INFORME DE ACTIVIDADES

CONTRATO NUMERO 2022-0792

diciembre 01 al 31 de 2024

1. Introducción 7
2. Objetivo del Informe 7
3. Alcance 8
4. AVANCE TÉCNICO 9
4.1. Conectividad Y Red de Comunicaciones 9
4.1.1. Canales instalados en el mes y entregables 10
4.1.2. Pruebas de Saturación Bidireccionales 12
4.2. Centro de Datos 13
4.2.1. Centro de Datos Principal 13
4.2.1.1. Aplicaciones 13
4.2.1.2. Bases de Datos 15
4.2.2. Centro de Datos Alterno 15
4.2.2.1. Hosting Virtual (IaaS) 15
4.2.2.2. Dataguard Bases de Datos Megacenter 18
4.2.2.3. Servicios de Housing – Datacenter Alterno 20
4.2.2.4. Servicios de DRP 20
4.3. Seguridad informática 21
4.3.1. Plataformas Administradas 22
4.3.1.1. FortiGate Triara 22
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 29
4.3.3.1.1. Categoría Seguridad 29

4.3.3.1.2. Categoría Disponibilidad *30*
4.3.3.1.3. Categoría Rendimiento *30*
4.3.3.1.4. Threat Hunting *31*
4.3.4. Análisis de Vulnerabilidades ICETEX *31*
4.3.4.1. Resumen de Vulnerabilidades 32
4.3.4.2. Conclusiones Vulnerabilidades 33
4.4. Servicios de nube *33*
5. GESTION FISICA DE LA EJECUCIÓN *33*
6. GESTION PRESUPUESTAL *35*
7. GESTION ADMINISTRATIVA *36*
8. Servicio De Colaboración *38*
8.1. Disponibilidad del servicio – sedes Regionales 39
8.2. Disponibilidad del servicio – sedes Bogotá (aguas - ángel) 39
8.3. Gestión de incidencias y requerimientos – sedes regionales 40
8.4. Gestión de incidencias y requerimientos – Bogotá (Aguas - Angel) 41
9. GESTION DE RIESGOS Y PROBLEMAS *44*
10. INDICADORES CLAVE DE DESEMPEÑO *46*
10.1. ANS por Disponibilidad de canales de comunicaciones: *46*
10.1.1. Canal de Replicación (Triara – Megacenter) 49
10.2. ANS por Disponibilidad de servidores: *50*
10.2.1. Disponibilidad TRIARA para los servicios de página web 51
10.2.2. Análisis componente Liferay Producción 59
10.2.3. Backup Servidores Triara 63
11. CONTROL DE CAMBIOS *65*
12. PLAN DE TRABAJO DE LOS PROXIMOS MESES *66*
14. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC *74*
14.1. Aumento de la capacidad de Ancho de Banda en algunas de las sedes de la Entidad *74*
14.2. Una capacitación al año de seguridad Informática y servicios conexos *78*
14.3. TB de capacidad de almacenamiento *78*
14.4. Se oferta Ítem de "Wifi" para la gente en 19 sedes *79*

15. CONCLUSIONES 80
16. PENDIENTES 82
16.1. Administrador WEB MASTER 82
16.2. Administrador Networking 82
16.3. Administrador Base de datos 82
16.4. Administrador de aplicaciones 83
16.5. Integrador Nube 83
16.6. Seguridad 83
17. ANEXOS 83
17.1. Almacenamiento 83
17.2. Aplicaciones 84
17.3. Bases De Datos 84
17.4. Ejecución Presupuestal 84
17.5. Seguridad 85
17.6. Soporte Y Monitoreo 85
17.7. Data center Alterno: 86
17.8. Data Center Principal: 86

INDICE DE TABLAS

TABLA 1 CASOS NETWORKING ATENDIDOS EN EL MES-FORMATO ICETEX 12
TABLA 2 CASOS ATENDIDOS 12
TABLA 3 CANALES PRUEBAS DE SATURACIÓN EJECUTADAS EN EL MES DE DICIEMBRE 12
TABLA 4 CANALES PENDIENTES PRUEBAS DE SATURACIÓN 13
TABLA 5 ACTIVIDADES DE DESPLIEGUES 14
TABLA 6 REQUERIMIENTOS DE VALIDACIÓN 14
TABLA 7 RESOLUCIÓN DE INCIDENTES 15
TABLA 8 SERVICIOS REPLICADOS – DATACENTER MEGACENTER 17
TABLA 9 TOP 05 MÁQUINAS MAYOR TASA DE TRANSFERENCIA 17
TABLA 10 TOP 05 MÁQUINAS MENOR TASA DE TRANSFERENCIA 18
TABLA 11 FECHAS CON MENOR REPLICACIÓN 18
TABLA 12 DISTRIBUCIÓN TRIMESTRAL DE REPLICACIÓN 18
TABLA 13 DISPONIBILIDAD DE SERVICIOS DE HOUSING – DATA CENTER ALTERNO 20
TABLA 14 TOP 10 DE LOS PORTALES MÁS UTILIZADOS 28
TABLA 15 INVENTARIO DE DISPOSITIVOS 31
TABLA 16 GRUPO ESPECIALISTAS 34
TABLA 17 GRUPO ADMINISTRATIVO 34
TABLA 18 ALIADOS PARA EL PROYECTO 35
TABLA 19 DISTRIBUCIÓN MÓDULOS DE VIDEOCONFERENCIA POR SEDE 39
TABLA 20 DISTRIBUCIÓN TRIMESTRAL DE REQUERIMIENTOS Y/O INCIDENTES 44
TABLA 21 NIVEL DE RIESGO 45
TABLA 22 GRADO DE RIESGO 45
TABLA 23 DISPONIBILIDAD DE CANALES 49
TABLA 24 DISPONIBILIDAD CANALES “INTERNET PARA LA GENTE” 49
TABLA 25 DISPONIBILIDAD CANALES “SDWAN” 49
TABLA 26 CÓDIGOS RELACIONADOS DISPONIBILIDAD SERVICIOS EN HOUSING – DATACENTER PRINCIPAL 51
TABLA 27 DISPOSITIVOS EN HOUSING – DATACENTER PRINCIPAL 51
TABLA 28 ACTUALIZACIÓN – ANÁLISIS COMPONENTE LIFERAY DICIEMBRE 62
TABLA 29 DISTRIBUCIÓN TRIMESTRAL DE ACCESO POR USUARIOS 62
TABLA 30 DISTRIBUCIÓN TRIMESTRAL DE BACKUP EJECUTADOS 65
TABLA 31 DISTRIBUCIÓN TRIMESTRAL DE BACKUP POR SERVICIOS 65
TABLA 32 CONTROLES DE CAMBIO DICIEMBRE 66
TABLA 33 PLANES DE TRABAJO 70
TABLA 34 CANALES ANCHOS DE BANDA ACTUALES VS ANCHOS DE BANDA OFRECIDOS 78
TABLA 35 CAPACIDADES DE ALMACENAMIENTO CONTRATADO 78
TABLA 36 CAPACIDADES DE ALMACENAMIENTO APROVISIONADO 79
TABLA 37 WIFI PARA LA GENTE INSTALADOS 79
TABLA 38 WIFI PARA LA GENTE PENDIENTES 80

INDICE DE ILUSTRACIONES

ILUSTRACIÓN 1 CASOS DEL PROYECTÓ GESTIONADOS ARANDA BD 15
ILUSTRACIÓN 2 REPORTES DE REPLICACIÓN SRM A SITIO ALTERNO – DICIEMBRE 16
ILUSTRACIÓN 3 EVIDENCIA DATAGUARD REPLICADO A MEGACENTER BD 20
ILUSTRACIÓN 4 CONSUMO CANAL MPLS 22
ILUSTRACIÓN 5 CONSUMO CANAL INTERNET SEDES 23
ILUSTRACIÓN 6 CONSUMO CANAL INTERNET DATA CENTER 23
ILUSTRACIÓN 7 FILTRADO – WEB – (FORTIGATE – TRIARA) 23
ILUSTRACIÓN 8 INSPECCIÓN – SSL – (FORTIGATE – TRIARA) 24
ILUSTRACIÓN 9 ANTIVIRUS Y ANTIMALWARE – PERIMETRAL (FORTIGATE – TRIARA) 24
ILUSTRACIÓN 10 CONSUMO CANAL MPLS AGUAS 25
ILUSTRACIÓN 11 CONSUMO CANAL MPLS MEDELLÍN 25
ILUSTRACIÓN 12 CONFIGURACIÓN FORTIWEB 26
ILUSTRACIÓN 13 ESTADO SEGURIDAD SOPHOS 27
ILUSTRACIÓN 14 EVIDENCIA GRÁFICA ESTADÍSTICAS DE PORTALES 27
ILUSTRACIÓN 15 TOTAL DE ALERTAS DE SEGURIDAD 30
ILUSTRACIÓN 16 TOTAL DE ALERTAS DE DISPONIBILIDAD 30
ILUSTRACIÓN 17 TOTAL DE ALERTAS DE DISPONIBILIDAD 30
ILUSTRACIÓN 18 CANTIDAD TOTAL DE HALLAZGOS IDENTIFICADOS 32
ILUSTRACIÓN 19 PAGO PARAFISCALES 35
ILUSTRACIÓN 20 EJECUCIÓN PRESUPUESTAL 36
ILUSTRACIÓN 21 DISPONIBILIDAD DE SERVICIO VIDEOCONFERENCIA SEDES REGIONALES – DICIEMBRE 2024 39
ILUSTRACIÓN 22 DISPONIBILIDAD DE SERVICIO VIDEOCONFERENCIA SEDES BOGOTÁ – DICIEMBRE 2024 40
ILUSTRACIÓN 23 INCIDENTES / REQUERIMIENTOS SEDES REGIONALES – DICIEMBRE 2024 40
ILUSTRACIÓN 24 PRUEBA DE FUNCIONAMIENTO SEDE CHAPINERO – NOVIEMBRE 2024 41
ILUSTRACIÓN 25 MÓDULO FUNCIONAL SALA 8VO PISO PRESIDENCIA – VISITA DICIEMBRE 2024 42
ILUSTRACIÓN 26 EVIDENCIA MÓDULO FUNCIONAL SEDE AGUAS 65, PISO 4 - VISITA DICIEMBRE 2024 42
ILUSTRACIÓN 27 EVIDENCIA MÓDULO FUNCIONAL SEDE AGUAS PISO 6 – VISITA DICIEMBRE 2024 43
ILUSTRACIÓN 28 EVIDENCIA MÓDULO FUNCIONAL SEDE AGUAS PISO 2 – VISITA DICIEMBRE 2024 43
ILUSTRACIÓN 29 VERIFICACIÓN MÓDULO SEDE ANGEL – PISO 2 – DICIEMBRE 2024 44
ILUSTRACIÓN 30 MATRIZ DE RIESGOS 46
ILUSTRACIÓN 31 UPTIME – PORTAL WEB WEB.ICETEX.GOV.CO 52
ILUSTRACIÓN 32 MÉTRICA DE VISITANTES PORTAL WEB WEB.ICETEX.GOV.CO 52
ILUSTRACIÓN 33 MÉTRICA DE USUARIO POR PAÍS - PORTAL WEB WEB.ICETEX.GOV.CO 53
ILUSTRACIÓN 34 NODO 1 – VISTA GENERAL – INR0243 53
ILUSTRACIÓN 35 NODO 1 CPU 54
ILUSTRACIÓN 36 NODO 1 MEMORIA 55
ILUSTRACIÓN 37 NODO 1 ALMACENAMIENTO 56
ILUSTRACIÓN 38 NODO 2 – VISTA GENERAL – INR0242 56
ILUSTRACIÓN 39 NODO 2 CPU 57
ILUSTRACIÓN 40 NODO 2 MEMORIA 58
ILUSTRACIÓN 41 NODO 2 ALMACENAMIENTO 58
ILUSTRACIÓN 42 EVIDENCIA BACKUP SERVIDORES RESUMEN BACKUPS Y SU ESTADO 64

RESUMEN EJECUTIVO

1. Introducción

Este informe contiene la información relacionada con las actividades ejecutadas por INFOTIC y sus aliados en el periodo comprendido entre el 01 al 31 de diciembre de 2024, para tal fin se cuenta con la información generada por el grupo de 10 especialistas y 3 profesionales administrativos con los cuales soportan y garantizan la atención de servicios especializados descritos en el alcance del proyecto como son:

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

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

- Firma del Acta de Inicio suscrita el 30 de diciembre del 2022, con fecha de iniciación del 19 de enero del 2023. Cumplida al 100%.
- Fase de Transición. Que comprendió desde el 19 de enero hasta el 31 de marzo de 2023. Esta fase se encuentra cumplida al 100%.
- Fase de operación. Inició desde el 1 de abril de 2023, cuenta con un avance en la ejecución del 58.33 % que representa los 21 meses que lleva dentro de la fase de Operación el proyecto.

El presente informe del mes de diciembre del 2024 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 diciembre de 2024, 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 diciembre conforme a los frentes definidos por el ICETEX, así:

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

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

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

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

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

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

4. AVANCE TÉCNICO

4.1. Conectividad Y Red de Comunicaciones

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

Respecto al canal de Backup que resta por instalar, se ha coordinado con el operador su instalación.

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

En cuanto a la gestión de vulnerabilidades, se cuenta con los resultados de los escaneos de vulnerabilidades realizados por ICETEX con la herramienta TENABLE y continúa ejecutando actividades de remediación para las vulnerabilidades de nivel medio y bajo.

Respecto a la implementación de IPv6, se ha trabajado con los especialistas de seguridad en las pruebas correspondientes, configurando las interfaces MPLS de los firewalls en Aguas, Triara y Megacenter para habilitar la comunicación entre sedes utilizando IPv6. Actualmente se tiene un 46% de avance en la implementación, el cual se puede evidenciar en el anexo Evidencias de implementación de IPv6.pdf. Evidencias implementacion IPv6.pdf

Se acuerda que en el mes de enero de 2025 se realice una reunión conjunta en el cual se establezcan las actividades de implementación de IPv6 para el año 2025, lo cual se evidencia también en este documento en el numeral **12. Plan de trabajo de los próximos meses**.

4.1.1. Canales instalados en el mes y entregables

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

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

Se solicitó por parte de ICETEX un canal de datos principal y backup para una nueva sede en la ciudad de Puerto Carreño -Vichada, INFOTIC envió la propuesta del canal el día 17 de diciembre y se encuentra en gestión del área comercial de INFOTIC de enviar el valor definitivo de los canales para poder llegar a un acuerdo con ICETEX y proceder con la instalación.

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

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

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

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

En conclusión, se tiene el 100.00% de los servicios de Internet para la gente.

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

En conclusión, los canales instalados cuentan con el 100.00% del ancho de banda contratado. A través de la herramienta SolarWinds se realiza el monitoreo mensual de disponibilidad de los canales y se genera el respectivo informe, el cual puede consultarse en el siguiente link Reporte Mensual Disponibilidad INFOTIC Diciembre 2024.pdf

Los casos atendidos durante el mes están disponibles en la tabla a continuación (en el link Aranda SERVICE DESK® Web Edition y se puede acceder a un mayor nivel de detalle a través de la herramienta Aranda:

FECHA Y HORA DEL REPORTE	LUGAR CON LA FALLA	Código de servicio	NÚMERO DE CASO	DURACIÓN HHH:mm:ss
27/12/2024	Internet/Redes >> Inc Falla Conectividad Red WIFI Corporativa Falla internet CEP Leticia	INR0000378	IM-290737-4-81438	4:00:00
26/12/2024	REVISIÓN CANAL TUNJA	INR0104	IM-290646-4-81412	4:00:00
26/12/2024	REVISION CANAL IBAGUE	INR0073	IM-290643-4-81410	4:00:00
26/12/2024	REVISION CANALES		IM-290637-4-81407	4:00:00
26/12/2024	Internet/Redes >> Inc Falla de Conectividad a la Red		IM-290622-4-81403	4:00:00
26/12/2024	Internet/Redes >> Inc Falla de Conectividad a la Red		IM-290591-4-81396	4:00:00
23/12/2024	Arauca >> Evento de afectación de servicio.	INR0110	IM-290382-4-81332	4:00:00
18/12/2024	Arauca >> Evento de afectación de servicio.	INR0110	IM-289981-4-81185	4:00:00
16/12/2024	Internet/Redes >> Inc Falla de Conectividad a la Red		IM-289692-4-81116	4:00:00
16/12/2024	Internet/Redes >> Inc Falla de Conectividad a la Red		IM-289675-4-81110	4:00:00
16/12/2024	Internet/Redes >> Inc Falla de Conectividad a la Red		IM-289672-4-81108	4:00:00
12/12/2024	Leticia >> Evento de afectación del servicio	INR0000378	IM-289403-4-81029	4:00:00
02/12/2024	Popayan >> Evento de afectación de servicio.		IM-288581-4-80838	4:00:00

02/12/2024	Internet/Redes >> Inc Degradación del Servicio-Falla Internet Leticia	INR0000378	IM-288527-4-80821	4:00:00

Tabla 1 Casos Networking atendidos en el mes-Formato ICETEX

Los casos atendidos durante el mes están disponibles en el Registro Aranda Diciembre 2024.xlsx

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 observó un aumento del 35.71% en los casos, atribuido a fallos en el servicio por parte del proveedor y a bloqueos de puertos en los equipos de la sede.

Mes	No. Casos
Diciembre	14
Noviembre	9

Tabla 2 Casos atendidos

4.1.2. Pruebas de Saturación Bidireccionales

Se continua con la realización de las pruebas de saturación bidireccionales y se pueden consultar los (05) canales donde se ejecutaron las pruebas en el mes de diciembre de 2024, los cuales relacionan en el siguiente link: Pruebas de saturación Diciembre

El cronograma de ejecución se envía semanalmente al ICETEX y en promedio se han ejecutado las pruebas de saturación en 7 sedes mensuales.

CIUDAD	Enlace - Tipo medio	Código Servicio	Fecha de Saturación
POPAYAN	Principal / IPVPN	INR0032	23/12/2024
BARRANQUILLA	Backup/ IPVPN	INR0103	23/12/2024
MANIZALES	Principal / IPVPN	INR0088	26/12/2024
MEDELLIN	Principal / IPVPN	INR0132	26/12/2024
MOCOA	Backup/ IPVPN	INR0136	26/12/2024

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

CIUDAD	Enlace - Tipo medio	Código Servicio
POPAYAN	Principal / IPVPN	INR0035
BOGOTA(AGUAS)	Principal / IPVPN	INR0036
BOGOTA(AGUAS)	Backup/ IPVPN	INR0037
BUENAVENTURA	Principal / IPVPN	INR0051
ARMENIA	Backup/ IPVPN	INR0072
ARMENIA	Principal / IPVPN	INR0074
IBAGUE	Backup/ IPVPN	INR0076
PEREIRA	Backup/ IPVPN	INR0077

MONTERIA	Backup/ IPVPN	INR0081
VILLAVICENCIO	Backup/ IPVPN	INR0084
MANIZALES	Backup/ IPVPN	INR0087
BARRANQUILLA	Backup/ IPVPN	INR0100
BARRANQUILLA	Principal / IPVPN	INR0103
CARTAGENA	Backup/ IPVPN	INR0107
CARTAGENA	Principal / IPVPN	INR0109
ARAUCA	Principal / IPVPN	INR0110
MEDELLIN	Backup/ IPVPN	INR0132
MOCOA	Backup/ IPVPN	INR0136
TUMACO	Principal / IPVPN	INR0147
SANTA MARTA	Backup/ IPVPN	INR0152
CALI	Backup/ IPVPN	INR0153
SANTA MARTA	Principal / IPVPN	INR0154
RIOHACHA	Principal / IPVPN	INR0162
BOGOTA(ANGEL)	Principal / IPVPN	INR0272
BOGOTA(ANGEL)	Principal / IPVPN	INR0273

Tabla 4 Canales pendientes pruebas de saturación

En resumen, se ha alcanzado un 61% de pruebas de saturación hasta el 31 de diciembre, se incluirá para el próximo mes la ejecución de una prueba adicional sobre el canal INR0000320 correspondiente al Internet Reverso para Portales (Salida de los portales https://portal.ICETEX.gov.co/portal y www.ICETEX.gov.co hacia internet en centro de cómputo principal) para verificar el aumento de ancho de banda aplicado al canal.

Sin embargo teniendo en cuenta que las convocatorias de ICETEX van hasta el 16 de febrero del 2025, se espera sólo que después de esta fecha sea aprobada la ejecución de estas pruebas de saturación porque este canal es el principal de salida a Internet y se corre el riesgo de afectar la operación al realizar esta saturación y por lo tanto se debe coordinar en un tiempo que no presente afectación del servicio.

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 veinticinco (25) casos registrados en la herramienta de mesa de servicio Aranda, clasificados en tres principales categorías: **actualización de aplicaciones**, **acceso al servidor de pruebas**, **publicación de URL y Actualización de Backend y frontend**.

A continuación, se detalla el alcance y resultados:

- **Tareas Relacionadas con Despliegues y Actualizaciones**

Se ejecutaron diez y siete (17) tareas relacionadas con la implementación, actualización y despliegue de componentes clave en las plataformas del Portal Transaccional y Comunidad ICETEX, asegurando su funcionalidad y mejorando el desempeño de los servicios tales como:

Despliegues de nuevos componentes	Actualizaciones de sistemas existentes	Mejoras específicas
Frontend y backend de ComunidadICETEXFront y ComunidadICETEXBackend.	➢ LoginPortalTransaccionalFront y LoginPortalTransaccionalApi. ➢ Backend y frontend de ComunidadICETEX en varias iteraciones. ➢ Frontend de Cuentas Abandonadas. ➢ Servicio WSApiServiceICETEX.	Redireccionamiento de la URL del formulario integral. Estas acciones fortalecieron la estabilidad de las aplicaciones y facilitaron nuevas funcionalidades alineadas con las necesidades institucionales.

Tabla 5 Actividades de despliegues

- **Requerimientos de validación y acceso**

Se gestionaron dos (2) requerimientos enfocados en habilitar acceso a servidores de pruebas y validar configuraciones críticas tales como:

Validación funcional	Accesos configurados
Revisión de la aplicación de Voto Electrónico y modificación de la cadena de conexión de su base de datos.	Servidores relacionados con el Portal Transaccional, Cargue de Archivos y Voto Electrónico. Estas configuraciones garantizaron la continuidad de pruebas y el soporte técnico.

Tabla 6 Requerimientos de validación

- **Redireccionamiento y resolución de errores**

Se abordaron ocho (8) incidentes críticos relacionados con la funcionalidad del portal:

Resolución de incidentes en el portal www.ICETEX.gov.co
➢ Error de autenticación en aplicaciones. ➢ Restablecimiento del servicio tras caída completa del portal principal del día 7 de diciembre (12m-1:30 pm) ➢ Estas acciones fueron restablecidas rápidamente con el fin de garantizar la operación del portal, asegurando un impacto mínimo para los usuarios finales.

Tabla 7 Resolución de incidentes

4.2.1.2. Bases de Datos

- La operación de las bases de ICETEX se mantuvo en óptimo rendimiento sin presentar indisponibilidad.
- Se atendieron los diferentes casos en los tiempos establecidos por los ANS de la entidad.
- Se atendieron casos fuera del soporte por la necesidad del cliente y por la situación coyuntural de la entidad con las tutelas presentadas.
- Disponibilidad de BD:

  Disponibilidad del Clusterware BD para el mes de diciembre 2024 100%:
- Casos Del proyectó Gestionados:

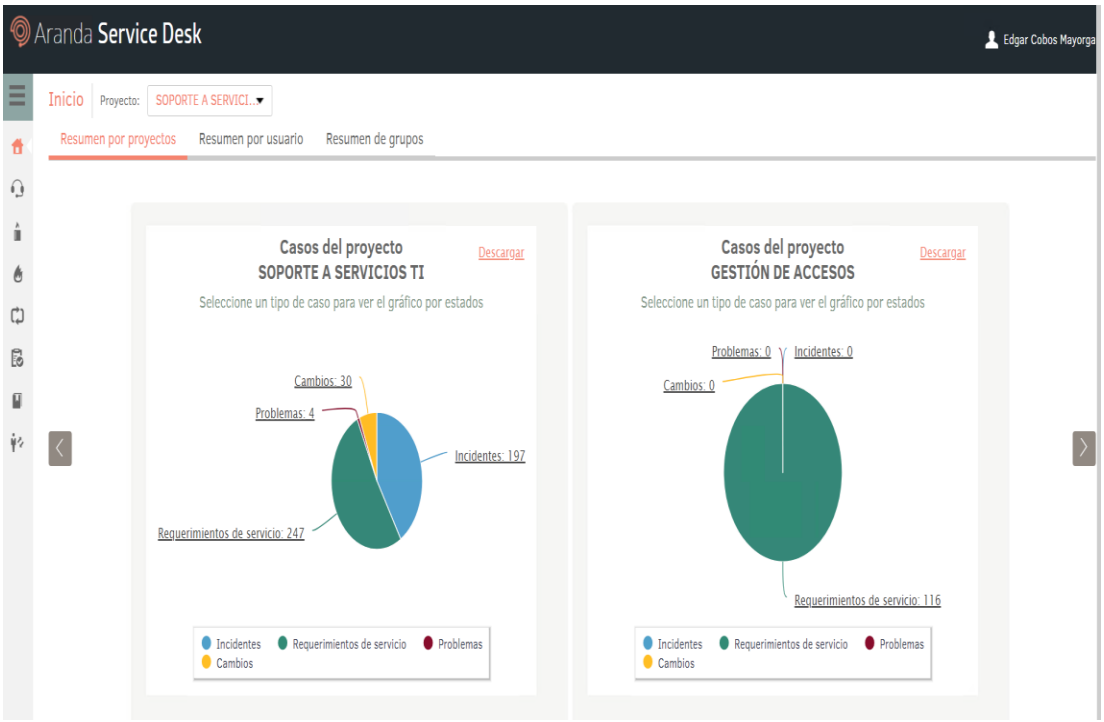


Ilustración 1 Casos Del proyectó Gestionados Aranda BD

4.2.2. Centro de Datos Alterno

4.2.2.1. Hosting Virtual (IaaS)

En el transcurso del mes de diciembre, se mantuvo en constante replicación las 13 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 diciembre 2024.pdf, cuyo reporte refleja el consolidado de los informes mensuales y que se están entregando periódicamente, a continuación se puede ver el último reporte diario del mes.

Claro

Site Recovery Manager - Estado Replicas INFOTIC

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

General

Name	Count
OK	13

Grupo de protección: PG_INFOTIC_7 (1)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0226_INFOTIC_REP	OK	5 of 5	Dec 3, 2024	29.91 MB	5 minutes

Grupo de protección: PG_INFOTIC_6 (2)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0228_INFOTIC_REP	OK	1 of 1	Dec 3, 2024	45.68 MB	1 hour
INR0229_INFOTIC_REP	OK	1 of 1	Dec 3, 2024	9.98 MB	1 hour

Grupo de protección: PG_INFOTIC_1 (2)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0233_INFOTIC_REP	OK	6 of 6	Dec 3, 2024	2.9 MB	30 minutes
INR0262_INFOTIC_REP	OK	1 of 1	Dec 3, 2024	7.16 MB	1 hour

Grupo de protección: PG_INFOTIC_5 (1)

VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0236_INFOTIC_REP	OK	2 of 2	Dec 3, 2024	53.76 MB	2 hours

Ilustración 2 Reportes de replicación SRM a Sitio Alterno – diciembre

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

#	INR Replicación	Host name	Servicio	Virtual Machine MEGACENTER
3	INR0206	Ictxsisgesapp	Sisgestion	INR0229_INFOTIC_REP
4	INR0220	ICETEXboglxorfeo1	ORFEO	INR0233_INFOTIC_REP
5	INR0219	ICETEXboglxorfeo2	ORFEO	INR0262_INFOTIC_REP
6	INR0208	ICTXBOGSRVPT1	Portal Transaccional	INR0236_INFOTIC_REP
7	INR0209	ICETEXbogbalserver1	Portal productivo (liferay)	INR0237_INFOTIC_REP
8	INR0210	ICETEXbogliferaynfs	Portal productivo (liferay)	INR0238_INFOTIC_REP
9	INR0217	ICETEXbogelasticserver1	Portal productivo (liferay)	INR0239_INFOTIC_REP
10	INR0218	ICETEXbogliferayserver1	Portal productivo (liferay)	INR0243_INFOTIC_REP
11	INR0215	ICETEXboglxdarumasrv1	DARUMA	INR0244_INFOTIC_REP
12	INR0213	ICETEXboglxdarumasrv2	DARUMA	INR0245_INFOTIC_REP
13	INR0214	ICETEXboglxxroad1	XROAD	INR0249_INFOTIC_REP

Tabla 8 Servicios replicados – Datacenter Megacenter

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

- Durante el mes de diciembre del 2024: se presentó el **Incremental Sync** en la maquina **INR0226_INFOTIC_REP** durante los días 01, 02 y 23.

- No se presenta información de los días 10, 14 y 17 de diciembre, esto debido a que la herramienta no genero el reporte, pero se realizó la replicación correspondiente.

- Se presenta el **Not active** en la maquina **INR0236_INFOTIC_REP** a partir del 13 al 31 de diciembre.

- Para el mes de diciembre se tiene el siguiente TOP 05 de las maquinas con mayor tasa de transferencia fueron:

INR	HOST NAME	MB
INR0239	icetexbogelasticserver1	17456.99
INR0238	icetexbogliferaynfs	15416.5
INR0243	icetexbogliferayserver1	5675.8
INR0226	icetexbogwsmira	4214.55
INR0229	ictxsisgesapp	1693.46

Tabla 9 TOP 05 máquinas mayor tasa de transferencia

- Para el mes de diciembre se tiene el siguiente TOP 05 de las maquinas con menor tasa de transferencia fueron:

INR	HOST NAME	MB
INR0245	icetexboglxdarumasrv2	102.21
INR0233	icetexboglxorfeo1	202.46

INR0262	icetexboglxorfeo2	248.41
INR0249	icetexboglxxroad1	631.41
INR0237	icetexbogbalserver1	719.94

Tabla 10 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
25-dic	Miércoles	390.03
30-dic	Lunes	399.69
28-dic	Sábado	488.47
27-dic	Viernes	498.39
26-dic	Jueves	513.55
24-dic	Martes	672.92
29-dic	Domingo	747.57

Tabla 11 Fechas con menor replicación

- Durante el último trimestre la replicación que se realiza entre el data center principal TRIARA y el data center alterno MEGACENTER tuvo un promedio de transferencia de data de 34466.55 MB y se presenta un aumento de 58.12% entre noviembre y diciembre, que equivale a 29534.78 MB.

Mes	MB replicadas
Octubre	31304.28
Noviembre	21280.29
Diciembre	50815.07

Tabla 12 Distribución trimestral de replicación

4.2.2.2. Dataguard Bases de Datos Megacenter

Durante el mes de diciembre de 2024 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 diciembre.pdf

10.1.18.120 - Conexión a Escritorio remoto

oracle@cxvodacontg011:~

```
[oracle@cxvodacontg011 ~]$ ps -fea|grep pmon
oracle    1171   634  0 14:50 pts/2    00:00:00 grep --color=auto pmon
grid      8054     1  0  2024 ?        00:03:14 asm_pmon_+ASM
oracle    8605     1  0  2024 ?        00:08:14 ora_pmon_ICTXCYCD
oracle    9044     1  0  2024 ?        00:09:04 ora_pmon_ICETEXD
oracle    9531     1  0  2024 ?        00:05:08 ora_pmon_LIFERAYD
oracle   10396     1  0  2024 ?        00:09:05 ora_pmon_APOTEOSD
oracle   10746     1  0  2024 ?        00:09:07 ora_pmon_APOTNEWD
oracle   11132     1  0  2024 ?        00:05:07 ora_pmon_VIGIADTG
oracle   11573     1  0  2024 ?        00:05:07 ora_pmon_LANDICTD
oracle   12543     1  0  2024 ?        00:09:00 ora_pmon_APLICATD
[oracle@cxvodacontg011 ~]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.4.0 Production on Tue Jan 7 14:50:50 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                77531                77531 31/12/2024 17:02 31/12/2024 17:02
         2                77518                77518 31/12/2024 14:40 31/12/2024 14:40

SQL>
```

10.1.18.120 - Conexión a Escritorio remoto

oracle@cxvodacontg011:~

```
[oracle@cxvodacontg011 ~]$ ps -fea|grep pmon
oracle    1171   634  0 14:50 pts/2    00:00:00 grep --color=auto pmon
grid      8054     1  0  2024 ?        00:03:14 asm_pmon_+ASM
oracle    8605     1  0  2024 ?        00:08:14 ora_pmon_ICTXCYCD
oracle    9044     1  0  2024 ?        00:09:04 ora_pmon_ICETEXD
oracle    9531     1  0  2024 ?        00:05:08 ora_pmon_LIFERAYD
oracle   10396     1  0  2024 ?        00:09:05 ora_pmon_APOTEOSD
oracle   10746     1  0  2024 ?        00:09:07 ora_pmon_APOTNEWD
oracle   11132     1  0  2024 ?        00:05:07 ora_pmon_VIGIADTG
oracle   11573     1  0  2024 ?        00:05:07 ora_pmon_LANDICTD
oracle   12543     1  0  2024 ?        00:09:00 ora_pmon_APLICATD
[oracle@cxvodacontg011 ~]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.4.0 Production on Tue Jan 7 14:50:50 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               77531               77531 31/12/2024 17:02 31/12/2024 17:02
         2               77518               77518 31/12/2024 14:40 31/12/2024 14:40

SQL>
```

Ilustración 3 Evidencia Dataguard replicado a Megacenter BD

Se generó la consulta de los archives recibidos y aplicados de la base de datos de ICTXCYCD a 31/12/2024 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 diciembre al 100%:

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

Tabla 13 Disponibilidad de Servicios de Housing – Data Center Alterno

4.2.2.4. Servicios de DRP

Se solicito al operador CLARO las fechas disponibles entre enero y febrero del 2025 para la realización del primer DRP del 2025.
A la fecha no se tiene respuesta para organizar con el ICETEX y los demás aliados la ejecución de las pruebas correspondientes.

4.3. Seguridad informática

Durante el mes de diciembre de 2024, se efectuaron las actividades relacionadas con la administración y gestión de la seguridad perimetral.

Dentro de los eventos del mes, se ha realizado apoyo en las pruebas de saturación que está realizando el proveedor CLARO en los canales de internet de las distintas sedes de la entidad. También se detectaron alertas de posibles ataques que no fueron detectados por el FortiWeb, se valida y en la mayoría de los casos se trató de direcciones IP maliciosas que intentaron realizar acciones que comprometieran alguna de las aplicaciones que protege el WAF, por lo cual se procede con su bloqueo en los firewalls de la entidad.

También se presentaron eventos en el WAF de tráfico permitido, lo cual se comprobó que este fue catalogado como un evento sustancial debido a que se presentó sobre una firma que aplicaba sobre Apache y la aplicación que se alertó no usa esta plataforma en su estructura, también se logró demostrar que los demás eventos detectados posteriormente fueron bloqueados por las firmas de seguridad del WAF configurada sobre la aplicación web. Estas actividades incluyeron la resolución de las alertas de tráfico de la red que genera el SOC, en el FortiSIEM se detectaron durante el mes múltiples eventos relacionados con tráfico permitido desde direcciones IP enmarcadas en listas de amenazas.

Se revisaron y analizaron los eventos para asegurar que no representaran una amenaza para la seguridad de la red y se tomaron las respectivas acciones para contener posibles amenazas. Se implementaron medidas de seguridad adicionales para prevenir accesos no autorizados y se realizó seguimiento continuo.

Dentro de los alertamientos recibidos durante el mes se presentaron eventos de escaneos e intentos de explotación de vulnerabilidades en las cuales se evidencio que algunos fueron eventos controlados por parte de ICETEX y de parte del aliado estratégico de INFOTIC y que no representaban riesgo real para la entidad. Los demás eventos se procedieron con el respectivo bloqueo en los dispositivos de seguridad perimetral.

Se atendieron los casos de Aranda donde se presentaron fallas de acceso a algunos servicios de la entidad y solicitudes de acceso a nuevos servicios donde se aplican cambios y configuraciones nuevas en los equipos de seguridad perimetral permitiendo estos accesos solicitados. También se presentaron solicitudes por parte de Networking para accesos a equipos de MPLS del ISP para que el mismo realizara pruebas de saturación de canales de las sedes remotas. En total se atendieron 31 casos de Aranda y 5 casos fuera de Aranda para un total de 36 casos durante el mes de diciembre los cuales se referencian en el ítem 12.2. Gestión de casos del Reporte mensual ICETEX_V2 diciembre 2024.pdf

En el mes de diciembre, se actualizaron los certificados SSL de los sitios web de la entidad y algunos

servicios como VPN, por parte de seguridad, se ha acompañado en estos cambios de certificados y se han cambiado de manera oportuna para evitar brechas de seguridad o indisponibilidad de alguno de los servicios que se prestan.

Estos certificados permiten que los sitios web de la entidad y demás servicios brinden seguridad a los usuarios que los utilizan y que las plataformas cuenten con unos niveles de seguridad óptimos que permitan asegurar que la información que pasa por estos canales cumpla con los protocolos de seguridad de manera eficaz.

Se requiere la validación del área de riesgos para avanzar en la implementación, la cual debe realizarse de manera segmentada por áreas para optimizar el soporte y adaptarse a las necesidades específicas de cada usuario.

4.3.1. Plataformas Administradas

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

- FortiWeb
- FortiSandbox
- FortiGate
- Sophos Endpoint
- FortiSIEM

4.3.1.1. FortiGate Triara

A nivel de sistema, el firewall de Triara (FortiGate 1800F), no presenta afectaciones en cuanto a licenciamiento o performance; actualmente se encuentra en la versión de FortiOS 7.2.9, la cual es una de las versiones reciente más estables.

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

En cuanto a las Interfases, Se observa el tráfico hacia la MPLS en promedio 3.85 Mbps [INR0185 CLARO(MPLS_DC)] en la última semana, tal como se puede ver en la Ilustración.

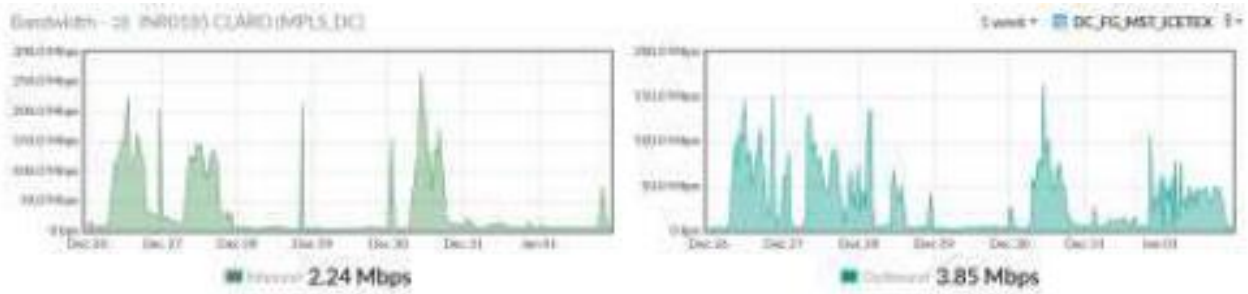


Ilustración 4 Consumo Canal MPLS

Se observa en la Ilustración 6, se observa tráfico hacia la WAN-SEDES-ICETEX [INR0264 (INTE_SEDES_ICTX)] en promedio 547.80 kbps en la última semana.

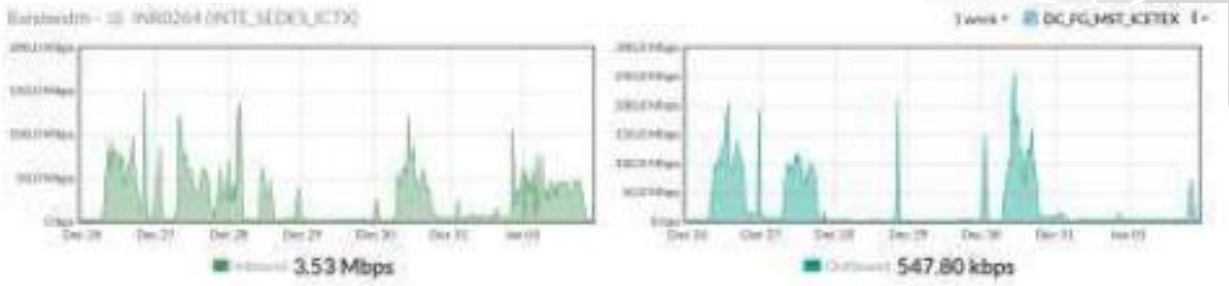


Ilustración 5 Consumo Canal Internet Sedes

En la Ilustración 7, se observa tráfico hacia la INTENET DATACENTER [INTERNET_DC_INR0000320 (Inet_claro)] en promedio 16.21 Mbps en la última semana.

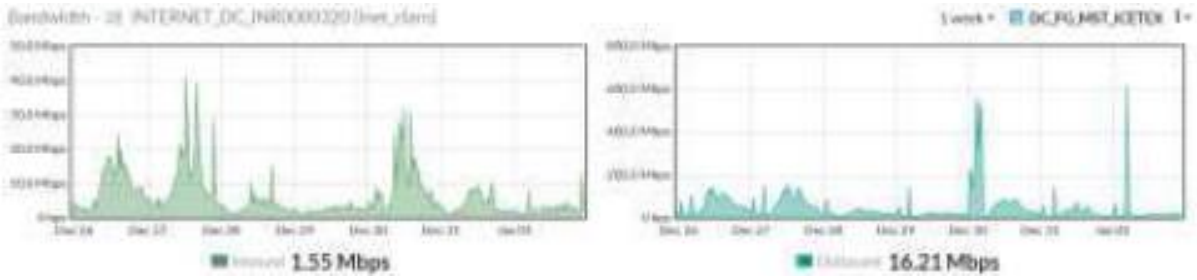


Ilustración 6 Consumo Canal Internet Data Center

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
Navegacionpcs_Comware	Perfil con restricciones	2
Navegacionpcs_Comware_con_redes	Perfil con restricciones	2
WF-Aerolineas	RF-186510-7-9612 24/03/2022	0
WF-Avanzado	Perfil para FSSO Navegación Avanzada	30
WF-Comunicaciones	Perfil para FSSO comunicaciones	2
WF-General	Perfil para todos	4
WF-General_Sedes	Perfil para todos	1
WF-Redessociales	Perfil para FSSO Navegación Avanzada	0
WF-Tesoreria	Perfil con restricciones específicas por auditoria	4
WF-Tesoreria_Sala_Segura	Permisos para equipos de Sala Segura de Tesoreria	0
WF-VIP	Perfil para FSSO Navegación VIP	13
WF-webtransfer	Perfil para FSSO Navegación Avanzada	1
default	Perfil con las mínimas restricciones	3
wifi-default	Perfil de FULL acceso para pruebas	1

Ilustración 7 Filtrado – WEB – (FortiGate – Triara)

Name	Comments	Ref
Prueba certificate-inspection	Read-only SSL handshake inspection profile.	13
Pruebas liferay		0
certificate-inspection	Read-only SSL handshake inspection profile.	373
certificate-inspection_ICETEX	SSL para BUS de servicios	29
custom-deep-inspection	Customizable deep inspection profile.	0
deep-inspection	Read-only deep inspection profile.	0
no-inspection	Read-only profile that does no inspection.	200

Ilustración 8 Inspección – SSL – (FortiGate – Triara)

Name	Comments	Ref
AV-FSB	HTTP,SMTP FULL FSB	37
AV-FTP	FTP FULL FSB	0
AV-HTTP	HTTP con FSB	26
AV-HTTP&CIFS	HTTP,CIFS con FSB	4
AV-HTTP_Mobile	HTTP, mobile con FSB	0
AV-SMTP	SMTP FULL FSB	1
default	ALL con FSB	44
ICETEX		50
Prueba	ALL con FSB	0
prueba2		60
wifi-default	ALL monitoreo sin FSB	1

Ilustración 9 Antivirus y Antimalware – Perimetral (FortiGate – Triara)

4.3.1.2. FortiGate Aguas

A nivel de sistema, el firewall de Aguas (FortiGate 600F), no presenta afectaciones en cuanto a licenciamiento o performance; actualmente se encuentra en la versión de FortiOS 7.2.9, la cual es una de las versiones reciente más estables.

En cuanto a las Interfases, se observa en la Ilustración 10 el tráfico hacia la MPLS de la sede de Aguas con un promedio de 3.08 Mbps (Port7) en la última semana.

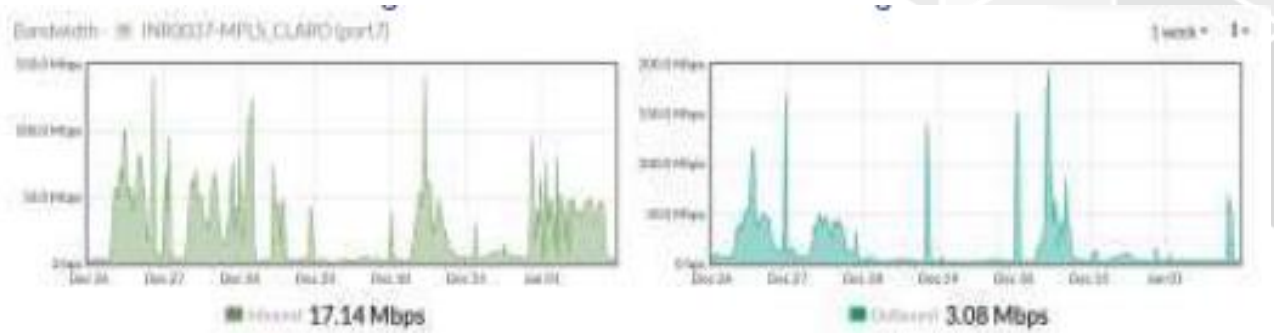


Ilustración 10 Consumo Canal MPLS Aguas

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 7.2.9, 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.

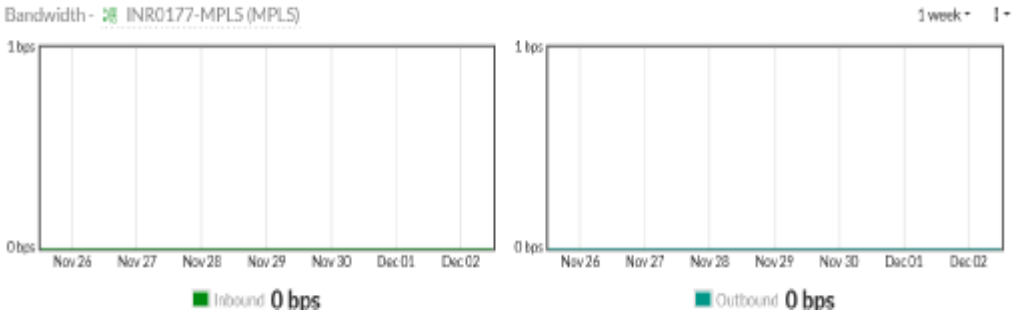


Ilustración 11 Consumo Canal MPLS Medellín

4.3.1.4. FortiWeb 2000F

A nivel de sistema del FortiWeb en la siguiente gráfica se presenta la configuración actual y su versión de Firmware. La versión de firmware está en el 7.4.4, la cual es una de las versiones actuales y más estables, en referencia con las buenas prácticas dadas por el fabricante FORTINET.

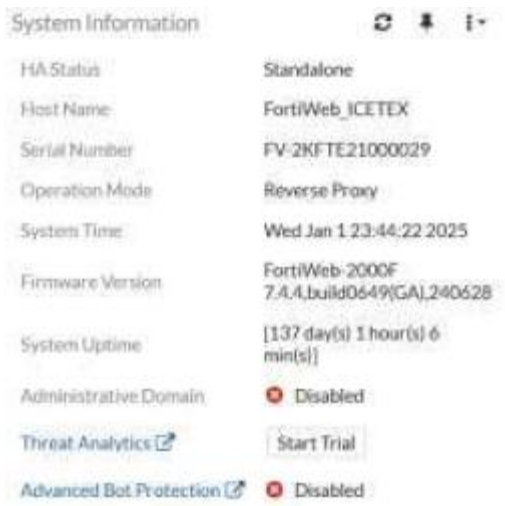


Ilustración 12 Configuración FortiWeb

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 versión 7.4.4 la cual es una de las versiones actuales más estables. Sin embargo, cabe aclarar que, a nivel de licenciamiento, este equipo no tiene un licenciamiento vigente en este momento. Se debe realizar mesa técnica conjunta entre ICETEX e INFOTIC para revisar las alternativas de solución respecto al licenciamiento.

4.3.1.6. FortiSandBox

A nivel de sistema, el Sandbox (FortiSandBox 1000D) muestra su configuración actual y su versión de firmware que actualmente se encuentra en la versión 3.2.4 siendo esta la última versión disponible para este dispositivo, ya que está en proceso de EOL (término empleado por el fabricante para describir un producto que pronto será reemplazado por una nueva generación de tecnología).

4.3.1.7. Sophos EndPoint

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

Se ha informado a ICETEX que en la gestión de la consola de antivirus Sophos se evidenciaba una notificación de caducidad de la licencia de mayor compatibilidad con Windows, en este momento ya se encuentra caducada desde el 30 de agosto de 2024. Esta licencia permite la compatibilidad con versiones del sistema operativo Windows (Server 2008, 2012, Windows 7 y Windows 8, etc.) con el agente de antivirus de Sophos.
Se alertó que la falta de este licenciamiento provoca incompatibilidad y falta de elementos de protección que brinda el agente Sophos a estos sistemas operativos y que representan una brecha de seguridad importante, desde ICETEX se encuentran en gestión el proceso de la renovación de este componente. Se debe realizar mesa técnica conjunta entre ICETEX e INFOTIC para revisar las

alternativas de solución respecto al licenciamiento.

Ilustración 13 Estado Seguridad Sophos

4.3.2. Estadística de Portales

Durante el mes de diciembre 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 diciembre 2024.pdf]

Como se puede ver en la Ilustración 15, en el periodo de tiempo analizado se presenta un promedio de 300 GB de tráfico general hacia los portales protegidos por el FortiWeb Apps Nuevas donde el portal de web.ICETEX.gov.co y www.ICETEX.gov.co, lo cual es un comportamiento normal para este tipo de transacciones de acuerdo con la actividad de los usuarios y las convocatorias vigentes.

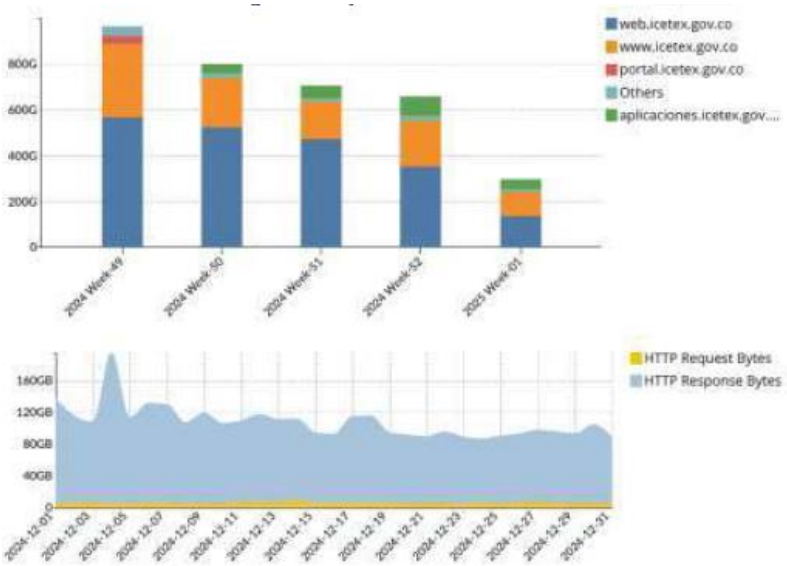


Ilustración 14 Evidencia Gráfica Estadísticas de Portales

Adicional en la Tabla 13, podemos ver los 10 portales más utilizados de acuerdo con la cantidad de solicitudes, siendo web.ICETEX.gov.co el primero de este top:

5. TOP 10 PORTALES MÁS UTILIZADOS

Tabla 1 Top 10 Portales más utilizados

#	HTTP Host	HTTP Request Bytes	HTTP Response Bytes
1	web.icetex.gov.co	102.22 GB	1.87 TB
2	www.icetex.gov.co	22.78 GB	940.31 GB
3	aplicaciones.icetex.gov.co	37.38 GB	221.79 GB
4	portal.icetex.gov.co	1.66 GB	78.09 GB
5	comunidad.icetex.gov.co	238.60 MB	23.87 GB
6	web.icetex.gov.co:443	1.67 MB	137.50 MB
7	192.168.91.27	1.13 MB	67.40 MB
8	www.icetex.gov.co:443	4.37 MB	40.98 MB
9	186.84.73.154	242.85 KB	30.13 MB
10	186.84.73.158	141.52 KB	26.63 MB

Tabla 14 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 diciembre 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 [250102 Informe Mensual SOC-TH ICETEX Diciembre 2024.pdf]

El sistema FortiSIEM ofrece más de 100 tableros de monitoreo, incluyendo tableros personalizados que permiten a ICETEX visualizar en tiempo real las amenazas detectadas, los ataques mitigados y los ataques más frecuentes, lo que mejora significativamente la gestión de la seguridad. Esta capacidad de personalización y seguimiento es fundamental para fortalecer la defensa ante ciberamenazas.

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

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

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

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

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

Indicadores de compromiso (IOC):

- **IOC – Malware DOMINIOS:3898**
- **IOC – Malware IPs:5276**
- **IOC – Malware HASH:1606**
- **IOC – Malware URL:780**

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 250102 Informe Mensual SOC-TH ICETEX Diciembre 2024.pdf se ven las alertas generadas a lo largo del periodo monitoreado, dichas alertas se clasifican en 3 categorías principales de monitoreo, las cuales corresponden a Seguridad, Disponibilidad y Rendimiento,a continuación, se presenta un resumen de cada una de ellas, sin embargo, el detalle del tratamiento que se realizó a cada uno de los casos se debe revisar en el Informe mencionado anteriormente.

4.3.3.1.1. Categoría Seguridad

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

Severity	Cantidad de ...
Medium	4,304
High	605
Low	194

Ilustración 15 Total de alertas de seguridad

Durante el período evaluado se presentaron 605 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.

4.3.3.1.2. Categoría Disponibilidad

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

Severity	Cantidad de ...
Medium	67,378
Low	944
High	84

Ilustración 16 Total de alertas de disponibilidad

4.3.3.1.3. Categoría Rendimiento

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

Severity	Cantidad de ...
Medium	6,324
High	1,442

Ilustración 17 Total de alertas de Disponibilidad

4.3.3.1.4. Threat Hunting

Se lleva a cabo el proceso de "Threat Hunting" de manera proactiva mediante la realización de boletines de ciber amenazas y la utilización de la plataforma MISP (Malware Information Sharon Platform) del First (Forum of Incident Response Team).

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

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

4.3.4. Análisis de Vulnerabilidades ICETEX

Durante este mes, se logró completar el análisis de todos los activos tecnológicos, alcanzando una cobertura total del 100%. Esto permitió identificar que, aunque persisten vulnerabilidades importantes sin resolver, se observó una mejora parcial en la implementación de cifrados seguros. El análisis incluyó la evaluación detallada de servicios críticos, destacando problemas en criptografía débil y configuraciones inseguras, lo que llevó a clasificar el nivel de riesgo actual como alto. La información generada contribuirá a priorizar la mitigación de los riesgos más críticos y fortalecer la seguridad general de la entidad.

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

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

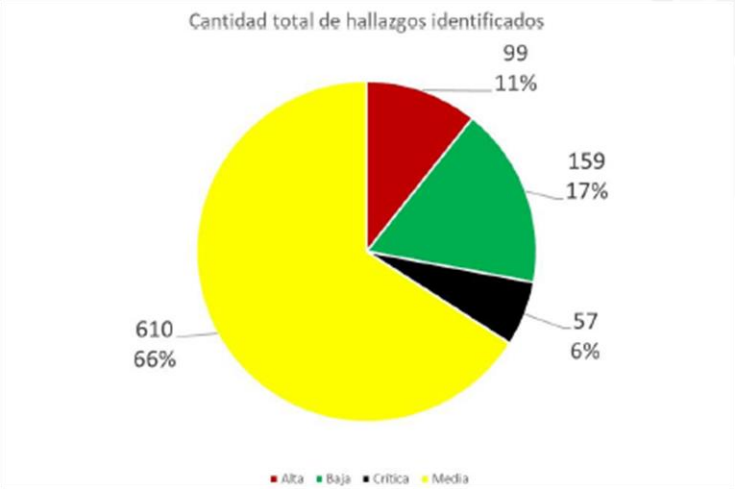


Ilustración 18 Cantidad Total de Hallazgos identificados

4.3.4.1. Resumen de Vulnerabilidades

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

Categorías de Mayor Riesgo

Vulnerabilidades de Sistemas Operativos y Servidores

- Windows Server 2003 obsoleto
- IIS 6.0 no soportado
- Sistemas operativos desactualizados
- SMBv1 habilitado

Vulnerabilidades de Aplicaciones

- Apache Tomcat obsoleto y con múltiples fallos
- Liferay Portal con Remote Code Execution
- PHP versiones no soportadas

Riesgos de Acceso Remoto

- BlueKeep (RDP Remote Code Execution)
- Microsoft Message Queue Server RCE
- SMB NULL Session Authentication

Debilidades Criptográficas

- SSL versiones 2 y 3 activas
- Certificados con algoritmos de hash débiles
- Cipher suites de seguridad media

4.3.4.2. Conclusiones Vulnerabilidades

- Riesgo Alto: Las vulnerabilidades críticas encontradas (como Ghostcat, BlueKeep, EternalBlue, y las versiones obsoletas de Apache Tomcat, IIS, PHP, Windows, y SQL Server) exponen los sistemas a graves riesgos de explotación remota y ejecución de código arbitrario. Estos fallos deben ser corregidos con urgencia para evitar la explotación por actores maliciosos.

- Impacto potencial: La explotación exitosa de estas vulnerabilidades puede permitir la ejecución remota de código, escalación de privilegios, y acceso no autorizado a sistemas y bases de datos sensibles. Los impactos pueden incluir la pérdida de datos, acceso no autorizado a la infraestructura, y posibles interrupciones del servicio, cabe recalcar que se cuenta con un monitoreo 7*24 por parte del SOC donde se identifica los comportamientos y se mitigan los riesgos.
- Recomendación de Remediación: Es recomendable que todas las vulnerabilidades sean tratadas lo más rápido posible, comenzando con las más críticas (como las de ejecución remota de código) y avanzando hacia aquellas que involucran configuraciones desactualizadas. Esto incluye aplicar parches de seguridad disponibles y actualizar todos los sistemas a versiones compatibles y soportadas. Además, deshabilitar los protocolos obsoletos y reforzar las políticas de seguridad ayudará a mitigar riesgos adicionales.

4.4. Servicios de nube

El proceso de integración en la nube se está trabajando en conjunto entre INFOTIC e ICETEX para actualizar los procedimientos para la creación, actualización, mantenimiento, soporte y eliminación de los elementos que se crean en la nube, y todo esto asociarlo a los TAGs que se deben tener en cuenta en el tema de administración de este tipo de componentes tecnológicos. También se está gestionando la actualización del inventario de aplicaciones para determinar cuáles pueden pasar a la nube para optimizar recursos en el ICETEX.

5. GESTION FISICA DE LA EJECUCIÓN

El contrato 2022-0792 con fecha de perfeccionamiento del acta de inicio del 30 de diciembre del 2022, donde se establece un plazo del contrato de 39 meses, el cual se compone de una fase de transición de 03 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 01 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 diciembre del 2024 del proyecto, se encuentra en la fase de operación de

los servicios contemplados en el alcance llevando ejecutados 19 meses que equivale al 52.78% 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 diciembre del 2024:

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

Tabla 16 Grupo especialistas

El siguiente es el grupo administrativo que estuvo en el desarrollo de la operación del mes de diciembre del 2024:

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 diciembre del 2024:

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

Los siguientes son los pagos de parafiscales del grupo de trabajo:

- Grupo INFOTIC

aportes en línea

Resumen de Pago por Administradora

DATOS GENERALES DEL APORTANTE

Identificación	dv	Razon Social	Clase Aportante	Sucursal Principal	Direccion	Ciudad-Departamento	Teléfono	Exonerado SENA e ICBF
NIT 900068796	1	INFOTIC S.A	B - MENOS DE 200 COTIZANTES	BOGOTA	CL 93 B N° 13 - 44 PISO 2	BOGOTA-BOGOTA D.E.	7466000	Si

DATOS GENERALES DE LA LIQUIDACION

Periodo		Clave		Tipo	Fecha		Pago		
Pensión	Salud	Pago	Plantilla	Plantilla	Limite	Pago	Banco	Dias Mora	Valor
2024-12	2025-01	1170424780	9479847274	E	2025/01/24	2025/01/03	BANCO DE OCCIDENTE	0	$4,509,600

RESUMEN DE PAGO

RIESGO	CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES	VALOR A PAGAR
AFP (ADMINISTRADORAS: 2)				3	$2,993,300	$0	$0	$2,993,300
COLPENSIONES	25-14	900,336,004	7	2	$2,465,300	$0	$0	$2,465,300
PORVENIR	230301	800,224,808	8	1	$528,000	$0	$0	$528,000
ARL (ADMINISTRADORAS: 1)				3	$92,100	$0	$0	$92,100
POSITIVA COMPAÑIA DE SEGUROS	14-23	860,011,153	6	3	$92,100	$0	$0	$92,100
CCF (ADMINISTRADORAS: 1)				3	$712,100	$0	$0	$712,100
COMFACUNDI	CCF26	860,045,904	7	3	$712,100	$0	$0	$712,100
EPS (ADMINISTRADORAS: 3)				3	$712,100	$0	$0	$712,100
COMPENSAR	EPS008	860,066,942	7	1	$360,000	$0	$0	$360,000
NUEVA E.P.S.	EPS037	900,156,264	2	1	$220,100	$0	$0	$220,100
SANITAS	EPS005	800,251,440	6	1	$132,000	$0	$0	$132,000
TOTAL				**3**	**$4,509,600**	**$0**	**$0**	**$4,509,600**

Ilustración 19 Pago Parafiscales

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	
CONCEPTO	***VALOR***
VALOR INICIAL DEL CONTRATO	***$ 31.398.996.857,96***
VALOR VIGENCIA 2023	*$7.856.847.477*
VALOR EJECUTADO 2023	*$5.550.607.398,60*
VALOR BOLSA VIGENCIA 2023	*$360.000.000*
VALOR BOLSA EJECUTADO 2023	*$0*
VALOR VIGENCIA 2024	*$10.475.796.636*
VALOR EJECUTADO 2024	*$8.116.163.716,21*
VALOR BOLSA VIGENCIA 2024	*$480.000.000*
VALOR BOLSA EJECUTADO 2024	*$0*

EJECUCIÓN PRESUPUESTAL						
CONCEPTO						***VALOR***
VALOR ADICIONES *(si aplica, especificar el o los números de adición)*						*$ 0,00*
VALOR REDUCCIÓN *(si aplica)*						*$ 0,00*
VALOR POR OTRO CONCEPTO *(si aplica)*						*$ 0,00*
VALOR TOTAL DEL CONTRATO						***$ 31.398.996.857,96***
VALOR PAGADO						
Pago No. 1 -	mes:	Abril	de	2023	$ 537.090.736,00	
Pago No. 2 -	mes:	Mayo	de	2023	$ 544.104.546,00	
Pago No. 3 -	mes:	Junio	de	2023	$ 596.978.314,00	
Pago No. 4 -	mes:	Julio	de	2023	$ 624.431.841,60	
Pago No. 5 -	mes:	Agosto	de	2023	$ 650.825.466,00	
Pago No. 6 -	mes:	Septiembre	de	2023	$ 661.959.450,00	
Pago No. 7 -	mes:	Octubre	de	2023	$ 641.792.285,00	
Pago No. 8 -	mes:	Noviembre	de	2023	$ 630.348.564,00	
Pago No. 9 -	mes:	Diciembre	de	2023	$ 663.076.196,00	
Pago No. 10 -	mes:	Enero	de	2024	$ 681.934.328,00	$13.666.771.114,81
Pago No. 11 -	mes:	Febrero	de	2024	$ 732.950.101,55	
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	
En validación - Pago No. 21 -	mes:	Diciembre	de	2024	$ 807,011,747.83	
VALOR CAUSADO QUE NO SE HA PAGADO *(valor a pagar factura)* *						$ 807,011,747.83
VALOR TOTAL EJECUTADO *(valor pagado + valor causado no pagado)*						$14,473,782,862.64
SALDO DEL CONTRATO *(valor total del contrato – valor total ejecutado)*						$16,925,213,995.32
PORCENTAJE DE EJECUCIÓN						46.09%
** 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**						

Ilustración 20 Ejecución Presupuestal

7. GESTION ADMINISTRATIVA

7.1. Profesionales

El detalle de las actividades realizadas por cada uno de los ingenieros especialistas se puede consultar en el siguiente link : Informe mensual especialistas diciembre 2024.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	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	1
SEDES REGIONALES				
4	Sala de video conferencia o	Bogotá - Chapinero	Calle 57 No. 8-69 Local	1

ÍTEMS	SERVICIO	CIUDAD	DIRECCIÓN	CANTIDAD
	sala virtual (Tamaño 55")		46 - 48 y 50	
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 19 Distribución módulos de videoconferencia por sede

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

8.1. Disponibilidad del servicio – sedes Regionales

En la verificación realizada para el pasado mes de diciembre del 2024 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.

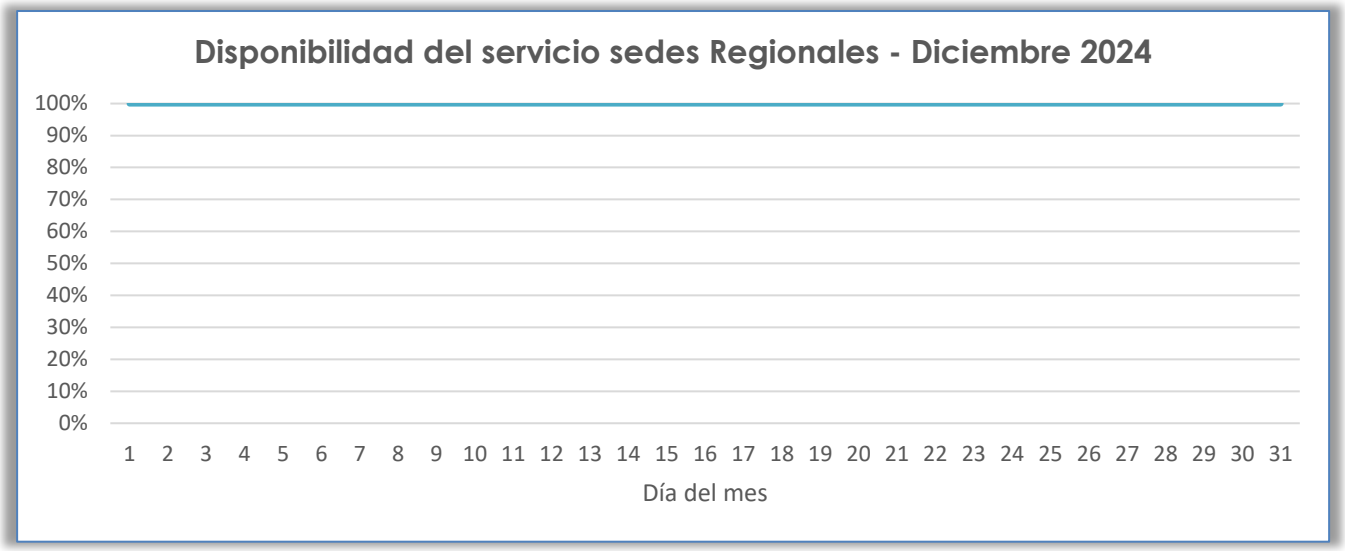


Ilustración 21 Disponibilidad de servicio videoconferencia sedes regionales – diciembre 2024

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

En la verificación realizada en el mes de diciembre del 2024 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.

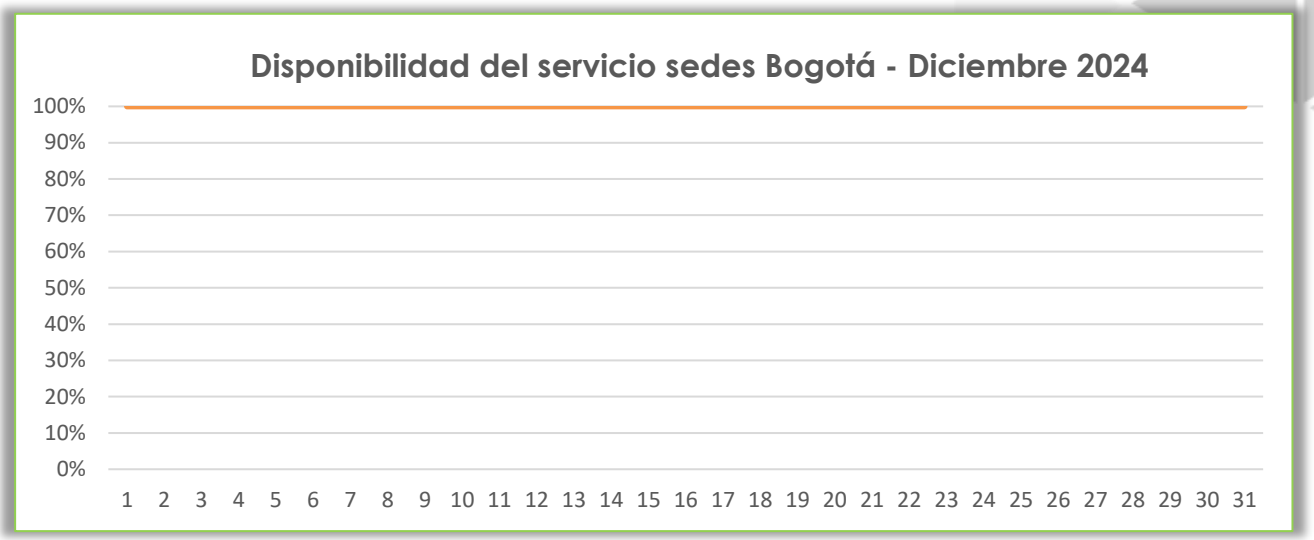


Ilustración 22 Disponibilidad de servicio videoconferencia sedes Bogotá – diciembre 2024

8.3. Gestión de incidencias y requerimientos – sedes regionales

Para el periodo de diciembre, comprendido entre el 1 y el 31 del mes, en las sedes Regionales (Cali, Barranquilla, Bucaramanga y Medellín) no se generaron solicitudes especiales que requirieran atención y gestión de soporte técnico, tampoco se reportaron incidencias a nivel del servicio para estas sedes durante el periodo, sin embargo, se generaron requerimientos para gestionar permisos de acceso con el fin de realizar mantenimientos preventivos en los módulos que se encuentran en las sedes regionales, adicional, como cada periodo, se contó con la disponibilidad para recibir cualquier solicitud de soporte (Incidencia/requerimiento) o apoyo concerniente a la solución de videoconferencia desplegada.

Ilustración 23 Incidentes / Requerimientos sedes regionales – diciembre 2024

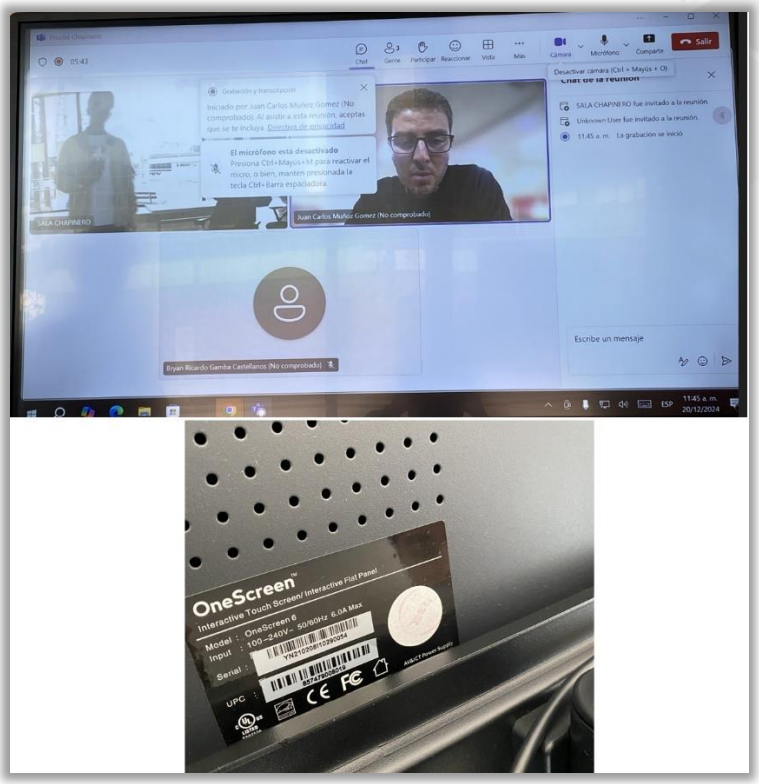


Ilustración 24 Prueba de funcionamiento sede chapinero – noviembre 2024

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

Para el periodo comprendido entre el 1 y el 31 de diciembre, 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, como se viene realizando, 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 realizada a la sede de Aguas y Ángel (y Chapinero evidenciada en la anterior sección), con la persona que realiza el apoyo técnico frecuente para revisión de los equipos y atención de requerimientos, se realizaron nuevamente pruebas de funcionamiento, limpieza superficial de los módulos, inspección visual y los ajustes requeridos parta descartar incidencias en los equipos y poder garantizar continuidad del servicio. En estas revisiones no se encontraron novedades y los módulos se encuentran funcionando de manera correcta y con la regularidad requerida. La solicitud de ingreso para la visita se realizó mediante el caso RF-290208-8-21547.

Ilustración 25 Módulo funcional sala 8vo piso Presidencia – Visita diciembre 2024

En las visitas regulares se realizan pruebas de funcionamiento en los módulos de cada piso de la sede Aguas para validar el funcionamiento normal del servicio, además de inspección visual de desgaste de elementos y conexiones para garantizar funcionamiento correcto y brindar servicio sin interrupciones.

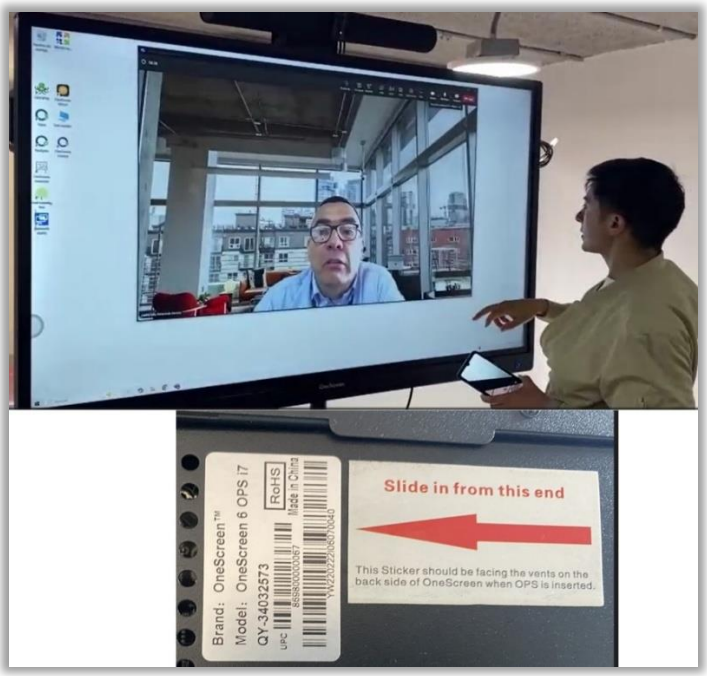


Ilustración 26 Evidencia módulo funcional sede Aguas 65, piso 4 - Visita diciembre 2024

Al igual que en los anteriores módulos, se revisó funcionalidad en el módulo de la sala de reuniones del piso No. 2 (Caso RF-290474-8-21571) y 6 se validó y confirmó funcionamiento al igual que las demás salas.

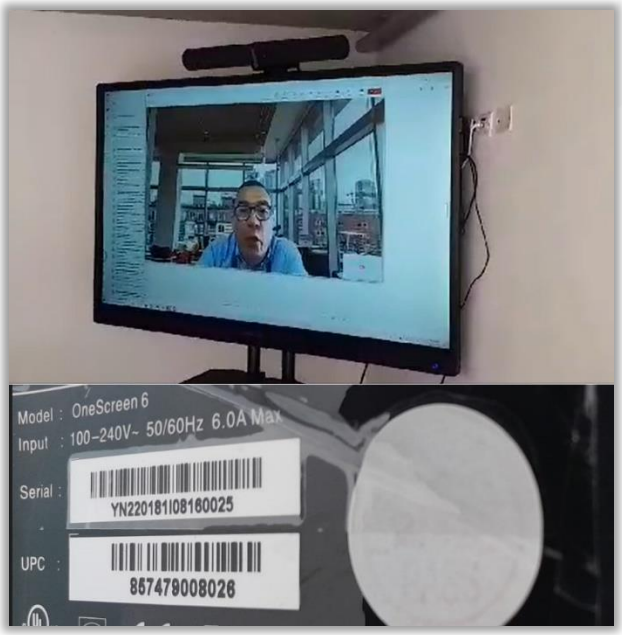


Ilustración 27 Evidencia módulo funcional sede Aguas piso 6 – Visita diciembre 2024

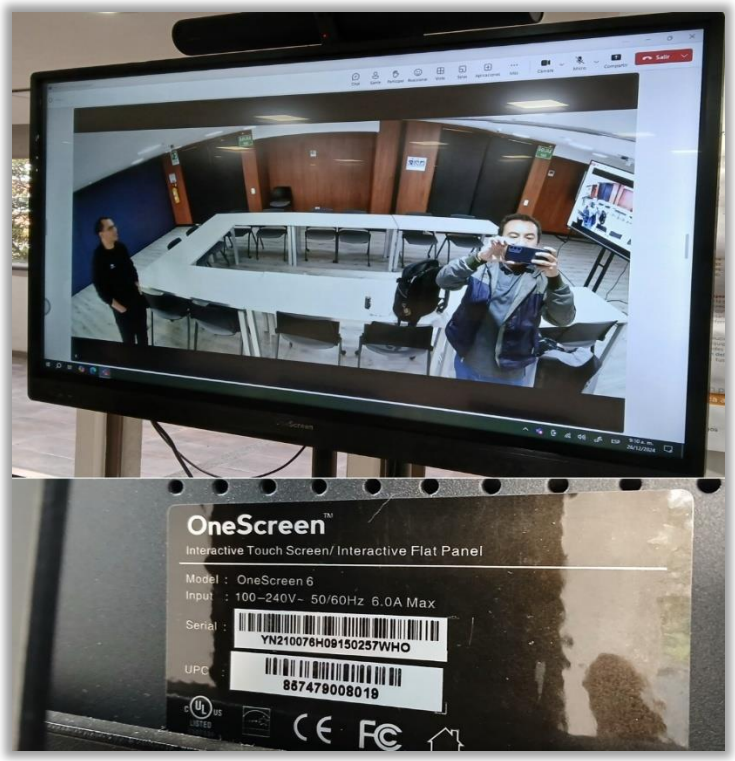


Ilustración 28 Evidencia módulo funcional sede Aguas Piso 2 – Visita diciembre 2024

Por último, se procede con la revisión del módulo de la sede Ángel, el cual evidencia funcionamiento con normalidad sin presentar incidencias.

Ilustración 29 Verificación módulo sede Angel – piso 2 – diciembre 2024

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

- Visita en sitio para pruebas de funcionamiento y limpieza externa módulos instalados en la ciudad de Bogotá, Aguas, Ángel y Chapinero.
- Informe mensual de operación del servicio y reporte técnico de visitas a sedes Regionales.

Las evidencias se pueden encontrar en el siguiente [Informe actividades Módulos videoconferencia ICETEX Diciembre 2024.pdf]

Durante los últimos 03 meses se presentaron los siguientes requerimientos y/o incidentes durante la prestación del servicio de videoconferencia:

	Octubre	Noviembre	Diciembre
Requerimiento	0	4	0
Incidentes	0	0	0

Tabla 20 Distribución trimestral de requerimientos y/o incidentes

Para el mes de diciembre 2024 no se presentaron afectaciones en el servicio de video conferencia en las sedes del ICETEX.

9. GESTION DE RIESGOS Y PROBLEMAS

La matriz de riesgos es fundamental en la gestión del proyecto, ya que permite evaluar tanto la probabilidad de ocurrencia de riesgos como su impacto potencial en el ICETEX, facilitando así la toma de decisiones informadas. Su uso contribuye a una mejor planificación y mitigación de riesgos en el desarrollo del proyecto.

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.

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 21 Nivel de riesgo

- Tabla de grado de riesgo

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

Tabla 22 Grado de riesgo

- 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 30 Matriz de riesgos

10. INDICADORES CLAVE DE DESEMPEÑO

10.1. ANS por Disponibilidad de canales de comunicaciones:

Durante el mes de diciembre, 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 va actualizando a medida que se realizan las ampliaciones de las canales acordadas contractualmente, se tienen los reportes:

Reporte Mensual Disponibilidad INFOTIC Diciembre 2024.pdf

Informe mensual ALLOT diciembre 2024.pdf

Se carga en el repositorio un documento en Excel con el análisis del comportamiento de los canales para el mes de diciembre ANS_Diciembre_2024.xlsx

Sede	Categoría	INR	%MES
BOGOTAD.C.	Principal/FO (Sede Aguas)	INR0037	100,00%
	Backup /FO (Sede Aguas)	INR0036	100,00%
	Principal/IPVPN (Sede Chapinero)	INR0022	100,00%
	Backup /IPVPN (Sede chapinero)	INR0020	100,00%
	Principal/IPVPN (Angel)	INR0272	100,00%
	Backup /IPVPN (Angel)	INR0273	100,00%
IBAGUE	Principal/IPVPN	INR0073	99,98%

Sede	Categoría	INR	%MES
	Backup/IPVPN	INR0076	98,43%
LETICIA	Principal/Satelital	INR0000373	96,81%
NEIVA	Principal/IPVPN	INR0039	100,00%
	Backup/IPVPN	INR0041	100,00%
TUNJA	Principal/IPVPN	INR0104	100,00%
	Backup/IPVPN	INR0106	98,51%
VILLAVICENCIO	Principal/IPVPN	INR0085	99,97%
	Backup/IPVPN	INR0084	100,00%
ARMENIA	Principal/IPVPN	INR0074	100,00%
	Backup/IPVPN	INR0072	99,93%
MANIZALES	Principal/IPVPN	INR0088	99,99%
	Backup/IPVPN	INR0087	100,00%
MEDELLIN	Principal/IPVPN	INR0133	99,14%
	Backup/IPVPN	INR0132	99,27%
APARTADO	Principal/IPVPN	INR0144	99,33%
PEREIRA	Principal/IPVPN	INR0079	99,98%
	Backup/IPVPN	INR0077	100,00%
QUIBDO	Principal/IPVPN	INR0014	100,00%
	Backup/IPVPN		
BARRANQUILLA	Principal/IPVPN	INR0103	99,95%
	Backup/IPVPN	INR0100	99,95%
CARTAGENA	Principal/IPVPN	INR0109	99,13%
	Backup/IPVPN	INR0107	99,55%
MONTERIA	Principal/IPVPN	INR0080	100,00%
	Backup/IPVPN	INR0081	100,00%
RIOHACHA	Principal/IPVPN	INR0164	100,00%
	Backup/IPVPN	INR0162	97,33%
SANTAMARTA	Principal/IPVPN	INR0154	100,00%
	Backup/IPVPN	INR0152	100,00%
SINCELEJO	Principal/IPVPN	INR0095	99,91%
	Backup/IPVPN	INR0097	99,91%
SANANDRES	Principal/IPVPN	INR0000367 INR0000369	81,87%
BARRANCABERMEJA	Principal/IPVPN		
SANGIL	Principal/IPVPN		
BUCARAMANGA	Principal/IPVPN	INR0062	99,91%
	Backup/IPVPN	INR0061	99,91%
CUCUTA	Principal/IPVPN	INR0044	100,00%
	Backup/IPVPN	INR0047	100,00%
VALLEDUPAR	Principal/IPVPN	INR0091	100,00%
	Backup/IPVPN	INR0090	99,68%
YOPAL	Principal/IPVPN	INR0121	100,00%

Sede	Categoría	INR	%MES
	Backup/IPVPN	INR0123	100,00%
ARAUCA	Principal/IPVPN	INR0110	90,23%
CALI	Principal/IPVPN	INR0151	100,00%
	Backup/IPVPN	INR0153	100,00%
BUENAVENTURA	Principal/IPVPN	INR0051	98,85%
MOCOA	Principal/IPVPN	INR0135	99,95%
	Backup/Satelital	INR0136	100,00%
PASTO	Principal/IPVPN	INR0130	100,00%
	Backup/IPVPN	INR0131	100,00%
POPAYAN	Principal/IPVPN	INR0035	96,49%
	Backup/IPVPN	INR0032	99,92%
TUMACO	Principal/IPVPN	INR0147	99,42%
DCTRIARA	MPLSPP	INR0266	100,00%
	MPLS Backup	INR0171	100,00%
DCTRIARA	NOC claro de dedicado (DWDM)2GTriaramegacentro	INR0224	100,00%
Canal entre Sitio principal Icetex-Dirección General-Aguas	Principal/IPVPN		100,00%
	Backup/IPVPN		100,00%
BOGOTAD.C.	Internet (Sede Aguas)	INR0034	100,00%
DC Megacentro	DCMEGACENTER–CONTIGENCIA–MPLSPPAL	INR0177	100,00%
DCTRIARA	DCMEGACENTER–CONTIGENCIA–MPLSBK	INR0230	100,00%
DC Megacentro	Internet	INR0268	100,00%
Banco de la Republica hasta Edificio Dirección General ICETEX	Ubicado en Data center Principal. Interconectado a través de red MPLS	INR0000289	100,00%
DECEVAL hasta Edificio de ICETEX Dirección General	Ubicado en Data center Principal. Interconectado a través de red MPLS	INR0000317	99,99%
DECEVAL hasta Edificio de ICETEX Dirección General	UbicadoenDatacenterPrincipal.interconectadoatravesderedMPLS(Backup)	INR0000318	99,99%
Salidadelportaleshttps://portal.icetex.gov.co/portalywww.icetex.gov.cohaciainternetencentrodecómputoprincipal	Internet Reverso para Portales	INR0000320	100,00%

Sede	Categoría	INR	%MES
Salidadelportaleshttps://portal.icetex.gov.co/portalywww.icetex.gov.cohaciainternetencentrodecómputodecontingencia	Internet Reverso para Portales	INR0274	100,00%
DCTRIARA	allotentralizado800Mtriara(equipo)	INR0270	100,00%

Tabla 23 Disponibilidad de Canales

Durante el mes de diciembre 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	99.95%
BUCARAMANGA	INTERNET PARA LA GENTE	INR0057	99.91%
CALI	INTERNET PARA LA GENTE	INR0160	100.00%
AGUAS	INTERNET PARA LA GENTE	INR0029	99.99%
CHAPINERO	INTERNET PARA LA GENTE	INR0015	100.00%
MEDELLIN	INTERNET PARA LA GENTE	INR0122	99.14%
APARTADO	INTERNET PARA LA GENTE	INR0140	99.34%
ARAUCA	INTERNET PARA LA GENTE	INR0115	90.23%
LETICIA	INTERNET PARA LA GENTE	INR0000378	96.90%
QUIBDO	INTERNET PARA LA GENTE	INR0021	100.00%
RIOHACHA	INTERNET PARA LA GENTE	INR0159	99.91%
SAN ANDRES	INTERNET PARA LA GENTE	INR0000368	81.86%
YOPAL	INTERNET PARA LA GENTE	INR0127	100.00%
MOCOA	INTERNET PARA LA GENTE	INR0141	99.95%

Tabla 24 Disponibilidad canales "Internet para la gente"

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

Sede	Categoría	INR	% Mes
SD WAN AGUAS	SD WAN	INR0033 / 000334	100.00%
SD WAN MOCOA	SD WAN	INR0139 / 000333	99.95%
SD WAN LETICIA	SD WAN	INR0000374	96.84%
SD WAN SANANDRES	SDWAN	INR0000371	81.03%

Tabla 25 Disponibilidad Canales "SDWAN"

10.1.1. Canal de Replicación (Triara – Megacenter)

El proyecto tiene asignado dos (02) canales de comunicación con un ancho de banda de 02 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 diciembre funcionó correctamente y no

se presentó afectación en la prestación del servicio.

La evidencia se encuentra en el Informe mensual replicacion diciembre 2024.pdf

10.2. ANS por Disponibilidad de servidores:

La herramienta de monitoreo para disponibilidad de servidores es ELK y el informe de disponibilidad es el que permite la revisión de los ANS Reporte Monitoreo ICETEX Diciembre 2024-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	100%
INR0241	icetexbogelasticserver3	100%
INR0242	icetexbogliferayserver2	99.99%
INR0243	icetexbogliferayserver1	99.99%
INR0244	icetexboglxdarumasrv1	100%
INR0245	icetexboglxdarumasrv2	100%
INR0246	iceteboglxdarumatest	100%
INR0247	preprodsec-icetexboglxxroad2n	100%
INR0248	icetexboglxxroad3	100%
INR0249	xroadsec-icetexboglxxroad1	100%
INR0250	qasec-icetexboglxxroadtest	100%
INR0262	icetexboglxorfeo2	100%
INR0276	cxvodaprodn011	100%
INR0277	cxvodaprodn021	100%
INR0278	cxvodacontn011	100%
INR0240	icetexbogelasticserver2	100%
INR0260	icetexbogosbognfs1	100%
INR0252	icetexbogosbognfs2	100%
INR0236	ictxbogsrvpt1	100%
INR0235	ictxbogsrvpt2	100%
INR0000322	ictxcontroldoc	100%
INR0226	mira	99.99%
INR0253	bastion	100%

Cod Servicio	Hostname	Disponibilidad
INR251	Openshift	100%
INR254	Openshift	100%
INR255	Openshift	100%
INR256	Openshift	100%
INR257	Openshift	100%
INR258	Openshift	100%
INR259	Openshift	100%

Tabla 26 Códigos relacionados Disponibilidad Servicios en Housing – Datacenter Principal

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

#	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, los cuales tuvieron un **UPTIME del [99,92%]** tal como se evidencia en la gráfica a continuación.

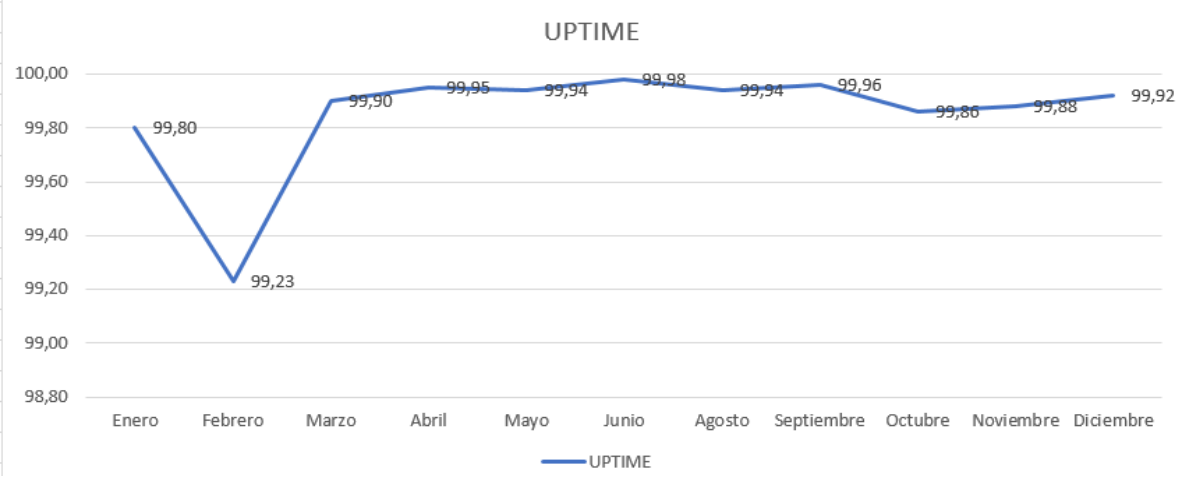


Ilustración 31 UPTIME – Portal WEB web.ICETEX.gov.co

Durante el mes de diciembre se evidenció un comportamiento estable del portal WEB institucional y se cumplió con el porcentaje de disponibilidad de este con un porcentaje del **99,92%,** 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 676 mil usuarios, con 459 mil usuarios nuevos. El tiempo de interacción medio es de 2 minutos 26 segundos, señalando el interés de la audiencia en las diferentes páginas del portal web.ICETEX.gov.co.

Ilustración 32 Métrica de visitantes Portal WEB web.ICETEX.gov.co

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

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

Ilustración 33 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 domingo 1 de diciembre desde las 0:00 am hasta las 9:00 am del martes 31 de diciembre de 2.024.

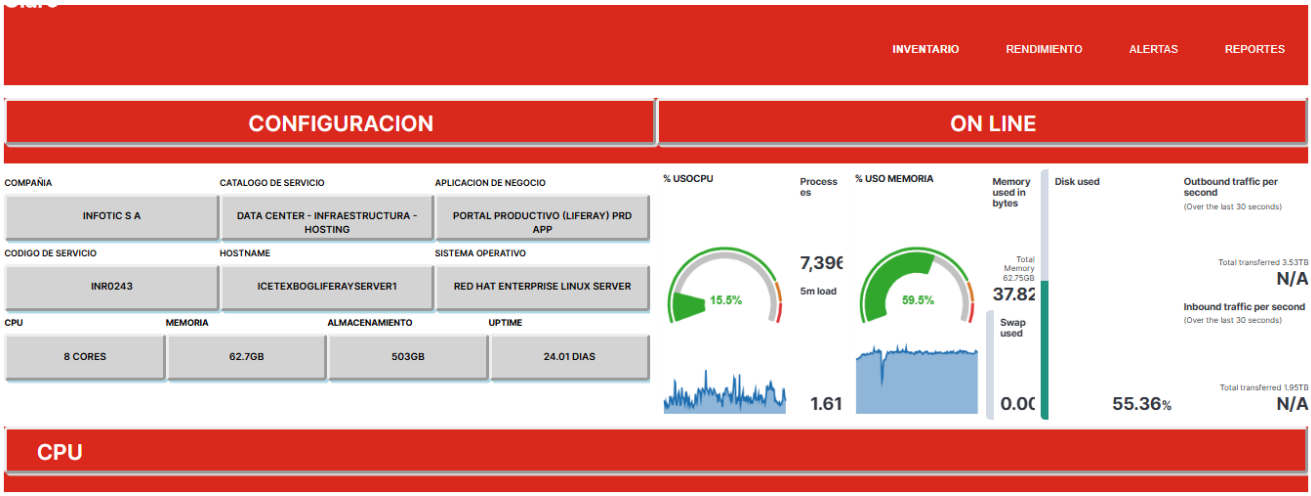


Ilustración 34 NODO 1 – Vista General – INR0243

Ilustración 35 NODO 1 CPU

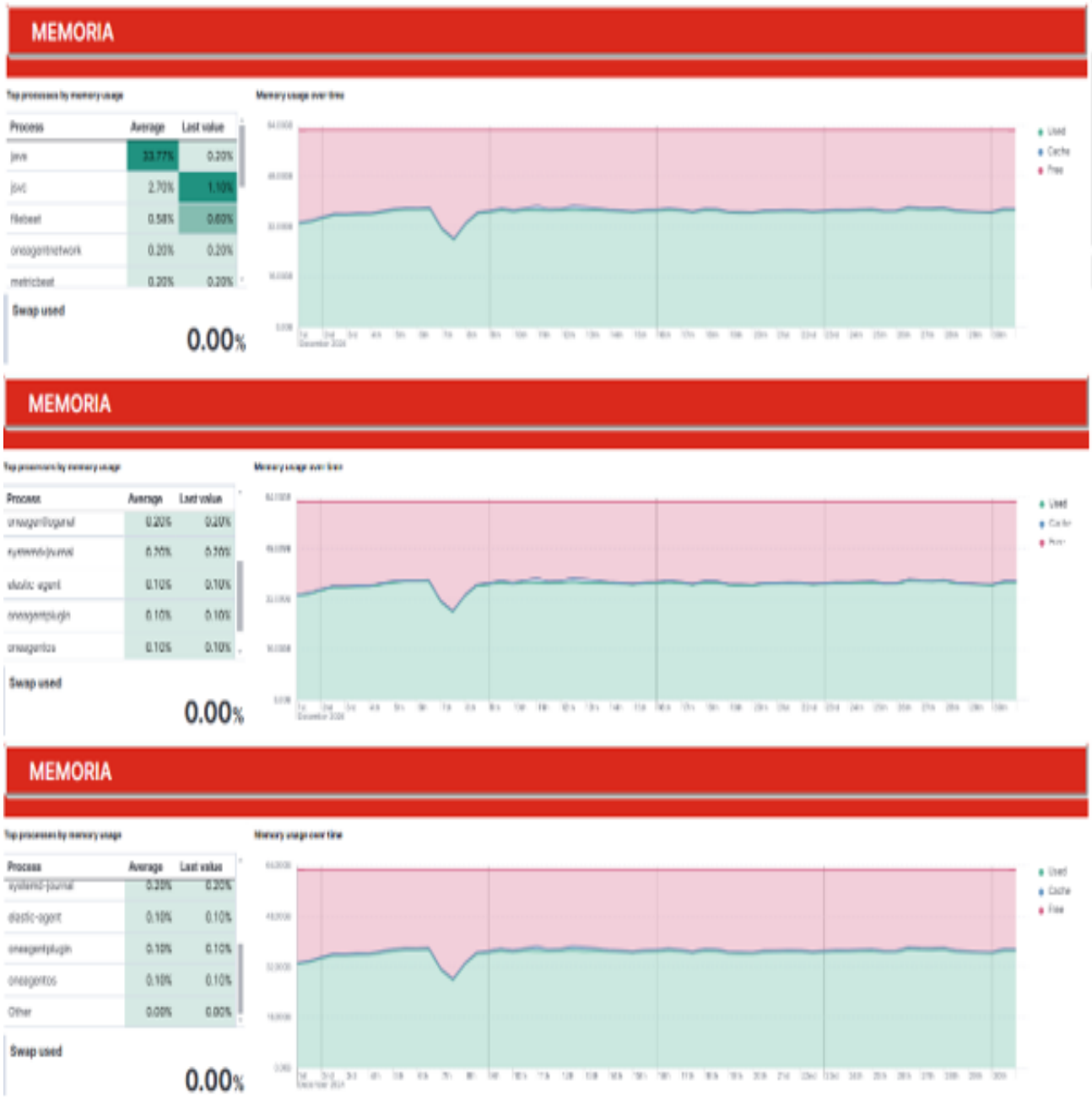


Ilustración 36 NODO 1 Memoria

Ilustración 37 NODO 1 Almacenamiento

Ilustración 38 NODO 2 – Vista General – INR0242

Ilustración 39 NODO 2 CPU

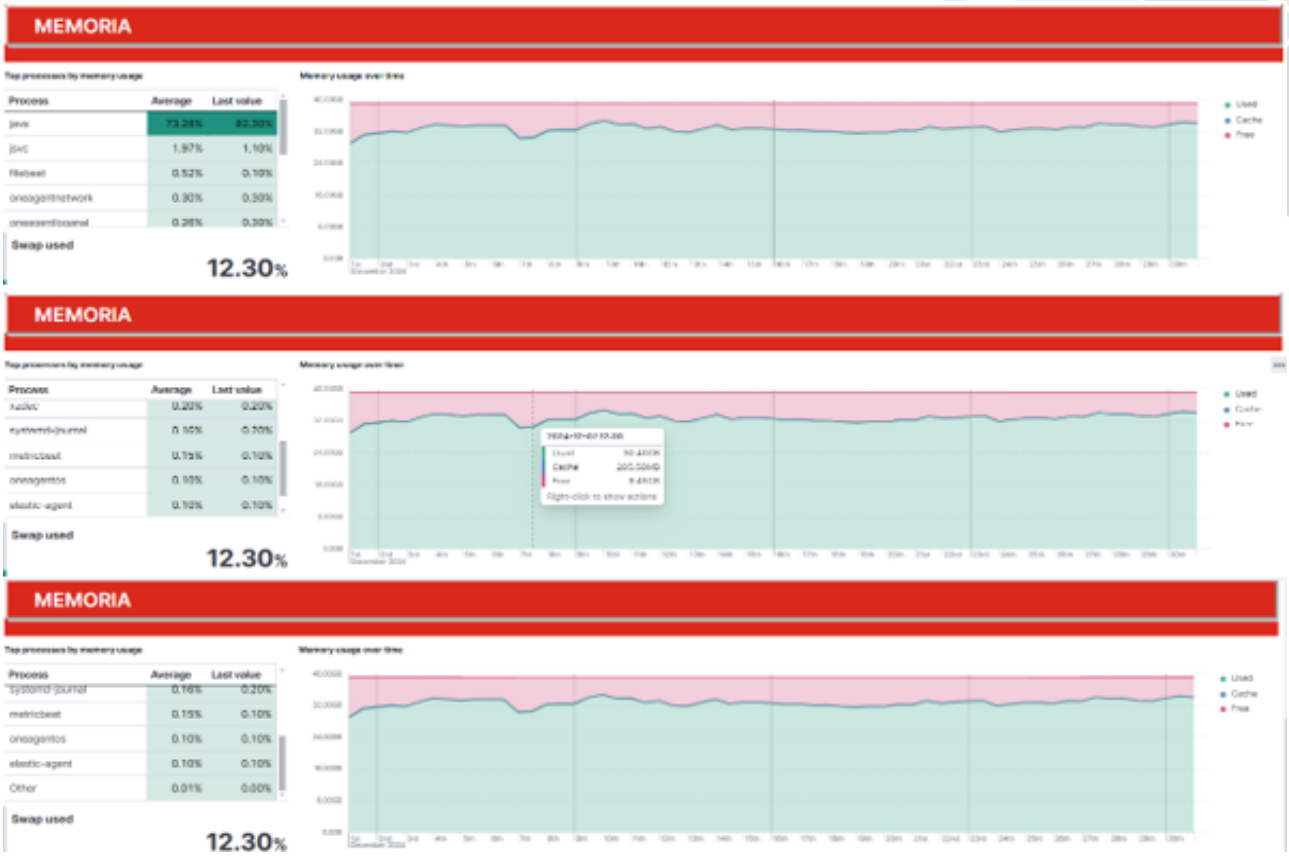


Ilustración 40 NODO 2 Memoria

Entre el 1 y el 31 de diciembre, no hubo consumo de memoria SWAP en el nodo 2, debido a que se ejecutó 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, el partner Claro no volvió a emitir alarmas de consumo de SWAP en nodo 2.

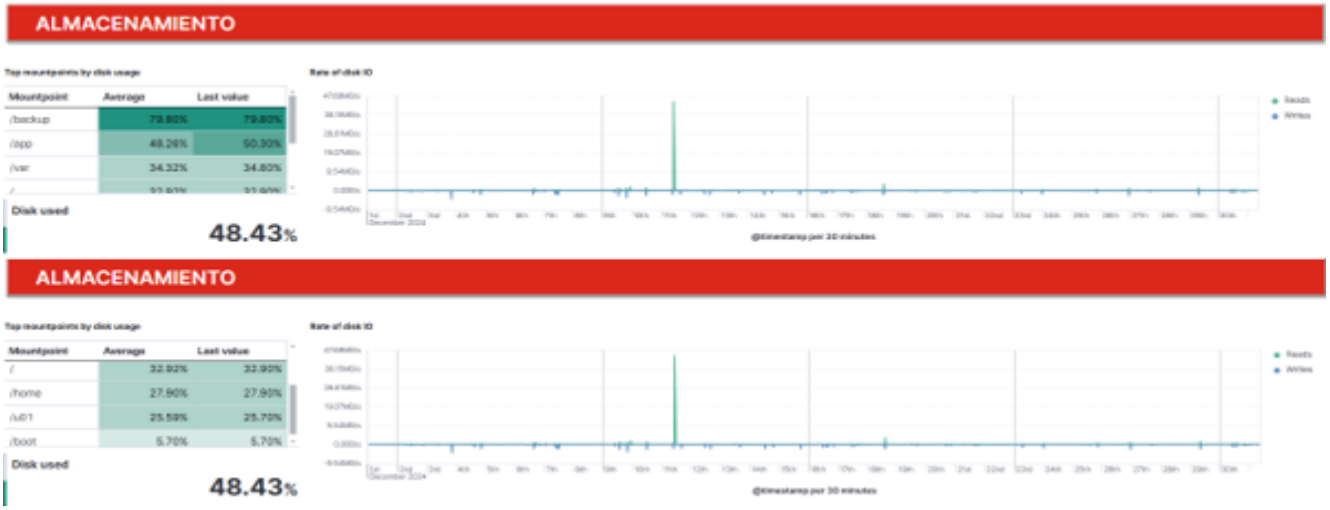


Ilustración 41 NODO 2 Almacenamiento

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

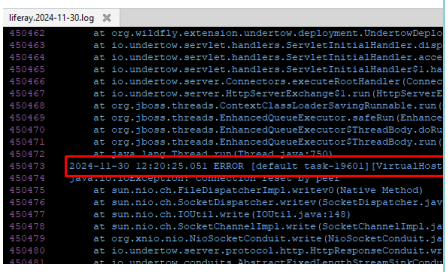
10.2.2. Análisis componente Liferay Producción

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

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

UNIDAD	HALLAZGO	OBSERVACIONES
MEMORIA RAM	**Nodo 1** total de memoria RAM – 65.79 GB. **Nodo 2** total de memoria RAM – 41.02 GB	En espera de **la autorización** para disponer y configurar la memoria necesaria para que los dos nodos queden iguales.
SISTEMA OPERATIVO	La última versión del UPDATE **del Sistema Operativo Red Hat Enterprise 7.2**, donde está alojada el servidor de Liferay 7.3.10 GA1	Está pendiente de programarse la actividad en el mes de diciembre. Se tiene previsto realizar la actividad de actualización de sistema operativo Linux Red Hat 7.9 de acuerdo al N° de Caso Claro **1116300** con el minutograma compartido por Claro. Los servicios pendientes por actualizar son los siguientes: Nodo 1 – Portal ICETEX - INR0243, Nodo 2 – Portal ICETEX - INR0242, Nodo 1 – Elasticsearch - INR0239, Nodo 2 – Elasticsearch - INR0240, Nodo 3 – Elasticsearch - INR0241 Posterior a esta actividad de actualización, un recurso de migración de realizar el cambio de Liferay 7.3 a la versión 7.4 DXP o 7.4 Quarter Released.
DISCO DURO	El espacio en disco utilizado por el CMS Liferay en el **nodo 1 es 291**	Comportamiento normal.

UNIDAD	HALLAZGO	OBSERVACIONES
	GB. El espacio disponible es de 86 GB. El espacio en disco utilizado por el CMS Liferay en el **nodo 2 es 184 GB**. El espacio disponible es de 194 GB.	Se trabaja en la exportación de logs comprimidos en formato .zip al servicio NFS, ruta: /nfs/nodo1logs /nfs/nodo2logs 2. Nodo1-Liferay [root@icetexbogliferayserver1 ~] Filesystem Size Us /dev/mapper/rhel-root 45G 1 devtmpfs 32G tmpfs 32G tmpfs 32G 32 tmpfs 32G /dev/mapper/app-appvol 394G 29 /dev/sda1 4.0G 23 /dev/mapper/rhel-home 16G 1. /dev/mapper/rhel-var 19G 7. 192.168.20.42:/nfs1 503G 38 192.168.20.42:/nfs 503G 11 tmpfs 6.3G tmpfs 6.3G tmpfs 6.3G [root@icetexbogliferayserver1 ~] 3. Nodo2-Liferay [root@icetexbogliferayserver2 ~] Filesystem Size Us /dev/mapper/rhel-root 45G 1 devtmpfs 20G tmpfs 20G tmpfs 20G 8 tmpfs 20G /dev/sda1 4.0G 23 /dev/mapper/app-appvol 394G 18 /dev/mapper/rhel-home 16G 4. /dev/mapper/rhel-var 19G 6. 192.168.20.42:/nfs1 503G 38 192.168.20.42:/nfs 503G 11 tmpfs 4.0G tmpfs 4.0G tmpfs 4.0G [root@icetexbogliferayserver2 ~]
FILE SYSTEM	El espacio en disco utilizado por el CMS Liferay en el **nodo 1 es 426 MB.** El espacio en disco utilizado por el CMS Liferay en el **nodo 2 es 443 MB.**	
PARCHES DE SEGURIDAD	**Nodo 1** - activation-key-dxpproduction-7.3-icetex-	Pendiente de aprobación por parte

UNIDAD	HALLAZGO	OBSERVACIONES
	publicportal 40.xml activation-key-dxpproduction-7.3-icetex-publicportal - icetexbogliferayserver1.xml **Nodo 2** - activation-key-dxpproduction-7.3-icetex-publicportal - icetexbogliferayserver2.xml	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.
VOLUMEN DE LOGS	Registro de logs entre finales de noviembre comienzos de diciembre.	Se registró error de conexión a base de datos el 30 de noviembre entre las 12:20 y 12:32. La falla se presentó por una alta concurrencia en nodo 1 y 2, fue necesario detener el servicio de WildFly y luego hacer un reinicio del nodo 2, se restableció el portal ICETEX a las 12:55 pm. En la siguiente línea, se muestra una interrupción abrupta en la conexión con el servidor de aplicaciones.  La siguiente línea, se muestra que hubo una conexión establecida en algún momento, pero cuando se intentó confirmar, la conexión ya no estaba abierta. Lo que concluye en perdida de paquetes o dropped.

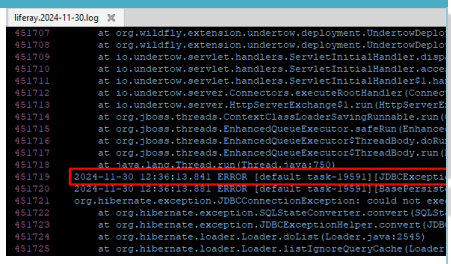
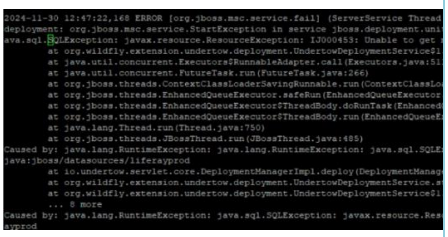
UNIDAD	HALLAZGO	OBSERVACIONES
		 La siguiente línea, registra que hubo un error de conexión con la base de datos de Oracle – datasource - liferayprod.  Posterior a este incidente, no volvieron a registrar errores en la carpeta logs.

Tabla 28 Actualización – Análisis componente LIFERAY diciembre

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

	Octubre	Noviembre	Diciembre
Usuarios mes	379000	487000	676000
Usuarios nuevos	263000	263000	459000
Tiempo acceso (min)	147	147	146

Tabla 29 Distribución trimestral de acceso por usuarios

Durante el último trimestre se presentó un promedio de 514000 usuarios que accedieron al portal web, presentando para el mes de diciembre un aumento en el número de usuarios que ingresaron a la página de la entidad del 27.96% que corresponde a 189000 usuarios.

A nivel de los usuarios nuevos que accedieron a la página se tiene que en promedio durante el último trimestre se tiene 2328333, presentando para el mes diciembre un aumento en el número de accesos nuevos que corresponde a 196000 usuarios.

El tiempo que emplearon los usuarios una vez ingresaron a la página web durante el último trimestre correspondió a 147 minutos, presentando para el mes de diciembre una reducción de 01 minuto que corresponde a 146 minutos.

Las siguientes Url´s están siendo monitoreadas desde la herramienta ELK y en el mes de diciembre tuvieron la siguiente disponibilidad:

- http://www.icetex.gov.co disponibilidad: 99.92%
- http://web.icetex.gov.co disponibilidad: 100.00%
- url faltante adicionarla

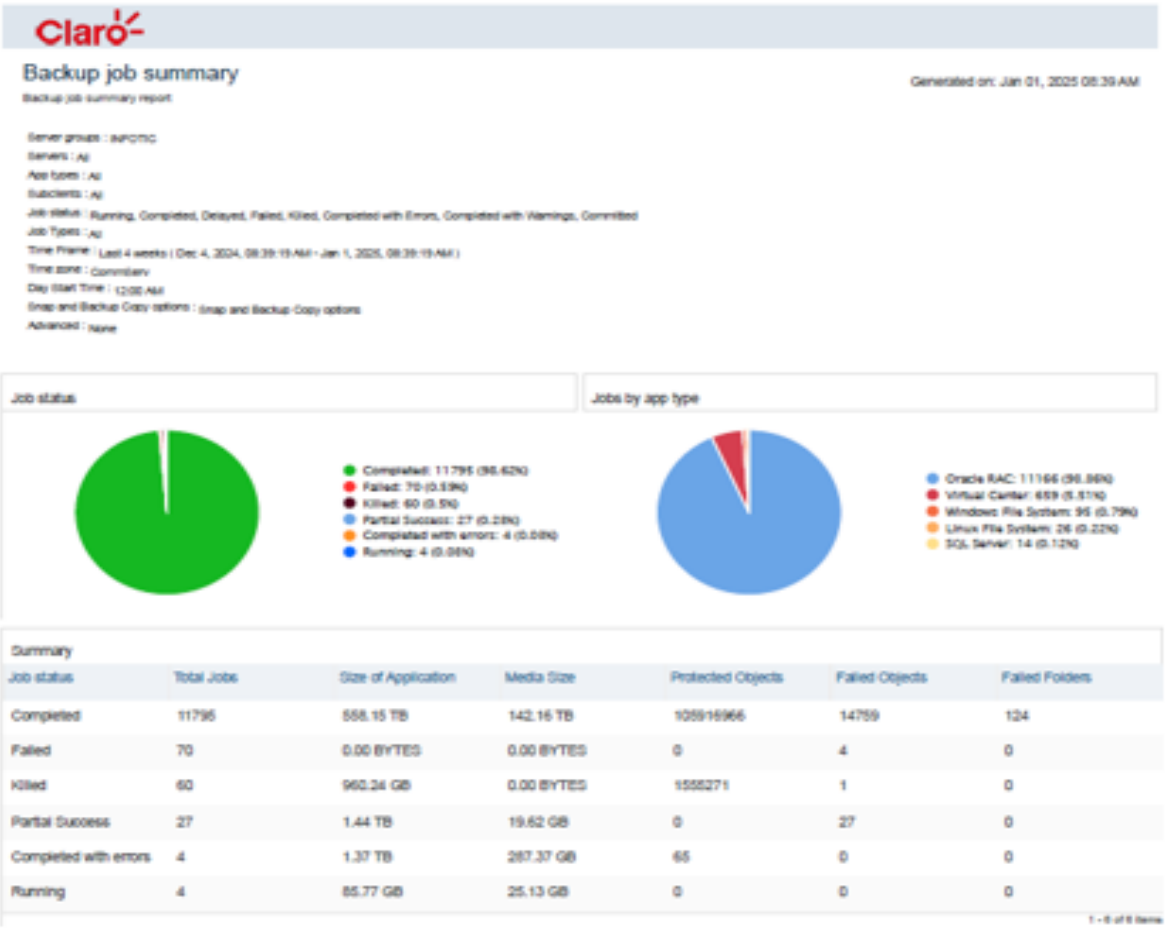
10.2.3. Backup Servidores Triara

Durante el periodo de diciembre 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 diciembre 2024.pdf donde se adjunta el reporte de los backups que se genera automáticamente desde la herramienta que se utiliza para realizar las copias, y de forma manual se le ha colocado en formato de INFOTIC, es de aclarar que la ley establece que no se pueden modificar los documentos que son generados de forma automática por herramientas tecnológica para dar la seguridad y tranquilidad que el documento cumple con las condiciones de calidad, integralidad y confiabilidad de la información.

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 diciembre el resultado de la ejecución de los Backup fue:



Claro

Backup job summary

Backup job summary report

Generated on: Jan 01, 2025 08:39 AM

Server groups : INFOTIC
Servers : All
App types : 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 (Dec 4, 2024, 08:39:19 AM - Jan 1, 2025, 08:39:19 AM)
Time zone : Commserv
Day Start Time : 12:00 AM
Snap and Backup Copy options : Snap and Backup Copy options
Advanced : None

Job status

Jobs by app type

Summary

Job status	Total Jobs	Size of Application	Media Size	Protected Objects	Failed Objects	Failed Folders
Completed	11795	558.15 TB	142.16 TB	1059116966	14759	124
Failed	70	0.00 BYTES	0.00 BYTES	0	4	0
Killed	60	960.24 GB	0.00 BYTES	1555271	1	0
Partial Success	27	1.44 TB	19.62 GB	0	27	0
Completed with errors	4	1.37 TB	287.37 GB	65	0	0
Running	4	85.77 GB	25.13 GB	0	0	0

1 - 6 of 6 Items

Ilustración 42 Evidencia Backup servidores resumen Backups y su estado

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

El total del tamaño de la información respalda en cintas de Backups para el mes de diciembre corresponde a 558.15 TB, donde 98.62% se completó en el primer lanzamiento del robot con un total de 562.01 TB de información.

El 93.36% está representado en el respaldo dado a la información del Oracle RAC, que equivale a 528.40 TB.

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

Tareas	Octubre	Noviembre	Diciembre
Completado	99.22%	97.07%	98.62%
Fallido	0.3%	1.79%	0.59%
Cancelados	0.2%	0.7%	0.5%
Terminados parcialmente	0.24%	0.29%	0.23%
Completado con errores	0.03%	0.1%	0.03%

Tareas	Octubre	Noviembre	Diciembre
En Proceso	0.01%	0.05%	0.03%
Tamaño	**468.21 TB**	**356.94 TB**	**562.01 TB**

Tabla 30 Distribución trimestral de Backup ejecutados

- El promedio de los Backups completado del último trimestre en el primer lanzamiento del robot fue de 98.30%, donde el mes con mayor nivel de ejecución fue octubre con 99.22%; el 1.38% corresponde a los siguientes parámetros: éxito parcial, fallido, terminado, completado con errores y en progreso.
- El promedio de toma Backups Fallido durante el último trimestre corresponde a 0.0089%, el mes donde más se presentó un mayor porcentaje de fallas fue noviembre con el 1.79%

	Octubre	Noviembre	Diciembre
Oracle RAC	92.56%	86.85%	93.36%
Virtual Center	6.25%	11.81%	5.51%
Windows File System	0.81%	1.86%	0.79%
Linux File System	0.29%	0.82%	0.22%
SQL Server	0.10%	0.15%	0.12%
RFEV	0.00%	0.01%	0.00%

Tabla 31 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 90.92% donde el mes con mayor tamaño de información respaldada fue diciembre con el 93.36%

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

NOTA 2: la evidencia se genera diariamente en el reporte que se entrega de forma automática por parte del operador tecnológico a los correos que el ICETEX solicito y en el informe mensual se anexan todas los soportes y evidencias de la ejecución de las políticas de Backup, es de acotar que en el mes de agosto del 2024, se entregó al ICETEX la política actualizada y vigente de la toma de Backup, link del repositorio de evidencias de Backup Backup Diario y el informe de Backup Informe de Backups

11. CONTROL DE CAMBIOS

Durante el mes de diciembre 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
1089	PAM Actualizaciones del Sistema Operativo seguridad segundo semestre 2024 PRD	19-nov-24	04-dic-24	Exitoso	Se realiza la actualización del sistema operativo correctamente
1108	Actualización del sistema operativo (LINUX) de la versión 7.2 a la 7.9	19-dic-24	no se ejecuto	no se ejecuto	Se requiere ambiente de prueba para poder proceder a la actualización

Tabla 32 Controles de cambio diciembre

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-ene-25	Está pendiente coordinar la sesión con los especialistas de ICETEX.
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-ene-25	Está pendiente coordinar la sesión con los especialistas de ICETEX.
Se debe realizar mesa técnica conjunta entre ICETEX e INFOTIC para revisar las alternativas de solución frente a la gestión de vulnerabilidades.	INFOTIC - ICETEX	01-dic-24	15-feb-25	Está pendiente coordinar la sesión con los especialistas de seguridad **(seguimiento el 10-ene-25)**
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	15-feb-25	Está pendiente coordinar la sesión con los especialistas de ICETEX.

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
Se trabaja en la copia de los logs al servidor NFS en la carpeta: /nfs	INFOTIC - ICETEX	01-dic-24	28-feb-25	Se ejecuto el 11 de diciembre 2024 – ***Resultado: EXITOSO***
Actualización el sistema operativo LINUX de la versión 7.2 a la versión 7.9	INFOTIC - ICETEX	01-dic-24	28-feb-25	Se requiere un ambiente pruebas. Esta evaluando la parte financiera para proceder a solicitar la aprobación de ICETEX.
Actualización de Liferay de la versión 7.3 a la 7.4	INFOTIC - ICETEX	01-dic-24	28-feb-25	LIFERAY recomienda que primero se debe actualizar en todas las maquinas el sistema operativo y luego proceder con el cambio de versión. Apenas se realicen las pruebas se definirá la fecha de actualización.
Verificar la configuración de los equipos de LAN y WAN que hace falta para el funcionamiento de IPv6.	INFOTIC - ICETEX	01-dic-24	28-feb-25	Se solicito al operador CLARO la revisión de la configuración entregada para dar cumplimiento a la configuración de IPv6. ***(seguimiento el 14 de enero del 2025)***
Traslado de los equipos de servicio de internet para la nueva sede de Arauca	INFOTIC - ICETEX	01-dic-24	28-feb-25	Se realizo la solicitud con el operador CLARO, se realiza la instalación de un canal provisional en la semana del 07 al 10 de enero, el canal definitivo

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
				queda en la primera semana de febrero. ***(seguimiento 14 de enero del 2025)***
Instalación del canal Backup de Quibdó	INFOTIC - ICETEX	01-dic-24	28-feb-25	La administración del centro comercial donde esta las instalaciones de ICETEX, dio la aprobación para ejecutar la instalación, se está coordinando con el grupo de CLARO ***(seguimiento 14 de enero del 2025)***
Instalación del canal principal de Puerto Carreño	INFOTIC - ICETEX	01-dic-24	28-feb-25	Se recibió la propuesta de CLARO y está en costeo por parte de INFOTIC ***(seguimiento 15 de enero de 2025)***
Nueva configuración de SD WAN en triara	INFOTIC - ICETEX	01-dic-24	28-feb-25	CLARO está preparando la oferta comercial para el traslado de Aguas a Triara y la nueva configuración desde Triara.
Instalación de los certificados SSL que el ICETEX va a adquirir	INFOTIC - ICETEX	01-dic-24	28-feb-25	El ultimo certificado fue instalado el 04 de diciembre del 2024. **Resultado: Exitoso**
Gestión de la administración Azure nube	INFOTIC - ICETEX	01-dic-24	28-feb-25	Se coordinará la sesión con ICETEX para definir las acciones a

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
				implementar.
Políticas e inventarios de las creaciones en la nube	INFOTIC - ICETEX	01-dic-24	28-feb-25	Se coordinará la sesión con ICETEX para definir las acciones a implementar.
Seguimiento a la adquisición de los Takedown por parte de ICETEX	INFOTIC - ICETEX	01-dic-24	28-feb-25	Se envió un correo el 29 de noviembre informando que no se cuentan con más Takedown y no se ha recibido respuesta por parte de ICETEX.
Capacitación en seguridad al grupo de especialistas de seguridad del ICETEX	INFOTIC - ICETEX	01-dic-24	28-feb-25	Se programará la capacitación una vez se tenga definido el grupo de seguridad y el tema de interés
Monitoreo de los diferentes servicios realizados por el SOC. Revisión conjunta entre ICETEX – INFOTIC	INFOTIC - ICETEX	01-dic-24	28-feb-25	Se revisará en la primera sesión de pares de seguridad. ***Fecha 10 de enero del 2025***
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-feb-25	Se coordinará la sesión con los ingenieros de CLARO, INFOTIC e ICETEX para revisar y generar la solución ***Fecha propuesta: 18 de enero del 2025***
Realizar mesa técnica entre ICETEX e INFOTIC para la revisión del alcance de Antivirus.	INFOTIC - ICETEX	01-dic-24	28-feb-25	Se revisará en la primera sesión de pares de seguridad. ***Fecha 10 de enero del 2025***
Reunión técnica de aclaraciones del diagrama de red para la realización del DRP Link	INFOTIC - ICETEX	01-dic-24	28-feb-25	Se coordinará la sesión con los

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
Minutograma tecnico DRP Noviembre actualizado.xlsx pestaña diagrama.				ingenieros de CLARO, INFOTIC e ICETEX para revisar y generar la solución ***Fecha propuesta: 21 de enero del 2025***
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.	NFOTIC - ICETEX		28-feb-25	Se coordinará la sesión con los ingenieros de CLARO, INFOTIC e ICETEX para revisar y generar la solución ***Fecha propuesta: 23 de enero del 2025***
Internet para la gente (5) faltantes				

Tabla 33 Planes de trabajo

13. RECOMENDACIONES DEL CONTRATISTA AL ICETEX

Las siguientes son las recomendaciones para el mes de diciembre 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 MÁSTER

- Solicitud de renovación de soporte Liferay, está vigente hasta el 31 de diciembre de 2024. 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.

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.

13.5. Administrador de aplicaciones

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

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

- Se realizarán sesiones conjuntas entre ICETEX e INFOTIC para revisar los costos mensuales y procedimientos que requieran ser ajustados en AZURE.

- Apoyar al ICETEX dando lineamientos que ayuden en la creación, definición y/o modificación de los procedimientos y cronogramas para las creaciones de futuras de recursos masivos, en este caso, VMs si es el caso.

- Continuar con la remediación de los hallazgos, en el correo se respondieron algunas dudas, pero falta la implementación de las TAGs, solicitadas para tener un mayor seguimiento sobre los recursos y su monitoreo, para este punto se apoyará el ICETEX dando lineamientos para la creación de los TAGs necesarios.

- Organizar sesiones de trabajo conjuntas entre ICETEX e INFOTIC que permitan levantar la información pendiente para comprender las necesidades, solicitantes, aprobadores y finalmente, justificaciones de lo existente, la entidad debe contar con una documentación e inventario de todo lo que existe en la nube como también, aplicaciones de la entidad.

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

- Construir con el ICETEX una matriz de perfiles de AZURE de acuerdo con las necesidades de la entidad, para evitar que los administradores de office 365 utilicen cuentas administradoras en la nube haciendo uso de todos los poderes y permisos administrativos sin regulación ni aprobación previa, se necesita identificar el usuario root en los Linux evitando su identificación.

13.7. Seguridad

- Se debe evaluar la mejor forma a nivel de seguridad la conmutación hacia Medellín generando el menor costo de tiempo, se revisará con el operador tecnológico para determinar alternativas.

- 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, se presentaran las opciones disponibles en el mercado para que mediante una mesa técnica entre ICETEX e INFOTIC para definir cual cumple los requisitos del ICETEX.

- 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 servidores de Directorio Activo con el SIEM.

- 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.

- Evaluar los riesgos sobre las plataformas en la nube y considerar aplicar plataformas de seguridad para los ambientes cloud que cuenta la entidad ya que estos contienen servicios críticos para la misma.

- Se debe realizar la integración de los activos críticos de la compañía a la plataforma de SIEM, no se ha podido logar por la falta de recursos de este.

- Se debe realizar la validación si los usuarios conectados a la VPN y los que hacen uso de la VPN punto a punto, es necesario que naveguen a través del ICETEX. Se realizará sesiones conjuntas entre INFOTIC e ICETEX para evaluar las VPN y determinar las acciones a seguir, se presentará el resultado en el mes de diciembre.

- En las sesiones conjuntas entre el ICETEX e INFOTIC se revisará la aplicabilidad de segmentar las políticas de acuerdo con la necesidad y no otorgar acceso de toda una red o todos los servicios.

- Con el perfilamiento de la navegación generado por ICETEX, se realizará un análisis para determinar el estado y en sesiones con el ICETEX e INFOTIC generar las acciones a seguir, se presentará un informe al respecto en mes de diciembre.

- Validar la autenticación de doble factor para todas las plataformas misionales del ICETEX. Se encuentra en validación de la entidad.

- Realizar autenticación a través del LDAPS, para la gestión de las plataformas de seguridad.

- Validar la posibilidad de la integración de la consola Sophos con SIEM, para tal fin de evaluaran los recursos de hardware y software para realizar la integración, se presentará el informe con el resultado en el mes de diciembre.

- Validar la posibilidad de la integración de una VPN para la gestión desde DT alterno Medellín como acceso adicional en caso de que se presente alguna falla por el canal dedicado de MPLS. Continuamos a la espera de respuesta de la entidad.

- Realizar la contención automática de equipos que se identifiquen en la red como maliciosos. Se encuentra en validación de la entidad.

- 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, para este punto el administrador del SOC cuenta con una ficha técnica de los recursos recomendamos y que se socializaran con el ICETEX para determinar el plan de acción.

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 el mes anterior, permitiendo un aumento en la capacidad de ancho de banda conforme a lo establecido en el ANEXO # 2. esta información se puede evidenciar a través de la herramienta de monitoreo Solar Winds y se verifica mensualmente en la facturación de ICETEX.

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

CIUDAD	Enlace - Tipo medio	INR	BW-Mínimo Requerido (MBPS)	Ancho de Banda actual	Ancho de Banda Ofrecido según Anexo 2.1
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 I NR0000369	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

CIUDAD	Enlace - Tipo medio	INR	BW-Mínimo Requerido (MBPS)	Ancho de Banda actual	Ancho de Banda Ofrecido según Anexo 2.1
PASTO	Principal / IPVPN	INR0130	18	20	20
	Backup / IPVPN	INR0131	8	10	10
POPAYAN	Principal / IPVPN	INR0035	20	20	20
	Backup / IPVPN	INR0032	5	5	5
TUMACO	Principal / IPVPN	INR0147	18	20	
WAN general (concentrador total red)	Principal /IPVPN	INR0266	1000	1000	1024
	Backup / IPVPN	INR0171	1000	1000	1024
Conectividad dedicada a funciones de réplica para eventos de DRP.	DWDM	INR0224	2000	2000	2048
Canal entre Sitio principal e ICETEX - Dirección General - Aguas	Principal /IPVPN	0	1000		1024
	Backup / IPVPN	0	600		600
BOGOTA ICETEX - Carrera 3 No. 18-32 - Sede Aguas - INTERNET bk	BOGOTA ICETEX - Carrera 3 No. 18-32 - Sede Aguas - INTERNET	INR0034	70	70	70
MEGACENTER MPLS BACKUP MEDELLIN	Conectividad brindada a través de la red MPLS, con acceso a los dos Datacenter	INR0177	500	500	500
Salida a Internet para toda la WAN desde Bogotá EN CENTRO DE COMPUTO principal	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0230	500	500	500
Internet Dedicado Navegación centralizada Megacenter	Internet Backup	INR0268	400	400	400
Banco de la Republica hasta Edificio Dirección General ICETEX	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0000289	40	40	40

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

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

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

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

14.3. TB de capacidad de almacenamiento

Este almacenamiento fue entregado y la evidencia es la siguiente:
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 35 Capacidades de almacenamiento contratado

Aprovisionado se tienen las siguientes capacidades instaladas:

EJECUTADO		
TRIARA	**ALMACENAMIENTO APROVISIONADO (TB)**	Evidencia
Almacenamiento MVs VMware	49,6	RV Tools

EJECUTADO		
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 36 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 venido cumpliendo y hasta el momento se tiene wifi en las 14 sedes donde ICETEX cuenta con oficinas y quedan pendientes 5 las cuales durante este mes fueron indicadas por Icetex para iniciar la gestión y son (Manizales, Armenia, Cartagena, Sincelejo, 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 37 WIFI para la gente instalados

Sede	Ancho de Banda	INR	Dirección
Manizales	10 Megas	INR0088	Calle 23 No. 23-16 Piso 3 - Edif. Caja Social de Ahorros
Armenia	10 Megas	INR0074	Calle 21 No. 16-37
Cartagena	10 Megas	INR0109	CR 32 # 9 - 36 ED BANCO DE ESTADO OF 901 Y 902
Sincelejo	10 Megas	INR0095	Calle 23 No. 19-28 Local 3
Pasto	10 Megas	INR0130	Carrera 3 # 3-26 Edificio Atlantis - Piso 4 - Oficina 405

Tabla 38 WIFI para la gente pendientes

15. CONCLUSIONES

- Administrar bien las contraseñas y permisos ayuda a que solo las personas autorizadas puedan acceder a información importante, reduciendo riesgos de seguridad.

- Es importante mejorar los recursos del FortiSIEM ya que esta herramienta para que pueda monitorear otros sistemas importantes como bases de datos, aplicaciones internas y equipos ya que las herramientas de monitoreo permiten detectar problemas rápidamente, facilitando una respuesta oportuna y minimizando riesgos.

- Configurar un control de acceso a la red basado en los servidores de la entidad ayuda a limitar quién puede entrar a ciertas partes de la red o internet, reduciendo el riesgo de que alguien termine en sitios peligrosos.

- Añadir autenticación de doble factor a las conexiones externas VPN de los funcionarios aumentaría la seguridad y protegería la información sensible que se transmite por estos medios.

- Ajustar las reglas de seguridad ha permitido controlar mejor el uso de los recursos clave de la red, garantizando que solo lo necesario esté accesible y fortaleciendo la protección.

- Incorporar soluciones que controlen quién puede conectarse a la red aumentaría la seguridad y ayudaría a prevenir o reducir el impacto de problemas potenciales.

- Los reportes del SOC han ayudado a identificar y cerrar posibles brechas, evitando que amenazas

importantes lleguen a afectar la infraestructura crítica de la entidad.

- Durante el mes de diciembre se evidenció un comportamiento estable del portal WEB institucional y se cumplió con el porcentaje de disponibilidad de este con un porcentaje del **99,92%** adicional en este informe mensual se incluyeron métricas e indicadores que contribuyen al entendimiento y al comportamiento del servicio.

- La mejora continua tanto en la presentación del informe como en la atención del servicio generan valor al cliente haciendo que evidencie un aumento en la satisfacción en la prestación del servicio.

- 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 observó un Aumento del 5% en los casos, atribuido a fallos en el servicio por parte del proveedor y a bloqueos de puertos en los equipos de la sede.

- Cada caso fue cerrado tras notificar a los funcionarios del servicio operativo sobre las incidencias pendientes con el proveedor, lo que representa una Aumento del 7% en relación con el mes anterior.

- El progreso en la instalación de los canales es del 99%, con solo las implementaciones de Quibdó Backup

- En cuanto a la instalación de señaléticas, también se ha alcanzado un avance del 98%, quedando únicamente la señalética de Cali, que actualmente se encuentra en proceso de fabricación.

- Se llevarán a cabo reuniones semanales a nivel interno con el objetivo de completar el proyecto de IPv6 junto a ICETEX, que presenta un avance del 55%. Estamos a la espera de que Infotic programe las instalaciones de los cables Ethernet restantes para finalizar el 45% pendiente.

- La disponibilidad de las bases de datos fue del 100% para el mes de diciembre de 2024.

- Se resolvieron aproximadamente 530 casos asignados a los administradores de base de dato en diciembre de 2024 en los tiempos estipulados por prioridad.

- Los casos atendidos en el mes de diciembre de 2024 aumentaron en un 8% respecto al mes de noviembre.

- Se atendieron todas las reuniones solicitadas por el cliente durante el mes de diciembre de 2024.

- 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.

- El aumento de los casos se debió a las nuevas convocatorias que debieron ser atendidas por el cliente, aunque su aumento no fue significativo

- Los casos estaban relacionados con accesos a servicios a través de conexiones FTP, también se escalaron errores presentados en algunas aplicaciones críticas del ICETEX y también se ejecutaron tareas de cambios que conllevaron a la actualización de archivos .dll sobre diversos Web Service que están configurados en los servidores web IIS.

- Gracias al enfoque proactivo de los administradores de soluciones, todos los casos fueron abordados oportunamente y se logró una resolución efectiva de las solicitudes, incidentes y tareas d cambio reportados.

16. PENDIENTES

16.1. Administrador WEB MASTER

- Con respecto al ticket de soporte Liferay N° **121996**, el analista Rodrígo Farias sugiere que se realice el proceso de Staging para tener un versionamiento lo más parecido al portal productivo como ambiente local, el procedimiento es ideal realizar pruebas antes de las publicaciones. Este proceso requiere una ventana de mantenimiento debido a que puede ocurrir intermitencia en el portal ICETEX en el momento que se realice el proceso clonación.

- Solicitud de renovación de soporte Liferay, está vigente hasta el 31 de diciembre de 2024. Es necesario adquirir de manera urgente la renovación debido a que hay varios procesos pendientes por validar con los analistas de soporte Liferay, el apoyo es constante. En caso de no pagarse la renovación del soporte, desde el 1 de enero de 2025, no es posible acceder a la cuenta jmartinezsi.cont@icetex.gov.co desde la URL https://help.liferay.com/.

16.2. Administrador Networking

- Definición de la configuración de IPv6 para las sedes que tienen router de voz.

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

- Instalación del canal de Backup de Quibdó.

- Traslado del canal de Arauca.

- Configuración de la red SD WAN para realizar las pruebas.

16.3. Administrador Base de datos

- Migración base de datos APLICATI 11.2.0.4 a 19C.

- 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.

16.4. Administrador de aplicaciones

- Seguimiento a la adquisición de los certificados SSL que se encuentran pendientes de adquirir.

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 de Azure, este inventario debe tener versiones de lenguajes de programación, en el informe de septiembre se reportó que solo es soportada la versión .Net 8 y la entidad aún cuenta con versiones .Net 6 en sus Datacenter, aun cuando mi alcance es sólo Azure y sus políticas con mejores prácticas (gobernanza), es una oportunidad para que las buenas prácticas de la nube se apliquen también en los Datacenter de la entidad.

16.6. Seguridad

- Continuar 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 de un total de 680 hay actualmente 602. 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.

- Mejoramiento del informe para una entrega de valor, en evaluación continua de parte de seguridad de ICETEX, para aceptación de los cambios, Se ha actualizado el formato de informe mensual según las solicitudes realizadas por parte de la Entidad.

17. ANEXOS

17.1. Almacenamiento

Backups Diarios

- Backups diarios diciembre (31 reportes)
  Backup Diario diciembre

Informe de Backups:

- Consolidado mensual Backup diciembre
  Consolidado diario backup diciembre 2024.pdf

- Informe Backup diciembre 2024
  Informe Backups mes de diciembre 2024.pdf

17.2. Aplicaciones

- Informe actividades Módulos videoconferencia ICETEX diciembre 2024
  Informe actividades Módulos videoconferencia ICETEX Diciembre 2024.pdf

- Informe mensual Administrador de Soluciones diciembre 2024
  Informe diciembre 2024 Administrador de soluciones.pdf

- Informe mensual Administrador Web Master diciembre 2024
  Informe diciembre 2024 Administrador web master.pdf

- Informe mensual Integrador Nube diciembre 2024
  Informe diciembre 2024 Integrador Nube.pdf

17.3. Bases De Datos

- Informe de evidencias Dataguard Megacenter diciembre 2024
  INFOTIC_ICETEX - Evidencias Dataguard Megacenter diciembre.pdf

- Informe mensual Administrador de Bases de datos diciembre 2024
  Informe diciembre 2024 Administrador bases de datos.pdf

17.4. Ejecución Presupuestal

- Conciliación diciembre consolidado
  Conciliación Diciembre_consolidado.xlsx

- Consolidado informe mensual especialistas diciembre
  Informe mensual especialistas diciembre 2024.pdf

- Informe de Gestión Servicio diciembre 2024
  Informe mensual especialistas diciembre 2024.pdf

17.5. Seguridad

- Informe Mensual MARCA-OSINT ICETEX diciembre 2024
  250102 Informe Mensual MARCA-OSINT ICETEX Diciembre 2024.pdf

- Informe Mensual Seguridad diciembre 2024
  Reporte mensual ICETEX_V2 diciembre 2024.pdf

- Informe Mensual SOC - ICETEX diciembre 2024
  250102 Informe Mensual SOC-TH ICETEX Diciembre 2024.pdf

- Informe técnico análisis de vulnerabilidades ICETEX diciembre
  INFORME TÉCNICO ANÁLISIS DE VULNERABILIDADES ICETEX (Diciembre).pdf

- Reporte de IPS diciembre
  Reporte de IPS de Diciembre_infotic_2024.pdf

Reporte total ataques recibidos-SIEM:

- Denegados diciembre 01-15
  Denegados Dic 01-15.pdf

- Denegados diciembre 16-31
  Dengados Dic 16-31.pdf

17.6. Soporte Y Monitoreo

Canales

- ANS diciembre 2024
  ANS_Canales_Diciembre_2024.xlsx

- Informe mensual Administrador de Networking diciembre 2024
  Informe diciembre 2024 Administrador Networking.pdf

- Informe Mensual Disponibilidad diciembre 2024
  Reporte Mensual Disponibilidad INFOTIC Diciembre 2024.pdf

Graficas de consumo:

- Informe Mensual ALLOT diciembre 2024
  Informe mensual ALLOT diciembre 2024.pdf

- **Pruebas Nuevas de Saturación Canales diciembre**
  Pruebas de saturación Diciembre

17.7. Data center Alterno:

Replicación

- Informe mensual replicación diciembre 2024
  Informe mensual replicacion diciembre 2024.pdf

- Reportes diarios diciembre
  Replicacion

17.8. Data Center Principal:

- Reporte Monitoreo ICETEX diciembre 2024-ELK
  Reporte Monitoreo ICETEX Diciembre 2024-ELK.pdf

Revisión técnica

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