1. PERIODO DEL INFORME

PERÍODO A QUE CORRESPONDE EL INFORME	01-03-2025 31-03-2025

2. DATOS DEL SUPERVISOR

NOMBRE DEL SUPERVISOR	JUAN LEONARDO BERDELLA SIERRA Y VICTOR RAUL BAUTISTA GALINDO
DEPENDENCIA	Dirección de Tecnología
CARGO	Director de Tecnología y Coordinador de Infraestructura

3. DATOS DEL CONTRATO

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

4. SEGUIMIENTO GESTIÓN CONTRACTUAL = NO APLICA

El siguiente cuadro debe ser diligenciado solo para personas naturales:

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

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

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

5. PRODUCTOS ENTREGABLES = NO APLICA

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

OBSERVACIONES: (SI A ELLO HUBIERE LUGAR)

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

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___

SE ANEXA AL PRESENTE INFORME CERTIFICACIÓN PARA PAGO EN EL MES DE XXXX DE LA EJECUCIÓN CORRESPONDIENTE DE LOS SERVICIOS PRESTADOS EN EL PERIODO DEL MES DE xxxxx

Presenta informes de los servicios prestados en FEBRERO de 2025

No se genera pago en el periodo supervisado para los meses de enero y febrero de 2025, se adelanta conciliación de aplicación de ANS sobre los servicios prestados.

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

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

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

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

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

SI __X_____	NO _____	NO APLICA _____

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

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

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

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

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

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

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

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

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

OBSERVACIONES: (SI A ELLO HUBIERE LUGAR)

11. EJECUCIÓN PRESUPUESTAL

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

12. ANÁLISIS MATERIALIZACIÓN Y MITIGACIÓN DEL RIESGO:

¿DURANTE LA EJECUCIÓN SE MATERIALIZÓ ALGÚN RIESGO?

SI ☐ **NO** ☒

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

13. RECIBO A SATISFACCIÓN:

En el periodo supervisado no se genera pago por no concluir concertación de ANS para los meses de enero y febrero de 2025.

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** **JUAN LEONARDO BERDELLA SIERRA** **No. CC 1.064.990.615**
	FIRMA DEL SUPERVISOR **VICTOR RAUL BAUTISTA GALINDO** **No. CC. 79.352.968**

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

Al contestar cite Radicado 2025000145440-R Id: 5922838 Folios: 1 Fecha: 05-05-2025 09:55:07 Anexos: 1 Remitente: Destinatario:

5 de Mayo de 2025

PARA:

DE: - INFOTIC S.A

ASUNTO:

PDF DEL DOCUMENTO ELECTRÓNICO #FVE1812

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-1812

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 9:42:51 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 MARZO DE 2025. SERVICIOS OPERACIÓN MES DE MARZO DE 2025 (INCLUIDO IVA): $ 835.412.061 (-) DESCUENTOS INCLUIDO IVA: CONECTIVIDAD Y RED DE COMUNICACIONES: -$20.145.298 CENTRO DE DATOS: -$29.047,628 TOTAL DESCUENTO CON IVA: - $49.192.926 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	$ 660,688,349.00	$660,688,349.00	$ 786,219,135.00

IMPUESTOS	BASE	TASA	TOTAL
IVA	$660,688,349	19 %	$125,530,786

SETECIENTOS OCHENTA Y SEIS MILLONES DOSCIENTOS DIECINUEVE MIL CIENTO TREINTA Y CINCO PESOS M/CTE *****

Notas

facturacion_electronica@icetex.gov.co

RESPONSABLE: MONICA VILLAMIZAR

VALOR BRUTO	$660,688,349.00
DESCUENTO	$0.00
SUBTOTAL	$660,688,349.00
IVA	$125,530,786.00
TOTAL FACTURA	$786,219,135.00

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 99b054001c1c25523119a531c6d4c160d31c7aedce84e1f88ed3435ca14085363eca5096b3bdd6d2bdcd197d0fa84953

FIRMA DIGITAL:

PHLvDU5Wk5QxjArxWJYgnj8VAmAmHXSLW1xhNrJKq8oMG3j0Kfz1TMlNvtMM/Ry3VVMh5/tiwgQI7LbIHfjoL8oJUf3DB/gVTJVI3DfFcGGxkIizTY3SpWQYzSA+uulMyobEw+W/fxT7TYoR9NrJDTznvIHpDqJ9FoddPqBUZwSzqe/f6u5jpdfpXTu9LPDQgBNzfyaqMHoiD4B4i/bT5od//SnlBcCRmi/TlX1sgUqWTg4coBy0Gk+BRdjxuu7jdCiSJNS6kISpc/yXWDGPzs1UudNMz3jVaY2u9TO5d1yP4f+PrwDe0R5XTHqc206wTaUbd9IyPD6Zab9cTN17Dw==

FECHA DIAN: 2025-05-05 09:44:02-05:00

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

Marzo 01 al 31 de 2025

versión	*Observaciones*	*Fecha*	*Responsable*
1.0	Versión Inicial	02/04/2025	Francisco Pulido
1.1	Versión Final	30/04/2025	Maria Victoria Suárez

1. Introducción 8
2. Objetivo del Informe 8
3. Alcance 9
4. AVANCE TÉCNICO 10
4.1. Conectividad Y Red de Comunicaciones 10
4.1.1. Canales instalados en el mes y entregables 11
4.1.1.1. Solicitudes Nuevas Instalación de canales: 12
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 15
4.2.2. Centro de Datos Alterno 17
4.2.2.1. Hosting Virtual (IaaS) 17
4.2.2.2. Dataguard Bases de Datos Megacenter 19
4.2.2.3. Servicios de Housing – Datacenter Alterno 20
4.2.2.4. Servicios de DRP 20
4.3. Seguridad informática 20
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 26
4.3.2. Estadística de Portales 27
4.3.3. Servicio de centro de Operaciones de Seguridad (SOC) 28
4.3.3.1. Alertas o Incidentes de Seguridad Detectados 30
4.3.3.1.1. Categoría Seguridad 30
4.3.3.1.4. Threat Hunting 35

4.3.4. Análisis de Vulnerabilidades ICETEX 36
4.3.4.1. Resumen de Vulnerabilidades 37
4.3.4.2. Conclusiones Vulnerabilidades 38
4.3.5. REPORTE DE IPS 39
5. GESTION FISICA DE LA EJECUCIÓN 40
6. GESTION PRESUPUESTAL 41
7. GESTION ADMINISTRATIVA 42
8. Servicio De Colaboración 44
8.1. Disponibilidad del servicio – sedes Regionales 45
8.2. Disponibilidad del servicio – sedes Bogotá (aguas - ángel) 45
8.3. Gestión de incidencias y requerimientos – sedes regionales 46
8.4. Gestión de incidencias y requerimientos – Bogotá (Aguas - Angel) 47
9. GESTION DE RIESGOS Y PROBLEMAS 52
10. INDICADORES CLAVE DE DESEMPEÑO 54
10.1. ANS por Disponibilidad de canales de comunicaciones: 54
10.1.1. Canal de Replicación (Triara – Megacenter) 56
10.2. ANS por Disponibilidad de servidores: 56
10.2.1. Disponibilidad TRIARA para los servicios de página web 58
10.2.2. Análisis componente Liferay Producción 68
10.2.2. SERVICIO NFS – BACKUP DE NODOS 1 Y 2 DEL PORTAL ICETEX 70
10.2.3. Backup Servidores Triara 73
11. CONTROL DE CAMBIOS 76
12. PLAN DE TRABAJO DE LOS PROXIMOS MESES 76
14. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC 82
14.1. Aumento de la capacidad de Ancho de Banda en algunas de las sedes de la Entidad 82
14.2. Una capacitación al año de seguridad Informática y servicios conexos 84
14.3. TB de capacidad de almacenamiento 84
14.4. Se oferta Ítem de "Wifi" para la gente en 19 sedes 85
15. CONCLUSIONES 86
16. PENDIENTES 87
16.1. Administrador WEB MASTER 87

16.2. Administrador Networking *87*
16.3. Administrador Base de datos *87*
16.4. Administrador de aplicaciones *87*
16.5. Integrador Nube *88*
16.6. Seguridad *88*
17. ANEXOS *88*
17.1. Almacenamiento *88*
17.2. Aplicaciones *89*
17.3. Bases De Datos *89*
17.4. Ejecución Presupuestal *89*
17.5. Seguridad *89*
17.6. Soporte Y Monitoreo *90*
17.7. Data center Alterno: *90*
17.8. Data Center Principal: *91*

TABLA 1 IMPLEMENTACIÓN IP VERSIÓN 6 OFICINAS CON GATEWAY DE VOZ 11
TABLA 2 CASOS ATENDIDOS NETWORKING COMPARATIVO MES ANTERIOR 12
TABLA 3 CANALES PRUEBAS DE SATURACIÓN EJECUTADAS EN EL MES DE MARZO 2025 13
TABLA 4 CANALES PENDIENTES PRUEBAS DE SATURACIÓN 13
TABLA 5 CASOS DE ARANDA APLICACIONES 14
TABLA 6 SERVICIOS REPLICADOS – DATACENTER MEGACENTER 17
TABLA 7 TOP 05 MÁQUINAS MAYOR TASA DE TRANSFERENCIA 18
TABLA 8 TOP 05 MÁQUINAS MENOR TASA DE TRANSFERENCIA 18
TABLA 9 FECHAS CON MENOR REPLICACIÓN 18
TABLA 10 DISTRIBUCIÓN TRIMESTRAL DE REPLICACIÓN 19
TABLA 11 DISPONIBILIDAD DE SERVICIOS DE HOUSING – DATA CENTER ALTERNO 20
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 INVENTARIO DE DISPOSITIVOS 36
TABLA 16 GRUPO ESPECIALISTAS 40
TABLA 17 GRUPO ADMINISTRATIVO 40
TABLA 18 ALIADOS PARA EL PROYECTO 41
TABLA 19 EJECUCIÓN PRESUPUESTAL 42
TABLA 20 DISTRIBUCIÓN MÓDULOS DE VIDEOCONFERENCIA POR SEDE 44
TABLA 21 DISTRIBUCIÓN TRIMESTRAL DE REQUERIMIENTOS Y/O INCIDENTES 52
TABLA 22 NIVEL DE RIESGO 53
TABLA 23 GRADO DE RIESGO 54
TABLA 24 DISPONIBILIDAD DE CANALES 55
TABLA 25 DISPONIBILIDAD CANALES “INTERNET PARA LA GENTE” 56
TABLA 29 CÓDIGOS RELACIONADOS DISPONIBILIDAD SERVICIOS EN HOUSING – DATACENTER PRINCIPAL 57
TABLA 27 DISPOSITIVOS EN HOUSING – DATACENTER PRINCIPAL 57
TABLA 28 ACTUALIZACIÓN – ANÁLISIS COMPONENTE LIFERAY MARZO 70
TABLA 29 SERVICIO NFS– BACKUP DE NODOS 1 Y 2 DEL PORTAL ICETEX 72
TABLA 30 DISTRIBUCIÓN TRIMESTRAL DE ACCESO POR USUARIOS 72
TABLA 31 DISTRIBUCIÓN TRIMESTRAL DE BACKUP EJECUTADOS 75
TABLA 32 DISTRIBUCIÓN TRIMESTRAL DE BACKUP POR SERVICIOS 75
TABLA 33 CONTROLES DE CAMBIO MARZO 76
TABLA 34 PLANES DE TRABAJO 79
TABLA 35 CANALES ANCHOS DE BANDA ACTUALES VRS ANCHOS DE BANDA OFRECIDOS 84
TABLA 36 CAPACIDADES DE ALMACENAMIENTO CONTRATADO 85
TABLA 37 CAPACIDADES DE ALMACENAMIENTO APROVISIONADO 85
TABLA 38 WIFI PARA LA GENTE INSTALADOS 86
TABLA 39 WIFI PARA LA GENTE PENDIENTES 86

ILUSTRACIÓN 1 CASOS GESTIONADOS ARANDA APLICACIONES 14
ILUSTRACIÓN 2 DISPONIBILIDAD DE LAS BASES DE DATOS PRINCIPALES ICTXCYC Y APOTEOSY 15
ILUSTRACIÓN 3 CASOS DEL PROYECTO GESTIONADOS ARANDA BASES DE DATOS 16
ILUSTRACIÓN 4 REPORTES DE REPLICACIÓN SRM A SITIO ALTERNO – MARZO 2025 17
ILUSTRACIÓN 5 EVIDENCIA DATAGUARD REPLICADO A MEGACENTER BD 19
ILUSTRACIÓN 6 CONSUMO CANAL MPLS 22
ILUSTRACIÓN 7 CONSUMO CANAL INTERNET SEDES 22
ILUSTRACIÓN 8 CONSUMO CANAL INTERNET DATA CENTER 23
ILUSTRACIÓN 9 FILTRADO – WEB – (FORTIGATE – TRIARA) 23
ILUSTRACIÓN 10 INSPECCIÓN – SSL – (FORTIGATE – TRIARA) 24
ILUSTRACIÓN 11 ANTIVIRUS Y ANTIMALWARE – PERIMETRAL (FORTIGATE – TRIARA) 24
ILUSTRACIÓN 12 CONSUMO CANAL MPLS AGUAS 25
ILUSTRACIÓN 13 CONSUMO CANAL MPLS MEDELLÍN 25
ILUSTRACIÓN 14 CONFIGURACIÓN FORTIWEB 26
ILUSTRACIÓN 15 ESTADO SEGURIDAD SOPHOS 27
ILUSTRACIÓN 16 EVIDENCIA GRÁFICA ESTADÍSTICAS DE PORTALES 28
ILUSTRACIÓN 17 TOTAL DE ALERTAS DE SEGURIDAD 30
ILUSTRACIÓN 18 ATAQUES IPS PERMITIDOS 31
ILUSTRACIÓN 19 ATAQUES IPS DETECTADOS 32
ILUSTRACIÓN 20 PUERTOS ENTRANTES DE PÚBLICO A PRIVADO (PERMITIDOS) 32
ILUSTRACIÓN 21 PUERTOS SALIENTE DE PÚBLICO A PRIVADO (PERMITIDOS) 33
ILUSTRACIÓN 22 FALLOS DE INICIO DE SESIÓN WINDOWS 33
ILUSTRACIÓN 23 FALLOS DE INICIO DE SESIÓN LINUX 34
ILUSTRACIÓN 24 FALLOS DE INICIO DE SESIÓN DISPOSITIVOS DE RED 34
ILUSTRACIÓN 25 FALLOS DE INICIO DE SESIÓN VPN 35
ILUSTRACIÓN 26 CUENTAS BLOQUEADOS 35
ILUSTRACIÓN 27 CRONOGRAMA DE ACTIVIDADES. 37
ILUSTRACIÓN 28 CANTIDAD TOTAL DE HALLAZGOS IDENTIFICADOS 37
ILUSTRACIÓN 29 DISPONIBILIDAD DE SERVICIO VIDEOCONFERENCIA SEDES REGIONALES – MARZO 2025 45
ILUSTRACIÓN 30 DISPONIBILIDAD DE SERVICIO VIDEOCONFERENCIA SEDES BOGOTÁ – MARZO 2025 46
ILUSTRACIÓN 31 INCIDENTES / REQUERIMIENTOS SEDES REGIONALES – MARZO 2025 46
ILUSTRACIÓN 32 PRUEBA DE FUNCIONAMIENTO VISITA SEDE CHAPINERO – MARZO 2025 47
ILUSTRACIÓN 33 LIMPIEZA OPS SALA 6TO PISO – VISITA REVISIÓN MARZO 2025 48
ILUSTRACIÓN 34 EVIDENCIA MÓDULO FUNCIONAL SEDE AGUAS 65´´, PISO 4 - VISITA MARZO 2025 49
ILUSTRACIÓN 35 EVIDENCIA MÓDULO SEDE AGUAS 65”, PISO 2 – VISITA DE REVISIÓN MARZO 2025 50
ILUSTRACIÓN 36 EVIDENCIA MÓDULO SEDE ÁNGEL 65” – VISITA DE REVISIÓN MARZO 2025 51
ILUSTRACIÓN 37 MATRIZ DE RIESGOS 53
ILUSTRACIÓN 38 UPTIME – PORTAL WEB WEB.ICETEX.GOV.CO 58
ILUSTRACIÓN 39 MÉTRICA DE VISITANTES PORTAL WEB WEB.ICETEX.GOV.CO 58
ILUSTRACIÓN 40 MÉTRICA ADQUISICIÓN USUARIOS PORTAL WEB WEB.ICETEX.GOV.CO 59
ILUSTRACIÓN 41 MÉTRICA DE USUARIO POR PAÍS - PORTAL WEB WEB.ICETEX.GOV.CO 60
ILUSTRACIÓN 42 NODO 1 – VISTA GENERAL – INR0243 61
ILUSTRACIÓN 43 NODO 1 CPU 62
ILUSTRACIÓN 44 NODO 1 MEMORIA 63
ILUSTRACIÓN 45 NODO 1 ALMACENAMIENTO 64
ILUSTRACIÓN 46 NODO 2 – VISTA GENERAL – INR0242 64
ILUSTRACIÓN 47 NODO 2 CPU 65
ILUSTRACIÓN 48 NODO 2 MEMORIA SWAP 66
ILUSTRACIÓN 49 NODO 2 MEMORIA 67
ILUSTRACIÓN 50 NODO 2 ALMACENAMIENTO 67
ILUSTRACIÓN 51 EVIDENCIA BACKUP SERVIDORES RESUMEN BACKUPS Y SU ESTADO 74

RESUMEN EJECUTIVO

1. Introducción

Este informe contiene la información relacionada con las actividades ejecutadas por INFOTIC con ocasión de la celebración del contrato 2022-0792, durante el periodo comprendido entre el 01 al 31 de marzo de 2025. Para tal fin se cuenta con la información generada por el grupo de 9 especialistas y 3 profesionales administrativos con los cuales se soportan y garantizan la atención de servicios especializados descritos en el alcance del proyecto como son:

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

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

- Firma del Acta de Inicio suscrita el 30 de diciembre del 2022, con fecha de iniciación del 19 de enero del 2023. Cumplida al 100%.
- Fase de Transición. Que comprendió desde el 19 de enero hasta el 31 de marzo de 2023. Esta fase se encuentra cumplida al 100%.
- Fase de operación. Inició desde el 1 de abril de 2023, cuenta con un avance en la ejecución del 66 % que representa los 24 meses que lleva dentro de la fase de Operación el proyecto.

El presente informe, correspondiente al mes de marzo 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 marzo 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 marzo conforme a los frentes definidos por el ICETEX, así:

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

- **Centro de datos**
  El informe presenta el estado de los dos (2) Centros de Datos que contempla el proyecto ICETEX: un (01) centro de cómputo principal (TRIARA) y un (01) centro de cómputo secundario o 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 y nos encontramos en la gestión de la instalación de los canales pendientes.

Nos encontramos a la espera de los resultados del último escaneo de vulnerabilidades efectuado, con el fin de ajustar las acciones de remediación y/o mitigación que correspondan a INFOTIC.

Con respecto a la implementación de IPv6, se ha trabajado con nuestros especialistas de seguridad en las pruebas correspondientes. Asimismo, se ha avanzado en la documentación he entrega de informes conforme a los lineamientos periódicos de ICETEX.

En el presente mes se avanzó con la instalación del canal de Backup de la agencia de Quibdó culminándose la instalación de la UM de BK. Se encuentra pendiente, por parte del ICETEX, la Cross-conexión desde el cuarto de equipos del Centro Comercial hasta el cuarto de equipos de la agencia.

Dado que dicho cableado es responsabilidad de la administración del Centro Comercial en conjunto con ICETEX, se requiere que dicho la habilitación de los puntos de red deba concertarse entre ambas partes. Al respecto es necesario indicar que nuestra gerencia de servicios a remitido diferentes comunicaciones, vía correo electrónico, advirtiendo de esta situación.

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

Se han venido adelantando sesiones de seguimiento para la implementación de IPV6, avanzando en la configuración de las oficinas tal y como se evidencia en la siguiente tabla:

SEDE	Fecha
Quibdó	19/3/2025
Montería	25/3/2025
Pereira	27/3/2025
Cartagena	3/3/2025
Armenia	7/3/2025
Pasto	13/3/2025
Ibagué	13/3/2025

Tabla 1 Implementación IP Versión 6 oficinas con Gateway de Voz

Las sedes faltantes, por configurar las direcciones Ipv6, son Medellín, Bucaramanga, Valledupar, Santa Marta y Leticia.

Se ha incluido en numeral **12. Plan de trabajo de los próximos meses**. Las actividades planeadas en esta materia.

4.1.1. Canales instalados en el mes y entregables

El balance a la fecha, de los canales instalados es el siguiente:

- 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. En cuanto a los dos faltantes: uno corresponde al canal de Backup de la oficina ubicada en la ciudad de Quibdó, cuyo retraso es debido a temas administrativos del centro comercial en 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.

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 enlace:

https://icetex.sharepoint.com/:f:/r/sites/Infraestructura/Documentos%20compartidos/DATACENTER%20INFOTIC/Ejecucion%20INFOTIC/24_Marzo%202025/Soporte%20y%20Monitoreo/Canales?csf=1&web=1&e=I2VdDD

4.1.1.1. Solicitudes Nuevas Instalación de canales:

Se tiene las siguientes solicitudes de instalación de nuevos canales:

- (1) canal de datos principal para una nueva sede en la ciudad de Puerto Carreño -Vichada.
- (1) canal de datos principal para una nueva sede en la ciudad de Puerto Inírida-Guainía.
- (5) Servicios de Internet para la gente para las sedes de Manizales, Armenia, Cartagena, Sincelejo y Pasto, los cuales se encuentran en proceso de elaboración de la oferta comercial.

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

https://icetex.sharepoint.com/:x:/r/sites/Infraestructura/Documentos%20compartidos/NETWORKING%202023/casos%20aranda%20por%20mes/Registro%20Aranda%20Marzo%202025.xlsx?d=w351ab6d3774b49cea5155b56b4722076&csf=1&web=1&e=VfsUhW

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 se presentó una disminución considerable y los casos corresponden a eventos sobre los canales.

Mes	No. Casos
Febrero 2025	87
Marzo 2025	33

Tabla 2 Casos atendidos Networking comparativo mes anterior

4.1.2. Pruebas de Saturación Bidireccionales

Durante el mes de marzo se adelantaron las siguientes pruebas:

INR	ENLACE	SEDE	Fecha de Saturación	Pruebas de saturación
INR0036	BACKUP	AGUAS	05/03/2025	ok
INR0072	BACKUP	ARMENIA	05/03/2025	ok
INR0074	PRINCIPAL	ARMENIA	05/03/2025	ok
INR0273	BACKUP	ANGEL	28/3/2025	ok
INR0000320	PRINCIPAL	800M a 1000GB	15/03/2025	ok

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

La evidencia de estas pruebas puede ser consultada en el siguiente enlace:

https://teams.microsoft.com/l/message/19:2c5bbae4-e9d3-44fe-aef0-b97c3a37ce93_e0d71eba-2d3c-47f1-88b3-b33b53c0685c@unq.gbl.spaces/1743611640219?context=%7B%22contextType%22%3A%22chat%22%7D

A la fecha quedan pendientes de adelantar las siguientes pruebas:

INR	ENLACE	SEDE
INR0037	PRINCIPAL	AGUAS
INR0076	BACKUP	IBAGUE
INR0107	BACKUP	CARTAGENA

Tabla 4 Canales pendientes pruebas de saturación

En resumen, se ha alcanzado un 96% de pruebas de saturación hasta el 31 de marzo de 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 diecisiete (17) casos registrados en la herramienta de mesa de servicio Aranda, clasificados en las siguientes categorías:

Ilustración 1 Casos Gestionados Aranda Aplicaciones

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

#	Fecha	Actividad	Estado	Evidencias
1	03/03/2025	Tarea 517354 Requerimiento 17493 - Acceso al servidor de pruebas 10.1.18.65	Solucionado	Tarea 517354 Requerimiento 17493 - Acceso al servidor de pruebas 10.1.18.65.pdf
2	03/03/2025	Tarea 517355 Requerimiento 17494 - Acceso al servidor de pruebas 10.1.18.65	Solucionado	Tarea 517355 Requerimiento 17494 - Acceso al servidor de pruebas 10.1.18.65.pdf
3	03/03/2025	Tarea 517356 Requerimiento 17495 - Acceso al servidor de pruebas 10.1.18.65	Solucionado	Tarea 517356 Requerimiento 17495 - Acceso al servidor de pruebas 10.1.18.65.pdf
4	05/03/2025	Tarea 517638 Requerimiento 17523 - Acceso al servidor de pruebas 10.1.18.124	Solucionado	Tarea 517638 Requerimiento 17523 - Acceso al servidor de pruebas 10.1.18.124.pdf
5	05/03/2025	Incidente 83079 – Fallas Aplicación Servinpro por actualización de archivos jboss	Solucionado	Incidente 83079 – Fallas Aplicación Servinpro por actualización de archivos jboss.pdf
6	05/03/2025	Incidente 82878 – Falla en la Generación de Reportes Gestión crédito en Servidor MIRA y C&CTEX	Solucionado	Incidente 82878 – Falla en la Generación de Reportes Gestion Credito en Servidor MIRA y C&CTEX.pdf
7	06/03/2025	Incidente 83123 – Bloqueo de usuario en el servidor 10.1.18.29	Solucionado	Incidente 83123 – Bloqueo de usuario en el servidor 10.1.18.29.pdf
8	07/03/2025	Tarea 517792 Requerimiento 17530 - Acceso al servidor de pruebas 10.1.18.124	Solucionado	Tarea 517792 Requerimiento 17530 - Acceso al servidor de pruebas 10.1.18.124.pdf
9	07/03/2025	Tarea 517861 – Cambio 1132 – Despliegue Front WebsitePSE – Persona jurídica	Solucionado	Tarea 517861 – Cambio 1132 – Despliegue Front WebsitePSE – Persona Juridica.pdf
10	11/03/2025	Tarea 518116 Requerimiento 17622 - Acceso al servidor de pruebas 10.1.18.124	Solucionado	Tarea 518116 Requerimiento 17622 - Acceso al servidor de pruebas 10.1.18.124.pdf
11	14/03/2025	Requerimiento 101700 – Copia de archivo asp Aplicativo C&CTEX producción Internet	Solucionado	Requerimiento 101700 – Copia de archivo asp Aplicativo C&CTEX producción Internet.pdf
12	14/03/2025	Requerimiento 101702 – Verificación de URL y cadena de conexión Ambiente Preprod aplicación Cuentas Inactivas	Solucionado	Requerimiento 101702 – Verificación de URL y cadena de conexión Ambiente Preprod aplicación Cuentas Inactivas.pdf
13	18/03/2025	Tarea 518588 Requerimiento 17672 - Acceso al servidor de pruebas 10.1.18.65	Solucionado	Tarea 518588 Requerimiento 17672 - Acceso al servidor de pruebas 10.1.18.65.pdf
14	19/03/2025	Requerimiento 101795 – Activación de ServicioApiRestCore en el servidor 192.168.51.165	Solucionado	Requerimiento 101795 – Activación de ServicioApiRestCore en el servidor 192.168.51.165.pdf
15	19/03/2025	Tarea 518632 Requerimiento 17662 – Acceso de apineda al servidor de pruebas 10.1.18.65	Solucionado	Tarea 518632 Requerimiento 17662 – Acceso de apineda al servidor de pruebas 10.1.18.65.pdf
16	19/03/2025	Tarea 518794 Requerimiento 101829 - Actualiza Backend Cuentas Inactivas	Solucionado	Tarea 518794 Requerimiento 101829 - Actualiza Backend Cuentas Inactivas.pdf
17	25/03/2025	Tarea 518870 Cambio 17708 – Permisos FTP Usuarios crédito	Solucionado	Tarea 518870 Cambio 17708 – Permisos FTP Usuarios Credito.pdf

Tabla 5 casos de Aranda aplicaciones

Continuamos observando que los casos están vinculados al acceso a servicios mediante conexiones FTP. Asimismo, se reportaron errores en algunas aplicaciones críticas de Icetex y se llevaron a cabo tareas de modificación que resultaron en la actualización de archivos .dll en varios Web Services configurados en los servidores web IIS.

Durante el mes de marzo de 2025, se han llevado a cabo varias actividades adicionales, tales como:

1. DEPURACION LOGS SERVIDOR ICTXSRVNETCOR01 MARZO 18 DE 2025.pdf
2. Informe Falla de Correo por bloqueo de Spamhaus de la IP 186.84.155.234.pdf

4.2.1.2. Bases de Datos

- Se resolvieron 570 casos asignados a los administradores de base de dato en marzo de 2025 en los tiempos estipulados por prioridad.
- Los casos atendidos en el mes de marzo de 2025 aumentaron en un 25% más con respecto al mes de febrero de 2025.
- Se atendieron todas las reuniones solicitadas por el cliente durante el mes de marzo de 2025.
- Se actualizaron las bases de datos de replicación del DRP centro alterno.
- Se realizaron las copias solicitadas en producción y restauradas en pruebas para los diferentes schemas.

➢ La disponibilidad del Clusterware BD para el mes de MARZO 2025 fue del 100% como se evidencia en la siguiente ilustración:

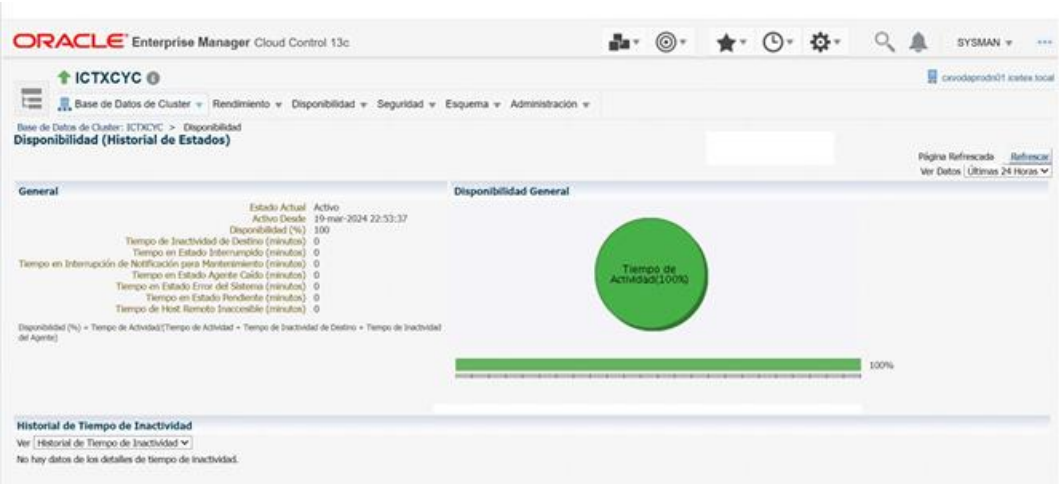


Ilustración 2 Disponibilidad de las Bases de Datos principales ICTXCYC y APOTEOSY

- 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 realizaron ajustes base de datos de SGDEA producción.
- Se generaron los logs de auditoria base de datos CORE.
- Se generaron restauraciones solicitadas con éxito
- Se ejecutaron los scripts solicitados satisfactoriamente
- Se realizó acompañamiento en despliegues de aplicaciones.

Casos del proyecto Gestionados por Bases de datos:

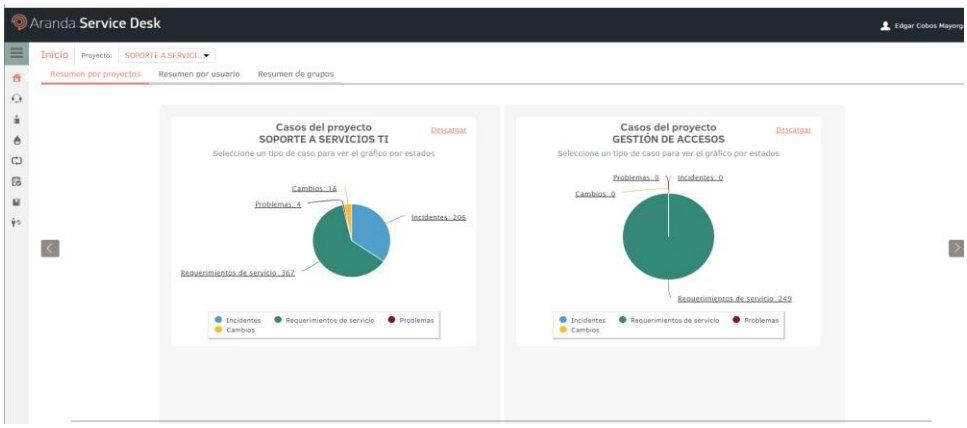


Ilustración 3 Casos del proyecto Gestionados Aranda Bases de datos

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 214 G.

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.

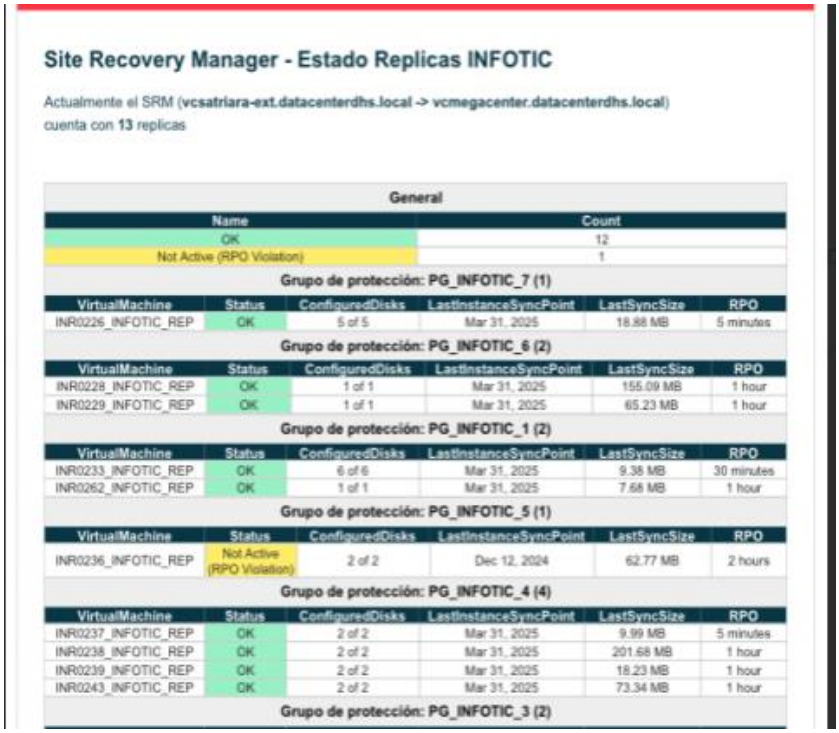
Permisos de usuarios en las bases de datos:

- 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.

4.2.2. Centro de Datos Alterno

4.2.2.1. Hosting Virtual (IaaS)

En el transcurso del mes de marzo, se mantuvo en constante replicación las máquinas virtuales configuradas, estos servidores se replicaron desde el origen en Triara hasta Megacenter usando la herramienta nativa de VMware, Site Recovery Manager (SRM) el detalle de las máquinas virtuales replicadas se puede evidenciar en el Informe mensual replicacion Marzo 2025.pdf, cuyo reporte refleja el consolidado de los informes mensuales y que se están entregando periódicamente, a continuación se puede ver el último reporte diario del mes.



Site Recovery Manager - Estado Replicas INFOTIC

Actualmente el SRM (**vcsatriara-ext.datacenterdhs.local -> vcmegacenter.datacenterdhs.local**) cuenta con **13** replicas

General

Name	Count
OK	12
Not Active (RPO Violation)	1

Grupo de protección: PG_INFOTIC_7 (1)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0226_INFOTIC_REP	OK	5 of 5	Mar 31, 2025	18.88 MB	5 minutes

Grupo de protección: PG_INFOTIC_6 (2)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0228_INFOTIC_REP	OK	1 of 1	Mar 31, 2025	155.09 MB	1 hour
INR0229_INFOTIC_REP	OK	1 of 1	Mar 31, 2025	65.23 MB	1 hour

Grupo de protección: PG_INFOTIC_1 (2)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0233_INFOTIC_REP	OK	6 of 6	Mar 31, 2025	9.38 MB	30 minutes
INR0262_INFOTIC_REP	OK	1 of 1	Mar 31, 2025	7.68 MB	1 hour

Grupo de protección: PG_INFOTIC_5 (1)

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

Grupo de protección: PG_INFOTIC_4 (4)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0237_INFOTIC_REP	OK	2 of 2	Mar 31, 2025	9.99 MB	5 minutes
INR0238_INFOTIC_REP	OK	2 of 2	Mar 31, 2025	201.68 MB	1 hour
INR0239_INFOTIC_REP	OK	2 of 2	Mar 31, 2025	18.23 MB	1 hour
INR0243_INFOTIC_REP	OK	2 of 2	Mar 31, 2025	73.34 MB	1 hour

Grupo de protección: PG_INFOTIC_3 (2)

Ilustración 4 Reportes de replicación SRM a Sitio Alterno – marzo 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
13	INR0208	ICTXBOGSRVPT1	Portal Transaccional	INR0236_INFOTIC_REP

Tabla 6 Servicios replicados – Datacenter Megacenter

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

- Durante el mes de marzo de 2025: se mantiene la alerta de **Not Active** en la maquina **INR0236_INFOTIC_REP** 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 llegaron los reportes de replicación para los días 17, 23, 24, 28 y 30 de marzo, este reporte es reemplazado con el siguiente reporte por lo que posteriormente no se puede reenviar; sin embargo, se llevó a cabo la replicación correspondiente.

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

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

Top	INR	HOST NAME	MB
1	INR0238	icetexbogliferaynfs	21724.39
2	INR0243	icetexbogliferayserver1	5273.17
3	INR0226	icetexbogwsmira	3839.85
4	INR0229	ictxsisgesapp	2877.68
5	INR0228	ictxsisgesbd	1651.14

Tabla 7 TOP 05 máquinas mayor tasa de transferencia

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

Top	INR	HOST NAME	MB
1	INR0249	icetexboglxxroad1	361.19
2	INR0233	icetexboglxorfeo1	279.18
3	INR0262	icetexboglxorfeo2	265.556
4	INR0237	icetexbogbalserver1	250.2
5	INR0245	icetexboglxdarumasrv2	122.96

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-mar	lunes	551.82
18-mar	martes	598.81
13-mar	jueves	662.75
31-mar	lunes	694.1
21-mar	viernes	697.11
26-mar	miércoles	705.65
16-mar	domingo	715.71
03-mar	lunes	745.29
09-mar	domingo	793.95
02-mar	domingo	1151.23

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 36361.8 MB y se presenta un aumento de 15% entre febrero y marzo, que equivale a 5096.26 MB.

Mes	MB replicadas
Marzo	38788.07
Febrero	33691.81
Enero	36605.64

Tabla 10 Distribución trimestral de replicación

4.2.2.2. Dataguard Bases de Datos Megacenter

Durante el mes de marzo 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 Marzo 2025.pdf

```
oracle@cxvodacontg011:~
[oracle@cxvodacontg011 ~]$ ps -fea|grep pmon
grid      8054     1  0  2024 ?        00:13:17 asm_pmon_+ASM
oracle    8605     1  0  2024 ?        00:33:41 ora_pmon_ICTXCYCD
oracle    9044     1  0  2024 ?        00:37:12 ora_pmon_ICETEXD
oracle    9531     1  0  2024 ?        00:20:52 ora_pmon_LIFERAYD
oracle   10396     1  0  2024 ?        00:37:21 ora_pmon_APOTEOSD
oracle   10746     1  0  2024 ?        00:37:25 ora_pmon_APOTNEWD
oracle   11132     1  0  2024 ?        00:20:51 ora_pmon_VIGIADTG
oracle   11573     1  0  2024 ?        00:20:52 ora_pmon_LANDICTD
oracle   12543     1  0  2024 ?        00:36:56 ora_pmon_APLICATD
oracle   16438 15868  0 20:00 pts/4    00:00:00 grep --color=auto pmon
[oracle@cxvodacontg011 ~]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.4.0 Production on Wed Apr 2 20:00:12 2025

Copyright (c) 1982, 2013, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production
With the Partitioning, Automatic Storage Management, OLAP, Data Mining
and Real Application Testing options

SQL> sta fapplyb.sql

    Thread Last Sequence Received Last Sequence Applied TIME_RECEIVED    TIME_APPLIED
---------- -------------------- -------------------- ---------------- ----------------
         1                78616                78616 31/03/2025 20:00 31/03/2025 20:00
         2                78603                78603 31/03/2025 20:00 31/03/2025 20:00

SQL>
```

Ilustración 5 Evidencia Dataguard replicado a Megacenter BD

Se generó la consulta de los archives recibidos y aplicados de la base de datos de ICTXCYCD a 31/03/2025 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 marzo al 100%:

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

Tabla 11 Disponibilidad de Servicios de Housing – Data Center Alterno

4.2.2.4. Servicios de DRP

Se continúan con las sesiones de trabajo semanales para la coordinación del primer DRP del 2025, el 11 de marzo se envió a ICETEX el minuto grama en el cual se requiere que se confirmen y/o actualicen los responsables de las actividades y, las eventuales observaciones al mismo.

Además, producto de las sesiones celebradas en el periodo de reporte, se tienen las siguientes definiciones:

1. Se realizará el DRP habilitando las máquinas virtuales en la herramienta de replicación, es decir no habría retorno de las máquinas virtuales de réplica (MEGACENTER) a las máquinas virtual de origen (TRIARA), esto con el fin de mantener la operación en el centro de datos principal activa durante la prueba del DRP.
2. Se modifica la fecha de ejecución del DRP para el 2 de junio del 2025
3. Reducir los tiempos de ejecución de la sesión del DRP.
4. Los miembros del grupo de trabajo de INFOTIC estarán de forma presencial en las instalaciones de ICETEX el día de la sesión del DRP
5. Desde INFOTIC se recomienda de las personas de Infraestructura y de riesgos de ICETEX estén de forma presencial en la ejecución del DRP.

El documento general con el Plan de Pruebas para el 2025 compartido por el Operador aliado se puede consultar en el Link: Plan de pruebas DRP INFOTIC_ICETEX-2025.pdf
El minuto grama remitido se relaciona en el link: CXXX_Minutograma_PruebaDRP_INFOTIC_ICETEX.xlsx

4.3. Seguridad informática

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

- se presentaron eventos de autenticación simultanea de 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.

- Se bloquearon servicios de scanner online que se estaban utilizando para esta actividad, 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 31 direcciones IPs maliciosas que intentaban conexiones desde distintos puertos a los servicios web de la entidad.

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

- Se corrigieron errores en el FortiSIEM a través de la actualización realizada el día 14 de marzo de 2025, donde se pasó de la versión 7.3.0 a la 7.3.1, esta actividad se hizo con el aval de la entidad y mediante el cambio en Aranda # 1134.

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 y configuraciones de segmentos sobre IPv6 de las sedes externas de la entidad por solicitud del área de Networking. En total se atendieron 39 casos de Aranda durante el mes de marzo los cuales se referencian en el ítem 12.2. Gestión de casos Operador de seguridad del Reporte Mensual ICETEX_v2- MARZO.pdf

Se han realizado acompañamientos para distintas actividades de diferentes áreas de la entidad, una de ellas tiene que ver con sesiones semanales para tratar un tema de fraude que se presentó sobre un desembolso realizado de manera fraudulenta. Debido a las limitaciones que tiene el SIEM actualmente, no fue posible obtener información de las bases de datos que fueron manipuladas para esta actividad, ya que este actualmente no se encuentra monitoreando ninguna de las bases de datos debido a falta de recursos del SIEM para asignarle este monitoreo.

4.3.1. Plataformas Administradas

Las plataformas administradas por INFOTIC tanto las de propiedad del ICETEX como las que se encuentran en modalidad de IaaS son las siguientes:

- 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 1200G [INR0185 CLARO(MPLS_DC)] durante el último mes., tal como se puede ver en la Ilustración 5.

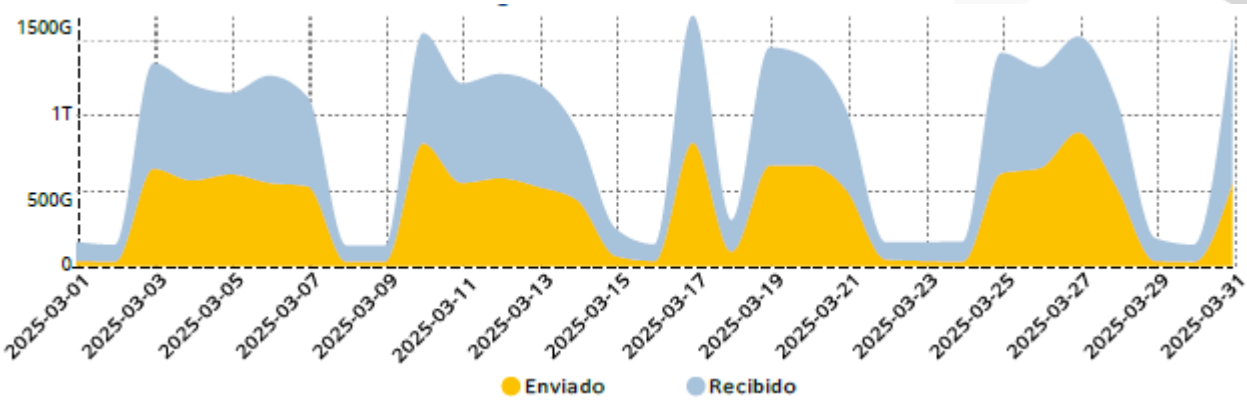


Ilustración 6 Consumo Canal MPLS

Se observa en la Ilustración 6, tráfico hacia la WAN-SEDES-ICETEX [INR0264 (INTE_SEDES_ICTX)] en promedio 1100G durante el último mes.

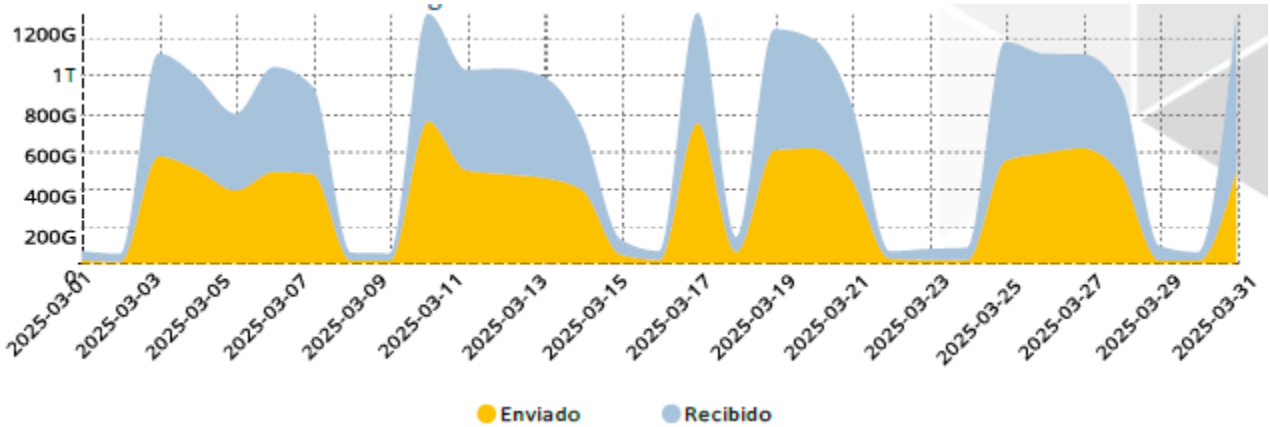


Ilustración 7 Consumo Canal Internet Sedes

En la Ilustración 7, se observa tráfico hacia la INTENET DATACENTER [INTERNET_DC_INR0000320 (Inet_claro)] en promedio 450G durante el último mes.

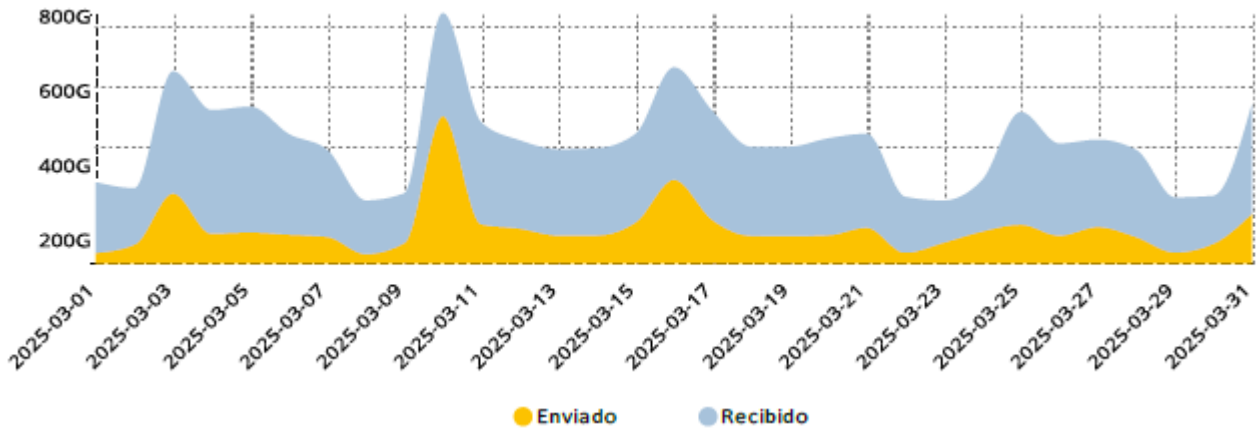


Ilustración 8 Consumo Canal Internet Data Center

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 WF-Avanzado	Perfil para FSSO Navegación Avanzada	30
WEB WF-VIP	Perfil para FSSO Navegación_VIP	15
WEB WF-General	Perfil para todos	5
WEB WF-Tesoreria	Perfil con restricciones especificas por auditoria.	4
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-Comunicaciones	Perfil para FSSO comunicaciones	2
WEB WF-General_Sedes	Perfil para todos	1
WEB WF-Sede_Ibague_YT	27022025/InfoTIC/Tarea Aranda 517214 (17458) Se solicita el acc...	1
WEB WF-wetransfer	Perfil para FSSO Navegación Avanzada	1
WEB wifi-default	Perfil de FULL acceso para pruebas	1

Ilustración 9 Filtrado – WEB – (FortiGate – Triara)

Name	Comments	Ref.
SSL certificate-inspection	Read-only SSL handshake inspection profile.	415
SSL no-inspection	Read-only profile that does no inspection.	218
SSL certificate-inspection_ICETEX	SSL para BUS de servicios	29
SSL Prueba certificate-inspection	Read-only SSL handshake inspection profile.	12
SSL certificate-inspection_2780	Read-only SSL handshake inspection profile.	1
SSL custom-deep-inspection	Customizable deep inspection profile.	0
SSL deep-inspection	Read-only deep inspection profile.	0

Ilustración 10 Inspección – SSL – (FortiGate – Triara)

Name	Comments	Ref.
AV AV-FSB	HTTP,SMTP FULL FSB	67
AV ICETEX		63
AV prueba2		60
AV default	ALL con FSB	43
AV AV-HTTP	HTTP con FSB	26
AV AV-HTTP&CIFS	HTTP,CIFS con FSB	4
AV AV-SMTP	SMTP FULL FSB	1
AV wifi-default	ALL monitoreo sin FSB	1

Ilustración 11 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 7.4.7, 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 en la Ilustración 11 el tráfico hacia la MPLS de la sede de Aguas con un promedio de 800G (Port7) en el último mes.

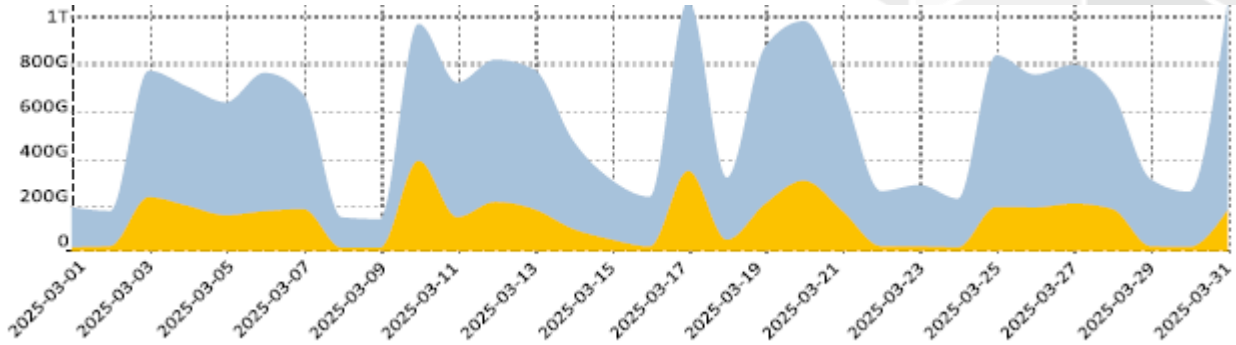


Ilustración 12 Consumo Canal MPLS Aguas

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.

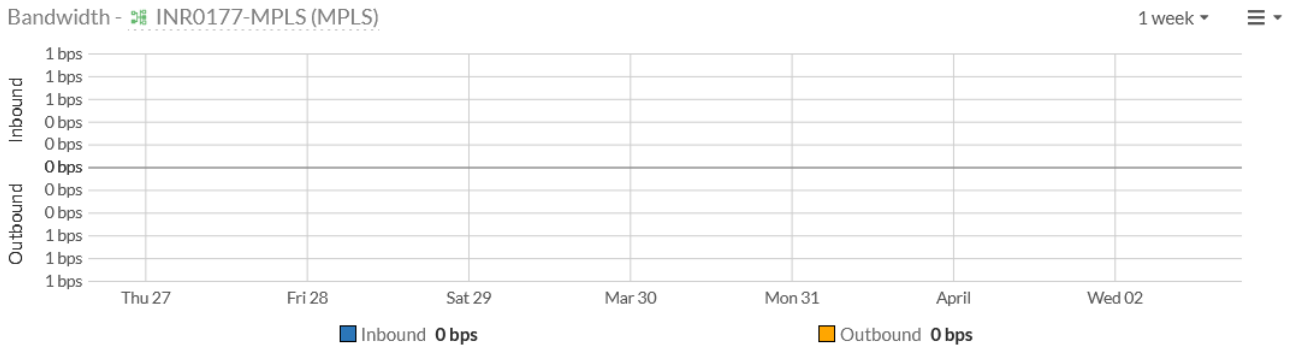


Ilustración 13 Consumo Canal MPLS Medellín

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.

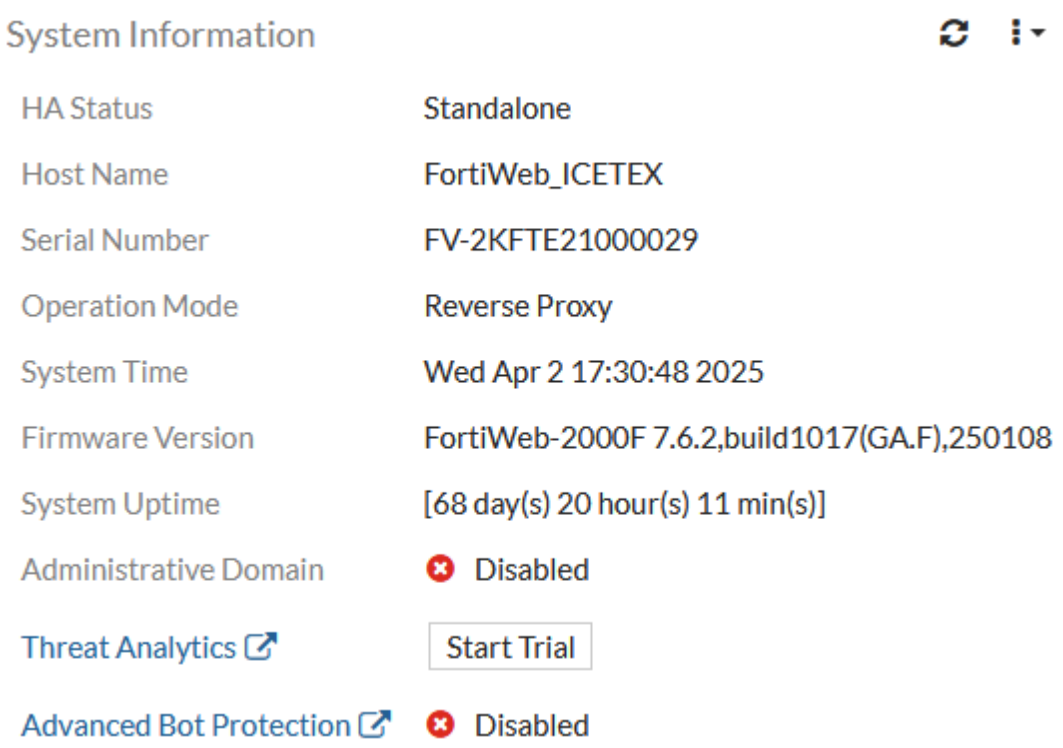


Ilustración 14 Configuración FortiWeb

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.

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

Ilustración 15 Estado Seguridad Sophos

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 marzo, se inició la revisión por parte del ICETEX e INFOTIC estos temas pendientes.

4.3.2. Estadística de Portales

Durante el mes de marzo se continuo con el monitoreo permanente a los portales sobre los que opera el ICETEX, manteniendo, las alertas y reportes a tiempo en caso de que se presentara algún evento que pudiera ocasionar una interrupción en la prestación de los servicios que se ofrecen a través de los portales, este informe se encuentra detallado en el documento Reporte Mensual ICETEX_v2- MARZO.pdf

Como se puede ver en la Ilustración 15, en el mes de marzo, se presenta un promedio de 1200GB de tráfico general hacia los portales protegidos por el FortiWeb donde el portal de web.icetex.gov.co y 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.

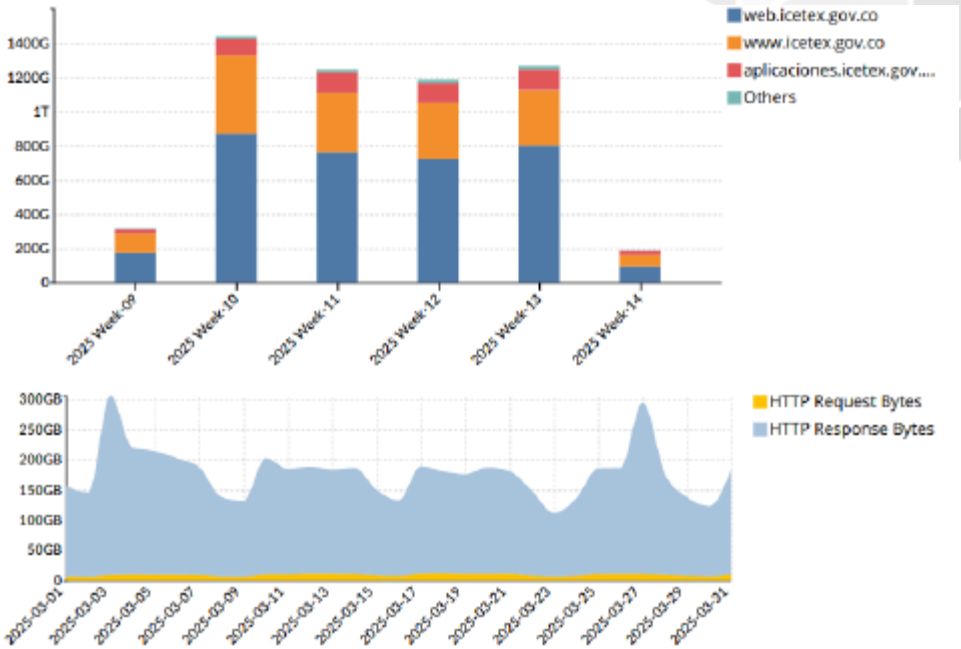


Ilustración 16 Evidencia Gráfica Estadísticas de Portales

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

#	HTTP Host	HTTP Request Bytes	HTTP Response Bytes
1	web.icetex.gov.co	225.30 GB	3.10 TB
2	www.icetex.gov.co	27.70 GB	1.50 TB
3	aplicaciones.icetex.gov.co	22.72 GB	460.23 GB
4	portal.icetex.gov.co	2.14 GB	59.03 GB
5	comunidad.icetex.gov.co	246.24 MB	14.86 GB
6	identidad.icetex.gov.co	17.69 MB	189.29 MB
7	186.84.73.158	482.15 KB	101.63 MB
8	comunidad.icetex.gov.co:443	500.11 KB	96.74 MB
9	(186.84.73.154) web.icetex.gov.co	784.05 KB	95.37 MB
10	web.icetex.gov.co:443	1.74 MB	91.68 MB

Tabla 12 Top 10 de los Portales más utilizados

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

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

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

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):

Un indicador de compromiso puede venir dado bajo la forma de un nombre de archivo, el nombre de un proceso en el administrador de tareas, una URL o dirección IP, comportamiento anómalo en el tráfico web, intentos de inicio de sesión fallidos, entre otros tantos más.

Los siguientes indicadores son colectados por los Analistas del SOC, a través de convenios con el FISRT, con otros CSIRT, e Inteligencia y Caza Amenazas.

Indicadores de compromiso (IOC)	Marzo 2025	Febrero 2025	Enero 2025
IOC – Malware DOMINIOS	3.919	3.919	3.919
IOC – Malware IPs	8.483	5.278	5.278
IOC – Malware HASH	1.621	1.612	1.612
IOC – Malware URL	780	780	780

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 250401 Informe Mensual SOC-TH ICETEX Marzo 2025.pdf se ven las alertas generadas a lo largo del periodo monitoreado, dichas alertas se clasifican en 3 categorías principales de monitoreo, las cuales corresponden a Seguridad, Disponibilidad y Rendimiento, a partir de este informe se presenta un resumen de las alertas de seguridad y se incluye amenazas cibernéticas, sin embargo, el detalle del tratamiento que se realizó a cada uno de los casos se debe revisar en el Informe mencionado anteriormente.

4.3.3.1.1. Categoría Seguridad

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

Severity	Cantidad de ...
Medium	15,590
High	3,630
Low	266

Ilustración 17 Total de alertas de seguridad

Durante el período evaluado se presentaron 3630 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 marzo 2025	Alertas de Seguridad febrero 2025	Alertas de Seguridad enero 2025
High	3630	2557	352
Medium	15590	36881	22668
Low	266	380	256

Tabla 14 comparativo Alertas de Seguridad

En el mes de marzo con respecto al mes anterior:

- Las amenazas de seguridad de severidad “Alta” aumentaron en un 42%
- Las amenazas de seguridad de severidad “Media” disminuyeron en un 58%
- Las amenazas de seguridad de severidad “Baja” disminuyeron en un 30%

El tráfico malicioso fue bloqueado, sin embargo, se recomienda la verificación de los equipos origen con el fin de descartar presencia de malware.

4.3.3.1.2. Amenazas de Ciberseguridad

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

- **Top Ataques IPS:** Se representa el Top 10 de los ataques IPS permitidos y denegados detectados por los dispositivos de ciberseguridad perimetral.

3.1.1 FortiGate: Top IPS Ataques Permitidos - WX 16:23

Attack Name	Severity	Source IP	Firewall Action	Informational URL	COUNT(Matc...
Apache.Optionsbleed.Scanner	High	31 10.1.24.49	detected	http://www.fortinet.com/ids/VID44633	2
GitLab.CE.EE.lint.include_merged_ya...	High	85.215.61.232	detected	http://www.fortinet.com/ids/VID57484	1
ToolTalk.ttdbserverd.Access	High	90 10.10.100.33	detected	http://www.fortinet.com/ids/VID12139	1
ToolTalk.ttdbserverd.Access	High	90 10.10.100.147	detected	http://www.fortinet.com/ids/VID12139	1
VMware.vCenter.CVE-2021-21985.Re...	High	85.215.61.232	detected	http://www.fortinet.com/ids/VID50443	1
SSL.Anonymous.Ciphers.Negotiation	Low	192.168.19.122	detected	http://www.fortinet.com/ids/VID43544	220
Port.Scanning	Low	90 10.10.100.33	detected	http://www.fortinet.com/ids/VID43814	29
Port.Scanning	Low	90 10.10.100.147	detected	http://www.fortinet.com/ids/VID43814	25
TCP.Split.Handshake	Medium	41 10.1.6.33	detected	http://www.fortinet.com/ids/VID26339	12
TCP.Split.Handshake	Medium	54 10.1.1.57	detected	http://www.fortinet.com/ids/VID26339	4
TCP.Split.Handshake	Medium	31 10.1.2.3	detected	http://www.fortinet.com/ids/VID26339	4
TCP.Split.Handshake	Medium	47 10.1.6.25	detected	http://www.fortinet.com/ids/VID26339	4
TCP.Split.Handshake	Medium	70 172.16.224.64	detected	http://www.fortinet.com/ids/VID26339	4
TCP.Split.Handshake	Medium	10.1.2.2	detected	http://www.fortinet.com/ids/VID26339	3
TCP.Split.Handshake	Medium	10.1.2.26	detected	http://www.fortinet.com/ids/VID26339	3

Ilustración 18 ataques IPS permitidos

3.1.1 FortiGate: Top IPS Ataques Denegados - WX 16:23

Attack Name	Severity	Source IP	Firewall Action	Informational URL	COUNT(Matc...
Generic.Path.Traversal.Detection	Medium	90 10.10.100.147	dropped	http://www.fortinet.com/ids/VID56270	2,582
Generic.Path.Traversal.Detection	Medium	90 10.10.100.33	dropped	http://www.fortinet.com/ids/VID56270	2,019
Nessus.Scanner	Medium	90 10.10.100.147	dropped	http://www.fortinet.com/ids/VID47971	2,016
Nessus.Scanner	Medium	90 10.10.100.33	dropped	http://www.fortinet.com/ids/VID47971	1,734
Web.Server.Password.File.Access	Medium	90 10.10.100.147	dropped	http://www.fortinet.com/ids/VID43336	1,352
Apache.Log4j.Error.Log.Remote.Code....	Medium	90 10.10.100.147	dropped	http://www.fortinet.com/ids/VID51006	1,312
Apache.Log4j.Error.Log.Remote.Code....	Medium	90 10.10.100.33	dropped	http://www.fortinet.com/ids/VID51006	1,138
Web.Server.Password.File.Access	Medium	90 10.10.100.33	dropped	http://www.fortinet.com/ids/VID43336	917
Atlassian.Confluence.CVE-2021-26084...	Medium	64.188.99.192	dropped	http://www.fortinet.com/ids/VID50727	580
HTTP.URI.SQL.Injection	Medium	90 10.10.100.147	dropped	http://www.fortinet.com/ids/VID15621	461
MS.IIS.Web.Server.Path.Traversal	Medium	90 10.10.100.147	dropped	http://www.fortinet.com/ids/VID12015	301
MS.IIS.Web.Server.Path.Traversal	Medium	90 10.10.100.33	dropped	http://www.fortinet.com/ids/VID12015	291
Cross.Site.Scripting	Medium	90 10.10.100.147	dropped	http://www.fortinet.com/ids/VID17702	249
HTTP.URI.SQL.Injection	Medium	90 10.10.100.33	dropped	http://www.fortinet.com/ids/VID15621	232
ALFA.TEaM.Web.Shell	Medium	165.22.107.189	dropped	http://www.fortinet.com/ids/VID53229	228

Ilustración 19 ataques IPS detectados

- **Top Perímetro:** Principales Puertos Entrantes por Conexiones (Trafico Permitido).

Protocolo	Puerto Destino Privado	Cantidad Eventos
	443	93,431,289
HTTPS	443	4,880,503
HTTP	80	80,651
icmp/8/0	0	36,504
TCP/440	440	18,134
TCP/458	458	16,083
DNS	53	5,040
TCP/450	450	3,041
TCP/448	448	2,194
UDP-High_Ports	8014	635
Web Access	80	128
SSH	22	1
Snmp-Read-Only	39657	1
Snmp-Read-Only	40409	1
Snmp-Read-Only	51168	1
Snmp-Read-Only	55828	1
Snmp-Read-Only	55940	1
Snmp-Read-Only	56843	1
Snmp-Read-Only	58367	1
Snmp-Read-Only	59996	1

Ilustración 20 Puertos entrantes de público a privado (Permitidos)

Principales Puertos Salientes por Conexiones (Trafico Permitido)

Protocolo	Puerto Destino publi...	Cantidad Eventos
HTTPS	443	91,926,642
SSL	443	87,363,436
DNS	53	23,355,411
HTTP	80	21,895,752
Microsoft-Azure	443	19,969,281
Microsoft-Office365	443	19,012,805
Google-Web	443	11,604,622
Microsoft-Office365.Published	443	9,490,971
Google-DNS	53	8,968,001
Microsoft-Outlook	443	8,243,457
UDP_443	443	7,203,529
SSH	990	6,290,517
Amazon-AWS.EC2	443	6,242,844
Snmp-Read-Only	443	5,434,852
Microsoft-Azure	990	5,307,479
Amazon-AWS	443	5,255,787
Akamai-CDN	443	4,813,677
Amazon-AWS.EC2	80	3,690,218
Microsoft-Teams.Published.Worldwide.Allow	443	3,270,485
Microsoft-Microsoft.Update	443	2,733,698

Ilustración 21 Puertos saliente de público a privado (Permitidos)

Top de Accesos Fallidos

Failed Windows Login 8:52

Source IP	User	Server	COUNT(Matc...
10.1.2.13	gbernal	90 ictxsrvfs.ice...	12,284
10.10.100.117	4 wherrerab	90 ictxsrvfs.ice...	10,996
10.10.100.130	JUAN PABLO	90 ictxsrvfs.ice...	3,430
90 10.1.2.4	gbernal	90 ictxsrvfs.ice...	3,074
73 10.1.2.36	gbernal	90 ictxsrvfs.ice...	3,025
172.22.1.27	ibohorquezs	90 ictxsrvfs.ice...	2,963
10.10.100.27	20 lorduz	90 ictxsrvfs.ice...	2,450
10.1.8.3	Jrojas	90 ictxsrvfs.ice...	2,391
10.10.100.113	lrincon	90 ictxsrvfs.ice...	2,387
10.10.100.111	gbernal	90 ictxsrvfs.ice...	2,326

Ilustración 22 Fallos de Inicio de sesión Windows

Failed Unix Login 17:20

No data

Ilustración 23 Fallos de Inicio de sesión Linux

Failed Network Login 17:39

Source IP	User	Reporting Device	COUNT(Matc...
42 192.1.1.15	FortiAnalyzerUser	42 DC_FG_MST_ICE...	205
172.16.224.148	ymartinezf	77 DCAGUAS_FG_MS...	8
172.16.224.233	atiuso	77 DCAGUAS_FG_MS...	8
172.22.1.27	ibohorquezs	77 DCAGUAS_FG_MS...	7
172.16.224.153	dherrerato	77 DCAGUAS_FG_MS...	5
36 172.16.224.170	msuarezo	77 DCAGUAS_FG_MS...	5
172.16.224.174	dblancoj	77 DCAGUAS_FG_MS...	5
172.16.224.188	ognecco	77 DCAGUAS_FG_MS...	5
172.16.225.20	nbeltranc	77 DCAGUAS_FG_MS...	5
2 172.16.224.79	yalfonsos	77 DCAGUAS_FG_MS...	4

Ilustración 24 Fallos de Inicio de sesión Dispositivos de red

Failed VPN Login 17:25

Reporting IP	User	COUNT(Matc...
42 192.1.1.15	****0632	1
42 192.1.1.15	+57	1
42 192.1.1.15	+573023012347	1
42 192.1.1.15	+573104800472	1
42 192.1.1.15	+573115519367	1
42 192.1.1.15	..__.mag889gbe	1
42 192.1.1.15	._..ICsGpa	1
42 192.1.1.15	00000109690	1
42 192.1.1.15	0001302872	1
42 192.1.1.15	0002233770	1

Ilustración 25 Fallos de Inicio de sesión VPN

Account Lockout 8:35

Server	User	COUNT(Matc...
85 ictxsrvfs.icetex.local	Soporte	5

Ilustración 26 Cuentas bloqueados

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), se puede ampliar la información en el reporte del SOC en el link: 250401 Informe Mensual SOC-TH ICETEX Marzo 2025.pdf

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

El objetivo fundamental es detectar y mitigar posibles amenazas antes de que se materialice un incidente de

seguridad. Los resultados obtenidos durante el periodo de monitoreo con relación al tráfico detectado proveniente de la entidad en interacción con estos actores maliciosos y se relacionan en el informe mensual del SOC en el link: Reporte Mensual ICETEX_v2- MARZO.pdf

4.3.4. Análisis de Vulnerabilidades ICETEX

Durante la Fase 4 del análisis de vulnerabilidades se mantuvo una cobertura del 100% sobre los activos tecnológicos, permitiendo una validación individual de cada hallazgo con su respectiva evidencia.

Se eliminaron dos falsos positivos: **CGI Generic XSS (HTTP Headers)** y **Spring4Shell (CVE-2022-22965)**, al comprobarse que no representaban riesgo real.

A pesar de los avances en la desactivación de **TLS 1.0/1.1** y mejoras en cifrados, persisten vulnerabilidades críticas sin gestionar.

Se identificó un alto grado de **obsolescencia tecnológica**, con versiones sin soporte de **SQL Server, Apache Tomcat, Oracle, sistemas operativos Windows, PHP y VMware**, lo cual representa un riesgo significativo.

También se detectó el uso de **criptografía débil** en protocolos como **SSLv2 y SSLv3**, y configuraciones inseguras en servicios como **SSH, SSL y SMB**, lo que mantiene el entorno con un **nivel de riesgo alto**.

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 15 Inventario de dispositivos

Como parte de la gestión realizada a nivel de análisis de vulnerabilidades, para el presente informe y de acuerdo con el cronograma general, se menciona el rango de tiempo de ejecución de las diferentes pruebas, esto basado en la metodología propuesta, y a su vez, con el alcance de dispositivos que fueron objeto de análisis.

A nivel técnico se detallan las siguientes actividades:

INFOTIC SOLUCIONES INTELIGENTES / ICETEX	Cronograma detallado ejecución de pruebas de análisis de vulnerabilidades				Versión: 1	
			Fecha de Inicio del Proyecto	lunes, 03/07/2023		
Actividad	**Responsable**	**Cumplimiento**	**Fecha de inicio**	**Fecha Final**	**Dias**	**Franja horaria**
Ejecución 4 - 100% RETEST		**100%**	1/11/2024	04/04/2025	135	8:00 AM - 12:00M
Mes 20 - Marzo 2025	Wexler	**100%**	1/03/2025	31/03/2025	30	8:00 AM - 12:00M
Pruebas de conectividad a los objetivos - Fase de reconocimiento.	Wexler	**100%**	2/03/2025	14/03/2025	10	8:00 AM - 12:00M
Identificación de dispositivos- Fase enumeración	Wexler	**100%**	14/03/2025	25/03/2025	7	8:00 AM - 12:00M
Identificación de vulnerabilidades - Fase de escaneo	Wexler	**100%**	14/03/2025	25/03/2025	7	8:00 AM - 12:00M
Elaboración de informes - Fase de documentación	Wexler	**100%**	25/03/2025	04/04/2025	8	8:00 AM - 12:00M

Ilustración 27 Cronograma de actividades.

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 AV_ABR_RETEST4_2025.pdf

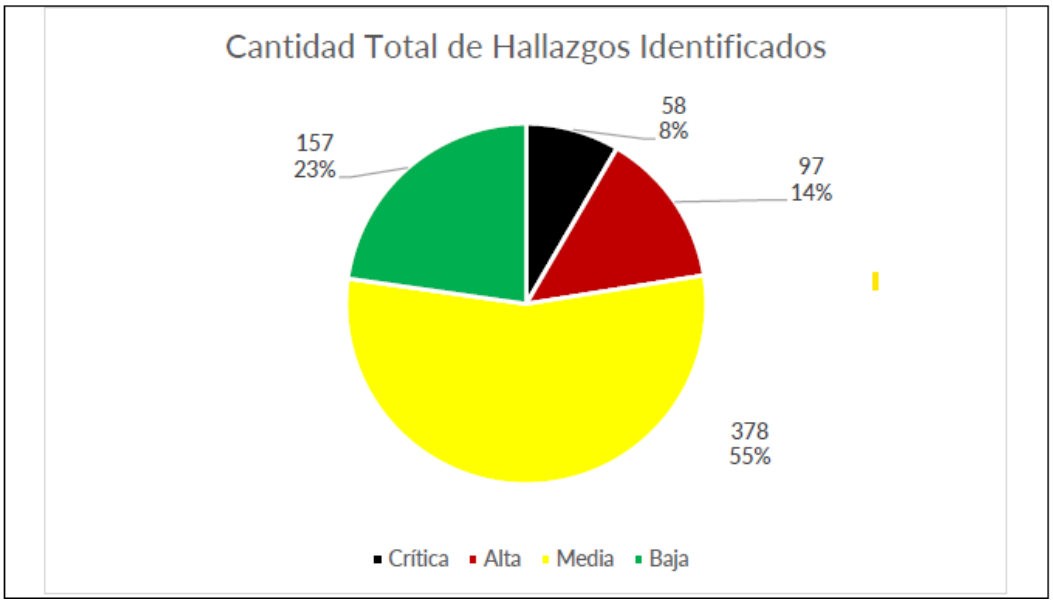


Ilustración 28 Cantidad Total de Hallazgos identificados

4.3.4.1. Resumen de Vulnerabilidades

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 sugiere realizar una mesa técnica entre ICETEX e INFOTIC para revisar las alternativas de solución frente a la gestión de vulnerabilidades.

El resumen de las vulnerabilidades se puede revisar a más detalle en el numeral 11. Resumen de vulnerabilidades del INFORME TÉCNICO AV_ABR_RETEST4_2025.pdf

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:**
- 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 Reporte_de_IPS_de_Marzo_infotic_2025.pdf se observa que desde la dirección IP 85.215.61.232 se están llevando a cabo ataques al API de Aranda, el cual está expuesto a través del puerto 80. Es especialmente preocupante la firma VMware.vCenter.CVE-2021-21985.Remote.Code.Execution (https://www.fortiguard.com/encyclopedia/ips/50443), ya que permite la ejecución remota de código en entornos VMware. Debido a los riesgos que esto conlleva, se recomienda mantener activo el servicio solo por geolocalización en las áreas donde se va a utilizar y bloquear este tipo de firmas de seguridad para mitigar posibles amenazas.

Se ha observado que desde las redes internas se están realizando escaneos, cifrado y intentos de accesos no autorizados a los usuarios mediante el protocolo RPC. En consecuencia, el área de seguridad está llevando a cabo una validación de firmas de seguridad, tales como: SSL.Anonymous.Ciphers.Negotiation, Apache.Camel.XSLT.Component.XXE, ToolTalk.ttdbserverd.Access, entre otras. El objetivo es mitigar los riesgos identificados sin afectar los servicios de la entidad.

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.

Se recomienda que el ICETEX delegue a un responsable para temas de nube, con quien se puedan coordinar las labores de escalamientos internos y toma de decisiones, dado que, a la fecha de presentación de este informe,

no contamos con este interlocutor.

Con el fin de elaborar recomendaciones de migración a la nube se requiere, por parte del ICETEX, del inventario de aplicaciones y máquinas virtuales que se planean migrar a la nube con el fin de efectuar un análisis y proceder a proponer alternativas tendientes a optimizar los 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 marzo del 2025 del proyecto, se encuentra en la fase de operación de los servicios contemplados en el alcance llevando ejecutados 24 meses que equivale al 66% 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 marzo del 2025:

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

Tabla 16 Grupo especialistas

El siguiente es el grupo administrativo que estuvo en el desarrollo de la operación del mes de marzo 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 17 Grupo Administrativo

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

marzo del 2025:

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

Tabla 18 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	$ 2,298,991,138	$480,000,000	$0	$8,167,341,148.11

CONCEPTO						***VALOR***
VALOR TOTAL DEL CONTRATO						***$ 31,398,996,857.96***
VALOR PAGADO						$ 14,441,737,171.00
Pago No. 1 -	mes:	Abril	de	2023	$ 537.090.736,00	
Pago No. 2 -	mes:	Mayo	de	2023	$ 544.104.546,00	
Pago No. 3 -	mes:	Junio	de	2023	$ 596.978.314,00	
Pago No. 4 -	mes:	Julio	de	2023	$ 624.431.841,60	
Pago No. 5 -	mes:	Agosto	de	2023	$ 650.825.466,00	
Pago No. 6 -	mes:	Septiembre	de	2023	$ 661.959.450,00	
Pago No. 7 -	mes:	Octubre	de	2023	$ 641.792.285,00	
Pago No. 8 -	mes:	Noviembre	de	2023	$ 633,094,717.00	
Pago No. 9 -	mes:	Diciembre	de	2023	$ 663.076.196,00	
Pago No. 10 -	mes:	Enero	de	2024	$ 681.934.328,00	
Pago No. 11 -	mes:	Febrero	de	2024	$ 732,950,102.00	

Pago No. 12 -	mes:	Marzo	de	2024	$ 733.890.372,09	
Pago No. 13 -	mes:	Abril	de	2024	$ 730,351,368.00	
Pago No. 14 -	mes:	Mayo	de	2024	$ 719,104,204.57	
Pago No. 15 -	mes:	Junio	de	2024	$ 713,673,218.00	
Pago No. 16 -	mes:	Julio	de	2024	$ 751,372,731.00	
Pago No. 17 -	mes:	Agosto	de	2024	$755,684,192.00	
Pago No. 18 -	mes:	Septiembre	de	2024	$ 752,502,515.00	
Pago No. 19 -	mes:	Octubre	de	2024	$ 770,522,532.00	
Pago No. 20 -	mes:	Noviembre	de	2024	$ 774,178,154.00	
Pago No. 21 -	mes:	Diciembre	de	2024	$ 772,219,902.00	
Pendiente - Pago No. 22 -	mes:	Enero	de	2025	$ 740,982,385.00	
Pendiente - Pago No. 23 -	mes:	Febrero	de	2025	$ 771,789,618.00	
Pendiente - Pago No. 23 -	mes:	Marzo	de	2025	$ 786,219,135.00	
VALOR CAUSADO QUE NO SE HA PAGADO *(valor a pagar factura)* *						$ 786,219,135.00
VALOR TOTAL EJECUTADO *(valor pagado + valor causado no pagado)*						$ 16,740,728,309
SALDO DEL CONTRATO *(valor total del contrato – valor total ejecutado)*						$ 14,658,268,549
PORCENTAJE DE EJECUCIÓN						53.32%
** 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 19 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 MARZO 2025.pdf
Reporte Mensual ICETEX_v2- MARZO.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 20 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

A continuación, se describen las incidencias y requerimientos presentados durante el mes de marzo 2025 en los módulos de videoconferencia, que los integran 4 módulos de 65” y los 6 de 55” instalados en las diferentes sedes de la tabla anterior.

8.1. Disponibilidad del servicio – sedes Regionales

En la verificación realizada para el pasado mes de marzo 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.

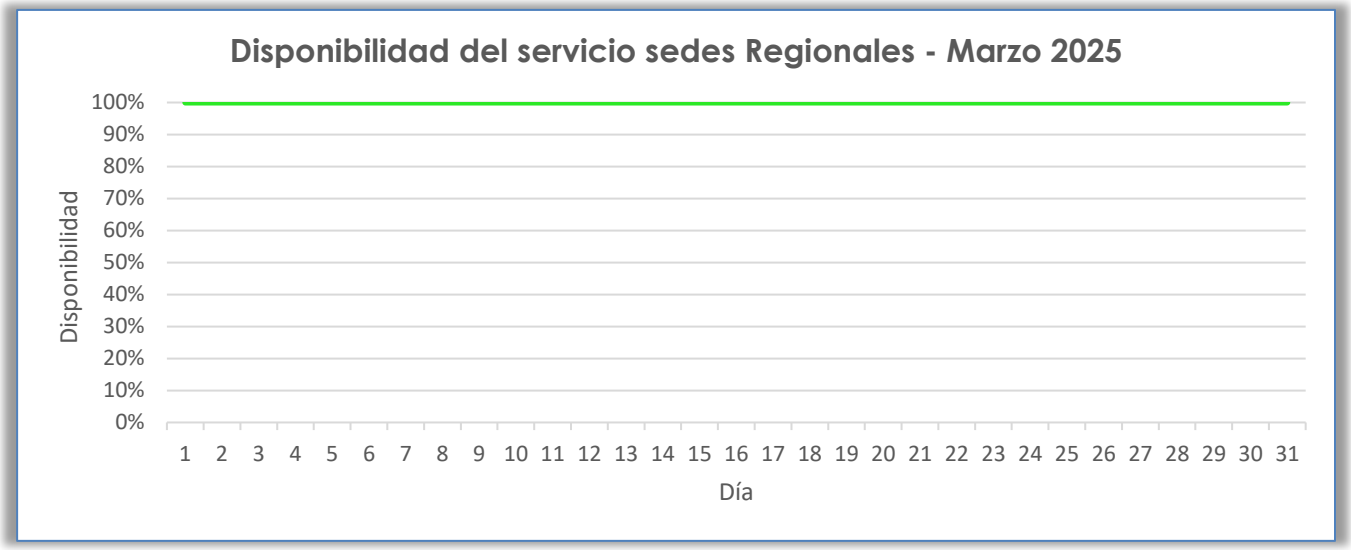


Ilustración 29 Disponibilidad de servicio videoconferencia sedes regionales – marzo 2025

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

En la verificación realizada en el mes de marzo de 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.

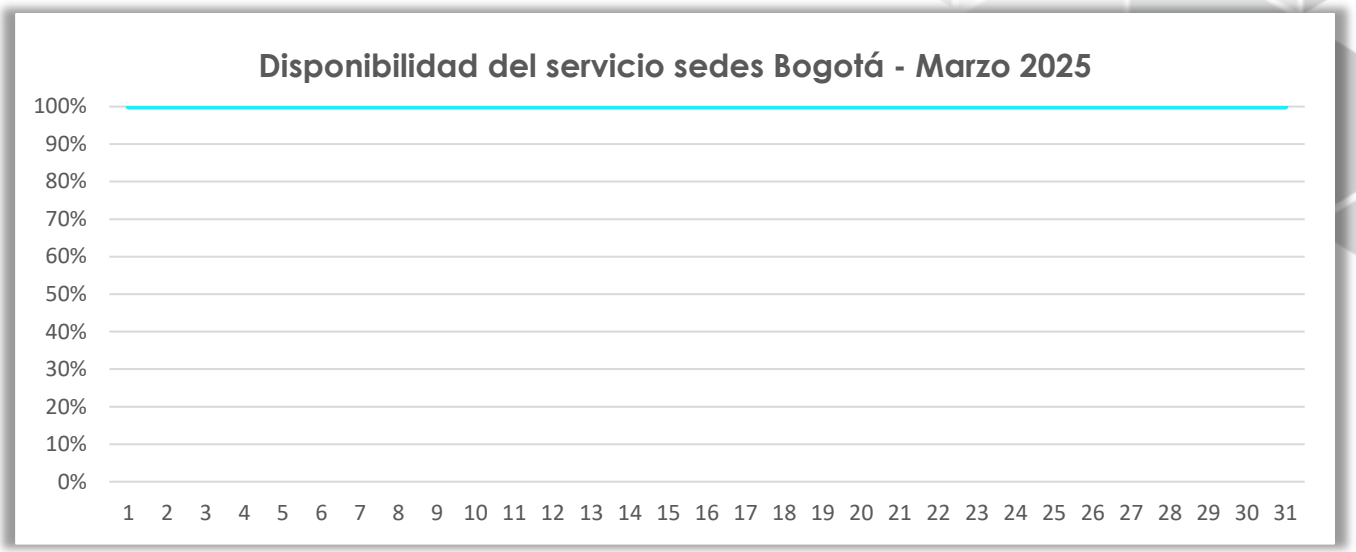


Ilustración 30 Disponibilidad de servicio videoconferencia sedes Bogotá – marzo 2025

8.3. Gestión de incidencias y requerimientos – sedes regionales

Para el periodo de marzo del 2025, comprendido entre el 1 y el 31 del mes, en las sedes Regionales (Cali, Barranquilla, Bucaramanga, Medellín y Chapinero) 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 31 Incidentes / Requerimientos sedes regionales – marzo 2025

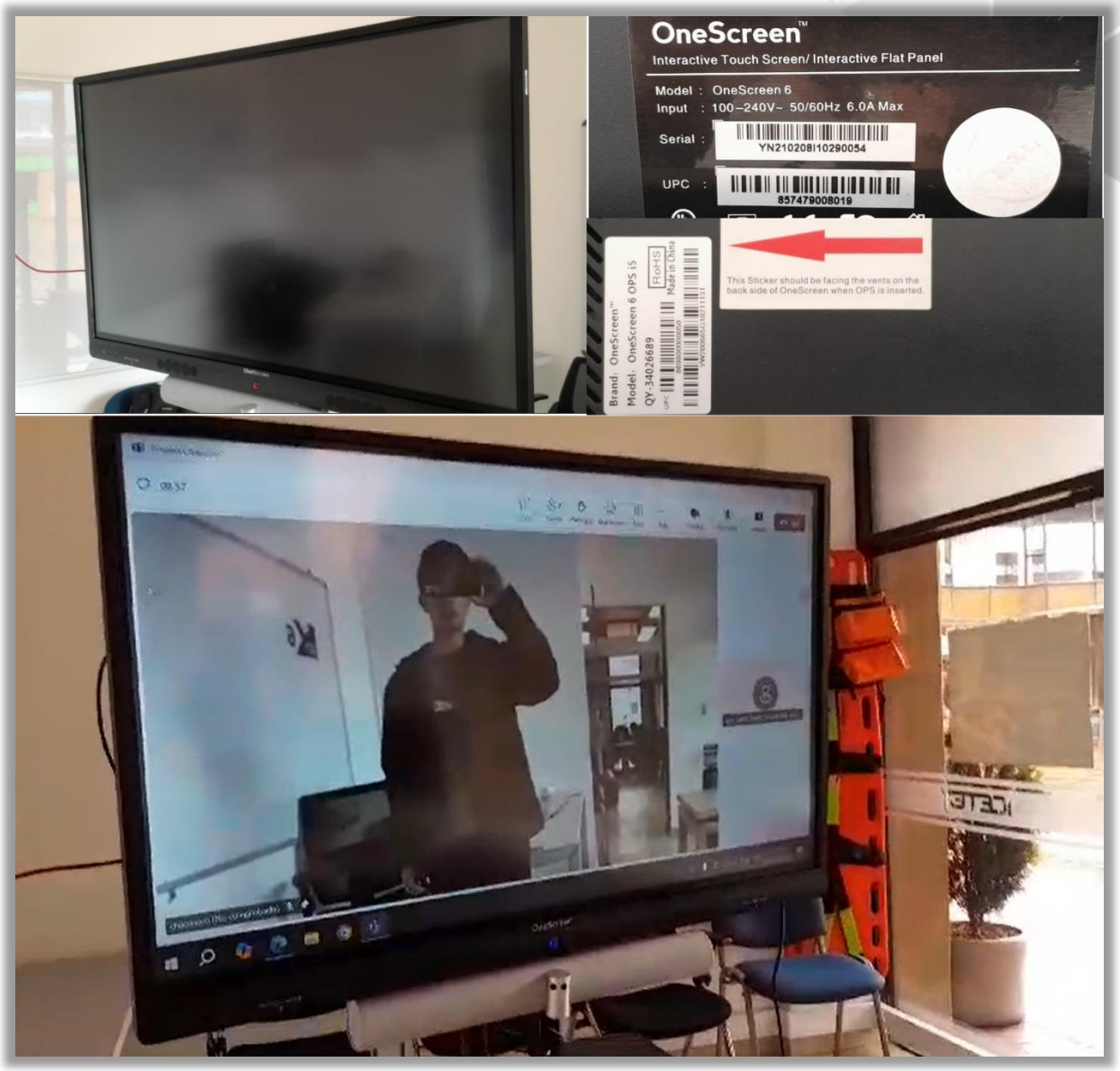


Ilustración 32 Prueba de funcionamiento visita sede chapinero – marzo 2025

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

Para el periodo comprendido entre el 1 y el 31 de marzo 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 la visita periódica realizada a la sede de Aguas, 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-297353-8-22412.

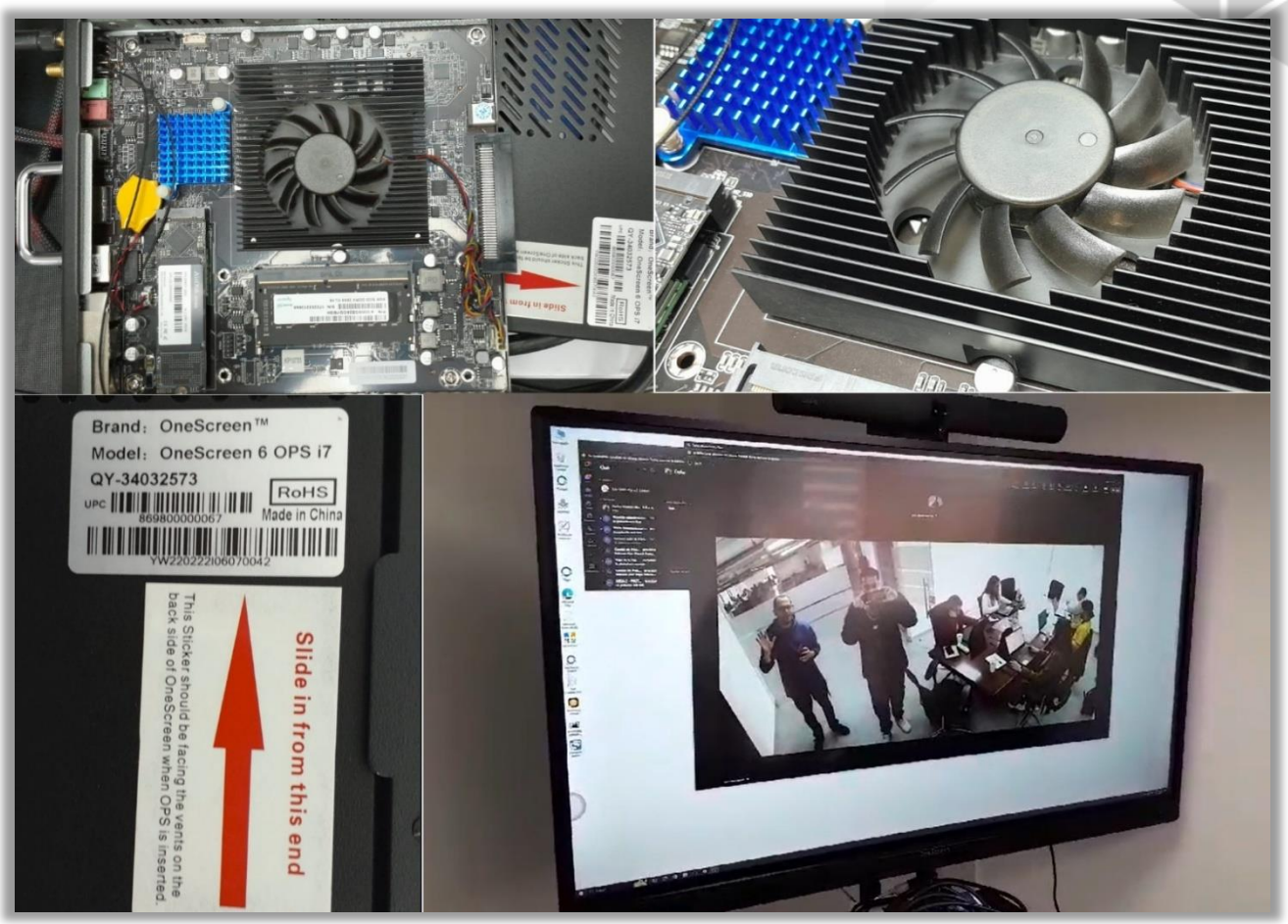


Ilustración 33 Limpieza OPS sala 6to piso – Visita revisión marzo 2025

Para la OPS del módulo piso 6, se realizó mantenimiento preventivo de limpieza interna como se aprecia en la ilustración anterior, además de limpieza superficial y del ventilador de la OPS para eliminar suciedad en el dispositivo, aplicando limpia contactos en las partes electrónicas internas, como se vienen realizando en las demás salas, posterior a eso, se realizan las pruebas en el módulo para confirmar el correcto funcionamiento.

Durante la visita se realizaron pruebas de funcionamiento y revisión en los módulos de los demás pisos de la sede Aguas que contaron con disponibilidad para revisión, ya que en algunas ocasiones las salas se encuentran en uso, por lo cual no se intervienen, sin embargo, se valida el funcionamiento correcto del módulo y del servicio, y se prioriza la revisión para visitas posteriores, además, se realiza inspección visual de desgaste de elementos y conexiones para garantizar servicio sin interrupciones en acompañamiento del personal de mesa de ayuda de la entidad, Ilustración 33. En el resto de las salas de esta sede en particular

ya se realizó mantenimiento preventivo interno de las OPS.

Ilustración 34 Evidencia módulo funcional sede Aguas 65´´, piso 4 - Visita marzo 2025

Para el módulo ubicado en el auditorio del piso 2 – sede Aguas, se realiza el proceso de limpieza superficial de las partes del módulo para eliminar suciedad, inspección de desgaste de partes y se valida

funcionamiento posterior a la revisión (Ilustración 35).

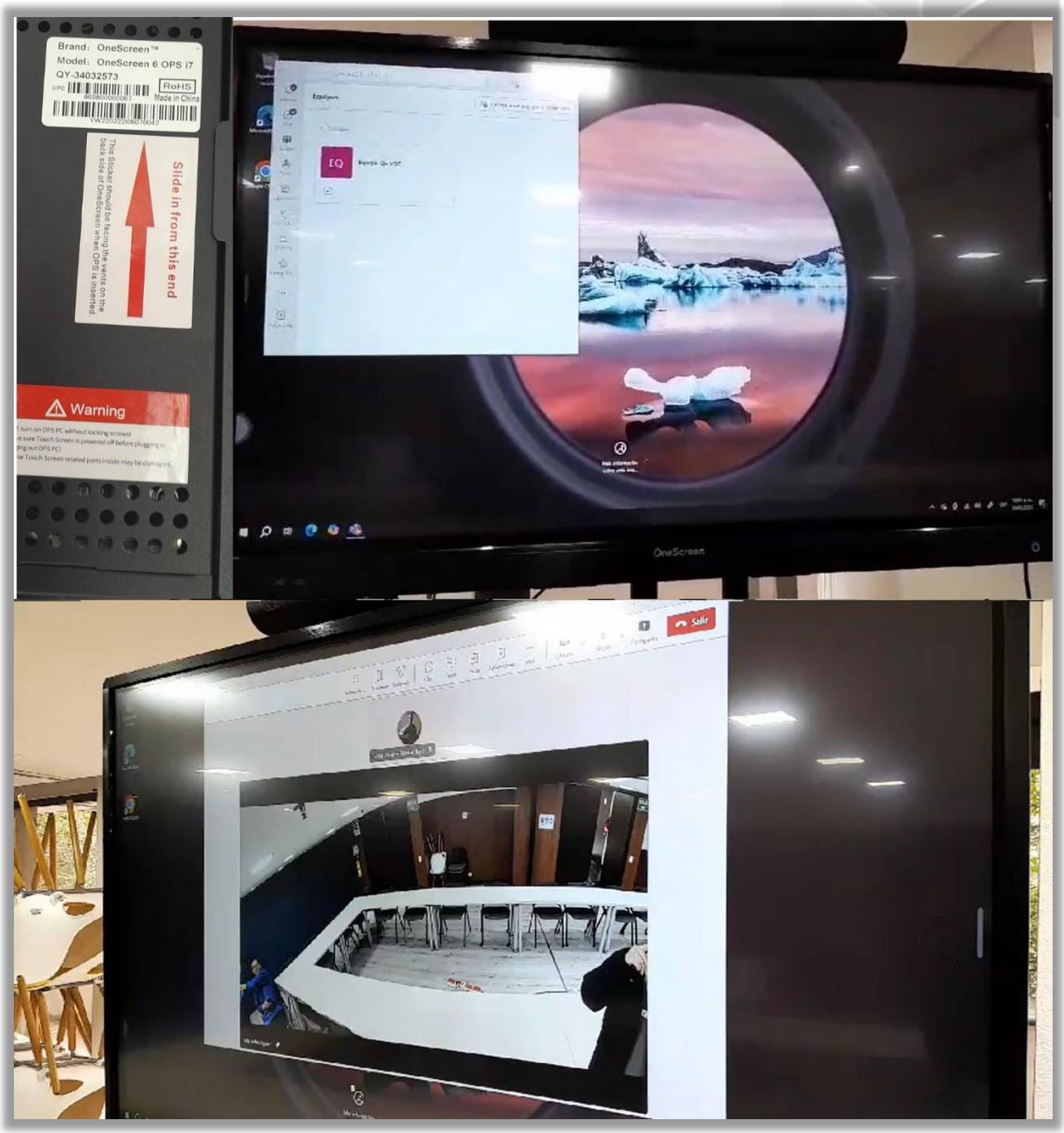


Ilustración 35 Evidencia Módulo sede Aguas 65", piso 2 – Visita de revisión marzo 2025

Para la sede Icetex Ángel, al igual que en el piso 6 de aguas, se realizó mantenimiento preventivo realizando limpieza superficial y limpieza interna de la OPS, como se aprecia en la ilustración 36, con el fin de eliminar

suciedad del ventilador de la OPS para en el dispositivo y de las partes electrónicas internas para mejorar rendimiento de la misma, como se ha venido realizando en las demás salas, posterior a eso, se realizan las pruebas en el módulo para confirmar el correcto funcionamiento.

Ilustración 36 Evidencia Módulo sede Ángel 65" – Visita de revisión marzo 2025

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

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

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

- Visita en sitio en sedes de Bogotá, para realizar pruebas de funcionamiento, inspección de los módulos y posterior limpieza interna y externa principalmente de las OPS de los módulos instalados en la sede Aguas,

Ángel y chapinero de la ciudad de Bogotá, para garantizar la prestación continua del servicio y validar que no se estén presentado novedades y/o incidencias.

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

- Inicio de gestión para realizar visitas en sedes Regionales de Icetex durante el transcurso del mes de abril con el fin de realizar mantenimientos preventivos de los módulos de videoconferencia que se encuentran en estas sedes.

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

Durante los últimos 3 meses no se han presentado requerimientos y/o incidentes durante la prestación del servicio de videoconferencia.

	Marzo	Febrero	Enero
Requerimiento	0	0	0
Incidentes	0	0	0

Tabla 21 Distribución trimestral de requerimientos y/o incidentes

Para el mes de marzo 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 37 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 22 Nivel de riesgo

- Tabla de grado de riesgo

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

Tabla 23 Grado de riesgo

10. INDICADORES CLAVE DE DESEMPEÑO

10.1. ANS por Disponibilidad de canales de comunicaciones:

Durante el mes de marzo 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 Marzo 2025.pdf
Informe Mensual ALLOT marzo 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 marzo ANS_Marzo_2025.xlsx

Sede	Categoría	INR	%MES
BOGOTAD.C.	Principal/FO (Sede Aguas)	INR0037	100.00%
	Backup /FO (Sede Aguas)	INR0036	99.95%
	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	93.57%
	Backup/IPVPN	INR0076	93.61%
LETICIA	Principal/Satelital	INR0000373	94.73%
NEIVA	Principal/IPVPN	INR0039	99.98%
	Backup/IPVPN	INR0041	100.00%
TUNJA	Principal/IPVPN	INR0104	100.00%
	Backup/IPVPN	INR0106	99.98%
VILLAVICENCIO	Principal/IPVPN	INR0085	100.00%
	Backup/IPVPN	INR0084	99.98%
ARMENIA	Principal/IPVPN	INR0074	99.69%
	Backup/IPVPN	INR0072	99.72%
MANIZALES	Principal/IPVPN	INR0088	100.00%
	Backup/IPVPN	INR0087	98.93%
MEDELLIN	Principal/IPVPN	INR0133	100.00%
	Backup/IPVPN	INR0132	99.98%
APARTADO	Principal/IPVPN	INR0144	99.69%
PEREIRA	Principal/IPVPN	INR0079	100.00%
	Backup/IPVPN	INR0077	99.95%
QUIBDO	Principal/IPVPN	INR0014	99.83%
	Backup/IPVPN		0%

Sede	Categoría	INR	%MES
BARRANQUILLA	Principal/IPVPN	INR0103	100.00%
	Backup/IPVPN	INR0100	99.83%
CARTAGENA	Principal/IPVPN	INR0109	99.87%
	Backup/IPVPN	INR0107	99.68%
MONTERIA	Principal/IPVPN	INR0080	99.95%
	Backup/IPVPN	INR0081	99.95%
RIOHACHA	Principal/IPVPN	INR0164	100.00%
	Backup/IPVPN	INR0162	99.98%
SANTAMARTA	Principal/IPVPN	INR0154	99.95%
	Backup/IPVPN	INR0152	100.00%
SINCELEJO	Principal/IPVPN	INR0095	99.77%
	Backup/IPVPN	INR0097	99.78%
SANANDRES	Principal/IPVPN	INR0000367 INR0000369	99.97%
BARRANCABERMEJA	Principal/IPVPN		0%
SANGIL	Principal/IPVPN		0%
BUCARAMANGA	Principal/IPVPN	INR0062	99.93%
	Backup/IPVPN	INR0061	100.00%
CUCUTA	Principal/IPVPN	INR0044	99.97%
	Backup/IPVPN	INR0047	100.00%
VALLEDUPAR	Principal/IPVPN	INR0091	99.38%
	Backup/IPVPN	INR0090	99.03%
YOPAL	Principal/IPVPN	INR0121	99.97%
	Backup/IPVPN	INR0123	99.97%
ARAUCA	Principal/IPVPN	INR0110	99.87%
CALI	Principal/IPVPN	INR0151	99.99%
	Backup/IPVPN	INR0153	100.00%
BUENAVENTURA	Principal/IPVPN	INR0051	99.77%
MOCOA	Principal/IPVPN	INR0135	99.58%
	Backup/Satelital	INR0136	99.44%
PASTO	Principal/IPVPN	INR0130	99.81%
	Backup/IPVPN	INR0131	100.00%
POPAYAN	Principal/IPVPN	INR0035	99.93%
	Backup/IPVPN	INR0032	99.82%
TUMACO	Principal/IPVPN	INR0147	84.91%
DCTRIARA	MPLSPP	INR0266	99.9%
	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	100.00%
DCTRIARA	DCMEGACENTER–CONTIGENCIA–MPLSBK	INR0230	99.8%
DC Megacentro	Internet	INR0268	99.8%
Banco de la Republica hasta Edificio Dirección General ICETEX	Ubicado en Data center Principal. Interconectado a través de red MPLS	INR0000289	99.75%
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 24 Disponibilidad de Canales

Durante el mes de marzo 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	99.81%
BUCARAMANGA	INTERNET PARA LA GENTE	INR0057	100.00%
CALI	INTERNET PARA LA GENTE	INR0160	99.99%
AGUAS	INTERNET PARA LA GENTE	INR0029	100.00%
CHAPINERO	INTERNET PARA LA GENTE	INR0015	100.00%
MEDELLIN	INTERNET PARA LA GENTE	INR0122	100.00%
APARTADO	INTERNET PARA LA GENTE	INR0140	99.7%
ARAUCA	INTERNET PARA LA GENTE	INR0115	99.68%
LETICIA	INTERNET PARA LA GENTE	INR0000378	94.79%
QUIBDO	INTERNET PARA LA GENTE	INR0021	100.00%
RIOHACHA	INTERNET PARA LA GENTE	INR0159	100.00%
SAN ANDRES	INTERNET PARA LA GENTE	INR0000368	99.98%
YOPAL	INTERNET PARA LA GENTE	INR0127	99.97%
MOCOA	INTERNET PARA LA GENTE	INR0141	99.81%

Tabla 25 Disponibilidad canales "Internet para la gente"

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 marzo continúa su funcionamiento correctamente sin novedades que afectaran la prestación del servicio.

La evidencia se encuentra en el Informe mensual replicacion Marzo 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 Marzo 2025-ELK.pdf

Cod Servicio	Hostname	Disponibilidad
INR0228	ictxsisgesbd	100%
INR0229	ictxsisgesapp	100%
INR0233	icetexboglxorfeo1	100%
INR0234	ictxprusisgapp	100%
INR0237	icetexbogbalserver1-r	100%
INR0238	icetexbogliferaynfs	100%
INR0239	icetexbogelasticserver1	99,98%
INR0241	icetexbogelasticserver3	100%
INR0242	icetexbogliferayserver2	99,99%
INR0243	icetexbogliferayserver1	100%
INR0244	icetexboglxdarumasrv1	100%
INR0245	icetexboglxdarumasrv2	100%
INR0246	iceteboglxdarumatest	100%
INR0247	preprodsec-icetexboglxxroad2n	100%
INR0248	icetexboglxxroad3	100%

Cod Servicio	Hostname	Disponibilidad
INR0249	xroadsec-icetexboglxxroad1	100%
INR0250	qasec-icetexboglxxroadtest	99,99%
INR0262	icetexboglxorfeo2	100%
INR0276	cxvodaprodn011	99,77%
INR0277	cxvodaprodn021	100%
INR0278	cxvodacontn011	100%
INR0240	icetexbogelasticserver2	100%
INR0260	icetexbogosbognfs1	100%
INR0252	icetexbogosbognfs2	100%
INR0236**	ictxbogsrvpt1	100%
INR0235**	ictxbogsrvpt2	100%
INR0000322	ictxcontroldoc	100%
INR0226	mira	100%
INR0253*	bastion	100%
INR251	Openshift	99,99%
INR254	Openshift	100%
INR255	Openshift	100%
INR256	Openshift	100%
INR257	Openshift	99,99%
INR258*	Openshift	100%
INR259	Openshift	100%

Tabla 26 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, 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

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 27 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 marzo un **UPTIME del [99,988%]** tal como se evidencia en la gráfica a continuación.

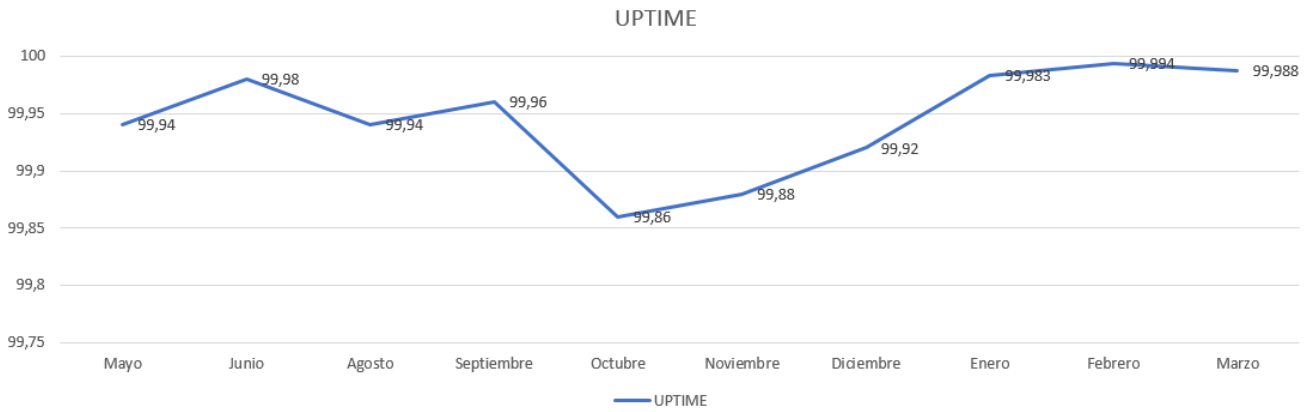


Ilustración 38 UPTIME – Portal WEB web.ICETEX.gov.co

Durante el mes de marzo se evidenció un comportamiento estable del portal WEB institucional y se cumplió con el porcentaje de disponibilidad de este con un porcentaje del **99,988%,** 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 354 mil usuarios, con 230 mil usuarios nuevos. El tiempo de interacción medio es de un minuto, señalando el interés de la audiencia en las diferentes páginas del portal web.ICETEX.gov.co.

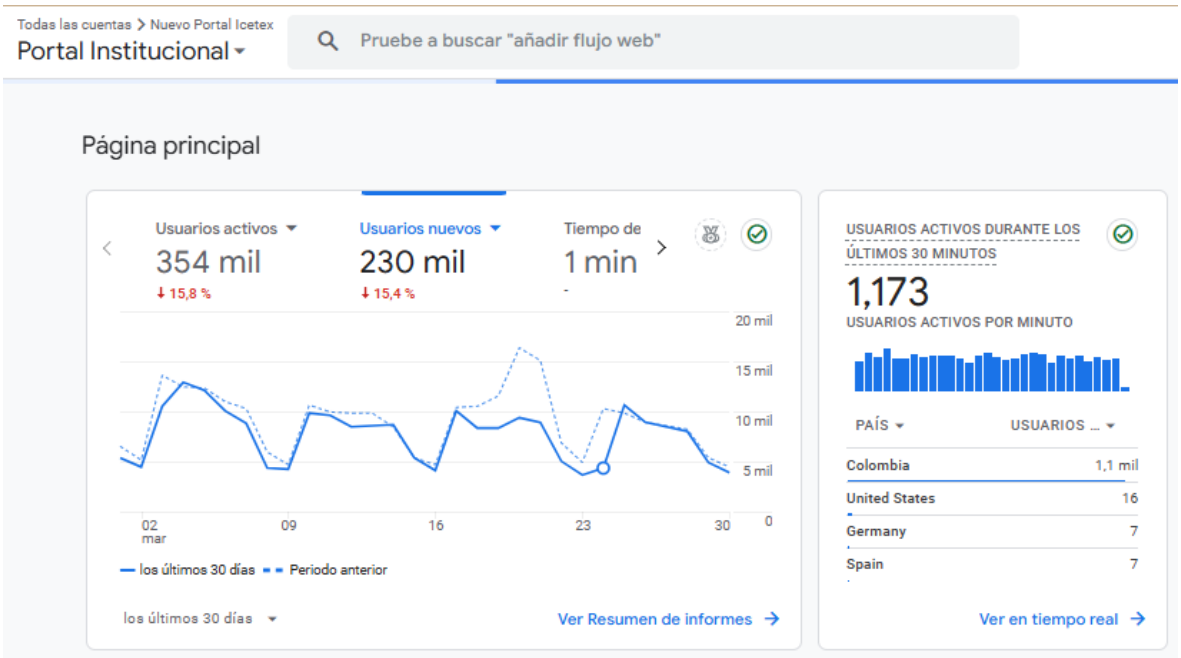


Ilustración 39 Métrica de visitantes Portal WEB web.ICETEX.gov.co

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

Adquisición de usuarios: Primer grupo de canales principal del usuario (Grupo de canales predeterminado)

	Primer grupo de...redeterminado)	Total de usuarios	Usuarios nuevos	Usuarios recurrentes	Tiempo de interacción medio por usuario activo	Sesiones con interacción por usuario activo	Número de Todos los ev
	Total	356.992 100 % respecto al total	220.521 100 % respecto al total	168.929 100 % respecto al total	1 min y 50 s Media 0 %	1,31 Media 0 %	100 % resp
1	Organic Search	224.397 (62,86 %)	134.124 (60,82 %)	115.793 (68,55 %)	1 min y 59 s	1,36	3.099.9
2	Direct	107.508 (30,11 %)	67.264 (30,5 %)	47.390 (28,05 %)	1 min y 37 s	1,30	1.468.18
3	Referral	18.788 (5,26 %)	15.033 (6,82 %)	5.736 (3,4 %)	1 min y 39 s	1,04	187.3
4	Organic Social	4.947 (1,39 %)	3.818 (1,73 %)	844 (0,5 %)	39 s	0,71	31.3
5	Unassigned	192 (0,05 %)	168 (0,08 %)	48 (0,03 %)	1 min y 50 s	1,18	2.2
6	Email	119 (0,03 %)	89 (0,04 %)	39 (0,02 %)	2 min y 06 s	1,01	1.2
7	Paid Search	50 (0,01 %)	2 (<0,01 %)	43 (0,03 %)	2 min y 35 s	1,00	5
8	Organic Video	43 (0,01 %)	19 (<0,01 %)	23 (0,01 %)	1 min y 45 s	1,64	5
9	Organic Shopping	4 (<0,01 %)	4 (<0,01 %)	0 (0 %)	1 s	0,25	1
10	Paid Other	4 (<0,01 %)	0 (0 %)	2 (<0,01 %)	2 s	0,50	2

Ilustración 40 Métrica adquisición usuarios Portal WEB web.ICETEX.gov.co

Métricas de usuario: Se evidencia que el país que más visita el portal WEB es Colombia, seguido de Estados Unidos. Por otra parte, la ciudad que más visita el portal WEB es Bogotá seguida de Medellín.

El idioma que predomina es el español seguido por el idioma inglés.

Ilustración 41 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 1 de marzo desde las 0:00 am hasta las 11:59 am del 31 de marzo de 2.025.

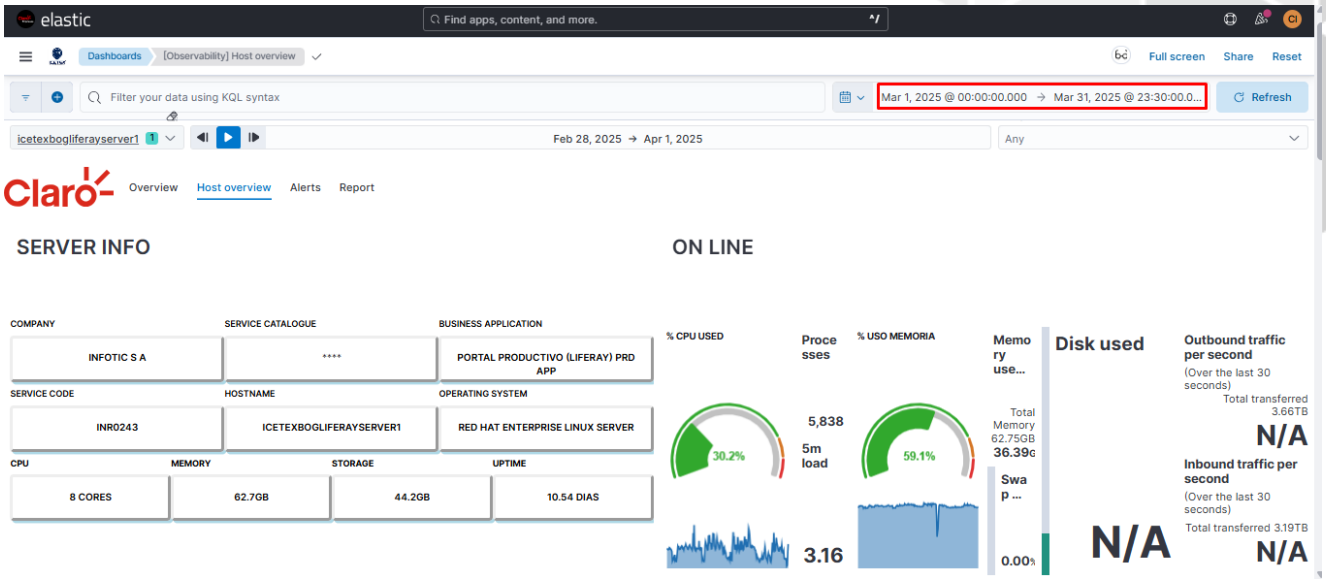


Ilustración 42 NODO 1 – Vista General – INR0243

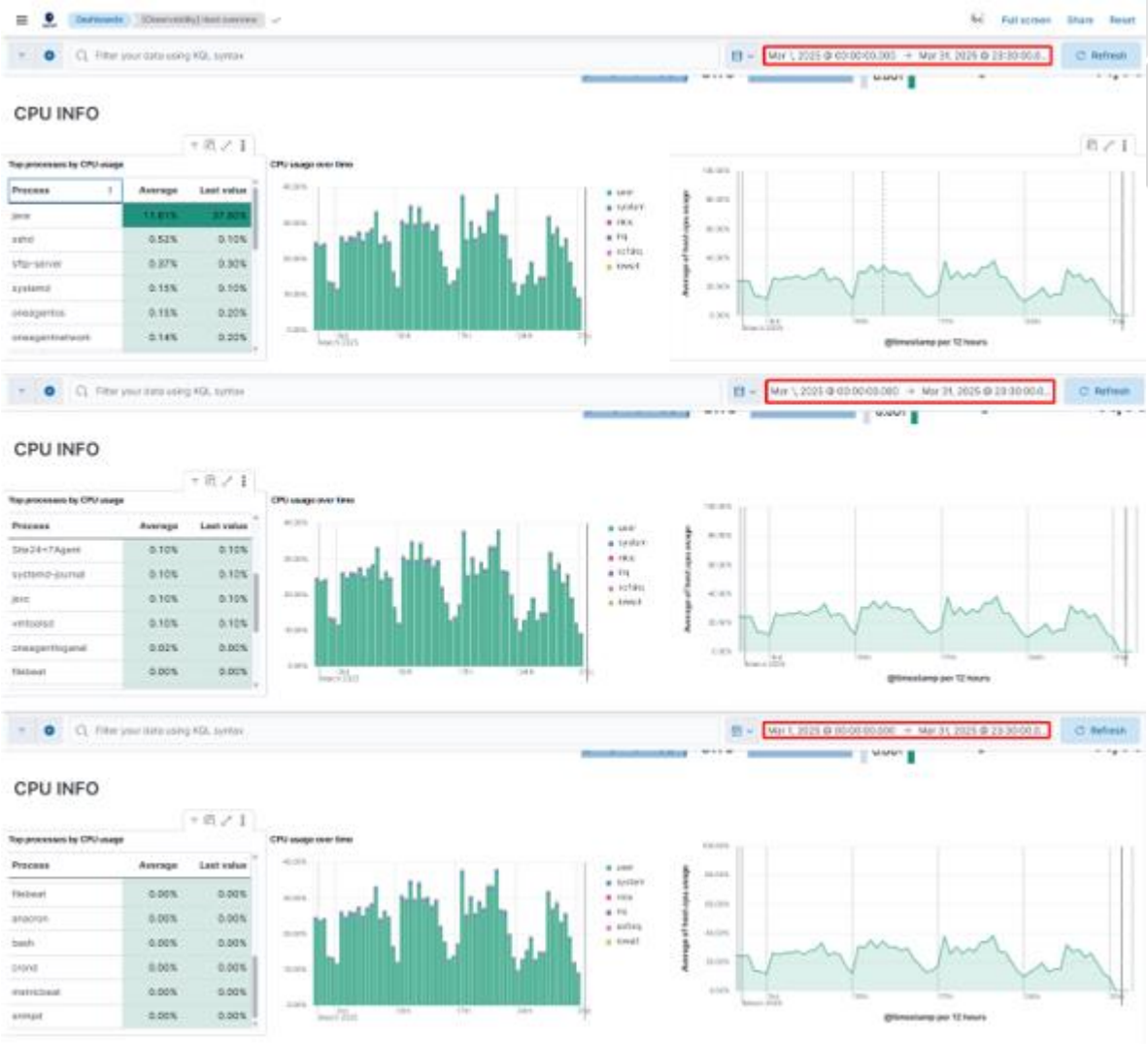


Ilustración 43 NODO 1 CPU

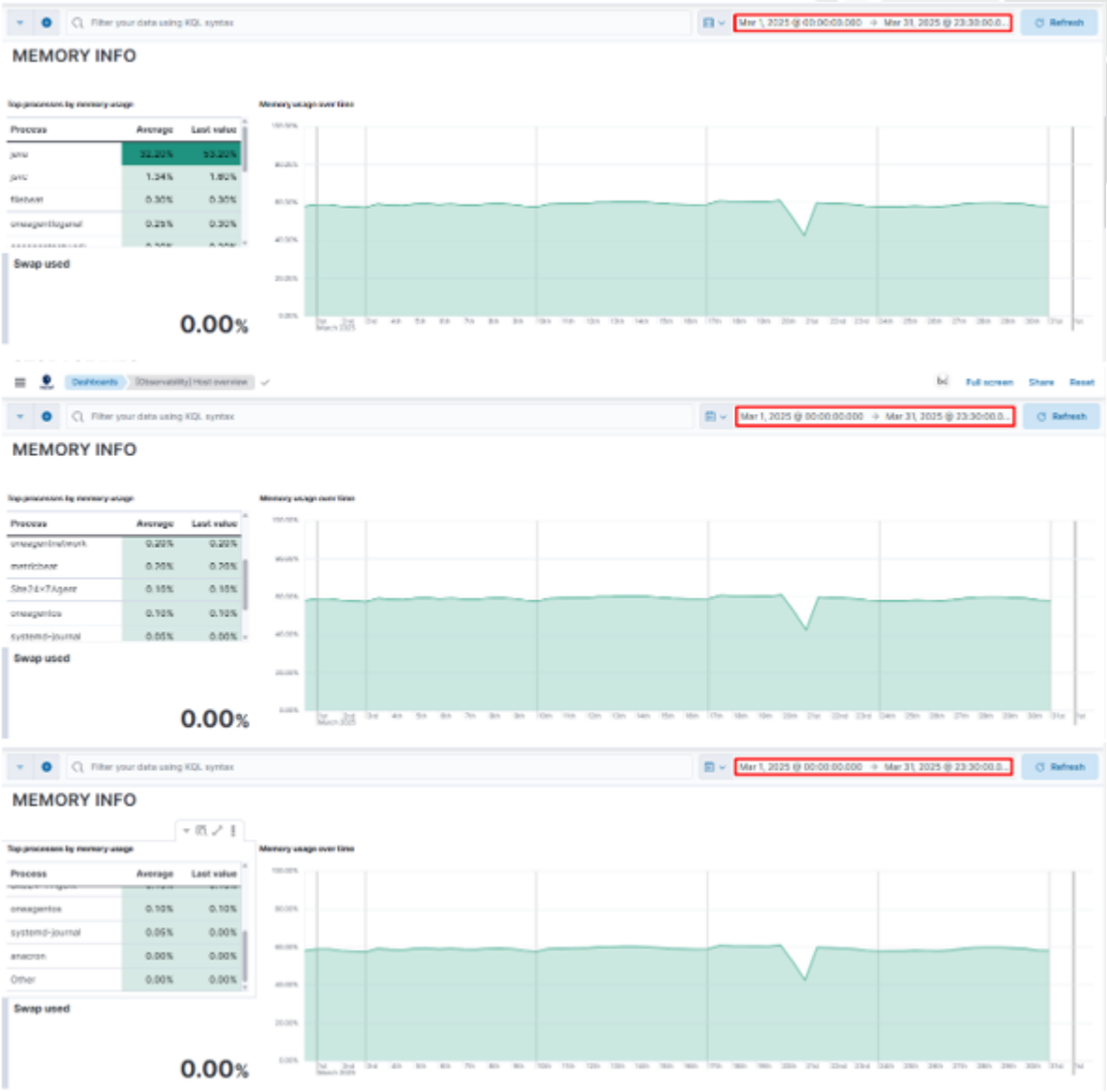


Ilustración 44 NODO 1 Memoria

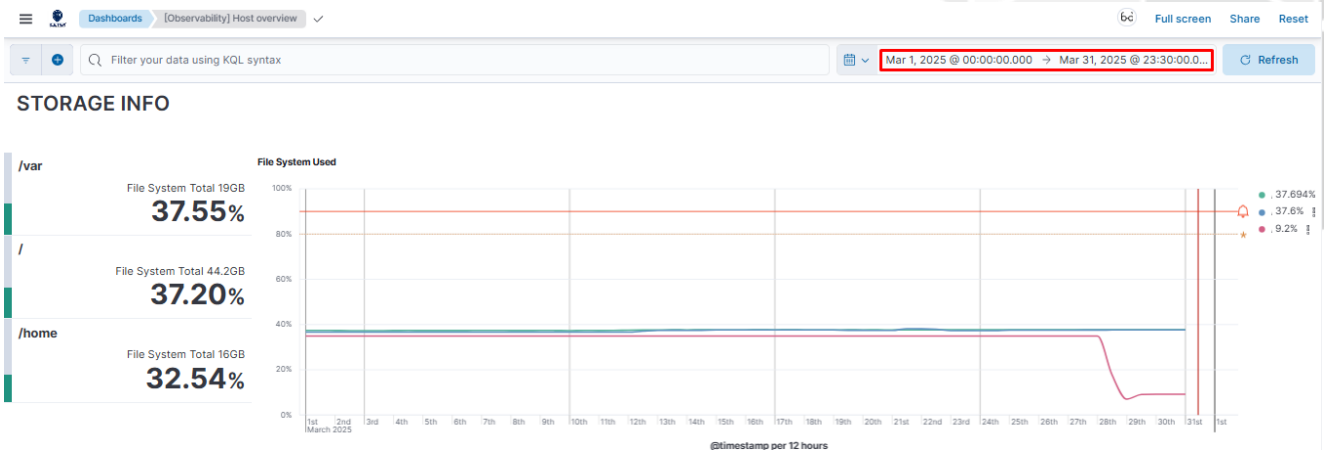


Ilustración 45 NODO 1 Almacenamiento

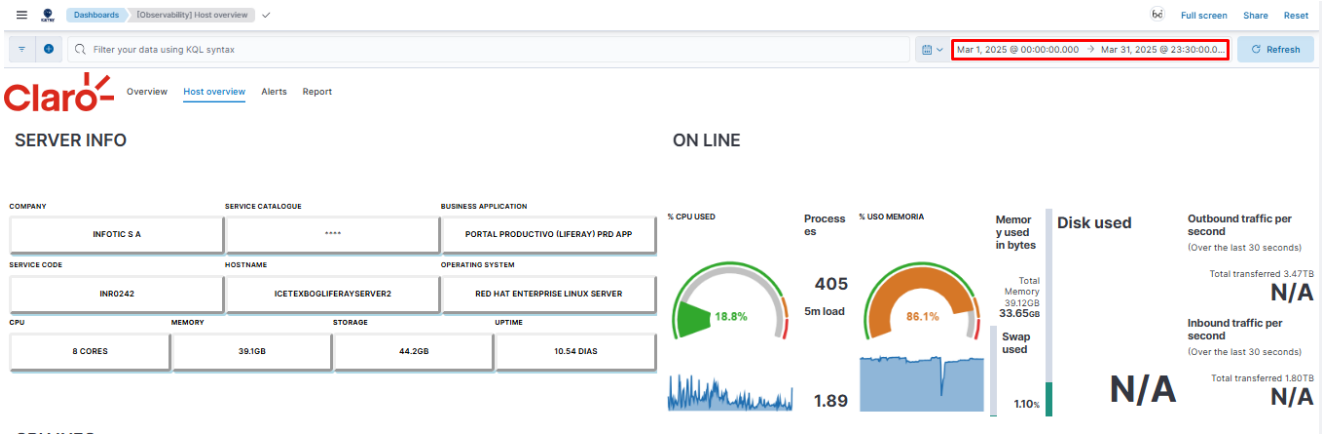


Ilustración 46 NODO 2 – Vista General – INR0242

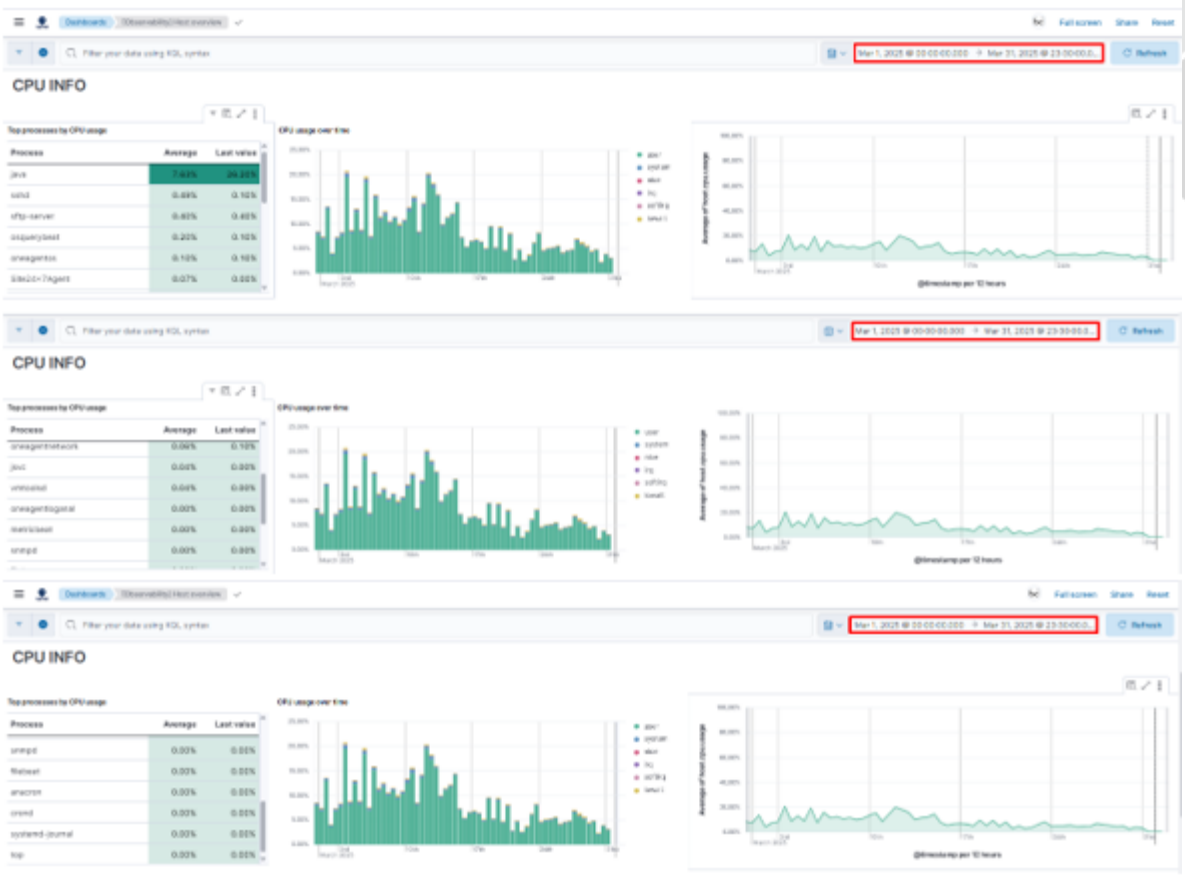


Ilustración 47 NODO 2 CPU

Entre el 1 y el 31 de marzo, 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. Esta implementación ha permitido que el consumo de memoria SWAP en el nodo 2 se mantenga en niveles moderados. Así, al 28 de marzo de 2025 a las 11:57 a.m., el porcentaje de SWAP disponible es del 100%, como se puede observar en la captura de pantalla adjunta. Por lo tanto, el aliado Claro no ha enviado más alertas por correo electrónico relacionadas con un alto consumo de SWAP en el nodo 2.

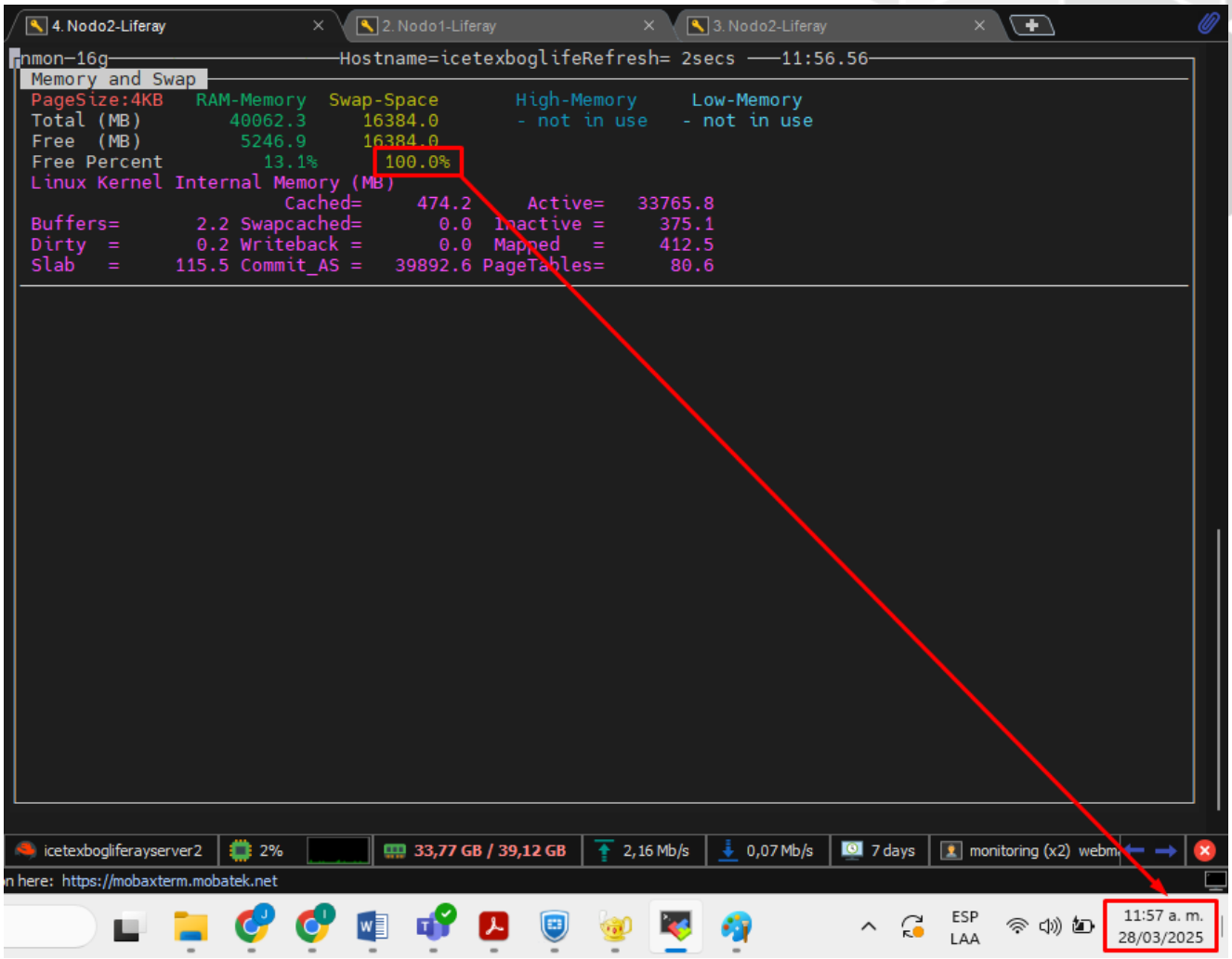


Ilustración 48 NODO 2 memoria SWAP

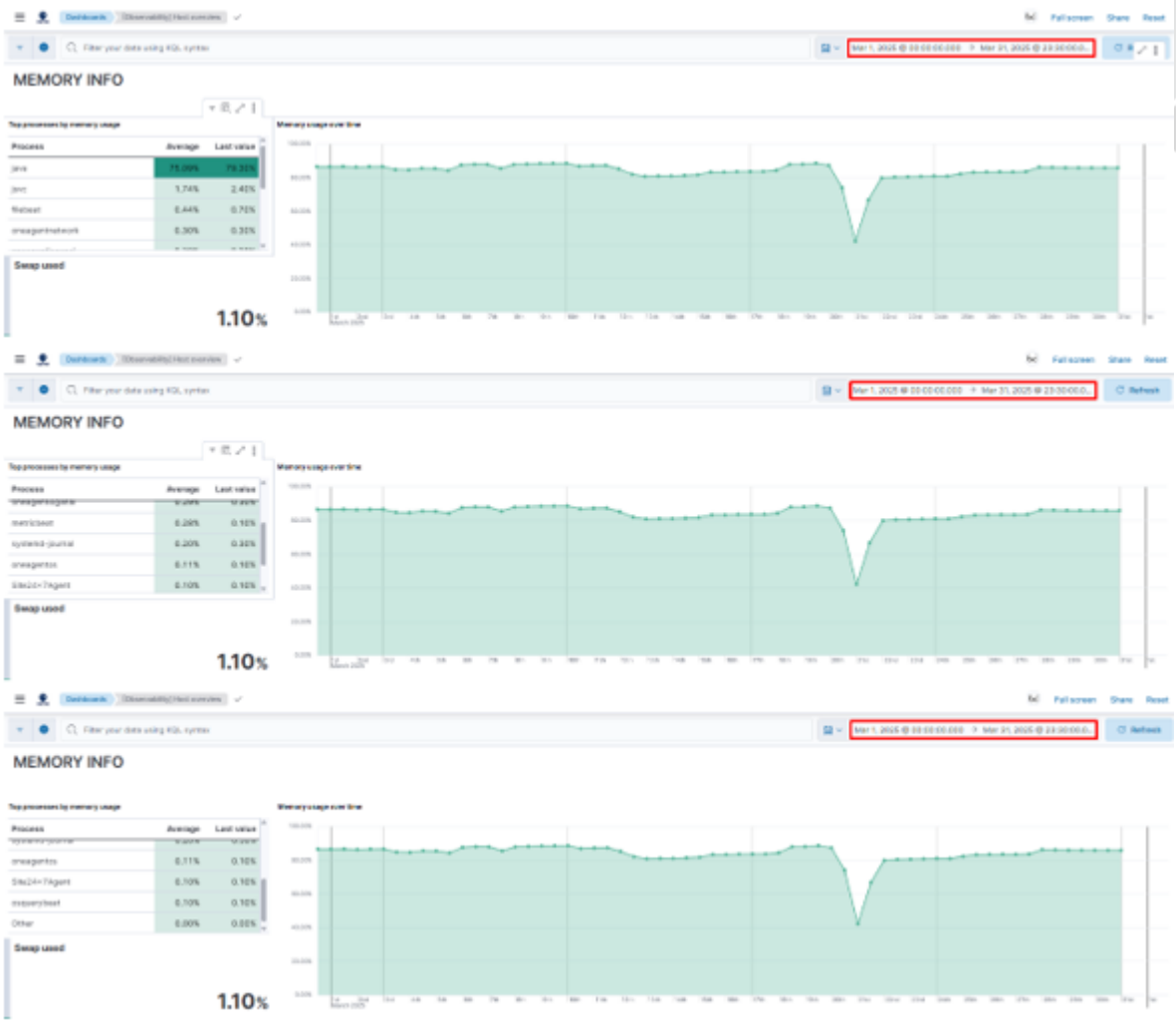


Ilustración 49 NODO 2 Memoria

Ilustración 50 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 coordinar la actividad de actualización de sistema operativo Linux Red Hat 7.9. 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, se requiere un recurso de migración de realizar el cambio de Liferay 7.3 a la versión 7.4 DXP.
DISCO DURO	El espacio en disco utilizado por el CMS Liferay en el **nodo 1 es 132 GB**. El espacio disponible es de 244 GB. El espacio en disco utilizado por el CMS Liferay en el **nodo 2 es 200 GB**. El espacio disponible es de 194 GB.	**NODO 1** Comportamiento normal. Con el proceso de eliminación de logs en el nodo 1 del portal ICETEX realizado el 27 de marzo por parte del ingeniero de Claro Freddy Alexander Castro Navarro, se cuenta con un espacio disponible de **256 GB**. 5. Nodo1-Lifer ✕ 3. Nodo2-Life ✕ [root@icetexbogliferayserver1 ~]# df Filesystem Size Used Av /dev/mapper/rhel-root 45G 16G devtmpfs 32G 0 tmpfs 32G 0 tmpfs 32G 233M tmpfs 32G 0 /dev/sda1 4.0G 236M 3 /dev/mapper/app-appvol 394G 120G 2 /dev/mapper/rhel-var 19G 7.2G /dev/mapper/rhel-home 16G 1.2G 192.168.20.42:/nfs1 503G 381G 192.168.20.42:/nfs 503G 127G 3 tmpfs 6.3G 0 6 tmpfs 6.3G 0 6 [root@icetexbogliferayserver1 ~]# df Se realizó la exportación de los logs del nodo 1 al servicio NFS, a continuación, se detalla el proceso:

UNIDAD	HALLAZGO	OBSERVACIONES
		El 28 de marzo se copian de los logs (.xml y .log por fecha) del año 2025 comprimidos en formato .zip a la ruta **/nfs/nodo1logs/2025/**
FILE SYSTEM	El espacio en disco utilizado por el CMS Liferay al 28 de marzo de 2025 3:29 p.m en el **nodo 1 es 120 GB.** El espacio en disco utilizado por el CMS Liferay al 28 de marzo de 2025 3:29 p.m en el **nodo 2 es 21 GB.**	Cabe resaltar que la copia a la ruta /nfs/nodo1logs/2025/ de los archivos .log y .xml se realizó hasta el **2025-03-11**. También se procedió con la eliminación de los archivos server.log alojados en la ruta: **/app/liferay/wildfly-17.0.1/standalone/log/** Se realizó copia hasta el archivo **server.log.2025-03-14** en el nodo 1. Por consiguiente, los archivos server.log del nodo 1, se comprimieron en el archivo **server_log_nodo1.zip** y se copiaron al servicio NFS en la ruta **/nfs/nodo1logs/server_log_nodo1**. **NODO 2** Comportamiento normal. Con el proceso de eliminación de logs en el nodo 2 del portal ICETEX realizado el 27 de marzo por parte del ingeniero de Claro Freddy Alexander Castro Navarro, se cuenta con un espacio disponible de **357 GB**. 7.Nodo2-Life X 5.Nodo1-Life X 4.Nodo2-Life X 2.Nodo1-Li [root@icetexbogliferayserver2 ~]# df -h Filesystem Size Used Avail Use% Mounted on /dev/mapper/rhel-root 45G 15G 28G 34% / devtmpfs 20G 0 20G 0% /dev tmpfs 20G 0 20G 0% /dev/shm tmpfs 20G 97M 20G 1% /run tmpfs 20G 0 20G 0% /sys/fs/cgroup /dev/mapper/app-appvol 394G 21G 357G 6% /app /dev/mapper/rhel-var 19G 6.9G 13G 37% /var /dev/sda1 4.0G 235M 3.8G 6% /boot /dev/mapper/rhel-home 16G 5.5G 11G 35% /home 192.168.20.42:/nfs 503G 125G 353G 27% /u01 192.168.20.42:/nfs1 503G 381G 97G 80% /backup tmpfs 4.0G 0 4.0G 0% /run/user/1030 tmpfs 4.0G 0 4.0G 0% /run/user/1008 tmpfs 4.0G 0 4.0G 0% /run/user/0 [root@icetexbogliferayserver2 ~]# Se realizó la exportación de los logs del nodo 2 al servicio NFS, a continuación, se detalla el proceso: El 28 de marzo se copian de los logs (.xml y .log por fecha) del año 2025 comprimidos en formato .zip a la ruta **/nfs/nodo2logs/2025/** Cabe resaltar que la copia a la ruta /nfs/nodo2logs/2025/ de los archivos .log y .xml se realizó hasta el **2025-03-11**.

UNIDAD	HALLAZGO	OBSERVACIONES
		También se procedió con la eliminación de los archivos server.log alojados en la ruta: **/app/liferay/wildfly-17.0.1/standalone/log/** Se realizó copia hasta el archivo **server.log.2025-03-14** en el nodo 2. Por consiguiente, los archivos server.log del nodo 2, se comprimieron en el archivo **server_log_nodo2.zip** y se copiaron al servicio NFS en la ruta **/nfs/nodo2logs/server_log_nodo2**.
PARCHES DE SEGURIDAD	**Nodo 1** - activation-key-dxpproduction-7.3-icetex-publicportal 40.xml activation-key-dxpproduction-7.3-icetex-publicportal - icetexbogliferayserver1.xml **Nodo 2** - activation-key-dxpproduction-7.3-icetex-publicportal - icetexbogliferayserver2.xml	Pendiente de aprobación por parte del cliente de la renovación de soporte Liferay. Con la renovación se garantiza que el recurso que realice la actividad de migración obtenga del fabricante el instalador de Liferay 7.4 DXP para WildFly y sus parches de seguridad.
VOLUMEN DE LOGS	Registro de logs entre finales de noviembre comienzos de diciembre.	No se registran errores de logs en los nodos 1 y 2 del portal ICETEX. Está pendiente una reunión con los ingenieros de Claro para que ellos realicen la eliminación de los logs del nodo 2 desde el 11 de diciembre de 2023 hasta el 31 de diciembre de 2024.

Tabla 28 Actualización – Análisis componente LIFERAY Marzo

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 148 GB, espacio disponible 331 GB y porcentaje usado 31%. **Partición NFS1** total de espacio en disco – 503 GB, espacio usado 381 GB, espacio disponible 97 GB y porcentaje usado 80%.	2. Nodo1-Liferay / 3. Nodo2-Liferay [root@icetexbogliferaynfs ~]# df -h Filesystem Size Used Avail U devtmpfs 3.8G 0 3.8G tmpfs 3.8G 0 3.8G tmpfs 3.8G 417M 3.4G tmpfs 3.8G 0 3.8G /dev/mapper/cl_icetexbogliferaynfs-root 50G 13G 38G /dev/mapper/nfs-u01 503G 148G 331G /dev/mapper/nfs1-backup 503G 381G 97G /dev/mapper/cl_icetexbogliferaynfs-home 42G 14G 29G /dev/sda1 976M 409M 500M tmpfs 775M 0 775M tmpfs 775M 0 775M tmpfs 775M 0 775M [root@icetexbogliferaynfs ~]# **NODO 1** 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/2025/** del servicio NFS.

UNIDAD	HALLAZGO	OBSERVACIONES
		2. Nodo1-Liferay / 3. Nodo2-Liferay [root@icetexbogliferaynfs nodo1logs]# cd 2025 [root@icetexbogliferaynfs 2025]# [root@icetexbogliferaynfs 2025]# ll total 618068 -rw-r--r--. 1 root root 1576567 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 5221240 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 5593143 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 4051537 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 2923444 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 3180637 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 9095854 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 9087594 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 8556490 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 6566886 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 3307636 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 2173807 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 6646295 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 5940339 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 5896637 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 6675603 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 7147148 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 6738919 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 5300768 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 8392489 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 9266623 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 8507258 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 312477420 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 6849118 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 4160612 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 3329268 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 6743750 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 6522418 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 5529688 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 6141178 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 5923979 Mar 28 16:26 liferay.2025-01 -rw-r--r--. 1 root root 3081406 Mar 28 16:26 liferay.2025-02 -rw-r--r--. 1 root root 2931318 Mar 28 16:26 liferay.2025-02 -rw-r--r--. 1 root root 6088058 Mar 28 16:26 liferay.2025-02 -rw-r--r--. 1 root root 7658618 Mar 28 16:26 liferay.2025-02 **NODO 2** Se realizó la copia de los archivos logs comprimidos en formato .zip del nodo 2 del portal ICETEX (.xml y .log por fecha) a la carpeta **/nfs/nodo2logs/2025/** del servicio NFS.

UNIDAD	HALLAZGO	OBSERVACIONES
		2. Nodo1-Liferay / 3. Nodo2-Liferay [root@icetexbogliferaynfs nodo2logs]# [root@icetexbogliferaynfs nodo2logs]# cd 2025 [root@icetexbogliferaynfs 2025]# [root@icetexbogliferaynfs 2025]# ll total 462052 -rw-r--r--. 1 root root 1400401 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 6914152 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 7795088 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 5388208 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 3811716 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 3907966 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 13280875 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 14081732 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 11317948 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 9006820 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 3967903 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 3098617 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 10131169 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 8489588 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 10447785 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 11208372 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 6898108 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 3262703 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 2632509 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 8559913 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 8601418 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 7466026 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 30663723 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 7009875 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 3446152 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 2054451 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 7573522 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 7374589 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 6662447 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 6980352 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 5252148 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 2715921 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 2338452 Mar 28 16:29 liferay.2025- -rw-r--r--. 1 root root 6545121 Mar 28 16:29 liferay.2025-

Tabla 29 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:

	Marzo 2025	Febrero 2025	Enero 2025
Usuarios mes	354000	446000	558000
Usuarios nuevos	230000	291000	373000
Tiempo acceso (seg)	60	119	137

Tabla 30 Distribución trimestral de acceso por usuarios

Durante el último trimestre, el portal web recibió un promedio de 452,667usuarios, lo que refleja un interés significativo en los servicios y contenidos ofrecidos por la entidad. Sin embargo, al analizar los datos correspondientes al mes de Febrero, se observó una disminución del 21% en el número de usuarios que accedieron a la página. Esta caída representa aproximadamente 92,000 usuarios menos.

Durante el último trimestre, se ha observado que, en promedio 298,000 nuevos usuarios accedieron a la página. Sin embargo, es importante destacar una tendencia negativa en relación con los accesos nuevos en marzo, la cifra de usuarios nuevos experimentó una disminución del 21%, lo que representa un total de 61,000 usuarios.

Las siguientes Url´s están siendo monitoreadas desde la herramienta ELK y en el mes de marzo tuvieron la disponibilidad del 100.00%:

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

10.2.3. Backup Servidores Triara

Durante el periodo de marzo se realizaron los Backups de acuerdo con las políticas definida por el ICETEX, las cuales desde su inicio se implementaron en el Datacenter. Se puede verificar en el documento, Informe Backups mes de Marzo 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 marzo el resultado de la ejecución de los Backups fue:

Backup job summary

Backup job summary report

CommCell	All
Company	All
Server groups	INFOTIC
Servers	All
App types / Workloads	All
Subclients	All
Job status	Running, Completed, Delayed, Failed, Killed, Completed with Errors, Completed with Warnings, Committed
Job types	All
Time frame	Last 4 Weeks (Mar 4, 2025, 08:40:01 AM - Apr 1, 2025, 08:40:01 AM)
Time zone	Afghanistan Standard Time
Day Start Time	12:00 AM
Snap and Backup Copy options	All
Advanced	All
Max number of jobs to return	4000

Job status

Jobs by app type / workload

Summary

Job status	Total Jobs	Size of Application	Estimated Media Size	Protected Objects	Failed Objects	Failed Folders
Completed	3250	200.90 TB	47.62 TB	112823987	10620	53
Killed	66	888.93 GB	0.00 KB	0	20	0
Failed	25	15.29 GB	0.00 KB	0	13	0
Completed with errors	5	114.60 GB	661.69 GB	39	3	0
In Progress	1	864.32 GB	0.00 KB	0	1	0

Ilustración 51 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 marzo corresponde a 200.9 TB, donde 97.1% se completó en el primer lanzamiento del robot con un total de 202.78 TB de información.

El 76.79% 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	Enero	Febrero	Marzo
Completado	97.89%	98.36%	97.10%
Fallido	0.78%	0.71%	0.75%
Cancelados	0.78%	0.00%	1.97%
Terminados parcialmente	0.47%	0.81%	0%
Completado con errores	0.04%	0.03%	0.15%
En Proceso	0.02%	0.06%	0.03%
Runinng	0.02%	0.03%	0%
Tamaño (TB)	341.45	214.09	202.78

Tabla 31 Distribución trimestral de Backup ejecutados

El promedio de los Backups completado del último trimestre en el primer lanzamiento del robot fue de 97.78%, donde el mes con mayor nivel de ejecución fue febrero con 98.36%, el 2.9% corresponde a los siguientes parámetros: Fallido, Cancelados, Terminados parcialmente, Completado con errores y en Proceso.

El promedio de toma Backups Fallido durante el último trimestre corresponde a 0.75%, el mes donde más se presentó un mayor porcentaje de fallas fue enero con el 0.78%

	Enero	**Febrero**	**Marzo**
Oracle RAC	86.52%	77.24%	76.79%
Virtual Center	11.87%	19.01%	18.58%
Windows File System	1.47%	2.55%	3.35%
Linux File System	0.45%	0.76%	0.81%
SQL Server	0.18%	0.45%	0.48%

Tabla 32 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 80.18% donde el mes con mayor tamaño de información respaldada fue enero con el 86.52%

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.

La evidencia se genera diariamente en el reporte que se entrega de forma automática por parte del operador tecnológico a los correos que el ICETEX solicito y en el informe mensual se anexan todas los soportes y evidencias de la ejecución de las políticas de Backup, la política actualizada y vigente de la toma de Backup, se encuentra en el link del repositorio Backup Diario y el informe de Backup Informe de Backup

11. CONTROL DE CAMBIOS

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

No. Cambio	Alcance	Fecha De Creación	Fecha De Ejecución	Resultado	Observaciones
1134	Actualización de FortiSIEM versión 7.3.0 a la 7.3.1	13/03/2025	14/03/2025	Exitoso	Se corrigieron errores en el FortiSIEM a través de la actualización.
1135	Reinicio controlado del nodo 1 del cluster de BD Oracle máquina virtual INR0276 para recuperar gestión de administración del servidor.	14/03/2025	14/03/2025	Exitoso	Se recupera la gestión de administración del servidor.

Tabla 33 Controles de cambio marzo

12. PLAN DE TRABAJO DE LOS PROXIMOS MESES

Se adjunta la tabla del plan de trabajo:

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
Se debe realizar mesa técnica conjunta entre ICETEX e INFOTIC para revisar las alternativas de solución respecto al licenciamiento de las herramientas de seguridad (perimetral y antivirus)	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se inicio la revisión del tema en los comités de pares que se inició el **13/02/2025** donde Se recomendó por parte de los especialistas de seguridad de INFOTIC a Icetex, la renovación de FortiSandbox en la nube y del WAF en la nube, con el fin de evitar el pago de años anteriores. Teniendo en cuenta que FortiSandbox ya no recibe actualizaciones. En cuanto al antivirus de Sophos, se encuentra pendiente la renovación para Windows 7 y Windows 2008, y se comentó por ICETEX que están considerando alternativas. **Avance 20/03/2025** ICETEX espera por parte de INFOTIC de una Propuesta de continuidad del licenciamiento vencido. Soporte de la sesión ver el acta: Acta pares de seguridad 13 20-03-2025.docx
Se debe realizar mesa técnica conjunta entre ICETEX e INFOTIC para revisar las lecciones aprendidas del último DRP y generar los planes de trabajo correspondientes antes de programar el próximo DRP debido a que la Oficina de Riesgos de ICETEX no dio por aceptado el segundo DRP realizado el 4 de noviembre de 2024.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se tiene pendiente la definición del alcance del próximo DRP, se define con ICETEX generar sesión ICETEX-INFOTIC-OPERADOR CLARO para retomar el tema con la opción del WAF virtual expuesto por INFOTIC y de Icetex incluir al ing. Carlos cruz quien es el supervisor encargado. Se iniciaron las reuniones semanales de seguimiento para coordinación del nuevo DRP la primera sesión se realizó el 25/02/2025, el primer DRP del 2025 se propone por parte de ICETEX para el día 02 de junio 2025.
Se debe realizar mesa técnica conjunta entre ICETEX e INFOTIC para revisar las alternativas de solución frente a la gestión de vulnerabilidades.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Con respecto a las vulnerabilidades de los Portales y seguridades a nivel de cabeceras está pendiente la respuesta a los especialistas de seguridad de INFOTIC del correo: de asunto: seguridades aplicadas desde el WAF—ambiente de pruebas. El ingeniero Jhon Pava reenviara el correo a ICETEX para retomar el tema e involucrar a los interesados.

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
				Se iniciará la discusión sobre el tema en los comités de pares de seguridad que se reactivarán en febrero. **Avance 13/02/2025:** Con respecto a lad vulnerabilidad de los Portales y seguridades a nivel de cabeceras está pendiente la respuesta a los especialistas de seguridad de INFOTIC del correo: de asunto: seguridades aplicadas desde el WAF—ambiente de pruebas. El ingeniero Jhon Pava reenviara el correo a ICETEX para retomar el tema e involucrar a los interesados. **Avance 20/03/2025:** Se acuerda que Infotic seguirá enviando los insumos para el comité de vulnerabilidad cada tres meses como se había definidos con los especialistas de seguridad el año anterior, se envía correo el día de hoy con las Presentaciones comités de Logs y Vulnerabilidades Cuarto Trimestre 2024 y Primer trimestre del 2025. Soporte de la sesión ver el acta Acta pares de seguridad 13 20-03-2025.docx
Se debe realizar mesa técnica conjunta entre ICETEX e INFOTIC para revisar los informes de Backup, su forma de presentación frente a las necesidades de ICETEX, los resultados periódicos de las pruebas de restauración y en caso de requerirse, realizar los planes de trabajo correspondientes.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Continua pendiente coordinar la sesión con los especialistas de ICETEX.
Actualización el sistema operativo LINUX de la versión 7.2 a la versión 7.9	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se está revisando desde INFOTIC el procedimiento y responsables para la realización de las actualizaciones de S.O. y pruebas de sobre los servidores del Portal de ICETEX.
Actualización de Liferay de la versión 7.3 a la 7.4	INFOTIC - ICETEX	01-dic-24	28-mar-25	Depende del numeral anterior y la actualización del soporte de liferay.
Verificar la configuración de los equipos de LAN y WAN que hace falta para el funcionamiento de IPv6.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se está haciendo seguimiento a estos temas de implementación de IPV6 en las sesiones señales que se comenzaron en febrero.
Instalación del canal Backup de Quibdó	INFOTIC - ICETEX	01-dic-24	28-feb-25	El canal de Backup de Quibdó, ya quedó instalado en el cuarto de comunicaciones del centro comercial el 27/02/2025, para habilitar el servicio en el local es necesario que Icetex solicite a la administración del CC Airplan la Cross-conexión desde el cuarto de equipos del CC hasta el cuarto de equipos de la agencia de Icetex. Ese cableado es exclusivo del CC. Se envía correo con esta solicitud a Icetex 24/02/2025, 27/02/2025 y 05/03/2025
Instalación del canal principal de Puerto Carreño	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se envía el 11/02/2025 la OFERTA PV-594-1 ICETEX - INFOTIC: instalación recursos tecnológicos sede Puerto Carreño, la instalación del canal es aprobado por ICETEX y se inicia el proceso de instalación el cual demora de 30 a 60 días.
Nueva configuración de SD WAN en triara	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se está trabajando en el tema hay que enviar una información y se acuerda que estos temas se van a

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
				trabajar en conjunto Networking y seguridad, es una mejora en la solución instalada. **Avance 20/03/2025:** Se está revisando internamente en Infotic los puntos del SDWAN , para dar respuesta a Icetex.
Gestión de la administración Azure nube	INFOTIC - ICETEX	01-dic-24	28-mar-25	Para efectos de poder avanzar en la este frente, se requiere la designación del personal ,por parte de ICETEX, para retomar las sesiones de trabajo y así, definir el plan a seguir.
Políticas e inventarios de las creaciones en la nube	INFOTIC - ICETEX	01-dic-24	28-mar-25	Para efectos de poder avanzar en la este frente, se requiere la designación del personal, por parte de ICETEX, para retomar las sesiones de trabajo y así, definir el plan a seguir.
Seguimiento a la adquisición de los Takedown por parte de ICETEX	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se envió un correo el 29 de noviembre 2024 notificando a ICETEX que no hay más Takedown disponibles, se espera respuesta de ICETEX. Claudia de Wexler envía a INFOTIC las alternativas para reportar estas páginas desde el ICETEX. **Avance 20/03/2025:** La herramienta de Monitoreo Axur incluye entre sus recursos, el servicio de Takedown. El paquete adquirido para este proyecto ofrecía 20 takedowns adicionales como valor agregado, pero no estaban incluidos en la oferta comercial inicial. En Octubre del 2024 la entidad a través del Ingeniero Hector Dussan, ha solicitado 6 takedowns adicionales que superan el límite establecido. Si se requieren más Takedowns el Icetex debe solicitar a INFOTIC la propuesta comercial, de lo contrario los sitios se podrán seguir reportando pero no bajando. Soporte de la sesión ver el acta: Acta pares de seguridad 13 20-03-2025.docx
Capacitación en seguridad al grupo de especialistas de seguridad del ICETEX	INFOTIC - ICETEX	01-dic-24	28-mar-25	**Avance 20/03/20** Se coordinó la fecha de capacitación con el Icetex el 03/04/2025. Soporte de la sesión ver el acta: Acta pares de seguridad 13 20-03-2025.docx
Monitoreo de los diferentes servicios realizados por el SOC. Revisión conjunta entre ICETEX – INFOTIC	INFOTIC - ICETEX	01-dic-24	28-mar-25	Realizar una revisión conjunta para determinar si los dispositivos se están monitoreando. **Avance 20/03/20** Infotic envió a Icetex el día de hoy un reporte con los dispositivos que se están monitoreando por el SOC para ser validados por el Icetex, correo de asunto: Dispositivos monitoreados FortiSIEM. Destinatarios: Raul Fernando Gutierrez Tecano <rfgutierrez@icetex.gov.co>; Victor Raul Bautista Galindo <VBautista@icetex.gov.co>; Sandra Milena Garcia Hernandez <sgarciah.cont@icetex.gov.co>; Carlos Alberto Roldan Rios <croldan.cont@icetex.gov.co> Soporte de la sesión ver el acta: Acta pares de seguridad 13 20-03-2025.docx
Revisar la parametrización de restricción y los problemas ocasionados a la conexión, para activar el agente de antivirus en las bases de datos.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Continua pendiente la sesión con los ingenieros de CLARO, INFOTIC e ICETEX para revisar y generar la solución.

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
Realizar mesa técnica entre ICETEX e INFOTIC para la revisión del alcance de Antivirus.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Perfiles de navegación se enviaron a Icetex y está pendiente de que confirmen si se van a aplicar. Jairo Acevedo INFOTIC, enviará el correo para retomar. Se iniciará la discusión sobre el tema en los comités de pares de seguridad que se reactivarán en febrero. **Avance 17/02/2025** : Perfiles de navegación se enviaron a Icetex y está pendiente de que confirmen si se van a aplicar. Jairo Acevedo INFOTIC, enviara el correo para retomar el tema **Avance 20/03/2025** Jairo Acevedo INFOTIC, envió el al ICETEX el correo para retomar el tema. Asunto: RE: Informe Filtrado web Sophos Destinatarios: Raul Fernando Gutierrez Tecano <rfgutierrez@icetex.gov.co>; Carlos Eduardo Cruz Gonzalez <ccruz@icetex.gov.co>; Sandra Milena Garcia Hernandez <sgarciah.cont@icetex.gov.co>; Juan Leonardo Berdella Sierra <jberdella@icetex.gov.co> Soporte de la sesión ver el acta: Acta pares de seguridad 13 20-03-2025.docx
Reunión técnica de aclaraciones del diagrama de red para la realización del DRP Link Minutograma tecnico DRP Noviembre actualizado.xlsx pestaña diagrama.	INFOTIC - ICETEX	01-dic-24	28-feb-25	Depende del nuevo alcance que se defina del DRP.
Realizar mesa de trabajo técnica en la cual se exponga claramente el cumplimiento de la implementación del canal DWDM de acuerdo con el anexo 2.1 punto 19 a satisfacción de ICETEX.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se realizó una sesión el 27/02/2025 personal de preventa de CLARO y Especialista de Networking de ICETEX donde se aclaran dudas frente al cumplimiento del canal de replicación frente al requerimiento contractual. Icetex acepta el canal de replicación entregado pero deja de condición que INFOTIC entregue la evidencia que permita comprobar el ancho de banda entregado **de** 2 GB.
Solicitud de instalación de (5) Internet para la gente en las Oficinas ICETEX de Manizales, Armenia, Cartagena, Sincelejo y Pasto.	INFOTIC - ICETEX	01-dic-24	28-mar-25	Se encuentra del lado comercial de INFOTIC la propuesta, una vez se tenga se enviará a ICETEX.
Solicitud de Monitoreo de la LAN de todas las sedes	INFOTIC -ICETEX	01-dic-24	28-mar-25	Se realizó el requerimiento al aliado de CLARO para dar respuesta a solicitud de ICETEX .

Tabla 34 Planes de trabajo

13. RECOMENDACIONES DEL CONTRATISTA AL ICETEX

Las siguientes son las recomendaciones para el mes de marzo 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

CIUDAD	Enlace - Tipo medio	INR	BW- Mínimo Requerido (MBPS)	Ancho de Banda actual	Ancho de Banda Ofrecido según Anexo 2.1
	Backup / IPVPN	INR0087	8	10	10
MEDELLIN	Principal / IPVPN	INR0133	63	100	100
	Backup / IPVPN	INR0132	15	20	20
APARTADO	Principal / IPVPN	INR0144	15	20	20
PEREIRA	Backup / IPVPN	INR0079	18	20	20
	Principal / IPVPN	INR0077	8	10	10
QUIBDO	Principal / IPVPN	INR0014	18	20	20
	Backup / IPVPN	0	8		
BARRANQUILLA	Principal / IPVPN	INR0103	63	100	100
	Backup / IPVPN	INR0100	15	20	20
CARTAGENA	Principal / IPVPN	INR0109	18	20	20
	Backup / IPVPN	INR0107	8	10	10
MONTERIA	Principal / IPVPN	INR0080	18	20	20
	Backup / IPVPN	INR0081	8	10	10
RIOHACHA	Principal / IPVPN	INR0164	18	20	20
	Backup / IPVPN	INR0162	8	10	10
SANTA MARTA	Principal / IPVPN	INR0154	18	20	20
	Backup / IPVPN	INR0152	8	10	10
SINCELEJO	Principal / IPVPN	INR0095	15	20	20
	Backup / IPVPN	INR0097	5	5	5
SAN ANDRES	Principal / IPVPN	INR0000367 INR0000369	8	8	8
BARRANCABERMEJA	Principal / IPVPN	0	18		20
SAN GIL	Principal / IPVPN	0	10		10
BUCARAMANGA	Principal / IPVPN	INR0062	26	30	30
	Backup / IPVPN	INR0061	12	20	20
CUCUTA	Principal / IPVPN	INR0044	18	20	20
	Backup / IPVPN	INR0047	8	10	10
VALLEDUPAR	Principal / IPVPN	INR0091	18	20	20
	Backup / IPVPN	INR0090	8	10	10
YOPAL	Principal / IPVPN	INR0121	18	20	20
	Backup / IPVPN	INR0123	8	10	8
ARAUCA	Principal / IPVPN	INR0110	15	20	15
CALI	Principal / IPVPN	INR0151	63	100	100
	Backup / IPVPN	INR0153	15	20	20
BUENAVENTURA	Principal / IPVPN	INR0051	10	10	10
MOCOA	Principal / IPVPN	INR0135	10	10	10
	Backup / Satelital	INR0136	5	5	5
PASTO	Principal / IPVPN	INR0130	18	20	20
	Backup / IPVPN	INR0131	8	10	10
POPAYAN	Principal / IPVPN	INR0035	20	20	20
	Backup / IPVPN	INR0032	5	5	5
TUMACO	Principal / IPVPN	INR0147	18	20	
WAN general (concentrador total red)	Principal /IPVPN	INR0266	1000	1000	1024
	Backup / IPVPN	INR0171	1000	1000	1024
Conectividad dedicada a funciones de réplica para eventos de DRP.	DWDM	INR0224	2000	2000	2048
Canal entre Sitio principal e ICETEX - Dirección General - Aguas	Principal /IPVPN	0	1000		1024
	Backup / IPVPN	0	600		600
BOGOTA ICETEX - Carrera 3 No. 18-32 - Sede Aguas - INTERNET bk	BOGOTA ICETEX - Carrera 3 No. 18-32 - Sede Aguas - INTERNET	INR0034	70	70	70
MEGACENTER MPLS BACKUP MEDELLIN	Conectividad brindada a través de la red MPLS, con acceso a los dos Datacenter	INR0177	500	500	500

CIUDAD	Enlace - Tipo medio	INR	BW- Mínimo Requerido (MBPS)	Ancho de Banda actual	Ancho de Banda Ofrecido según Anexo 2.1
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
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 35 Canales anchos de Banda actuales VrS anchos de banda ofrecidos

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

Se programó la primera capacitación en seguridad para el día **3 de abril de 2025**, en el horario de **2:00 p.m. a 4:00 p.m.** esta sesión es organizada por **ICETEX**, específicamente por el área de comunicaciones, y está dirigida a todos los usuarios de la entidad.

Se continuará con la programación de las (2) capacitaciones pendientes de acuerdo con la disponibilidad de ICETEX.

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 36 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 37 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 38 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 39 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.
- Seguimiento de la instalación de los canales MPLS de las nuevas sedes de Puerto Carreño y Puerto Inírida.

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

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

16.5. Integrador Nube

- 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 537-497, agregando un total de 40 políticas como parte del afinamiento de políticas con tráfico 0. 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 continúa con el mejoramiento del informe mensual conforme han surgido observaciones por parte de la entidad, en evaluación continua por parte de esta, para aceptación de los cambios que se realizan. Se ha actualizado el formato de informe mensual según las solicitudes realizadas por parte de la Entidad.

- Se está solicitando información al área de tecnología sobre los usuarios de directorio activo que utilizan la VPN SSL para conectarse a la red de ICETEX. Esto con el fin de poder implementar un doble factor de autenticación y así reforzar la seguridad en esta conexión.

17. ANEXOS

17.1. Almacenamiento

Backups Diarios:

- Backups diarios marzo 2025 (31 reportes) Backup Diario

Informe de Backups:

- Consolidado mensual Backup marzo Consolidado Diario de Backup marzo 2025.pdf
- Informe Backup marzo 2025 Informe Backups mes de Marzo 2025.pdf

17.2. Aplicaciones

- Informe actividades Módulos videoconferencia ICETEX Marzo 2025
  Informe actividades Módulos videoconferencia ICETEX Marzo 2025.pdf

- Informe mensual Administrador de Soluciones marzo 2025
  Informe Mensual InfoTIC Administrador de Soluciones Marzo 2025.pdf

- Informe mensual Administrador Web Master marzo 2025
  Informe Mensual InfoTIC Webmaster Marzo 2025.pdf

- Informe mensual Integrador Nube marzo 2025
  Informe Mensual InfoTIC Integrador de Nube Marzo2025.pdf

17.3. Bases De Datos

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

- Informe mensual Administrador de Bases de datos marzo 2025
  Informe Mensual InfoTIC DBA Marzo 2025.pdf

17.4. Ejecución Presupuestal

- Conciliación Marzo consolidado
  Conciliación Marzo_consolidado.xlsx

- Consolidado informe mensual especialistas marzo
  INFORME MENSUAL MARZO 2025.pdf

- Informe de Gestión Servicio marzo 2025
  Informe de Gestion Servicio Marzo 2025.pdf

17.5. Seguridad

- Informe Mensual MARCA-OSINT ICETEX marzo 2025
  250401 Informe Mensual MARCA-OSINT ICETEX Marzo 2025.pdf

- Informe Mensual Seguridad marzo 2025
  Reporte Mensual ICETEX_v2- MARZO.pdf

- Informe Mensual SOC - ICETEX marzo 2025
  250401 Informe Mensual SOC-TH ICETEX Marzo 2025.pdf

- Informe técnico análisis de vulnerabilidades ICETEX marzo 2025
  INFORME TÉCNICO AV_ABR_RETEST4_2025.pdf

- Reporte de IPS marzo 2025
  Reporte de IPS de Marzo_infotic_2025.pdf

Reporte total ataques recibidos-SIEM:

- Denegados marzo 1-15
  Denegados marzo 1-15.pdf

- Denegados marzo 16-31
  Denegados marzo 16-31.pdf

17.6. Soporte Y Monitoreo

Canales

- ANS marzo 2025 ANS_Marzo_2025.xlsx

- Informe mensual Administrador de Networking marzo 2025
  Informe Marzo 2025 Administrador Redes_v3.pdf

- Informe Mensual Disponibilidad marzo 2025
  Reporte Mensual Disponibilidad INFOTIC Marzo 2025.pdf

Graficas de consumo:

- Informe Mensual ALLOT marzo 2025
  Informe Mensual ALLOT marzo 2025.pdf

- Pruebas Nuevas de Saturación Canales marzo 2025
  Pruebas de Saturación Marzo

17.7. Data center Alterno:

Replicación

- Informe mensual replicación marzo 2025
  Informe mensual replicacion Marzo 2025.pdf
- Reportes diarios marzo 2025 (26 reportes)

Replicación

17.8. Data Center Principal:

- Reporte Monitoreo ICETEX marzo 2025-ELK
  Reporte Monitoreo ICETEX Marzo 2025-ELK.pdf

- Controles de Cambios Marzo
  Control de Cambios

Revisión técnica

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