Windows File System: 7 (4.58%)
Linux File System: 2 (1.31%)
SQL Server: 1 (0.65%)

Summary

Job status	Total Jobs	Size of Application	Media Size	Protected Objects	Failed Objects	Failed Folders
Completed	144	9.13 TB	1.11 TB	8522896	823	46
Failed	4	0.00 BYTES	0.00 BYTES	0	4	0
Partial Success	2	111.80 GB	1.89 GB	0	2	0
In Progress	1	527.79 GB	1.66 GB	0	1	0
No Run	1	0.00 BYTES	0.00 BYTES	0	0	0
Running	1	2.17 TB	9.46 GB	2756702	0	0

Ilustración 42 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 enero corresponde a 336.69 TB, donde 97.89% se completó en el primer lanzamiento del robot con un total de 341.45 TB de información.

El 86.52%% 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	Noviembre	Diciembre	Enero 2025
Completado	97.07%	98.62%	97.89%
Fallido	1.79%	0.59%	0.78%
Cancelados	0.7%	0.5%	0.78%
Terminados parcialmente	0.29%	0.23%	0.47%
Completado con errores	0.1%	0.03%	0.04%

Tareas	Noviembre	Diciembre	Enero 2025
En Proceso	0.05%	0.03%	0.02%
Tamaño	**356.94 TB**	**562.01 TB**	**341.45 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 97.86%, donde el mes con mayor nivel de ejecución fue diciembre con 98.62%, el 2.09% 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 1.05%, el mes donde más se presentó un mayor porcentaje de fallas fue noviembre con el 1.79%

	Noviembre	Diciembre	Enero 2025
Oracle RAC	86.85%	93.36%	86.52%
Virtual Center	11.81%	5.51%	11.87%
Windows File System	1.86%	0.79%	1.47%
Linux File System	0.82%	0.22%	0.45%
SQL Server	0.15%	0.12%	0.18%

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 88.91% 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 Backups.

11. CONTROL DE CAMBIOS

Durante el mes de enero 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		

Tabla 36 Controles de cambio enero

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 iniciará la discusión sobre el tema en los comités de pares de seguridad que se reactivarán en febrero.
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	Está pendiente coordinar la sesión con los especialistas de ICETEX.
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	Se iniciará la discusión sobre el tema en los comités de pares de seguridad que se reactivarán en febrero.
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 requiere un ambiente pruebas. Está evaluando la parte financiera para proceder a solicitar la aprobación de ICETEX.
Actualización de Liferay de la versión 7.3 a la 7.4	INFOTIC - ICETEX	01-dic-24	28-mar-25	LIFERAY recomienda que primero se debe actualizar en todas las maquinas el sistema operativo y luego proceder con

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
				el cambio de versión. Apenas se realicen las pruebas se definirá la fecha de actualización.
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 programará una reunión con el operador CLARO para examinar la configuración proporcionada y asegurar el cumplimiento de la configuración de IPv6.(Febrero)
Traslado de los equipos de servicio de internet para la nueva sede de Arauca	INFOTIC - ICETEX	01-dic-24	28-feb-25	Se llevó a cabo la instalación de un canal provisional en enero, y el traslado al canal definitivo se efectuará en la primera semana de febrero.
Instalación del canal Backup de Quibdó	INFOTIC - ICETEX	01-dic-24	28-feb-25	La administración del centro comercial donde esta las instalaciones de ICETEX, dio la aprobación para ejecutar la instalación, se está coordinando con el grupo de CLARO.
Instalación del canal principal de Puerto Carreño	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se recibió la propuesta de CLARO y está en costeo por parte de INFOTIC .
Nueva configuración de SD WAN en triara	INFOTIC - ICETEX	01-dic-24	28-mar-25	CLARO está preparando la oferta comercial para el traslado de Aguas a Triara y la nueva configuración desde Triara.
Gestión de la administración Azure nube	INFOTIC -	01-dic-24	28-mar-25	Se coordinará la

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
	ICETEX			sesión con ICETEX para definir las acciones a implementar.
Políticas e inventarios de las creaciones en la nube	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se coordinará la sesión con ICETEX para definir las acciones a implementar.
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 notificando a ICETEX que no hay más Takedown disponibles, se espera respuesta de ICETEX.
Capacitación en seguridad al grupo de especialistas de seguridad del ICETEX	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se programará la capacitación una vez se tenga definido el grupo de seguridad y el tema de interés.
Monitoreo de los diferentes servicios realizados por el SOC. Revisión conjunta entre ICETEX – INFOTIC	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se iniciará la discusión sobre el tema en los comités de pares de seguridad que se reactivarán en febrero.
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 ***Fecha propuesta: Febrero***
Realizar mesa técnica entre ICETEX e INFOTIC para la revisión del alcance de Antivirus.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se iniciará la discusión sobre el tema en los comités de pares de seguridad que se reactivarán en febrero.
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	Se coordinará la sesión con los ingenieros de CLARO, INFOTIC e

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
				ICETEX para revisar y generar la solución ***Fecha propuesta: Febrero***
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 coordinará la sesión con los ingenieros de CLARO, INFOTIC e ICETEX para revisar y generar la solución ***Fecha propuesta: Febrero***
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	CLARO está preparando la oferta comercial ya se tiene la viabilidad en las direcciones enviadas.
Solicitud de Monitoreo de la LAN de todas las sedes	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se revisará la solicitud y enviará la respuesta al Icetex

Tabla 37 Planes de trabajo

Nota: Se extiende la fecha de finalización de la ejecución de los planes de trabajo, considerando que en el mes de enero aún no se dispone de los especialistas pares del ICETEX necesarios para llevar a cabo todas las sesiones de trabajo propuestas en el mes de diciembre.

13. RECOMENDACIONES DEL CONTRATISTA AL ICETEX

Las siguientes son las recomendaciones para el mes de enero 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

Solicitud de renovación del soporte de Liferay, que estuvo activo hasta el 31 de diciembre de 2024 y se prorrogó por garantía hasta el 31 de enero de 2025. Es imperativo actualizar el soporte para garantizar la colaboración del fabricante en varios procesos, tales como la obtención de nuevos instaladores, parches de seguridad, claves de licencia para el entorno productivo, así como para pruebas y desarrollo (localhost), y posteriormente 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: Luego del daño del equipo en la sede de San Andres, se informa a ICETEX que actualmente no hay disponibilidad de equipos adicionales para reemplazos futuros en caso de que surjan nuevos daños.

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

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

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 Symantec en las bases de datos sigue inactivo 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 329G.

13.5. Administrador de aplicaciones

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

- Las aplicaciones que estén en Framework .Net Classic que sean migradas a un Framework más actual y soporte vigente, en la actualidad los ambientes de pruebas cuentan con Framework actualizado, para que se validen la funcionalidad de las aplicaciones legadas.

- Que las aplicaciones que estén implementadas en sistemas operativos obsoletos sean migradas a Servidores con sistemas operativos de versiones actuales y con soporte de Microsoft.

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

13.6. Integrador Nube

- Recomendaciones en temas de costos (posibilidad de ahorro no aplicada en el año pasado y anteriores, también, conclusión de lo pagado anualmente vs haber adquirido las máquinas virtuales usadas como escritorio remoto como mejor alternativa).
- Configuraciones y malas prácticas permanentes (usuarios identificables por convención de la entidad nombre y apellido, hay usuarios que se conectan con cuentas administradoras de office 365 que al ser administradores hacen imposible su identificación dentro de la compañía).

- Recomendación para el correcto uso de la nube en la entidad, esto es, selección de aplicaciones productivas y de gran visibilidad en la nube para ahorrar esfuerzos en soportes, ventanas, configuraciones (entre otras dependencias) que implican los Datacenter o centros de datos en réplica resaltando el tiempo de respuesta y grado de afectación como papel principal.

- Recomendación de perfiles para el correcto uso de la nube y perfiles faltantes, esto es, perfiles responsables para monitoreos, configuraciones a máquinas virtuales, backups, escalamientos, entre otros actores en una nube que interactúan entre sí reorganizando y reduciendo dependencias manuales y horas hombre al memento de hallazgos.

- Falta de procedimientos y seguimiento a autorización de creación de recursos para detección de responsables, es difícil y a veces imposible encontrar la razón de la existencia de recursos encontrados, responsable o persona que lo autoriza, no hay una política ni formato claro donde se pueda auditar la creación de recursos para evitar sobrecostes.

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.

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

CIUDAD	Enlace - Tipo medio	INR	BW- Mínimo Requerido (MBPS)	Ancho de Banda actual	Ancho de Banda Ofrecido según Anexo 2.1
	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
	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

CIUDAD	Enlace - Tipo medio	INR	BW- Mínimo Requerido (MBPS)	Ancho de Banda actual	Ancho de Banda Ofrecido según Anexo 2.1
	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
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

CIUDAD	Enlace - Tipo medio	INR	BW- Mínimo Requerido (MBPS)	Ancho de Banda actual	Ancho de Banda Ofrecido según Anexo 2.1
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, está 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

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

16.4. Administrador de aplicaciones

- Se recomienda a los usuarios finales que a pesar de que se les da atención a todas las solicitudes, estas se deben gestionar a través de la mesa de servicio de Aranda, ya que todavía existen casos que se atienden sin haber un registro de estos.

- Las aplicaciones que estén en Framework .Net Classic que sean migradas a un Framework más actual y soporte.

- Que las aplicaciones que estén implementadas en sistemas operativos obsoletos sean migradas a Servidores con sistemas operativos de versiones actuales y con soporte de Microsoft.

- Se recomienda que cada aplicación web debe tener su respectivo servidor.

16.5. Integrador Nube

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

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

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

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.

17. ANEXOS

17.1. Almacenamiento

Backups Diarios:

- Backups diarios enero 2025 (31 reportes) Backup Diario

Informe de Backups:

- Consolidado mensual Backup enero Consolidado diario backup Enero 2025.pdf
- Informe Backup enero 2024 Informe Backups mes de enero 2025.pdf

17.2. Aplicaciones

- Informe actividades Módulos videoconferencia ICETEX enero 2025
  Informe actividades Módulos videoconferencia ICETEX Enero 2025.pdf
- Informe mensual Administrador de Soluciones enero 2025
  Informe Enero 2025 Administrador de Soluciones.pdf
- Informe mensual Administrador Web Master enero 2025
  Informe Enero 2025 Administrador Web Master.pdf
- Informe mensual Integrador Nube enero 2025
  Informe Enero 2025 Integrador Nube.pdf

17.3. Bases De Datos

- Informe de evidencias Dataguard Megacenter enero 2025
  INFOTIC_ICETEX - Evidencias Dataguard Megacenter Enero 2025.pdf
- Informe mensual Administrador de Bases de datos enero 2025
  Informe Enero 2025 Administrador base de datos.pdf

17.4. Ejecución Presupuestal

- Conciliación enero consolidado
  Conciliación Enero_consolidado.xlsx

- Consolidado informe mensual especialistas enero
  INFORME MENSUAL ENERO 2025.pdf

- Informe de Gestión Servicio enero 2025
Informe de Gestion Servicio Enero 2025.pdf

17.5. Seguridad

- Informe Mensual MARCA-OSINT ICETEX enero 2025
250201 Informe Mensual MARCA-OSINT ICETEX Enero 2025.pdf

- Informe Mensual Seguridad enero 2025
Reporte Mensual ICETEX_v2- ENERO.pdf

- Informe Mensual SOC - ICETEX enero 2025
250201 Informe Mensual SOC-TH ICETEX Enero 2025.pdf

- Informe técnico análisis de vulnerabilidades ICETEX enero 2025
INFORME TÉCNICO ANÁLISIS DE VULNERABILIDADES ICETEX Enero2025).pdf

- Reporte de IPS enero 2025
Reporte de IPS de Enero_infotic_2025.pdf

Reporte total ataques recibidos-SIEM:

- Denegados enero 1-15
Denegados enero 1-15.pdf

- Denegados enero 16-31
Denegados enero 16-31.pdf

17.6. Soporte Y Monitoreo

Canales

- ANS enero 2025 ANS_Enero_2025.xlsx

- Informe mensual Administrador de Networking enero 2025
Informe Enero 2025 Administrador Networking.pdf

- Informe Mensual Disponibilidad enero 2025
Reporte Mensual Disponibilidad INFOTIC Enero 2025.pdf

Graficas de consumo:

- Informe Mensual ALLOT enero 2025

Informe Mensual ALLOT Enero 2025.pdf

- Pruebas Nuevas de Saturación Canales enero 2025

Pruebas de Saturación Enero

17.7. Data center Alterno:

Replicación

- Informe mensual replicación enero 2025

Informe mensual replicacion Enero 2025.pdf

- Reportes diarios enero 2025 (26 reportes)

Replicaciones

17.8. Data Center Principal:

- Reporte Monitoreo ICETEX enero 2025-ELK

Reporte Monitoreo ICETEX Enero 2025-ELK.pdf

Revisión técnica

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