

|                          |                                                                                                           |                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>Código: F319</b>      | <b>INFORME MENSUAL DE SUPERVISIÓN<br/>VERIFICACIÓN CUMPLIMIENTO DE LAS<br/>OBLIGACIONES CONTRACTUALES</b> |  |
| <b>Versión: 5</b>        |                                                                                                           |                                                                                     |
| <b>Fecha: 18/06/2024</b> |                                                                                                           |                                                                                     |
| <b>Página 1 de 5</b>     |                                                                                                           |                                                                                     |

1

|                                             |    |    |    |   |    |    |    |
|---------------------------------------------|----|----|----|---|----|----|----|
| <b>PERÍODO A QUE CORRESPONDE EL INFORME</b> | 01 | 11 | 24 | A | 30 | 11 | 24 |
|---------------------------------------------|----|----|----|---|----|----|----|

2

**DATOS DEL SUPERVISOR**

|                              |                                                             |
|------------------------------|-------------------------------------------------------------|
| <b>NOMBRE DEL SUPERVISOR</b> | VICTOR MANUEL MONDRAGON MACA Y VÍCTOR RAÚL BAUTISTA GALINDO |
| <b>DEPENDENCIA</b>           | Vicepresidencia de Operaciones                              |
| <b>CARGO</b>                 | Director de Tecnología y Coordinador de Infraestructura     |

3

**DATOS DEL CONTRATO**

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

4

**SEGUIMIENTO CONTRACTUAL**

| <b>NÚMERO DE LA OBLIGACIÓN</b> | <b>OBLIGACIÓN ESPECIFICAS<br/>(Relacionar obligaciones pactadas en el Contrato)</b>                                                                                                                                                                                                                                                    | <b>ASIGNADO PARA EL PERIODO (DE CORTE SEGÚN EL CONTRATO)</b> |           | <b>RECIBIDO A SATISFACCIÓN</b> |           |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|-----------|--------------------------------|-----------|
|                                |                                                                                                                                                                                                                                                                                                                                        | <b>Si</b>                                                    | <b>No</b> | <b>Si</b>                      | <b>No</b> |
| 1.                             | Ejecutar el objeto contratado en el tiempo y forma establecida, de conformidad con la propuesta presentada y aceptada que hace parte integral del contrato y con el anexo técnico y demás documentos del proceso.                                                                                                                      | X                                                            |           |                                |           |
| 2.                             | Suscribir el acta de inicio.                                                                                                                                                                                                                                                                                                           | X                                                            |           | X                              |           |
| 3.                             | Entregar todos los planes de implementación en los siguientes tres días hábiles a la fecha de la firma del acta de inicio, EL CONTRATISTA deberá, cubrir las etapas de preoperativos e implementación, los cuales serán revisados y aprobados en conjunto con el personal asignado por la Vicepresidencia de Operaciones y Tecnología. | X                                                            |           | X                              |           |
| 4.                             | Detallar y ejecutar las actividades preoperativas, empalme y mantenimiento de la calidad del servicio. Los servicios descritos anteriormente deben estar apoyados en herramientas metodológicas y técnicas por parte del proponente.                                                                                                   | X                                                            |           | X                              |           |
| 5.                             | Detallar el Plan de Trabajo con las correspondientes etapas de transición y operación, y garantizar las pruebas preliminares de la solución, las cuales                                                                                                                                                                                | X                                                            |           | X                              |           |

|                          |                                                                                                           |                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>Código: F319</b>      | <b>INFORME MENSUAL DE SUPERVISIÓN<br/>VERIFICACIÓN CUMPLIMIENTO DE LAS<br/>OBLIGACIONES CONTRACTUALES</b> |  |
| <b>Versión: 5</b>        |                                                                                                           |                                                                                     |
| <b>Fecha: 18/06/2024</b> |                                                                                                           |                                                                                     |
| <b>Página 2 de 5</b>     |                                                                                                           |                                                                                     |

| NÚMERO DE LA OBLIGACIÓN | OBLIGACIÓN ESPECIFICAS<br>(Relacionar obligaciones pactadas en el Contrato)                                                                                                                                                                                                                                                                                                                                                                                      | ASIGNADO PARA EL PERIODO (DE CORTE SEGÚN EL CONTRATO) |    | RECIBIDO A SATISFACCIÓN |    |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|----|-------------------------|----|
|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Si                                                    | No | Si                      | No |
|                         | deben ser aprobadas por el supervisor del contrato asignado por ICETEX antes de su paso a producción.                                                                                                                                                                                                                                                                                                                                                            |                                                       |    |                         |    |
| 6.                      | Detallar dentro del Plan de implementación las fases de transición y operación, Ingeniería de Detalle, revisión de la configuración actual de la infraestructura de acuerdo con el anexo técnico #1.                                                                                                                                                                                                                                                             | X                                                     |    | X                       |    |
| 7.                      | Asignar un gerente de proyecto para la fase de transición, así como el equipo de trabajo requerido para la ejecución de esta fase Resolver en la modalidad 8x5 todas las consultas o solicitudes de soporte técnico que se presenten por parte de ICETEX durante la ejecución del contrato.                                                                                                                                                                      | X                                                     |    |                         |    |
| 8.                      | Comprobar que se hagan todas las pruebas o preconfiguraciones que garanticen que los nuevos licenciamientos no van a afectar la operación de los equipos de comunicaciones unificadas, ni redes de telecomunicaciones de ICETEX.                                                                                                                                                                                                                                 | X                                                     |    |                         |    |
| 9.                      | Entregar todo el software y licenciamiento que forme parte de la solución propuesta y entregada en producción por parte del contratista.                                                                                                                                                                                                                                                                                                                         | X                                                     |    |                         |    |
| 10.                     | Disponer de todos los recursos técnicos y humanos apropiados para garantizar el cumplimiento del objeto del presente proceso.                                                                                                                                                                                                                                                                                                                                    | X                                                     |    |                         |    |
| 11.                     | Entregar, instalar e integrar el nuevo licenciamiento, planear, diseñar e implementar todos los detalles técnicos de la solución, entregar los certificados de renovación de garantías del fabricante, entregar los informes y documentación técnica necesarios para la operación de la solución de acuerdo con los alcances y definiciones técnicas contempladas en el Anexo 01 - Especificaciones Técnicas Datacenter, Telecomunicaciones y Servicios Conexos. | X                                                     |    |                         |    |
| 12.                     | Proporcionar el soporte y la realización de la configuración aportando soluciones durante los tiempos de garantía y soporte técnico de acuerdo con los alcances del presente proceso.                                                                                                                                                                                                                                                                            | X                                                     |    |                         |    |
| 13.                     | Garantizar el Cumplimiento de los Acuerdos de Niveles de Servicio de acuerdo con Anexo 08 - Acuerdos de niveles de servicio.                                                                                                                                                                                                                                                                                                                                     | X                                                     |    |                         |    |
| 14.                     | Entregar los informes correspondientes al diseño de la solución, el Plan de Implementación, el Proceso de Implementación y los formatos de entrega en producción la totalidad de equipos.                                                                                                                                                                                                                                                                        | X                                                     |    | X                       |    |
| 15.                     | Entregar los correspondientes niveles de escalamiento para que ICETEX cuente con el soporte correctivo a la plataforma y cada uno de los elementos que formen parte de la solución propuesta por parte del contratista de acuerdo con los alcances del ANEXO No. 1 del presente Estudio Previo.                                                                                                                                                                  | X                                                     |    |                         |    |
| 16.                     | Realizar la gestión ante el fabricante, del soporte correctivo a toda la plataforma descrito en el Anexo 01 - Especificaciones Técnicas Datacenter, Telecomunicaciones y Servicios Conexos, renovación de garantías con fabricante del presente proceso, cuando sea requerido.                                                                                                                                                                                   | X                                                     |    |                         |    |
| 17.                     | Entregar un informe técnico relacionado con la Implementación de licencias de acuerdo con los alcances del Anexo 01 - Especificaciones Técnicas Datacenter, Telecomunicaciones y Servicios Conexos. y la correspondiente renovación de licenciamiento propuesta.                                                                                                                                                                                                 |                                                       |    | X                       |    |
| 18.                     | Brindar capacitación o transferencia de conocimiento y entrega la solución en producción.                                                                                                                                                                                                                                                                                                                                                                        |                                                       | X  |                         |    |
| 19.                     | Garantizar durante todo el plazo del contrato la disponibilidad de la totalidad del personal mínimo requerido. Cualquier modificación del equipo de trabajo deberá ser aprobada por el supervisor de contrato, quien se reserva el derecho de aceptar el cambio. Este cambio se debe realizar con personal que tenga una experiencia equivalente o superior a los perfiles del personal originalmente propuesto.                                                 | X                                                     |    |                         |    |
| 20.                     | Presentar al supervisor del contrato, al momento de la suscripción del acta de inicio, las hojas de vida del equipo de trabajo requerido.                                                                                                                                                                                                                                                                                                                        | X                                                     |    | X                       |    |

**OBSERVACIONES: (SI A ELLO HUBIERE LUGAR)**

Se da continuidad con la operación de los servicios para el mes de noviembre de 2024.

|                   |                                                                                                  |                                                                                     |
|-------------------|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Código: F319      | INFORME MENSUAL DE SUPERVISIÓN<br>VERIFICACIÓN CUMPLIMIENTO DE LAS<br>OBLIGACIONES CONTRACTUALES |  |
| Versión: 5        |                                                                                                  |                                                                                     |
| Fecha: 18/06/2024 |                                                                                                  |                                                                                     |
| Página 3 de 5     |                                                                                                  |                                                                                     |

5

PRODUCTOS ENTREGABLES

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

**OBSERVACIONES: (SI A ELLO HUBIERE LUGAR)**

Presenta informes de octubre de 2024.

Proveedor no presenta la facturación del periodo correspondiente a septiembre de 2024 y octubre de 2024, en consolidación de ANS de los meses sin facturar.

6

¿PROCEDE PAGO EN ESTE PERIODO?

|                          |                                     |
|--------------------------|-------------------------------------|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| SI                       | NO                                  |

**EN CASO DE PROCEDER PAGO SE ANEXA AL PRESENTE INFORME CERTIFICACIÓN PARA PAGO**

No se presenta pago en el periodo supervisado.

7

RELACIÓN DE PAGOS A LA SEGURIDAD SOCIAL Y APORTES PARAFISCALES (SI APLICA)

|  |
|--|
|  |
|--|

8

¿ENTREGÓ INFORME DE ACTIVIDADES?

|                                     |                          |                          |
|-------------------------------------|--------------------------|--------------------------|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| SI                                  | NO                       | NO APLICA                |

9

EJECUCIÓN PRESUPUESTAL

|                              | VIGENCIA (2024)      |
|------------------------------|----------------------|
| VALOR DEL CONTRATO           | \$31.398.996.857,96  |
| VALOR ADICIÓN (Si aplica)    | \$ 0                 |
| VALOR A PAGAR (Si aplica)    | \$ 0                 |
| VALOR EJECUTADO              | \$ 11.372.314.067,00 |
| VALOR PENDIENTE POR EJECUTAR | \$ 20.026.682.790,96 |

10

ANÁLISIS MATERIALIZACIÓN Y MITIGACIÓN DEL RIESGO:

¿DURANTE LA EJECUCIÓN SE MATERIALIZÓ ALGÚN RIESGO?

SI \_\_\_\_ NO X

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

11

REEVALUACIÓN DE CONTRATISTAS / PROVEEDORES:

En caso de ser último pago diligencie la siguiente información de acuerdo con los siguientes parámetros:

|        |           |             |             |
|--------|-----------|-------------|-------------|
| 2 MALO | 3 REGULAR | 4 ACEPTABLE | 5 EXCELENTE |
|--------|-----------|-------------|-------------|

| ASPECTO                       | DESCRIPCIÓN                                                                                                                                                                                                                                                                                          | PUNTAJE |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| CUMPLIMIENTO                  | Las actividades desarrolladas durante el contrato cumplieron con las obligaciones establecidas, los requerimientos técnicos y procedimentales de acuerdo con los lineamientos de la Entidad.                                                                                                         | 5       |
|                               | Las actividades fueron entregadas con oportunidad según las fechas previstas en el contrato o solicitadas por el supervisor.                                                                                                                                                                         | 4       |
| CALIDAD                       | Los productos o entregables cumplen con especificaciones técnicas establecidas en el Contrato                                                                                                                                                                                                        | 3       |
|                               | El personal asignado fue suficiente y tenía las competencias necesarias para ejecutar todas las actividades del contrato.                                                                                                                                                                            | 2       |
| OPORTUNIDAD DE LA INFORMACIÓN | Todas las facturas / cuentas de cobro y sus soportes, la documentación contractual requerida durante la ejecución y la documentación postcontractual fueron entregados y/o publicados de acuerdo con lo establecido en el contrato, procesos y procedimientos internos y normatividad legal vigente. | 5       |
|                               | Entregó informe definitivo de acuerdo con el numeral 2 de la cláusula “Entregables” contemplado dentro del contrato                                                                                                                                                                                  | 1       |

|                   |                                                                                                           |                                                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Código: F319      | <b>INFORME MENSUAL DE SUPERVISIÓN<br/>VERIFICACIÓN CUMPLIMIENTO DE LAS<br/>OBLIGACIONES CONTRACTUALES</b> |  |
| Versión: 5        |                                                                                                           |                                                                                     |
| Fecha: 18/06/2024 |                                                                                                           |                                                                                     |
| Página 5 de 5     |                                                                                                           |                                                                                     |

|                                 |                            |
|---------------------------------|----------------------------|
| REEVALUACIÓN GENERAL            | (Promedio de los puntajes) |
| OBSERVACIONES A LA REEVALUACION |                            |
|                                 |                            |

**NOTA:** Adicionalmente en el último pago se deberá diligenciar el mismo resultado dentro del siguiente formulario con el fin de consolidar la información de acuerdo con lo dispuesto en la Norma ISO 9001 de 2015:

[https://forms.office.com/Pages/ResponsePage.aspx?id=oBw9XnV\\_FECUlgAkkWe-3IzLIMQr2ZVBio5893WxRH1UM0QyVII3N1NVR0pCQIZaTEhLWTRQUU9LOS4u](https://forms.office.com/Pages/ResponsePage.aspx?id=oBw9XnV_FECUlgAkkWe-3IzLIMQr2ZVBio5893WxRH1UM0QyVII3N1NVR0pCQIZaTEhLWTRQUU9LOS4u)

**FECHA DE ELABORACIÓN:** 30/11/2024



VICTOR MANUEL MONDRAGON MACA  
Supervisor  
DIRECTOR DE TECNOLOGIA



VÍCTOR RAÚL BAUTISTA GALINDO  
Supervisor  
Coordinador de Infraestructura



# **INFORME DE ACTIVIDADES DEL CONTRATO**

CONTRATO NUMERO  
2022-0792

Octubre 01 al 31 de 2024

|                                                                                                 |           |
|-------------------------------------------------------------------------------------------------|-----------|
| <b>1. INTRODUCCIÓN .....</b>                                                                    | <b>6</b>  |
| <b>2. OBJETIVOS .....</b>                                                                       | <b>8</b>  |
| <b>3. RESUMEN EJECUTIVO .....</b>                                                               | <b>9</b>  |
| <b>4. SEGURIDAD.....</b>                                                                        | <b>12</b> |
| <b>4.1. Filtrado Web de Sophos.....</b>                                                         | <b>12</b> |
| <b>4.2. Estadística de Portales .....</b>                                                       | <b>12</b> |
| <b>4.3. Estado General de las Plataformas .....</b>                                             | <b>14</b> |
| ➤ <b>FortiGate Triara.....</b>                                                                  | <b>14</b> |
| ➤ <b>FortiGate Aguas .....</b>                                                                  | <b>16</b> |
| ➤ <b>FortiGate Medellín .....</b>                                                               | <b>17</b> |
| ➤ <b>Fortiweb 2000F .....</b>                                                                   | <b>18</b> |
| ➤ <b>Fortiweb 2000E .....</b>                                                                   | <b>18</b> |
| ➤ <b>FortiSandBox.....</b>                                                                      | <b>19</b> |
| <b>4.4. Estado de Salud de los Equipos de Seguridad .....</b>                                   | <b>20</b> |
| <b>4.5. Servicio de centro de Operaciones de Seguridad (SOC) .....</b>                          | <b>20</b> |
| <b>4.6. Monitoreo de Marca-Estrategia OSINT-SOC.....</b>                                        | <b>22</b> |
| ➤ <b>Casos relacionados con Fraudes Digitales.....</b>                                          | <b>23</b> |
| ➤ <b>Casos Relacionados Con Fuga De Datos.....</b>                                              | <b>23</b> |
| ➤ <b>Casos Relacionados Con El Módulo Piratería Online.....</b>                                 | <b>24</b> |
| ➤ <b>Casos Relacionados Con El Módulo Deep &amp; Dark Web .....</b>                             | <b>24</b> |
| ➤ <b>Casos Reportados A La Entidad .....</b>                                                    | <b>25</b> |
| <b>4.7. Análisis de Vulnerabilidades Icetex.....</b>                                            | <b>25</b> |
| ➤ <b>Resumen de Vulnerabilidades .....</b>                                                      | <b>26</b> |
| ➤ <b>Conclusiones Vulnerabilidades.....</b>                                                     | <b>27</b> |
| ➤ <b>Recomendaciones Vulnerabilidades .....</b>                                                 | <b>27</b> |
| <b>4.8. Recomendaciones Generales Seguridad.....</b>                                            | <b>28</b> |
| <b>4.9. Recomendaciones Especificas .....</b>                                                   | <b>30</b> |
| <b>4.10. Conclusiones Seguridad .....</b>                                                       | <b>32</b> |
| <b>5. SOPORTE Y MONITOREO .....</b>                                                             | <b>34</b> |
| <b>5.1. Monitoreo y revisión de ANS y línea Base .....</b>                                      | <b>34</b> |
| <b>5.1.1. Conectividad .....</b>                                                                | <b>34</b> |
| ➤ <b>Internet Para La Gente .....</b>                                                           | <b>39</b> |
| ➤ <b>Canales SDWAN .....</b>                                                                    | <b>41</b> |
| ➤ <b>Canal de Replicación (Triara – Megacenter) .....</b>                                       | <b>41</b> |
| ➤ <b>Señalética (Internet para la gente).....</b>                                               | <b>41</b> |
| ➤ <b>Gestión Equipo Networking Aseguramiento Políticas de Seguridad de la Información .....</b> | <b>42</b> |
| <b>5.1.2. Conclusiones Del Servicio De Conectividad .....</b>                                   | <b>43</b> |
| <b>5.1.3. Recomendaciones Del Servicio De Conectividad .....</b>                                | <b>44</b> |
| <b>5.2. Datacenter Principal .....</b>                                                          | <b>44</b> |
| <b>5.2.1. Disponibilidad de Servicios – Datacenter Principal.....</b>                           | <b>47</b> |

|                                                                                 |           |
|---------------------------------------------------------------------------------|-----------|
| <b>5.2.2. Disponibilidad TRIARA para los servicios de página web.....</b>       | <b>49</b> |
| <b>Recomendaciones.....</b>                                                     | <b>51</b> |
| <b>5.2.3. Análisis componente Liferay Producción .....</b>                      | <b>51</b> |
| <b>5.2.4. Backup Servidores Triara .....</b>                                    | <b>55</b> |
| <b>5.2.5. Recomendaciones Backups .....</b>                                     | <b>57</b> |
| <b>5.3. Datacenter Alterno .....</b>                                            | <b>58</b> |
| <b>5.3.1. Hosting Virtual (IaaS) .....</b>                                      | <b>58</b> |
| <b>5.3.2. Dataguard BBDD Megacenter .....</b>                                   | <b>60</b> |
| <b>5.3.3. Disponibilidad de Servicios de Housing – Datacenter Alterno.....</b>  | <b>61</b> |
| <b>5.3.4. Servicios de DRP.....</b>                                             | <b>61</b> |
| <b>6. ALMACENAMIENTO .....</b>                                                  | <b>63</b> |
| <b>7. APLICACIONES .....</b>                                                    | <b>64</b> |
| <b>7.1. Actividades De Operación.....</b>                                       | <b>64</b> |
| <b>7.2. Profesionales Especializados.....</b>                                   | <b>64</b> |
| ➤ <b>Especialista en Base de Datos DBA.....</b>                                 | <b>64</b> |
| ➤ <b>Especialista Web Máster.....</b>                                           | <b>65</b> |
| ➤ <b>Administrador de Soluciones.....</b>                                       | <b>65</b> |
| ➤ <b>Especialista de Networking .....</b>                                       | <b>65</b> |
| <b>8. Servicios de Videoconferencia .....</b>                                   | <b>66</b> |
| ➤ <b>Disponibilidad del servicio – sedes Bogotá (aguas - ángel).....</b>        | <b>67</b> |
| ➤ <b>Gestión De Incidencias Y Requerimientos – Sedes Regionales.....</b>        | <b>67</b> |
| ➤ <b>Gestión de incidencias y requerimientos – Bogotá (Aguas - Angel) .....</b> | <b>69</b> |
| <b>9. BASES DE DATOS.....</b>                                                   | <b>72</b> |
| ➤ <b>Bases De Datos Oracle Y Tamaño .....</b>                                   | <b>72</b> |
| <b>Conclusiones Bases de Datos.....</b>                                         | <b>73</b> |
| <b>10. CONTROL DE CAMBIOS.....</b>                                              | <b>73</b> |
| <b>11. CALCULO DE CONCILIACION DE LOS SERVICIOS DEL MES DE OCTUBRE .....</b>    | <b>74</b> |
| <b>12. PLAN DE TRABAJO .....</b>                                                | <b>75</b> |
| <b>13. RECOMENDACIONES .....</b>                                                | <b>79</b> |
| <b>14. CONCLUSIONES GENERALES .....</b>                                         | <b>82</b> |

## INDICE DE TABLAS

|                                                                                               |    |
|-----------------------------------------------------------------------------------------------|----|
| Tabla 1 Top 10 de los Portales más utilizados .....                                           | 14 |
| Tabla 2 Total casos por módulo - octubre .....                                                | 25 |
| Tabla 3 Resumen de Vulnerabilidades .....                                                     | 27 |
| Tabla 4 Recomendaciones plataformas de seguridad .....                                        | 31 |
| Tabla 5 Recomendaciones de seguridad para ICETEX .....                                        | 32 |
| Tabla 6 Disponibilidad de canales.....                                                        | 36 |
| Tabla 7 Canales instalados.....                                                               | 37 |
| Tabla 8 Canales pendientes por instalar o en proceso de instalación.....                      | 37 |
| Tabla 9 Canales pruebas de saturación ejecutadas hasta octubre.....                           | 38 |
| Tabla 10 Canales pendientes pruebas de saturación .....                                       | 38 |
| Tabla 11 Canales pendientes por ampliar corte octubre .....                                   | 39 |
| Tabla 12 Disponibilidad canales “Internet para la gente” .....                                | 39 |
| Tabla 13 Disponibilidad canales “SDWAN” .....                                                 | 41 |
| Tabla 14 Estado de la instalación de la señalética de Wifi .....                              | 42 |
| Tabla 15 Evidencia del resumen del Monitoreo CPU- Memoria ELK.....                            | 46 |
| Tabla 16 Evidencia del resumen del Monitoreo CPU-Memoria Servidores OpenShift - ELK .....     | 46 |
| Tabla 17 Evidencia del resumen del monitoreo ELK .....                                        | 47 |
| Tabla 18 Código relacionados disponibilidad servicios en Hosing – Data center Principal ..... | 48 |
| Tabla 19 Disponibilidad de servicios de Hosing -Data center principal.....                    | 49 |
| Tabla 20 Actualización – Análisis componente Liferay octubre .....                            | 53 |
| Tabla 21 Distribución trimestral de accesos por usuarios.....                                 | 54 |
| Tabla 22 Distribución trimestral de backup ejecutados.....                                    | 57 |
| Tabla 23 Distribución trimestral de backup por servidores .....                               | 57 |
| Tabla 24 Servicios replicados – DataCenter Megacenter .....                                   | 60 |
| Tabla 25 Distribución trimestral de replicación.....                                          | 60 |
| Tabla 26 Disponibilidad de los servidores Housing – Datacenter Alerno.....                    | 61 |
| Tabla 27 Recursos – Datacenter Alterno Anexo #3 EC-Alternos IAS.....                          | 63 |
| Tabla 28 Distribución módulos de videoconferencia por sede .....                              | 66 |
| Tabla 29 Distribución trimestral de requerimientos y/o incidentes .....                       | 72 |
| Tabla 30 Tamaño BD Oracle .....                                                               | 72 |
| Tabla 31 Controles de cambio octubre.....                                                     | 74 |
| Tabla 32 Ejecución Presupuestal .....                                                         | 74 |

## INDICE DE ILUSTRACIONES

|                                                                                                  |    |
|--------------------------------------------------------------------------------------------------|----|
| Ilustración 1 Evidencia Estado de seguridad del Sophos.....                                      | 12 |
| Ilustración 2 Evidencia Gráfica Estadísticas de Portales.....                                    | 13 |
| Ilustración 3 Estado General de las Plataformas-FortiGate-Triara.....                            | 14 |
| Ilustración 4 Consumo canal MPLS.....                                                            | 15 |
| Ilustración 5 Consumo canal Internet Sedes .....                                                 | 15 |
| Ilustración 6 Consumo canal Internet Datacenter.....                                             | 15 |
| Ilustración 7 Estado General de las Plataformas-FortiGate-Aguas.....                             | 16 |
| Ilustración 8 Consumo canal MPLS Aguas .....                                                     | 16 |
| Ilustración 9 Estado General de las Plataformas-FortiGate-Medellín .....                         | 17 |
| Ilustración 10 Consumo canal MPLS Datacenter Alterno (Medellín) .....                            | 17 |
| Ilustración 11 Estado General de las Plataformas-Fortiweb 2000F .....                            | 18 |
| Ilustración 12 Estado General de las Plataformas-Fortiweb 2000E .....                            | 19 |
| Ilustración 13 Estado General de las Plataformas- Seguridad FortiSandBox .....                   | 19 |
| Ilustración 14 Total de alertas de seguridad .....                                               | 21 |
| Ilustración 15 Total de alertas de disponibilidad.....                                           | 21 |
| Ilustración 16 Total de alertas de disponibilidad.....                                           | 22 |
| Ilustración 17 Total Tickets analizados en octubre relacionados a Fraudes Digitales.....         | 23 |
| Ilustración 18 Total Tickets analizados en octubre relacionados a Fuga de Datos .....            | 24 |
| Ilustración 199 Total Tickets analizados en octubre relacionados a piratería OnLine .....        | 24 |
| Ilustración 20 Total Tickets analizados en octubre relacionados a Deep & Dark Web .....          | 25 |
| Ilustración 21 Diagrama de red Nuevo Propuesto por Networking .....                              | 43 |
| Ilustración 22 UPTIME: Portal WEB web.icetex.gov.co .....                                        | 49 |
| Ilustración 23 Métrica de visitantes Portal WEB web.icetex.gov.co .....                          | 50 |
| Ilustración 24 Métrica de usuario Portal WEB web.icetex.gov.co .....                             | 50 |
| Ilustración 25 Nodo 1 Vista general.....                                                         | 54 |
| Ilustración 26 Nodo 2 vista general .....                                                        | 54 |
| Ilustración 27 Evidencia Backup Servidores Job Status .....                                      | 56 |
| Ilustración 28 Evidencia Backup Servidores Jobs por Tipo de Aplicación .....                     | 56 |
| Ilustración 29 Evidencia Backup servidores resumen Backups y su estado .....                     | 56 |
| Ilustración 30 Reportes de replicación SRM a Sitio Alterno, octubre 31 2024 .....                | 59 |
| Ilustración 31 Evidencia Dataguard replicado o Megacenter BD .....                               | 60 |
| Ilustración 32 Disponibilidad de servicio videoconferencia sedes regionales – octubre 2024 ..... | 67 |
| Ilustración 33 Disponibilidad de servicio videoconferencia sedes Bogotá – octubre 2024 .....     | 67 |
| Ilustración 34 Incidencias / Requerimientos sedes regionales – octubre 2024 .....                | 68 |
| Ilustración 35 Prueba de funcionamiento sede chapinero – octubre 2024 .....                      | 68 |
| Ilustración 36 Módulo funcional sala 8 piso presidencia – visita octubre 2024.....               | 69 |
| Ilustración 37 Evidencia módulo funcional sede aguas 65 – piso 4 – visita octubre 2024.....      | 70 |
| Ilustración 38 Verificación módulo sede ángel – octubre 2024 .....                               | 71 |

## 1. INTRODUCCIÓN

Este informe contiene la información relacionada con las actividades ejecutadas por INFOTIC en el periodo comprendido entre el 01 al 31 de octubre de 2024, para tal fin se cuenta con un grupo de 10 especialistas y 03 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
- Colaboración
- Centro de Datos
- Seguridad informática
- Servicios de nube
- Servicios Conexos

A la fecha el contrato 2022-0792 que mediante acta de inicio suscrita el 30 de diciembre del 2022, con fecha de iniciación del 19 de enero del 2023, ejecución de los servicios en operación el 1 de abril de 2023, cuenta con un avance en la ejecución del 47.2 % que representa los 17 meses que lleva de ejecución del proyecto que tiene como objetivo *“Servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el ICETEX”*.

El presente informe del mes de octubre de 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 acordado en el contrato.

El informe cuenta adicionalmente con los siguientes anexos que se encuentran en el repositorio de ICETEX para su revisión, evaluación y comentarios:

### **Almacenamiento**

#### **Backus Diarios**

- Backups diarios

#### **Informe de Backus**

- Consolidado mensual Backup octubre
- Reporte Backup octubre 2024

### **Aplicaciones**

- Informe actividades Módulos videoconferencia ICETEX octubre 2024
- Informe mensual Administrador de Soluciones octubre 2024
- Informe mensual Administrador Web Máster octubre 2024
- Informe mensual Integrador Nube octubre 2024

## **Bases De Datos**

- Informe de evidencias Dataguard Megacenter octubre 2024
- Informe mensual Administrador de Bases de datos octubre 2024

## **Control De Cambios**

- Reporte control de cambios octubre

## **Ejecución Presupuestal**

- Conciliación octubre consolidado
- Consolidado informe mensual especialistas octubre
- Informe de Gestión Servicio octubre 2024
- Presentación informe octubre

## **Seguridad**

- Informe Mensual MARCA-OSINT ICETEX octubre 2024
- Informe Mensual Seguridad octubre 2024
- Informe Mensual SOC - TH ICETEX octubre 2024
- Informe técnico análisis de vulnerabilidades Icetex octubre
- Reporte de IPS octubre

## **Reporte total ataques recibidos-SIEM**

- Denegados octubre 01-15
- Denegados octubre 16-31

## **Soporte Y Monitoreo Canales**

- ANS octubre 2024
- Informe mensual Administrador de Networking octubre 2024
- Informe Mensual Disponibilidad octubre 2024

## **Actas De Entrega**

### **Graficas de consumo**

- Informe Mensual ALLOT octubre 2024

## **Pruebas De Saturación**

### **Pruebas Nuevas de Saturación Canales**

### **Data center Alterno**

### **DRP**

- Informe prueba Conectividad Test DRP Icetex\_20241004
- Informe Gerencial ICETEX Prueba Test

## Replicación

- Informe mensual replicación octubre 2024
- Reportes diarios octubre

## Data Center Principal

- Reporte Monitoreo ICETEX octubre 2024-ELK

## 2. OBJETIVO

Presentar el informe de actividades ejecutadas por INFOTIC durante el periodo del 01 al 31 de octubre de 2024, con el fin de determinar el estado, la evolución y disponibilidad de cada una de las gestiones en los diferentes servicios prestados al ICETEX en virtud de la ejecución del contrato, para lo cual se han considerado la recolección de mediciones, 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 accesos, actualizaciones y parches de seguridad.  
Indicadores de incidentes de seguridad y estado de cumplimiento con políticas de ciberseguridad.

- Servicios de Nube:

Reporte de uso de servicios en la nube, desempeño y cumplimiento de niveles de servicio (SLA).  
Descripción de servicios implementados o integrados en el entorno híbrido o multi-nube.

- Servicios Conexos:

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

### 3. RESUMEN EJECUTIVO

En el presente informe se muestra el reporte de las actividades ejecutadas por INFOTIC durante el periodo con el fin de establecer la evolución de cada una de las gestiones en los diferentes servicios prestados al ICETEX.

**Seguridad:** se tuvo las actividades relacionadas con la administración y gestión de la seguridad perimetral.

Dentro de los eventos del mes se realizó configuración de una nueva VPN S2S entre ICETEX y ASPIDA para permitir los servicios de control de acceso y servicios de vigilancia que tiene la Entidad con esta empresa.

También se detectaron alertas de posibles ataques que no fueron detectados por el FortiWeb, se valida con el operador Webmaster, quien indica que las URLs reportadas se encuentran dentro del portal web.icetex.gov.co y este Endpoint se utiliza para extender la sesión de un usuario sin necesidad de recargar la página y por lo cual se consideró como un comportamiento normal del sitio y no fue necesario tomar acciones defensivas en este caso.

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. (8 de octubre, 16 de octubre y 28 de octubre). 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.

Los eventos de escaneos e intentos de explotación de vulnerabilidades reportados por el SOC durante el mes fueron controlados y no representaron un riesgo real para ICETEX, algunos fueron realizados por parte del área de seguridad de ICETEX y otros por el aliado estratégico de INFOTIC. Esto resalta la efectividad de las medidas de seguridad implementadas.

Se atienden los casos de Aranda donde se presentaron faltas 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.

Se atienden los casos de Aranda donde se presentaron faltas 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 21 casos de Aranda y 3 casos fuera de Aranda para un total de 24 casos durante el mes de octubre los cuales se referencian en el ítem de casos.

En el mes de octubre, se han cambiado 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.

Conectividad: Se mantuvo la estabilidad en la operación de los canales de conectividad, garantizando el ancho de banda requerido por ICETEX.

Se gestionaron los casos reportados que afectaban los canales o la herramienta de monitoreo y se coordinó con el operador la instalación de los canales pendientes.

Se corrigieron todas las vulnerabilidades de nivel Crítico y Alto detectadas en el último escaneo y se da continuidad a la remediación de aquellas de nivel Medio y Bajo, según lo indicado en los informes generados por parte de ICETEX con ayuda de la herramienta TENABLE.

Se trabajó en la implementación de IPv6, configurando las interfaces MPLS de los firewalls en Aguas, Triara y Megacenter para habilitar la comunicación entre sedes utilizando IPv6.

Se avanzó en la documentación conforme a los lineamientos de ICETEX.

**Servicios de Colaboración:** Durante el periodo de octubre se garantizó estabilidad y continuidad del servicio de módulos de videoconferencia en las diferentes sedes de la entidad.

Se realizaron pruebas de funcionamiento y limpieza externa de todos los módulos instalados en las sedes de Bogotá, donde se validó el funcionamiento correcto de cada uno, con el apoyo del técnico encargado para este fin, y acompañamiento de personal de la mesa de ayuda de la entidad.

Con el fin de garantizar continuidad del servicio y correcto funcionamiento de los módulos en las sedes regionales, se coordinaron visitas técnicas en cada ciudad (iniciando por las sedes de Medellín y Barranquilla) para iniciar el mes de noviembre, con el fin de realizar mantenimientos preventivos de los equipos y revisiones de funcionamiento o desgaste de piezas que se puedan presentar en los componentes de los módulos para evitar incidencias en la disponibilidad del servicio, revisiones que se continuaran coordinando de manera frecuente, de acuerdo al plan de mantenimientos proyectado para el año entrante, a lo largo del periodo contractual de prestación del servicio. Las evidencias de las actividades realizadas serán registradas en el informe del periodo en el repositorio asignado por el ICETEX, realicen por periodos.

**Centro de Datos:** Los servicios del centro de datos funcionaron de forma normal, en los servidores administrados se realizaron publicaciones sobre las aplicaciones (FrontEnd y BackEnd) tales como: PSE, C&CTEX, TransUnion, Alivios, Desembolsos, Cargue Archivos, etc., las cuales están implementadas en sitios y webservice del servidor web IIS en ambientes de producción, para ello se despliegan nuevas actualizaciones que ejecutan los desarrolladores conforme se van presentando requerimientos que solicitan las áreas funcionales para un mejor desempeño y manejo para los usuarios internos y externos del ICETEX; además se realizaron monitoreo sobre el uso del hardware a nivel de los recursos de CPU, memoria RAM, almacenamiento y sobre del sistema operativo Microsoft Windows Server con respecto a tareas programadas, procesos, revisión de eventos (logs) y AppPool en los servidores ya que es importante mantener el óptimo desempeño, disponibilidad y funcionalidad de las aplicaciones.

Se evidenció un comportamiento estable del portal WEB institucional y se cumplió con el porcentaje de disponibilidad de este con un porcentaje del 99,86% adicional en este informe mensual se incluyeron métricas e indicadores que contribuyen al entendimiento y al comportamiento del servicio.

**Personal del Proyecto en Sitio:** El personal del proyecto operó de manera normal.

Desde INFOTIC se manifestó el riesgo que existe por la falta de las cintas de Backup. La supervisión del contrato está gestionando el proceso de adquisición de dichas cintas al interior del ICETEX para cubrir el proceso de Backups. Desde INFOTIC se ha dado cumplimiento con la gestión de backups.

El presente informe evidencia, además:

- El comportamiento de los canales conforme a los casos reportados en Aranda.
- Reporte que evidencia el rendimiento de la conectividad en términos de capacidad de procesamiento y consumo de recursos durante el mes de octubre del 2024 y la correcta operación de los centros de cómputo tanto principal como alterno.
- Reportes que evidencia la disponibilidad de los servidores y demás equipos de Infraestructura en el centro de datos principal.
- Reporte que evidencia la replicación de las máquinas virtuales desde el centro de datos principal al centro de datos alterno.
- Reporte de monitoreo que se realiza desde los diferentes dispositivos de seguridad que se tienen para la protección de la información de ICETEX.
- Resumen de las solicitudes escaladas a los ingenieros en sitio con sus respectivas recomendaciones.

A continuación, se relacionan los servicios prestados durante el mes de octubre de 2024.

## 4. SEGURIDAD

### 4.1. Filtrado Web de Sophos

Para el despliegue de Web Filter (Filtrado WEB), de Sophos, se ha informado en sesión de pares la necesidad de implementar este control de navegación desde el agente de antivirus. El tema se encuentra en análisis por parte de la oficina de riesgos e infraestructura para del comparativo entregado en el mes de agosto por parte de Seguridad y después de este análisis se definirá cómo se hará la implementación en base a las pruebas realizadas en meses anteriores. Por parte de seguridad se ha recomendado realizarlo de una manera segmentada.

Cabe aclarar que existe una política de Filtrado WEB por defecto, la cual es aplicada a todos los agentes de SOPHOS instalados en los equipos de la entidad, esta información se encuentra en los informes enviados por el operador de seguridad INFOTIC.

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 encuentra en gestión el proceso de la renovación de este componente.



Ilustración 1 Evidencia Estado de seguridad del Sophos

### 4.2. Estadística de Portales

Durante el mes de octubre 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- OCTUBRE.pdf](#) en el capítulo *PORTALES PROTEGIDOS POR EL WAF*.

Como se puede ver en la Ilustración 2, en el periodo de tiempo analizado se presenta un promedio de 800 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 fueron los más consultados, sobre todo en las semanas 42 a la 43 (14 de octubre a 27 de octubre), lo cual es un comportamiento normal para este tipo de transacciones de acuerdo con la actividad de los usuarios y las convocatorias vigentes.

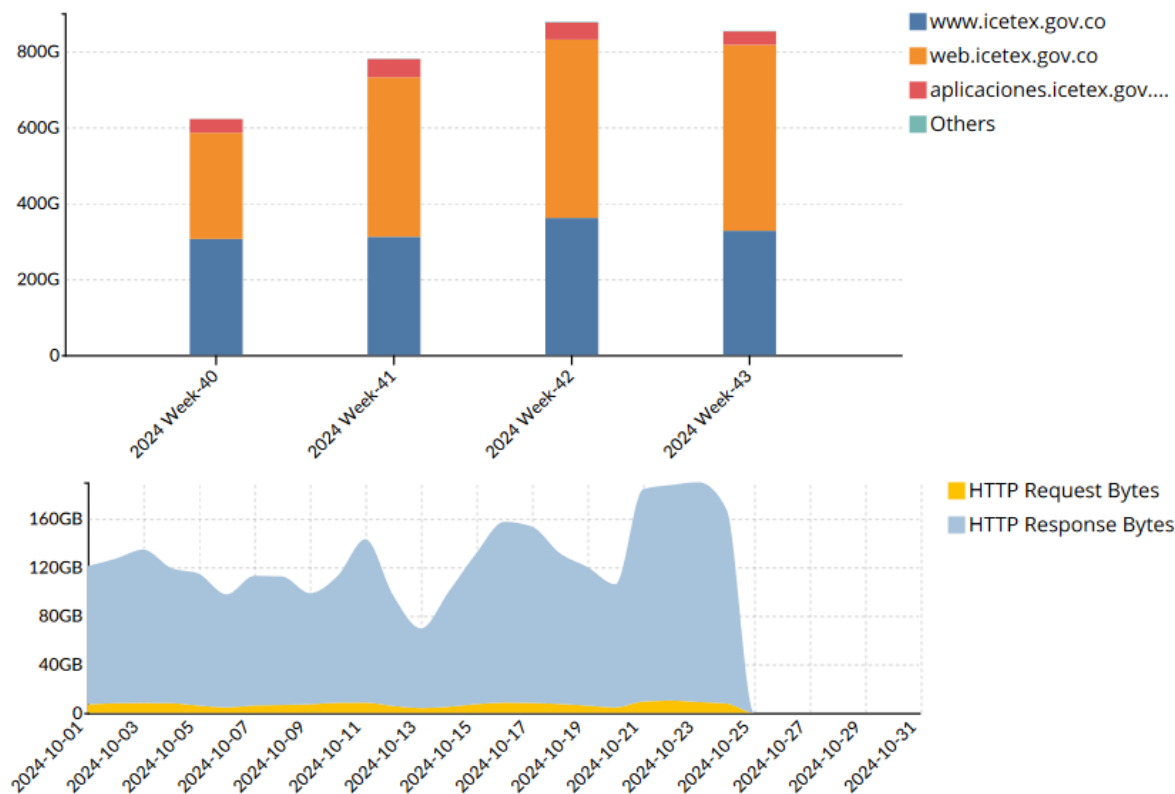


Ilustración 2 Evidencia Gráfica Estadísticas de Portales

Adicional en la Tabla 1, podemos ver los 10 portales más utilizados de acuerdo con la cantidad de solicitudes, siendo web.icetex.gov.co el primero de este top:

| # | HTTP Host                  | HTTP Request Bytes | HTTP Response Bytes |
|---|----------------------------|--------------------|---------------------|
| 1 | web.icetex.gov.co          | 123.70 GB          | 1.51 TB             |
| 2 | www.icetex.gov.co          | 20.13 GB           | 1.19 TB             |
| 3 | aplicaciones.icetex.gov.co | 25.77 GB           | 153.48 GB           |
| 4 | comunidad.icetex.gov.co    | 30.15 MB           | 3.50 GB             |
| 5 | web.icetex.gov.co:443      | 1.08 MB            | 172.79 MB           |

| #  | HTTP Host                   | HTTP Request Bytes | HTTP Response Bytes |
|----|-----------------------------|--------------------|---------------------|
| 6  | comunidad.icetex.gov.co:443 | 659.52 KB          | 128.74 MB           |
| 7  | portal.icetex.gov.co        | 4.02 MB            | 91.31 MB            |
| 8  | 186.84.73.227               | 591.00 KB          | 73.08 MB            |
| 9  | 186.84.73.157               | 266.32 KB          | 47.22 MB            |
| 10 | 186.84.73.163               | 244.23 KB          | 43.73 MB            |

Tabla 1 Top 10 de los Portales más utilizados

### 4.3. Estado General de las Plataformas

En el documento [Reporte Mensual ICETEX- OCTUBRE.pdf](#) se puede encontrar el Informe de Gestión Mensual que contiene información relevante de seguridad para el mes de octubre en lo concerniente a la administración de plataformas incluidas las que son de propiedad del ICETEX y las IaaS:

- FortiWeb
- FortiSandbox
- FortiGate
- Sophos Endpoint
- FortiSIEM

#### ➤ FortiGate Triara

##### System Information

|               |                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------|
| Hostname      | DC_FG_MST_ICETEX                                                                                       |
| Serial Number | FG180FTK22901087  |
| Firmware      | v7.2.9 build1688 (Mature)                                                                              |
| Mode          | NAT                                                                                                    |
| System Time   | 2024/11/01 09:34:36                                                                                    |
| Uptime        | 75:11:35:41                                                                                            |
| WAN IP        |  186.84.155.234     |

Ilustración 3 Estado General de las Plataformas-FortiGate-Triara

Como se evidencia en la Ilustración 3, 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 56.70 Mbps [INR0185 CLARO(MPLS\_DC)] en la última semana, tal como se puede ver en la Ilustración 4.

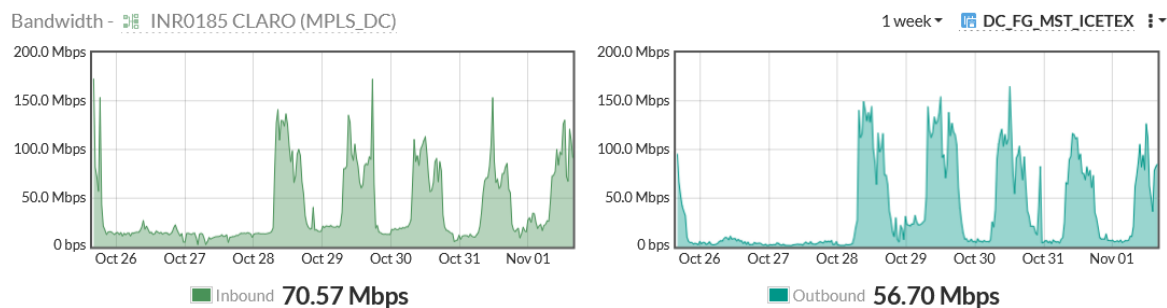


*Ilustración 4 Consumo canal MPLS*

Se observa en la Ilustración 5, que el tráfico hacia la WAN-SEDES-ICETEX [INR0264 (INTE\_SEDES\_ICTX)] en promedio es de 38.49 Mbps en la última semana de octubre.

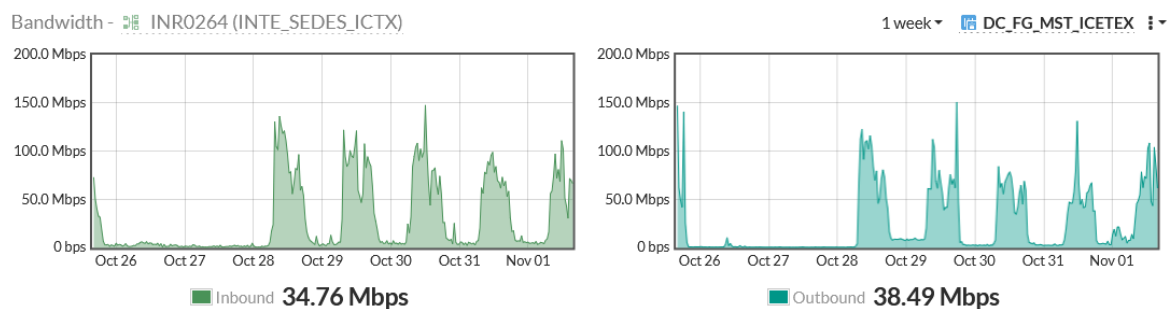


*Ilustración 5 Consumo canal Internet Sedes*

En la Ilustración 6, se observa el tráfico hacia INTERNET DATACENTER [INTERNET\_DC\_INR0000320 (Inet\_claro)] el cual en promedio fue de 73.27 Mbps en la última semana de octubre

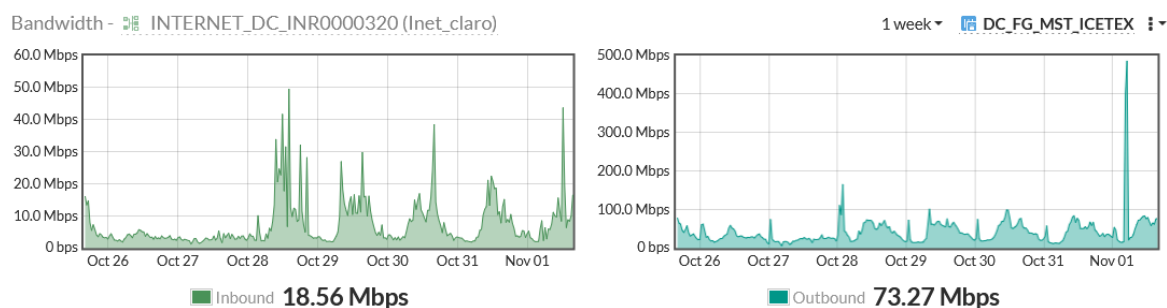


*Ilustración 6 Consumo canal Internet Datacenter*

## ➤ FortiGate Aguas

### System Information

|               |                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------|
| Hostname      | DCAGUAS_FG_MST_ICETEX                                                                                |
| Serial Number | FG6H0FTB22902021  |
| Firmware      | v7.2.9 build1688 (Mature)                                                                            |
| Mode          | NAT                                                                                                  |
| System Time   | 2024/11/01 09:40:16                                                                                  |
| Uptime        | 75:12:00:05                                                                                          |
| WAN IP        |  186.84.155.234     |

*Ilustración 7 Estado General de las Plataformas-FortiGate-Aguas*

A nivel de sistema, en la ilustración 7 se ve el firewall de Aguas (FortiGate 600F), evidenciando que 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, como se observa en la Ilustración 8, el tráfico hacia la MPLS de la sede de Aguas tuvo un promedio de 72.20 Mbps (Port7) en la última semana presente del presente mes.

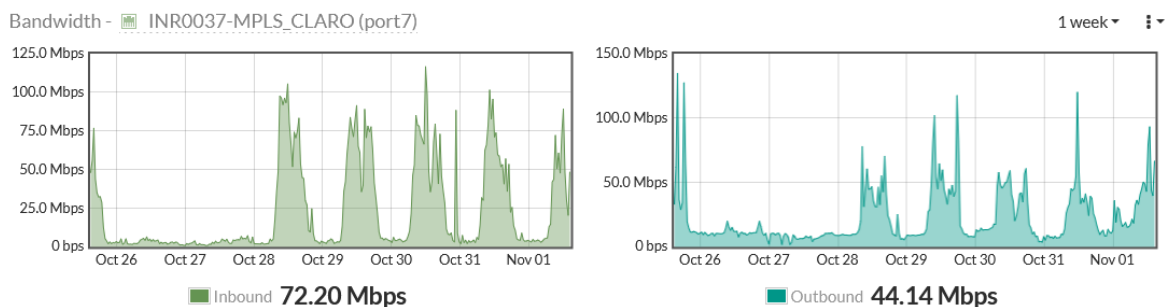


*Ilustración 8 Consumo canal MPLS Aguas*

➤ **FortiGate Medellín**

### System Information

|               |                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------|
| Hostname      | DCB_FG_MST_ICETEX                                                                                    |
| Serial Number | FG6H0FTB22902086  |
| Firmware      | v7.2.9 build1688 (Mature)                                                                            |
| Mode          | NAT                                                                                                  |
| System Time   | 2024/11/01 09:42:31                                                                                  |
| Uptime        | 75:11:24:47                                                                                          |
| WAN IP        |  190.145.153.186    |

*Ilustración 9 Estado General de las Plataformas-FortiGate-Medellín*

A nivel de sistema, se muestra en la Ilustración 9, que el firewall de Medellín (FortiGate 600F), no presenta afectaciones en cuanto a licenciamiento o performance y 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 10, que la interfaz de la MPLS del Data Center de Medellín no presenta tráfico debido a que este se tiene como Data Center Alterno.

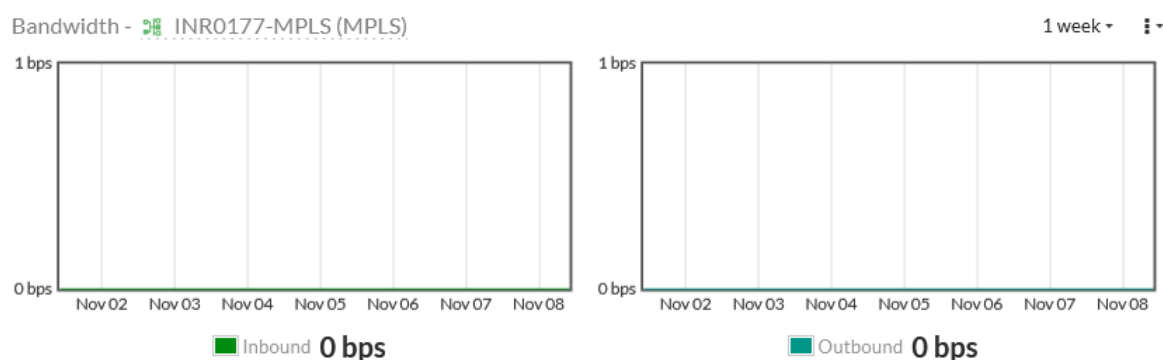


*Ilustración 10 Consumo canal MPLS Datacenter Alterno (Medellín)*

### ➤ Fortiweb 2000F

| System Information                        |                                              | ↺ | ⬇ | ⓘ |
|-------------------------------------------|----------------------------------------------|---|---|---|
| HA Status                                 | Standalone                                   |   |   |   |
| Host Name                                 | FortiWeb_ICETEX                              |   |   |   |
| Serial Number                             | FV-2KFTE21000029                             |   |   |   |
| Operation Mode                            | Reverse Proxy                                |   |   |   |
| System Time                               | Fri Nov 1 09:43:17 2024                      |   |   |   |
| Firmware Version                          | FortiWeb-2000F<br>7.4.4,build0649(GA),240628 |   |   |   |
| System Uptime                             | [75 day(s) 11 hour(s) 5 min(s)]              |   |   |   |
| Administrative Domain                     | ✖ Disabled                                   |   |   |   |
| Threat Analytics <a href="#">↗</a>        | <div>Start Trial</div>                       |   |   |   |
| Advanced Bot Protection <a href="#">↗</a> | ✖ Disabled                                   |   |   |   |

*Ilustración 11 Estado General de las Plataformas-Fortiweb 2000F*

A nivel de sistema, en la Ilustración 11 se muestra que 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.

### ➤ Fortiweb 2000E

A nivel de sistema, en la ilustración 12 se muestra el FortiWeb y su configuración actual y versión de Firmware 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.

| System Information    |                                                                                                  | 🔄 ⬇️ ⌵ |
|-----------------------|--------------------------------------------------------------------------------------------------|--------|
| HA Status             | Active-Passive                                                                                   |        |
| Cluster Name          | Icetex                                                                                           |        |
| Cluster Members       | ICTX_FORTIWEB1/ FV-2KE3117000046<br>(Primary)<br>ICTX_FORTIWEB2/ FV-2KE3117000032<br>(Secondary) |        |
| Serial Number         | FV-2KE3117000046                                                                                 |        |
| Operation Mode        | Reverse Proxy                                                                                    |        |
| System Time           | Fri Nov 1 10:03:46 2024                                                                          |        |
| Firmware Version      | FortiWeb-2000E 7.4.4,build0649(GA),240628                                                        |        |
| System Uptime         | [75 day(s) 11 hour(s) 10 min(s)]                                                                 |        |
| Administrative Domain | 🛑 Disabled                                                                                       |        |
| Threat Analytics      | <a href="#">Start Trial</a>                                                                      |        |

*Ilustración 12 Estado General de las Plataformas-Fortiweb 2000E*

## ➤ FortiSandBox

| System Information                   |                                                                | ✎ 🔄 ✕ |
|--------------------------------------|----------------------------------------------------------------|-------|
| Unit Type                            | Standalone                                                     |       |
| Host Name                            | fsa.icetex.gov.co <a href="#">[Change]</a>                     |       |
| Serial Number                        | FSA1KD3A17000156                                               |       |
| System Time                          | Fri Nov 1 10:05:59 2024 -05 <a href="#">[Change]</a>           |       |
| Firmware Version                     | v3.2.4,build0279 (GA) <a href="#">[All firmwares]</a>          |       |
| System Configuration                 | Last Backup: 2024-03-07 21:04 <a href="#">[Backup/Restore]</a> |       |
| Current User                         | jairo.acevedo                                                  |       |
| Uptime                               | 238 day(s) 12 hour(s) 24 minute(s)                             |       |
| Windows VM                           | ✅ <a href="#">[Upload License]</a>                             |       |
| Microsoft Office                     | ✅ <a href="#">[Upload License]</a>                             |       |
| VM Internet Access                   | ✅                                                              |       |
| FDN Download Server                  | ✅                                                              |       |
| Community Cloud Server               | ✅                                                              |       |
| Web Filtering Server                 | ✅                                                              |       |
| Antivirus DB Contract                | 🛑 2023-06-20                                                   |       |
| Web Filtering Contract               | 🛑 2023-06-20                                                   |       |
| MTA Contract                         | 🛑 No Contract                                                  |       |
| MacOS VM Contract                    | 🛑 No Contract                                                  |       |
| Industry Security Signature Contract | 🛑 No Contract                                                  |       |

*Ilustración 13 Estado General de las Plataformas- Seguridad FortiSandBox*

A nivel de sistema, en la Ilustración 13 visualizamos que 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 este está en proceso de EOL (término empleado por el fabricante para describir un producto que pronto será reemplazado por una nueva generación de tecnología)

#### ➤ **Sophos Endpoint**

Como se observa en la Ilustración 1, 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.

### **4.4. Estado de Salud de los Equipos de Seguridad**

En el transcurso del mes de octubre se mantuvo el monitoreo en el tráfico WAN hacia la MPLS, revisando permanentemente el estado de estas el cual tuvo un comportamiento normal, esto se puede en las gráficas de consumos de los canales de las plataformas en resumen en numeral 4.3 de este informe o más ampliamente en el documento [Informe Mensual Seguridad Octubre 2024.pdf](#)

### **4.5. Servicio de centro de Operaciones de Seguridad (SOC)**

Durante el mes de octubre en el ICETEX, el SOC ha continuado en su adaptación y evolución conforme al cambio en las necesidades del ICETEX por lo cual de manera permanente se mantiene actualizado de acuerdo con la nueva realidad. El detalle se puede ver en el siguiente link [Informe Mensual SOC - TH ICETEX octubre 2024.pdf](#)

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.

Por último, se define un proceso de reporte acorde con los acuerdos de niveles de servicio establecidos y una recopilación de lo reportado de cara a la gestión del SOC de manera mensual. 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 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)

### ➤ Alertas o incidentes de seguridad detectados

En el [Informe Mensual SOC - TH ICETEX octubre 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 y 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.

### ➤ 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   | 4,609           |
| High     | 436             |
| Low      | 293             |

*Ilustración 14 Total de alertas de seguridad*

### ➤ 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   | 84,256          |
| Low      | 656             |
| High     | 88              |

*Ilustración 15 Total de alertas de disponibilidad*

### ➤ 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   | 5,242           |
| High     | 1,119           |

*Ilustración 16 Total de alertas de disponibilidad*

## ➤ 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 se relacionan en el informe mensual [Informe Mensual SOC - TH ICETEX octubre 2024.pdf](#)

## 4.6. Monitoreo de Marca-Estrategia OSINT-SOC

Para el mes de octubre y de acuerdo con lo programado se continuó con el monitoreo de marca, donde se implementó la estrategia OSINT(Open Source Intelligence), como técnicas y herramientas que permitan recopilar información pública, analizar los datos y correlacionarlos convirtiéndolos en conocimiento útil, de forma tal que el SOC sea una fuente importante y de primera línea para informar al supervisor del contrato frente a campañas en redes sociales, en la Deep Web en la Dark Net en contra del ICETEX, investigación de sitios web y apps que intenten suplantar al ICETEX y sus servicios, lo cual permitirá tomar acciones inmediatas y activar planes de emergencia ante situaciones de ciberseguridad con el servicio de monitoreo de la plataforma AXUR.

Durante el transcurso del mes se fueron incluyendo parámetros de acuerdo con lo requerido por el ICETEX, cabe anotar que como los métodos de utilización fraudulenta de marca cambian también nuestro sistema evoluciona. El detalle se puede ver en el siguiente [Informe Mensual MARCA-OSINT ICETEX octubre 2024.pdf](#).

El monitoreo de protección marca y OSINT a través de la herramienta AXUR, fue configurada al inicio de proyecto con información propia de la entidad con el fin de monitorear, detectar y eliminar aquellos riesgos y fraudes online que son una gran amenaza para la reputación y la seguridad de su

marca en la Internet, a través de los siguientes servicios o módulos:

- Fuga de datos: Credenciales y datos sensibles expuestos.
- Piratería Online: Ventas y distribuciones no autorizadas.
- Deep & Dark Web: Mención de la marca en entornos no indexados.

Los resultados de forma resumida para este mes, desde los diferentes frentes son los siguientes, sin embargo, el detalle de cada uno de los casos se puede ver ampliamente en el [Informe Mensual MARCA-OSINT ICETEX octubre 2024.pdf](#) . :

### ➤ Casos relacionados con Fraudes Digitales

Durante el periodo evaluado, se presentaron 65 casos, de los cuales 62 fueron descartados, teniendo en cuenta que algunos no tenían relación y otros solo hacían mención de la entidad y 03 casos fueron reportados a la entidad y se encuentran en estado de tratamiento.

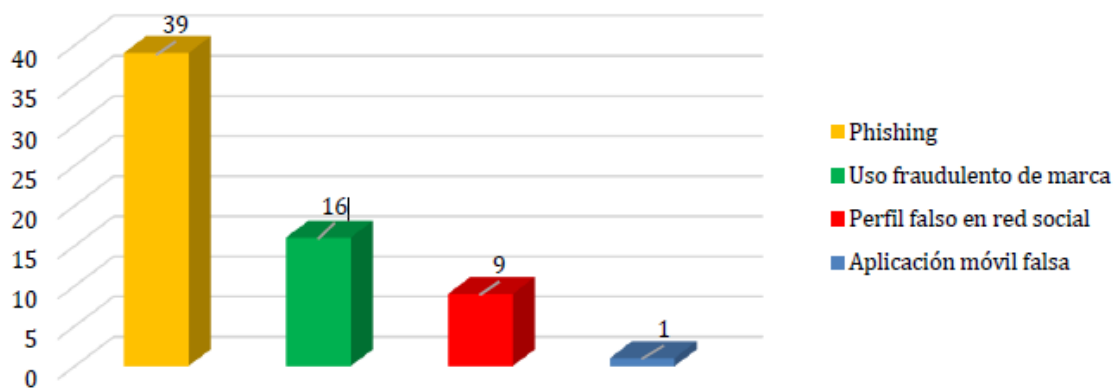


*Ilustración 17 Total Tickets analizados en octubre relacionados a Fraudes Digitales*

### ➤ Casos Relacionados Con Fuga De Datos

Se presentaron 38 casos, de los cuales todos fueron descartados, teniendo en cuenta que algunos no tenían relación con la entidad o solo se hacía mención de esta.

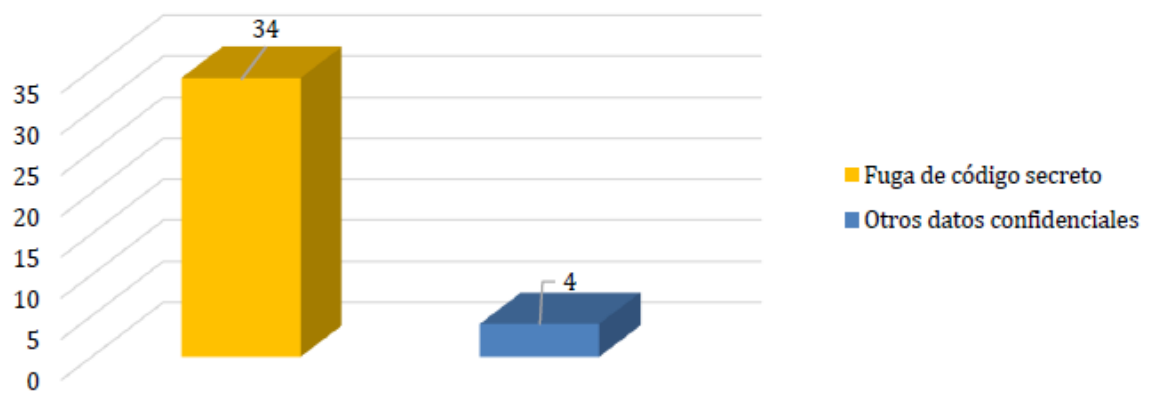


Ilustración 18 Total Tickets analizados en octubre relacionados a Fuga de Datos

#### ➤ Casos Relacionados Con El Módulo Piratería Online

Se presentaron 03 casos, de los cuales 2 fueron reportados a la entidad y se encuentran en estado de tratamiento y 01 caso fue descartado, teniendo en cuenta que solo se hacía mención del nombre de la marca.



Ilustración 19 Total Tickets analizados en octubre relacionados a piratería OnLine

#### ➤ Casos Relacionados Con El Módulo Deep & Dark Web

Se presentaron 8 casos relacionados con la Deep & Dark Web, los cuales fueron descartados, teniendo en cuenta que solo se mencionaba la marca en forma de burla o en algunos casos no tenía relación con la entidad.

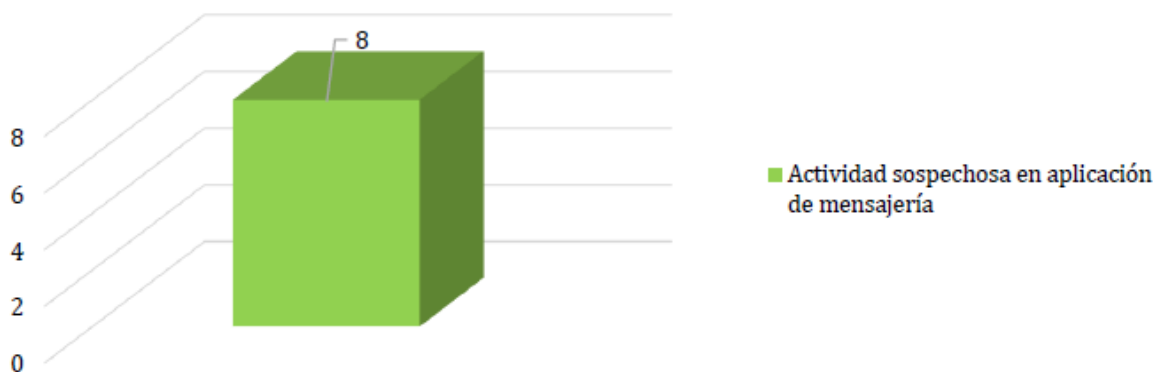


Ilustración 20 Total Tickets analizados en octubre relacionados a Deep & Dark Web

### ➤ Casos Reportados A La Entidad

Se reportaron 4 casos a la entidad, de los cuales a todos se les realizó la gestión correspondiente y se encuentran en tratamiento.

| CLASIFICACIÓN DE LA ALERTA | ESTADO RESUELTO | ESTADO NO RESUELTO | ESTADO EN TRATAMIENTO | ESTADO DESCARTADA | TOTAL GENERAL |
|----------------------------|-----------------|--------------------|-----------------------|-------------------|---------------|
| Fraudes Digitales          | 0               | 0                  | 3                     | 62                | 65            |
| Fuga De Datos              | 0               | 0                  | 0                     | 38                | 38            |
| Piratería Online           | 0               | 0                  | 2                     | 1                 | 3             |
| Deep & Dark Web            | 0               | 0                  | 0                     | 8                 | 8             |
| Total General              | 0               | 0                  | 5                     | 109               | 114           |

Tabla 2 Total casos por módulo - octubre

### 4.7. Análisis de Vulnerabilidades Ictetex

Durante el presente mes, se realizó un análisis exhaustivo de la seguridad de los activos de información de la organización, con un enfoque particular en servidores críticos y servicios de red. Las actividades fueron respaldadas por herramientas de evaluación avanzadas como Nessus Professional, OpenVAS, Burp Suite Pro y Kali Linux. Estos análisis permitieron identificar y priorizar vulnerabilidades clave, así como proponer acciones correctivas. Las actividades más destacadas incluyen:

- **Revisión de configuraciones de seguridad:** Se encontraron varias configuraciones inseguras en servicios como SMB, SSH y Terminal Services, que fueron documentadas y corregidas para reducir el riesgo de accesos no autorizados y ataques de intermediario (MitM).
- **Evaluación de criptografía y protocolos de comunicación:** Las herramientas utilizadas detectaron el uso de algoritmos y protocolos obsoletos, como el cifrado CBC en SSH y el uso de TLS 1.0/1.1. Se brindaron recomendaciones para la migración a versiones más seguras como TLS 1.2 o superior y el uso de cifrados más robustos como AES.
- **Escaneo y auditoría de puertos:** El análisis de puertos permitió identificar aquellos que representaban vectores de ataque significativos. Se propuso su cierre o filtrado como una

medida de fortalecimiento de la seguridad perimetral.

- **Mejora continua:** La comparación con evaluaciones previas mostró una reducción en la cantidad y severidad de las vulnerabilidades detectadas, lo cual es indicativo de una mejora en la postura de seguridad de los activos evaluados. La implementación de recomendaciones anteriores fue fundamental para la reducción del riesgo.

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 \(Octubre\).pdf](#):

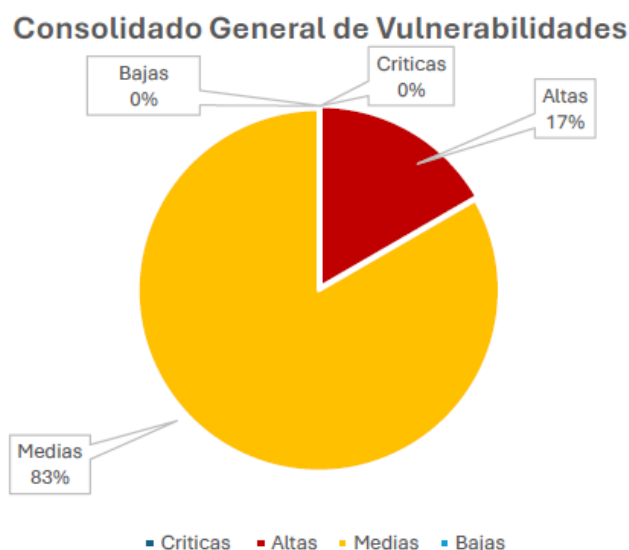


*Ilustración 21 Consolidado porcentual de las vulnerabilidades identificadas*

### ➤ Resumen de Vulnerabilidades

A continuación, se presenta un resumen consolidado de las vulnerabilidades identificadas durante las pruebas de seguridad realizadas. Este resumen se estructura en una tabla que detalla para cada vulnerabilidad su nivel de severidad, el identificador o ID asignado, el nombre de la vulnerabilidad y los dispositivos, sistemas o componentes que se verían afectados en caso de una explotación.

| Severidad | ID       | Vulnerabilidad                                        | Dispositivos afectados                                                                                                              |
|-----------|----------|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| High      | VULN-001 | SSL Medium Strength Cipher Suites Supported (SWEET32) | IP Equipos Finales: 10.1.1.20, 10.1.1.23, 10.1.1.33, 10.1.1.42, 10.1.1.62, 10.1.4.85, 10.1.11.8, 10.1.16.60 Puerto TCP/3389 (msrdp) |
| Medium    | VULN-002 | TLS Version 1.0 Protocol Detection                    | IP Equipo Final: 10.1.1.20, 10.1.1.23, 10.1.1.33, 10.1.1.42, 10.1.1.62, 10.1.4.85, 10.1.11.8, 10.1.16.60 Puerto TCP/3389            |

|                       |          |                                                                             |                                                                                                                                              |
|-----------------------|----------|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Medium</b>         | VULN-003 | TLS VersionVersión 1.1 Protocol<br>Deprecated                               | IP Equipo Final:10.1.1.20,<br>10.1.1.23, 10.1.1.33, 10.1.1.42,<br>10.1.1.62, 10.1.4.85, 10.1.11.8,<br>10.1.16.60<br>Puerto TCP/3389          |
| <b>Medium</b>         | VULN-005 | SSL RC4 Cipher Suites Supported<br>(Bar Mitzvah)                            | IP Equipo Final: 10.1.1.20,<br>10.1.1.23, 10.1.1.33, 10.1.1.42,<br>10.1.1.62, 10.1.4.85, 10.1.11.8<br>Puerto TCP/3389                        |
| <b>Medium</b>         | VULN-006 | SMB Signing not required                                                    | IP Equipo Final: 10.1.6.5,<br>10.1.16.85 Puerto TCP/3389                                                                                     |
| <b>Total, General</b> | VULN-007 | Terminal Services Doesn't Use<br>Network Level Authentication<br>(NLA) Only | IP Equipo Final: 10.1.1.20,<br>10.1.1.23, 10.1.1.33, 10.1.1.42,<br>10.1.1.62, 10.1.4.85, 10.1.11.8,<br>10.1.16.60<br>Puerto TCP/3389 (msrdp) |

*Tabla 3 Resumen de Vulnerabilidades*

### ➤ Conclusiones Vulnerabilidades

Luego de las pruebas técnicas realizadas sobre la infraestructura tecnológica mencionadas en el alcance del escaneo, se detectó la existencia de diversas vulnerabilidades que comprometen la seguridad de la información y la continuidad de las operaciones.

Las configuraciones de cifrado inseguras, como el soporte de cifrados de fuerza media y el uso de protocolos obsoletos, representan un riesgo elevado para la infraestructura, exponiéndola a posibles ataques que explotan vulnerabilidades conocidas.

La ausencia de configuraciones de autenticación reforzada en servicios críticos, como SMB y Terminal Services, incrementa el riesgo de accesos no autorizados y compromete la continuidad de las operaciones en caso de un ataque.

La infraestructura evaluada requiere mejoras en sus controles de seguridad para alinearse con las prácticas recomendadas y estándares actuales. La presencia de protocolos y configuraciones inseguras evidencia la necesidad de una revisión y actualización constantes para minimizar la exposición a amenazas y garantizar la protección efectiva de los activos de información.

### ➤ Recomendaciones Vulnerabilidades

Entre las principales recomendaciones propuestas para mejorar el estado de seguridad frente a las vulnerabilidades reportadas se destacan:

- Actualizar los protocolos de cifrado y deshabilitar versiones obsoletas: Se recomienda deshabilitar TLS 1.0 y TLS 1.1 en toda la infraestructura y asegurar que los servicios utilicen al menos TLS 1.2 o versiones superiores, las cuales proporcionan un nivel de seguridad adecuado frente a ataques modernos.

- Eliminar los cifrados de fuerza media y RC4: Deshabilitar los cifrados de fuerza media (vulnerabilidad SWEET32) y el cifrado RC4 (vulnerabilidad Bar Mitzvah) en todos los servicios que soporten TLS y SSL, ya que estos cifrados presentan riesgos elevados y están desaconsejados por los estándares de seguridad actuales.
- Habilitar SMB Signing en todos los servidores y dispositivos de usuario final: Implementar la firma de SMB obligatoria para proteger la integridad de las comunicaciones SMB, reduciendo el riesgo de interceptación y manipulación de datos durante el tránsito.
- Configurar la Autenticación a Nivel de Red (NLA) en Terminal Services: Activar la Autenticación a Nivel de Red (NLA) en todos los servicios de Terminal Services para asegurar que solo los usuarios autenticados tengan acceso, lo cual reduce la superficie de ataque frente a intentos de acceso no autorizados.
- Realizar auditorías de seguridad periódicas: Implementar una política de auditoría de seguridad regular que permita monitorear y evaluar continuamente las configuraciones de cifrado, autenticación y otros controles críticos, asegurando así que la infraestructura mantenga una postura de seguridad alineada con los estándares actuales.

El detalle del análisis de vulnerabilidades se puede consultar en el documento: [INFORME TÉCNICO ANÁLISIS DE VULNERABILIDADES ICETEX \(Octubre\).pdf](#)

- Observaciones de ICETEX Vulnerabilidades:

Dado que no se han cerrado todas las vulnerabilidades identificadas en el ejercicio de Ethical Hacking del primer semestre de 2024, se solicita que INFOTIC incluya en los informes mensuales un detalle de todas las actividades y avances en curso. Esto debe incluir las acciones ejecutadas por los especialistas en sitio de INFOTIC y/o los aliados estratégicos expertos en seguridad informática, en coordinación con los líderes de seguridad de ICETEX. El objetivo es mitigar los riesgos asociados a las vulnerabilidades, tanto internas como externas, que puedan afectar la operación de ICETEX.

El cierre de vulnerabilidades se realiza en conjunto con ICETEX, INFOTIC y los aliados del proyecto. Para ello, se elabora un inventario de las vulnerabilidades, asignándolas a los responsables según las líneas de servicio. En esta etapa, se clasifican las vulnerabilidades que pueden gestionarse y aquellas que no, como las asociadas a equipos fuera de soporte del fabricante. Además, ICETEX realiza escaneos continuos para validar las remediaciones realizadas por el proveedor con el propósito de garantizar su mitigación e identificar nuevas vulnerabilidades.

#### **4.8. Recomendaciones Generales Seguridad**

- Con respecto a la gestión que se ha venido realizando, se recomienda continuar con las validaciones y retroalimentación para cierres de casos, con el fin de mitigar las brechas de seguridad detectadas a través de la plataforma de monitoreo de protección de marca y OSINT.
- Con respecto a los casos de Fraudes Digitales – Aplicación móvil falsa – Phishing recordar las medidas a considerar:

- Verificar el portal y aplicación si corresponde y son propiedad de la entidad.
  - En el caso que no se considere un fraude para la entidad responder este correo y se procederá a cerrar el caso como Resuelto.
- Con respecto a los casos de Piratería Online – Producto falso o Venta Irregular recordar las medidas a considerar:
- Verificar la venta publicada si se trata de un producto o venta falso o si corresponde y es propiedad de la entidad.
  - Si estos productos o ventas están autorizados o no representa un Fraude digital, responder el correo para marcar los tickets como Cerrado: Resuelto.
- Verificar el estado de los dispositivos monitoreados y realizar depuración de equipos que no se encuentren en operación.
- Verificar con software antimalware, los equipos con direcciones IP origen relacionados en la alerta “Tráfico Permitido o Denegado Hacia IoC Maliciosas – WX” la cual detecta tráfico hacia direcciones IP “maliciosas”. Lo anterior puede indicar que el equipo con IP Origen probablemente está infectado por malware y está intentando conexiones a servidores de comando y control (C&C) o está tratando de iniciar una infección, independientemente si fue negado o permitido el tráfico.
- Realizar bloqueo de las direcciones IP origen o destinos identificadas como maliciosas en indicadores de compromisos- IoC, en los equipos de seguridad perimetral.
- Verificar y aumentar los recursos del FortiSIEM, como se ha solicitado desde meses anteriores, en razón a que se están presentando alertas críticas de almacenamiento de logs eventos y de CPU que impiden el correcto desarrollo de reportes mensuales.
- Verificar los dispositivos que están presentando errores para la lectura de eventos desde el FortiSIEM a través de los protocolos WMI y VM\_SDK.
- Verificar las alertas y reportes enviados y en lo posible dar respuesta o retroalimentar al SOC con el actualizar cada uno casos y realizar las correspondientes excepciones o filtros con el fin de disminuir las alertas y falsos positivos.
- Revisar los dispositivos que se encuentran en las alertas de rendimiento y si es posible aumentar la capacidad de recursos que en ellos se usan para evitar demoras y/o retrasos de servicio. Por ahora ningún servicio se ha visto indisponible a causa de recursos internos de los dispositivos que se usan para llevar a cabo dichos servicios.
- Cabe resaltar que cada reporte generado o emitido desde el área del SOC, se le realizo su respectivo informe describiendo el análisis aplicado en cada uno y se reportó por correo, además se realizó un control de las alertas presentadas y un seguimiento a los casos.

#### 4.9. Recomendaciones Específicas

| Recomendación                                                                                                                                                                               | Estado                                                                                                                                                                                                                                                                                                                  | Criticidad | Fecha de notificación a ICETEX                           | Responsable                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|----------------------------------------------------------|--------------------------------------------------------------------------------------|
| Se deben segmentar las políticas de acuerdo con la necesidad y no otorgar acceso de toda una red o todos los servicios.                                                                     | Al depurar las políticas en los firewalls, se ha venido analizando el tráfico que pasa sobre las políticas con origen, destino, puertos en ALL y en base a este análisis se ha ido alineando estas políticas para permitir solo el tráfico necesario y cerrar brechas de seguridad asociadas a esta configuración.      | Media      | N/A                                                      | N/A                                                                                  |
| Se debe trabajar en el perfilamiento de la navegación de acuerdo con lo entregado por ICETEX.                                                                                               | Se sigue a la espera por parte de ICETEX la definición de los grupos. A nivel de la consola de Antivirus y en base a las pruebas que se han realizado, se está a la espera de exponer los resultados y que ICETEX tome la decisión en cuanto a cómo se implementara estos perfiles de Web filter.                       | Media-alta | 06/09/2023                                               | Lideres de NETWORKING de parte de INFOTIC y lideres de networking de parte de ICETEX |
| Realizar autenticación a través del LDAP, para la gestión de las plataformas de seguridad.                                                                                                  | Se integra el FortiGate de Triara, se evalúa la posibilidad con las otras plataformas. Se está a la espera de una sesión para implementar LDAP seguro con certificado y que este sea compartido por ICETEX para aplicarlo en el firewall y fortalecer la capa de seguridad con respecto a la autenticación de usuarios. | Media      | 29/07/2024                                               | Lideres de NETWORKING de parte de INFOTIC y lideres de networking de parte de ICETEX |
| Validar la posibilidad de la integración de la Consola Sophos con SIEM.                                                                                                                     | Se debe ampliar la capacidad del SIEM. En este momento se tiene una integración entre las plataformas para captura de logs sobre las API de Sophos y los eventos que este reporta y se visualizan correctamente en el SIEM.                                                                                             | Baja       |                                                          |                                                                                      |
| 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. | En revisión de ICETEX                                                                                                                                                                                                                                                                                                   | Baja       |                                                          |                                                                                      |
| Realizar la contención automática de equipos que se identifiquen en la red como maliciosos                                                                                                  | En revisión de ICETEX                                                                                                                                                                                                                                                                                                   | Media      | 30/07/2024<br>23/09/2024                                 | Lideres de NETWORKING de parte de INFOTIC y lideres de networking de parte de ICETEX |
| Realizar el aumento de recursos a la plataforma de FortiSIEM (CPU, Memoria y disco) y hacer                                                                                                 | En revisión de ICETEX                                                                                                                                                                                                                                                                                                   | Alta       | 21/07/2023-<br>05/02/2024-<br>25/07/2024-<br>19/09/2024- | Lideres de NETWORKING de parte de INFOTIC y lideres de                               |

|                                                                                                                       |                                                                                            |      |            |                               |
|-----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|------|------------|-------------------------------|
| un cambio de arquitectura con el objetivo de mejorar.                                                                 |                                                                                            |      | 03/10/2024 | networking de parte de ICETEX |
| Se debe evaluar la mejor forma a nivel de seguridad la conmutación hacia Medellín generando el menor costo de tiempo. | Se está evaluando y los ejercicios de prueba test y DRP nos orientaran sobre el ejercicio. | Baja |            |                               |

*Tabla 4 Recomendaciones plataformas de seguridad*

| Recomendación                                                                                                                                                              | Estado                                                                                                                                                                                                                                                                                                                 | Criticidad | Fecha de notificación a ICETEX | Responsable                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|--------------------------------|---------------------------------------------------------------------------------------------------|
| Garantizar la segmentación de la red que permita claramente definir qué servicios deben ser alcanzados por cada usuario.                                                   | Como parte de las pruebas de IPv6, se están realizando pruebas de DHCPv6 en la red para que el servidor entregue direccionamiento IPv6 a las redes de la Entidad y que esta segmentación cumpla los estándares del protocolo IPv6.                                                                                     | Media      | 26/09/2023                     | Lideres de NETWORKING de parte de INFOTIC y lideres de networking de parte de ICETEX              |
| Se recomienda una tecnología que permita realizar análisis de tráfico de la red (NTA-Network Traffic Analysis).                                                            | En revisión de ICETEX                                                                                                                                                                                                                                                                                                  | Alta       | N/A                            | N/A                                                                                               |
| Se recomienda una tecnología que permita la gestión o validación de privilegios de accesos (IAM). Evitar configurar usuarios y claves dentro de las aplicaciones de ICETEX | En revisión de ICETEX                                                                                                                                                                                                                                                                                                  | Alta       | N/A                            | N/A                                                                                               |
| Validar a nivel de punto final los equipos que se han visto involucrados con comportamiento malicioso.                                                                     | Se evalúa por parte de ICETEX. Se hace seguimiento por parte del SOC quien reporta comportamiento malicioso. Sin embargo, es necesario establecer políticas de conexión de equipos externos BYOD debido a que muchos de los casos reportados por el SOC vienen de equipos personales que no hacen parte de la Entidad. | Critica    | N/A                            | N/A                                                                                               |
| Integrar los servidores de Directorio Activo con el SIEM.                                                                                                                  | Se debe evaluar la capacidad del SIEM, se espera plan de mejora.                                                                                                                                                                                                                                                       | Media      | 29/07/2024                     | Lideres de NETWORKING de parte de INFOTIC y lideres de networking de parte de ICETEX seguridad de |

|                                                                                                                                                                                                            |                                                                  |       |                                                        |                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|-------|--------------------------------------------------------|--------------------------------------------------------------------------------------|
|                                                                                                                                                                                                            |                                                                  |       |                                                        | parte de ICETEX                                                                      |
| Integrar los equipos que hacen parte del proceso de pagos con el SIEM.                                                                                                                                     | Se debe evaluar la capacidad del SIEM, se espera plan de mejora. | Media | 21/07/2023-05/02/2024-25/07/2024-19/09/2024-03/10/2024 | Lideres de NETWORKING de parte de INFOTIC y lideres de networking de parte de ICETEX |
| Adquirir un equipo Firewall para correo para prevenir brechas de seguridad asociadas al uso del correo electrónico y que este es susceptible a muchos tipos de amenazas.                                   | En revisión de ICETEX                                            | Alta  | 08/03/2024                                             | Lideres de NETWORKING de parte de INFOTIC y lideres de networking de parte de ICETEX |
| Evaluar los riesgos sobre las plataformas en la nube y considerar aplicar plataformas de seguridad para los ambientes Cloud que cuenta la entidad ya que estos contienen servicios críticos para la misma. | En revisión de ICETEX                                            | Alta  | N/A                                                    | N/A                                                                                  |
| Se debe realizar la integración de los activos críticos de la compañía a la plataforma de SIEM, no se ha podido lograr por la falta de recursos de este.                                                   | En revisión de ICETEX                                            | Alta  | 21/07/2023-05/02/2024-25/07/2024-19/09/2024-03/10/2024 | Lideres de NETWORKING de parte de INFOTIC y lideres de networking de parte de ICETEX |

Tabla 5 Recomendaciones de seguridad para ICETEX

#### 4.10. Conclusiones Seguridad

- El uso de herramientas de monitoreo como el SIEM facilita la detección y respuesta rápida a incidentes de seguridad. Estas herramientas ayudan a identificar problemas desde el principio, permitiendo una reacción rápida y reduciendo el tiempo necesario para responder a situaciones de riesgo.
- Optimizar las políticas de seguridad ha permitido manejar mejor el tráfico de red hacia dispositivos críticos. Esto garantiza que solo las partes de la red y los puertos necesarios estén disponibles para su uso, reforzando así la seguridad.
- Los informes del SOC han sido clave para reducir posibles puntos de ataque. La detección temprana de actividad inusual ha permitido bloquear amenazas antes de que afecten la infraestructura de la Entidad.
- Gestionar de forma adecuada las credenciales de usuario reduce significativamente los riesgos. Una buena administración de contraseñas y permisos ayuda a asegurar que solo las personas autorizadas accedan a áreas sensibles.

- Las políticas para el uso de dispositivos personales (BYOD) mejoran la seguridad. Estas políticas permiten el uso controlado de dispositivos personales, ayudando a prevenir riesgos como la pérdida de datos y el acceso no autorizado.

## OBSERVACIONES DE ICETEX

En cuanto al cumplimiento del contrato, se destacan las siguientes observaciones:

- **Ausencia del WAF en el Datacenter alternativo:** Este asunto ha sido señalado en varias ocasiones y se han enviado requerimientos para su implementación.

Para el WAF de la data center alternativo, se han realizado consultas jurídicas sobre las condiciones técnicas presentadas en el contrato entre las entidades ICETEX – INFOTIC, una vez se tengan las conclusiones del análisis se implementará la solución a que haya lugar.

- **Tiempos de respuesta ante incidentes y solicitudes escaladas:** Se solicita a INFOTIC revisar los tiempos de respuesta para incidentes o solicitudes escaladas desde ICETEX o el SOC, ya que se han observado demoras significativas en la atención.

Se coordinará una sesión en el mes de diciembre entre el SOC, INFOTIC e ICETEX para revisar los tiempos de respuesta que se están utilizando para generar las acciones necesarias y ajustar de ser necesario, el SOC siempre ha presentado los documentos y soportes sobre la gestión que ellos realizan, se pudo presentar una demora entre la ejecución de la actividad y él envió del soporte, pero los tiempos de atención siempre han estado acorde a lo requerido en el proyecto.

- **Licenciamiento del antivirus SOPHOS:** Es necesario gestionar el licenciamiento para el complemento de SOPHOS en sistemas operativos obsoletos, ya que actualmente se encuentra vencido, lo que expone a vulnerabilidades a los equipos deprecados.

Para el para sistemas operativos obsoletos, se han realizado consultas jurídicas sobre la interpretación dada a las condiciones técnicas presentadas en el contrato entre las entidades ICETEX – INFOTIC, una vez se tengan las conclusiones del análisis se implementará la solución a que haya lugar.

Adicionalmente, se ha identificado una **indisponibilidad recurrente en el SIEM** durante los últimos fines de semana.

Este problema podría estar relacionado con un subaprovisionamiento de recursos, lo que provoca el agotamiento de la capacidad de procesamiento y afecta el funcionamiento de la consola del SIEM, lo cual debe ser documentado y registrado.

Para el SIEM se buscará realizar una sesión entre INFOTIC – WEXLER e ICETEX para analizar las recomendaciones presentadas por el grupo de seguridad de INFOTIC para aumentar el preforma de la máquina para mejorar el funcionamiento y desempeño de este componente.

## 5. SOPORTE Y MONITOREO

### 5.1. Monitoreo y revisión de ANS y línea Base

- Las herramientas de monitoreo para conectividad SolarWinds y 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 octubre 2024.pdf](#)  
[Informe Mensual ALLOT octubre 2024.pdf](#)
- Se carga en el repositorio un documento en Excel con el análisis del comportamiento de los canales para el mes de octubre [ANS Octubre 2024.xlsx](#)
- Las herramientas de monitoreo para disponibilidad de servidores es ELK (URL: <https://viewer.odin.claro.com.co/> ) y el informe de disponibilidad es el que permite la revisión de los ANS [Reporte Monitoreo ICETEX Octubre 2024-ELK.pdf](#)

#### 5.1.1. Conectividad

Durante el mes de octubre, los canales principales y Backup instalados operaron de manera normal, se realizó monitoreo del servicio de los canales mediante la herramienta SolarWinds, a través de la cual se obtuvieron los reportes de comportamiento de los canales instalados, de acuerdo con el siguiente link:

| Sede          | Categoría                          | INR        | % Mes  |
|---------------|------------------------------------|------------|--------|
| BOGOTA D.C.   | Principal / FO (Sede Aguas)        | INR0037    | 100%   |
|               | Backup / FO (Sede Aguas)           | INR0036    | 100%   |
|               | Principal / IPVPN (Sede Chapinero) | INR0022    | 100%   |
|               | Backup / IPVPN (Sede chapinero)    | INR0020    | 100%   |
|               | Principal / IPVPN (Ángel)          | INR0272    | 99.62% |
|               | Backup / IPVPN (Ángel)             | INR0273    | 94.71% |
| IBAGUE        | Principal / IPVPN                  | INR0073    | 99.98% |
|               | Backup / IPVPN                     | INR0076    | 100%   |
| LETICIA       | Principal / Satelital              | INR0000373 | 99.50% |
| NEIVA         | Principal / IPVPN                  | INR0039    | 100%   |
|               | Backup / IPVPN                     | INR0041    | 100%   |
| TUNJA         | Principal / IPVPN                  | INR0104    | 100%   |
|               | Backup / IPVPN                     | INR0106    | 100%   |
| VILLAVICENCIO | Principal / IPVPN                  | INR0085    | 99.83% |
|               | Backup / IPVPN                     | INR0084    | 99.31% |
| ARMENIA       | Principal / IPVPN                  | INR0074    | 100%   |
|               | Backup / IPVPN                     | INR0072    | 99.85% |
| MANIZALES     | Principal / IPVPN                  | INR0088    | 99.99% |

| Sede            | Categoría          | INR                       | % Mes  |
|-----------------|--------------------|---------------------------|--------|
|                 | Backup / IPVPN     | INR0087                   | 96.97% |
| MEDELLIN        | Principal / IPVPN  | INR0133                   | 100%   |
|                 | Backup / IPVPN     | INR0132                   | 100%   |
| APARTADO        | Principal / IPVPN  | INR0144                   | 98.93% |
| PEREIRA         | Principal / IPVPN  | INR0079                   | 99.98% |
|                 | Backup / IPVPN     | INR0077                   | 100%   |
| QUIBDO          | Principal / IPVPN  | INR0014                   | 99.74% |
|                 | Backup / IPVPN     |                           | 0.00%  |
| BARRANQUILLA    | Principal / IPVPN  | INR0103                   | 100%   |
|                 | Backup / IPVPN     | INR0100                   | 100%   |
| CARTAGENA       | Principal / IPVPN  | INR0109                   | 99.78% |
|                 | Backup / IPVPN     | INR0107                   | 100%   |
| MONTERIA        | Principal / IPVPN  | INR0080                   | 100%   |
|                 | Backup / IPVPN     | INR0081                   | 100%   |
| RIOHACHA        | Principal / IPVPN  | INR0164                   | 99.95% |
|                 | Backup / IPVPN     | INR0162                   | 99.64% |
| SANTA MARTA     | Principal / IPVPN  | INR0154                   | 99.79% |
|                 | Backup / IPVPN     | INR0152                   | 99.83% |
| SINCELEJO       | Principal / IPVPN  | INR0095                   | 98.44% |
|                 | Backup / IPVPN     | INR0097                   | 99.22% |
| SAN ANDRES      | Principal / IPVPN  | INR0000367/<br>INR0000369 | 99.65% |
| BARRANCABERMEJA | Principal / IPVPN  | No instalados             | 0.00%  |
| SAN GIL         | Principal / IPVPN  | No instalados             | 0.00%  |
| BUCARAMANGA     | Principal / IPVPN  | INR0062                   | 99.97% |
|                 | Backup / IPVPN     | INR0061                   | 100%   |
| CUCUTA          | Principal / IPVPN  | INR0044                   | 99.76% |
|                 | Backup / IPVPN     | INR0047                   | 99.72% |
| VALLEDUPAR      | Principal / IPVPN  | INR0091                   | 100%   |
|                 | Backup / IPVPN     | INR0090                   | 99.98% |
| YOPAL           | Principal / IPVPN  | INR0121                   | 99.24% |
|                 | Backup / IPVPN     | INR0123                   | 99.98% |
| ARAUCA          | Principal / IPVPN  | INR0110                   | 98.83% |
| CALI            | Principal / IPVPN  | INR0151                   | 100%   |
|                 | Backup / IPVPN     | INR0153                   | 100%   |
| BUENAVENTURA    | Principal / IPVPN  | INR0051                   | 100%   |
| MOCOIA          | Principal / IPVPN  | INR0135                   | 90.89% |
|                 | Backup / Satelital | INR0136                   | 91.13% |
| PASTO           | Principal / IPVPN  | INR0130                   | 99.98% |
|                 | Backup / IPVPN     | INR0131                   | 100%   |
| POPAYAN         | Principal / IPVPN  | INR0035                   | 100%   |
|                 | Backup / IPVPN     | INR0032                   | 100%   |

| Sede                                                                                                                                                                                                                        | Categoría                                                                      | INR        | % Mes    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|------------|----------|
| TUMACO                                                                                                                                                                                                                      | Principal / IPVPN                                                              | INR0147    | 91.44%   |
| WAN general (concentrador total red)                                                                                                                                                                                        | MPLS PP                                                                        | INR0266    | 99.78%   |
| WAN general (concentrador total red)                                                                                                                                                                                        | MPLS Backup                                                                    | INR0171    | 100%     |
| Conectividad dedicada a funciones de réplica para eventos de DRP.                                                                                                                                                           | DWDM                                                                           | INR0224    | 100.00 % |
| Canal entre Sitio principal e ICETEX - Dirección General - Aguas                                                                                                                                                            | Principal /IPVPN                                                               |            | 0%       |
|                                                                                                                                                                                                                             | Backup / IPVPN                                                                 |            | 0%       |
| Salida Internet contingencia - Dirección General - Aguas                                                                                                                                                                    | Ubicado en sede AGUAS interconectado a través de red MPLS                      | INR0034    | 100%     |
| Canal entre Sitio contingencia ICETEX - Dirección General - Aguas                                                                                                                                                           | Conectividad brindada a través de la red MPLS, con acceso a los dos Datacenter | INR0177    | 100%     |
| 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    | 100%     |
| Internet Dedicado Navegación centralizada Metacentro                                                                                                                                                                        | Internet Backup                                                                | INR0268    | 100%     |
| Banco de la Republica hasta Edificio Dirección General ICETEX                                                                                                                                                               | Ubicado en Datacenter Principal, interconectado a través de red MPLS           | INR0000289 | 100%     |
| DECEVAL hasta Edificio de ICETEX Dirección General.                                                                                                                                                                         | Ubicado en Datacenter Principal, interconectado a través de red MPLS           | INR0000317 | 100%     |
| DECEVAL hasta Edificio de ICETEX Dirección General.                                                                                                                                                                         | Ubicado en Datacenter Principal, interconectado a través de red MPLS (Backup)  | INR0000318 | 100%     |
| Salida de portales <a href="https://portal.icetex.gov.co/portal">https://portal.icetex.gov.co/portal</a> y <a href="http://www.icetex.gov.co">www.icetex.gov.co</a> hacia internet en centro de cómputo principal           | Internet Reverso para Portales                                                 | INR0000320 | 100.00 % |
| Salida de los portales <a href="https://portal.icetex.gov.co/portal">https://portal.icetex.gov.co/portal</a> y <a href="http://www.icetex.gov.co">www.icetex.gov.co</a> hacia internet en centro de cómputo de contingencia | Internet Reverso para Portales                                                 | INR0274    | 100.00 % |

Tabla 6 Disponibilidad de canales

A continuación, se listan las sedes y el estado de sus canales:

| Sede                    | INR canal  | BW (MB) | Fecha de Instalación | ESTADO    |
|-------------------------|------------|---------|----------------------|-----------|
| Leticia canal principal | INR0000373 | 8M      | 01/10/2024           | Entregado |
| Leticia SD WAN          | INR0000374 | 10MB    | 28/10/2024           | Entregado |
| San Andrés SD WAN       | INR0000371 | 10MB    | 21/10/2024           | Entregado |

Tabla 7 Canales instalados

| SERVICIO                        | OBSERVACIONES          |
|---------------------------------|------------------------|
| Quibdó canal de datos de Backup | En fase de instalación |

Tabla 8 Canales pendientes por instalar o en proceso de instalación

Los canales de datos principales para Barrancabermeja y San Gil, no ha sido posible avanzar teniendo en cuenta que aún el Ictex no tiene oficina en dichas ciudades.

Se están realizando las pruebas de saturación bidireccionales y se pueden consultar las (18) de los canales que se hicieron en el mes en el siguiente link: [Pruebas Nuevas de Saturación Canales](#)

| INR        | ENLACE    | SEDE        | Fecha de Saturación |
|------------|-----------|-------------|---------------------|
| INR0022    | PRINCIPAL | CHAPINERO   | 22/10/2024          |
| INR0020    | BACKUP    | CHAPINERO   | 22/10/2024          |
| INR0014    | PRINCIPAL | QUIBDO      | 18/10/2024          |
| INR0032    | BACKUP    | POPAYAN     | 28/10/2024          |
| INR0039    | PRINCIPAL | NEIVA       | 28/08/2024          |
| INR0041    | BACKUP    | NEIVA       | 28/08/2024          |
| INR0044    | PRINCIPAL | CUCUTA      | 21/10/2024          |
| INR0047    | BACKUP    | CUCUTA      | 22/10/2024          |
| INR0061    | BACKUP    | BUCARAMANGA | 21/10/2024          |
| INR0062    | PRINCIPAL | BUCARAMANGA | 21/10/2024          |
| INR0073    | PRINCIPAL | IBAGUE      | 28/08/2024          |
| INR0079    | PRINCIPAL | PEREIRA     | 20/09/2024          |
| INR0088    | PRINCIPAL | MANIZALES   | 30/08/2024          |
| INR0090    | BACKUP    | VALLEDUPAR  | 22/10/2024          |
| INR0091    | PRINCIPAL | VALLEDUPAR  | 22/10/2024          |
| INR0095    | PRINCIPAL | SINCELEJO   | 18/10/2024          |
| INR0097    | BACKUP    | SINCELEJO   | 18/10/2024          |
| INR0104    | PRINCIPAL | TUNJA       | 30/08/2024          |
| INR0121    | PRINCIPAL | YOPAL       | 24/10/2024          |
| INR0123    | BACKUP    | YOPAL       | 24/10/2024          |
| INR0130    | PRINCIPAL | PASTO       | 28/10/2024          |
| INR0131    | BACKUP    | PASTO       | 28/10/2024          |
| INR0133    | PRINCIPAL | MEDELLIN    | 24/09/2024          |
| INR0135    | PRINCIPAL | MOCOA       | 24/10/2024          |
| INR0144    | PRINCIPAL | APARTADO    | 26/09/2024          |
| INR0000367 | PRINCIPAL | SAN ANDRES  | 29/07/2024          |

| INR        | ENLACE    | SEDE    | Fecha de Saturación |
|------------|-----------|---------|---------------------|
| INR0000373 | PRINCIPAL | LETICIA | 7/10/2024           |

Tabla 9 Canales pruebas de saturación ejecutadas hasta octubre

| 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      | Principal / IPVPN   | INR0080         |
| MONTERIA      | Backup/ IPVPN       | INR0081         |
| VILLAVICENCIO | Backup/ IPVPN       | INR0084         |
| VILLAVICENCIO | Principal / IPVPN   | INR0085         |
| MANIZALES     | Backup/ IPVPN       | INR0087         |
| BARRANQUILLA  | Backup/ IPVPN       | INR0100         |
| BARRANQUILLA  | Principal / IPVPN   | INR0103         |
| TUNJA         | Backup/ IPVPN       | INR0106         |
| CARTAGENA     | Backup/ IPVPN       | INR0107         |
| CARTAGENA     | Principal / IPVPN   | INR0109         |
| ARAUCA        | Principal / IPVPN   | INR0110         |
| MEDELLIN      | Backup/ IPVPN       | INR0132         |
| MOCOA         | Backup/ IPVPN       | INR0136         |
| TUMACO        | Principal / IPVPN   | INR0147         |
| CALI          | Principal / IPVPN   | INR0151         |
| SANTA MARTA   | Backup/ IPVPN       | INR0152         |
| CALI          | Backup/ IPVPN       | INR0153         |
| SANTA MARTA   | Principal / IPVPN   | INR0154         |
| RIOHACHA      | Principal / IPVPN   | INR0162         |
| RIOHACHA      | Backup/ IPVPN       | INR0164         |
| BOGOTA(ANGEL) | Principal / IPVPN   | INR0272         |
| BOGOTA(ANGEL) | Principal / IPVPN   | INR0273         |

Tabla 10 Canales pendientes pruebas de saturación

En conclusión, se lleva un porcentaje de 47.36% de pruebas de saturación ejecutadas al 31 de octubre, se prestó el servicio en las sedes del ICETEX brindando conectividad y sin interrumpir la

operación del Instituto.

Durante el mes de octubre no se realizaron ampliaciones, en las tablas a continuación se presenta los servicios de conectividad contratados con sus respectivas capacidades ofrecidas y se compara con las cargas prestadas:

| CIUDAD                                                                                                                                                                                                                                                                                                                | Enlace - Tipo medio            | Código Servicio | BW- Mínimo Requerido (MBPS) | Ancho de Banda Ofrecido | Ancho de Banda Prestado | Diferencia (MBPS) |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|-----------------|-----------------------------|-------------------------|-------------------------|-------------------|
| NEIVA                                                                                                                                                                                                                                                                                                                 | Principal / IPVPN              | INR0039         | 18                          | 20                      | 18                      | 2                 |
| Salida de portales<br><a href="https://portal.icetex.gov.co/portal">https://portal.icetex.gov.co/portal</a><br>y <a href="https://portal.icetex.gov.co/portal">https://portal.icetex.gov.co/portal</a><br>y <a href="http://www.icetex.gov.co">www.icetex.gov.co</a> hacia internet<br>en centro de cómputo principal | Internet Reverso para Portales | INR0000320      | 800                         | 1024                    | 800                     | 224               |

Tabla 11 Canales pendientes por ampliar corte octubre

### ➤ Internet Para La Gente

Durante el mes de octubre el servicio de Internet para la gente se prestó sin interrupciones en todas las catorce sedes contratadas donde ICETEX cuenta con oficina con, estas son:

| Sede         | Categoría              | INR        | % Mes  |
|--------------|------------------------|------------|--------|
| BARRANQUILLA | INTERNET PARA LA GENTE | INR0094    | 100%   |
| BUCARAMANGA  | INTERNET PARA LA GENTE | INR0057    | 99.97% |
| CALI         | INTERNET PARA LA GENTE | INR0160    | 99.99% |
| AGUAS        | INTERNET PARA LA GENTE | INR0029    | 100%   |
| CHAPINERO    | INTERNET PARA LA GENTE | INR0015    | 100%   |
| MEDELLIN     | INTERNET PARA LA GENTE | INR0122    | 100%   |
| APARTADO     | INTERNET PARA LA GENTE | INR0140    | 98.95% |
| ARAUCA       | INTERNET PARA LA GENTE | INR0115    | 98.83% |
| LETICIA      | INTERNET PARA LA GENTE | INR0000378 | 99.51% |
| QUIBDO       | INTERNET PARA LA GENTE | INR0021    | 99.74% |
| RIOHACHA     | INTERNET PARA LA GENTE | INR0159    | 99.95% |
| SAN ANDRES   | INTERNET PARA LA GENTE | INR0000368 | 99.64% |
| YOPAL        | INTERNET PARA LA GENTE | INR0127    | 99.22% |
| MOCOA        | INTERNET PARA LA GENTE | INR0141    | 90.79% |

Tabla 12 Disponibilidad canales "Internet para la gente"

### OBSERVACIONES SOBRE MONITOREO DE CANALES

Se encontraron diferencias en los porcentajes de disponibilidad reportados y los verificados por ICETEX, en el siguiente cuadro se detalla el resultado de la verificación acordada:

| CIUDAD                                                                                                                                                                                                            | Enlace - Tipo medio            | LLAVE CON ARCHIVO SEGUIMIENTO   | CÓDIGO                   | % Descuento ANS |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|---------------------------------|--------------------------|-----------------|
| BOGOTA D.C.                                                                                                                                                                                                       | Principal / IPVPN (Angel)      | Principal / IPVPN (Angel)       | INR0272                  | 99,63%          |
| BOGOTA D.C.                                                                                                                                                                                                       | Backup / IPVPN (Angel)         | Backup / IPVPN (Angel)          | INR0273                  | 94,72%          |
| LETICIA                                                                                                                                                                                                           | Principal / Satelital          | Principal / Satelital LETICIA   | INR0000373               | 99,53%          |
| VILLAVICENCIO                                                                                                                                                                                                     | Principal / IPVPN              | Principal / IPVPN VILLAVICENCIO | INR0085                  | 99,84%          |
| VILLAVICENCIO                                                                                                                                                                                                     | Backup / IPVPN                 | Backup / IPVPN VILLAVICENCIO    | INR0084                  | 99,32%          |
| ARMENIA                                                                                                                                                                                                           | Principal / IPVPN              | Principal / IPVPN ARMENIA       | INR0072                  | 100,00%         |
| ARMENIA                                                                                                                                                                                                           | Backup / IPVPN                 | Backup / IPVPN ARMENIA          | INR0074                  | 99,32%          |
| APARTADO                                                                                                                                                                                                          | Principal / IPVPN              | Principal / IPVPN APARTADO      | INR0144                  | 98,96%          |
| PEREIRA                                                                                                                                                                                                           | Backup / IPVPN                 | Backup / IPVPN PEREIRA          | INR0079                  | 99,99%          |
| QUIBDO                                                                                                                                                                                                            | Principal / IPVPN              | Principal / IPVPN QUIBDO        | INR0014                  | 99,75%          |
| CARTAGENA                                                                                                                                                                                                         | Principal / IPVPN              | Principal / IPVPN CARTAGENA     | INR0109                  | 99,79%          |
| MONTERIA                                                                                                                                                                                                          | Backup / IPVPN                 | Backup / IPVPN MONTERIA         | INR0081                  | 99,79%          |
| RIOHACHA                                                                                                                                                                                                          | Principal / IPVPN              | Principal / IPVPN RIOHACHA      | INR0164                  | 99,96%          |
| RIOHACHA                                                                                                                                                                                                          | Backup / IPVPN                 | Backup / IPVPN RIOHACHA         | INR0162                  | 99,66%          |
| SINCELEJO                                                                                                                                                                                                         | Principal / IPVPN              | Principal / IPVPN SINCELEJO     | INR0095                  | 98,46%          |
| SINCELEJO                                                                                                                                                                                                         | Backup / IPVPN                 | Backup / IPVPN SINCELEJO        | INR0097                  | 98,27%          |
| SAN ANDRES                                                                                                                                                                                                        | Principal / IPVPN              | Principal / IPVPN SAN ANDRES    | INR0000367<br>INR0000369 | 99,66%          |
| CUCUTA                                                                                                                                                                                                            | Principal / IPVPN              | Principal / IPVPN CUCUTA        | INR0044                  | 99,77%          |
| CUCUTA                                                                                                                                                                                                            | Backup / IPVPN                 | Backup / IPVPN CUCUTA           | INR0047                  | 99,73%          |
| YOPAL                                                                                                                                                                                                             | Backup / IPVPN                 | Backup / IPVPN YOPAL            | INR0123                  | 99,99%          |
| ARAUCA                                                                                                                                                                                                            | Principal / IPVPN              | Principal / IPVPN ARAUCA        | INR0110                  | 98,84%          |
| MOCOA                                                                                                                                                                                                             | Principal / IPVPN              | Principal / IPVPN MOCOA         | INR0135                  | 91,38%          |
| MOCOA                                                                                                                                                                                                             | Backup / Satelital             | Backup / Satelital MOCOA        | INR0136                  | 91,63%          |
| PASTO                                                                                                                                                                                                             | Principal / IPVPN              | Principal / IPVPN PASTO         | INR0130                  | 99,99%          |
| TUMACO                                                                                                                                                                                                            | Principal / IPVPN              | Principal / IPVPN TUMACO        | INR0147                  | 91,48%          |
| WAN general (concentrador total red)                                                                                                                                                                              | Principal / IPVPN              | MPLS TRIARA PPAL                | <b>INR0266</b>           | 99,79%          |
| Conectividad dedicada a funciones de réplica para eventos de DRP.                                                                                                                                                 | DWDM                           | DWDM L2L (NO MONITOREADO)       | INR0224                  | 100,00%         |
| Salida de portales <a href="https://portal.icetex.gov.co/portal">https://portal.icetex.gov.co/portal</a> y <a href="http://www.icetex.gov.co">www.icetex.gov.co</a> hacia internet en centro de cómputo principal | Internet Reverso para Portales | MEGACENTER MPLS PPAL MEDELLIN   | <b>INR0177</b>           | 99,78%          |
| APARTADO                                                                                                                                                                                                          | APARTADO                       | ICETEX APARTADO                 | INR0140                  | 98,96%          |
| ARAUCA                                                                                                                                                                                                            | ARAUCA                         | ICETEX ARAUCA                   | INR0115                  | 98,84%          |
| LETICIA                                                                                                                                                                                                           | LETICIA                        | ICETEX LETICIA                  | INR0000378               | 99,54%          |

|            |            |                   |            |        |
|------------|------------|-------------------|------------|--------|
| QUIBDO     | QUIBDO     | ICETEX QUIBDO     | INR0021    | 99,76% |
| RIOHACHA   | RIOHACHA   | ICETEX RIOHACHA   | INR0159    | 99,96% |
| SAN ANDRES | SAN ANDRES | ICETEX SAN ANDRES | INR0000368 | 99,66% |
| YOPAL      | YOPAL      | ICETEX YOPAL      | INR0127    | 99,24% |
| MOCOA      | MOCOA      | ICETEX MOCOA      | INR0141    | 91.28% |

### ➤ Canales SDWAN

Durante el mes de octubre, se completó la instalación de los canales SD WAN definidos contractualmente a continuación se presenta la su disponibilidad durante el mes:

| Sede              | Categoría | INR                 | % Mes  |
|-------------------|-----------|---------------------|--------|
| SD WAN AGUAS      | SD WAN    | INR0033 / INR000334 | 100%   |
| SD WAN MOCOA      | SD WAN    | INR0139 / INR000333 | 90.85% |
| SD WAN SAN ANDRES | SD WAN    | INR0000371          | 100%   |
| SD WAN LETICIA    | SD WAN    | INR0000374          | 99.39% |

Tabla 13 Disponibilidad canales "SDWAN"

### ➤ Canal de Replicación (Triara – Megacenter)

Dentro del contrato 2022-079, se estableció un canal dedicado para la comunicación entre los Datacenter Principal (Triara), y el Datacenter alternativo (Megacenter), como acción de mejora del servicio y con el ánimo de que ICETEX cuente con lo mejor y lo último que están manejando los operadores de tecnología a nivel de velocidad de transmisión y la seguridad que debe contener la información que se replica INFOTIC y su aliado estratégico CLARO ha puesto a su disposición el canal LAN 2 LAN, hasta el momento no ha sido recibido por ICETEX sin embargo el canal ha funcionado correctamente y no se presentó afectación en la prestación del servicio.

La evidencia se encuentra en el [Informe mensual replicacion octubre 2024.pdf](#)

### ➤ Señalética (Internet para la gente)

La señalética para el uso de la red WIFI en las oficinas, se encuentran entregadas trece, continua pendiente la señalética correspondiente a la ciudad de Cali, se encuentra en proceso de elaboración se ha retrasado porque tuvo un problema de avería en el transporte y de esta forma tiene un proceso distinto antes de volver a generar su elaboración por lo tanto la fecha tentativa que esta señalética quede instalada es a 15 de enero de 2025.

A continuación, se presenta la relación de las señaléticas entregadas y su fecha de entrega y/o instalación en sitio.

| Ciudad         | Fecha Entrega | Estado             |
|----------------|---------------|--------------------|
| Barranquilla   | 14-feb-24     | Instalada en sitio |
| Bucaramanga    | 14-feb-24     | Instalada en sitio |
| Cali           | Pendiente     | En elaboración     |
| Bogotá (Aguas) | 15-mar-24     | Instalada en sitio |
| Bogotá (Chapi) | 13-mar-24     | Instalada en sitio |
| Medellín       | 06-mar-24     | Instalada en sitio |
| Apartado       | 29-feb-24     | Instalada en sitio |
| Arauca         | 20-feb-24     | Instalada en sitio |
| San Andrés     | 18-junio-24   | Instalada en sitio |
| Riohacha       | 20-feb-24     | Instalada en sitio |
| Yopal          | 21-feb-24     | Instalada en sitio |
| Mocoa          | 26-feb-24     | Instalada en sitio |
| Quibdó         | 26-feb-24     | Instalada en sitio |
| Leticia        | 28-octubre-24 | Instalada en sitio |

*Tabla 14 Estado de la instalación de la señalética de Wifi*

## ➤ Gestión Equipo Networking Aseguramiento Políticas de Seguridad de la Información

Durante octubre, en la infraestructura de ICETEX, se ha implementado DHCP Snooping como medida de seguridad para proteger la red institucional contra ataques relacionados con el protocolo DHCP. Esta funcionalidad, habilitada en los switches de la red, permite filtrar el tráfico DHCP y prevenir la suplantación de servidores DHCP.

Funcionamiento en ICETEX:

- Clasificación de puertos: Los switches de ICETEX clasifican los puertos como "confiables" (conectados a los servidores DHCP legítimos de la institución) o "no confiables" (conectados a los equipos de los usuarios).
- Filtrado de tráfico DHCP: DHCP Snooping verifica la información de los paquetes DHCP, como la dirección MAC del cliente y la dirección IP asignada. Solo los mensajes DHCP provenientes de puertos confiables (servidores DHCP autorizados) son reenviados a la red, bloqueando cualquier intento de asignación de direcciones IP desde fuentes no autorizadas.
- Protección para IPv4 e IPv6: ICETEX utiliza DHCP Snooping tanto para IPv4 como para IPv6, asegurando la integridad de la asignación de direcciones en ambos protocolos.

Beneficios para ICETEX:

- Prevención de ataques: DHCP Snooping protege la red de ICETEX contra ataques de suplantación de DHCP y agotamiento de direcciones IP, que podrían interrumpir los servicios de red y comprometer la seguridad de la información.
- Mayor control de la red: Permite un mayor control sobre la asignación de direcciones IP y la configuración de red, asegurando que solo los servidores DHCP autorizados

- proporcionen información a los dispositivos.
- Fortalecimiento de la seguridad: Contribuye a fortalecer la postura de seguridad general de la red de ICETEX, protegiendo la información y los recursos institucionales.

En resumen, la implementación de DHCP Snooping en ICETEX es una medida de seguridad fundamental para proteger la red institucional, garantizar la integridad de la asignación de direcciones IP y prevenir ataques relacionados con el protocolo DHCP.

#### ➤ Continuidad A La Integración Con El Protocolo IPv6

Las sedes Faltantes por configurar las direcciones IPv6 son: Cali, Medellín, Quibdó, Montería, Pereira, Bucaramanga, Valledupar, Santa Marta, Sincelejo, Villavicencio, Tunja, Cartagena, San Andrés, Armenia, Pasto, Ibagué, Yopal, Manizales, Neiva, Leticia.

Las cuales se les ha informado al ICETEX que componentes se requieren para completar la configuración que se debe implementar en las sedes que tiene router de voz.

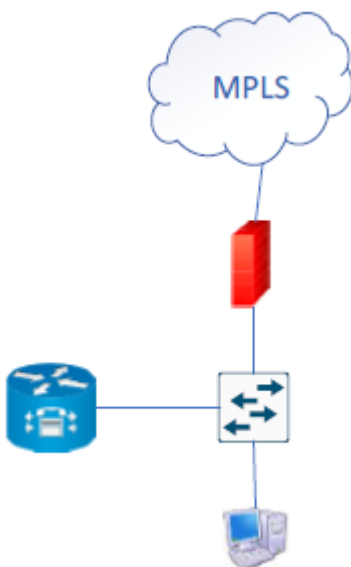


*Ilustración 21 Diagrama de red Nuevo Propuesto por Networking*

Este avance parcial a nivel de enrutamiento será trabajo en los próximos meses de ejecución del contrato.

#### 5.1.2. Conclusiones Del Servicio De Conectividad

- 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 incremento del 88% en los casos, atribuido a fallos en el servicio por parte del proveedor y a bloqueos de puertos en los equipos de la sede.

Los siguientes son los casos que se atendieron en el mes de septiembre y octubre donde se observa un crecimiento del 88%

|            |    |
|------------|----|
| Septiembre | 17 |
| Octubre    | 32 |

- Cada caso fue cerrado tras notificar a los funcionarios del servicio operativo sobre las incidencias pendientes con el proveedor, lo que representa una reducción del 10% en relación con el mes anterior.
- En cuanto a la instalación de canales sólo está pendiente de Quibdó el canal de Backup.

### 5.1.3. Recomendaciones Del Servicio De Conectividad

- **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:** Notificar a ICETEX la falta de equipos adicionales para reemplazos futuros.
- **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.
- **Seguridad de la VLAN 50 (SALA SEGURA):** Se recomienda que la VLAN 50, donde se encuentran los 6 computadores encargados de realizar los pagos, sea exclusiva para estos equipos.

Ante las observaciones formuladas por el ICETEX sobre las actividades para adelantadas para dar continuidad a la implementación del protocolo IPV6 se da respuesta en el documento [INFOTIC ICETEX - IPV6 Observaciones ICETEX.pdf](#)

### 5.2. Datacenter Principal

Para el mes de octubre de 2024 se prestó el servicio de manera normal.

Respecto al consumo de servicio en las máquinas y como se podrá observar en la imagen más adelante, el valor promedio del consumo no supera el valor máximo permitido.

Durante todo el periodo se continuó con el seguimiento permanente de todos los servicios y no se presentaron novedades en la operación.

Se continua con el monitoreo de los servidores en la herramienta ELK, cuyo reporte de disponibilidad se puede consultar en el siguiente link: [Reporte Monitoreo ICETEX Octubre 2024-ELK.pdf](#)

En la tabla 14 se muestra el reporte de uso de CPU y de memoria de los servidores de ICETEX especificando el hostname, código de servicio asignado en el operador de servicio, pico máximo, pico mínimo y promedio de uso durante el mes.

| Hostname                      | Servicio                               | Código de servicio | AVG CPU USAGE |
|-------------------------------|----------------------------------------|--------------------|---------------|
| cxvodacontg011                | Base de Datos Oracle Contingencia      | INR0278            | 7.85%         |
| cxvodaprodn011                | Base de Datos Oracle Producción Nodo 1 | INR0276            | 48.30%        |
| cxvodaprodn021                | Base de Datos Oracle Producción Nodo 2 | INR0277            | 41.77%        |
| icetexbogbalserv1             | Portal Liferay                         | INR0237            | 13.57%        |
| icetexbogelasticserver1       | Portal Liferay                         | INR0239            | 1.00%         |
| icetexbogelasticserver2       | Portal Liferay                         | INR0240            | 0.25%         |
| icetexbogelasticserver3       | Portal Liferay                         | INR0241            | 0.98%         |
| icetexbogliferaynfs           | Portal Liferay                         | INR0238            | 15.15%        |
| icetexbogliferayserver1_R     | Portal Liferay                         | INR0243            | 18.76%        |
| icetexbogliferayserver2_R     | Portal Liferay                         | INR0242            | 4.79%         |
| icetexboglxdarumasrv1         | Daruma                                 | INR0244            | 4.36%         |
| icetexboglxdarumasrv2         | Daruma                                 | INR0245            | 1.38%         |
| iceteboglxdarumatest          | Daruma test                            | INR0246            | 1.24%         |
| icetexboglxorfeo1             | Orfeo                                  | INR0233            | 0.34%         |
| icetexboglxorfeo2             | Orfeo                                  | INR0262            | 0.40%         |
| icetexboglxroad3              | Xroad                                  | INR0248            | 0.61%         |
| icetexosbognfs1               | Server NFS1                            | INR0260            | 12.46%        |
| icetexosbognfs2               | Server NFS2                            | INR0252            | 4.89%         |
| icetexbogPortalTransacServer1 | Server antiguo de Portal Transaccional | INR0236            | 0.61%         |
| icetexbogPortalTransacServer2 | Server antiguo de Portal Transaccional | INR0235            | 1.24%         |
| ictxprusisgapp                | Pruebas de Aplicación Sisgestión       | INR0234            | 19.69%        |
| ictxisgesapp                  | Aplicación Sisgestión                  | INR0229            | 4.58%         |
| ictxisgesbd                   | Base de Datos de Sisgestión            | INR0228            | 4.24%         |

| Hostname            | Servicio   | Código de servicio | AVG CPU USAGE |
|---------------------|------------|--------------------|---------------|
| ictxsrctrldoc       | ControlDoc | INR0000322         | 2.50%         |
| icetexbogwsmira     | Mira       | INR0226            | 14.60%        |
| icetexboglxroad2n   | Xroad      | INR0247            | 1.23%         |
| icetexboglxroadtest | Xroad test | INR0250            | 1.00%         |
| icetexboglxroad1    | Xroad      | INR0249            | 2.00%         |

Tabla 15 Evidencia del resumen del Monitoreo CPU- Memoria ELK

En la Tabla 16 se muestra el reporte de uso de CPU y de memoria de los servidores de Openshift de ICETEX especificando el nombre de la máquina virtual, promedio de uso de CPU y de Memoria, pico máximo de uso, pico mínimo de uso durante el mes.

| VM NAME                 | Servicio         | Código de servicio | AVG VM CPU.USED.GHZ |
|-------------------------|------------------|--------------------|---------------------|
| gate-vfpz6-master-0     | Master Openshift | INR0251            | 2,334.22            |
| gate-vfpz6-worker-lfmk4 | Worker Openshift | INR0254            | 913.88              |
| gate-vfpz6-worker-64vd2 | Worker Openshift | INR0255            | 1,849.77            |
| gate-vfpz6-worker-5smdz | Worker Openshift | INR0256            | 831.34              |
| gate-vfpz6-worker-vjtj6 | Worker Openshift | INR0257            | 1,999.39            |
| gate-vfpz6-master-2     | Master Openshift | INR0258            | 1,578.19            |
| gate-vfpz6-master-1     | Master Openshift | INR0259            | 2,419.92            |
| VM NAME                 | Servicio         | Código de servicio | AVG VM MEN.USED.GHZ |
| gate-vfpz6-master-0     | Master Openshift | INR0251            | 35.38               |
| gate-vfpz6-worker-lfmk4 | Worker Openshift | INR0254            | 7.36                |
| gate-vfpz6-worker-64vd2 | Worker Openshift | INR0255            | 14.45               |
| gate-vfpz6-worker-5smdz | Worker Openshift | INR0256            | 4.52                |
| gate-vfpz6-worker-vjtj6 | Worker Openshift | INR0257            | 13.27               |
| gate-vfpz6-master-2     | Master Openshift | INR0258            | 23.95               |
| gate-vfpz6-master-1     | Master Openshift | INR0259            | 35.65               |

Tabla 16 Evidencia del resumen del Monitoreo CPU-Memoria Servidores OpenShift - ELK

En la ilustración 34 se muestra el reporte de uso de discos de los servidores de ICETEX especificando el hostname de la máquina virtual, código de servicio asignado en el operador de servicio, file System, pico máximo de uso del filesystem, pico mínimo de uso de cada file System y porcentaje promedio de uso del file System de cada una de las máquinas virtuales en el mes.

| REPORTE USO DISCOS        |                    |                |                                        |
|---------------------------|--------------------|----------------|----------------------------------------|
| Hostname                  | Código de servicio | AVG DISK USAGE | Servicio                               |
| cxvodacontg011            | INR0278            | 1.9            | Base de Datos Oracle Contingencia      |
| cxvodaprodn021            | INR0277            | 2              | Base de Datos Oracle Producción Nodo 1 |
| icetexboglobserver1       | INR0237            | 34.24          | Portal Liferay                         |
| icetexbogelasticserver1   | INR0239            | 38.53          | Portal Liferay                         |
| icetexbogelasticserver2   | INR0240            | 27.1           | Portal Liferay                         |
| icetexbogelasticserver3   | INR0241            | 31.4           | Portal Liferay                         |
| icetexbogliferaynfs       | INR0238            | 21.04          | Portal Liferay                         |
| icetexbogliferayserver1_R | INR0243            | 36.59          | Portal Liferay                         |
| icetexbogliferayserver2_R | INR0242            | 32.93          | Portal Liferay                         |
| icetexboglxdarumasrv1     | INR0244            | 45.86          | Daruma                                 |
| icetexboglxdarumasrv2     | INR0245            | 72.34          | Daruma                                 |
| iceteboglxdarumatest      | INR0246            | 79.94          | Daruma test                            |
| icetexboglxorfeo1         | INR0233            | 49.46          | Orfeo                                  |
| icetexboglxorfeo2         | INR0262            | 75.3           | Orfeo                                  |
| icetexboglxroad3          | INR0248            | 39.7           | Xroad                                  |
| icetexboglxroad2n         | INR0247            | 30.3           | Xroad                                  |
| icetexboglxroadtest       | INR0250            | 43.62          | Xroad Test                             |
| icetexboglxroad1          | INR0249            | 35.7           | Xroad                                  |

Tabla 17 Evidencia del resumen del monitoreo ELK

### 5.2.1. Disponibilidad de Servicios – Datacenter Principal

A continuación, se presenta la imagen del promedio de disponibilidad de los servidores que se encuentran en Datacenter Triara:

En la Ilustración 35, se muestra el porcentaje de disponibilidad que tuvo cada uno de los servidores durante el mes, evidenciando que todos presentaron disponibilidad entre 99.99% a 100%:

En la Tabla 16, se muestra la tabla de homologación donde se relacione el código de servicio y el hostname del servidor, tal como se acordó con ICETEX desde el Informe de Febrero:

| # | Cod Servicio | Hostname              | Servicio               | Disponibilidad |
|---|--------------|-----------------------|------------------------|----------------|
| 1 | INR0228      | ictxisgesbd           | BD sisgestión          | 100%           |
| 2 | INR0229      | ictxisgesapp          | App sisgestión         | 100%           |
| 3 | INR0233      | icetexboglxorfeo1     | Orfeo                  | 99.99%         |
| 4 | INR0234      | ictxprusigapp         | Pruebas App sisgestión | 100%           |
| 5 | INR0237      | icetexboglobserver1-r | Portal web Liferay     | 100%           |
| 6 | INR0238      | icetexbogliferaynfs   | Portal web Liferay     | 100%           |

|    |            |                                  |                                        |        |
|----|------------|----------------------------------|----------------------------------------|--------|
| 7  | INR0239    | icetexbogelasticserver1          | Portal web Liferay                     | 100%   |
| 8  | INR0241    | icetexbogelasticserver3          | Portal web Liferay                     | 100%   |
| 9  | INR0242    | icetexbogliferayserver2          | Portal web Liferay                     | 100%   |
| 10 | INR0243    | icetexbogliferayserver1          | Portal web Liferay                     | 99.99% |
| 11 | INR0244    | icetexboglxdarumasrv1            | Daruma                                 | 100%   |
| 12 | INR0245    | icetexboglxdarumasrv2            | Daruma                                 | 100%   |
| 13 | INR0246    | iceteboglxdarumatest             | Daruma test                            | 100%   |
| 14 | INR0247    | preprodsec-<br>icetexboglxroad2n | Xroad preproducción                    | 100%   |
| 15 | INR0248    | icetexboglxroad3                 | Xroad                                  | 100%   |
| 16 | INR0249    | xroadsec-<br>icetexboglxroad1    | Xroad                                  | 99.99% |
| 17 | INR0250    | qasec-<br>icetexboglxroadtest    | Xroad                                  | 100%   |
| 18 | INR0262    | icetexboglxorfeo2                | Orfeo                                  | 100%   |
| 19 | INR0276    | cxvodaprodn011                   | BD Oracle prod nodo 1                  | 100%   |
| 20 | INR0277    | cxvodaprodn021                   | BD Oracle prod nodo 2                  | 100%   |
| 21 | INR0278    | cxvodacontn011                   | BD Oracle contingencia                 | 100%   |
| 22 | INR0240    | icetexbogelasticserver2          | Portal web Liferay                     | 100%   |
| 23 | INR0260    | icetexbogosgognfs1               | Server NFS1                            | 100%   |
| 24 | INR0252    | icetexbogosgognfs2               | Server NFS1                            | 100%   |
| 25 | INR0236    | ictxbogsrvpt1                    | Server antiguo de Portal Transaccional | 100%   |
| 26 | INR0235    | ictxbogsrvpt2                    | Server antiguo de Portal Transaccional | 100%   |
| 27 | INR0000322 | ictxcontroldoc                   | Controldoc                             | 99.99% |
| 28 | INR0226    | mira                             | Mira                                   | 99.99% |
| 29 | INR0253    | bastion                          | Bastión Openshift                      | 100%   |
| 30 | INR251     | OpenShift                        | Openshift                              | 100%   |
| 31 | INR254     | OpenShift                        | Openshift                              | 100%   |
| 32 | INR255     | OpenShift                        | Openshift                              | 100%   |
| 33 | INR256     | OpenShift                        | Openshift                              | 100%   |
| 34 | INR257     | OpenShift                        | Openshift                              | 100%   |
| 35 | INR258     | OpenShift                        | Openshift                              | 100%   |
| 36 | INR259     | OpenShift                        | Openshift                              | 100%   |

*Tabla 18 Código relacionados disponibilidad servicios en Housing – Data center Principal*

El siguiente cuadro presenta el porcentaje de disponibilidad de los dispositivos de seguridad, switches, controladoras y Enclosure de almacenamiento que se encuentran en Housing en el Datacenter principal y su disponibilidad durante el mes:

| No. | Dispositivo                                                                                         | Marca    | Modelo         | Meta ANS | Disponibilidad |
|-----|-----------------------------------------------------------------------------------------------------|----------|----------------|----------|----------------|
| 1   | FORTIWEB01                                                                                          | Fortinet | 2000E          | 99,80%   | 100%           |
| 2   | FORTIWEB02                                                                                          | Fortinet | 2000E          | 99,80%   | 100%           |
| 3   | FORTIAUTH01                                                                                         | Fortinet | 1000D          | 99,80%   | 100%           |
| 4   | FORTIAUTH02                                                                                         | Fortinet | 1000D          | 99,80%   | 100%           |
| 5   | FORTISANDBOX                                                                                        | Fortinet | 1000D          | 99,80%   | 100%           |
| 6   | Cisco 3650X                                                                                         | Cisco    | WS-C3650-48TQ  | 99,80%   | 100%           |
| 7   | Cisco 3560X SW                                                                                      | Cisco    | WS-C3650-48TQ  | 99,80%   | 100%           |
| 8   | Switch DELL Networking                                                                              | Dell     | N4032 24 ports | 99,80%   | 100%           |
| 9   | Controladora SAN Dell Compellent                                                                    | Dell     | SC8000         | 99,80%   | 100%           |
| 10  | Controladora SAN Dell Compellent                                                                    | Dell     | SC8000         | 99,80%   | 100%           |
| 11  | Enclosure Discos SAN                                                                                | Dell     | EN-SC200       | 99,80%   | 100%           |
| 12  | Enclosure Discos SAN                                                                                | Dell     | EN-SC220       | 99,80%   | 100%           |
| 13  | Enclosure Discos SAN                                                                                | Dell     | EN-SC200       | 99,80%   | 100%           |
| 14  | Enclosure Discos SAN                                                                                | Dell     | EN-SC220       | 99,80%   | 100%           |
| 15  | Enclosure Discos SAN                                                                                | Dell     | EN-SC220       | 99,80%   | 100%           |
| 16  | Enclosure Discos SAN                                                                                | Dell     | EN-SC200       | 99,80%   | 100%           |
| 17  | Enclosure Dell Blade – Principal 5 Servidor – Blade M1000, 6 IOM Slot B2 -Tarjeta Enclosure - M1000 | Dell     | M1000E         | 99,80%   | 100%           |

Tabla 19 Disponibilidad de servicios de Hosing -Data center principal

## 5.2.2. 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 [99,86%]** tal como se evidencia en la gráfica a continuación.

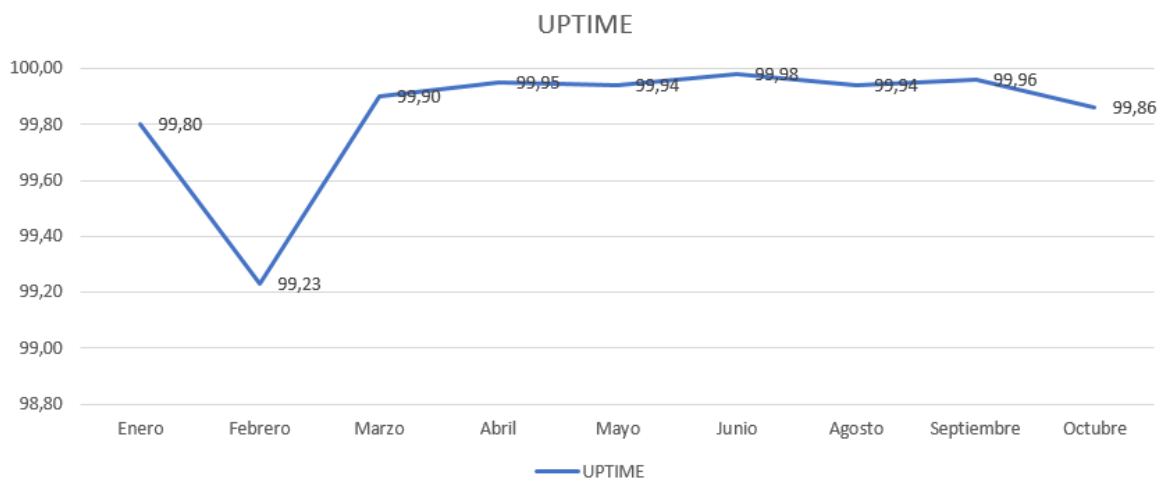


Ilustración 22 UPTIME: Portal WEB web.icetex.gov.co

Durante el mes de octubre se evidenció un comportamiento estable del portal WEB institucional y se cumplió con el porcentaje de disponibilidad de este con un porcentaje del **99,86%** adicional en

este informe mensual se incluyeron 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 379 mil usuarios, con 263 mil usuarios nuevos. El tiempo de interacción medio es de 2 minutos 27 segundos, señalando el interés de la audiencia en las diferentes páginas del portal web.icetex.gov.co

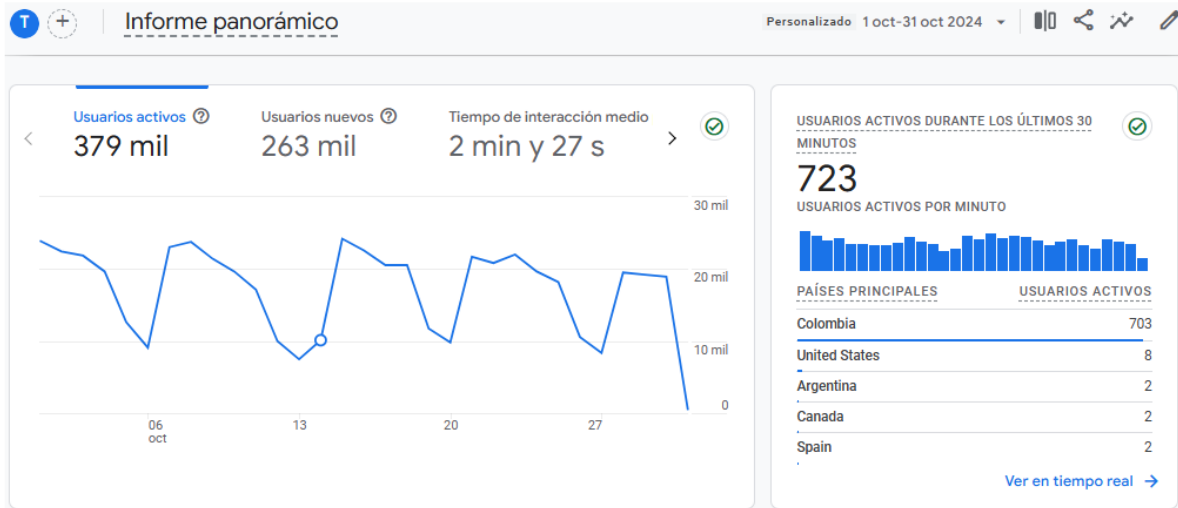


Ilustración 23 Métrica de visitantes Portal WEB web.icetex.gov.co

**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.

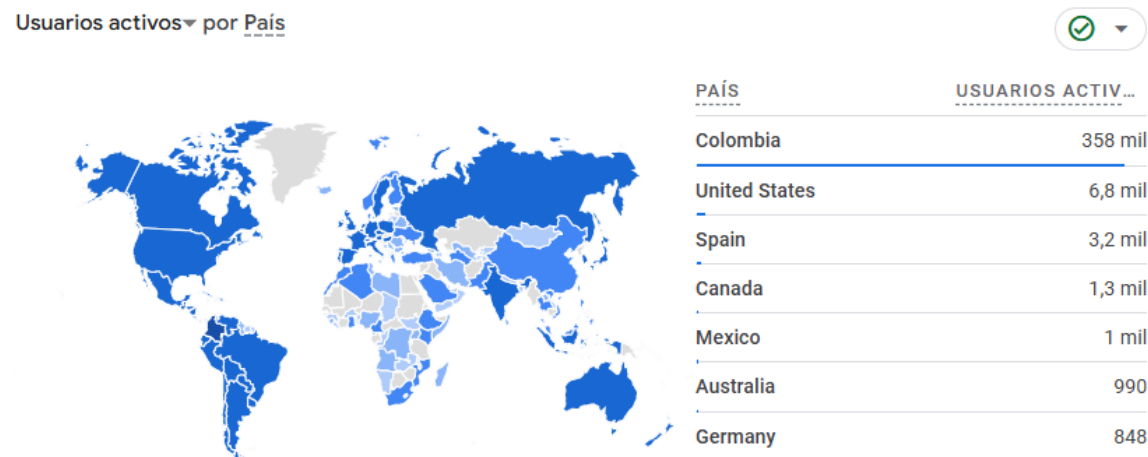


Ilustración 24 Métrica de usuario Portal WEB web.icetex.gov.co

**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.

## Recomendaciones

- 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.
- Solicitud de disco en la nube o disco externo para realizar copias de los logs del portal, archivos de configuración standalone.xml, domain.xml, output.log y server.log. En el momento no se dispone de un disco para realizar copias de seguridad.
- ICETEX debe adquirir el certificado SSL por parte del cliente ICETEX, se debió instalar un certificado provisional (Wildcard) por parte del especialista de seguridad y está activo hasta el viernes 13 de diciembre de 2024, 6:59:59 p.m.

### 5.2.3. 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 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.<br>Nodo 2 total de memoria RAM – 41.02 GB                                                                                                                                                                                                                                                                                                           | En espera de la autorización de ICETEX para disponer y configurar la memoria necesaria para que los dos nodos queden iguales. |
| DISCO DURO  | El espacio en disco utilizado por el CMS Liferay en el nodo 1 es 272 GB. El espacio disponible es de 104 GB.<br>El espacio en disco utilizado por el CMS Liferay en el nodo 2 es 152 GB. El espacio disponible es de 226 GB.<br>El nodo 1 está comenzando a quedar con poco espacio en disco duro, en el mes noviembre va a quedar con menos de 100 GB.El nodo 1 comienza a quedar con poco | Comportamiento normal.                                                                                                        |

|                      |                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | <p>espacio en disco duro, en noviembre quedará con menos de 100 GB.</p> <p>En espera de autorización por parte del cliente ICETEX para disponer de más espacio en disco duro.</p>                                                                                                  | <pre>[root@icetexbogliferayserv1 ~]# df -h Filesystem      Size  Used Avail Use% Mounted on /dev/mapper/rhel-root    45G   16G   27G   37% / devtmpfs         32G    0    32G    0% /dev tmpfs            32G    0    32G    0% /dev/shm tmpfs            32G   81M   32G    1% /run tmpfs            32G    0    32G    0% /sys/fs/cgroup /dev/mapper/app-appvol  394G  272G  104G   73% /app /dev/mapper/rhel-var     19G   6.9G   13G   37% /var /dev/mapper/rhel-home    16G  842M   16G    6% /home /dev/sda1          4.0G  236M   3.8G    6% /boot 192.168.20.42:/nfs1      503G  381G   97G   80% /backup 192.168.20.42:/nfs      503G  137G  341G   29% /u01 tmpfs             6.3G    0   6.3G    0% /run/user/1033 tmpfs             6.3G    0   6.3G    0% /run/user/0 [root@icetexbogliferayserv1 ~]#</pre> <pre>[root@icetexbogliferayserv2 ~]# df -h Filesystem      Size  Used Avail Use% Mounted on /dev/mapper/rhel-root    45G   14G   29G   33% / devtmpfs         20G    0   20G    0% /dev tmpfs            20G   4.3G   16G   22% /dev/shm tmpfs            20G   2.0G   18G   11% /run tmpfs            20G    0   20G    0% /sys/fs/cgroup /dev/mapper/app-appvol  394G  152G  226G   41% /app /dev/mapper/rhel-home    16G   4.5G   12G   28% /home /dev/sda1          4.0G  235M   3.8G    6% /boot /dev/mapper/rhel-var     19G   6.8G   13G   36% /var tmpfs             4.0G    0   4.0G    0% /run/user/0 tmpfs             4.0G    0   4.0G    0% /run/user/1030 192.168.20.42:/nfs1      503G  381G   97G   80% /backup 192.168.20.42:/nfs      503G  137G  341G   29% /u01 tmpfs             4.0G    0   4.0G    0% /run/user/1008 You have new mail in /var/spool/mail/root [root@icetexbogliferayserv2 ~]#</pre> |
| FILE SYSTEM          | <p>El espacio en disco utilizado por el CMS Liferay en el <b>nod0 1 es 424 MB.</b></p> <p>El espacio en disco utilizado por el CMS Liferay en el <b>nod0 2 es 441 MB.</b></p>                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| PARCHES DE SEGURIDAD | <p><b>Nod0 1</b> - activation-key-dxpproduction-7.3-icetex-publicportal 40.xml</p> <p>activation-key-dxpproduction-7.3-icetex-publicportal - icetexbogliferayserv1.xml</p> <p><b>Nod0 2</b> - activation-key-dxpproduction-7.3-icetex-publicportal - icetexbogliferayserv2.xml</p> | <p>Pendiente de solicitar al cliente, la renovación de soporte Liferay para poder seguir obteniendo los parches de seguridad en la versión 7.3. También para poder migrar a la versión 7.4 y obtener actualización de los parches de seguridad en la versión 7.4.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

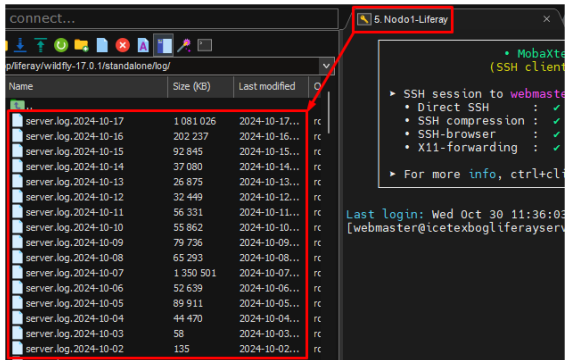
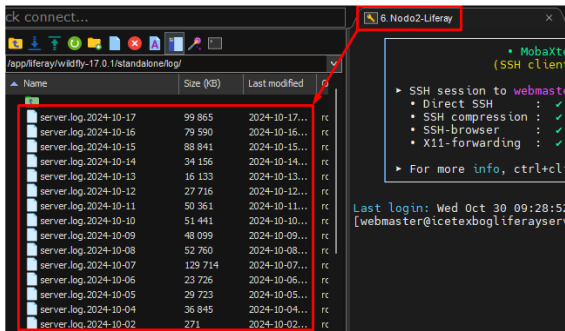
|                        |                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>VOLUMEN DE LOGS</p> | <p>Entre el registro histórico del <b>nodo 1 y el nodo 2</b>, hay una diferencia de 21 días.</p> | <p>Se registró error de base de datos del 2 al 17 de octubre en la carpeta /app/liferay/wildfly-17.0.1/standalone/log/ de nodo 1 y 2.</p> <p><b>Nodo 1</b></p>  <p><b>Nodo 2</b></p>  <p>con un mensaje de error en nodo 1 y 2:<br/>La razón fue por la recarga de caché y temporales en los nodos 1 y 2 del portal, no se estaba visualizando completo el menú principal y algunos contenidos web emitían error de permisos.<br/>Posterior al reinicio no se registraron más logs en la carpeta /app/liferay/wildfly-17.0.1/standalone/log/</p> |
| <p>Liferay</p>         | <p>Se encuentra en la versión 7.3.10 GA1</p>                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <p>Elasticsearch</p>   | <p>Se encuentra en la versión 7.9.3</p>                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

Tabla 20 Actualización – Análisis componente Liferay octubre

En la ilustración del nodo 1 se evidencia el comportamiento de la CPU, Memoria y almacenamiento los cuales no superan los límites configurados:

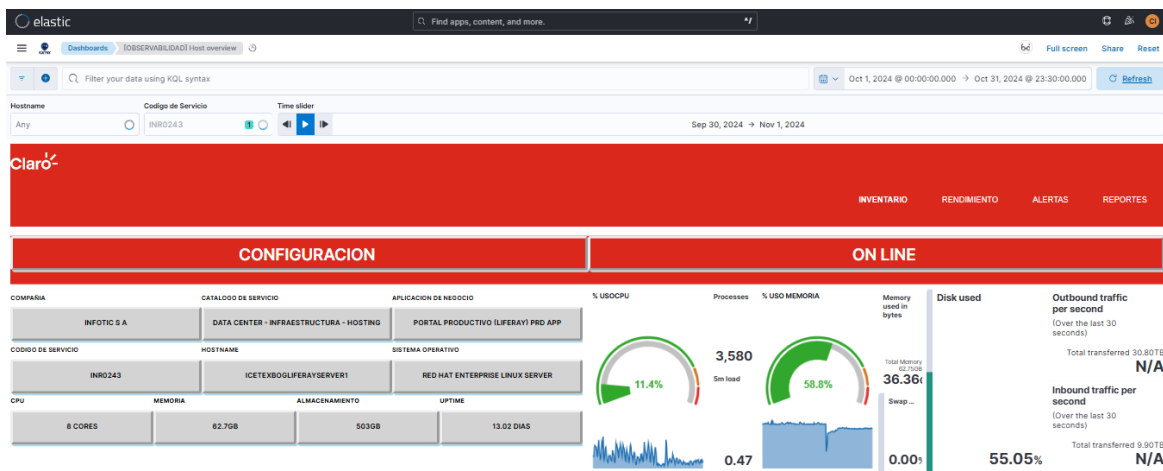


Ilustración 25 Nodo 1 Vista general

En la ilustración del nodo 2 se evidencia el comportamiento de la CPU, Memoria y almacenamiento, es de aclarar que se presenta un alto consumo de memoria debido a que tiene un performance inferior al nodo1, se solicitó a ICETEX la autorización para adquirir los componentes necesarios para tener los dos nodos idénticos.

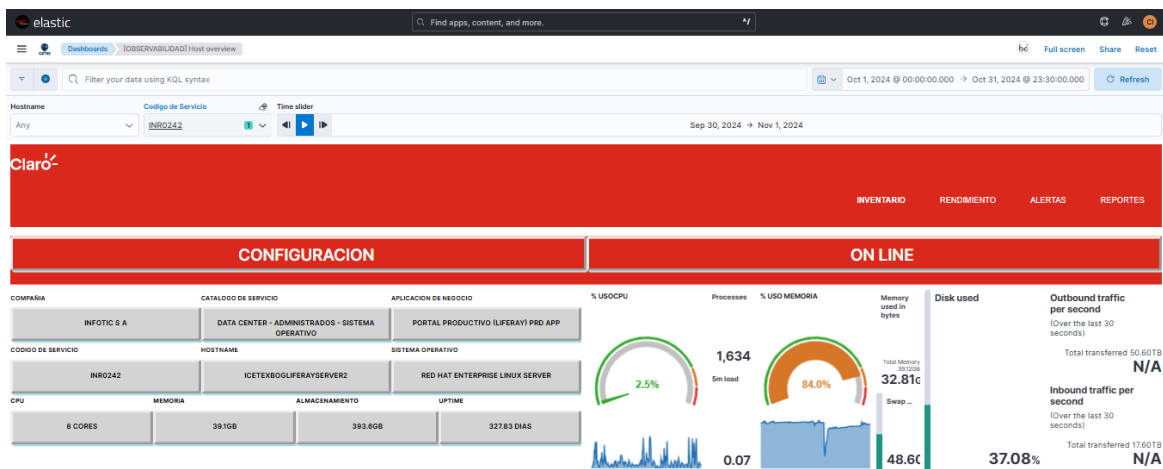


Ilustración 26 Nodo 2 vista general

## ➤ Análisis

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

|                            | Agosto | Septiembre | Octubre |
|----------------------------|--------|------------|---------|
| <b>Usuarios mes</b>        | 438000 | 387000     | 379000  |
| <b>Usuarios nuevos</b>     | 301000 | 267000     | 263000  |
| <b>Tiempo acceso (min)</b> | 145    | 126        | 147     |

Tabla 21 Distribución trimestral de accesos por usuarios

Durante el último trimestre se presentó un promedio de 401333 usuarios que accedieron al portal web, presentando para el mes de octubre una disminución en el número de usuarios que ingresaron

a la página de la entidad del 2.07% que corresponde a 8000 usuarios.

A nivel de los usuarios nuevos que accedieron a la página se tiene que en promedio durante el último trimestre se tiene 277000, presentando para el mes octubre una disminución del 1.50% que corresponde a 4000 usuarios nuevos que no ingresaron al portal de la entidad.

El tiempo que emplearon los usuarios una vez ingresaron a la página web de la durante el último trimestre correspondió a 135.5 minutos, presentando un aumento para el mes de octubre de 16.7% que corresponde a 21 minutos.

#### **5.2.4. Backup Servidores Triara**

Durante el periodo de octubre 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, [Consolidado mensual backup octubre 2024.pdf](#) donde se adjunta el reporte [Reporte Backups mes de octubre 2024.pdf](#), el cual 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, integridad 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, manipulada, 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.

Esta información debe ser trasladada a las cintas de Backup que ICETEX entregara para proceder a la custodia externa de la información.

En la actualidad se cuenta con la custodia de 294 cintas de forma externa en las instalaciones de VISE, la información que contienen corresponde a la información historia entrega en custodia a partir del 23 de agosto del 2023.

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

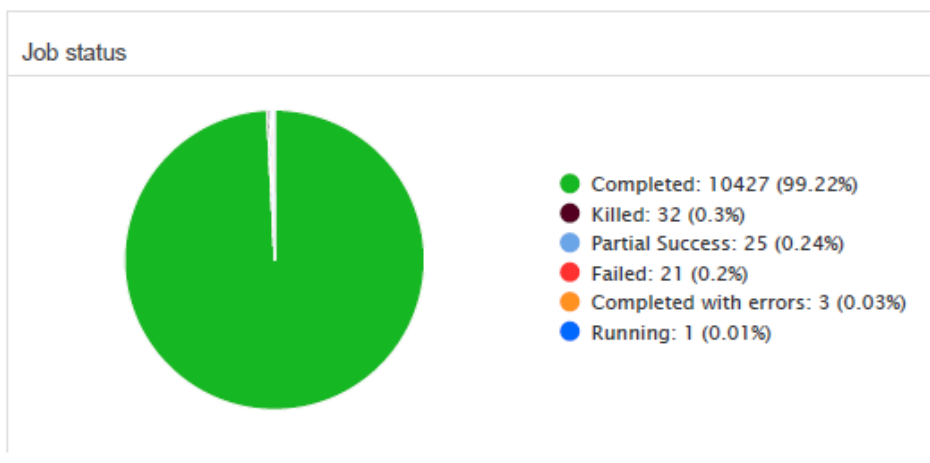


Ilustración 27 Evidencia Backup Servidores Job Status

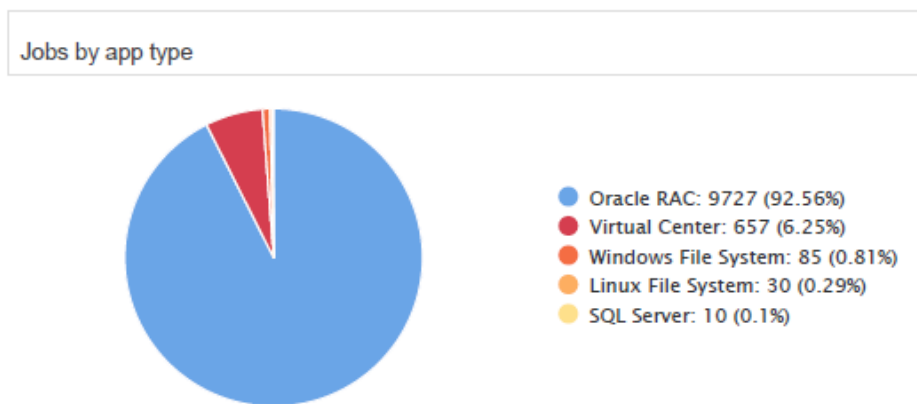


Ilustración 28 Evidencia Backup Servidores Jobs por Tipo de Aplicación

| Summary               |            |                     |            |                   |                |                |
|-----------------------|------------|---------------------|------------|-------------------|----------------|----------------|
| Job status            | Total Jobs | Size of Application | Media Size | Protected Objects | Failed Objects | Failed Folders |
| Completed             | 10427      | 466.78 TB           | 98.30 TB   | 110237583         | 8747           | 386            |
| Killed                | 32         | 0.00 BYTES          | 0.00 BYTES | 0                 | 1              | 0              |
| Partial Success       | 25         | 1.42 TB             | 21.62 GB   | 0                 | 25             | 0              |
| Failed                | 21         | 4.23 GB             | 0.00 BYTES | 0                 | 21             | 0              |
| Completed with errors | 3          | 4.44 GB             | 946.08 MB  | 13                | 0              | 0              |
| Running               | 1          | 0.00 BYTES          | 0.00 BYTES | 0                 | 0              | 0              |

1 - 6 of 6 items

Ilustración 29 Evidencia Backup servidores resumen Backups y su estado

## ➤ Análisis

El total del tamaño de la información respalda en cintas de Backups para el mes de octubre corresponde a 468.20867 TB, donde 99.22% se completó en el primer lanzamiento del robot con un total de 464.556642 TB de información.

El 92.56% está representado en el respaldo dado a la información del Oracle RAC, que equivale a 433.373945 TB.

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

|                               | Agosto | Septiembre | Octubre |
|-------------------------------|--------|------------|---------|
| <b>Completado</b>             | 98.55% | 95.67%     | 99.22%  |
| <b>Éxito Parcial</b>          | 0.56%  | 0.62%      | 0.24%   |
| <b>Fallido</b>                | 0.15%  | 2.94%      | 0.20%   |
| <b>Terminado</b>              | 0.66%  | 0.72%      | 0.30%   |
| <b>Completado con errores</b> |        | 0.05%      | 0.03%   |
| <b>En progreso</b>            | 0.08%  |            | 0.01%   |

Tabla 22 Distribución trimestral de backup ejecutados

- El promedio de los Backups completado del último trimestre en el primer lanzamiento del robot fue de 97.81%, donde el mes con mayor nivel de completado fue octubre con 99.22%; el 0.78% 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 1.25%, el mes donde más se presentó un mayor porcentaje de fallas fue septiembre con el 2.94%

|                            | Agosto | Septiembre | Octubre |
|----------------------------|--------|------------|---------|
| <b>Oracle RAC</b>          | 81.78% | 80.57%     | 92.56%  |
| <b>Virtual Center</b>      | 15.42% | 16.24%     | 6.25%   |
| <b>Windows File System</b> | 1.99%  | 2.19%      | 0.81%   |
| <b>Linux File System</b>   | 0.54%  | 0.60%      | 0.29%   |
| <b>SQL Server</b>          | 0.28%  | 0.40%      | 0.10%   |

Tabla 23 Distribución trimestral de backup por servidores

- El servicio que ocupó el mayor porcentaje en la toma de backup fue el ORACLE RAC.
- El promedio del último trimestre del respaldo de Oracle RAC fue de 84.97% donde el mes con mayor tamaño de información respaldada fue octubre con el 92.56%

**NOTA:** 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.

### 5.2.5. Recomendaciones Backups

- Definir pronto el proceso que entrega de las cintas de Backup o acordar la forma de facturación de las cintas.
- Contemplar la opción de enviar a la nube las copias de seguridad históricos que se encuentran en la custodia externa para realizar reducción de costos y dar aprovechamiento de nube

existente.

### 5.3. Datacenter Alterno

#### 5.3.1. Hosting Virtual (IaaS)

En el transcurso del mes de octubre se mantuvieron en constante replicación las máquinas virtuales, 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 octubre 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.

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

- Durante el mes de octubre del 2024: se presentó el error **Not Active (RPO Violation)** en la maquina **INR0233\_INFOTIC\_REP** durante los días 06, 07, 09, 10, 12, 13, 14, 15, 16, 19, 20, **INR0236\_INFOTIC\_REP** durante los días 02, 06, 08, y **INR0238\_INFOTIC\_REP** durante los días 02, 05, 06, 07, 12, 13, 14, 15, 16, 20, 21 los cuales fueron corregidos y continuo normalmente en los días siguientes.
- Durante el mes de octubre del 2024: se presentó el error Incremental Sync en la maquina INR0233\_INFOTIC\_REP durante los días 21 y 23 INR0236\_INFOTIC\_REP durante el día 23.
- No se presenta información del 30 de octubre, esto debido a que la herramienta no genero el reporte, pero se realizó la replicación correspondiente.

**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          | Oct 31, 2024          | 5.98 MB      | 5 minutes  |
| Grupo de protección: PG_INFOTIC_6 (2) |        |                 |                       |              |            |
| VirtualMachine                        | Status | ConfiguredDisks | LastInstanceSyncPoint | LastSyncSize | RPO        |
| INR0228_INFOTIC_REP                   | OK     | 1 of 1          | Oct 31, 2024          | 32.4 MB      | 1 hour     |
| INR0229_INFOTIC_REP                   | OK     | 1 of 1          | Oct 31, 2024          | 105.3 MB     | 1 hour     |
| Grupo de protección: PG_INFOTIC_1 (2) |        |                 |                       |              |            |
| VirtualMachine                        | Status | ConfiguredDisks | LastInstanceSyncPoint | LastSyncSize | RPO        |
| INR0233_INFOTIC_REP                   | OK     | 6 of 6          | Oct 31, 2024          | 5.83 MB      | 30 minutes |
| INR0262_INFOTIC_REP                   | OK     | 1 of 1          | Oct 31, 2024          | 6.22 MB      | 1 hour     |
| Grupo de protección: PG_INFOTIC_5 (1) |        |                 |                       |              |            |
| VirtualMachine                        | Status | ConfiguredDisks | LastInstanceSyncPoint | LastSyncSize | RPO        |

Ilustración 30 Reportes de replicación SRM a Sitio Alterno, octubre 31 2024

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         | ictxisgesbd       | Sisgestion                  | INR0228_INFOTIC_REP        |
| 3 | INR0206         | ictxisgesapp      | Sisgestion                  | INR0229_INFOTIC_REP        |
| 4 | INR0220         | icetexboglxorfeo1 | ORFEO                       | INR0233_INFOTIC_REP        |
| 5 | INR0219         | icetexboglxorfeo2 | ORFEO                       | INR0262_INFOTIC_REP        |
| 6 | INR0208         | ICTXBOGSRVPT1     | Portal Transaccional        | INR0236_INFOTIC_REP        |
| 7 | INR0209         | icetexbogbalserv1 | Portal productivo (liferay) | INR0237_INFOTIC_REP        |

|    |         |                         |                             |                     |
|----|---------|-------------------------|-----------------------------|---------------------|
| 8  | INR0210 | icetexbogliferaynfs     | Portal productivo (liferay) | INR0238_INFOTIC_REP |
| 9  | INR0217 | icetexbogelasticserver1 | Portal productivo (liferay) | INR0239_INFOTIC_REP |
| 10 | INR0218 | icetexbogliferayserver1 | Portal productivo (liferay) | INR0243_INFOTIC_REP |
| 11 | INR0215 | icetexboglxdarumasrv1   | DARUMA                      | INR0244_INFOTIC_REP |
| 12 | INR0213 | icetexboglxdarumasrv2   | DARUMA                      | INR0245_INFOTIC_REP |
| 13 | INR0214 | icetexboglxroad1        | XROAD                       | INR0249_INFOTIC_REP |

Tabla 24 Servicios replicados – DataCenter Megacenter

## ➤ Análisis

| Agosto   | Septiembre | Octubre  |
|----------|------------|----------|
| 11541.59 | 15966.78   | 31304.28 |

Tabla 25 Distribución trimestral de replicación

Durante el último trimestre la replicación que se realiza entre el data center principal TRIARA y el data center alterno MEGA CENTER tuvo un promedio de transferencia de data de 19606.217 MB y se presenta un crecimiento del 48.99 % entre septiembre y octubre, que equivale a 15337.5 MB.

### 5.3.2. Dataguard BBDD Megacenter

Durante el mes de octubre 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 Octubre.pdf](#)

```

oracle@cxvodacontg011:~$ ps -feal|grep pmon
oracle 4881 1 0 Oct04 ? 00:06:53 ora_pmon_LIFERAYD
grid 6046 1 0 Jul27 ? 00:15:03 asm_pmon_+ASM
oracle 7047 1 0 Jul27 ? 00:34:38 ora_pmon_ICETEXD
oracle 7343 1 0 Jul27 ? 00:36:30 ora_pmon_APOTEOSD
oracle 7736 1 0 Jul27 ? 00:34:40 ora_pmon_APOTNEWD
oracle 8246 1 0 Jul27 ? 00:19:06 ora_pmon_VIGIADTG
oracle 8572 1 0 Jul27 ? 00:19:05 ora_pmon_LANDICTD
oracle 9297 1 0 Jul27 ? 00:34:55 ora_pmon_APLICATD
oracle 11890 1 0 Oct04 ? 00:12:44 ora_pmon_ICTXCYPD
oracle 17870 15850 0 18:33 pts/0 00:00:00 grep --color=auto pmon
oracle@cxvodacontg011:~$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.4.0 Production on Wed Nov 6 18:33:19 2024
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 77517 77517 31/10/2024 18:15 31/10/2024 18:15
2 57997 57997 31/10/2024 18:25 31/10/2024 18:25

SQL> sta uapPLY

Thread Last Sequence Received Last Sequence Applied Difference
-----
1 77517 77517 0
2 57997 57997 0

```

Ilustración 31 Evidencia Dataguard replicado o Megacenter BD

Se generó la consulta de los archivos recibidos y aplicados de la base de datos de ICTXCYCD a 31/10/2024 18:25 con diferencia cero (0) archivos sin aplicar, lo cual es evidencia que la replicación se encuentra sincronizada

### 5.3.3. Disponibilidad de Servicios de Housing – Datacenter Alterno

A continuación, se presentan las máquinas alojadas en el Datacenter alternativo en Medellín, las cuales estuvieron disponibles todo el mes de octubre al 100%:

| No. | Dispositivo                | Marca | Modelo         | Meta ANS | Disponibilidad |
|-----|----------------------------|-------|----------------|----------|----------------|
| 1   | Switch CISCO               | CISCO | 3560           | 99,80%   | 100%           |
| 2   | Switch DELL Networking     | Dell  | N4032 24 ports | 99,80%   | 100%           |
| 3   | Servidor rack Vmware       | Dell  | PowerEdge R630 | 99,80%   | 100%           |
| 4   | Servidor rack Vmware       | Dell  | PowerEdge R630 | 99,80%   | 100%           |
| 5   | Storage Controladora - SAN | Dell  | CT-SC8000      | 99,80%   | 100%           |
| 6   | Storage Controladora - SAN | Dell  | CT-SC8000      | 99,80%   | 100%           |

*Tabla 26 Disponibilidad de los servidores Housing – Datacenter Alterno*

### 5.3.4. Servicios de DRP

Se realizaron reuniones de seguimiento entre INFOTIC y CLARO y otras con ICETEX, INFOTIC y CLARO donde se generó el objetivo y el alcance para el desarrollo del DRP, el cual se programó para el 03 de noviembre del 2024. Para la ejecución de la actividad se confirmó que de acuerdo con las lecciones aprendidas del DRP de junio del 2024, el personal debería estar en sitio para mejorar los tiempos de respuesta y tener un mayor control sobre las evidencias entregadas como soporte de la actividad.

INFOTIC se encargará de realizar la gestión necesaria para tener al personal de CLARO en las instalaciones físicas donde se vaya a desarrollar el DRP en la fecha programada.

ICETEX solicitó la entrega de dos minutogramas, un minutograma con el detalle técnico a ejecutar y otro condensando las actividades que sería un minutograma ejecutivo.

El 04 de octubre del 2024, se realizó la prueba TEST en horario hábil, a nivel de documentación se puede consultar el minutograma en el siguiente link:

[C1115614\\_Minutograma\\_ICETEX\\_DRP\\_TEST\\_Ope.xlsx](#)

Este documento está compuesto por las siguientes páginas:

- Explicación del minutograma: En esta hoja se tiene una corta explicación de cómo se debe diligenciar el minutograma

- Ejecución y plan retorno: En esta hoja esta del detalle de cada una de las actividades a realizar en el DRP.
- Direccionamiento: en esta hoja están relacionada la información de los equipos de cómputo que hacen parte de la ejecución del DRP
- Diagramas: en esta hoja están dos graficas con la ingeniería de detalle que contempla la ejecución del DRP

Es de tener en cuenta que para poder ejecutar la prueba TEST de acuerdo con el documento presentado, se ha tenido la revisión y aprobación por parte de la Mesa de Cambios de ICETEX de acuerdo con las delimitaciones y alcances, así como las restricciones observadas en el procedimiento.

Dentro de la prueba del segundo semestre del 2024 se incluyó la verificación del RTO y RPO, una vez se ejecute el DRP se presentara en el informe el resultado de estas dos variables, es de aclarar que en el mes de julio de 2024 se envió un correo donde el operador tecnológico CLARO informaba que técnicamente el menor tiempo que se puede configurar para estas mediciones es de 05 minutos, adicionalmente se revisó con el operador tecnológico CLARO cuales eran los umbrales que se tenían establecidos para estas variables y lograr el cumplimiento del contrato.

Las pruebas previas al DRP han permitido validar como debe funcionar las plataformas y aplicaciones en este escenario, al igual que permite calcular y optimizar los tiempos necesarios en cada cambio que se debe realizar para que en un escenario de DRP se pueda realizar de la manera más eficiente y correcta y de mitigar los errores que se puedan cometer al realizar esta actividad.

#### **Observaciones de ICETEX sobre el DRP:**

ICETEX ha reiterado en varias reuniones y comunicados que los planes e infraestructura proporcionados por INFOTIC para el DRP deben cumplir con lo siguiente:

Según el documento “OFERTA COMERCIAL N° PV-2022-310-1” (28 de diciembre de 2022), firmado por Adolfo Antonio Tejada Díaz, ICETEX, en el numeral 4.8, se especifica que la solución debe contemplar mecanismos de contingencia entre los canales principal y backup, incluyendo una conectividad dedicada a funciones de réplica para eventos de DRP, como se describe en el Anexo 2.1.

En el numeral 5.8 del mismo documento, también se detalla que INFOTIC debe diseñar e implementar una solución que permita mantener una réplica síncrona del portal web de ICETEX en el Data Center alternativo, para asegurar la disponibilidad en caso de fallas graves. Esto incluye la creación de un Plan de Recuperación de Desastres (DRP) que garantice la restauración del servicio en menos de 2 horas desde el Data Center alternativo, con procedimientos, guías y responsables claramente definidos. Además, se deben realizar pruebas semestrales para validar el funcionamiento de los portales en el Data Center alternativo.

INFOTIC también debe cumplir con los requisitos mínimos para el WAF, que deben incluir un producto líder en el cuadrante de Gartner. Sin embargo, INFOTIC no ha entregado la configuración de las conexiones del WAF en el Data Center alternativo y ha presentado una arquitectura que no resuelve adecuadamente los requisitos de DRP. Contar con un único servicio de WAF en el Data Center principal gestionando también el alternativo crea un punto único de falla, lo que va en contra de

las buenas prácticas de seguridad informática y gestión de centros de datos. Esta configuración pone en riesgo tanto la disponibilidad de los portales como la seguridad del sistema, y cualquier falla en el WAF podría comprometer gravemente el servicio, lo que sería responsabilidad de INFOTIC.

**RTA:** Para el WAF de la data center alterno, se han realizado consultas jurídicas sobre la interpretación dada a las condiciones técnicas presentadas en el contrato entre las entidades ICETEX – INFOTIC, una vez se tengan las conclusiones del análisis se implementará la solución a que haya lugar.

## 6. ALMACENAMIENTO

Teniendo en cuenta que ICETEX ha solicitado realizar la replicación de más máquinas virtuales, se realizó con el operador Claro el análisis del consumo tanto de CPU, memoria y disco duro de las máquinas virtuales replicadas frente a las acordadas según el Anexo #3 - Parte 6 Alterno IAS, encontrando que las 13 Máquinas virtuales que se están replicando tenemos:

- 9 máquinas que superaron la capacidad de Almacenamiento.
- 10 máquinas que superaron la capacidad de memoria, sin embargo, la diferencia más significativa corresponde a dos servidores de Portal web INR0239-icetexbogelasticserver1 y INR0243-icetexbogliferayserver1 que están 32 GB de memoria por encima del definido en la línea base.

En conclusión, 9 Máquinas Virtuales de las 13 replicadas en el Datacenter alterno están utilizando un almacenamiento mayor al provisionado inicialmente para cada uno de los servidores según el Anexo 3 y que las 13 máquinas virtuales replicadas están ocupando el **94.5%** de almacenamiento total definido en el Anexo #3 - Parte 6 Alterno IAS.

| Almacenamiento<br>Anexo #3 - Parte 6<br>Alterno IAS TB | Almacenamiento<br>Utilizado<br>actualmente TB | Diferencia (TB) | VM replicada                 |
|--------------------------------------------------------|-----------------------------------------------|-----------------|------------------------------|
| 11.0                                                   | 11.3                                          | 0.26            | icetexboglخورفو1.localdomain |
| 0.3                                                    | 0.3                                           | 0.01            | icetexboglخورفو2.localdomain |
| 0.3                                                    | 0.5                                           | 0.20            | ICTXSIGESBD.icetex.local     |
| 0.1                                                    | 0.2                                           | 0.08            | xroadsec                     |
| 0.3                                                    | 0.9                                           | 0.59            | icetexbogbalsever1-r         |
| 0.9                                                    | 0.9                                           | 0.03            | icetexbogliferayserver1      |
| 0.9                                                    | 0.9                                           | 0.03            | icetexbogelasticserver1      |
| 0.2                                                    | 0.2                                           | 0.02            | ICTXBOGSRVPT1.icetex. local  |
| 0.2                                                    | 1.6                                           | 1.37            | MIRA                         |
| 14.3                                                   | 16.9                                          | 2.6             |                              |

Tabla 27 Recursos – Datacenter Alterno Anexo #3 EC-Alternio IAS

En cuanto al excedente de memoria se definió con ICETEX realizar el ajuste de la memoria en los dos servidores de Portal y devolverlos a los valores definidos en la línea base, sin embargo, para no desmejorar el rendimiento de los mismo se realizará una revisión y se presentará a ICETEX cual sería

el consumo real de estos servidores y así definir en cuanto se reduce la memoria y por consiguiente acordar con el ICETEX como se ajustará en términos de facturación dicho consumo adicional.

Se puede ver el soporte de este análisis en el siguiente link: [MEGACENTER-REPLICACION\\_2908.xlsx](#)

## 7. APLICACIONES

Para garantizar una operación eficiente, la ejecución exitosa del contrato y la entrega oportuna de los servicios activos a la Entidad, INFOTIC cuenta con un equipo de profesionales altamente capacitados que se encuentran disponibles en el trabajo. Estos recursos humanos han sido asignados según los roles y responsabilidades establecidos en el contrato. Su presencia en sitio asegura una comunicación fluida, una supervisión constante y la capacidad de abordar cualquier desafío o requerimiento de manera rápida y efectiva. Nuestro compromiso es proporcionar un servicio de calidad, cumpliendo con los estándares acordados y satisfaciendo las necesidades de la Entidad.

### 7.1. Actividades De Operación

Para el presente periodo evaluado, que corresponde al mes de octubre, se atendieron las solicitudes e incidentes que fueron generadas por parte de ICETEX, los profesionales especializados que se encuentran asignados a la ejecución del proyecto desarrollaron y atendieron estas solicitudes con todo el profesionalismo y la calidad que se requiere.

La disponibilidad y trazabilidad para las tareas asignadas a cada uno de los especialistas se encuentra controlada por el gerente de proyecto asignado donde se evidencia a través del [CONSOLIDADO INFORME MENSUAL ESPECIALISTAS OCTUBRE.pdf](#) el cumplimiento a satisfacción de las funciones que deben gestionar cada uno de estos contratados para el desarrollo del presente contrato.

### 7.2. Profesionales Especializados.

El detalle de las actividades realizadas por cada uno de los ingenieros especialistas se puede consultar en el [CONSOLIDADO INFORME MENSUAL ESPECIALISTAS OCTUBRE.pdf](#)

#### ➤ 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.
- **Especialista Web Máster**

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

- **Funciones básicas:** Se presenta un informe anexo con la información sobre las actividades que realizan en el desarrollo de sus funciones.
- **Informes:** 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.
- **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 backup
- **Especialista de 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 de saturación, informe de disponibilidad, consumo de canales, ANS de canales,

➤ **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.

➤ **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 e informe de vulnerabilidades, reporte de IPS.

## 8. Servicios de Videoconferencia

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

| ÍTEM                    | SERVICIO                                              | CIUDAD             | DIRECCIÓN                                                   | CANTIDAD |
|-------------------------|-------------------------------------------------------|--------------------|-------------------------------------------------------------|----------|
| 1                       | Sala de vídeo conferencia a sala virtual (Tamaño 65") | Bogotá - Aguas     | Carrera 3 No. 18-32                                         | 3        |
| 2                       | Sala de vídeo conferencia a sala virtual (Tamaño 65") | Bogotá - Ángel     | Cl. 19 #6-68 piso 17                                        | 1        |
| 3                       | Sala de video conferencia a sala virtual (Tamaño 55") | Bogotá - Aguas     | Carrera 3 No. 18-32                                         | 1        |
| <b>SEDES REGIONALES</b> |                                                       |                    |                                                             |          |
| 4                       | Sala de vídeo conferencia a sala virtual (Tamaño 55") | Bogotá - Chapinero | Calle 57 No. 8-69 Local 46 - 48 y 50                        | 1        |
| 5                       | Sala de video conferencia a sala virtual (Tamaño 55") | Barranquilla       | Calle 70 #53-74 piso 3                                      | 1        |
| 6                       | Sala de video conferencia a sala virtual (Tamaño 55") | Bucaramanga        | CR 29 # 45 - 45, Ofi. 703                                   | 1        |
| 7                       | Sala de video conferencia a sala virtual (Tamaño 55") | Cali               | Calle 5 No. 66B - 67, Centro Cultural El Capitolio – Piso 3 | 1        |
| 8                       | Sala de video conferencia a sala virtual (Tamaño 55") | Medellín           | Calle 52 No. 47-42 Piso 10 Ofi. 1002                        | 1        |

*Tabla 28 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

En la verificación realizada para el pasado mes de octubre del 2024 sobre la solución de videoconferencia en las sedes regionales, se encontró que la solución completa presentó estado activo con disponibilidad del 100% para el periodo del presente informe, además es importante resaltar que se cuenta con todos los requerimientos realizados en las especificaciones técnicas del contrato.

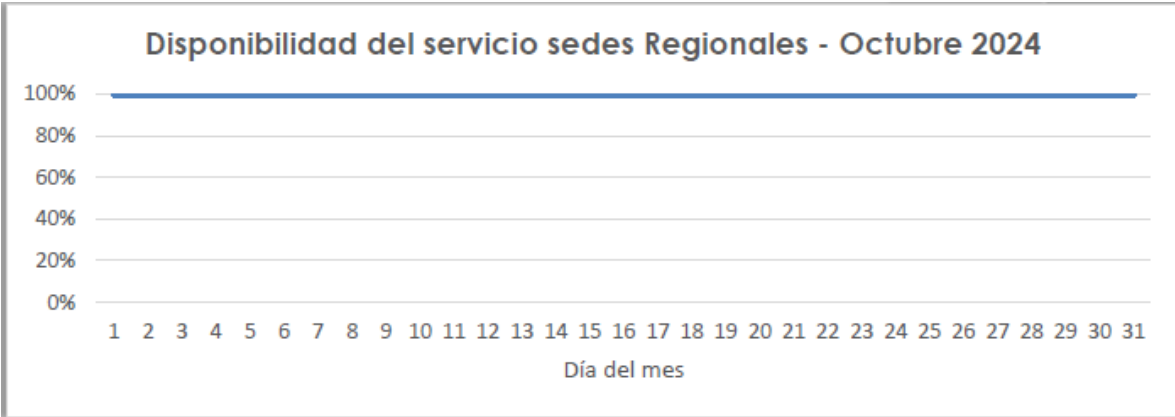


Ilustración 32 Disponibilidad de servicio videoconferencia sedes regionales – octubre 2024

➤ **Disponibilidad del servicio – sedes Bogotá (aguas - ángel)**

En la verificación realizada en el mes de octubre 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% para el periodo del presente informe, en estado activo, además es importante resaltar que se cuenta con todos los requerimientos realizados en las especificaciones técnicas del contrato.

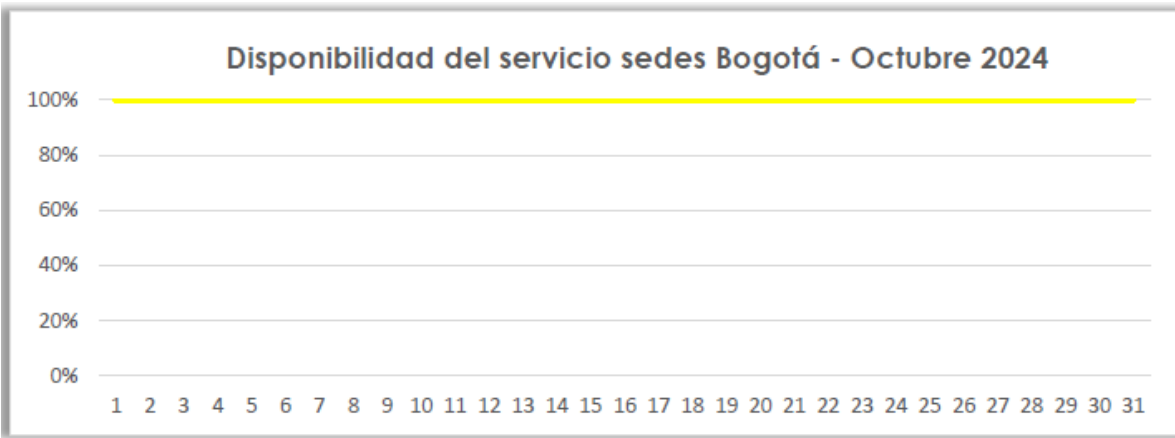


Ilustración 33 Disponibilidad de servicio videoconferencia sedes Bogotá – octubre 2024

➤ **Gestión De Incidencias Y Requerimientos – Sedes Regionales**

Para el periodo comprendido entre el 1 y el 31 de octubre, en las sedes Regionales (Cali,

Barranquilla, Bucaramanga y Medellín) no se generaron solicitudes especiales que requirieran atención y gestión de soporte técnico, tampoco se reportaron incidencias a nivel del servicio para estas sedes durante el periodo, sin embargo, se contó con la disponibilidad para recibir cualquier solicitud de soporte (Incidencia/requerimiento) o apoyo concerniente a la solución de videoconferencia desplegada.

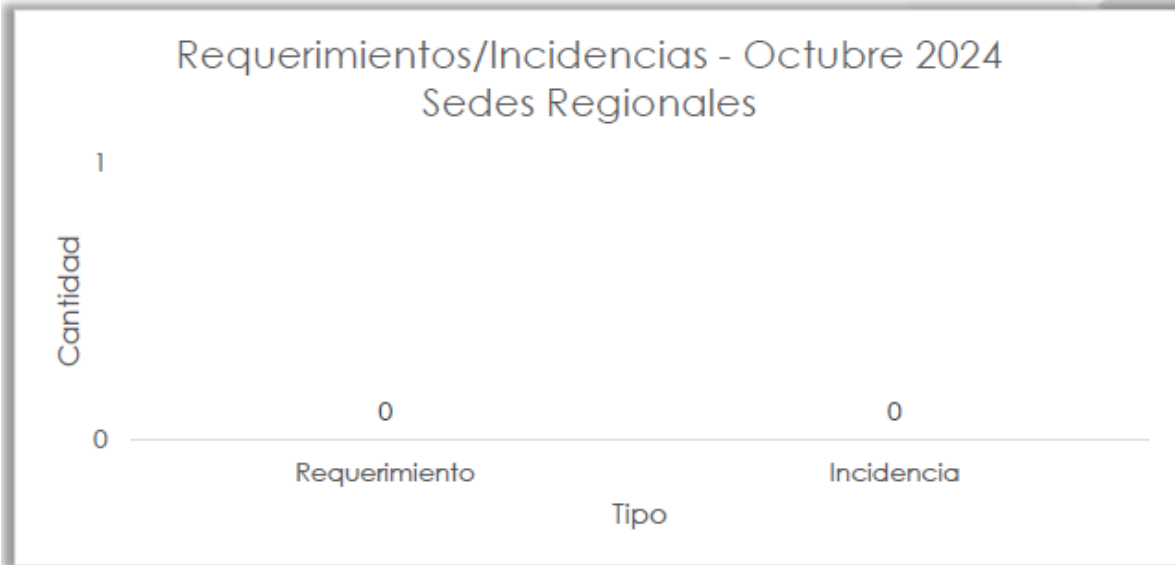


Ilustración 34 Incidencias / Requerimientos sedes regionales – octubre 2024



Ilustración 35 Prueba de funcionamiento sede chapinero – octubre 2024

➤ **Gestión de incidencias y requerimientos – Bogotá (Aguas - Angel)**

Para el periodo comprendido entre el 1 y el 31 de octubre, 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 en los periodos anteriores, se contó con la disponibilidad 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, con la persona que realiza el apoyo técnico frecuente para revisión de los equipos, se realizaron pruebas de funcionamiento, limpieza superficial de los módulos, revisiones y los ajustes requeridos para descartar incidencias en los equipos y poder garantizar continuidad del servicio. En las revisiones realizadas 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-286017-8-20950.



*Ilustración 36 Módulo funcional sala 8 piso presidencia – visita octubre 2024*

En la visita de revisión mensual de los equipos se realizan pruebas de funcionamiento en los módulos de cada piso de la sede Aguas para validar el funcionamiento normal del servicio.



*Ilustración 37 Evidencia módulo funcional sede aguas 65 – piso 4 – visita octubre 2024*

En la sala de reuniones del piso No. 2 se validó y confirmó funcionamiento, teniendo en cuenta que en el momento de la visita se encontraba en desarrollo reunión en esta sala con uso del módulo sin recibir reporte de incidencias.

Además, se verifica funcionamiento del módulo ubicado en la sede Ángel como se visualiza en la Ilustración 49.



*Ilustración 38 Verificación módulo sede ángel – octubre 2024*

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

- Visita en sitio para realizar pruebas de funcionamiento y limpieza externa módulos Aguas, Ángel y Chapinero.
- Coordinación de personal técnico, disponibilidad de fechas e inicio de permisos de ingreso para el mes de noviembre en sedes Regionales (Barranquilla, Bucaramanga, Medellín y Cali) con el fin de realizar revisión y mantenimientos preventivos de módulos.

Las evidencias se pueden encontrar en el siguiente [Informe actividades Módulos videoconferencia ICETEX octubre 2024.pdf](#)

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

|                      | Agosto | Septiembre | Octubre |
|----------------------|--------|------------|---------|
| <b>Requerimiento</b> | 0      | 2          | 0       |
| <b>Incidentes</b>    | 0      | 0          | 0       |

*Tabla 29 Distribución trimestral de requerimientos y/o incidentes*

Durante el mes de octubre no se presentaron solicitudes de requerimientos ni incidentes en la prestación del servicio de videoconferencia.

## Conclusiones Videoconferencia

- Durante el periodo comprendido entre 1 y 31 de octubre se prestó un servicio de calidad conforme a los requerimientos contractuales y se ha brindado el soporte de acuerdo con las necesidades realizadas por el cliente. El servicio presentó continuidad durante el transcurso del mes del presente informe.
- En la infraestructura a nivel del servicio se presenta un nivel de disponibilidad acorde a lo establecido en el contrato.
- Se cuenta con disponibilidad continua para atender todas solicitudes de soporte técnico para estas plataformas y apoyo que sea requerido.

## 9. BASES DE DATOS

La operación de las bases de ICETEX se mantuvo en optimo 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.

### ➤ Bases De Datos Oracle Y Tamaño

A continuación, se relacionan las BD Oracle con su tamaño actual:

| Base de Datos      | Tamaño (GB)     |
|--------------------|-----------------|
| ICTXCYC            | 4.192           |
| ICETEX             | 196             |
| APLICATI           | 243             |
| APOTEOSY           | 453             |
| VIGIAPRD           | 101             |
| LIFERAY LIFERAYPDB | 7               |
| LANDICTX           | 528             |
| SGDEA              | 89              |
| <b>TOTAL</b>       | <b>5.809 GB</b> |

*Tabla 30 Tamaño BD Oracle*

## Conclusiones Bases de Datos

- La disponibilidad de las bases de datos fue del 100% para el mes de octubre de 2024.
- Los casos atendidos en el mes de octubre de 2024 aumentaron en un 2% respecto al mes de anterior.
- Se resolvieron aproximadamente 480 casos asignados a los administradores de base de dato en octubre de 2024 en los tiempos estipulados por prioridad.
- 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 la cantidad de tutelas que debieron ser atendidas por el cliente, aunque su aumento no fue significativo.

## 10. CONTROL DE CAMBIOS

Durante el mes de octubre 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                                                                                                                                                                                                                                      |
|------------|---------------------------------------------------------------------------------------------|-------------------|--------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1065       | Instalar el agente del antivirus SYMANTEC en el equipo de ControlDoc.                       | 24-sep-24         | 28-sep-24          | Se reprograma | Se requiere una sesión con el proveedor de CONTROLDOC y INFOTIC (CLARO) para determinar cómo se debe instalar el agente de antivirus para no afectar el funcionamiento de la herramienta.                                                          |
| 1066       | Realizar la prueba TEST para el servicio del portal web                                     | 02-oct-24         | 04-oct-24          | Exitoso       |                                                                                                                                                                                                                                                    |
| 1075       | Reinicio del servicio de WildFly en los nodos 1 y 2 del portal web ICETEX.                  | 25-oct-24         | 26-oct-24          | No ejecutado  | Verificar el código que está funcionando para determinar el error o lo que hace falta para los dos que no funcionan                                                                                                                                |
| 1077       | Ejecución del DRP                                                                           | 30-oct-24         | 10-nov-24          | No ejecutado  | Se reprograma para noviembre                                                                                                                                                                                                                       |
| 1078       | Realizar la actualización del cluster de OpenShift pasar de la versión 4.10.28 a la 4.12.67 | 30-oct-24         | 08-nov-24          | No ejecutado  | De acuerdo con los hallazgos encontrados en las actividades prerequisites se define reprogramar la actividad hasta se subsanen dichos hallazgos y de esta manera no arriesgar la estabilidad de esta aplicación, que es crítica para la operación. |

|      |                                               |           |           |         |                                                                             |
|------|-----------------------------------------------|-----------|-----------|---------|-----------------------------------------------------------------------------|
| 1069 | Implementación del protocolo IP DHCP Shopping | 17-oct-24 | 26-oct-24 | exitoso | se configura en comando IP DHCP Shopping en todas las vlan de la sede Aguas |
|------|-----------------------------------------------|-----------|-----------|---------|-----------------------------------------------------------------------------|

Tabla 31 Controles de cambio octubre

## 11. CALCULO DE CONCILIACION DE LOS SERVICIOS DEL MES DE OCTUBRE

A la fecha la conciliación del mes de octubre con ICETEX se encuentra en proceso, el detalle de conciliación del mes anterior se puede ver en el siguiente enlace [Conciliación Octubre consolidado.xlsx](#)

### ➤ Ejecución Presupuestal

| EJECUCIÓN PRESUPUESTAL                                                                                                                                    |      |            |    |      |                   |                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------|------------|----|------|-------------------|----------------------|
| CONCEPTO                                                                                                                                                  |      |            |    |      |                   | VALOR                |
| VALOR INICIAL DEL CONTRATO                                                                                                                                |      |            |    |      |                   | \$ 31,398,996,857.96 |
| 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                                                                                                                                              |      |            |    |      |                   | \$ 11.372.314.066    |
| 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 |                      |
| 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 |                      |
| VALOR CAUSADO QUE NO SE HA PAGADO (valor a pagar factura) *                                                                                               |      |            |    |      |                   | \$0                  |
| VALOR TOTAL EJECUTADO (valor pagado + valor causado no pagado)                                                                                            |      |            |    |      |                   | \$ 11.372.314.066    |
| SALDO DEL CONTRATO (valor total del contrato – valor total ejecutado)                                                                                     |      |            |    |      |                   | \$ 20.026.682.792    |
| PORCENTAJE DE EJECUCIÓN                                                                                                                                   |      |            |    |      |                   | 36,22%               |
| * El valor causado no pagado corresponde a cuentas de cobro o facturas recibidos y aprobados a satisfacción por el supervisor o interventor para su pago* |      |            |    |      |                   |                      |

Tabla 32 Ejecución Presupuestal

## 12. PLAN DE TRABAJO

Se adjunta el plan de trabajo

| Actividades                                                                                                                                                                                                                                                                                                                              | Responsables     | Fecha Inicio | Fecha fin | Verificación |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|--------------|-----------|--------------|
| Durante el mes de octubre del 2024 a nivel de conectividad y redes se tiene el 98% de los canales instalados y en servicio teniendo pendiente el canal Backup de Quibdó y el de Leticia.                                                                                                                                                 | INFOTIC - ICETEX | 01-nov-24    | 31-ene-25 |              |
| La instalación de señaléticas, también se ha alcanzado un avance del 98%, quedando pendiente la sede de Cali, que actualmente se encuentra en proceso de fabricación.                                                                                                                                                                    | INFOTIC - ICETEX | 01-nov-24    | 31-ene-25 |              |
| Dentro del proceso de monitoreo de marca se presentó un crecimiento del 69.07% de los casos analizados por SOC siendo el parámetro más relevante el de la “piratería online” con un total de 1836 casos de los cuales se descartaron 1835 y se resolvió 01                                                                               | INFOTIC - ICETEX | 01-nov-24    | 31-ene-25 |              |
| Los dispositivos monitoreados por el SIEM solo el 20% de los dispositivos tienen métricas de seguridad, un 58% solo traen datos de disponibilidad y rendimiento, un 21% no trae ningún tipo de log o se encuentran inoperantes y un 1% posee errores de parcheo.                                                                         | INFOTIC - ICETEX | 01-nov-24    | 31-ene-25 |              |
| Dentro de los eventos del mes se detectaron alertas de posibles ataques que no fueron detectados por el FortiWeb, después de validaciones sobre el origen del tráfico se proceden a bloquear las direcciones IP de origen en el firewall perimetral que se sitúa antes del WAF para prevenir ataques sobre los sitios web de la entidad. | INFOTIC - ICETEX | 01-nov-24    | 31-ene-25 |              |

|                                                                                                                                                                                                                                                                                                                                                                   |                  |           |           |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-----------|-----------|--|
| Dentro de las actividades se detectaron eventos de DDoS el cual fue descartado ya que no se tiene información relevante que indicara que se tratara de algún ataque de este tipo ya que el puerto utilizado fue el TCP 443 (HTTPS) el cual es un puerto que se usa para los sitios web de la entidad y el origen no fue catalogado como malicioso.                | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| Se ajusta el minutograma final para la prueba test del DRP, la cual se definió su ejecución para el viernes 04 de octubre y la cual servirá para medir tiempos, evaluar tareas paralelas y probar los escenarios para la prueba definitiva de la cual aún no se tiene confirmada la fecha por parte de ICETEX tentativamente seria para el mes de noviembre 2024. | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| Para el WAF del Datacenter alternativo, se han realizado consultas jurídicas sobre la interpretación dada a las condiciones técnicas presentadas en el contrato entre las entidades ICETEX – INFOTIC, los avances se documentarán en los informes mensuales y una vez se tengan las conclusiones del análisis se implementará la solución a que haya lugar.       | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| Definir con ICETEX el procedimiento para la instalación y configuración de los Endpoints que quedan en bodega                                                                                                                                                                                                                                                     | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| En conjunto con el ICETEX se verificará el estado de los dispositivos monitoreados y realizar depuración de equipos que no se encuentren en operación.                                                                                                                                                                                                            | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| Depuración de las políticas en los firewalls, analizar el tráfico que pasa sobre las políticas con origen, destino, puertos en ALL y en base a este análisis alineando estas políticas para permitir sólo el tráfico necesario y cerrar brechas de seguridad asociadas a esta configuración.                                                                      | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |

|                                                                                                                                                                                                                                                                                                                                                                                                                                        |                  |           |           |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-----------|-----------|--|
| Segmentación las políticas de acuerdo con la necesidad y no otorgar acceso de toda una red o todos los servicios.                                                                                                                                                                                                                                                                                                                      | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| En conjunto con el ICETEX se trabajará en el perfilamiento de la navegación de acuerdo con lo entregado por ICETEX.                                                                                                                                                                                                                                                                                                                    | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| En conjunto con el ICETEX se validar la autenticación de doble factor para todas las plataformas misionales del ICETEX.                                                                                                                                                                                                                                                                                                                | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| En conjunto con el ICETEX revisar la autenticación a través del LDAP, para la gestión de las plataformas de seguridad.                                                                                                                                                                                                                                                                                                                 | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| En conjunto con el ICETEX Validar la posibilidad de la integración de la Consola Sophos con SIEM.                                                                                                                                                                                                                                                                                                                                      | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| Se realizará una sesión para revisar el tema del de licenciamiento vencido del <b>Fortiweb 2000E</b>                                                                                                                                                                                                                                                                                                                                   | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| Se realizará una mesa de trabajo para revisar el tema de las mejoras en la infraestructura en cuanto a controles de seguridad para alinearse con las prácticas recomendadas y estándares actuales. La presencia de protocolos y configuraciones inseguras evidencia la necesidad de una revisión y actualización constantes para minimizar la exposición a amenazas y garantizar la protección efectiva de los activos de información. | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| Se realizará una mesa de trabajo para revisar la recomendación sobre la necesidad de actualización de los protocolos de cifrado y deshabilitar versiones obsoletas: Se recomienda deshabilitar TLS 1.0 y TLS 1.1 en toda la infraestructura y asegurar que los servicios utilicen al menos TLS 1.2 o versiones superiores, las cuales proporcionan un nivel de seguridad adecuado frente a ataques modernos.                           | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |

|                                                                                                                                                                                                                                                                                                                                                                                                                                     |                  |           |           |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-----------|-----------|--|
| Realizar una sesión técnica para revisar con ICETEX la Seguridad de la VLAN 50 (SALA SEGURA) en la cual se recomienda que la VLAN 50, donde se encuentran los 6 computadores encargados de realizar los pagos, sea exclusiva para estos equipos.                                                                                                                                                                                    | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| 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. | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| Solicitud de disco en la nube o disco externo para realizar copias de los logs del portal, archivos de configuración standalone.xml, domain.xml, output.log y server.log. En el momento no se dispone de un disco para realizar copias de seguridad.                                                                                                                                                                                | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| ICETEX debe adquirir el certificado SSL por parte del cliente ICETEX, se debió instalar un certificado provisional (Wildcard) por parte del especialista de seguridad y está activo hasta el viernes 13 de diciembre de 2024, 6:59:59 p.m.                                                                                                                                                                                          | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| Realizar Reuniones de mesa técnica para definir las lecciones aprendidas, los planes de trabajo correspondientes y las fechas opcionales de la próxima prueba de DRP.                                                                                                                                                                                                                                                               | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| Realizar sesiones técnicas sobre las lecciones aprendidas, los planes de trabajo correspondientes y las fechas opcionales de la próxima prueba de DRP.                                                                                                                                                                                                                                                                              | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |
| Realizar mesa de trabajo para revisar las recomendaciones generales de seguridad indicadas en el numeral 4.8.                                                                                                                                                                                                                                                                                                                       | INFOTIC - ICETEX | 01-nov-24 | 31-ene-25 |  |

|                                                                                                                                                             |                  |              |           |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|--------------|-----------|--|
| 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. | INFOTIC - ICETEX | 15- Nov - 24 | 31-ene-25 |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|--------------|-----------|--|

*Tabla 33 Ejecución Presupuestal*

### 13. RECOMENDACIONES

Las siguientes son las recomendaciones para el mes de octubre que desde cada servicio de especialistas asignados al proyecto ICETEX realizan para mejorar los diferentes ámbitos:

#### Networking

Reemplazo de Equipos Dañados: Notificar a ICETEX la falta de equipos adicionales para reemplazos futuros.

Renovación y Certificación de Cableado: Renovar o sustituir el cableado antiguo y certificar el nuevo.

Mantenimiento de Infraestructura: Realizar un mantenimiento integral de equipos y cableado, y renovar los dispositivos de red.

Seguridad de la VLAN 50 (SALA SEGURA): Se recomienda que la VLAN 50, donde se encuentran los 6 computadores encargados de realizar los pagos, sea exclusiva para estos equipos. Se incluyó la información sobre la "SALA SEGURA" en las recomendaciones, haciendo énfasis en la necesidad de aislar estos equipos por su importancia en las operaciones de pago. También se añadió la implementación de DHCP snooping como una medida de seguridad adicional.

Actualmente, al compartir la VLAN con otros usuarios de la red y utilizar una máscara /24, se incrementa el riesgo de seguridad.

Se sugiere cambiar la máscara a /28 para reducir el número de dispositivos en la VLAN y aislar estos equipos críticos.

DHCP Snooping: Se implementó DHCP snooping en la red para prevenir ataques de suplantación de DHCP y mejorar la seguridad de la red.

#### Bases De Datos

Se recomienda aumentar los siguientes componentes para atender las solicitudes que realiza el ICETEX, con 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.

Se está gestionando retirar los permisos de sudo a los usuarios INFOTIC, gawuser y dcscsf con esto usuarios podrían realizar actividades administrativas que no van con su role.

## **Backups**

Para el correcto funcionamiento del almacenamiento de Backup, se recomienda que el ICETEX realice la entrega programada de las cintas de backup para proceder realizar el descargue de los archivos de los equipos proveedor de tecnología, pasarlos a cinta y posterior traslado a custodia externa.

Contemplar la opción de enviar a la nube las copias de seguridad históricos que se encuentran en la custodia externa para realizar reducción de costos y dar aprovechamiento de nube existente.

## **Portal WEB**

Realizar la 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 las nuevas instalaciones 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.

Realizar copias de los logs del portal, archivos de configuración standalone.xml, domain.xml, output.log y server.log, en disco externo.

## **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 hacer un registro de estos.

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

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

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

## **Integración Nube**

Contar con accesos a Azure, como también, a la sección de análisis de costos para futuras validaciones y/o recomendaciones.

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

Continuar con la remediación de hallazgos, en el correo se respondieron algunas dudas, pero falta la

implementación de los tags solicitados para tener un mayor seguimiento sobre los recursos y su monitoreo.

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

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

## Seguridad

Es fundamental llevar a cabo la validación de los usuarios que acceden a la VPN, asegurando que tanto los conectados como los que utilizan la VPN punto a punto naveguen a través del ICETEX, lo que implica una colaboración efectiva entre INFOTIC e ICETEX.

Se debe trabajar en el perfilamiento de la navegación de acuerdo con lo entregado por ICETEX, para este tema se debe validar en conjunto con ICETEX la realización de un piloto para la navegación y las políticas propuestas, ejemplo comunicaciones, tesorería, contabilidad, dirección de tecnología, etc.

Se llevará a cabo una colaboración entre las partes involucradas y el ICETEX para implementar las recomendaciones, asegurando que cada uno contribuya desde su ámbito de acción. Esta sinergia es fundamental para el éxito de las iniciativas propuestas:

- Segmentar las políticas de acuerdo con la necesidad y no otorgar acceso de toda una red o todos los servicios.
- Validar la autenticación de doble factor para todas las plataformas misionales del ICETEX.
- Realizar autenticación a través del LDAPS, para la gestión de las plataformas de seguridad.
- Validar la posibilidad de la integración de la consola Sophos con SIEM.
- 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.
- Realizar la contención automática de equipos que se identifiquen en la red como maliciosos.
- Realizar el aumento de recursos a la plataforma de FortiSIEM (CPU, Memoria y disco) y hacer un cambio de arquitectura con el objetivo de mejorar.
- Garantizar la segmentación de la red que permita claramente definir qué servicios deben ser alcanzados por cada usuario.
- Se recomienda una tecnología que permita realizar análisis de tráfico de la red (NTA- Network

#### Traffic Análisis)

- 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.
- Integrar los equipos que hacen parte del proceso de pagos 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.

## 14. CONCLUSIONES GENERALES

La replicación entre los centros de datos TRIARA y MEGACENTER para las 13 máquinas virtuales en octubre fue exitosa, con una sincronización efectiva, un delta de sincronización de 31304.28 MB y sin interrupciones en la operación del ICETEX. Esto resalta la fiabilidad y disponibilidad continua de los sistemas involucrados.

En el último mes, se observó una notable disminución del 94.2% en los casos analizados por SOC, destacando la "piratería online" como el aspecto más relevante, con solo tres casos reportados. De estos, uno fue descartado y dos se encuentran en tratamiento.

La lentitud y los errores en la generación de reportes del SIEM se deben a que la capacidad del servidor que soporta los módulos de FortiSIEM ha alcanzado su límite de almacenamiento en disco. Es crucial abordar esta limitación para mejorar el rendimiento y la eficiencia en la elaboración de informes mensuales.

Se ha logrado configurar el 45.4% de las sedes de ICETEX para la navegación en IPv6, mientras que para el resto se evaluará la opción de configuración adecuada debido a la presencia de routers de voz que no permiten usar la misma configuración implementada en las demás sedes.

Las bases de datos del ICETEX operan de manera eficiente, con una réplica activa entre sus centros de datos y la resolución de 480 casos escalados, lo que refleja un crecimiento del 2.18% comparado con el mes anterior.

Se llevó a cabo la depuración de los sistemas de archivos en los servidores de Portal web debido a un consumo superior al 80%. Esta acción busca optimizar el rendimiento y la capacidad de los servidores afectados.

Se presentaron al comité de cambios cuatro solicitudes de ventanas de mantenimiento, las cuales aprobadas, ejecutadas exitosamente y documentadas de acuerdo con los procedimientos del ICETEX.

La tasa de éxito de los backups realizados en octubre fue notablemente alta, alcanzando el 99.22%, lo que indica un desempeño eficiente, aunque un pequeño porcentaje un 00.78% requirió acciones correctivas para asegurar la integridad total de la información respaldada.

En el presente mes, el ICETEX no ha requerido la restauración de copias de seguridad. Esto indica una posible estabilidad en sus sistemas y procesos operativos.

La instalación de la señalética para wifi en todas las sedes ha alcanzado un avance del 98%. Esto indica que se está cerca de completar con todas las sedes instaladas hasta el momento.

En octubre, la única tarea pendiente en conectividad es la instalación del canal de Backup en Quibdó.