

|                          |                                                                                                                                                    |                                                                                     |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>Código:</b> F319      | <b>INFORME MENSUAL DE GESTIÓN<br/>SUPERVISIÓN, VERIFICACIÓN Y RECIBO A<br/>SATISFACCIÓN DEL CUMPLIMIENTO DE LAS<br/>OBLIGACIONES CONTRACTUALES</b> |  |
| <b>Versión:</b> 8        |                                                                                                                                                    |                                                                                     |
| <b>Fecha:</b> 05/03/2025 |                                                                                                                                                    |                                                                                     |
| <b>Página</b> 1 de 4     |                                                                                                                                                    |                                                                                     |

1. PERIODO DEL INFORME

|                                      |            |            |
|--------------------------------------|------------|------------|
| PERÍODO A QUE CORRESPONDE EL INFORME | 01-09-2025 | 30-09-2025 |
|--------------------------------------|------------|------------|

2. DATOS DEL SUPERVISOR

|                       |                                             |
|-----------------------|---------------------------------------------|
| NOMBRE DEL SUPERVISOR | JAIME ALEJANDRO BECERRA ACOSTA              |
| DEPENDENCIA           | VICEPRESIDENCIA DE OPERACIONES Y TECNOLOGÍA |
| CARGO                 | Vicepresidente de Operaciones y Tecnología  |

3. DATOS DEL CONTRATO

|                                                                                                                                                                    |                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| OBJETO: Servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el ICETEX |                                                              |
| NÚMERO DE CONTRATO                                                                                                                                                 | 2022-0792                                                    |
| FECHA DE SUSCRIPCIÓN                                                                                                                                               | 30/12/2022                                                   |
| FECHA DE PERFECCIONAMIENTO Y EJECUCIÓN                                                                                                                             | 30/12/2022                                                   |
| CONTRATISTA                                                                                                                                                        | INFOTIC S.A.S                                                |
| CÉDULA DE CIUDADANÍA O NIT                                                                                                                                         | 900.068.796-1                                                |
| VALOR (incluido IVA)                                                                                                                                               | \$31.398.996.857,96                                          |
| PLAZO                                                                                                                                                              | 39 meses (3 meses de implementación y 36 meses de operación) |
| FECHA DE INICIO                                                                                                                                                    | 19/01/2023                                                   |
| FECHA DE FINALIZACIÓN                                                                                                                                              | 19/04/2026                                                   |
| ADICIÓN (SI APLICA)                                                                                                                                                | \$2.761.480.370                                              |
| VALOR TOTAL CON ADICIÓN                                                                                                                                            | \$34.160.477.227,96                                          |
| PRÓRROGA (SI APLICA)                                                                                                                                               | N/A                                                          |
| SUSPENSIÓN (SI APLICA)                                                                                                                                             | N/A                                                          |

4. SEGUIMIENTO GESTIÓN CONTRACTUAL = NO APLICA

El siguiente cuadro debe ser diligenciado solo para personas naturales:

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

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

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

5. PRODUCTOS ENTREGABLES = NO APLICA

| 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)

|                          |                                                                                                                                                    |                                                                                     |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>Código: F319</b>      | <b>INFORME MENSUAL DE GESTIÓN<br/>SUPERVISIÓN, VERIFICACIÓN Y RECIBO A<br/>SATISFACCIÓN DEL CUMPLIMIENTO DE LAS<br/>OBLIGACIONES CONTRACTUALES</b> |  |
| <b>Versión: 8</b>        |                                                                                                                                                    |                                                                                     |
| <b>Fecha: 05/03/2025</b> |                                                                                                                                                    |                                                                                     |
| <b>Página 2 de 4</b>     |                                                                                                                                                    |                                                                                     |

Presenta informe de los servicios prestados en periodo de AGOSTO de 2025, se concertó la aplicación de ANS sobre los servicios prestados de acuerdo con el anexo técnico del contrato en el periodo de agosto 2025.

Se presentan descuentos por aplicación de ANS para los servicios prestados así:

- Aplicación de ANS para julio de 2025 con radicado 20255000825682-E Id: 6588889, descuento aplicado \$ 55.229.223
- Aplicación de ANS para agosto de 2025 con radicado 20255000954603-E Id: 6771079, descuento aplicado \$56.440.020

Los documentos del proyecto se encuentran en el SharePoint [Ejecucion INFOTIC](#)

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

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

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

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| SI <u>  X  </u>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | NO <u>      </u> |
| <p>SE ANEXA AL PRESENTE INFORME CERTIFICACIÓN PARA PAGO EN EL MES DE SEPTIEMBRE DE 2025 DE LA EJECUCIÓN CORRESPONDIENTE DE LOS SERVICIOS PRESTADOS EN:</p> <ul style="list-style-type: none"> <li>- Servicios de JULIO 2025 por valor de SETECIENTOS SETENTA Y OCHO MILLONES QUINIENTOS ONCE MIL OCHOCIENTOS NOVENTA Y SIETE PESOS M/CTE, de acuerdo con memorando 20255000835834-E Id: 6609345, se aplica descuento. \$55.229.223 por aplicación de ANS.</li> <li>- Servicios de AGOSTO 2025 por valor de SETECIENTOS SETENTA Y SIETE MILLONES TRECIENTOS UN MIL CIENTO PESOS M/CTE, de acuerdo con memorando 20255000954603-E Id: 6771079, se aplica descuento. \$56.440.020 por aplicación de ANS.</li> </ul> |                  |

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

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

| Mes y año | Número de planilla | Salud | Pensión | ARL |
|-----------|--------------------|-------|---------|-----|
|           |                    | \$    | \$      | \$  |
|           |                    |       |         |     |

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

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

|                 |                  |                         |
|-----------------|------------------|-------------------------|
| SI <u>  X  </u> | NO <u>      </u> | NO APLICA <u>      </u> |
|-----------------|------------------|-------------------------|

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

|                          |                                                                                                                                                    |                                                                                     |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>Código: F319</b>      | <b>INFORME MENSUAL DE GESTIÓN<br/>SUPERVISIÓN, VERIFICACIÓN Y RECIBO A<br/>SATISFACCIÓN DEL CUMPLIMIENTO DE LAS<br/>OBLIGACIONES CONTRACTUALES</b> |  |
| <b>Versión: 8</b>        |                                                                                                                                                    |                                                                                     |
| <b>Fecha: 05/03/2025</b> |                                                                                                                                                    |                                                                                     |
| <b>Página 3 de 4</b>     |                                                                                                                                                    |                                                                                     |

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

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

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

|          |          |                     |
|----------|----------|---------------------|
| SI _____ | NO _____ | NO APLICA ____X____ |
|----------|----------|---------------------|

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

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

|          |          |                     |
|----------|----------|---------------------|
| SI _____ | NO _____ | NO APLICA ____X____ |
|----------|----------|---------------------|

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

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

|                                                 |
|-------------------------------------------------|
| <b>OBSERVACIONES: (SI A ELLO HUBIERE LUGAR)</b> |
|                                                 |

**11. EJECUCIÓN PRESUPUESTAL**

|                                     | <b>VIGENCIA (AÑO)</b> |
|-------------------------------------|-----------------------|
| <b>VALOR DEL CONTRATO</b>           | \$31.398.996.857,96   |
| <b>VALOR ADICIÓN (Si aplica)</b>    | \$2.761.480.370       |
| <b>VALOR TOTAL DEL CONTRATO</b>     | \$34.160.477.227,96   |
| <b>VALOR A PAGAR (Si aplica)</b>    | \$ 1.555.812.997      |
| <b>VALOR EJECUTADO</b>              | \$ 20.670.629.986     |
| <b>VALOR PENDIENTE POR EJECUTAR</b> | \$ 13.489.847.242,96  |

**12. ANÁLISIS MATERIALIZACIÓN Y MITIGACIÓN DEL RIESGO:**

¿DURANTE LA EJECUCIÓN SE MATERIALIZÓ ALGÚN RIESGO?

SI ☐ NO ☒

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

**13. RECIBO A SATISFACCIÓN:**

El **VICEPRESIDENTE DE OPERACIONES Y TECNOLOGÍA** con designación de supervisión de acuerdo con memorando 20252200006793-I Id: 6206675 de fecha 24 de junio de 2025, **JAIME ALEJANDRO BECERRA ACOSTA**, recibe a satisfacción la entrega de los servicios objeto de facturación aquí

|                          |                                                                                                                                                    |                                                                                     |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>Código: F319</b>      | <b>INFORME MENSUAL DE GESTIÓN<br/>SUPERVISIÓN, VERIFICACIÓN Y RECIBO A<br/>SATISFACCIÓN DEL CUMPLIMIENTO DE LAS<br/>OBLIGACIONES CONTRACTUALES</b> |  |
| <b>Versión: 8</b>        |                                                                                                                                                    |                                                                                     |
| <b>Fecha: 05/03/2025</b> |                                                                                                                                                    |                                                                                     |
| <b>Página 4 de 4</b>     |                                                                                                                                                    |                                                                                     |

relacionados, por parte del contratista INFOTIC S.A.S identificado(a) con NIT 900.068.796-1 para los servicios prestados en los periodos de: JULIO y AGOSTO de 2025.

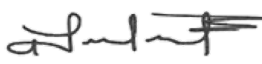
Se deja constancia que Infotíc entregó el informe de gestión del mes de agosto y que la facturación de los servicios prestados en dicho periodo fue revisada y aprobada al proveedor, en virtud de lo anterior se aprueba realizar trámite de pago para las siguientes facturas:

- Servicios de JULIO 2025 con No. **FVE-1980** por valor de **SETECIENTOS SETENTA Y OCHO MILLONES QUINIENTOS ONCE MIL OCHOCIENTOS NTA Y SIETE PESOS M/CTE**, de acuerdo con memorando 20255000835834-E Id: 6609345
- Servicio de AGOSTO 2025 con No. **FVE-2016** por valor de **SETECIENTOS SETENTA Y SIETE MILLONES TRESCIENTOS UN MIL CIEN PESOS M/CTE**, de acuerdo con memorando 20255000954603-E Id: 6771079.

**Nota: Se adjuntan los siguientes documentos como parte integral del presente informe para dar trámite al pago del mes de julio de 2025.**

- 1.1. Notificación de valor a facturar mes de julio de 2025
- 1.2. Confirmación de valor a facturar mes de julio de 2025
- 1.3. Factura FVE-1980 JULIO de fecha 01 de septiembre de 2025
- 1.4. Certificación parafiscales mes de agosto de 2025.
- 1.5. Informe de Gestión Servicio julio 2025-INFOTIC
- 2.1. Notificación de valor a facturar mes de agosto de 2025
- 2.2. Confirmación de valor a facturar mes de agosto de 2025
- 2.3. Factura FVE-2016 AGOSTO de fecha 24 de septiembre de 2025
- 2.4. Certificación parafiscales mes de agosto de 2025.
- 2.5. Informe de Gestión Servicio agosto 2025-INFOTIC

En constancia se firma en Bogotá D.C. a los 24 días del mes de septiembre de 2025.

| <b>Presentó:</b>                                                                                                                                                | <b>Aprobó:</b>                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <br><b>FIRMA DEL CONTRATISTA<br/>MONICA VILLAMIZAR<br/>No. CC 26.862.573</b> | <br><b>FIRMA DEL SUPERVISOR<br/>JAIME ALEJANDRO BECERRA ACOSTA<br/>No. CC 12.647.308</b> |

Revisó: Armando Castro- Abogado VOT 

Carmenza Duran- Abogada VOT 

Revisó: Juan David Orozco Sequeda-Profesional Presupuesto-Administrativo 

Revisó: German Manuel Diaz Mejia 

Revisó: Joao Do Nelson Ducuara Serrato 



Responsables de IVA - No Somos Autorretenedores  
Desde el año 2022 al 2024  
7020-1 Actividad Principal 8,66% 6202 Otras Actividades 6,9%  
8299 Actividad Secundaria 9,66% 6209 Otras Actividades 9,66%  
Sociedad de economia mixta con participacion del 51% de  
Infimanizales

## INFOTIC S.A

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

Tel: 7466000 Fax: 7466000

Bogotá, D.C.

## Factura Electrónica De Venta

**FVE-1980**



### Cliente

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

**Fecha:** 9/1/2025 4:25:54 PM  
**Forma de pago:** CREDITO 30 DIAS  
**Moneda:** COP  
**Fecha vcto:** 10/1/2025 12:00:00 AM  
**Medio de pago**

| Servicio   | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Cant | Valor unitario    | Valor bruto      | Valor total       |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------|------------------|-------------------|
| VS90900102 | SERVICIOS ESPECIALIZADOS EN OUTSOURCING PARA LA CONECTIVIDAD, RED DE COMUNICACIONES, CENTRO DE DATOS Y SERVICIOS CONEXOS CON VALOR AGREGADO PARA EL ICETEX, DURANTE EL MES DE JULIO DE 2025.<br><br>SERVICIOS OPERACIÓN MES DE JULIO 2025 (INCLUIDO IVA): \$833.741.120 (-) DESCUENTOS INCLUIDO IVA: CONECTIVIDAD Y RED DE COMUNICACIONES: -\$19.880.860 CENTRO DE DATOS: -\$34.750.718 SERVICIO DE SEGURIDAD: \$597.644 TOTAL DESCUENTO CON IVA: - \$55.229.223<br><br>OBJETO DEL CONTRATO: SERVICIOS ESPECIALIZADOS EN OUTSOURCING PARA LA CONECTIVIDAD, RED DE COMUNICACIONES, CENTRO DE DATOS Y SERVICIOS CONEXOS CON VALOR AGREGADO PARA EL ICETEX. | 1.00 | \$ 654,211,678.00 | \$654,211,678.00 | \$ 778,511,897.00 |

| IMPUESTOS | BASE          | TASA | TOTAL         |
|-----------|---------------|------|---------------|
| IVA       | \$654,211,678 | 19 % | \$124,300,219 |

SETECIENTOS SETENTA Y OCHO MILLONES QUINIENTOS ONCE MIL OCHOCIENTOS NOVENTA Y SIETE PESOS M/CTE \*\*\*\*\*

### Notas

facturacion\_electronica@icetex.gov.co

RESPONSABLE: MONICA MARIA VILLAMIZAR SANCHEZ

|               |                  |
|---------------|------------------|
| VALOR BRUTO   | \$654,211,678.00 |
| DESCUENTO     | \$0.00           |
| SUBTOTAL      | \$654,211,678.00 |
| IVA           | \$124,300,219.00 |
| TOTAL FACTURA | \$778,511,897.00 |

**AUTORIZACIÓN NUMERACIÓN DE FACTURACIÓN** Resolución N°: 18764094170779 Numeración Desde: FVE 1855 Hasta: FVE 2000

**Vigencia Desde:** 2025/06/09 **Hasta:** 2026/06/09 **12 Meses**

**CUFE** f384621bc03ca113697b63fb2bf76e0f70647914b18b4813fde6d874b5548cb7c5d015ddb37a8e5e339052740d05299

### FIRMA DIGITAL:

rsdm1FTmoa6XTC3o4zgZkbLYO0MjP0JjxiUDJ8p/tXswKe2wXjTl9WBhfd9UuzSGjJamOUvwsLw0SCeLNgTg+c19eAPzjh483+OBjSpahEdR5VB7oKZtzX4OHpQ1X96kevg6zt2BSb20+0OgrGr9+tv5C0g+eR9NkgQB+BzLD+7BpURt6diOTQBIa+Qd3ybcCAMpiN9Wz1FY9lCP5JW6Z+tzmmYAKoJScldtI97NhXcEcN7Qh6dcOfhzrpz5WPoSPhtC0rrxL9Z8E+HQQ6TqLPXWwoVcAtrcdZHMQuDKtJ5LjE05yMQCAU6giJqs8vaaakFCT18DnXkKDb4xD5nCG==

**FECHA DIAN:** 2025-09-01 16:26:31-05:00

Emisor

Nombre Leable v Fecha de Entrega

**"SOMOS AGENTES RETENEDORES DE IVA"**

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

REIMPRESO

ORIGINAL

Página 1 de 1

**EL SUSCRITO REVISOR FISCAL DE INFOTIC S.A. CON NIT. 900.068.796-1,  
KATHERINE MUÑOZ CARDONA IDENTIFICADO CON CEDULA DE CIUDADANÍA  
No. 1.053.793.749 Y TARJETA PROFESIONAL 184969 –T EXPEDIDA  
POR LA JUNTA CENTRAL DE CONTADORES**

**CERTIFICA QUE**

1. A la fecha se encuentra en curso mi examen sobre los estados financieros de la Compañía por el año que terminará el 31 de diciembre de 2025.
2. El último pago se realizó el día cuatro (04) de julio de 2025, para los aportes correspondientes a salud del mes de julio de 2025 y para pensión, riesgos laborales y aportes parafiscales del mes de junio de 2025 mediante la planilla No. 9488250865, el último pago realizado para cancelar los aportes de sus trabajadores enviados en misión al Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior "Mariano Ospina Perez"–Icetex para el desarrollo del contrato número 792 de 2022, no estoy enterado de situaciones indicativas de inobservancia en el cumplimiento de las obligaciones legales provenientes del sistema de seguridad social en salud y lo correspondiente a riesgos laborales, pensión, ICBF, SENA y cajas de compensación Familiar de conformidad con el artículo 50 de la Ley 789 de diciembre de 2002 modificada por el artículo 9 de la Ley 828 de 2003, el artículo. 32 de la Ley 1150 de 2007 y el artículo 24 del Decreto 2106 de 2019.

**ANTE SOLICITUD ESPECIAL, CONSIDERAR LAS SIGUIENTES ALTERNATIVAS:**

3. La sociedad se encuentra beneficiada por la exoneración de aportes establecida en el artículo 65 de la Ley 1819 de 2016, por lo tanto, no posee obligaciones de pagos por los parafiscales correspondientes al SENA y al ICBF, así como las cotizaciones al Régimen Contributivo de Salud, correspondientes a los trabajadores que devenguen, individualmente considerados, menos de diez (10) salarios mínimos mensuales legales vigentes.

La presente certificación se expide en Manizales a los nueve (09) días del mes de julio de 2025, a solicitud de la administración de la compañía.

En cumplimiento con el artículo 2 de la ley 43 de 1990, mi firma como Revisor Fiscal en las Certificaciones se fundamenta en los libros de contabilidad. La información que no es de carácter contable fue verificada con las fuentes indicadas.



**KATHERINE MUÑOZ CARDONA**

Revisor Fiscal

Tarjeta Profesional No. **184969-T**

Designado por **CROWE CO S.A.S.**

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

| DATOS GENERALES DE LA LIQUIDACION |         |            |            |          |            |            |            |           |             |
|-----------------------------------|---------|------------|------------|----------|------------|------------|------------|-----------|-------------|
| Periodo                           |         | Clave      |            | Tipo     | Fecha      |            | Pago       |           |             |
| Pensión                           | Salud   | Pago       | Planilla   | Planilla | Limite     | Pago       | Banco      | Dias Mora | Valor       |
| 2025-06                           | 2025-07 | 1602991934 | 9488250865 | E        | 2025/07/22 | 2025/07/04 | BANCO ITAU | 0         | \$4,772,000 |

| RESUMEN DE PAGO              |        |             |    |           |                 |                |                        |               |  |
|------------------------------|--------|-------------|----|-----------|-----------------|----------------|------------------------|---------------|--|
| RIESGO                       | CODIGO | NIT         | DV | AFILIADOS | VALOR LIQUIDADO | INTERESES MORA | SALDOS E INCAPACIDADES | VALOR A PAGAR |  |
| AFP (ADMINISTRADORAS: 2)     |        |             |    | 3         | \$3,149,700     | \$0            | \$0                    | \$3,149,700   |  |
| COLPENSIONES                 | 25-14  | 900,336,004 | 7  | 2         | \$2,594,400     | \$0            | \$0                    | \$2,594,400   |  |
| PORVENIR                     | 230301 | 800,224,808 | 8  | 1         | \$555,300       | \$0            | \$0                    | \$555,300     |  |
| ARL (ADMINISTRADORAS: 1)     |        |             |    | 3         | \$91,300        | \$0            | \$0                    | \$91,300      |  |
| POSITIVA COMPAÑIA DE SEGUROS | 14-23  | 860,011,153 | 6  | 3         | \$91,300        | \$0            | \$0                    | \$91,300      |  |
| CCF (ADMINISTRADORAS: 1)     |        |             |    | 3         | \$781,700       | \$0            | \$0                    | \$781,700     |  |
| COMFACUNDI                   | CCF26  | 860,045,904 | 7  | 3         | \$781,700       | \$0            | \$0                    | \$781,700     |  |
| EPS (ADMINISTRADORAS: 2)     |        |             |    | 3         | \$749,300       | \$0            | \$0                    | \$749,300     |  |
| NUEVA E.P.S.                 | EPS037 | 900,156,264 | 2  | 1         | \$231,600       | \$0            | \$0                    | \$231,600     |  |
| SANITAS                      | EPS005 | 800,251,440 | 6  | 2         | \$517,700       | \$0            | \$0                    | \$517,700     |  |
| TOTAL                        |        |             |    | 3         | \$4,772,000     | \$0            | \$0                    | \$4,772,000   |  |

**EL SUSCRITO REVISOR FISCAL DE INFOTIC S.A. CON NIT. 900.068.796-1,  
KATHERINE MUÑOZ CARDONA IDENTIFICADO CON CEDULA DE CIUDADANÍA  
No. 1.053.793.749 Y TARJETA PROFESIONAL 184969 –T EXPEDIDA  
POR LA JUNTA CENTRAL DE CONTADORES**

**CERTIFICA QUE**

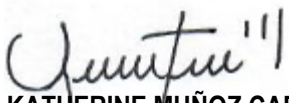
1. A la fecha se encuentra en curso mi examen sobre los estados financieros de la Compañía por el año que terminará el 31 de diciembre de 2025.
2. El último pago se realizó el día seis (06) de agosto de 2025, para los aportes correspondientes a salud del mes de agosto de 2025 y para pensión, riesgos laborales y aportes parafiscales del mes de julio de 2025 mediante la planilla No. 9489990888, el último pago realizado para cancelar los aportes de sus trabajadores enviados en misión al Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior “Mariano Ospina Perez”–Icetex para el desarrollo del contrato número 792 de 2022, no estoy enterado de situaciones indicativas de inobservancia en el cumplimiento de las obligaciones legales provenientes del sistema de seguridad social en salud y lo correspondiente a riesgos laborales, pensión, ICBF, SENA y cajas de compensación Familiar de conformidad con el artículo 50 de la Ley 789 de diciembre de 2002 modificada por el artículo 9 de la Ley 828 de 2003, el artículo. 32 de la Ley 1150 de 2007 y el artículo 24 del Decreto 2106 de 2019.

**ANTE SOLICITUD ESPECIAL, CONSIDERAR LAS SIGUIENTES ALTERNATIVAS:**

3. La sociedad se encuentra beneficiada por la exoneración de aportes establecida en el artículo 65 de la Ley 1819 de 2016, por lo tanto, no posee obligaciones de pagos por los parafiscales correspondientes al SENA y al ICBF, así como las cotizaciones al Régimen Contributivo de Salud, correspondientes a los trabajadores que devenguen, individualmente considerados, menos de diez (10) salarios mínimos mensuales legales vigentes.

La presente certificación se expide en Manizales a los ocho (08) días del mes de agosto de 2025, a solicitud de la administración de la compañía.

En cumplimiento con el artículo 2 de la ley 43 de 1990, mi firma como Revisor Fiscal en las Certificaciones se fundamenta en los libros de contabilidad. La información que no es de carácter contable fue verificada con las fuentes indicadas.



**KATHERINE MUÑOZ CARDONA**

Revisor Fiscal

Tarjeta Profesional No. **184969-T**

Designado por **CROWE CO S.A.S.**

## Planilla Integrada

### DATOS GENERALES DEL APORTANTE

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

### DATOS GENERALES DE LA LIQUIDACION

| Periodo |         | Clave      |            | Tipo     | Fecha      |            | Pago               |           |             |
|---------|---------|------------|------------|----------|------------|------------|--------------------|-----------|-------------|
| Pensión | Salud   | Pago       | Planilla   | Planilla | Limite     | Pago       | Banco              | Dias Mora | Valor       |
| 2025-07 | 2025-08 | 1683804909 | 9489990888 | E        | 2025/08/26 | 2025/08/06 | BANCO DE OCCIDENTE | 0         | \$4,758,100 |

### LIQUIDACION DETALLADA DE APORTES

| EMPLEADO                                         |         |          |                                 |                |                 |             |            |                                 |     |           |     |           |     |     |     |     |     | NOVEDADES        |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |            |  |  |  |
|--------------------------------------------------|---------|----------|---------------------------------|----------------|-----------------|-------------|------------|---------------------------------|-----|-----------|-----|-----------|-----|-----|-----|-----|-----|------------------|-----|-----|-----|------------------|---------------|-----|------------------|---------------|-----|------------------|---------------|--------|---------------------|------------------|------------|------------|--|--|--|
| No.                                              | Tipo id | No id    | Nombre                          | Tipo Cotizante | Horas Laboradas | Extran-jero | Temp. Ext. | Fecha Radicación en el Exterior | ing | Fecha ing | ret | Fecha ret | tde | tae | tdp | tap | vsp | Fecha Inicio vsp | cor | vst | sln | Fecha Inicio sln | Fecha Fin sln | ige | Fecha Inicio ige | Fecha Fin ige | lma | Fecha Inicio lma | Fecha Fin lma | vac-lr | Fecha Inicio vac-lr | Fecha Fin vac-lr | avp        | vct        |  |  |  |
| Sucursal: BOGOTA (3 Afiliados)                   |         |          |                                 |                |                 |             |            |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |            |  |  |  |
| Centro de Trabajo: CENTRO TRABAJO 1(3 Afiliados) |         |          |                                 |                |                 |             |            |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |            |  |  |  |
| Ciudad: BOGOTA Depto: BOGOTA D.E.(3 Afiliados)   |         |          |                                 |                |                 |             |            |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |            |  |  |  |
| 1                                                | CC      | 52934365 | PARRA BUSTOS ANGIE PAOLA        | Dependiente    | 169             | No          | No         |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |            |  |  |  |
| 2                                                | CC      | 79468174 | PULIDO FAJARDO FRANCISCO JAVIER | Dependiente    | 220             | No          | No         |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |            |  |  |  |
| 3                                                | CC      | 63513251 | SUAREZ OSORIO MARIA VICTORIA    | Dependiente    | 213             | No          | No         |                                 |     |           |     |           |     |     |     |     |     |                  |     | X   |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |            |  |  |  |
| Centro de Trabajo: MENSAJERIA(2 Afiliados)       |         |          |                                 |                |                 |             |            |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |            |  |  |  |
| Ciudad: BOGOTA Depto: BOGOTA D.E.(2 Afiliados)   |         |          |                                 |                |                 |             |            |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |            |  |  |  |
| 4                                                | CC      | 52934365 | PARRA BUSTOS ANGIE PAOLA        | Dependiente    | 51              | No          | No         |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     | X                | 2025/07/01 | 2025/07/07 |  |  |  |
| 5                                                | CC      | 63513251 | SUAREZ OSORIO MARIA VICTORIA    | Dependiente    | 7               | No          | No         |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        | L                   | 2025/07/01       | 2025/07/01 |            |  |  |  |
| Total Afiliados(3)                               |         |          |                                 |                |                 |             |            |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |            |  |  |  |

## Planilla Integrada

|                  |               |     |                  |               |     | SALARIO     |          |                 | PENSION        |      |             |        |                            |                  |                                 |                                |                             |                    |                   |             |                |                | SALUD       |     |           |                  |           |  |
|------------------|---------------|-----|------------------|---------------|-----|-------------|----------|-----------------|----------------|------|-------------|--------|----------------------------|------------------|---------------------------------|--------------------------------|-----------------------------|--------------------|-------------------|-------------|----------------|----------------|-------------|-----|-----------|------------------|-----------|--|
| Fecha Inicio vct | Fecha Fin vct | irt | Fecha Inicio irt | Fecha Fin irt | vip | Valor       | Integral | Tipo de Salario | Administradora | Dias | IBC         | Tarifa | Tarifa Alto Riesgo Pensión | Valor Cotización | Cotización Voluntaria Empleador | Cotización Voluntaria Afiliado | Fondo Solidaridad Pensional | Fondo Subsistencia | Valor No retenido | Total       | AFP Destino    | Administradora | Dias        | IBC | Tarifa    | Valor Cotización | Valor UP  |  |
|                  |               |     |                  |               |     |             |          |                 |                |      |             |        |                            |                  |                                 |                                |                             |                    |                   |             | \$3,182,600    |                |             |     |           |                  | \$757,100 |  |
|                  |               |     |                  |               |     |             |          |                 |                |      |             |        |                            |                  |                                 |                                |                             |                    |                   |             | \$3,020,100    |                |             |     |           |                  | \$716,900 |  |
|                  |               |     |                  |               |     |             |          |                 |                |      |             |        |                            |                  |                                 |                                |                             |                    |                   |             | \$3,020,100    |                |             |     |           |                  | \$716,900 |  |
|                  |               |     |                  |               |     | \$3,470,000 | No       | Fijo            | PORVENIR       | 23   | \$2,660,334 | 16%    | SIN RIESGO                 | \$425,700        | \$0                             | \$0                            | \$0                         | \$0                | \$0               | \$425,700   | SANITAS        | 23             | \$2,660,334 | 4%  | \$106,500 |                  |           |  |
|                  |               |     |                  |               |     | \$9,470,000 | No       | Fijo            | COLPENSIONES   | 30   | \$9,470,000 | 16%    | SIN RIESGO                 | \$1,515,200      | \$0                             | \$0                            | \$47,400                    | \$47,400           | \$0               | \$1,610,000 | SANITAS        | 30             | \$9,470,000 | 4%  | \$378,800 |                  |           |  |
|                  |               |     |                  |               |     | \$5,790,000 | No       | Fijo            | COLPENSIONES   | 29   | \$5,790,000 | 16%    | SIN RIESGO                 | \$926,400        | \$0                             | \$0                            | \$29,000                    | \$29,000           | \$0               | \$984,400   | NUEVA E. P. S. | 29             | \$5,790,000 | 4%  | \$231,600 |                  |           |  |
|                  |               |     |                  |               |     |             |          |                 |                |      |             |        |                            |                  |                                 |                                |                             |                    |                   | \$162,500   |                |                |             |     |           | \$40,200         |           |  |
|                  |               |     |                  |               |     |             |          |                 |                |      |             |        |                            |                  |                                 |                                |                             |                    |                   | \$162,500   |                |                |             |     |           | \$40,200         |           |  |
|                  |               |     |                  |               |     | \$3,470,000 | No       | Fijo            | PORVENIR       | 7    | \$809,667   | 16%    | SIN RIESGO                 | \$129,600        | \$0                             | \$0                            | \$0                         | \$0                | \$0               | \$129,600   | SANITAS        | 7              | \$809,667   | 4%  | \$32,400  |                  |           |  |
|                  |               |     |                  |               |     | \$5,790,000 | No       | Fijo            | COLPENSIONES   | 1    | \$193,000   | 16%    | SIN RIESGO                 | \$30,900         | \$0                             | \$0                            | \$1,000                     | \$1,000            | \$0               | \$32,900    | NUEVA E. P. S. | 1              | \$193,000   | 4%  | \$7,800   |                  |           |  |
|                  |               |     |                  |               |     |             |          |                 |                |      |             |        |                            |                  |                                 |                                |                             |                    |                   | \$3,182,600 |                |                |             |     |           | \$757,100        |           |  |

|     |           |             | CCF            |      |             |        |                  | RIESGOS                      |      |             |        |              |                  | PARAFISCALES |     |             |                       |             |                       |             |                       |            |                      |                       |
|-----|-----------|-------------|----------------|------|-------------|--------|------------------|------------------------------|------|-------------|--------|--------------|------------------|--------------|-----|-------------|-----------------------|-------------|-----------------------|-------------|-----------------------|------------|----------------------|-----------------------|
| C   | Total     | EPS Destino | Administradora | Dias | IBC         | Tarifa | Valor Cotización | Administradora               | Dias | IBC         | Tarifa | Clase Riesgo | Valor Cotización | Dias         | IBC | Tarifa SENA | Valor Cotización SENA | Tarifa ICBF | Valor Cotización ICBF | Tarifa ESAP | Valor Cotización ESAP | Tarifa MEN | Valor Cotización MEN | Exonerado SENA e ICBF |
|     | \$757,100 |             |                |      |             |        | \$724,700        |                              |      |             |        |              | \$93,700         |              |     |             | \$0                   |             | \$0                   |             | \$0                   |            |                      | \$0                   |
|     | \$716,900 |             |                |      |             |        | \$716,900        |                              |      |             |        |              | \$93,700         |              |     |             | \$0                   |             | \$0                   |             | \$0                   |            |                      | \$0                   |
|     | \$716,900 |             |                |      |             |        | \$716,900        |                              |      |             |        |              | \$93,700         |              |     |             | \$0                   |             | \$0                   |             | \$0                   |            |                      | \$0                   |
| \$0 | \$106,500 |             | COMFACUNDI     | 23   | \$2,660,333 | 4%     | \$106,500        | POSITIVA COMPANIA DE SEGUROS | 23   | \$2,660,334 | 0.522% | 1            | \$13,900         | 23           | \$0 | 0%          | \$0                   | 0%          | \$0                   | 0%          | \$0                   | 0%         | \$0                  | \$1                   |
| \$0 | \$378,800 |             | COMFACUNDI     | 30   | \$9,470,000 | 4%     | \$378,800        | POSITIVA COMPANIA DE SEGUROS | 30   | \$9,470,000 | 0.522% | 1            | \$49,500         | 30           | \$0 | 0%          | \$0                   | 0%          | \$0                   | 0%          | \$0                   | 0%         | \$0                  | \$1                   |
| \$0 | \$231,600 |             | COMFACUNDI     | 29   | \$5,790,000 | 4%     | \$231,600        | POSITIVA COMPANIA DE SEGUROS | 29   | \$5,790,000 | 0.522% | 1            | \$30,300         | 29           | \$0 | 0%          | \$0                   | 0%          | \$0                   | 0%          | \$0                   | 0%         | \$0                  | \$1                   |
|     | \$40,200  |             |                |      |             |        | \$7,800          |                              |      |             |        |              | \$0              |              |     |             | \$0                   |             | \$0                   |             | \$0                   |            | \$0                  |                       |
|     | \$40,200  |             |                |      |             |        | \$7,800          |                              |      |             |        |              | \$0              |              |     |             | \$0                   |             | \$0                   |             | \$0                   |            | \$0                  |                       |
| \$0 | \$32,400  |             | COMFACUNDI     | 7    | \$0         | 0%     | \$0              | POSITIVA COMPANIA DE SEGUROS | 7    | \$809,667   | 0%     | 1            | \$0              | 7            | \$0 | 0%          | \$0                   | 0%          | \$0                   | 0%          | \$0                   | 0%         | \$0                  | \$1                   |
| \$0 | \$7,800   |             | COMFACUNDI     | 1    | \$193,000   | 4%     | \$7,800          | POSITIVA COMPANIA DE SEGUROS | 1    | \$193,000   | 0%     | 1            | \$0              | 1            | \$0 | 0%          | \$0                   | 0%          | \$0                   | 0%          | \$0                   | 0%         | \$0                  | \$1                   |
|     | \$757,100 |             |                |      |             |        | \$724,700        |                              |      |             |        |              | \$93,700         |              |     |             | \$0                   |             | \$0                   |             | \$0                   |            |                      | \$0                   |

## Planilla Integrada

| DATOS GENERALES DEL APORTANTE     |         |              |             |                             |            |                    |                           |                        |           |                       |
|-----------------------------------|---------|--------------|-------------|-----------------------------|------------|--------------------|---------------------------|------------------------|-----------|-----------------------|
| Identificación                    | dv      | Razon Social |             | Clase Aportante             |            | Sucursal Principal | Direccion                 | Ciudad-Departamento    | Teléfono  | Exonerado SENA e ICBF |
| NIT 900068796                     | 1       | INFOTIC S A  |             | B - MENOS DE 200 COTIZANTES |            | BOGOTA             | CL 93 B N° 13 - 44 PISO 2 | BOGOTA-BOGOTA D.E.     | 7466000   | Si                    |
| DATOS GENERALES DE LA LIQUIDACION |         |              |             |                             |            |                    |                           |                        |           |                       |
| Periodo                           |         | Clave        |             | Tipo                        | Fecha      |                    | Pago                      |                        |           |                       |
| Pensión                           | Salud   | Pago         | Planilla    | Planilla                    | Limite     | Pago               | Banco                     |                        | Días Mora | Valor                 |
| 2025-07                           | 2025-08 | 1683804909   | 9489990888  | E                           | 2025/08/26 | 2025/08/06         | BANCO DE OCCIDENTE        |                        | 0         | \$4,758,100           |
| RESUMEN DE PAGO                   |         |              |             |                             |            |                    |                           |                        |           |                       |
| RIESGO                            |         | CODIGO       | NIT         | DV                          | AFILIADOS  | VALOR LIQUIDADO    | INTERESES MORA            | SALDOS E INCAPACIDADES |           | VALOR A PAGAR         |
| AFP (ADMINISTRADORAS: 2)          |         |              |             |                             | 3          | \$3,182,600        | \$0                       | \$0                    |           | \$3,182,600           |
| COLPENSIONES                      |         | 25-14        | 900,336,004 | 7                           | 2          | \$2,627,300        | \$0                       | \$0                    |           | \$2,627,300           |
| PORVENIR                          |         | 230301       | 800,224,808 | 8                           | 1          | \$555,300          | \$0                       | \$0                    |           | \$555,300             |
| ARL (ADMINISTRADORAS: 1)          |         |              |             |                             | 3          | \$93,700           | \$0                       | \$0                    |           | \$93,700              |
| POSITIVA COMPAÑIA DE SEGUROS      |         | 14-23        | 860,011,153 | 6                           | 3          | \$93,700           | \$0                       | \$0                    |           | \$93,700              |
| CCF (ADMINISTRADORAS: 1)          |         |              |             |                             | 3          | \$724,700          | \$0                       | \$0                    |           | \$724,700             |
| COMFACUNDI                        |         | CCF26        | 860,045,904 | 7                           | 3          | \$724,700          | \$0                       | \$0                    |           | \$724,700             |
| EPS (ADMINISTRADORAS: 2)          |         |              |             |                             | 3          | \$757,100          | \$0                       | \$0                    |           | \$757,100             |
| NUEVA E.P.S.                      |         | EPS037       | 900,156,264 | 2                           | 1          | \$239,400          | \$0                       | \$0                    |           | \$239,400             |
| SANITAS                           |         | EPS005       | 800,251,440 | 6                           | 2          | \$517,700          | \$0                       | \$0                    |           | \$517,700             |
| TOTAL                             |         |              |             |                             | 3          | \$4,758,100        | \$0                       | \$0                    |           | \$4,758,100           |

REPUBLICA DE COLOMBIA  
IDENTIFICACION PERSONAL  
CEDULA DE CIUDADANIA

1.053.793.749

NUMERO

MUÑOZ CARDONA

APELLIDOS

KATHERINE

NOMBRES

Katherine Muñoz Cardona

FIRMA



INDICE DERECHO

FECHA DE NACIMIENTO  
MANIZALES  
(CALDAS)

25-MAR-1989

LUGAR DE NACIMIENTO

1.60

A+

F

ESTATURA

G.S. RH

SEXO

28-MAR-2007 MANIZALES

FECHA Y LUGAR DE EXPEDICION

REGISTRADOR NACIONAL  
JUAN CARLOS GALINDO VACHA



P-0900100-35159751-F-1053793749-20070610

0018107161C 02 239409704

República de Colombia  
Ministerio de Comercio, Industria y Turismo

UNIDAD ADMINISTRATIVA ESPECIAL **JUNTA CENTRAL DE CONTADORES**

**184969-T**

**KATHERINE MUÑOZ CARDONA**  
C.C. 1053793749  
RES. INSCRIPCION 848 DEL 23/12/2013  
UNIVERSIDAD DE MANIZALES



  
**JOSE ORLANDO RAMIREZ ZULUAGA**  
DIRECTOR GENERAL

**273465** **196340**

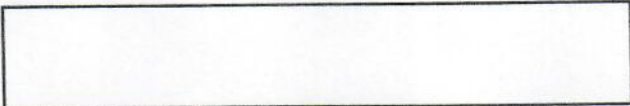
Identificación Plástica S.A. 180942/0119

República de Colombia  
Ministerio de Comercio, Industria y Turismo

UNIDAD ADMINISTRATIVA ESPECIAL **JUNTA CENTRAL DE CONTADORES**

Esta tarjeta es el único documento que lo acredita como Contador Público de acuerdo con lo establecido en la Ley 43 de 1990. Es personal e intransferible.

Agradecemos a quien encuentre esta tarjeta comunicarse al PBX: (57)(1) 644 4450 o devolverla a la UAE – Junta Central de Contadores a la Carrera 16 No. 97- 46 Of.301 en Bogotá D.C.



FIRMA

UNIDAD  
ADMINISTRATIVA  
ESPECIAL

**JUNTA CENTRAL  
DE CONTADORES**



Certificado No:

170F7AHE045407E0

**LA REPUBLICA DE COLOMBIA**

**MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO**

**UNIDAD ADMINISTRATIVA ESPECIAL**

**JUNTA CENTRAL DE CONTADORES**

**CERTIFICA A:  
QUIEN INTERESE**

Que el contador público **KATHERINE MUÑOZ CARDONA** identificado con CÉDULA DE CIUDADANÍA No 1053793749 de MANIZALES (CALDAS) Y Tarjeta Profesional No 184969-T SI tiene vigente su inscripción en la Junta Central de Contadores y desde la fecha de Inscripción.

**NO REGISTRA ANTECEDENTES DISCIPLINARIOS \*\*\*\*\***  
\*\*\*\*\*  
\*\*\*\*\*

Dado en BOGOTA a los 21 días del mes de Abril de 2025 con vigencia de (3) Meses, contados a partir de la fecha de su expedición.

  
SANDRA MILENA BARRIOS PULIDO  
**DIRECTOR GENERAL**

ESTE CERTIFICADO DIGITAL TIENE PLENA VALIDEZ DE CONFORMIDAD CON LO ESTABLECIDO EN EL ARTICULO 2 DE LA LEY 527 DE 1999, DECRETO UNICO REGLAMENTARIO 1074 DE 2015 Y ARTICULO 6 PARAGRAFO 3 DE LA LEY 962 DEL 2005

Para confirmar los datos y veracidad de este certificado, lo puede consultar en la página web [www.jcc.gov.co](http://www.jcc.gov.co) digitando el número del certificado



Responsables de IVA - No Somos Autorretenedores  
Desde el año 2022 al 2024  
7020-1 Actividad Principal 8,66% 6202 Otras Actividades 6,9%  
8299 Actividad Secundaria 9,66% 6209 Otras Actividades 9,66%  
Sociedad de economia mixta con participacion del 51% de  
Infimanizales

## INFOTIC S.A

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

Tel: 7466000 Fax: 7466000

Bogotá, D.C.

## Factura Electrónica De Venta

**FVE-2016**



### Cliente

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

**Fecha:** 9/24/2025 3:08:38 PM  
**Forma de pago:** CREDITO 30 DIAS  
**Moneda:** COP  
**Fecha vcto:** 10/24/2025 12:00:00 AM  
**Medio de pago**

| Servicio   | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Cant | Valor unitario    | Valor bruto      | Valor total       |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------|------------------|-------------------|
| VS90900102 | SERVICIOS ESPECIALIZADOS EN OUTSOURCING PARA LA CONECTIVIDAD, RED DE COMUNICACIONES, CENTRO DE DATOS Y SERVICIOS CONEXOS CON VALOR AGREGADO PARA EL ICETEX, DURANTE EL MES DE AGOSTO DE 2025.<br><br>SERVICIOS OPERACIÓN MES DE AGOSTO 2025 (INCLUIDO IVA): \$833.741.120 (-) DESCUENTOS INCLUIDO IVA: CONECTIVIDAD Y RED DE COMUNICACIONES: -\$16.798.291 CENTRO DE DATOS: -\$39.044.084 SERVICIO DE SEGURIDAD: \$597.644 TOTAL DESCUENTO CON IVA: -\$56.440.020<br><br>OBJETO DEL CONTRATO 2022-0792: SERVICIOS ESPECIALIZADOS EN OUTSOURCING PARA LA CONECTIVIDAD, RED DE COMUNICACIONES, CENTRO DE DATOS Y SERVICIOS CONEXOS CON VALOR AGREGADO PARA EL ICETEX. | 1.00 | \$ 653,194,202.00 | \$653,194,202.00 | \$ 777,301,100.00 |

| IMPUESTOS | BASE          | TASA | TOTAL         |
|-----------|---------------|------|---------------|
| IVA       | \$653,194,202 | 19 % | \$124,106,898 |

|                                                                                                                                                                                                           |                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SETECIENTOS SETENTA Y SIETE MILLONES TRESCIENTOS UN MIL CIEN PESOS M/CTE</b><br>*****<br><br><b>Notas</b><br>facturacion_electronica@icetex.gov.co<br><br>RESPONSABLE: MONICA MARIA VILLAMIZAR SANCHEZ | <b>VALOR BRUTO</b> \$653,194,202.00<br><b>DESCUENTO</b> \$0.00<br><b>SUBTOTAL</b> \$653,194,202.00<br><b>IVA</b> \$124,106,898.00<br><b>TOTAL FACTURA</b> \$777,301,100.00 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**AUTORIZACIÓN NUMERACIÓN DE FACTURACIÓN** Resolución N°: 18764098498982 Numeración Desde: FVE 2001 Hasta: FVE 4000

**Vigencia Desde:** 2025/09/11 **Hasta:** 2027/09/11 **24 Meses**

**CUFE** f24145dc2541d4b2986725b50d486b57d5fdf211c29df33e84385df3d59acaefe1cc9be2c1b631dbe9a32fed4d2b092

### FIRMA DIGITAL:

Jj+6xEhUmZK2g/KOt+P6pwTj6McmsCUGLUTg4G9QC/VwimhgOjqHJwQsSxSwbrMXxXKiQIDXwn/xoqCNnUrVuM7JWmj9oUILqFy5DZZYqQh0Oavly9Dh3RkphYW  
lQvVMHddiCg7VAFSJHU6aWFZZFJeEg5pDwz2EeOWwriboF6tC8CJ46p87cJv5vqUEdX/M1ZsKbLYt4HqkUI7X6NBcdNzgF77uUDuTCoX08VupPLnwNGo3SpcHl2Nj  
q89icoFO9PN0PEYvN/6l6g+Ajlif3j6AozkPP1u3p+Z0iQuTvHb15Al9f080YuAKWC0roPA6XB+fPsOE4BBs4olu9ggeTw==

**FECHA DIAN:** 2025-09-24 15:10:06-05:00

Emisor

Nombre Leable v Fecha de Entrega

**"SOMOS AGENTES RETENEDORES DE IVA"**

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

REIMPRESO

ORIGINAL

Página 1 de 1

**EL SUSCRITO REVISOR FISCAL DE INFOTIC S.A. CON NIT. 900.068.796-1,  
KATHERINE MUÑOZ CARDONA IDENTIFICADO CON CEDULA DE CIUDADANÍA  
No. 1.053.793.749 Y TARJETA PROFESIONAL 184969 –T EXPEDIDA  
POR LA JUNTA CENTRAL DE CONTADORES**

**CERTIFICA QUE**

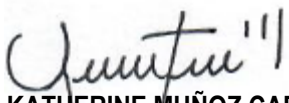
1. A la fecha se encuentra en curso mi examen sobre los estados financieros de la Compañía por el año que terminará el 31 de diciembre de 2025.
2. El último pago se realizó el día seis (06) de agosto de 2025, para los aportes correspondientes a salud del mes de agosto de 2025 y para pensión, riesgos laborales y aportes parafiscales del mes de julio de 2025 mediante la planilla No. 9489990888, el último pago realizado para cancelar los aportes de sus trabajadores enviados en misión al Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior "Mariano Ospina Perez"–Icetex para el desarrollo del contrato número 792 de 2022, no estoy enterado de situaciones indicativas de inobservancia en el cumplimiento de las obligaciones legales provenientes del sistema de seguridad social en salud y lo correspondiente a riesgos laborales, pensión, ICBF, SENA y cajas de compensación Familiar de conformidad con el artículo 50 de la Ley 789 de diciembre de 2002 modificada por el artículo 9 de la Ley 828 de 2003, el artículo. 32 de la Ley 1150 de 2007 y el artículo 24 del Decreto 2106 de 2019.

**ANTE SOLICITUD ESPECIAL, CONSIDERAR LAS SIGUIENTES ALTERNATIVAS:**

3. La sociedad se encuentra beneficiada por la exoneración de aportes establecida en el artículo 65 de la Ley 1819 de 2016, por lo tanto, no posee obligaciones de pagos por los parafiscales correspondientes al SENA y al ICBF, así como las cotizaciones al Régimen Contributivo de Salud, correspondientes a los trabajadores que devenguen, individualmente considerados, menos de diez (10) salarios mínimos mensuales legales vigentes.

La presente certificación se expide en Manizales a los ocho (08) días del mes de agosto de 2025, a solicitud de la administración de la compañía.

En cumplimiento con el artículo 2 de la ley 43 de 1990, mi firma como Revisor Fiscal en las Certificaciones se fundamenta en los libros de contabilidad. La información que no es de carácter contable fue verificada con las fuentes indicadas.



**KATHERINE MUÑOZ CARDONA**

Revisor Fiscal

Tarjeta Profesional No. **184969-T**

Designado por **CROWE CO S.A.S.**

## Planilla Integrada

### DATOS GENERALES DEL APORTANTE

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

### DATOS GENERALES DE LA LIQUIDACION

| Periodo |         | Clave      |            | Tipo     | Fecha      |            | Pago               |           |             |
|---------|---------|------------|------------|----------|------------|------------|--------------------|-----------|-------------|
| Pensión | Salud   | Pago       | Planilla   | Planilla | Limite     | Pago       | Banco              | Dias Mora | Valor       |
| 2025-07 | 2025-08 | 1683804909 | 9489990888 | E        | 2025/08/26 | 2025/08/06 | BANCO DE OCCIDENTE | 0         | \$4,758,100 |

### LIQUIDACION DETALLADA DE APORTES

| EMPLEADO                                         |         |          |                                 |                |                 |             |            |                                 |     |           |     |           |     |     |     |     |     | NOVEDADES        |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |     |  |  |  |
|--------------------------------------------------|---------|----------|---------------------------------|----------------|-----------------|-------------|------------|---------------------------------|-----|-----------|-----|-----------|-----|-----|-----|-----|-----|------------------|-----|-----|-----|------------------|---------------|-----|------------------|---------------|-----|------------------|---------------|--------|---------------------|------------------|------------|-----|--|--|--|
| No.                                              | Tipo id | No id    | Nombre                          | Tipo Cotizante | Horas Laboradas | Extran-jero | Temp. Ext. | Fecha Radicación en el Exterior | ing | Fecha ing | ret | Fecha ret | tde | tae | tdp | tap | vsp | Fecha Inicio vsp | cor | vst | sln | Fecha Inicio sln | Fecha Fin sln | ige | Fecha Inicio ige | Fecha Fin ige | lma | Fecha Inicio lma | Fecha Fin lma | vac-lr | Fecha Inicio vac-lr | Fecha Fin vac-lr | avp        | vct |  |  |  |
| Sucursal: BOGOTA (3 Afiliados)                   |         |          |                                 |                |                 |             |            |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |     |  |  |  |
| Centro de Trabajo: CENTRO TRABAJO 1(3 Afiliados) |         |          |                                 |                |                 |             |            |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |     |  |  |  |
| Ciudad: BOGOTA Depto: BOGOTA D.E.(3 Afiliados)   |         |          |                                 |                |                 |             |            |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |     |  |  |  |
| 1                                                | CC      | 52934365 | PARRA BUSTOS ANGIE PAOLA        | Dependiente    | 169             | No          | No         |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |     |  |  |  |
| 2                                                | CC      | 79468174 | PULIDO FAJARDO FRANCISCO JAVIER | Dependiente    | 220             | No          | No         |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |     |  |  |  |
| 3                                                | CC      | 63513251 | SUAREZ OSORIO MARIA VICTORIA    | Dependiente    | 213             | No          | No         |                                 |     |           |     |           |     |     |     |     |     |                  |     | X   |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |     |  |  |  |
| Centro de Trabajo: MENSAJERIA(2 Afiliados)       |         |          |                                 |                |                 |             |            |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |     |  |  |  |
| Ciudad: BOGOTA Depto: BOGOTA D.E.(2 Afiliados)   |         |          |                                 |                |                 |             |            |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |     |  |  |  |
| 4                                                | CC      | 52934365 | PARRA BUSTOS ANGIE PAOLA        | Dependiente    | 51              | No          | No         |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        | X                   | 2025/07/01       | 2025/07/07 |     |  |  |  |
| 5                                                | CC      | 63513251 | SUAREZ OSORIO MARIA VICTORIA    | Dependiente    | 7               | No          | No         |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        | L                   | 2025/07/01       | 2025/07/01 |     |  |  |  |
| Total Afiliados(3)                               |         |          |                                 |                |                 |             |            |                                 |     |           |     |           |     |     |     |     |     |                  |     |     |     |                  |               |     |                  |               |     |                  |               |        |                     |                  |            |     |  |  |  |

## Planilla Integrada

|                  |               |     |                  |               |     | SALARIO     |          |                 | PENSION        |      |             |        |                            |                  |                                 |                                |                             |                    |                   |       |             |                | SALUD |             |        |                  |           |  |
|------------------|---------------|-----|------------------|---------------|-----|-------------|----------|-----------------|----------------|------|-------------|--------|----------------------------|------------------|---------------------------------|--------------------------------|-----------------------------|--------------------|-------------------|-------|-------------|----------------|-------|-------------|--------|------------------|-----------|--|
| Fecha Inicio vct | Fecha Fin vct | irl | Fecha Inicio irl | Fecha Fin irl | vip | Valor       | Integral | Tipo de Salario | Administradora | Dias | IBC         | Tarifa | Tarifa Alto Riesgo Pensión | Valor Cotización | Cotización Voluntaria Empleador | Cotización Voluntaria Afiliado | Fondo Solidaridad Pensional | Fondo Subsistencia | Valor No retenido | Total | AFP Destino | Administradora | Dias  | IBC         | Tarifa | Valor Cotización | Valor UP  |  |
|                  |               |     |                  |               |     |             |          |                 |                |      |             |        |                            |                  |                                 |                                |                             |                    |                   |       | \$3,182,600 |                |       |             |        |                  | \$757,100 |  |
|                  |               |     |                  |               |     |             |          |                 |                |      |             |        |                            |                  |                                 |                                |                             |                    |                   |       | \$3,020,100 |                |       |             |        |                  | \$716,900 |  |
|                  |               |     |                  |               |     |             |          |                 |                |      |             |        |                            |                  |                                 |                                |                             |                    |                   |       | \$3,020,100 |                |       |             |        |                  | \$716,900 |  |
|                  |               |     |                  |               |     | \$3,470,000 | No       | Fijo            | PORVENIR       | 23   | \$2,660,334 | 16%    | SIN RIESGO                 | \$425,700        | \$0                             | \$0                            | \$0                         | \$0                | \$0               | \$0   | \$425,700   | SANITAS        | 23    | \$2,660,334 | 4%     | \$106,500        |           |  |
|                  |               |     |                  |               |     | \$9,470,000 | No       | Fijo            | COLPENSIONES   | 30   | \$9,470,000 | 16%    | SIN RIESGO                 | \$1,515,200      | \$0                             | \$0                            | \$47,400                    | \$47,400           | \$0               | \$0   | \$1,610,000 | SANITAS        | 30    | \$9,470,000 | 4%     | \$378,800        |           |  |
|                  |               |     |                  |               |     | \$5,790,000 | No       | Fijo            | COLPENSIONES   | 29   | \$5,790,000 | 16%    | SIN RIESGO                 | \$926,400        | \$0                             | \$0                            | \$29,000                    | \$29,000           | \$0               | \$0   | \$984,400   | NUEVA E. P. S. | 29    | \$5,790,000 | 4%     | \$231,600        |           |  |
|                  |               |     |                  |               |     |             |          |                 |                |      |             |        |                            |                  |                                 |                                |                             |                    |                   |       | \$162,500   |                |       |             |        |                  | \$40,200  |  |
|                  |               |     |                  |               |     |             |          |                 |                |      |             |        |                            |                  |                                 |                                |                             |                    |                   |       | \$162,500   |                |       |             |        |                  | \$40,200  |  |
|                  |               |     |                  |               |     | \$3,470,000 | No       | Fijo            | PORVENIR       | 7    | \$809,667   | 16%    | SIN RIESGO                 | \$129,600        | \$0                             | \$0                            | \$0                         | \$0                | \$0               | \$0   | \$129,600   | SANITAS        | 7     | \$809,667   | 4%     | \$32,400         |           |  |
|                  |               |     |                  |               |     | \$5,790,000 | No       | Fijo            | COLPENSIONES   | 1    | \$193,000   | 16%    | SIN RIESGO                 | \$30,900         | \$0                             | \$0                            | \$1,000                     | \$1,000            | \$0               | \$0   | \$32,900    | NUEVA E. P. S. | 1     | \$193,000   | 4%     | \$7,800          |           |  |
|                  |               |     |                  |               |     |             |          |                 |                |      |             |        |                            |                  |                                 |                                |                             |                    |                   |       | \$3,182,600 |                |       |             |        |                  | \$757,100 |  |

|     |           |             | CCF            |      |             |        | RIESGOS          |                              |      |             |        |              |                  |      | PARAFISCALES |             |                       |             |                       |             |                       |            |                      |                       |
|-----|-----------|-------------|----------------|------|-------------|--------|------------------|------------------------------|------|-------------|--------|--------------|------------------|------|--------------|-------------|-----------------------|-------------|-----------------------|-------------|-----------------------|------------|----------------------|-----------------------|
| C   | Total     | EPS Destino | Administradora | Días | IBC         | Tarifa | Valor Cotización | Administradora               | Días | IBC         | Tarifa | Clase Riesgo | Valor Cotización | Días | IBC          | Tarifa SENA | Valor Cotización SENA | Tarifa ICBF | Valor Cotización ICBF | Tarifa ESAP | Valor Cotización ESAP | Tarifa MEN | Valor Cotización MEN | Exonerado SENA e ICBF |
|     | \$757,100 |             |                |      |             |        | \$724,700        |                              |      |             |        |              | \$93,700         |      |              |             | \$0                   |             | \$0                   |             | \$0                   |            | \$0                  |                       |
|     | \$716,900 |             |                |      |             |        | \$716,900        |                              |      |             |        |              | \$93,700         |      |              |             | \$0                   |             | \$0                   |             | \$0                   |            | \$0                  |                       |
|     | \$716,900 |             |                |      |             |        | \$716,900        |                              |      |             |        |              | \$93,700         |      |              |             | \$0                   |             | \$0                   |             | \$0                   |            | \$0                  |                       |
| \$0 | \$106,500 |             | COMFACUNDI     | 23   | \$2,660,333 | 4%     | \$106,500        | POSITIVA COMPANIA DE SEGUROS | 23   | \$2,660,334 | 0.522% | 1            | \$13,900         | 23   | \$0          | 0%          | \$0                   | 0%          | \$0                   | 0%          | \$0                   | 0%         | \$0                  | \$1                   |
| \$0 | \$378,800 |             | COMFACUNDI     | 30   | \$9,470,000 | 4%     | \$378,800        | POSITIVA COMPANIA DE SEGUROS | 30   | \$9,470,000 | 0.522% | 1            | \$49,500         | 30   | \$0          | 0%          | \$0                   | 0%          | \$0                   | 0%          | \$0                   | 0%         | \$0                  | \$1                   |
| \$0 | \$231,600 |             | COMFACUNDI     | 29   | \$5,790,000 | 4%     | \$231,600        | POSITIVA COMPANIA DE SEGUROS | 29   | \$5,790,000 | 0.522% | 1            | \$30,300         | 29   | \$0          | 0%          | \$0                   | 0%          | \$0                   | 0%          | \$0                   | 0%         | \$0                  | \$1                   |
|     | \$40,200  |             |                |      |             |        | \$7,800          |                              |      |             |        |              | \$0              |      |              |             | \$0                   |             | \$0                   |             | \$0                   |            | \$0                  |                       |
|     | \$40,200  |             |                |      |             |        | \$7,800          |                              |      |             |        |              | \$0              |      |              |             | \$0                   |             | \$0                   |             | \$0                   |            | \$0                  |                       |
| \$0 | \$32,400  |             | COMFACUNDI     | 7    | \$0         | 0%     | \$0              | POSITIVA COMPANIA DE SEGUROS | 7    | \$809,667   | 0%     | 1            | \$0              | 7    | \$0          | 0%          | \$0                   | 0%          | \$0                   | 0%          | \$0                   | 0%         | \$0                  | \$1                   |
| \$0 | \$7,800   |             | COMFACUNDI     | 1    | \$193,000   | 4%     | \$7,800          | POSITIVA COMPANIA DE SEGUROS | 1    | \$193,000   | 0%     | 1            | \$0              | 1    | \$0          | 0%          | \$0                   | 0%          | \$0                   | 0%          | \$0                   | 0%         | \$0                  | \$1                   |
|     | \$757,100 |             |                |      |             |        | \$724,700        |                              |      |             |        |              | \$93,700         |      |              |             | \$0                   |             | \$0                   |             | \$0                   |            | \$0                  |                       |

## Planilla Integrada

| DATOS GENERALES DEL APORTANTE     |         |              |             |                             |            |                    |                           |                        |           |                       |
|-----------------------------------|---------|--------------|-------------|-----------------------------|------------|--------------------|---------------------------|------------------------|-----------|-----------------------|
| Identificación                    | dv      | Razon Social |             | Clase Aportante             |            | Sucursal Principal | Direccion                 | Ciudad-Departamento    | Teléfono  | Exonerado SENA e ICBF |
| NIT 900068796                     | 1       | INFOTIC S A  |             | B - MENOS DE 200 COTIZANTES |            | BOGOTA             | CL 93 B N° 13 - 44 PISO 2 | BOGOTA-BOGOTA D.E.     | 7466000   | Si                    |
| DATOS GENERALES DE LA LIQUIDACION |         |              |             |                             |            |                    |                           |                        |           |                       |
| Periodo                           |         | Clave        |             | Tipo                        | Fecha      |                    | Pago                      |                        |           |                       |
| Pensión                           | Salud   | Pago         | Planilla    | Planilla                    | Limite     | Pago               | Banco                     |                        | Días Mora | Valor                 |
| 2025-07                           | 2025-08 | 1683804909   | 9489990888  | E                           | 2025/08/26 | 2025/08/06         | BANCO DE OCCIDENTE        |                        | 0         | \$4,758,100           |
| RESUMEN DE PAGO                   |         |              |             |                             |            |                    |                           |                        |           |                       |
| RIESGO                            |         | CODIGO       | NIT         | DV                          | AFILIADOS  | VALOR LIQUIDADO    | INTERESES MORA            | SALDOS E INCAPACIDADES |           | VALOR A PAGAR         |
| AFP (ADMINISTRADORAS: 2)          |         |              |             |                             | 3          | \$3,182,600        | \$0                       | \$0                    |           | \$3,182,600           |
| COLPENSIONES                      |         | 25-14        | 900,336,004 | 7                           | 2          | \$2,627,300        | \$0                       | \$0                    |           | \$2,627,300           |
| PORVENIR                          |         | 230301       | 800,224,808 | 8                           | 1          | \$555,300          | \$0                       | \$0                    |           | \$555,300             |
| ARL (ADMINISTRADORAS: 1)          |         |              |             |                             | 3          | \$93,700           | \$0                       | \$0                    |           | \$93,700              |
| POSITIVA COMPAÑIA DE SEGUROS      |         | 14-23        | 860,011,153 | 6                           | 3          | \$93,700           | \$0                       | \$0                    |           | \$93,700              |
| CCF (ADMINISTRADORAS: 1)          |         |              |             |                             | 3          | \$724,700          | \$0                       | \$0                    |           | \$724,700             |
| COMFACUNDI                        |         | CCF26        | 860,045,904 | 7                           | 3          | \$724,700          | \$0                       | \$0                    |           | \$724,700             |
| EPS (ADMINISTRADORAS: 2)          |         |              |             |                             | 3          | \$757,100          | \$0                       | \$0                    |           | \$757,100             |
| NUEVA E.P.S.                      |         | EPS037       | 900,156,264 | 2                           | 1          | \$239,400          | \$0                       | \$0                    |           | \$239,400             |
| SANITAS                           |         | EPS005       | 800,251,440 | 6                           | 2          | \$517,700          | \$0                       | \$0                    |           | \$517,700             |
| TOTAL                             |         |              |             |                             | 3          | \$4,758,100        | \$0                       | \$0                    |           | \$4,758,100           |

**EL SUSCRITO REVISOR FISCAL DE INFOTIC S.A. CON NIT. 900.068.796-1,  
KATHERINE MUÑOZ CARDONA IDENTIFICADO CON CEDULA DE CIUDADANÍA  
No. 1.053.793.749 Y TARJETA PROFESIONAL 184969 –T EXPEDIDA  
POR LA JUNTA CENTRAL DE CONTADORES**

**CERTIFICA QUE**

1. A la fecha se encuentra en curso mi examen sobre los estados financieros de la Compañía por el año que terminará el 31 de diciembre de 2025.
2. El último pago se realizó el día cinco (05) de septiembre de 2025, para los aportes correspondientes a salud del mes de septiembre de 2025 y para pensión, riesgos laborales y aportes parafiscales del mes de agosto de 2025 mediante la planilla No. 9491469705, el último pago realizado para cancelar los aportes de sus trabajadores enviados en misión al Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior “Mariano Ospina Perez”–Icetex para el desarrollo del contrato número 792 de 2022, no estoy enterado de situaciones indicativas de inobservancia en el cumplimiento de las obligaciones legales provenientes del sistema de seguridad social en salud y lo correspondiente a riesgos laborales, pensión, ICBF, SENA y cajas de compensación Familiar de conformidad con el artículo 50 de la Ley 789 de diciembre de 2002 modificada por el artículo 9 de la Ley 828 de 2003, el artículo. 32 de la Ley 1150 de 2007 y el artículo 24 del Decreto 2106 de 2019.

**ANTE SOLICITUD ESPECIAL, CONSIDERAR LAS SIGUIENTES ALTERNATIVAS:**

3. La sociedad se encuentra beneficiada por la exoneración de aportes establecida en el artículo 65 de la Ley 1819 de 2016, por lo tanto, no posee obligaciones de pagos por los parafiscales correspondientes al SENA y al ICBF, así como las cotizaciones al Régimen Contributivo de Salud, correspondientes a los trabajadores que devenguen, individualmente considerados, menos de diez (10) salarios mínimos mensuales legales vigentes.

La presente certificación se expide en Manizales a los ocho (08) días del mes de septiembre de 2025, a solicitud de la administración de la compañía.

En cumplimiento con el artículo 2 de la ley 43 de 1990, mi firma como Revisor Fiscal en las Certificaciones se fundamenta en los libros de contabilidad. La información que no es de carácter contable fue verificada con las fuentes indicadas.



**KATHERINE MUÑOZ CARDONA**

Revisor Fiscal

Tarjeta Profesional No. **184969-T**

Designado por **CROWE CO S.A.S.**

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

| DATOS GENERALES DE LA LIQUIDACION |         |            |            |          |            |            |                    |           |             |
|-----------------------------------|---------|------------|------------|----------|------------|------------|--------------------|-----------|-------------|
| Periodo                           |         | Clave      |            | Tipo     | Fecha      |            | Pago               |           |             |
| Pensión                           | Salud   | Pago       | Planilla   | Planilla | Limite     | Pago       | Banco              | Dias Mora | Valor       |
| 2025-08                           | 2025-09 | 1755636923 | 9491469705 | E        | 2025/09/22 | 2025/09/05 | BANCO DE OCCIDENTE | 0         | \$4,746,000 |

| RESUMEN DE PAGO              |        |             |    |           |                 |                |                        |               |  |
|------------------------------|--------|-------------|----|-----------|-----------------|----------------|------------------------|---------------|--|
| RIESGO                       | CODIGO | NIT         | DV | AFILIADOS | VALOR LIQUIDADO | INTERESES MORA | SALDOS E INCAPACIDADES | VALOR A PAGAR |  |
| AFP (ADMINISTRADORAS: 2)     |        |             |    | 3         | \$3,149,600     | \$0            | \$0                    | \$3,149,600   |  |
| COLPENSIONES                 | 25-14  | 900,336,004 | 7  | 2         | \$2,594,400     | \$0            | \$0                    | \$2,594,400   |  |
| PORVENIR                     | 230301 | 800,224,808 | 8  | 1         | \$555,200       | \$0            | \$0                    | \$555,200     |  |
| ARL (ADMINISTRADORAS: 1)     |        |             |    | 3         | \$98,000        | \$0            | \$0                    | \$98,000      |  |
| POSITIVA COMPAÑIA DE SEGUROS | 14-23  | 860,011,153 | 6  | 3         | \$98,000        | \$0            | \$0                    | \$98,000      |  |
| CCF (ADMINISTRADORAS: 1)     |        |             |    | 3         | \$749,200       | \$0            | \$0                    | \$749,200     |  |
| COMFACUNDI                   | CCF26  | 860,045,904 | 7  | 3         | \$749,200       | \$0            | \$0                    | \$749,200     |  |
| EPS (ADMINISTRADORAS: 2)     |        |             |    | 3         | \$749,200       | \$0            | \$0                    | \$749,200     |  |
| NUEVA E.P.S.                 | EPS037 | 900,156,264 | 2  | 1         | \$231,600       | \$0            | \$0                    | \$231,600     |  |
| SANITAS                      | EPS005 | 800,251,440 | 6  | 2         | \$517,600       | \$0            | \$0                    | \$517,600     |  |
| TOTAL                        |        |             |    | 3         | \$4,746,000     | \$0            | \$0                    | \$4,746,000   |  |

REPUBLICA DE COLOMBIA  
IDENTIFICACION PERSONAL  
CEDULA DE CIUDADANIA

1.053.793.749

NUMERO

MUÑOZ CARDONA

APELLIDOS

KATHERINE

NOMBRES

Katherine Muñoz Cardona

FIRMA



INDICE DERECHO

FECHA DE NACIMIENTO  
MANIZALES  
(CALDAS)

25-MAR-1989

LUGAR DE NACIMIENTO

1.60

A+

F

ESTATURA

G.S. RH

SEXO

28-MAR-2007 MANIZALES

FECHA Y LUGAR DE EXPEDICION

REGISTRADOR NACIONAL  
JUAN CARLOS GALINDO VACHA



P-0900100-35159751-F-1053793749-20070610

0018107161C 02 239409704

UNIDAD  
ADMINISTRATIVA  
ESPECIAL

**JUNTA CENTRAL  
DE CONTADORES**



Certificado No:



**LA REPUBLICA DE COLOMBIA**

**MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO**

**UNIDAD ADMINISTRATIVA ESPECIAL**

**JUNTA CENTRAL DE CONTADORES**

**CERTIFICA A:  
QUIEN INTERESE**

Que el contador público **KATHERINE MUÑOZ CARDONA** identificado con CÉDULA DE CIUDADANÍA No 1053793749 de MANIZALES (CALDAS) Y Tarjeta Profesional No 184969-T SI tiene vigente su inscripción en la Junta Central de Contadores y desde los últimos 5 años.

**NO REGISTRA ANTECEDENTES DISCIPLINARIOS** \*\*\*\*\*  
\*\*\*\*\*  
\*\*\*\*\*

Dado en BOGOTA a los 9 días del mes de Julio de 2025 con vigencia de (3) Meses, contados a partir de la fecha de su expedición.

  
SANDRA MILENA BARRIOS PULIDO  
**DIRECTOR GENERAL**

ESTE CERTIFICADO DIGITAL TIENE PLENA VALIDEZ DE CONFORMIDAD CON LO ESTABLECIDO EN EL ARTICULO 2 DE LA LEY 527 DE 1999, DECRETO UNICO REGLAMENTARIO 1074 DE 2015 Y ARTICULO 6 PARAGRAFO 3 DE LA LEY 962 DEL 2005

Para confirmar los datos y veracidad de este certificado, lo puede consultar en la página web [www.jcc.gov.co](http://www.jcc.gov.co) digitando el número del certificado

República de Colombia  
Ministerio de Comercio, Industria y Turismo

UNIDAD ADMINISTRATIVA ESPECIAL **JUNTA CENTRAL DE CONTADORES**

**184969-T**

**KATHERINE MUÑOZ CARDONA**  
C.C. 1053793749  
RES. INSCRIPCION 848 DEL 23/12/2013  
UNIVERSIDAD DE MANIZALES



  
**JOSE ORLANDO RAMIREZ ZULUAGA**  
DIRECTOR GENERAL

**273465** **196340**

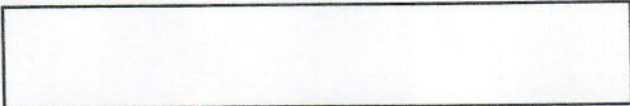
Identificación Plástica S.A. 180942/0119

República de Colombia  
Ministerio de Comercio, Industria y Turismo

UNIDAD ADMINISTRATIVA ESPECIAL **JUNTA CENTRAL DE CONTADORES**

Esta tarjeta es el único documento que lo acredita como Contador Público de acuerdo con lo establecido en la Ley 43 de 1990. Es personal e intransferible.

Agradecemos a quien encuentre esta tarjeta comunicarse al PBX: (57)(1) 644 4450 o devolverla a la UAE – Junta Central de Contadores a la Carrera 16 No. 97- 46 Of.301 en Bogotá D.C.



FIRMA



# **INFORME DE ACTIVIDADES DEL CONTRATO**

**CONTRATO NUMERO  
2022-0792**

**Julio 01 al 31 de 2025**

| versión | Observaciones   | Fecha      | Responsable             |
|---------|-----------------|------------|-------------------------|
| 1.0     | Versión Inicial | 01/08/2025 | Francisco Javier Pulido |

## Tabla de contenido

|                                                                          |           |
|--------------------------------------------------------------------------|-----------|
| <b>1. INTRODUCCIÓN.....</b>                                              | <b>9</b>  |
| <b>2. OBJETIVO DEL INFORME.....</b>                                      | <b>9</b>  |
| <b>3. ALCANCE.....</b>                                                   | <b>10</b> |
| <b>4. AVANCE TÉCNICO.....</b>                                            | <b>11</b> |
| <b>4.1. Conectividad y Red de Comunicaciones.....</b>                    | <b>11</b> |
| <b>4.1.1. Canales instalados en el mes y entregables .....</b>           | <b>13</b> |
| <b>4.1.1.1. Solicitudes Nuevas Instalación de canales .....</b>          | <b>14</b> |
| <b>4.1.2. Pruebas de Saturación Bidireccionales .....</b>                | <b>14</b> |
| <b>4.2. Centro de Datos .....</b>                                        | <b>14</b> |
| <b>4.2.1. Centro de Datos Principal.....</b>                             | <b>14</b> |
| 4.2.1.1. Aplicaciones .....                                              | 14        |
| 4.2.1.2. Bases de Datos .....                                            | 17        |
| <b>4.2.2. Centro de Datos Alterno.....</b>                               | <b>20</b> |
| 4.2.2.1. Hosting Virtual (IaaS) .....                                    | 20        |
| 4.2.2.2. Dataguard Bases de Datos Megacenter .....                       | 22        |
| 4.2.2.3. Servicios de Housing – Datacenter Alterno .....                 | 23        |
| 4.2.2.4. Servicios de DRP .....                                          | 23        |
| <b>4.3. Seguridad informática.....</b>                                   | <b>23</b> |
| <b>4.3.1.1. FortiGate Triara .....</b>                                   | <b>27</b> |
| <b>4.3.1.2. FortiGate Aguas.....</b>                                     | <b>30</b> |
| <b>4.3.1.3. FortiGate Medellín .....</b>                                 | <b>31</b> |
| <b>4.3.1.4. FortiWeb 2000F.....</b>                                      | <b>31</b> |
| <b>4.3.1.5. FortiWeb 2000E .....</b>                                     | <b>31</b> |
| <b>4.3.1.6. FortiSandBox .....</b>                                       | <b>32</b> |
| <b>4.3.1.7. FortiSIEM .....</b>                                          | <b>32</b> |
| <b>4.3.1.8. Sophos EndPoint .....</b>                                    | <b>33</b> |
| <b>4.3.2. Estadística de Portales .....</b>                              | <b>34</b> |
| <b>4.3.3. Servicio de centro de Operaciones de Seguridad (SOC) .....</b> | <b>35</b> |
| <b>4.3.3.1. Alertas o Incidentes de Seguridad Detectados.....</b>        | <b>37</b> |

|                                                                       |           |
|-----------------------------------------------------------------------|-----------|
| <b>4.3.3.1.1. Categoría Seguridad.....</b>                            | <b>37</b> |
| <b>4.3.3.1.2. Categoría Disponibilidad .....</b>                      | <b>39</b> |
| <b>4.3.3.1.3. Amenazas de Ciberseguridad.....</b>                     | <b>40</b> |
| <b>4.3.3.1.4. Threat Hunting.....</b>                                 | <b>43</b> |
| <b>4.3.4. Análisis de Vulnerabilidades ICETEX.....</b>                | <b>43</b> |
| 4.3.4.1. Resumen de Vulnerabilidades .....                            | 44        |
| 4.3.4.2. Conclusiones Vulnerabilidades .....                          | 45        |
| <b>4.3.5. Reporte De Ips .....</b>                                    | <b>46</b> |
| <b>4.4. Servicios de nube .....</b>                                   | <b>46</b> |
| <b>5. GESTION DE LA EJECUCIÓN CONTRACTUAL .....</b>                   | <b>47</b> |
| <b>6. GESTION PRESUPUESTAL .....</b>                                  | <b>47</b> |
| <b>7. GESTION ADMINISTRATIVA .....</b>                                | <b>48</b> |
| <b>7.1. Profesionales.....</b>                                        | <b>48</b> |
| <b>8. SERVICIO DE COLABORACIÓN .....</b>                              | <b>49</b> |
| <b>9. INDICADORES CLAVE DE DESEMPEÑO.....</b>                         | <b>51</b> |
| <b>9.1. ANS por Disponibilidad de canales de comunicaciones:.....</b> | <b>51</b> |
| 9.1.1. Canal de Replicación (Triara – Megacenter) .....               | 54        |
| <b>9.2. ANS por Disponibilidad de servidores: .....</b>               | <b>54</b> |
| 9.2.1. Disponibilidad TRIARA para los servicios de página web.....    | 56        |
| 9.2.2. Análisis componente Liferay Producción.....                    | 61        |
| 9.2.3. Backup Servidores Triara .....                                 | 61        |
| <b>10. CONTROL DE CAMBIOS.....</b>                                    | <b>63</b> |
| <b>11. PLAN DE TRABAJO DE LOS PROXIMOS MESES .....</b>                | <b>63</b> |
| <b>12. RECOMENDACIONES DEL CONTRATISTA AL ICETEX .....</b>            | <b>64</b> |
| 12.1. Licenciamiento De Software.....                                 | 64        |
| 12.2. Networking .....                                                | 65        |
| 12.3. Aplicaciones .....                                              | 65        |
| 12.4. Seguridad.....                                                  | 66        |
| 12.5. Bases De Datos.....                                             | 67        |
| 12.6. Integrador De Nube .....                                        | 67        |

|                                                                                                    |           |
|----------------------------------------------------------------------------------------------------|-----------|
| <b>13. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC.....</b>                                 | <b>68</b> |
| <b>13.1. Aumento de la capacidad de Ancho de Banda en algunas de las sedes de la Entidad .....</b> | <b>68</b> |
| <b>13.2. Una capacitación al año de seguridad Informática y servicios conexos.....</b>             | <b>68</b> |
| <b>13.3. TB de capacidad de almacenamiento .....</b>                                               | <b>68</b> |
| <b>13.4. Se oferta Ítem de “Wifi” para la gente en 19 sedes .....</b>                              | <b>69</b> |
| <b>14. CONCLUSIONES.....</b>                                                                       | <b>69</b> |
| <b>15. ANEXOS .....</b>                                                                            | <b>70</b> |

|                                                                                               |    |
|-----------------------------------------------------------------------------------------------|----|
| TABLA 1 ESTADO NUEVAS SOLICITUDES CANALES .....                                               | 11 |
| TABLA 2 NORMALIZACIÓN DE DIRECCIONES. ....                                                    | 13 |
| TABLA 3 CASOS ATENDIDOS NETWORKING COMPARATIVO MES ANTERIOR .....                             | 14 |
| TABLA 4 INVENTARIO PRINCIPALES SERVIDORES PRODUCCIÓN .....                                    | 16 |
| TABLA 5 ESTADO BD ORACLE .....                                                                | 17 |
| TABLA 6 CRECIMIENTO DE LAS BASES DE DATOS EN LOS ÚLTIMOS 7 MESES .....                        | 19 |
| TABLA 7 SERVICIOS REPLICADOS – DATACENTER MEGACENTER .....                                    | 21 |
| TABLA 8 TOP 5 MÁQUINAS MAYOR TASA DE TRANSFERENCIA .....                                      | 21 |
| TABLA 9 TOP 5 MÁQUINAS MENOR TASA DE TRANSFERENCIA.....                                       | 21 |
| TABLA 10 DISPONIBILIDAD DE SERVICIOS DE HOUSING – DATA CENTER ALTERNO .....                   | 23 |
| TABLA 11 DETALLE PLATAFORMAS SEGURIDAD ADMINISTRADAS INFOTIC .....                            | 27 |
| TABLA 12 LICENCIAMIENTO FORTIGATE .....                                                       | 27 |
| TABLA 13 LICENCIAMIENTO FORTIWEB .....                                                        | 31 |
| TABLA 14 CONFIGURACIÓN FORTISANDBOX 1000D.....                                                | 32 |
| TABLA 15 TOP 10 PORTALES MÁS UTILIZADOS.....                                                  | 35 |
| TABLA 16 COMPARATIVO – INDICADORES DE COMPROMISO .....                                        | 36 |
| TABLA 17 COMPARATIVO ALERTAS DE SEGURIDAD .....                                               | 38 |
| TABLA 18 EJECUCIÓN PRESUPUESTAL.....                                                          | 48 |
| TABLA 19 PERFILES Y ACTIVIDADES.....                                                          | 48 |
| TABLA 20 GRUPO ADMINISTRATIVO .....                                                           | 49 |
| TABLA 21 DISTRIBUCIÓN MÓDULOS DE VIDEOCONFERENCIA POR SEDE .....                              | 49 |
| TABLA 22 NIVEL DE RIESGO .....                                                                | 51 |
| TABLA 23 GRADO DE RIESGO .....                                                                | 51 |
| TABLA 24 DISPONIBILIDAD DE CANALES.....                                                       | 53 |
| TABLA 25 DISPONIBILIDAD CANALES “INTERNET PARA LA GENTE” .....                                | 54 |
| TABLA 26 CÓDIGOS RELACIONADOS DISPONIBILIDAD SERVICIOS EN HOUSING – DATACENTER PRINCIPAL..... | 55 |
| TABLA 27 DISPOSITIVOS EN HOUSING – DATACENTER PRINCIPAL.....                                  | 56 |
| TABLA 28 DISTRIBUCIÓN TRIMESTRAL DE ACCESO POR USUARIOS .....                                 | 56 |
| TABLA 29 CONTROLES DE CAMBIO JULIO .....                                                      | 63 |
| TABLA 30 PLANES DE TRABAJO .....                                                              | 63 |
| TABLA 31 CAPACIDADES DE ALMACENAMIENTO CONTRATADO .....                                       | 67 |
| TABLA 32 CAPACIDADES DE ALMACENAMIENTO APROVISIONADO .....                                    | 68 |
| TABLA 33 WIFI PARA LA GENTE INSTALADOS .....                                                  | 69 |
| TABLA 34 WIFI PARA LA GENTE PENDIENTES.....                                                   | 69 |
| TABLA 35 ANEXOS .....                                                                         | 70 |

|                                                                                                                       |      |
|-----------------------------------------------------------------------------------------------------------------------|------|
| ILUSTRACIÓN 1 DISPONIBILIDAD DEL CLUSTER .....                                                                        | 18   |
| ILUSTRACIÓN 2 DISPONIBILIDAD DE LAS BASES DE DATOS PRINCIPALES ICTXCYC Y APOTEOSYS .....                              | 18   |
| ILUSTRACIÓN 3 CASOS DEL PROYECTO GESTIONADOS ARANDA BASES DE DATOS .....                                              | 19   |
| ILUSTRACIÓN 4 REPORTES DE REPLICACIÓN SRM A SITIO ALTERNO – JULIO 2025.....                                           | 20   |
| ILUSTRACIÓN 5 FECHAS CON MAYOR REPLICACIÓN .....                                                                      | 22   |
| ILUSTRACIÓN 6 EVIDENCIA DATAGUARD REPLICADO A MEGACENTER BD.....                                                      | 23   |
| ILUSTRACIÓN 7 DIAGRAMA DE LA ARQUITECTURA DE SEGURIDAD .....                                                          | 24   |
| ILUSTRACIÓN 8 TOPOLOGÍA DE WAF CLOUD USADO EN PORTALES DE MEDELLÍN .....                                              | 24   |
| ILUSTRACIÓN 9 CONSUMO CANAL MPLS - PROMEDIO 1200G [INR0185 CLARO(MPLS_DC)] .....                                      | 28   |
| ILUSTRACIÓN 10 CONSUMO CANAL INTERNET SEDES - PROMEDIO 1100 GB WAN-SEDES-ICETEX [INR0264<br>(INTE_SEDES_ICTX)] .....  | 28   |
| ILUSTRACIÓN 11 CONSUMO CANAL INTERNET DATA CENTER- INTERNET DATACENTER [INTERNET_DC_INR0000320<br>(INET_CLARO)] ..... | 28   |
| ILUSTRACIÓN 12 FILTRADO – WEB – (FORTIGATE – TRIARA).....                                                             | 29   |
| ILUSTRACIÓN 13 INSPECCIÓN – SSL – (FORTIGATE – TRIARA).....                                                           | 29   |
| ILUSTRACIÓN 14 ANTIVIRUS Y ANTIMALWARE – PERIMETRAL (FORTIGATE – TRIARA).....                                         | 29   |
| ILUSTRACIÓN 15 CONSUMO CANAL MPLS AGUAS - PROMEDIO 800 GB .....                                                       | 30   |
| ILUSTRACIÓN 16 FILTRADO-WEB-(FORTIGATE-AGUAS).....                                                                    | 30   |
| ILUSTRACIÓN 17 INSPECCIÓN-SSL-(FORTIGATE-AGUAS) .....                                                                 | 30   |
| ILUSTRACIÓN 18 ANTIVIRUS Y ANTIMALWARE-PERIMETRAL-(FORTIGATE-AGUAS).....                                              | 31   |
| ILUSTRACIÓN 19 CONSUMO CANAL MPLS MEDELLÍN .....                                                                      | 31   |
| ILUSTRACIÓN 20 TRÁFICO GENERAL DE LOS PORTALES .....                                                                  | 32   |
| ILUSTRACIÓN 21 VERSIÓN ACTUAL FORTISIEM .....                                                                         | 32   |
| ILUSTRACIÓN 22 LICENCIAMIENTO FORTISIEM .....                                                                         | 33   |
| ILUSTRACIÓN 23 ESTADO SEGURIDAD SOPHOS .....                                                                          | 33   |
| ILUSTRACIÓN 24 UPTIME: PORTAL WEB WEB.ICETEX.GOV.CO [99,802%] .....                                                   | 34   |
| ILUSTRACIÓN 25 TRÁFICO GENERAL DE LOS PORTALES .....                                                                  | 35   |
| ILUSTRACIÓN 26 TOTAL DE ALERTAS DE SEGURIDAD.....                                                                     | 37   |
| ILUSTRACIÓN 27 TOP 5 DE ALERTAS DE SEGURIDAD ALTAS.....                                                               | 38   |
| ILUSTRACIÓN 28 TOP 5 DE ALERTAS DE DISPONIBILIDAD ALTAS .....                                                         | 39   |
| ILUSTRACIÓN 29 ATAQUES IPS PERMITIDOS .....                                                                           | 40   |
| ILUSTRACIÓN 30 ATAQUES IPS DENEGADOS .....                                                                            | 40   |
| ILUSTRACIÓN 31 PUERTOS ENTRANTES DE PÚBLICO A PRIVADO (PERMITIDOS) .....                                              | 41   |
| ILUSTRACIÓN 32 PUERTOS SALIENTE DE PÚBLICO A PRIVADO (PERMITIDOS).....                                                | 41   |
| ILUSTRACIÓN 33 FALLOS DE INICIO DE SESIÓN WINDOWS.....                                                                | 42   |
| ILUSTRACIÓN 34 FALLOS DE INICIO DE SESIÓN UNIX .....                                                                  | 42   |
| ILUSTRACIÓN 35 FALLOS DE INICIO DE SESIÓN VPN.....                                                                    | 42   |
| ILUSTRACIÓN 36 CUENTAS BLOQUEADOS .....                                                                               | 43   |
| ILUSTRACIÓN 37 CANTIDAD TOTAL DE HALLAZGOS IDENTIFICADOS .....                                                        | 44   |
| ILUSTRACIÓN 38 VULNERABILIDADES CRITICAS .....                                                                        | 45   |
| ILUSTRACIÓN 39 MATRIZ DE RIESGOS .....                                                                                | 500  |
| ILUSTRACIÓN 40 UPTIME – PORTAL WEB WEB.ICETEX.GOV.CO .....                                                            | 56   |
| ILUSTRACIÓN 41 MÉTRICA DE VISITANTES PORTAL WEB WEB.ICETEX.GOV.CO .....                                               | 57   |
| ILUSTRACIÓN 42 MÉTRICA ADQUISICIÓN USUARIOS PORTAL WEB WEB.ICETEX.GOV.CO .....                                        | 57   |
| ILUSTRACIÓN 43 MÉTRICA DE USUARIO POR PAÍS - PORTAL WEB WEB.ICETEX.GOV.CO.....                                        | 58   |
| ILUSTRACIÓN 44 MÉTRICA DE CIUDADES DE COLOMBIA- PORTAL WEB WEB.ICETEX.GOV.CO.....                                     | 58   |
| ILUSTRACIÓN 45 NODO 1 CPU .....                                                                                       | 5959 |
| ILUSTRACIÓN 46 NODO 1 MEMORIA .....                                                                                   | 60   |

|                                                                                                        |      |
|--------------------------------------------------------------------------------------------------------|------|
| ILUSTRACIÓN 47 NODO 1 ALMACENAMIENTO.....                                                              | 61   |
| ILUSTRACIÓN 48 EVIDENCIA BACKUP SERVIDORES RESUMEN GENERAL BACKUPS.....                                | 62   |
| ILUSTRACIÓN 49 EVIDENCIA BACKUP SERVIDORES RESUMEN BACKUPS Y SU ESTADO .....                           | 6263 |
| ILUSTRACIÓN 50 CONSOLIDADO DEL USO DEL ALMACENAMIENTO EN LOS DISCOS DEL SERVIDOR ICTXSRVNETCOR01 ..... | 6666 |

## 1. INTRODUCCIÓN

Este informe contiene la información relacionada con las actividades ejecutadas por INFOTIC con ocasión de la celebración del contrato 2022-0792, durante el periodo comprendido entre el 01 al 31 de julio de 2025. Para tal fin se cuenta con la información generada por el grupo de 10 especialistas y 3 profesionales administrativos con los cuales se soportan y garantizan la atención de servicios especializados descritos en el alcance del proyecto como son:

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

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

- Firma del Acta de Inicio suscrita el 30 de diciembre del 2022, con fecha de iniciación del 19 de enero del 2023. Cumplida al 100%.
- Fase de Transición. Que comprendió desde el 19 de enero hasta el 31 de marzo de 2023. Esta fase se encuentra cumplida al 100%.
- Fase de operación. Inició desde el 1 de abril de 2023, cuenta con un avance en la ejecución del 77.7 % que representa los 28 meses que lleva dentro de la fase de Operación el proyecto.

El presente informe, correspondiente al mes de julio del 2025, describe los servicios realizados durante el periodo por el equipo de profesionales y las herramientas tecnológicas asignadas y dispuestas por INFOTIC para desempeñar las funciones y atender los requerimientos del ICETEX según lo establecido en el contrato.

## 2. OBJETIVO DEL INFORME

Presentar las actividades ejecutadas por INFOTIC durante el periodo del 01 al 31 de julio de 2025, con el fin de determinar el estado, la gestión, evolución y la disponibilidad de los servicios especializados prestados al ICETEX en virtud de la ejecución del contrato, para lo cual se han considerado la recolección de mediciones desde las herramientas de monitoreo, el análisis y la producción de informes y reportes periódicos sobre cada una de las gestiones y demás informes especiales sobre los servicios prestados.

El presente informe comprende:

- **Administración de Seguridad, Redes y Telecomunicaciones:**  
Descripción de las acciones ejecutadas en la gestión de redes y telecomunicaciones, con énfasis en la estabilidad, disponibilidad y optimización de la infraestructura.  
Reporte de incidentes de seguridad, su impacto y las medidas correctivas implementadas.
- **Conectividad y Red de comunicaciones:**  
Estado de las redes LAN/WAN, su desempeño y disponibilidad.  
Indicadores de tráfico, calidad de servicio (QoS) y balanceo de cargas.

- **Centro de Datos:**  
Estado de operación de los centros de datos, incluyendo disponibilidad, desempeño de servidores, almacenamiento y virtualización.  
Acciones de mantenimiento preventivo y correctivo realizadas.
- **Seguridad Informática:**  
Medidas implementadas para proteger la información y la infraestructura, como monitoreo, control de acceso, actualizaciones y parches de seguridad.
- **Servicios de Nube:**  
Reporte de uso de servicios en la nube, desempeño y cumplimiento de niveles de servicio (SLA).  
Descripción de servicios implementados o integrados en el entorno 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. ALCANCE

El alcance comprende la descripción de las actividades de los servicios especializados durante el periodo del 01 al 31 de julio de 2025 conforme a los frentes definidos por el ICETEX, así:

- **Conectividad y red de comunicaciones**  
Este informe presenta el estado del servicio que comprende los componentes exigidos de la arquitectura de conectividad, comunicaciones, software, hardware y dispositivos de seguridad informática, mínimos necesarios para la operación de los servicios establecidos en el contrato 2022-0792.
- **Centro de datos**  
El informe presenta el estado de los dos (2) Centros de Datos que contempla el proyecto ICETEX: un (01) centro de cómputo principal (TRIARA) y un (01) centro de cómputo secundario o alerno (MEGACENTER), en los cuales se debe garantizar la disponibilidad de los servicios alojados allí, cumpliendo las condiciones mínimas tales como temperatura, seguridad, cableado estructurado, path-cord para conexión de servidores y demás appliance de la operación, así como unidades de racks (gabinetes exclusivos para ICETEX) requeridas, conexiones eléctricas, entre otras.
- **Seguridad informática**  
El presente informe describe las actividades del periodo que se realizaron con el fin de proveer el servicio de seguridad informática a nivel de administración y gestión para los equipos de seguridad de propiedad del ICETEX, para los servicios on-premise y para la implementación de controles de seguridad especificados por el modelo de seguridad digital de la Entidad, conforme a los lineamientos legales u otros a fin de fortalecer la seguridad informática de la Entidad.  
  
Este servicio de administración y gestión debe incluir, pero sin limitarse a ello la implementación - instalación de configuraciones, actualizaciones de software, análisis de dispositivos de red, análisis de procesos, procedimientos, actividades, método y reglas a fin de proteger la infraestructura que soporta la información del ICETEX contra riesgos que afecten su integridad, disponibilidad y confidencialidad.
- **Servicios de nube**  
El informe presenta el estado y detalle de los Servicios de Data Center Principal y Alterno los cuales se

encuentra bajo la modalidad de Housing y todos los servicios requeridos para nube privada, dejando claro que a través del contrato se busca integrar servicios de nube pública e híbrida. A la fecha todos los recursos actuales se están usando sin sobre dimensionamientos.

➤ **Servicios conexos**

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

## 4. AVANCE TÉCNICO

### 4.1. Conectividad y Red de Comunicaciones

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

Durante el presente periodo y a fin de destacar se atendieron un total de 15 solicitudes, con respecto al mes anterior hubo un decremento de 8 casos ya que se atendieron 23 solicitudes en el mes anterior. Se pueden constatar las evidencias de las atenciones efectuadas en el siguiente enlace: [casos aranda por mes](#)

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

En cuanto a la gestión de vulnerabilidades, todas las detectadas en el último escaneo han sido corregidas. Estamos a la espera de los resultados de un nuevo escaneo para atender cualquier vulnerabilidad adicional que se identifique. Respecto a la implementación de IPv6, se ha trabajado con los especialistas de seguridad en las pruebas correspondientes. Asimismo, se ha avanzado en la documentación y entrega de informes conforme a los lineamientos periódicos de ICETEX.

Referente a las solicitudes efectuadas por parte del ICETEX y canales que se encuentran pendientes se relacionan los pendientes:

| Sede           | Observación                                       |
|----------------|---------------------------------------------------|
| Puerto Carreño | A la espera de la definición por parte del ICETEX |
| Puerto Inírida | A la espera de la definición por parte del ICETEX |

*Tabla 1 Estado nuevas solicitudes canales*

Atendiendo la solicitud, efectuada por el ICETEX con relación a la instalación de los canales de puerto Inírida y puerto Carreño, se informó que el servicio está previsto entregarlo a través de una red MPLS que funciona con última milla satelital dedicado del proveedor satelital, por lo tanto, tiene la facilidad de tener SLA definidos, conexión a la red MPLS de Claro por la interconexión y configuración estándar. Sin embargo los costos de esta configuración deben ser validados por el ICETEX por cuanto los montos aprobados corresponden a la alternativa de entregar el servicio de MPLS por medio de los internet de Starlink, lo que implica adicionar equipos en el extremo destino (firewall fg40f) que puedan levantar algún túnel y así garantizar conectividad punta a punta hacia el origen, esto implicaría también intervención del firewall en el punto central y pruebas en conjunto, lo que nos llevan a que ya no sea una solución estándar, tampoco se asegurarían SLA ni BW dedicado y la navegación está sujeta al paquete de datos del plan.

En cuanto a la instalación del canal Backup de Quibdó se determinó que no se procederá a la instalación.

Resultado de las sesiones de conciliación del mes anterior, se determinó que el ICETEX no iba a pagar el Canal de Backup del Internet de Triara-800Mbps ni el canal de Backup del Internet de Megacenter-800Mbps por no encontrarse en la línea base del contrato, razón por la cual se procederá al retiro de los mismos.

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

La gestión de dispositivos de red es el proceso mediante el cual se gestionan y controlan los dispositivos de red, desde computadoras, servidores y teléfonos móviles hasta conmutadores y máquinas virtuales.

Esto incluye la implementación, la operación y el mantenimiento de todos los dispositivos físicos y virtuales que conforman la infraestructura de red. Actualmente los equipos de red están en buen estado, pero se encuentran en EOL and EOS (End-of-Sale and End-of-Life) esto quiere decir que los equipos ya no cuentan con garantía por parte del fabricante y tampoco son vendidos por los mismos se recomienda al Icetex adquirir equipos nuevos ya que la infraestructura actual cuenta con más de 15 años de antigüedad.

[https://icetex.sharepoint.com/:x:/r/sites/Infraestructura/\\_layouts/15/Doc.aspx?sourcedoc=%7BD8EB1425-7A43-4FA2-8B11-38665423B9B3%7D&file=inventario%20de%20equipos.xlsx&action=default&mobileredirect=true](https://icetex.sharepoint.com/:x:/r/sites/Infraestructura/_layouts/15/Doc.aspx?sourcedoc=%7BD8EB1425-7A43-4FA2-8B11-38665423B9B3%7D&file=inventario%20de%20equipos.xlsx&action=default&mobileredirect=true)

La topología actualizada, a la fecha, se encuentra en el siguiente enlace:

<https://icetex.sharepoint.com/sites/Infraestructura/Documentos%20compartidos/Forms/AllItems.aspx?id=%2Fsites%2FInfraestructura%2FDocumentos%20compartidos%2FTOPOLOGIAS%20DE%20AGUAS&viewid=2cd2befc%2D9f50%2D42c3%2Db53a%2D74e0122a42e3>

Con el fin de garantizar conectividad con el protocolo IPV6, hemos adelantado un plan de trabajo, cuyo estado a la fecha se presenta a continuación:

| SEDE             | Segmento IPv4  | Segmento IPv6      |
|------------------|----------------|--------------------|
| Aguas            | 10.255.0.0/24  | 2801:192:6:E0::/64 |
| Chapinero Bogotá | 10.255.1.0/24  | 2801:192:6:E1::/64 |
| Ángel Bogotá     | 10.255.2.0/24  | 2801:192:6:E2::/64 |
| Cali             | 10.255.3.0/24  | 2801:192:6:E3::/64 |
| Medellín         | 10.255.4.0/24  | 2801:192:6:E4::/64 |
| Buenaventura     | 10.255.5.0/24  | 2801:192:6:E5::/64 |
| Quibdó           | 10.255.6.0/24  | 2801:192:6:E6::/64 |
| Riohacha         | 10.255.7.0/24  | 2801:192:6:E7::/64 |
| Montería         | 10.255.8.0/24  | 2801:192:6:E8::/64 |
| Pereira          | 10.255.9.0/24  | 2801:192:6:E9::/64 |
| Bucaramanga      | 10.255.10.0/24 | 2801:192:6:EA::/64 |
| Popayán          | 10.255.11.0/24 | 2801:192:6:EB::/64 |
| Valledupar       | 10.255.12.0/24 | 2801:192:6:EC::/64 |
| Santa Marta      | 10.255.13.0/24 | 2801:192:6:ED::/64 |
| Barranquilla     | 10.255.14.0/24 | 2801:192:6:EE::/64 |
| Sincelejo        | 10.255.15.0/24 | 2801:192:6:EF::/64 |
| Tumaco           | 10.255.16.0/24 | 2801:192:6:F0::/64 |
| Cúcuta           | 10.255.17.0/24 | 2801:192:6:F1::/64 |

| SEDE          | Segmento IPv4  | Segmento IPv6      |
|---------------|----------------|--------------------|
| Villavicencio | 10.255.18.0/24 | 2801:192:6:F2::/64 |
| Tunja         | 10.255.19.0/24 | 2801:192:6:F3::/64 |
| Cartagena     | 10.255.20.0/24 | 2801:192:6:F4::/64 |
| San Andrés    | 10.255.21.0/24 | 2801:192:6:F5::/64 |
| Armenia       | 10.255.22.0/24 | 2801:192:6:F6::/64 |
| Arauca        | 10.255.23.0/24 | 2801:192:6:F7::/64 |
| Pasto         | 10.255.24.0/24 | 2801:192:6:F8::/64 |
| Ibagué        | 10.255.25.0/24 | 2801:192:6:F9::/64 |
| Apartado      | 10.255.26.0/24 | 2801:192:6:FA::/64 |
| Mocoa         | 10.255.27.0/24 | 2801:192:6:FB::/64 |
| Yopal         | 10.255.28.0/24 | 2801:192:6:FC::/64 |
| Manizales     | 10.255.29.0/24 | 2801:192:6:FD::/64 |
| Neiva         | 10.255.30.0/24 | 2801:192:6:FE::/64 |
| Angel         | 10.255.31.0/24 |                    |
| Leticia       | 10.255.32.0/24 | 2801:192:6:FF::/64 |

*Tabla 2 Normalización de direcciones.*

A fin de garantizar un adecuado funcionamiento, se ha previsto que el equipo de especialistas de seguridad procederá a configurar reglas de seguridad, en los firewalls, para las direcciones IPV6, empleando como guía las que se encuentran productivas a la fecha con direccionamiento IPV4. El plan de trabajo previsto puede ser consultado en el informe de nuestro especialista de networking.

En lo concerniente a las pruebas de los aplicativos del ICETEX, se adelantaron pruebas de acceso a las aplicaciones web de la entidad utilizando NAT64, dado que el portal web.icetex.gov.co, que incluye aplicaciones web no compatibles con IPv6, requiere este tipo de traducción de direcciones para asegurar el acceso. Este proceso de conversión de IPv6 a IPv4 es gestionado por el firewall de Triara, permitiendo así la comunicación con el WAF y las aplicaciones web en el servidor.

#### 4.1.1. Canales instalados en el mes y entregables

Durante el periodo de reporte no se han adelantado instalación de canales tanto principales como de backup.

**Canales Principales.** A la fecha, se ha instalado un total de 40 de los 43 canales MPLS principales previstos en la línea base. De los tres canales restantes, uno corresponde al canal entre el Sitio principal e ICETEX - Dirección General – Aguas, cuya instalación fue descartada por ICETEX. Los otros dos canales faltantes están relacionados con sedes donde ICETEX aún no dispone de oficinas, específicamente en Barrancabermeja y San Gil.

En resumen, hasta la fecha se ha completado la instalación del 100% de los canales principales de comunicación en las sedes especificadas en la línea base del contrato.

**Canales de Backup.** De los 32 canales de Backups previstos en la línea base, se han instalado 30, lo que representa un avance del 96,55%. Actualmente, queda pendiente la instalación del canal de Backup para la oficina en Quibdó, así como un canal entre el sitio principal e ICETEX - Dirección General - Aguas, cuya instalación ya fue descartada por ICETEX.

**Canales de internet para la gente.** El servicio de "internet para la gente" ha sido implementado en las 14

sedes solicitadas según el anexo técnico, logrando así un cumplimiento del 100% de lo previsto.

**Anchos de banda.** Los canales instalados cuentan con el 100% del ancho de banda contratado. Se lleva a cabo un monitoreo mensual de la disponibilidad de estos canales mediante la herramienta SolarWinds, generando un informe correspondiente que está disponible en el siguiente enlace: [Reporte Mensual Disponibilidad INFOTIC Julio 2025.pdf](#)

#### 4.1.1.1. Solicitudes Nuevas Instalación de canales

En el periodo no se han recibido solicitud de instalación de nuevos canales. Los casos atendidos durante el mes están disponibles en el siguiente enlace:

[Registro Aranda julio 2025.xlsx](#)

Todos los casos fueron gestionados exclusivamente a través de la herramienta Aranda, sin que se registrara atención por otros medios.

| Mes   | No. Casos |
|-------|-----------|
| Mayo  | 42        |
| Junio | 23        |
| Julio | 15        |

*Tabla 3 Casos atendidos Networking comparativo mes anterior*

#### 4.1.2. Pruebas de Saturación Bidireccionales

A la fecha no hay pruebas de saturación que se encuentren pendientes.

### 4.2. Centro de Datos

#### 4.2.1. Centro de Datos Principal

##### 4.2.1.1. Aplicaciones

Durante el mes de julio de 2025, se gestionaron y resolvieron un total de 16 actividades, clasificadas tareas de cambio e incidentes, todas documentadas con sus respectivas evidencias. A continuación, se presenta el detalle de estas:

##### Gestión de accesos y conectividad:

- Se otorgaron permisos de conexión a múltiples servidores de pruebas ubicados en las IPs 10.1.18.65, 10.1.18.124 y 10.1.18.29.
- Se resolvieron incidencias relacionadas con el acceso FTP y errores de conexión a servidores.

##### Actualización y despliegue de aplicaciones:

- Se realizaron cambios en componentes como Front WsDesembolsos, MEAC, TransunionAPI, y ApiMaestroPersonaRnec.
- Se actualizó y reemplazó el archivo condiciones2021.asp en los servidores C&CTEX y MIRA, asegurando la disponibilidad de información normativa vigente.

##### Atención a incidentes críticos:

- Se solucionó una falla en la conexión a base de datos de la aplicación Servinpro, mitigando el impacto

sobre la operación de esta solución.

Con el fin de garantizar el funcionamiento de las soluciones de manera eficiente y segura, se han revisado el estado de actualización de los parches de los sistemas operativos, y durante el mes se presentaron dos controles de cambio, el 1158 y el 1159 con el fin de proceder a efectuar las actualizaciones respectivas.

En cuanto al desempeño de los servidores, reiteramos nuestra preocupación sobre el servidor ICTXSRNSTCOR01 en donde se aloja la aplicación (es) CargueArchivos, ConciliacionesIES, Condonaciones, TransunionAPI, VotoElectronico, WebServiceServicioPasarelaKushki, WebSiteCondonacion, WebSitePortalTransaccional, WebsitePSE, WsApiSolicitudes, WsConciliacionesIES, WsCuentasAbandonaadasAPI, WsDynamics, WsPasarela y WsPortalTransaccional presenta, en su unidad F, un espacio de uso cercano al 90% generando un riesgo para el adecuado funcionamiento de la misma, por lo cual se recomienda al ICETEX revisar las políticas de respaldo sobre esa información, si se están ejecutando y alternativas para optimizar dicho espacio.

Con respecto al resto de servidores administrados, estos se encuentran en estado estable, sin eventos críticos, únicamente registros informativos normales.

Con base en los resultados exitosos obtenidos en preproducción, en la ventana comprendida entre las 10:00 p.m. del 24 de julio de 2025 y las 2:00 a.m. del 25 de julio de 2025, se realizó el paso a producción de los ajustes mencionados, quedando completamente implementados en el ambiente productivo, sin afectación para los usuarios finales.

Se continua con la actualización del inventario de los servidores con los servicios que allí se prestan, el cual puede ser consultado en el siguiente enlace [Revision\\_IIS\\_Julio2025.xlsx](#)

En cuanto a las actividades de validación de logs, se procedió a efectuar una revisión del visor de eventos en los servidores identificando que:

- Los registros analizados corresponden principalmente a eventos informativos, relacionados con operaciones normales del sistema y de las aplicaciones hospedadas.
- No se detectaron eventos críticos ni errores que comprometan la estabilidad, seguridad o el rendimiento de los servicios en los servidores evaluados.
- Se identificaron eventos habituales como:
  - Inicios y cierres de sesión.
  - Tareas programadas completadas.
  - Validaciones exitosas de servicios.
  - Estados normales de servicios de red y aplicaciones web.

De acuerdo con esta revisión podemos concluir que la infraestructura de servidores se encuentra en estado estable, sin indicios de fallas críticas ni anomalías relevantes en el periodo revisado. Este resultado refleja un funcionamiento adecuado de los sistemas, sin necesidad de acciones correctivas inmediatas.

Durante el mes de julio de 2025, se realizaron actividades orientadas a la verificación, validación y fortalecimiento de la configuración de seguridad (hardening) en servidores críticos de la infraestructura institucional tales como: ICTXSRVNETCOR01, MIRA, ICTXSRVAPPSMIX1, ICTXSRVAPPMIX2, ICTXSRVDCVAL01 y ICTXSRVMOODLE. Estas acciones forman parte del compromiso continuo con las buenas prácticas de seguridad de la información y buscan mitigar riesgos derivados de configuraciones débiles o vulnerabilidades conocidas.

El proceso incluyó la revisión técnica de parámetros clave del sistema operativo, servicios de red, protocolos

de comunicación, y servicios como IIS y Apache Tomcat, conforme a lineamientos establecidos en guías de seguridad de Microsoft y CIS Benchmarks.

En una primera revisión se validó el 1er grupo de parámetros de configuración, para sistemas operativos Windows, con el análisis y las recomendaciones de parte nuestra.

Con el objetivo de asegurar la protección de la información y la confidencialidad de las comunicaciones realizadas a través de los diferentes servicios web de la entidad, se lleva a cabo un control detallado sobre los certificados SSL asignados a los subdominios bajo el dominio institucional icetex.gov.co. Este control es fundamental para garantizar la disponibilidad y seguridad de los servicios ofrecidos a los usuarios, cumpliendo con las políticas institucionales de ciberseguridad y buenas prácticas en la administración de infraestructura tecnológica.

Esta información permite una supervisión efectiva del ciclo de vida de los certificados, facilitando la planeación de renovaciones y la mitigación de riesgos asociados a certificados expirados o mal gestionados. El detalle del estado de los certificados y sus fechas de expiración puede ser consultado en el informe de nuestros especialistas de soluciones.

La siguiente tabla detalla las características técnicas de los principales servidores en producción, especificando información clave como: nombre del servidor, dirección IP, sistema operativo, tipo de servidor web utilizado, así como los recursos de hardware disponibles (memoria RAM, capacidad de procesamiento – CPU, y almacenamiento).

Esta información es esencial para la toma de decisiones relacionadas con la administración de recursos, optimización de cargas de trabajo, y cumplimiento de políticas de seguridad y disponibilidad.

| SERVIDOR        | IP             | SISTEMA OPERATIVO                        | SERVIDOR WEB                                  | MEMORIA RAM | CPU    | ALMACENAMIENTO |
|-----------------|----------------|------------------------------------------|-----------------------------------------------|-------------|--------|----------------|
| ICTXSRVNETCOR01 | 192.168.51.165 | Windows Server 2016 Standard 64-bit      | IIS                                           | 27GB        | 16VCPU | 2TB            |
| ICTXSRVAPPSMIX1 | 192.168.51.135 | Windows Server 2019 Standard 64-bit      | IIS                                           | 12GB        | 4VCPU  | 200GB          |
| ICTXSRVDCVAL01  | 192.168.51.17  | Windows Server 2016 Standard 64-bit      | Apache Tomcat                                 | 8GB         | 4VCPU  | 140GB          |
| MIRA            | 192.168.20.4   | Windows Server 2008 R2 Enterprise 64-bit | IIS                                           | 32GB        | 12VCPU | 1,6TB          |
| KIOSKODIGITAL   | 192.1.1.22     | Windows Server 2008 R2 Enterprise 64-bit | IIS                                           | 16GB        | 4VCPU  | 650GB          |
| SRV_APLIC       | 192.1.1.4      | Windows Server 2003 R2 Standard Edition  | IIS                                           | 4GB         | 6VCPU  | 550GB          |
| ICTXSRVMOODLE   | 192.168.51.82  | Windows Server 2019 Standard 64-bit      | IIS                                           | 12GB        | 6VCPU  | 250GB          |
| ICTXSRVAPPSMIX2 | 192.168.51.139 | Windows Server 2019 Standard 64-bit      | Tarea programada CustomWindowsServiceNovacion | 8GB         | 4VCPU  | 150GB          |

*Tabla 4 Inventario principales servidores producción*

Se realizó la verificación de las actualizaciones instaladas en los servidores Windows ICTXSRVNETCOR01, ICTXSRVAPPSMIX1, ICTXSRVDCVAL01, ICTXSRVMOODLE y ICTXSRVAPPSMIX2, identificando que se

encuentran actualizadas.

Durante el mes de julio de 2025, se realizaron actividades orientadas a la verificación, validación y fortalecimiento de la configuración de seguridad (hardening) en servidores críticos de la infraestructura institucional tales como: ICTXSRVNETCOR01, MIRA, ICTXSRVAPPSMIX1, ICTXSRVAPPMIX2, ICTXSRVDCVAL01 y ICTXSRVMOODLE. Estas acciones forman parte del compromiso continuo con las buenas prácticas de seguridad de la información y buscan mitigar riesgos derivados de configuraciones débiles o vulnerabilidades conocidas.

El proceso incluyó la revisión técnica de parámetros clave del sistema operativo, servicios de red, protocolos de comunicación, y servicios como IIS y Apache Tomcat, conforme a lineamientos establecidos en guías de seguridad de Microsoft y CIS Benchmarks.

En el informe de los especialistas de soluciones, se presenta un resumen detallado de los hallazgos por servidor, identificando los puntos cumplidos, las áreas de mejora y las recomendaciones correspondientes para asegurar el cumplimiento de estándares mínimos de protección en cada entorno revisado.

#### 4.2.1.2. Bases de Datos

A continuación se presenta un cuadro resumen con el estado actual de las bases de datos administradas:

| BASES DE DATOS     | VERSION     | TAMAÑO |
|--------------------|-------------|--------|
| ASMn user grid     | 19.13.0.0.0 | GB     |
| ICTXCYC            | 11.0.2.0.4  | 4,683  |
| ICETEX             | 11.0.2.0.4  | 206    |
| APLICATI           | 11.0.2.0.4  | 243    |
| APOTEOSY           | 11.0.2.0.4  | 460    |
| VIGIAPRD           | 19.16.0.0   | 143    |
| LIFERAY LIFERAYPDB | 19.16.0.0   | 8.20   |
| LANDICTX           | 19.16.0.0   | 529    |
| SGDEA              | 19.16.0.0   | 124    |

*Tabla 5 Estado BD Oracle*

Resultado del proceso de administración se destacan las siguientes actividades:

- Se resolvieron los casos asignados a los administradores de base de datos en los tiempos estipulados por prioridad.
- Se atendieron todas las reuniones solicitadas por el ICETEX.
- Se realizaron los mantenimientos de los espacios de los filesystem /oracle /grid /opt /DATOS de las maquinas donde se encuentran alojadas las bases de datos para su correcto funcionamiento.
- Se validaron los respaldos de las bases de datos de los archivolog, backups incrementales y backup completos o full.
- Se validó la replicación de las bases de datos del datacenter Bogotá a centro alterno de Medellín Megacenter.
- Se realizaron las restauraciones solicitadas por ICETEX de ambiente de producción a ambiente de desarrollo.
- Se realizaron actividades de tuning base de datos SGDEA (Control Doc)
- Se realizaron los mantenimientos de los espacios de los filesystem /oracle /grid /opt /DATOS de las

- maquinas donde se encuentran alojadas las bases de datos para su correcto funcionamiento.
- La disponibilidad del Clusterware BD para el mes de julio 2025 fue del 100% como se evidencia en la siguiente ilustración:

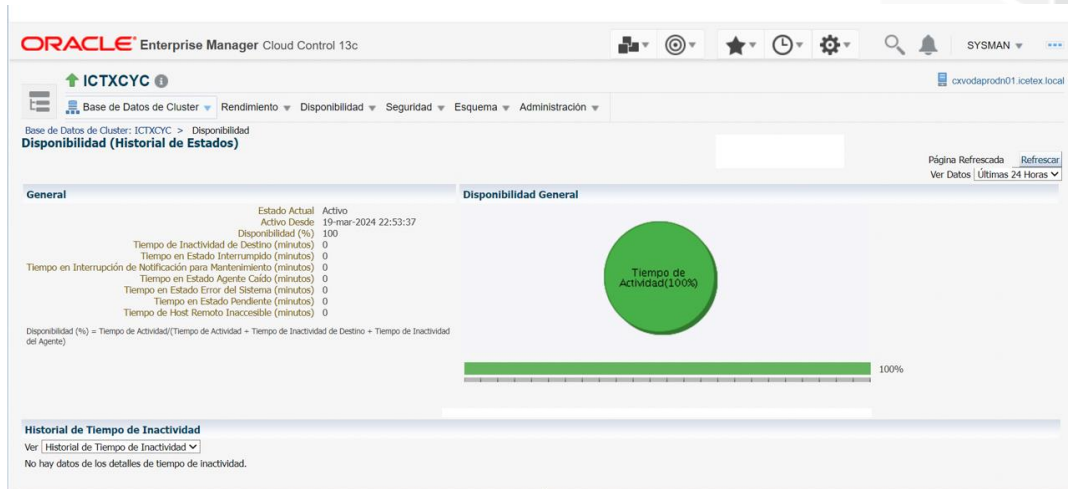


*Ilustración 1 Disponibilidad del cluster*

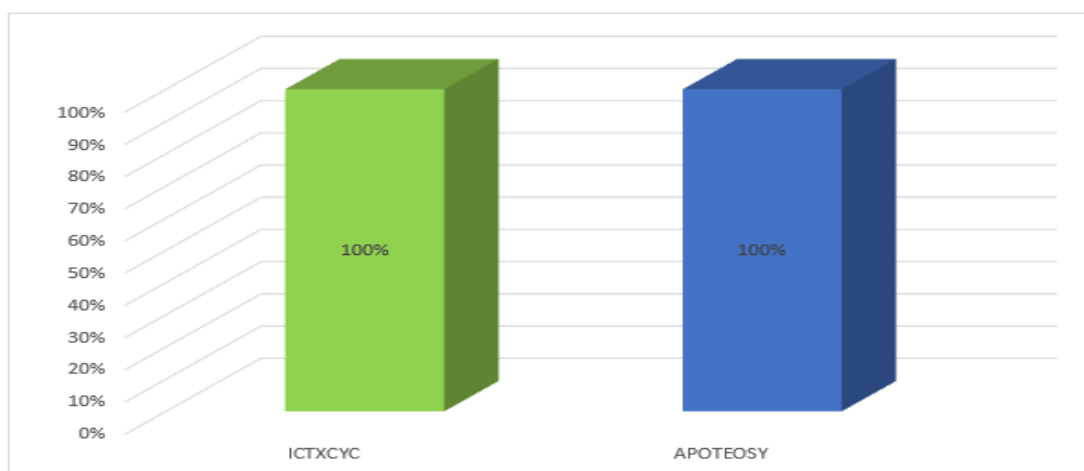


*Ilustración 2 Disponibilidad de las Bases de Datos principales ICTXCYC y APOTEOSY*

Se ha informado al ICETEX la carencia de recursos en el server de BD 10.1.4.95 para igualar los recursos del ambiente de pruebas a los de producción ya que en estos momentos la BD SICCI se encuentra funcionando con menos de ¼ de los recursos que el ambiente presenta en producción y los usuarios ya han escalado el tema en varias ocasiones, a nivel de BD se generó el análisis para el crecimiento de los recursos que se requieren sean asignados a nivel de S.O para posteriormente asignar estos a la BD SICCI.

En periodos pasados se elaboró una propuesta para el control de accesos a nivel de BD, sin tener respuesta por parte del ICETEX. A la fecha se tiene evidencia, por medio de consultas a la auditoría, que hay usuarios realizando DML's y DDL's en la BD empleando usuarios de aplicación sin ningún tipo de solicitud o control de cambio.

La versión de base de datos 11 G ya no tiene soporte por Oracle la versión que en este momento tiene

soporte es 19C y, en la actualidad, se cuentan con 5 base de datos operando en esta versión.

### ➤ Casos del proyecto Gestionados por Bases de datos:

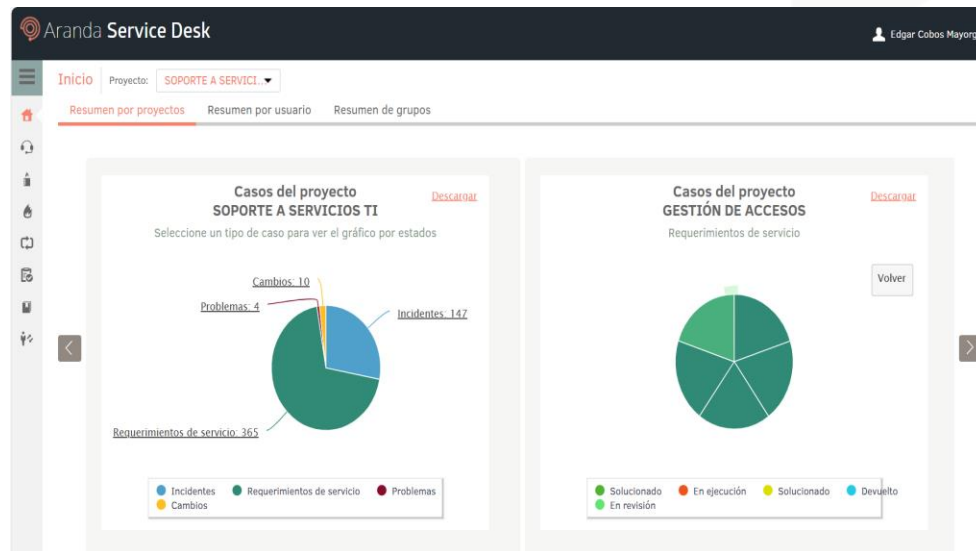


*Ilustración 3 Casos del proyecto Gestionados Aranda Bases de datos*

Desde Bases de datos se tienen las siguientes recomendaciones:

### Almacenamiento:

A continuación, se presenta el consumo del almacenamiento disponible, por cada una de las bases de datos administradas:

| BASE DE DATOS      | "DICIEMBRE 2024" | "ENERO - 2025" | "FEB-2025" | MARZO 2025" | ABRIL 2025" | "MAYO 2025" | "JUNIO 2025" | "JULIO 2025" |
|--------------------|------------------|----------------|------------|-------------|-------------|-------------|--------------|--------------|
| ICTXCYC            | 4,431.42         | 4,561.42       | 4,590      | 4,620       | 4,652       | 4,590       | 4,641        | 4,683        |
| ICETEX             | 202.2            | 203.00         | 204        | 204         | 204         | 202         | 203          | 206          |
| APLICATI           | 247              | 247.00         | 247        | 247         | 247         | 243         | 243          | 243          |
| APOTEOSY           | 473.5            | 475.00         | 483        | 485         | 485         | 458         | 459          | 460          |
| VIGIAPRD           | 111.2            | 111.20         | 114        | 116         | 120         | 133         | 137          | 143          |
| LIFERAY LIFERAYPDB | 8.2              | 8.2            | 8.20       | 8.20        | 8.20        | 8.20        | 8            | 8            |
| LANDICTX           | 533.5            | 533.5          | 533.5      | 533.5       | 533.5       | 529         | 529          | 529          |
| SGDEA              | 94               | 94             | 108        | 108         | 108         | 112         | 120          | 124          |
| TOTAL==>           | 6,101.02         | 6,233.32       | 6287.7     | 6321.7      | 6357.7      | 6,274.90    | 6,340.20     | 6,396.00     |

*Tabla 6 Crecimiento de las bases de datos en los últimos 7 meses*

- Se Aumentó el espacio del área de recuperación de las bases de datos productivas de 1TB a 2TB para tener una retención de 10 días o más.
- Se aprovisionó 1TB más de almacenamiento para las bases de datos de producción de las 8TB adicionales al cluster de producción. Esto implica que hay capacidad para un periodo de un año más, quedando pendiente por distribuir 16 TB.

### AntiVirus y seguridad:

- El antivirus de Symantec en las bases de datos sigue inactivo. Nos encontramos adelantando sesiones

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

necesarias para lograr una adecuada configuración que no genere indisponibilidad de los servicios de bases de datos.

#### Permisos de usuarios en las bases de datos:

- Sigue pendiente retirar permiso de sudo (de sistemas operativos) a los usuarios INFOTIC, GAWUSER Y DCSCAF con esto usuarios podrían realizar actividades administrativas que no van con su rol. Se sugiere que el ICETEX autorice la revocación de dichos permisos

#### Replicación

- Durante el mes de julio de 2025 se continuo con la replicación permanente de las BD Oracle al Datacenter alterno de acuerdo con las políticas establecidas, utilizando el Oracle Active Data Guard el cual garantiza una alta disponibilidad, protección de datos y recuperación ante desastres.

### 4.2.2. Centro de Datos Alterno

#### 4.2.2.1. Hosting Virtual (IaaS)

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

#### Site Recovery Manager - Estado Replicas INFOTIC

Actualmente el SRM (vcsatriara-ext.datacenterdhs.local -> vcmegacenter.datacenterdhs.local) cuenta con 11 replicas

| General                               |        |                 |                       |              |            |
|---------------------------------------|--------|-----------------|-----------------------|--------------|------------|
| Name                                  |        |                 |                       |              | Count      |
| OK                                    |        |                 |                       |              | 11         |
| Grupo de protección: PG_INFOTIC_7 (1) |        |                 |                       |              |            |
| VirtualMachine                        | Status | ConfiguredDisks | LastInstanceSyncPoint | LastSyncSize | RPO        |
| INR0226_INFOTIC_REP                   | OK     | 5 of 5          | Jul 31, 2025          | 28.41 MB     | 5 minutes  |
| Grupo de protección: PG_INFOTIC_6 (2) |        |                 |                       |              |            |
| VirtualMachine                        | Status | ConfiguredDisks | LastInstanceSyncPoint | LastSyncSize | RPO        |
| INR0228_INFOTIC_REP                   | OK     | 1 of 1          | Jul 31, 2025          | 138.88 MB    | 1 hour     |
| INR0229_INFOTIC_REP                   | OK     | 1 of 1          | Jul 31, 2025          | 123.13 MB    | 1 hour     |
| Grupo de protección: PG_INFOTIC_1 (2) |        |                 |                       |              |            |
| VirtualMachine                        | Status | ConfiguredDisks | LastInstanceSyncPoint | LastSyncSize | RPO        |
| INR0233_INFOTIC_REP                   | OK     | 2 of 2          | Jul 31, 2025          | 40.16 MB     | 30 minutes |
| INR0262_INFOTIC_REP                   | OK     | 1 of 1          | Jul 31, 2025          | 14.02 MB     | 1 hour     |
| Grupo de protección: PG_INFOTIC_4 (3) |        |                 |                       |              |            |
| VirtualMachine                        | Status | ConfiguredDisks | LastInstanceSyncPoint | LastSyncSize | RPO        |
| INR0238_INFOTIC_REP                   | OK     | 2 of 2          | Jul 31, 2025          | 648.38 MB    | 1 hour     |
| INR0239_INFOTIC_REP                   | OK     | 2 of 2          | Jul 31, 2025          | 37.66 MB     | 1 hour     |
| INR0243_INFOTIC_REP                   | OK     | 2 of 2          | Jul 31, 2025          | 126.95 MB    | 1 hour     |
| Grupo de protección: PG_INFOTIC_3 (2) |        |                 |                       |              |            |
| VirtualMachine                        | Status | ConfiguredDisks | LastInstanceSyncPoint | LastSyncSize | RPO        |
| INR0244_INFOTIC_REP                   | OK     | 1 of 1          | Jul 31, 2025          | 82.77 MB     | 1 hour     |
| INR0245_INFOTIC_REP                   | OK     | 1 of 1          | Jul 31, 2025          | 7.53 MB      | 5 minutes  |
| Grupo de protección: PG_INFOTIC_2 (1) |        |                 |                       |              |            |
| VirtualMachine                        | Status | ConfiguredDisks | LastInstanceSyncPoint | LastSyncSize | RPO        |
| INR0249_INFOTIC_REP                   | OK     | 2 of 2          | Jul 31, 2025          | 8.64 MB      | 5 minutes  |

Ilustración 4 Reportes de replicación SRM a Sitio Alterno – julio 2025

En la siguiente tabla se detallan los servidores con sus correspondientes servicios los cuales están

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

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         | icetexboglخورfeo1       | ORFEO                       | INR0233_INFOTIC_REP        |
| 5  | INR0219         | icetexboglخورfeo2       | ORFEO                       | INR0262_INFOTIC_REP        |
| 6  | INR0208 *       | ICTXBOGSRVPT1           | Portal Transaccional        | INR0236_INFOTIC_REP        |
| 7  | INR0209 **      | icetexboglserver1       | 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         | icetexbogldarumasrv1    | DARUMA                      | INR0244_INFOTIC_REP        |
| 12 | INR0213         | icetexbogldarumasrv2    | DARUMA                      | INR0245_INFOTIC_REP        |
| 13 | INR0214         | icetexboglxroad1        | XROAD                       | INR0249_INFOTIC_REP        |

*Tabla 7 Servicios replicados – Datacenter Megacenter*

\*Se detiene la replicación identificada con el código INR0208 que replica la máquina INR0236- ICTXBOGSRVPT1. Los recursos de esta última se distribuyen, en el centro de datos TRIARA, entre los servidores OPENSIFT identificados con los códigos de servicio INR0259, INR0258 e INR0251.

\*\* Se detiene la replicación INR0209 que replica la máquina virtual INR0237- icetexboglserver1, corresponde al antiguo balanceador, NGIX, que fue deshabilitado en TRIARA

A continuación se presentan las máquinas con mayores y menores tasas de transferencia:

| INR     | HOSTNAME            | MB        |
|---------|---------------------|-----------|
| INR0233 | icetexboglخورfeo1   | 239892.59 |
| INR0238 | icetexbogliferaynfs | 14850.7   |
| INR0228 | ictxisgesbd         | 7886.74   |
| INR0229 | ictxisgesapp        | 7064.24   |
| INR0226 | icetexbogwsmira     | 4312.85   |

*Tabla 8 TOP 5 máquinas mayor tasa de transferencia*

| INR     | HOSTNAME                | MB      |
|---------|-------------------------|---------|
| INR0245 | icetexbogldarumasrv2    | 221.31  |
| INR0262 | icetexboglخورfeo2       | 544.00  |
| INR0249 | icetexboglxroad1        | 964.36  |
| INR0239 | icetexbogelasticserver1 | 1566.39 |
| INR0244 | icetexbogldarumasrv1    | 1846.81 |

*Tabla 9 TOP 5 máquinas menor tasa de transferencia*

En cuanto a las fechas con mayor replicación presentada podemos observar el siguiente comportamiento:

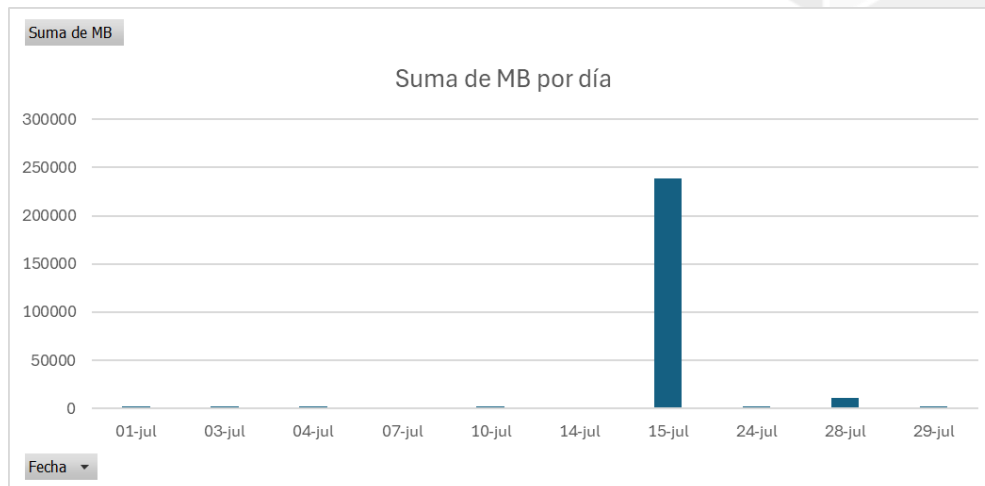


*Ilustración 5 Fechas con mayor replicación*

En julio, la actividad de replicación **se caracterizó por un predominio significativo de un evento masivo el día 15**. Dicho evento correspondió a una intervención sobre el servidor INR0233, el antiguo gestor documental, solicitada por ICETEX para redimensionar su disco y destinar dicho almacenamiento al servidor de Base de Datos Oracle. Posteriormente, el día 28, se registró otra jornada de elevada actividad básicamente sobre el Servidor INR0238 NFS de Portal probablemente por carga de contenidos o documento en el Portal. Los volúmenes de replicación observados en el resto de los días dentro del top 10 fueron sustancialmente inferiores en comparación con estos dos picos.

#### 4.2.2.2. Dataguard Bases de Datos Megacenter

Durante el mes de julio de 2025 se continuo con la replicación permanente de las BD Oracle al Datacenter alterno de acuerdo con las políticas establecidas, utilizando el Oracle Active DataGuard el cual garantiza una alta disponibilidad, protección de datos y recuperación ante desastres. Ver las evidencias en el documento [Informe Mensual InfoTIC DBA Julio 2025.pdf](#)

```

oracle@cxvodacontg011:~$ ps -fealgrep pmon
grid      8054      1 0 2024 ?        00:30:49 asm_pmon_+ASM
oracle    9044      1 0 2024 ?        01:18:45 ora_pmon_ICETEXD
oracle   10396      1 0 2024 ?        01:19:11 ora_pmon_APOTEOSD
oracle   10746      1 0 2024 ?        01:18:55 ora_pmon_APOTNEWD
oracle   11132      1 0 2024 ?        00:43:47 ora_pmon_VIGIADTG
oracle   11573      1 0 2024 ?        00:43:48 ora_pmon_LANDICTD
oracle   12543      1 0 2024 ?        01:18:07 ora_pmon_APLICATD
oracle   24368      1 0 Jun02 ?        00:21:41 ora_pmon_ICTXCYCD
oracle   24703      1 0 Jun02 ?        00:13:10 ora_pmon_LIFERAYD
oracle   28441 27867  0 08:50 pts/3    00:00:00 grep --color=auto pmon
[oracle@cxvodacontg011 ~]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.4.0 Production on Sat Aug 2 08:50:07 2025

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

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

SQL> sta apply

  Thread Last Sequence Received Last Sequence Applied Difference
  -----
        1             121229             121229             0
        2             87266             87266             0

SQL> sta fapplyb.sql

  Thread Last Sequence Received Last Sequence Applied TIME_RECEIVED  TIME_APPLIED
  -----
        1             121229             121229 31/07/2025 08:50 31/07/2025 08:50
        2             87266             87266 31/07/2025 08:50 31/07/2025 08:50

SQL> █
  
```

*Ilustración 6 Evidencia Dataguard replicado a Megacenter BD*

Se generó la consulta de los archivos recibidos y aplicados de la base de datos de ICTXCYCD a 31/07/2025 con diferencia cero (0) archivos sin aplicar, lo que evidencia la sincronización a nivel de Bases de datos Oracle.

#### 4.2.2.3. Servicios de Housing – Datacenter Alterno

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

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

*Tabla 10 Disponibilidad de Servicios de Housing – Data Center Alterno*

#### 4.2.2.4. Servicios de DRP

Nos encontramos a la espera de la definición del alcance de la prueba y de la fecha prevista de la misma, por parte del ICETEX.

### 4.3. Seguridad informática

Se presenta el diagrama de red actual que se tiene actualmente a nivel de los dispositivos de seguridad

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

perimetral y el componente de antivirus Sophos.

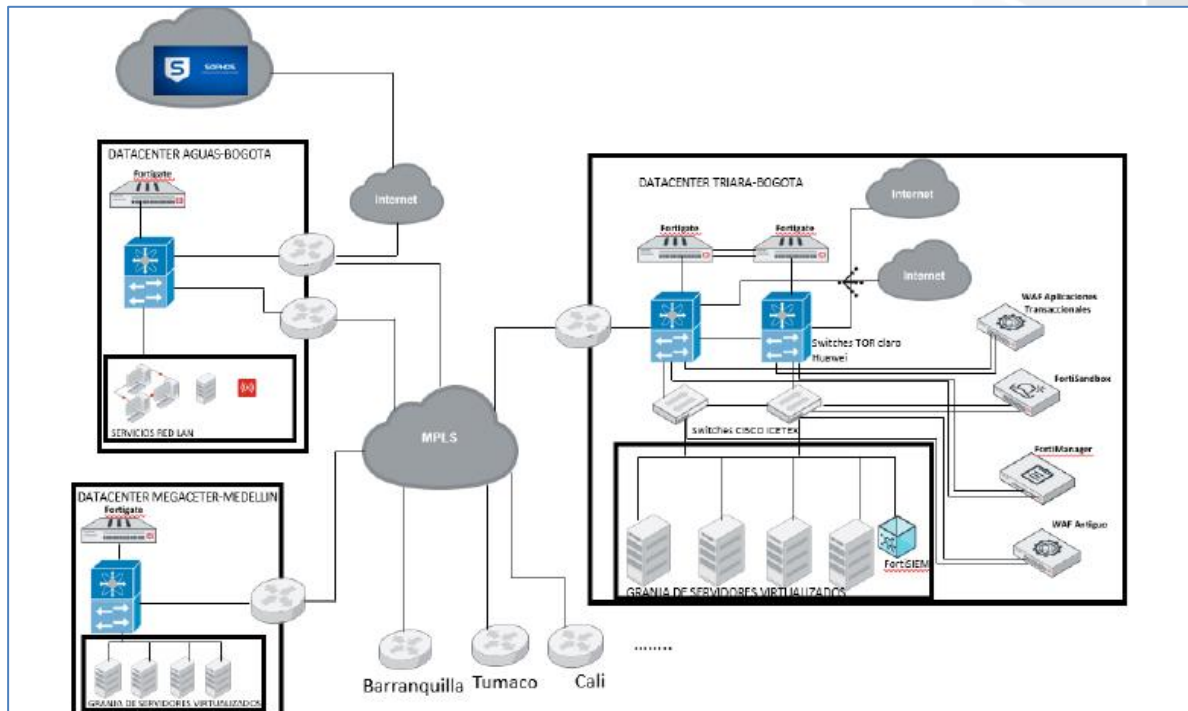


*Ilustración 7 Diagrama de la Arquitectura de Seguridad*

En la ilustración 8, se observa la implementación del WAF Cloud donde se utilizaron dos aplicaciones web para el DRP los cuales tienen como dominios: [webdrp.icetex.gov.co](http://webdrp.icetex.gov.co) y [drp.icetex.gov.co](http://drp.icetex.gov.co).

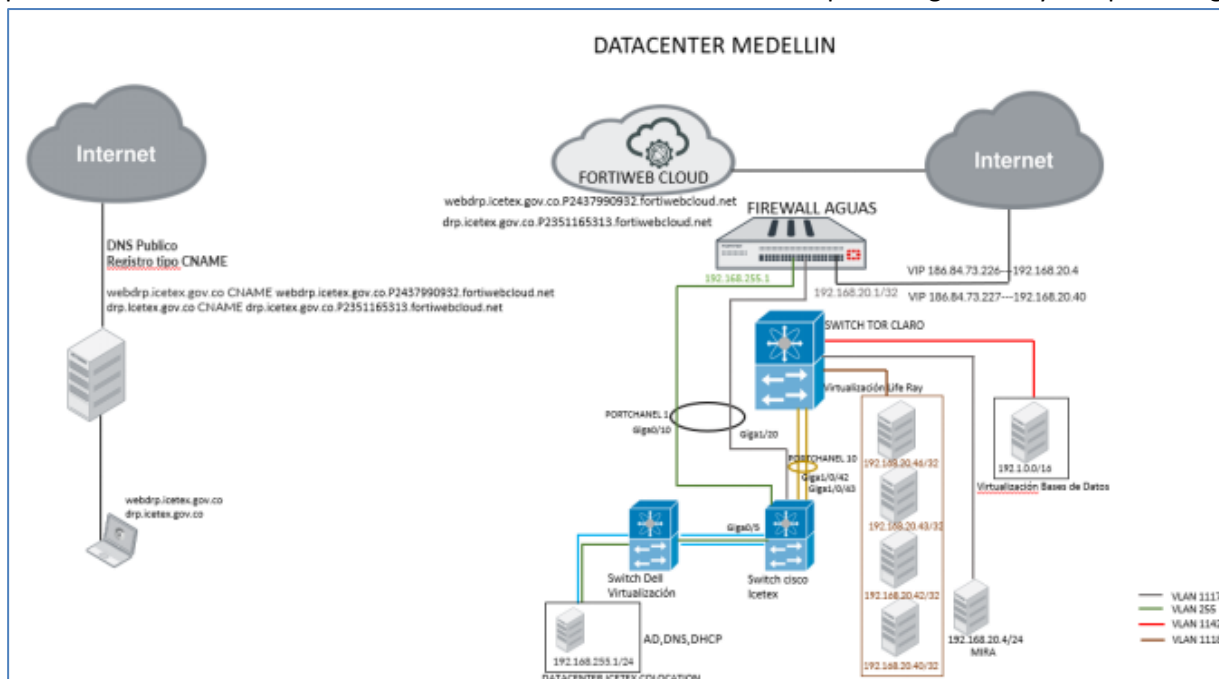


*Ilustración 8 Topología de WAF Cloud usado en portales de Medellín*

Sede principal-Bogotá, Colombia  
Calle 93B # 13-44, Segundo piso  
NIT:900.068.796-1  
Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
Cra. 24 No. 53ª-26 Arboleda Alta.  
NIT: 900.068.796-1  
Teléfono: (+606) 88612612

En la implementación del WAF alterno la configuración realizada se dio para la activación del DRP con servicios aislados, en el caso de un escenario real de activación del DRP se debe dar continuidad con las configuraciones productivas aplicándose con los dominios productivos (www.icetex.gov.co y web.icetex.gov.co) sin necesidad de recurrir a los dominios alternos (webdrp.icetex.gov.co). Las configuraciones restantes ya se encuentran aplicadas a dicho WAF.

Durante el mes de julio de 2025, se llevaron a cabo diversas actividades relacionadas con la administración y gestión de la seguridad perimetral de la entidad.

Se atendieron y resolvieron varios eventos de seguridad, incluyendo intentos de acceso no autorizado a la red detectados por el SOC. A través de FortiSiem se identificaron cuatro direcciones IP maliciosas que intentaron establecer conexiones hacia los servicios web institucionales desde diferentes puertos. Como respuesta, se implementaron medidas adicionales de seguridad, tales como ajustes en los perfiles de IPS, eliminación de políticas obsoletas y depuración de usuarios en el firewall FortiGate de Triara. Asimismo, se bloquearon servicios de escaneo en línea que estaban siendo utilizados para mapear servicios expuestos en el direccionamiento IP público de la entidad.

En cuanto a la gestión del firewall de la red, ubicado en la sede de Aguas, se continuó con el proceso de depuración de políticas. En el periodo se eliminaron reglas con tráfico igual a cero y otras que estaban duplicadas. Actualmente, se registran 536 políticas (13 nuevas incorporadas respecto al mes anterior como parte del proceso de afinamiento). Este trabajo continuará en los próximos meses, evaluando oportunidades para consolidar o eliminar reglas innecesarias. Las evidencias de esta gestión fueron incluidas en el numeral 6.2 del informe mensual de especialistas de seguridad del mes de julio, link: [Informe Mensual InfoTIC Seguridad Julio 2025.pdf](#)

Adicionalmente, se ha avanzado en la eliminación de objetos duplicados en dicho firewall, como parte de los esfuerzos de optimización y mejora continua del rendimiento de estos dispositivos.

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

#### **Gestión y fortalecimiento de la seguridad perimetral.**

Durante el mes de julio se mantuvo una gestión activa de la seguridad perimetral y endpoint, evidenciada en la atención de incidentes, requerimientos y tareas, así como en el monitoreo continuo de alertas mediante FortiSIEM, FortiGate, FortiWeb, Sophos y otros componentes del ecosistema de seguridad.

#### **Monitoreo de seguridad y respuesta ante incidentes**

En el presente mes hemos informado, a la supervisión, sobre una exposición no segura en internet que muestra detalles actuales de créditos y datos personales. Hemos identificado un sitio ajeno al ICETEX que, debido a esta vulnerabilidad, podría estar facilitando un proceso de recaudo fraudulento.

(Api: <https://aplicaciones.icetex.gov.co/WsApiSolicitudes/api/BusIcetex/GetDatosFacturaCore/0173731506-8> Sitio: <https://pagocreditoicetex.com/WebsitePSE/login.php>).

*Durante el desarrollo de nuestras actividades, hemos identificado APIs Accesibles Públicamente sin Tokenización estas vulnerabilidades que están siendo explotadas, de acuerdo a informaciones emitidas por nuestro SOC (Security Operation Center), como es el caso de la URL relacionada en el párrafo anterior.*

*Estas incidencias requieren una atención prioritaria debido a su impacto. Es importante señalar que, debido a la naturaleza de estas fallas, su subsanación recae directamente en el área de desarrollo de la entidad y, no*

se encuentra dentro del alcance la gestión o implementación de soluciones para este tipo de vulnerabilidades a nivel de código o arquitectura de las aplicaciones.

casos similares a este, los cuales detallamos a continuación y que requerirían igual atención:

- ✓ <https://www.icetex.gov.co/ApiEstadoCuenta/api/ExternalService/facturabyid2/1905959533-6>
- ✓ <https://aplicaciones.icetex.gov.co/WsApiSolicitudes/api/BusIcetex/GetCodigoServicioByReferencia/1905959533>
- ✓ <https://aplicaciones.icetex.gov.co/WsApiSolicitudes/api/BusIcetex/GetDatosFacturaCore/1905959533-6>
- ✓ <https://aplicaciones.icetex.gov.co/WsApiSolicitudes/api/BusIcetex/ConsultarBancosKushki/1919>
- ✓ <https://www.icetex.gov.co/portalacces/GestionCredito/renovar/cptRenovacionIES.asp?idSltud=6603687>

Solicitamos amablemente que esta situación sea revisada y atendida de acuerdo como determine el ICETEX por el equipo de desarrollo correspondiente.

### Detección Oportuna de Amenazas

Se identificaron múltiples eventos de seguridad como intentos de acceso no autorizado a través de VPNs desde el extranjero, tráfico hacia indicadores de compromiso (IoC) y ataques de denegación de servicio (DoS). La oportuna intervención del equipo permitió contener las amenazas, minimizar el riesgo y ajustar las configuraciones para prevenir eventos futuros.

### Ajustes y Afinamientos en Políticas de Seguridad

Se realizaron labores de depuración y optimización en las reglas de firewall, eliminando políticas obsoletas, duplicadas o sin tráfico, especialmente en el firewall de Aguas, mejorando la eficiencia y mantenibilidad de las reglas. También se fortalecieron las configuraciones IPv6.

### Plataformas Actualizadas y con Buen Rendimiento

Los dispositivos FortiGate, FortiWeb y FortiSandbox se encuentran operativos con versiones estables de firmware y dentro de los parámetros normales de rendimiento (uso de CPU, memoria y sesiones). No obstante, se detectaron dispositivos con licenciamiento vencido o en etapa de fin de vida útil, como el FortiWeb 2000E y el FortiSandbox 1000D, lo cual requiere acciones próximas.

### Cobertura y Contención con Sophos Endpoint

Se bloquearon múltiples amenazas, en su mayoría variantes de malware HTML y troyanos, desde diversas fuentes, especialmente del dominio “crearfuturo.co” y sitios externos maliciosos. A pesar de la buena cobertura, se identificaron equipos sin conexión al sistema de protección durante más de 9 meses, recomendándose su revisión y eventual retiro.

#### 4.3.1. Plataformas Administradas

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

| SERIAL           | MODELO          | UBICACIÓN FÍSICA   | OBSERVACIONES                                             |
|------------------|-----------------|--------------------|-----------------------------------------------------------|
| FG6H0FTB22902021 | FortiGate 600F  | Aguas              | Funciona como Firewall - Prestación como servicio infotic |
| FG180FTK22901087 | FortiGate 1800F | Data Center Triara | Funciona como Firewall - Prestación como servicio infotic |

| SERIAL           | MODELO                   | UBICACIÓN FÍSICA                  | OBSERVACIONES                                                          |
|------------------|--------------------------|-----------------------------------|------------------------------------------------------------------------|
| FG180FTK22901182 | FortiGate 1800F          | Backup Data Center Triara         | Funciona como Firewall - Prestación como servicio infotic              |
| FG6H0FTB22902086 | FortiGate 600F           | Data Center Megacenter Medellín   | Funciona como Firewall - Prestación como servicio infotic              |
| FV-2KFTE21000029 | FortiWeb 2000F           | Data Center Triara                | Función como WAF - Prestación como servicio infotic                    |
| FMG2HGT22000550  | FortiManager 200G        | Data Center Triara                | Prestación como servicio infotic                                       |
| FSMP000000001340 | FortiSIEM                | Máquina Virtual vmware de cliente | Funciona como correlacionador de eventos - En VMware de Icetex         |
| FV-2KE3117000046 | FortiWeb 2000E           | Data Center Triara                | Función como WAF - Propiedad de Icetex                                 |
| FV-2KE3117000032 | FortiWeb 2000E           | Data Center Triara                | Función como WAF - Propiedad de Icetex                                 |
| FSA1KD3A17000156 | FortiSandbox 1000D       | Data Center Triara                | Funciona como Escaneo de archivos - Propiedad de Icetex                |
| FAC1KD3A17000020 | FortiAuthenticator 1000D | Data Center Triara                | Funciona para autenticación y CA de certificados - Propiedad de Icetex |
| FAC1KD3A17000036 | FortiAuthenticator 1000D | Data Center Triara                | Propiedad de Icetex                                                    |

*Tabla 11 Detalle plataformas Seguridad administradas INFOTIC*

A continuación, se presenta el estado actual de los tiempos de soporte y vigencias de los dispositivos FortiGate administrados:

| Dispositivo                     | IP          | Licenciamiento | Fin Licenciamiento | Datacenter |
|---------------------------------|-------------|----------------|--------------------|------------|
| <b>FW Fortigate 1800F (MST)</b> | 10.0.0.53   | Si             | 18/05/2026         | Triara     |
| <b>FW Fortigate 1800F (SLV)</b> | 10.0.0.53   | Si             | 18/05/2026         | Triara     |
| <b>FW FortiGate 600F</b>        | 10.0.0.30   | Si             | 1/06/2026          | Megacenter |
| <b>FW FortiGate 600F</b>        | 10.1.100.33 | Si             | 11/05/2026         | Aguas      |

*Tabla 12 Licenciamiento FortiGate*

#### 4.3.1.1. FortiGate Triara

A nivel de sistema, el firewall de Triara (FortiGate 1800F), no presenta afectaciones en cuanto a licenciamiento o performance; actualmente se encuentra en la versión de FortiOS 7.4.8. la cual fue actualizada en el mes de julio de 2025.

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

A continuación se presentan los consumos en el presente mes:

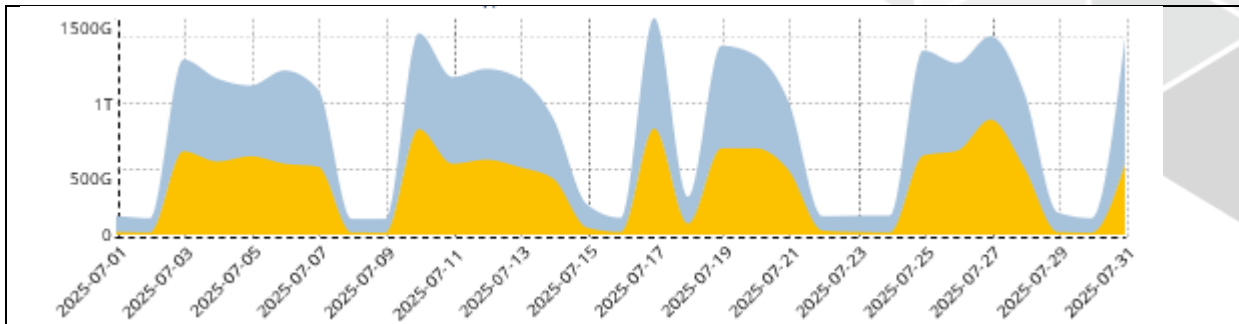


*Ilustración 9 Consumo canal MPLS - promedio 1200G [INR0185 CLARO(MPLS\_DC)]*

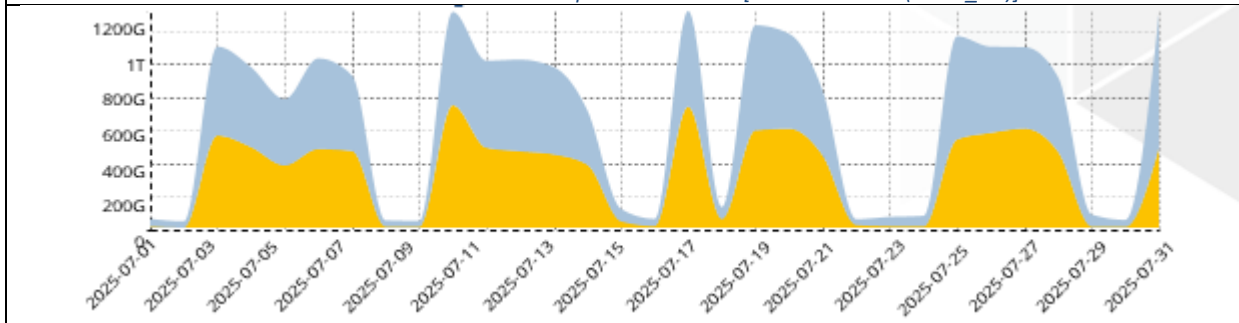


*Ilustración 10 Consumo canal Internet Sedes - Promedio 1100 GB WAN-SEDES-ICETEX [INR0264 (INTE\_SEDES\_ICTX)]*

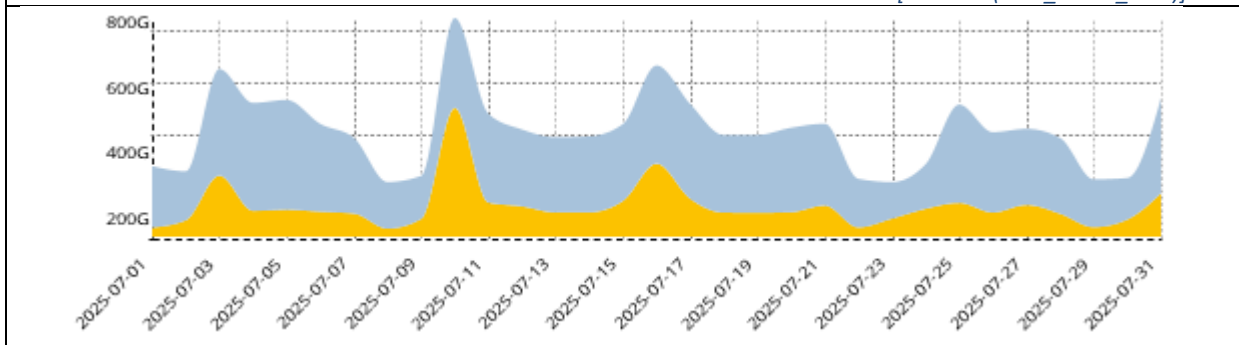


*Ilustración 11 Consumo Canal Internet Data Center- INTERNET DATACENTER [INTERNET\_DC\_INR0000320 (Inet\_claro)]*

A nivel de perfiles de UTM (UTM son fragmentos de texto que se añaden al final de la URL y que sirven para rastrear, con mayor precisión, el origen de las visitas a una web), se tienen los siguientes perfiles para Web Filter, Antivirus y SSL Inspection actualmente:

|     | Name                            | Comments                                                           | Ref. |
|-----|---------------------------------|--------------------------------------------------------------------|------|
| WEB | default                         | Perfil con las mínimas restricciones                               | 0    |
| WEB | Navegacionpcs_Comware           | Perfil con restricciones                                           | 2    |
| WEB | Navegacionpcs_Comware_con_redes | Perfil con restricciones                                           | 1    |
| WEB | WF-Avanzado                     | Perfil para FSSO Navegación Avanzada                               | 31   |
| WEB | WF-Comunicaciones               | Perfil para FSSO comunicaciones                                    | 2    |
| WEB | WF-General                      | Perfil para todos                                                  | 5    |
| WEB | WF-General_Sedes                | Perfil para todos                                                  | 1    |
| WEB | WF-Sede_Ibague_YT               | 27022025/InfoTIC/Tarea Aranda 517214 (17458) Se solicita el acc... | 1    |
| WEB | WF-Tesorería                    | Perfil con restricciones específicas por auditoría.                | 4    |
| WEB | WF-VIP                          | Perfil para FSSO Navegación_VIP                                    | 16   |
| WEB | WF-wetransfer                   | Perfil para FSSO Navegación Avanzada                               | 1    |
| WEB | wifi-default                    | Perfil de FULL acceso para pruebas                                 | 1    |

Ilustración 12 Filtrado – WEB – (FortiGate – Triara)

|     | Name                          | Comments                                    | Ref. |
|-----|-------------------------------|---------------------------------------------|------|
| SSL | custom-deep-inspection        | Customizable deep inspection profile.       | 0    |
| SSL | deep-inspection               | Read-only deep inspection profile.          | 0    |
| SSL | certificate-inspection_2780   | Read-only SSL handshake inspection profile. | 1    |
| SSL | certificate-inspection_IPv6   | Read-only SSL handshake inspection profile. | 1    |
| SSL | Prueba certificate-inspection | Read-only SSL handshake inspection profile. | 12   |
| SSL | certificate-inspection_ICETEX | SSL para BUS de servicios                   | 31   |
| SSL | no-inspection                 | Read-only profile that does no inspection.  | 230  |
| SSL | certificate-inspection        | Read-only SSL handshake inspection profile. | 400  |

Ilustración 13 Inspección – SSL – (FortiGate – Triara)

|    | Name         | Comments              | Ref. |
|----|--------------|-----------------------|------|
| AV | AV-FSB       | HTTP,SMTP FULL FSB    | 73   |
| AV | AV-HTTP      | HTTP con FSB          | 25   |
| AV | AV-HTTP&CIFS | HTTP,CIFS con FSB     | 4    |
| AV | AV-SMTP      | SMTP FULL FSB         | 1    |
| AV | default      | ALL con FSB           | 40   |
| AV | ICETEX       |                       | 65   |
| AV | prueba2      |                       | 57   |
| AV | wifi-default | ALL monitoreo sin FSB | 1    |

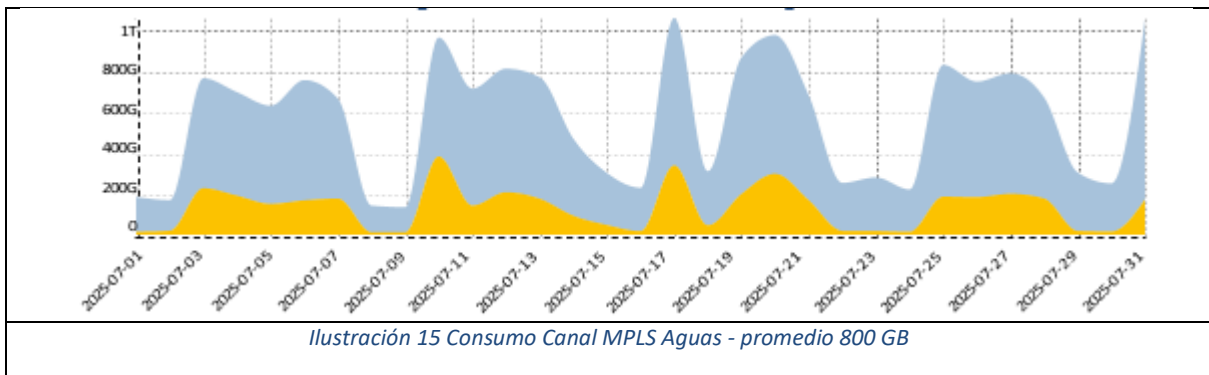
Ilustración 14 Antivirus y Antimalware – Perimetral (FortiGate – Triara)

#### 4.3.1.2. FortiGate Aguas

A nivel de sistema, el firewall de Aguas (FortiGate 600F), no presenta afectaciones en cuanto a licenciamiento o performance; actualmente se encuentra en la versión de FortiOS 7.4.8.

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

A continuación se presentan los consumos en el presente mes:



A nivel de perfiles de UTM, se tienen los siguientes perfiles para Web Filter, Antivirus y SSL Inspección actualmente:

|     | Name             | Comments                                           | Ref. |
|-----|------------------|----------------------------------------------------|------|
| WEB | default          | Default web filtering.                             | 0    |
| WEB | General_Icetex   |                                                    | 51   |
| WEB | monitor-all      | Monitor and log all visited URLs, flow-based.      | 0    |
| WEB | VIP_FUNCIONARIOS |                                                    | 3    |
| WEB | wifi-default     | Default configuration for offloading WiFi traffic. | 1    |

*Ilustración 16 Filtrado-Web-(FortiGate-Aguas)*

|     | Name                          | Comments                                    | Ref. |
|-----|-------------------------------|---------------------------------------------|------|
| SSL | certificate-inspection        | Read-only SSL handshake inspection profile. | 275  |
| SSL | certificate-inspection_WX     | Read-only SSL handshake inspection profile. | 2    |
| SSL | custom-deep-inspection        | Customizable deep inspection profile.       | 0    |
| SSL | custom-deep-inspection_icetex | Customizable deep inspection profile.       | 0    |
| SSL | deep-inspection               | Read-only deep inspection profile.          | 0    |
| SSL | no-inspection                 | Read-only profile that does no inspection.  | 239  |

*Ilustración 17 Inspección-SSL-(FortiGate-Aguas)*

| Name            | Comments                                           | Ref. |
|-----------------|----------------------------------------------------|------|
| AV-ICETEX       |                                                    | 242  |
| AV default      | Scan files and block viruses.                      | 4    |
| AV wifi-default | Default configuration for offloading WiFi traffic. | 1    |

Ilustración 18 Antivirus y Antimalware-Perimetral-(FortiGate-Aguas)

#### 4.3.1.3. FortiGate Medellín

A nivel de sistema, el firewall de Medellín (FortiGate 600F), no presenta afectaciones en cuanto a licenciamiento o performance; actualmente se encuentra en la versión de FortiOS 7.4.8. Para más información validar el portal del fabricante <https://docs.fortinet.com/product/fortigate/7.6>

Se observa en la Ilustración 18, que la interfaz de la MPLS del Data Center de Medellín no presenta tráfico debido a que este se tiene como Data Center Alterno.

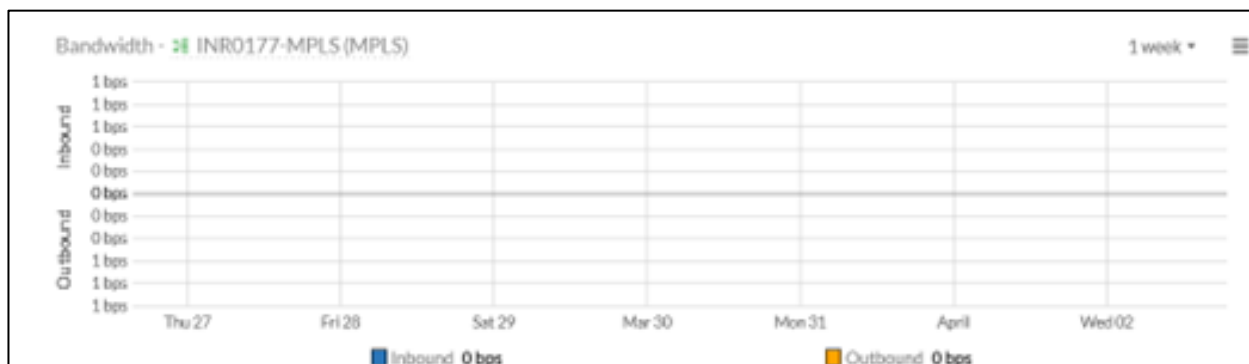


Ilustración 19 Consumo Canal MPLS Medellín

#### 4.3.1.4. FortiWeb 2000F

A nivel de sistema del FortiWeb en la siguiente ilustración se presenta la configuración actual y su versión de firmware está en la 7.6.4 la cual es una de las versiones actuales más estables.

#### 4.3.1.5. FortiWeb 2000E

A nivel de sistema, el FortiWeb presenta su configuración actual y su versión de Firmware que actualmente se encuentra en la 7.6.4. Sin embargo, cabe aclarar que, a nivel de licenciamiento, los equipos no tienen un licenciamiento vigente en este momento.

| Dispositivo                 | IP            | Propiedad Icetex | Licenciamiento | Fin Licenciamiento | DC     | End Of Order | Last Service Extension | End of support |
|-----------------------------|---------------|------------------|----------------|--------------------|--------|--------------|------------------------|----------------|
| Fortiweb1 2000E (WAF) (MST) | 10.0.0.251    | SI               | No             | 20/06/2023         | Triara | 13/01/2022   | 13/01/2026             | 13/01/2027     |
| Fortiweb2 2000E (WAF) (SLV) | 10.0.0.251    | SI               | No             | 20/06/2023         | Triara | 13/01/2022   | 13/01/2026             | 13/01/2027     |
| Fortiweb1 2000F (WAF)       | 192.168.91.10 | No               | Si             | 1/06/2026          | Triara | N/A          | N/A                    | N/A            |

Tabla 13 Licenciamiento FortiWeb

En el mes, se presenta un promedio de 1200GB de tráfico general hacia los portales protegidos por el FortiWeb donde el portal de web.icetex.gov.co y www.icetex.gov.co fueron los más utilizados en este periodo, lo cual es un comportamiento normal para este tipo de transacciones de acuerdo con la actividad de los usuarios y las convocatorias vigentes.

## 2.2.Top Hosts per Response Bytes

| #  | HTTP Host                      | HTTP Request Bytes | HTTP Response Bytes |
|----|--------------------------------|--------------------|---------------------|
| 1  | web.icetex.gov.co              | 1.96 GB            | 29.68 GB            |
| 2  | www.icetex.gov.co              | 216.22 MB          | 7.36 GB             |
| 3  | aplicaciones.icetex.gov.co     | 447.25 MB          | 2.61 GB             |
| 4  | comunidad.icetex.gov.co        | 2.27 MB            | 153.42 MB           |
| 5  | identidad.icetex.gov.co        | 62.59 KB           | 1.97 MB             |
| 6  | web.icetex.gov.co:443          | 29.59 KB           | 1.83 MB             |
| 7  | comunidad.icetex.gov.co:443    | 7.44 KB            | 1.35 MB             |
| 8  | appsitiospruebas.icetex.gov.co | 54.18 KB           | 822.69 KB           |
| 9  | 186.84.73.163                  | 2.68 KB            | 650.76 KB           |
| 10 | 186.84.73.154                  | 5.24 KB            | 643.16 KB           |

Ilustración 20 Tráfico General de los portales

### 4.3.1.6. FortiSandBox

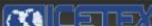
A nivel de sistema, el Sandbox (FortiSandBox 1000D) muestra su configuración actual y su versión de firmware que actualmente se encuentra en la 3.2.4 siendo esta la última versión disponible para este dispositivo, ya que está en EOL (término empleado por el fabricante para describir un producto que pronto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

| Dispositivo        | IP         | Propiedad Icetex | Licenciamiento | Fin Licenciamiento | DC     | End Of Order | Last Service Extension | End of support |
|--------------------|------------|------------------|----------------|--------------------|--------|--------------|------------------------|----------------|
| FortiSandbox 1000D | 10.0.0.249 | Si               | No             | 1/06/2023          | Triara | 2/04/2019    | 2/04/2023              | 2/04/2024      |

Tabla 14 Configuración FortiSandBox 1000D

### 4.3.1.7. FortiSIEM

En el presente periodo se efectuó el upgrade de la versión del FORTISIEM a la versión 7.4.0, tal y como se evidencia en la siguiente gráfica:



Dashboard

Analytics

Incidents

Cases

CMDB

Resources

Tasks

Admin

Setup

Device Support

Health

License

Content Update

Settings

Cloud Health

Collector Health

Agent Health

Replication Health

Automation Agent Health

1

Total

0

No Connection

0

Critical

0

Warning

1

Normal

Download Content

Search...

Columns

Last update at 10:51:35 PM

< 50

1/1

>

| Name           | IP Address  | Type               | Health | Last Status Updated       | Version    | EPS      | Load Average   | CPU |
|----------------|-------------|--------------------|--------|---------------------------|------------|----------|----------------|-----|
| FORTISIEM_ICTX | 192.1.1.100 | Supervisor With DB | Normal | Jul 31, 2025, 10:49:59 PM | 7.4.0.0435 | 3,846.07 | 4.87,5.22,4.68 | 32% |

Ilustración 21 Versión actual FORTISIEM

En esta sección se observa los datos del licenciamiento de la plataforma FortiSIEM y su consumo de procesos en un tiempo determinado.

| General Usage Nodes  |                                      |                |
|----------------------|--------------------------------------|----------------|
| Serial Number:       | FSMP000000001340                     | Upload License |
| Hardware ID:         | 4212F192-8EF3-61A8-F30D-4EAF9DE2E3F6 |                |
| License Hardware ID: | 4212F192-8EF3-61A8-F30D-4EAF9DE2E3F6 |                |
| License Type:        | Enterprise                           |                |
| FIPS Mode:           | Disabled                             |                |

| Attribute                 | Value | Expiry      |
|---------------------------|-------|-------------|
| Devices                   | 200   | Perpetual   |
| Total EPS                 | 2000  | Perpetual   |
| Agents                    | 100   | Perpetual   |
| UEBA                      | 75    | Perpetual   |
| IOC Service               | Valid | Apr 19,2026 |
| Maintenance and Support   | Valid | Apr 19,2026 |
| High Availability Service | N/A   | N/A         |

Ilustración 22 Licenciamiento FortiSIEM

#### 4.3.1.8. Sophos EndPoint

En la ilustración 23, se observa un resumen del estado de Seguridad del Endpoint donde actualmente se están cumpliendo en un 100% los puntos de seguridad de la plataforma de Sophos indicando protección de equipos, políticas y exclusiones.



Ilustración 23 Estado Seguridad Sophos

En cuanto al licenciamiento se cuenta con una vigencia hasta el 26 de junio de 2026.

Hay cuatro equipos, que se encuentran en estado no protegido, los cuales son: BOGARRIENDO88, BOGIMAC01, BOGVFAPC502, COWORKING11 y llevan más de 9 meses en algunos casos de no conectarse, recomendamos que la mesa revise los equipos.

En la sección 6.6.1 del informe de seguridad [Informe Mensual InfoTIC Seguridad Julio 2025.pdf](#) se detallan las amenazas contenidas por la herramienta el Sophos instalado en los equipos ordenadores y servidores.

### 4.3.2. Estadística de Portales

Durante el mes de julio de 2025 se continuo con el monitoreo permanente a los portales sobre los que opera el ICETEX, manteniendo, las alertas y reportes a tiempo en caso de que se presentara algún evento que pudiera ocasionar una interrupción en la prestación de los servicios que se ofrecen a través de los portales, este informe se encuentra detallado en el documento [Informe Mensual InfoTIC Seguridad Julio 2025.pdf](#),

A fin de mejorar la disponibilidad de los portales, nuestro Webmaster automatizó la tarea de administración de borrado de cache. Dicho despliegue se efectuó sobre los nodos 1 y 2 del portal ICETEX.

En cuanto a la disponibilidad del portal web de la entidad se presentan unos uptime superiores al 99,802% como se evidencia en la siguiente gráfica:

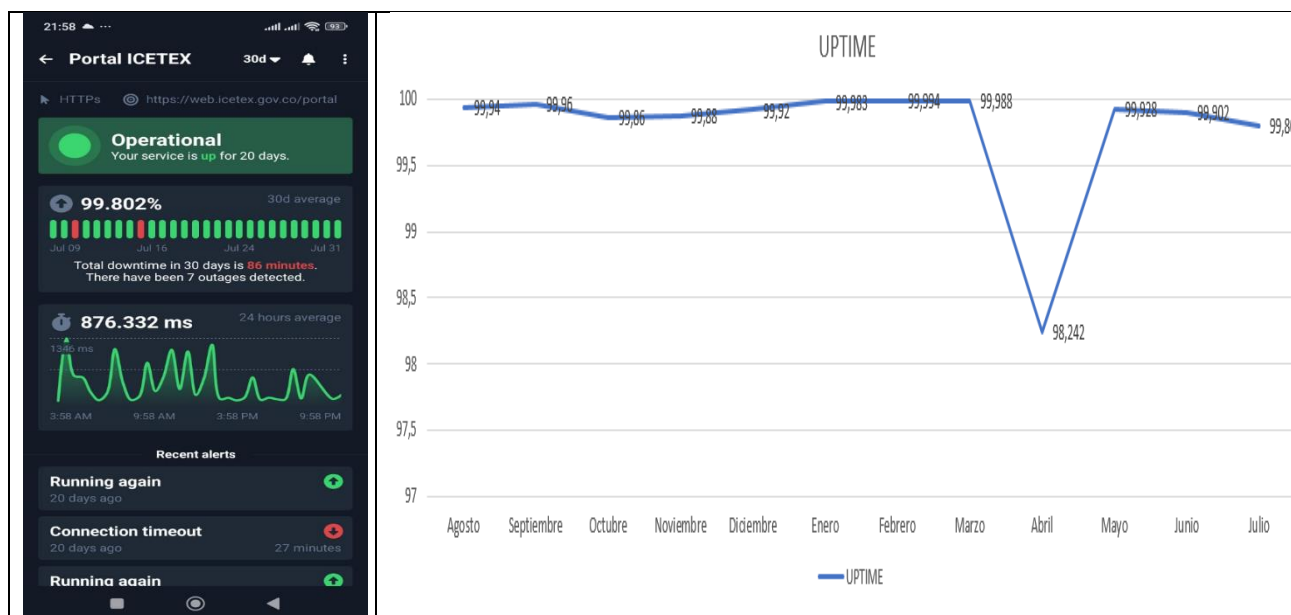


Ilustración 24 UPTIME: Portal WEB [web.icetex.gov.co](http://web.icetex.gov.co) [99,802%]

En cuanto al uso de recursos, estos se encuentran dentro de los umbrales normales, presentándose altos consumos en periodos particulares que corresponden a las solicitudes de actualizaciones y publicaciones de contenido en el portal web, incluye contenidos web, imágenes, banners, displays, videos, ADTs, fragmentos, actualización de URLs a través de la plantilla, redireccionamientos URL.

En el mes, se presenta un promedio de 1200GB de tráfico general hacia los portales protegidos por el FortiWeb donde el portal de [web.icetex.gov.co](http://web.icetex.gov.co) y [www.icetex.gov.co](http://www.icetex.gov.co) fueron los más utilizados en este periodo, lo cual es un comportamiento normal para este tipo de transacciones de acuerdo con la actividad de los usuarios y las convocatorias vigentes.

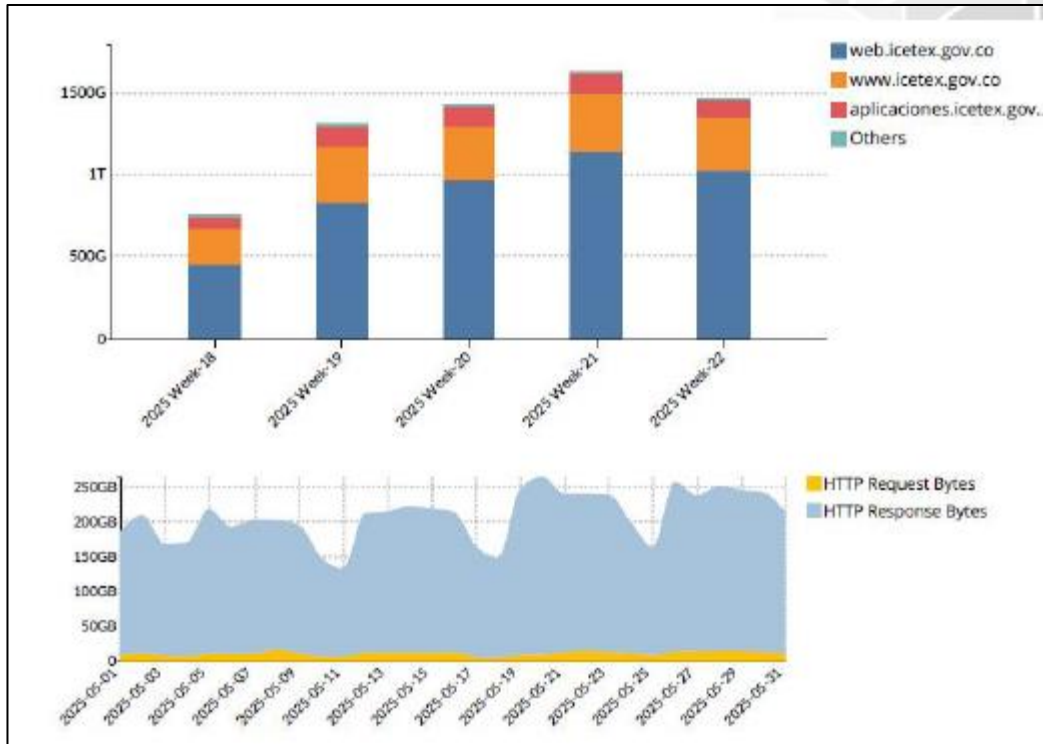


*Ilustración 25 Tráfico General De Los Portales*

En cuanto a los portales más utilizados, la estadística del presente mes es la siguiente:

| #  | HTTP Host                   | HTTP Request Bytes | HTTP Response Bytes |
|----|-----------------------------|--------------------|---------------------|
| 1  | web.icetex.gov.co           | 264.76 GB          | 4.01 TB             |
| 2  | www.icetex.gov.co           | 28.46 GB           | 1.44 TB             |
| 3  | aplicaciones.icetex.gov.co  | 36.87 GB           | 504.84 GB           |
| 4  | comunidad.icetex.gov.co     | 367.37 MB          | 26.19 GB            |
| 5  | portal.icetex.gov.co        | 675.65 MB          | 15.57 GB            |
| 6  | comunidad.icetex.gov.co:443 | 3.18 MB            | 403.22 MB           |
| 7  | web.icetex.gov.co:443       | 4.37 MB            | 235.40 MB           |
| 8  | identidad.icetex.gov.co     | 5.63 MB            | 129.57 MB           |
| 9  | web.icetex.gov.co:80        | 1.23 MB            | 121.79 MB           |
| 10 | www.icetex.gov.co:443       | 7.92 MB            | 117.60 MB           |

*Tabla 15 Top 10 Portales más utilizados*

Reiteramos nuestra solicitud relacionada con el soporte, por parte del fabricante, de la herramienta Liferay, aspecto que se ha informado en lo corrido del año 2025.

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

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. Actualmente el motor de búsqueda de amenazas está distribuido en cuatro criterios de búsqueda y correlación, los cuales son: compromiso del sistema, explotación

e instalación de agentes maliciosos, entrega y ataque, reconocimiento y sondeo y finalmente advertencia ambiental o anomalías detectadas sobre el rendimiento de la máquina. Dichos criterios distribuyen los alertas e incidentes de esta manera de acuerdo con el match que el sistema ejecute y categorice dentro de sus reglas de correlación previamente configuradas o implementadas por defecto. Las cuales detectan alertas e incidentes de tipo:

- Descarga de ejecutables sospechosos provenientes de un sitio de mala reputación
- Actividad de escaneo en la red, en función de descubrimiento de puertos
- Violación, infracción y vulneración de políticas de seguridad
- Detección de malware
- Detección de ataques (Fuerza Bruta, puerta trasera (Shell), Botnet o kit de explotación de un sitio malicioso, XSS, Inyección de SQL, DoS
- Monitoreo de alertas de autenticación
- Monitoreo de alertas de sistema
- Monitoreo de alarmas y alertas de seguridad
- Monitoreo de accesibilidad
- Monitoreo de bases de datos
- Alertas e incidentes de tráfico y navegación
- Alertas de acceso permitido a páginas web maliciosas o de baja reputación

A la fecha de presentación de este informe se encuentran definidas 2.370 reglas de seguridad, las cuales, tienen como fin reconocer cualquier posible vector de ataque, así como verificar que los equipos de seguridad perimetral (Firewall, IPS, NAC, etc.), estén bien configurados a nivel de sus políticas de seguridad.

Para los casos de uso de disponibilidad se cuenta con 170 reglas, que tienen como función principal alertar algún tipo de falla o indisponibilidad de los equipos de la entidad y hacer la respectiva notificación, en caso de requerirse, al ICETEX.

Para cualquier detalle relacionado con las reglas puede consultarse en el siguiente enlace [Informe Mensual SOC-TH ICETEX Julio 2025.pdf](#)

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

#### Indicadores de compromiso (IOC):

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

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

| Indicadores de compromiso (IOC) | Julio  | Junio  | Mayo   | Abril  | Marzo |
|---------------------------------|--------|--------|--------|--------|-------|
| IOC – Malware DOMINIOS          | 6.047  | 6.047  | 6.047  | 6.047  | 3.919 |
| IOC – Malware IPs               | 11.175 | 11.136 | 11.133 | 11.031 | 8.483 |
| IOC – Malware HASH              | 1.627  | 1.627  | 1.627  | 1.627  | 1.621 |
| IOC – Malware URL               | 4.564  | 4.564  | 4.564  | 4.564  | 780   |

*Tabla 16 Comparativo – Indicadores de Compromiso*

Después de efectuado el registro de alertas se considera y diseña la generación de alertas y niveles de criticidad, acorde con la experiencia del equipo consultor, aplicación de buenas prácticas y reuniones de trabajo efectuadas a nivel de infraestructura tecnológica alineado con el proceso de levantamiento de riesgos.

De acuerdo con las conexiones y las reglas configuradas sobre la herramienta de monitoreo SOC FortiSIEM, el cual analiza las alertas en busca de patrones de comportamiento inusuales; estas reglas estudian y conectan las alertas para evaluar su prioridad y confiabilidad.

En el Informe del SOC se presentan gráficas y tablas de los tipos de alertas presentados durante el periodo monitoreado de: Seguridad – Disponibilidad – Rendimiento, donde estos a su vez se encuentran distribuidos con niveles de severidad con tres colores:

- Rojo: severidad o criticidad ALTO (10-9)
- Amarillo: severidad o criticidad MEDIO (6-8)
- Verde: severidad o criticidad BAJO (1-5)

#### 4.3.3.1. Alertas o Incidentes de Seguridad Detectados

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

Destaca en este aspecto que El viernes 18 de julio de 2025, se realizó la notificación a ICETEX sobre el hallazgo reportado de un sitio fake <https://pagocreditoicetex.com/WebsitePSE/login.php> accediendo a información del ICETEX y efectuando actividades fraudulentas.

##### 4.3.3.1.1. Categoría Seguridad

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

| Severity | Cantidad de ... |
|----------|-----------------|
| Medium   | 9,711           |
| High     | 1,536           |
| Low      | 193             |

*Ilustración 26 Total de alertas de seguridad*

Durante el período evaluado de 11.440 alertas de seguridad identificadas, se presentaron con criticidad ALTA un total de 1.536 , equivalentes al 13% del periodo. En el informe mensual del SOC, se puede observar la cantidad según el tipo de alerta y se realiza una descripción de los tipos de alertas que mayor cantidad de

registros o que requieran una indagación más exacta. El comparativo, en los últimos 5 meses de 2025, se presenta a continuación:

| Severidad | Alertas de Seguridad julio | Alertas de Seguridad junio | Alertas de Seguridad mayo | Alertas de Seguridad abril | Alertas de Seguridad marzo |
|-----------|----------------------------|----------------------------|---------------------------|----------------------------|----------------------------|
| High      | 1.536                      | 825                        | 740                       | 2.897                      | 3630                       |
| Medium    | 9.711                      | 12.459                     | 9.806                     | 10.710                     | 15590                      |
| Low       | 193                        | 174                        | 198                       | 210                        | 266                        |

*Tabla 17 comparativo Alertas de Seguridad*

En cuanto a las alertas altas, el top 5 se presenta a continuación:

| Chart                               | Event Name                                                                | Criticidad | Criticidad | Tactica           | Cantidad de Alertas |
|-------------------------------------|---------------------------------------------------------------------------|------------|------------|-------------------|---------------------|
| <input checked="" type="checkbox"/> | Denegacion de Servicios desde Internet - WX Nivel3                        | High       | 9          | Impact            | 767                 |
| <input checked="" type="checkbox"/> | Critical large Outbound Transfer To Outside My Country ICETEX - WX N3     | High       | 9          |                   | 502                 |
| <input checked="" type="checkbox"/> | Trafico Permitido o Denegado Hacia IoC Maliciosas - WX Nivel3             | High       | 9          |                   | 69                  |
| <input checked="" type="checkbox"/> | Concurrent VPN Authentications To Same Account From Different Cities WXN2 | High       | 9          | Credential Access | 41                  |
| <input checked="" type="checkbox"/> | Successful VPN Logon From Outside My Country WXN2                         | High       | 9          | Credential Access | 32                  |

*Ilustración 27 Top 5 de Alertas de Seguridad Altas*

La alerta “Denegación de Servicios desde Internet - WX Nivel3” – esta alerta se genera cuando se detecta posible ataque de denegación de servicio (Dos - DDoS) basados en cantidad de tráfico.

La alerta: “Critical large Outbound Transfer To Outside My Country ICETEX - WX N3” – esta alerta se genera cuando se detecta una gran transferencia saliente (más de 10 GB en 40 minutos) desde un host interno a un destino externo que está fuera de mi país. Se recomienda verificar los envíos masivos hacia internet.

La alerta “Tráfico Permitido o Denegado hacia IP IoC Maliciosas - WX Nivel3” – La alerta se genera cuando se detecta de Tráfico permitido o denegado hacia Dominios, IP, HASH y URL, relacionadas en Indicadores de Compromiso - IoC de Malware recopilas por WX Nivel3.

Lo anterior indica que el equipo con IP Origen probablemente está infectado por malware y está intentando conexiones a servidores de comando y control (C&C) independientemente si fue negado o permitido el tráfico. A pesar de que muchas de las direcciones ip destino ya están bloqueadas lo anómalo es que un host de la red privada quiere establecer comunicación con direcciones sospechosas.

La alerta: “Concurrent VPN Authentications To Same Account From Different Cities WXN2” – esta alerta se genera cuando se detectan intentos de autenticaciones VPN simultáneas a la misma cuenta en un corto período de tiempo desde diferentes ciudades.

Al momento de verificar los eventos que generaron las alertas, se observa que estos corresponden a intentos de fuerza bruta con usuarios genéricos (helpdesk, guest, intranet, etc) hacia el servicio de la VPN SSL WEB. Se corroborar que en su gran mayoría, por no decir en su totalidad los eventos marcan como conexiones fallidas debido a que el usuario es desconocido y la razón de la alerta es que se intentaron los mismos usuarios desde 2 o más direcciones IP distintas en especial en ciudades de estados unidos. Se recomienda liminar la exposición de estos servicios a internet, ya sea a través del filtrado de direcciones IP o países con los cuales se tenga previstas la conexiones VPN.

La alerta “Successful VPN Logon From Outside My Country”– se genera cuando se detecta inicios de sesión éxitos por VPN desde otros países diferentes al país origen de la entidad. Se ajustó la regla para que no trajese el evento ssl-vpn-session-tunnel-up ya que no se considera una conexión exitosa.

#### 4.3.3.1.2. Categoría Disponibilidad

Durante el período evaluado se presentaron 2419 alertas de disponibilidad con criticidad ALTA, a continuación, se puede observar la cantidad según el tipo de alerta y se realiza una descripción de los tipos de alertas que mayor cantidad de registros presentaron y se realiza una descripción de los tipos de alertas que mayor cantidad de registros presentaron:

| Event Name                                                              | Criticidad | Criticidad | Tactica | Cantidad de Alertas |
|-------------------------------------------------------------------------|------------|------------|---------|---------------------|
| Network Device Down: no ping response - WX N3                           | High       | 10         | Impact  | 2,226               |
| Server Down: No Ping Response ICETEX                                    | High       | 10         |         | 1                   |
| SNMP Service Unavailable                                                | High       | 9          | Impact  | 170                 |
| EventDB: Event Retention Policy Violation                               | High       | 9          |         | 6                   |
| WMI or OMI Service Unavailable                                          | High       | 9          | Impact  | 6                   |
| FortiSIEM Agent Operational Error WXN2                                  | High       | 9          |         | 3                   |
| FortiSIEM Performance Monitoring Relay Not Working: All Devices delayed | High       | 9          |         | 3                   |
| FortiSIEM EPS License Exceeded                                          | High       | 9          |         | 1                   |
| Excessive Clock Skew Between Collector and Supervisor nodes             | High       | 9          |         | 1                   |
| Excessive External Event Dropped By License                             | High       | 9          |         | 1                   |
| Scheduled Report Send Error                                             | High       | 9          |         | 1                   |

*Ilustración 28 Top 5 de Alertas de Disponibilidad Altas*

A continuación, se presentan los análisis efectuados:

- “Network Device Down: no ping response - WX N3” – se genera cuando Detecta que un dispositivo no responde al ping. Se pierden 10 de cada 10 paquetes de ping. Esto puede deberse a que el host está inactivo o a un problema de enrutamiento.
- “EventDB: Event Retention Policy Violation” – se genera cuando Detecta violaciones de la política de retención de eventos. Esto podría indicar que se están eliminando, modificando o reteniendo logs de manera parcial, incumpliendo las políticas definidas por la entidad.
- “WMI or OMI Service Unavailable” – Esta alerta se genera cuando Detecta que el servicio WMI u OMI no está disponible. Nota: Se recomienda verificar el estado de los protocolos WMI de los dispositivos relacionados, los cuales se utilizan para enviar eventos de seguridad al SIEM; de lo contrario informar al SOC si el dispositivo se encuentra fuera de servicio con el fin de depurar y actualizar la base de datos del FortiSIEM – CMDB.
- “FortiSIEM Agent Operational Error WXN2” – Esta alerta se genera cuando se detectan errores operativos del agente FortiSIEM Linux/Windows: se desinstala, se detiene y no responde.
- “Excessive Clock Skew Between Collector and Supervisor nodes” – Esta alerta se genera cuando Detecta un desfase de reloj de más de 2 minutos entre el collector y el supervisor; esto provocará que las reglas en tiempo real no se activen para los eventos recibidos de ese recopilador.

#### 4.3.3.1.3. Amenazas de Ciberseguridad

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

- **Top Ataques IPS:** Se representa el Top de los ataques IPS permitidos y denegados detectados por los dispositivos de ciberseguridad perimetral. Se recomienda el bloqueo de los ataques de severidad alta detectados por el IPS y verificar los eventos o alertas de severidad media.

| Reporting Device                | Attack Name                     | Signature Id | Severity | Firewall Action | COUNT(Match... |
|---------------------------------|---------------------------------|--------------|----------|-----------------|----------------|
| 71 DC_FG_MST_ICETEX.icetex.L... | DNS PTR Records Scan            | 51391        | Low      | detected        | 7,395          |
| 2 DCAGUAS_FG_MST_ICETEX         | TCP Split Handshake             | 26339        | Medium   | detected        | 69             |
| 2 DCAGUAS_FG_MST_ICETEX         | Malicious File Downloading      | 32978        | Medium   | detected        | 12             |
| 71 DC_FG_MST_ICETEX.icetex.L... | Apache Camel XSLT Component XXE | 38143        | Medium   | detected        | 12             |
| 71 DC_FG_MST_ICETEX.icetex.L... | Malicious File Downloading      | 32978        | Medium   | detected        | 12             |

Ilustración 29 ataques IPS permitidos

| Reporting Device                | Attack Name                           | Signature Id | Severity | Firewall Action | COUNT(Match... |
|---------------------------------|---------------------------------------|--------------|----------|-----------------|----------------|
| 71 DC_FG_MST_ICETEX.icetex.L... | Nmap Script Scanner                   | 45360        | Medium   | dropped         | 1,047          |
| 71 DC_FG_MST_ICETEX.icetex.L... | PHPUnit Eval stdin PHP Remote Cod...  | 45765        | Medium   | dropped         | 982            |
| 71 DC_FG_MST_ICETEX.icetex.L... | ZGrab Scanner                         | 48805        | Medium   | dropped         | 698            |
| 71 DC_FG_MST_ICETEX.icetex.L... | Web Server Password File Access       | 43336        | Medium   | dropped         | 458            |
| 71 DC_FG_MST_ICETEX.icetex.L... | SystemBC Botnet                       | 49827        | Medium   | dropped         | 270            |
| 71 DC_FG_MST_ICETEX.icetex.L... | HTTP URI SQL Injection                | 15621        | Medium   | dropped         | 247            |
| 71 DC_FG_MST_ICETEX.icetex.L... | Remote CMD Shell                      | 12449        | Medium   | dropped         | 218            |
| 71 DC_FG_MST_ICETEX.icetex.L... | Bash Function Definitions Remote C... | 39294        | Medium   | dropped         | 201            |
| 71 DC_FG_MST_ICETEX.icetex.L... | Censys.io Scanner                     | 50899        | Medium   | dropped         | 195            |
| 71 DC_FG_MST_ICETEX.icetex.L... | Generic Path Traversal Detection      | 56270        | Medium   | dropped         | 139            |
| 71 DC_FG_MST_ICETEX.icetex.L... | WordPress REST API Username Enu...    | 48072        | Medium   | dropped         | 135            |
| 71 DC_FG_MST_ICETEX.icetex.L... | Linux Kernel TCP SACK Panic DoS       | 48103        | Medium   | dropped         | 125            |
| 71 DC_FG_MST_ICETEX.icetex.L... | Citrix SD-WAN Center Command Inj...   | 48208        | Medium   | dropped         | 88             |
| 71 DC_FG_MST_ICETEX.icetex.L... | Multiple Routers GPON formLogin R...  | 52588        | Medium   | dropped         | 73             |
| 71 DC_FG_MST_ICETEX.icetex.L... | Oracle WebLogic Server wls-wsat C...  | 45334        | Medium   | dropped         | 73             |

Ilustración 30 ataques IPS denegados

- **Top Perímetro:** A continuación de presentan el TOP de los eventos o tráfico de red organizado por los puertos TCP/UDP que más recibieron o enviaron bytes hacia Internet. Principales Puertos Entrantes por Conexiones (Tráfico Permitido).

| IP Protocol | Destination TCP/UDP Port | COUNT(Matched Events) | SUM(Sent Bytes64) | SUM(Received Bytes64) | SUM(Total Bytes64) |
|-------------|--------------------------|-----------------------|-------------------|-----------------------|--------------------|
| 6 (TCP)     | 443 (HTTPS)              | 46,099,100            | 10.61 TB          | 25.94 TB              | 36.55 TB           |
| 17 (UDP)    | 443                      | 666,277               | 69.91 GB          | 192.50 GB             | 262.49 GB          |
| 6 (TCP)     | 80 (HTTP)                | 299,046               | 2.02 GB           | 64.93 GB              | 66.95 GB           |
| 1 (ICMP)    | 0                        | 229,535               | 17.67 MB          | 17.67 MB              | 35.35 MB           |
| 17 (UDP)    | 53 (DOMAIN)              | 160,787               | 110.67 MB         | 214.31 MB             | 324.98 MB          |
| 6 (TCP)     | 440 (SGCP)               | 63,103                | 244.59 MB         | 1.66 GB               | 1.9 GB             |
| 6 (TCP)     | 458 (APPLEQTC)           | 47,933                | 154.78 GB         | 3.19 GB               | 157.97 GB          |
| 6 (TCP)     | 5228                     | 44,143                | 2.78 GB           | 3.63 GB               | 6.41 GB            |
| 17 (UDP)    | 547 (DHCPV6-SERVER)      | 24,278                | 121.24 MB         | 910.65 KB             | 122.13 MB          |
| 17 (UDP)    | 123 (NTP)                | 16,138                | 1.46 MB           | 722.51 KB             | 2.16 MB            |
| 6 (TCP)     | 5222                     | 15,284                | 2.56 GB           | 4.83 GB               | 7.39 GB            |
| 17 (UDP)    | 3478                     | 13,424                | 40.58 GB          | 83.31 GB              | 123.9 GB           |
| 17 (UDP)    | 389 (LDAP)               | 12,246                | 3.16 MB           | 2.44 MB               | 5.6 MB             |
| 17 (UDP)    | 500 (IPSec1)             | 6,266                 | 20.99 MB          | 22.52 MB              | 43.52 MB           |
| 6 (TCP)     | 447 (DDM-DFM)            | 5,926                 | 23.18 MB          | 263.1 MB              | 286.29 MB          |

*Ilustración 31 Puertos entrantes de público a privado (Permitidos)*

Se recomienda verificar si es necesario mantener expuestos a internet de los siguientes puertos conocidos como el 53 (DOMAIN), 123 (NTP) los cual comúnmente son autorizados como puertos de salida y no de entrada, así mismo confirmar otros puertos conocidos como el 440 (SGCP), 458 (APPLEQTC), 547 (DHCP) 447 (DDM-DFM), 389 (LDAP) los cuales en su mayoría son utilizados en entornos LAN o privados.

#### Principales Puertos Salientes por Conexiones (Tráfico Permitido)

| IP Protocol | Destination TCP/UDP Port | COUNT(Matched Events) | SUM(Sent Bytes64) | SUM(Received Bytes64) | SUM(Total Bytes64) |
|-------------|--------------------------|-----------------------|-------------------|-----------------------|--------------------|
| 6 (TCP)     | 443 (HTTPS)              | 319,930,109           | 110.36 TB         | 153 TB                | 263.36 TB          |
| 17 (UDP)    | 53 (DOMAIN)              | 52,717,496            | 30.18 GB          | 280.23 GB             | 310.42 GB          |
| 17 (UDP)    | 443                      | 46,306,298            | 4.3 TB            | 11.99 TB              | 16.29 TB           |
| 6 (TCP)     | 80 (HTTP)                | 21,866,691            | 52.11 TB          | 5.95 TB               | 58.06 TB           |
| 6 (TCP)     | 25 (SMTP)                | 7,735,554             | 5.64 GB           | 10.79 GB              | 16.44 GB           |
| 6 (TCP)     | 5228                     | 4,444,535             | 218.34 GB         | 319.47 GB             | 537.81 GB          |
| 6 (TCP)     | 4001 (Moxa Modbus RTU)   | 3,477,092             | 698.82 MB         | 1023.45 MB            | 1.87 GB            |
| 6 (TCP)     | 587 (SUBMISSION)         | 2,275,561             | 4.63 GB           | 3.87 GB               | 8.5 GB             |
| 17 (UDP)    | 123 (NTP)                | 2,118,006             | 807.28 GB         | 804.81 GB             | 1.57 TB            |
| 6 (TCP)     | 8810                     | 1,880,147             | 244.61 GB         | 235.57 GB             | 480.19 GB          |
| 17 (UDP)    | 3478                     | 1,512,247             | 3.87 TB           | 7.56 TB               | 11.44 TB           |
| 6 (TCP)     | 5222                     | 1,500,143             | 245.85 GB         | 596.85 GB             | 842.71 GB          |
| 17 (UDP)    | 4000 (ICQ)               | 1,379,688             | 48.15 GB          | 104.75 GB             | 152.9 GB           |
| 6 (TCP)     | 8812                     | 1,232,592             | 3.91 TB           | 6.33 TB               | 10.24 TB           |
| 6 (TCP)     | 8445                     | 705,836               | 411.69 GB         | 19.44 TB              | 19.84 TB           |

*Ilustración 32 Puertos saliente de público a privado (Permitidos)*

Se recomienda verificar si es necesario mantener tráfico hacia internet a través de los siguientes puertos conocidos como: 4001(Moxa Modbus RTU – Protocolo usado en entornos industriales/SCADA), 25(SMTP – Envío de correo electrónico no seguro), 5228(Google Play Services – Utilizado por dispositivos Android para actualizaciones), 4000(Mensajería ICQ, obsoleta y desactualizada)

## Top de Accesos Fallidos plataforma Windows:

| Source IP        | User          | Server                   | COUNT(Mat... |
|------------------|---------------|--------------------------|--------------|
| 10.2.254.216     | drodriguez    | 51 ictxsrvfs.icetex.l... | 1,160        |
| 40 172.16.224.65 | lparrac       | 51 ictxsrvfs.icetex.l... | 1,033        |
| 6 172.16.225.47  | jhernandezb   | 51 ictxsrvfs.icetex.l... | 782          |
| 34 192.168.61.1  | 28 aleimbachi | 41 MIRA                  | 550          |
| 10.2.254.215     | 12 jalberson  | 51 ictxsrvfs.icetex.l... | 498          |
| 10.2.254.101     | User          | 51 ictxsrvfs.icetex.l... | 479          |
| 10.2.254.216     | 12 jalberson  | 51 ictxsrvfs.icetex.l... | 435          |
| 10.2.254.2       | jpforero      | 51 ictxsrvfs.icetex.l... | 423          |
| 43 172.16.224.90 | 32 Londono    | 51 ictxsrvfs.icetex.l... | 402          |
| 10.2.254.1       | jpforero      | 51 ictxsrvfs.icetex.l... | 372          |

Ilustración 33 Fallos de Inicio de sesión Windows

| Source IP     | User      | Server                | COUNT(Mat... |
|---------------|-----------|-----------------------|--------------|
| 172.22.16.179 | C45082779 | icetexbogbalserver1-r | 124          |
| 172.22.16.179 | C46257933 | icetexbogbalserver1-r | 6            |
| 172.22.16.179 | C46099964 | icetexbogbalserver1-r | 1            |
| 172.22.16.179 | C46276576 | icetexbogbalserver1-r | 1            |

Ilustración 34 Fallos de Inicio de sesión Unix

| Reporting IP | User        | COUNT(Mat... |
|--------------|-------------|--------------|
| 192.1.1.15   | ldiaza      | 113          |
| 192.1.1.15   | dlacera     | 64           |
| 192.1.1.15   | lrojasm     | 61           |
| 192.1.1.15   | jruizcap    | 57           |
| 192.1.1.15   | yrodriguezr | 43           |
| 192.1.1.15   | nbaron      | 41           |
| 192.1.1.15   | scanner     | 40           |
| 192.1.1.15   | DCANO       | 38           |
| 192.1.1.15   | 35 MCORTESL | 37           |
| 192.1.1.15   | abc         | 33           |

Ilustración 35 Fallos de Inicio de sesión VPN

| Server                    | User    | COUNT(Mat... |
|---------------------------|---------|--------------|
| 51 ictxsrvfs.icetex.local | Soporte | 4            |

*Ilustración 36 Cuentas bloqueados*

#### 4.3.3.1.4. Threat Hunting

Se lleva a cabo el proceso de "Threat Hunting" de manera proactiva mediante la realización de boletines de ciber amenazas y la utilización de la plataforma MISP (Malware Information Sharon Platform) del First (Forum of Incident Response Team), los boletines pueden ser consultado en el numeral 4.4 Boletines del [Informe Mensual SOC-TH ICETEX Julio 2025.pdf](#)

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

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

Los indicadores de compromiso - IoC fueron recopilados por intercambio de información con algunas instituciones del Estado Colombiano, inteligencia de amenazas en plataformas públicas o privadas, como el FIRST, CISA, CSIRT'S y caza de amenazas en plataformas de ciberseguridad. Los análisis de dichos indicadores, así como sus recomendaciones se encuentran consignados en el documento [Informe Mensual SOC-TH ICETEX Julio 2025.pdf](#), es importante resaltar que Todo el tráfico fue bloqueado, sin embargo, se recomienda la verificación de los equipos con las direcciones IP origen privada.

#### 4.3.4. Análisis de Vulnerabilidades ICETEX

En julio de 2025 se realizó la Fase 6 del análisis de vulnerabilidades sobre 76 servidores críticos, con una cobertura total del 100%. Se identificaron 28 vulnerabilidades, destacando varias de criticidad alta y crítica, incluyendo sistemas sin soporte oficial (como versiones obsoletas de VMware vCenter y Microsoft SQL Server), vulnerabilidades en servicios de transferencia de archivos (CVE-2024-0204) y ejecución remota autenticada en entornos VMware (CVE-2025-41225).

También se detectaron configuraciones inseguras en SMB y RDP, uso de algoritmos criptográficos débiles (RC4, SWEET32, claves RSA <2048 bits), certificados SSL firmados con algoritmos inseguros o próximos a expirar, así como exposición innecesaria de servicios web y directorios explorables. Estos hallazgos refuerzan la necesidad de priorizar acciones de remediación en plataformas, configuraciones y controles criptográficos, conforme a estándares como NIST, ISO/IEC 27001:2022 y OWASP.

Se mantiene un alto nivel de obsolescencia tecnológica en componentes clave, lo que incrementa el riesgo general de la infraestructura. Los hallazgos actuales respaldan la necesidad de priorizar acciones correctivas y mejoras en configuración y actualización de sistemas.

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

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

A 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 Julio2025.pdf](#)

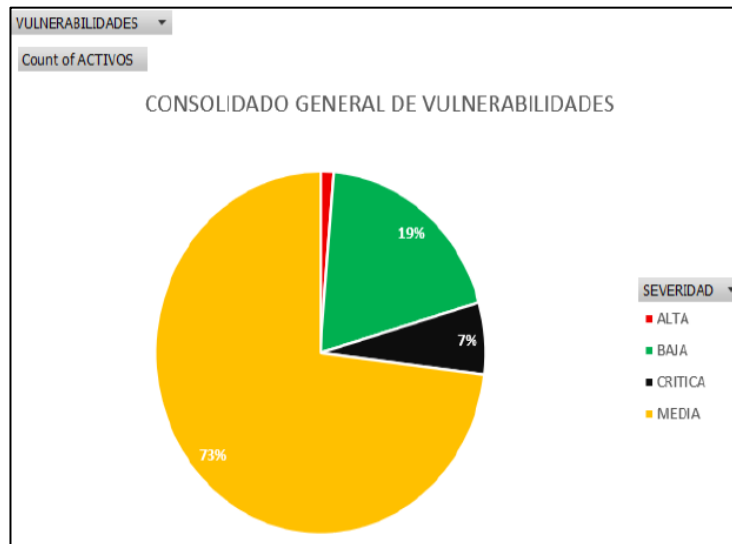


*Ilustración 37 Cantidad Total de Hallazgos identificados*

#### 4.3.4.1. Resumen de Vulnerabilidades

La recomendación fundamental es desarrollar e implementar un plan de mitigación de vulnerabilidades, priorizando la actualización tecnológica, el fortalecimiento de protocolos y la migración a versiones de la plataforma base (sistemas operativos, bases de datos, etc). Para efectos de apoyar el cierre de vulnerabilidades, según requerimientos de ICETEX, se sugiere realizar una mesa técnica para revisar las alternativas de solución.

El resumen de las vulnerabilidades se puede revisar a más detalle en el numeral 11. Resumen de vulnerabilidades del [Informe Técnico Análisis De Vulnerabilidades ICETEX Julio2025.pdf](#)

Destacan en los hallazgos las siguientes vulnerabilidades:

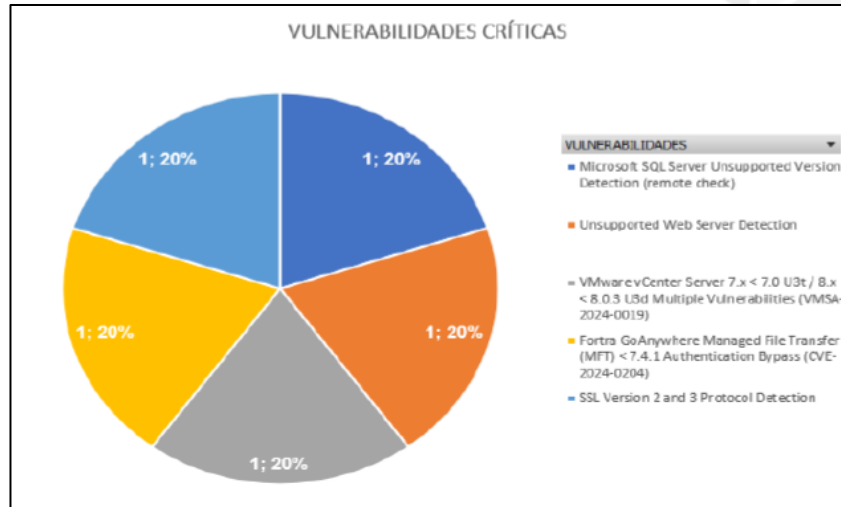


*Ilustración 38 Vulnerabilidades Críticas*

#### 4.3.4.2. Conclusiones Vulnerabilidades

La evaluación de vulnerabilidades correspondiente a la Fase 6, evidencia que, si bien existen avances puntuales, persisten riesgos críticos que afectan directamente la seguridad y disponibilidad de los activos tecnológicos. La presencia de sistemas sin soporte, configuraciones débiles en SMB, RDP y servicios web, y el uso de componentes criptográficos obsoletos, confirma una superficie de ataque amplia y explotable.

Esta situación se ve agravada por la proximidad del fin de soporte de varios sistemas utilizados, lo que pone en evidencia la necesidad urgente de acciones correctivas. En este contexto, se concluye que es necesario adoptar un enfoque técnico y estratégico, que incluya medidas inmediatas de remediación y una planificación estructurada de modernización tecnológica.

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

- **Actualizar y migrar sistemas sin soporte:** Reemplazar sistemas Windows sin soporte (VULN-001) y servidores web no compatibles (VULN-002) por versiones actualizadas que reciban mantenimiento de seguridad activo.
- **Aplicar Parches críticos.** Priorizar la mitigación de la vulnerabilidad BlueKeep (VULN-003 / CVE-2019-0708) mediante la instalación de parches oficiales, desactivación de RDP si no es necesario, y segmentación de red para limitar el alcance.
- **Endurecer configuraciones de red y servicios**
  - SMB: Deshabilitar SMBv1 y habilitar la firma de SMB.
  - Restringir métodos HTTP peligrosos como TRACE / TRACK (VULN-007).
  - Inhabilitar el listado de directorios web navegables (VULN-009) en servidores públicos o expuestos
- **Mejorar la seguridad de los servicios de escritorio remoto:**
  - Configurar Network Level Authentication (NLA) obligatoria (VULN-012).
  - Elevar el nivel de cifrado en RDP a FIPS-140 o equivalente (VULN-010, VULN-013).
  - Corregir vulnerabilidades relacionadas con ataques Man-in-the-Middle (VULN-005).

➤ **Fortalecer la gestión de certificados y cifrado**

- Renovar certificados SSL cercanos a expiración (VULN-008).
- Sustituir algoritmos de hashing débiles (VULN-006), como MD5 o SHA-1, por SHA-256 o superior.

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

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

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

#### **4.3.5. Reporte De Ips**

Del reporte de IPS [Reporte de IPS de Julio infotic 2025.pdf](#) se observan para el mes de julio algunos eventos permitidos por el IPS de TCP.Split.Handshake con orígenes desde redes internas eso debido a que se ha venido ajustando los perfiles de IPS pero aún falta hacerlo para esta firma como visualiza en el reporte.

Se recomienda aislar completamente la red de wifi invitados la del Icetex de la red de Icetex ya que pueden realizarse movimientos laterales y contaminar, es de saber que esta red no se puede tener algún control, pero se deben realizar también de filtros de consumo como shapers, en cuanto a la firma de IPS se tienen hace match con un indicador malicioso y se debe ajustar la firma para que realice el respectivo bloqueo. Para más información validar el enlace: <https://www.fortiguard.com/encyclopedia/ips/32978/malicious-file-downloading>.

Se recomienda seguir realizando bloqueos en el firewall de aguas de la firma TCP.Split.Handshake y aplicar los perfiles en las políticas según tráfico de origen ( wifi vip 172.16.224.0/22), según la recomendación del fabricante <https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-block-the-TCP-split-handshake-in-intrusion/ta-p/239186>.

Se observa que se detectó la firma en el IPS del firewall de triara Apache.Camel.XSLT.Component.XXE con la ip publica de origen 108.61.200.118 a la url destino [www.icetex.gov.co](http://www.icetex.gov.co) con ip del waf 192.168.91.17 ( información sobre la firma Intrusion Prevention | FortiGuard Labs), por lo tanto, se recomienda que se habilite en ips esta firma y que también la ip sea bloqueada.

#### **4.4. Servicios de nube**

Se recomienda que el ICETEX delegue a un responsable para temas de nube, con quien se puedan coordinar las labores de escalamientos internos y toma de decisiones, dado que, a la fecha de presentación de este informe, no contamos con este interlocutor.

Con el fin de elaborar recomendaciones de migración a la nube se requiere, por parte del ICETEX, del inventario de aplicaciones y máquinas virtuales que se planean migrar a la nube con el fin de efectuar un análisis y proceder a proponer alternativas tendientes a optimizar los recursos en el ICETEX.

Con el propósito de dar solución al boletín de seguridad titulado "**Boletín de seguridad COLCERT Fin del Soporte de Windows 10**", remitido el pasado mes de Febrero y, tras socializar la lista de máquinas virtuales con Windows 10 existentes en Azure se recomienda, como indican las mejores prácticas proporcionadas por el fabricante MicroSoft, la creación de estas máquinas en su versión de Windows 11 descartando la actualización directa de Windows 10 a Windows 11 en la misma máquina, pues es excesiva en costos.

Microsoft ha extendido el plazo hasta Octubre 14 del 2025 para realizar estas actualizaciones, por lo que se recomienda de forma urgida, al ICETEX, adelantar esta labor.

## 5. GESTION DE LA EJECUCIÓN CONTRACTUAL

El contrato 2022-0792 con fecha de perfeccionamiento del acta de inicio del 30 de diciembre del 2022, donde se establece un plazo del contrato de 39 meses, el cual se compone de una fase de transición de 3 meses y una fase de operación de 36 meses, el plazo comenzó a contar a partir de la firma del acta de inicio que fue el 12 de enero del 2023, y la ejecución de los servicios en fase de operación el 1 de abril de 2024, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato, es de aclarar que la fase de transición no es facturable.

En el presente informe del mes de julio del 2025 del proyecto, se encuentra en la fase de operación de los servicios contemplados en el alcance llevando ejecutados 28 meses que equivale al 77,7% de avance, para lo cual INFOTIC presenta:

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

## 6. GESTION PRESUPUESTAL

A continuación, se relacionan los pagos realizados por ICETEX a INFOTIC durante la ejecución del proyecto, de acuerdo con los informes presentados con la evidencia de las actividades realizadas:

| EJECUCIÓN PRESUPUESTAL     |                      |                      |                           |                            |                         |
|----------------------------|----------------------|----------------------|---------------------------|----------------------------|-------------------------|
| VALOR INICIAL DEL CONTRATO | VALOR VIGENCIA 2023  | VALOR EJECUTADO 2023 | VALOR BOLSA VIGENCIA 2023 | VALOR BOLSA EJECUTADO 2023 | VALOR NO EJECUTADO 2023 |
| \$ 31.398.996.857,96       | \$ 7,849,749,214.53  | \$5,550,607,398.60   | \$360,000,000             | \$2.700.000                | \$ 1,936,441,815.93     |
|                            | VALOR VIGENCIA 2024  | VALOR EJECUTADO 2024 | VALOR BOLSA VIGENCIA 2024 | VALOR BOLSA EJECUTADO 2024 | VALOR NO EJECUTADO 2024 |
|                            | \$ 10,466,332,286.04 | \$8,116,163,716.21   | \$480,000,000             | \$0                        | \$ 1,870,168,569.83     |
|                            | VALOR VIGENCIA 2025  | VALOR EJECUTADO 2025 | VALOR BOLSA VIGENCIA 2025 | VALOR BOLSA EJECUTADO 2025 | VALOR NO EJECUTADO 2025 |
|                            | \$ 10,466,332,286.04 | \$ 5,409,941,717     | \$480,000,000             | \$0                        | \$5,056,390,569.33      |
| CONCEPTO                   |                      |                      |                           |                            |                         |
| CONCEPTO                   |                      |                      |                           |                            | VALOR                   |
| VALOR TOTAL DEL CONTRATO   |                      |                      |                           |                            | \$ 31,398,996,857.96    |
| VALOR PAGADO               |                      |                      |                           |                            | \$ 17,519,048,629       |
| Pago No. 1 -               | mes:                 | Abril                | de                        | 2023                       |                         |
|                            |                      |                      |                           | \$ 537.090.736,00          |                         |
| Pago No. 2 -               | mes:                 | Mayo                 | de                        | 2023                       |                         |
|                            |                      |                      |                           | \$ 544.104.546,00          |                         |
| Pago No. 3 -               | mes:                 | Junio                | de                        | 2023                       |                         |
|                            |                      |                      |                           | \$ 596.978.314,00          |                         |
| Pago No. 4 -               | mes:                 | Julio                | de                        | 2023                       |                         |
|                            |                      |                      |                           | \$ 624.431.841,60          |                         |
| Pago No. 5 -               | mes:                 | Agosto               | de                        | 2023                       |                         |
|                            |                      |                      |                           | \$ 650.825.466,00          |                         |
| Pago No. 6 -               | mes:                 | Septiembre           | de                        | 2023                       |                         |
|                            |                      |                      |                           | \$ 661.959.450,00          |                         |
| Pago No. 7 -               | mes:                 | Octubre              | de                        | 2023                       |                         |
|                            |                      |                      |                           | \$ 641.792.285,00          |                         |
| Pago No. 8 -               | mes:                 | Noviembre            | de                        | 2023                       |                         |
|                            |                      |                      |                           | \$ 633,094,717.00          |                         |
| Pago No. 9 -               | mes:                 | Diciembre            | de                        | 2023                       |                         |
|                            |                      |                      |                           | \$ 663.076.196,00          |                         |
| Pago No. 10 -              | mes:                 | Enero                | de                        | 2024                       |                         |
|                            |                      |                      |                           | \$ 681.934.328,00          |                         |

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

|                                                                                                                                                           |      |            |    |      |                    |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------|------------|----|------|--------------------|--|
| Pago No. 11 -                                                                                                                                             | mes: | Febrero    | de | 2024 | \$ 732,950,102.00  |  |
| Pago No. 12 -                                                                                                                                             | mes: | Marzo      | de | 2024 | \$ 733.890.372,09  |  |
| Pago No. 13 -                                                                                                                                             | mes: | Abril      | de | 2024 | \$ 730,351,368.00  |  |
| Pago No. 14 -                                                                                                                                             | mes: | Mayo       | de | 2024 | \$ 719,104,204.57  |  |
| Pago No. 15 -                                                                                                                                             | mes: | Junio      | de | 2024 | \$ 713,673,218.00  |  |
| Pago No. 16 -                                                                                                                                             | mes: | Julio      | de | 2024 | \$ 751,372,731.00  |  |
| Pago No. 17 -                                                                                                                                             | mes: | Agosto     | de | 2024 | \$755,684,192.00   |  |
| Pago No. 18 -                                                                                                                                             | mes: | Septiembre | de | 2024 | \$ 752,502,515.00  |  |
| Pago No. 19 -                                                                                                                                             | mes: | Octubre    | de | 2024 | \$ 770,522,532.00  |  |
| Pago No. 20 -                                                                                                                                             | mes: | Noviembre  | de | 2024 | \$ 774,178,154.00  |  |
| Pago No. 21 -                                                                                                                                             | mes: | Diciembre  | de | 2024 | \$ 772,219,902.00  |  |
| Pago No. 22 -                                                                                                                                             | mes: | Enero      | de | 2025 | \$ 740,982,385.00  |  |
| Pago No. 23 -                                                                                                                                             | mes: | Febrero    | de | 2025 | \$ 771,789,618.00  |  |
| Pago No. 24 -                                                                                                                                             | mes: | Marzo      | de | 2025 | \$ 786,219,135.00  |  |
| Pago No. 25 -                                                                                                                                             | mes: | Abril      | de | 2025 | \$ 778,320,320.00  |  |
| Pendiente - Pago No. 26 -                                                                                                                                 | mes: | Mayo       | de | 2025 | \$ 778,015,139.00  |  |
| Pendiente - Pago No. 27 -                                                                                                                                 | mes: | Junio      | de | 2025 | \$ 776,103,223.00  |  |
| Pendiente - Pago No. 28 -                                                                                                                                 | mes: | Julio      | de | 2025 | \$ 778,511,897.00* |  |
| VALOR CAUSADO QUE NO SE HA PAGADO (valor a pagar factura) *                                                                                               |      |            |    |      | \$ 778,511,897.00  |  |
| VALOR TOTAL EJECUTADO (valor pagado + valor causado no pagado)                                                                                            |      |            |    |      | \$ 19,851,678,888  |  |
| SALDO DEL CONTRATO (valor total del contrato – valor total ejecutado)                                                                                     |      |            |    |      | \$ 11,547,317,970  |  |
| PORCENTAJE DE EJECUCIÓN                                                                                                                                   |      |            |    |      | 63.22%             |  |
| * 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 18 Ejecución Presupuestal

## 7. GESTION ADMINISTRATIVA

### 7.1. Profesionales

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

| Perfiles                        | Especialistas                                                       | Anexo                                                                              |
|---------------------------------|---------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Especialista Bases de datos DBA | Edgar Cobos Mayorga<br>Johan Cardozo - Apoyo                        | <a href="#">Informe Mensual InfoTIC DBA Julio 2025.pdf</a>                         |
| Especialista Web Máster         | Juan Carlos Martínez Sierra                                         | <a href="#">Informe Mensual InfoTIC Webmaster Julio 2025.pdf</a>                   |
| Especialista Integrador de nube | Jose Luis Mantilla Guiza                                            | <a href="#">Informe Mensual InfoTIC Integrador de Nube Julio 2025.pdf</a>          |
| Especialistas de Seguridad      | Jhon Alveiro Pava González<br>Edwin Morales                         | <a href="#">Informe Mensual InfoTIC Seguridad Julio 2025.pdf</a>                   |
| Especialistas de soluciones     | Jose Francisco Escobar Escorcía<br>Davis Alexander Mogollón Fandiño | <a href="#">Informe Mensual InfoTIC Administrador de Soluciones Julio 2025.pdf</a> |
| Especialista de Networking      | Carlos Alberto Roldan Ríos<br>Cristian Salgado - Apoyo              | <a href="#">Informe Mensual InfoTIC Administrador de Redes Julio 2025.pdf</a>      |

Tabla 19 Perfiles y Actividades

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

| NOMBRE COMPLETO                 | ROL RESPONSABLE             |
|---------------------------------|-----------------------------|
| María Victoria Suárez Osorio    | Gerente de Servicio         |
| Angie Paola Parra Bustos        | Documentadora               |
| Francisco Javier Pulido Fajardo | Gerente de Implementaciones |

*Tabla 20 Grupo Administrativo*

El pasado 31 de julio de 2025 recibimos comunicación 20255000725580-E Id: 6450045, remitida por el supervisor del contrato, solicitando el reemplazo del Gerente de implementaciones, aspecto que ya se encuentra en trámite por el área administrativa de INFOTIC.

## 8. SERVICIO DE COLABORACIÓN

Durante el mes de julio, el servicio de módulos de videoconferencia en las distintas sedes de la entidad se mantuvo operativo sin interrupciones ni problemas. Se aseguró el correcto funcionamiento de cada módulo y se dispuso de apoyo técnico para garantizar su operatividad. A lo largo de este periodo, no se registraron reportes de falta de disponibilidad del servicio en ninguna de las sedes.

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

*Tabla 21 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.

Con el fin de evitar fallos, asegurar un rendimiento óptimo y prolongar la vida útil de los equipos, se llevan a cabo revisiones periódicas y mantenimientos preventivos necesarios para garantizar la continuidad del servicio y el correcto funcionamiento de cada módulo instalado en las sedes de Ictetex.

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

- Visita en sitio en sedes de Bogotá, para realizar pruebas de funcionamiento, inspección de los módulos y posterior limpieza interna y externa de los módulos instalados en la sede Aguas, Ángel y chapinero, para garantizar la prestación continua del servicio y validar que no se estén presentado novedades y/o incidencias.
- Atención y solución de requerimientos para revisión de novedades presentadas.
- Informe mensual de operación y disponibilidad del servicio y reporte técnico de visitas a sedes Regionales, el cual se puede consultar en el link [Informe actividades Módulos videoconferencia ICETEX Julio2025.pdf](#)

Para el periodo comprendido entre el 1 y el 31 de julio de 2025, para las sedes de Bogotá Aguas y Ángel, se generó un (1) requerimiento para revisión de una novedad, relacionada con incidencia de funcionamiento por configuración de la resolución al realizar la conexión de un equipo portátil con Sistema operativo Windows 11, directamente a una pantalla, solicitud que fue atendida, solucionada y cerrada sin presentar indisponibilidad.

Adicional a este requerimiento, no se recibieron más solicitudes para gestión y atención del soporte técnico; tampoco fueron reportadas incidencias a nivel del servicio para estas sedes durante el mes del presente informe, no obstante, como cada periodo, se contó con la disponibilidad técnica para recibir cualquier requerimiento de soporte o solicitud de apoyo en lo concerniente a la solución de videoconferencia desplegada. La solicitud de gestión interna de ingreso a la entidad para la visita técnica se realizó mediante el caso RF-309300-8-23869.

## GESTION DE RIESGOS Y PROBLEMAS

Se construyó una tabla de nivel riesgo que contiene los factores a analizar cómo son severidad y probabilidad otorgando un rango de valor que representa cada uno de los niveles de ocurrencia, con los cuales se determina el nivel de riesgo. Cabe destacar que la determinación de estos valores no sigue una regla estricta, y puede ser ajustada de acuerdo con las necesidades del proyecto.

### ➤ Matriz de riesgos

Se adjunta la matriz de riesgo y de deja la evidencia del documento generado.

| No. | Actividad                                                                        | Peligro                                                                                                                                 | Consecuencia Riesgo                                                            | Medidas de control                                                                                        | Evaluacion del riesgo |                  |       | Medidas de control a implementar                                                                                                       | Responsable      |
|-----|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|-----------------------|------------------|-------|----------------------------------------------------------------------------------------------------------------------------------------|------------------|
|     |                                                                                  |                                                                                                                                         |                                                                                |                                                                                                           | Severidad (S)         | Probabilidad (P) | S x P |                                                                                                                                        |                  |
| 1   | Sin acceso a los servidores con los usuarios y contraseñas entregados            | No poder gestionar los servicios requeridos por el ICETEX                                                                               | Perdida de tiempo y dinero                                                     | Realizar pruebas mensualmente para confirmar el acceso a los servidores                                   | 3                     | 8                | 24    | Verificar con CLARO los cambios que realicen a nivel de la gestión corporativa                                                         | INFOTIC          |
| 2   | Instalación de agente de antivirus en los servidores de ICETEX                   | Sufrir ataques que pueden dañar la información o no permitir el desarrollo de los servicios instalados en los equipos                   | Fallas de seguridad                                                            | Inventario de los servidores identificando cuales tienen instalado y actualizado la versión del antivirus | 2                     | 6                | 12    | Mensualmente revisar los servidores asignados al proyecto revisando el estado del antivirus                                            | INFOTIC          |
| 3   | Parches de actualización de los sistemas operativos de los servidores del ICETEX | Se presentan vulnerabilidades a nivel de los servidores                                                                                 | Fallas de seguridad                                                            | Inventario de los servidores identificando la ultima versión de parches actualizada                       | 3                     | 6                | 18    | Verificación con los fabricantes sobre la ultima versión liberada y funcionando comparada con la instala actualmente en los servidores | INFOTIC          |
| 4   | Actualiación de servidores que son 2008 y 2012                                   | Se presentan vulnerabilidades a nivel de los servidores<br>Fallas en el funcionamiento de las aplicaciones instaladas en estos ewquipos | Fallas de seguridad                                                            | Inventario de los servidores                                                                              | 4                     | 8                | 32    | Verificación semanal del estado de los servidores                                                                                      | ICETEX - INFOTIC |
|     |                                                                                  |                                                                                                                                         | Reprocesos y altos costos ya que estos equipos no tienen soporte de fabricante | Inventario de las aplicaciones                                                                            |                       |                  |       | Verificación semanal del estado de las aplicaciones                                                                                    | ICETEX - INFOTIC |

*Ilustración 39 Matriz de riesgos*

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

### Matriz de riesgos ICETEX.xlsx

A partir de la identificación del nivel de riesgo relacionado al proyecto ICETEX, se pueden implementar estrategias que permitan mitigarlo o, incluso, eliminar los posibles obstáculos a los que se pueda enfrentar el ICETEX.

Durante la ejecución de un proyecto, existen una gran cantidad de factores que pueden determinar el nivel de riesgo, por lo que es importante diferenciar dos tipos:

- **Factores internos:** son aquellos que hacen parte esencial del desarrollo de la operación que se realiza en ICETEX y que tienen que ver con el alcance del proyecto, como lo pueden ser los servidores, aplicaciones, canales de comunicaciones, data center principal y externo.

**Factores externos:** son aquellos que se encuentran fuera del alcance de la empresa, y son de difícil identificación, tales como los fenómenos naturales o fenómenos económicos.

Para lo cual, se tiene:

- Tabla de nivel de riesgo

|                |   | PROBABILIDAD |         |           |          |           |
|----------------|---|--------------|---------|-----------|----------|-----------|
|                |   | IMPROBABLE   | POSIBLE | OCASIONAL | MODERADA | CONSTANTE |
| SEVERIDAD      |   | 2            | 4       | 6         | 8        | 10        |
| INSIGNIFICANTE | 1 | 2            | 4       | 6         | 8        | 10        |
| MENOR          | 2 | 4            | 8       | 12        | 16       | 20        |
| MODERADO       | 3 | 6            | 12      | 18        | 24       | 30        |
| CRITICO        | 4 | 8            | 16      | 24        | 32       | 40        |
| CATASTROFICO   | 5 | 10           | 20      | 30        | 40       | 50        |

*Tabla 22 Nivel de Riesgo*

- Tabla de grado de riesgo

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

*Tabla 23 Grado de riesgo*

## 9. INDICADORES CLAVE DE DESEMPEÑO

### 9.1. ANS por Disponibilidad de canales de comunicaciones:

Durante el mes de julio de 2025, los canales principales y Backup instalados operaron de manera normal, se realizó monitoreo del servicio de los canales mediante la herramienta SolarWinds, el informe de disponibilidad es el que permite la revisión de los ANS y se tiene la línea base de los canales instalados con sus anchos de banda iniciales la cual se actualizando con las ampliaciones de las canales acordadas contractualmente, se tiene el reporte [Reporte Mensual Disponibilidad INFOTIC Julio 2025.pdf](#)

También se puede consultar en el repositorio un documento en Excel con el análisis del comportamiento de

los canales para el mes de julio de 2025 [ANS Julio 2025.xlsx](#)

| Sede            | Categoría                        | INR                   | %MES    |
|-----------------|----------------------------------|-----------------------|---------|
| BOGOTAD.C.      | Principal/FO (Sede Aguas)        | INR0037               | 96.53%  |
|                 | Backup /FO (Sede Aguas)          | INR0036               | 99.98%  |
|                 | Principal/IPVPN (Sede Chapinero) | INR0022               | 100.00% |
|                 | Backup /IPVPN (Sede chapinero)   | INR0020               | 99.81%  |
|                 | Principal/IPVPN (Angel)          | INR0272               | 100.00% |
|                 | Backup /IPVPN (Angel)            | INR0273               | 97.89%  |
| IBAGUE          | Principal/IPVPN                  | INR0073               | 99.95%  |
|                 | Backup/IPVPN                     | INR0076               | 99.68%  |
| LETICIA         | Principal/Satelital              | INR0000373            | 99.47%  |
| NEIVA           | Principal/IPVPN                  | INR0039               | 100.00% |
|                 | Backup/IPVPN                     | INR0041               | 100.00% |
| TUNJA           | Principal/IPVPN                  | INR0104               | 100.00% |
|                 | Backup/IPVPN                     | INR0106               | 100.00% |
| VILLAVICENCIO   | Principal/IPVPN                  | INR0085               | 100.00% |
|                 | Backup/IPVPN                     | INR0084               | 100.00% |
| ARMENIA         | Principal/IPVPN                  | INR0074               | 100.00% |
|                 | Backup/IPVPN                     | INR0072               | 99.95%  |
| MANIZALES       | Principal/IPVPN                  | INR0088               | 99.84%  |
|                 | Backup/IPVPN                     | INR0087               | 100.00% |
| MEDELLIN        | Principal/IPVPN                  | INR0133               | 100.00% |
|                 | Backup/IPVPN                     | INR0132               | 100.00% |
| APARTADO        | Principal/IPVPN                  | INR0144               | 99.44%  |
| PEREIRA         | Principal/IPVPN                  | INR0079               | 100.00% |
|                 | Backup/IPVPN                     | INR0077               | 99.86%  |
| QUIBDO          | Principal/IPVPN                  | INR0014               | 96.95%  |
|                 | Backup/IPVPN                     |                       | 0       |
| BARRANQUILLA    | Principal/IPVPN                  | INR0103               | 100.00% |
|                 | Backup/IPVPN                     | INR0100               | 100.00% |
| CARTAGENA       | Principal/IPVPN                  | INR0109               | 99.28%  |
|                 | Backup/IPVPN                     | INR0107               | 98.98%  |
| MONTERIA        | Principal/IPVPN                  | INR0080               | 98.91%  |
|                 | Backup/IPVPN                     | INR0081               | 98.90%  |
| RIOHACHA        | Principal/IPVPN                  | INR0164               | 100.00% |
|                 | Backup/IPVPN                     | INR0162               | 100.00% |
| SANTAMARTA      | Principal/IPVPN                  | INR0154               | 99.74%  |
|                 | Backup/IPVPN                     | INR0152               | 99.88%  |
| SINCELEJO       | Principal/IPVPN                  | INR0095               | 100.00% |
|                 | Backup/IPVPN                     | INR0097               | 100.00% |
| SAN ANDRES      | Principal/IPVPN                  | INR0000367 INR0000369 | 97.78%  |
| BARRANCABERMEJA | Principal/IPVPN                  |                       | 0       |
| SANGIL          | Principal/IPVPN                  |                       | 0       |
| BUCARAMANGA     | Principal/IPVPN                  | INR0062               | 100.00% |
|                 | Backup/IPVPN                     | INR0061               | 100.00% |
| CUCUTA          | Principal/IPVPN                  | INR0044               | 99.97%  |
|                 | Backup/IPVPN                     | INR0047               | 99.97%  |
| VALLEDUPAR      | Principal/IPVPN                  | INR0091               | 100.00% |
|                 | Backup/IPVPN                     | INR0090               | 99.62%  |
| YOPAL           | Principal/IPVPN                  | INR0121               | 99.99%  |
|                 | Backup/IPVPN                     | INR0123               | 99.97%  |

 Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

 Sede Manizales, Colombia  
 Cra. 24 No. 53\*-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

| Sede                                                                                                                                                                                                                               | Categoría                                                                      | INR        | %MES     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|------------|----------|
| ARAUCA                                                                                                                                                                                                                             | Principal/IPVPN                                                                | INR0110    | 99.80%   |
| CALI                                                                                                                                                                                                                               | Principal/IPVPN                                                                | INR0151    | 100.00%  |
|                                                                                                                                                                                                                                    | Backup/IPVPN                                                                   | INR0153    | 100.00%  |
| BUENAVENTURA                                                                                                                                                                                                                       | Principal/IPVPN                                                                | INR0051    | 96.83%   |
| MOCOA                                                                                                                                                                                                                              | Principal/IPVPN                                                                | INR0135    | 98.96%   |
|                                                                                                                                                                                                                                    | Backup/Satelital                                                               | INR0136    | 97.40%   |
| PASTO                                                                                                                                                                                                                              | Principal/IPVPN                                                                | INR0130    | 100.00%  |
|                                                                                                                                                                                                                                    | Backup/IPVPN                                                                   | INR0131    | 100.00%  |
| POPAYAN                                                                                                                                                                                                                            | Principal/IPVPN                                                                | INR0035    | 100.00%  |
|                                                                                                                                                                                                                                    | Backup/IPVPN                                                                   | INR0032    | 99.70%   |
| TUMACO                                                                                                                                                                                                                             | Principal/IPVPN                                                                | INR0147    | 96.29%   |
| DCTRIARA                                                                                                                                                                                                                           | MPLSPP                                                                         | INR0266    | 100.00%  |
|                                                                                                                                                                                                                                    | MPLS Backup                                                                    | INR0171    | 100.00%  |
| DCTRIARA                                                                                                                                                                                                                           | INTERNET BK                                                                    | INR0221    | 100.00%  |
|                                                                                                                                                                                                                                    | INTERNET PP                                                                    | INR0264    | 100.00%  |
| DCTRIARA                                                                                                                                                                                                                           | NOC claro de dedicado (DWDM)2GTriaramegacentro                                 | INR0224    | 100.00%  |
| Canal entre Sitio principal Icetex- Dirección General-Aguas                                                                                                                                                                        | Principal/IPVPN                                                                |            | 0        |
|                                                                                                                                                                                                                                    | Backup/IPVPN                                                                   |            | 0        |
| BOGOTAD.C.                                                                                                                                                                                                                         | Internet (Sede Aguas)                                                          | INR0034    | 100.00%  |
| DC Megacentro                                                                                                                                                                                                                      | DCMEGACENTER- CONTIGENCIA-MPLSPPAL                                             | INR0177    | 100.00%  |
| DCTRIARA                                                                                                                                                                                                                           | DCMEGACENTER- CONTIGENCIA-MPLS BK                                              | INR0230    | 100.00%  |
| DC Megacentro                                                                                                                                                                                                                      | Internet                                                                       | INR0268    | 100.00%  |
| Banco de la Republica hasta Edificio Dirección General ICETEX                                                                                                                                                                      | Ubicado en Data center Principal. Interconectado a través de red MPLS          | INR0000289 | 100.00%  |
| DECEVAL hasta Edificio de ICETEX Dirección General                                                                                                                                                                                 | Ubicado en Data center Principal. Interconectado a través de red MPLS          | INR0000317 | 96.54%   |
| DECEVAL hasta Edificio de ICETEX Dirección General                                                                                                                                                                                 | Ubicado en Data center Principal. Interconectado a través de red MPLS (Backup) | INR0000318 | 98.32%   |
| Salida de portales <a href="https://portal.icetex.gov.co/portalywww.icetex.gov.co/haciainternetcenrodecómpuotoprincipal">https://portal.icetex.gov.co/portalywww.icetex.gov.co/haciainternetcenrodecómpuotoprincipal</a>           | Internet Reverso para Portales                                                 | INR0000320 | 100.00%  |
| Salida de portales <a href="https://portal.icetex.gov.co/portalywww.icetex.gov.co/haciainternetcenrodecómpuotodecontingencia">https://portal.icetex.gov.co/portalywww.icetex.gov.co/haciainternetcenrodecómpuotodecontingencia</a> | Internet Reverso para Portales                                                 | INR0274    | 100,00 % |
| DCTRIARA                                                                                                                                                                                                                           | Allot Centralizado 800M Triara(equipo)                                         | INR0270    | 100,00 % |

Tabla 24 Disponibilidad de Canales

Durante el mes de julio de 2025 el servicio de Internet para la gente se prestó sin interrupciones en todas las catorce sedes contratadas donde ICETEX cuenta con oficina, las cuales se relacionan a continuación:

| Sede         | Categoría              | INR     | % Mes   |
|--------------|------------------------|---------|---------|
| BARRANQUILLA | INTERNET PARA LA GENTE | INR0094 | 100.00% |
| BUCARAMANGA  | INTERNET PARA LA GENTE | INR0057 | 100.00% |

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

| Sede       | Categoría              | INR        | % Mes   |
|------------|------------------------|------------|---------|
| CALI       | INTERNET PARA LA GENTE | INR0160    | 100.00% |
| AGUAS      | INTERNET PARA LA GENTE | INR0029    | 96.52%  |
| CHAPINERO  | INTERNET PARA LA GENTE | INR0015    | 100.00% |
| MEDELLIN   | INTERNET PARA LA GENTE | INR0122    | 100.00% |
| APARTADO   | INTERNET PARA LA GENTE | INR0140    | 99.45%  |
| ARAUCA     | INTERNET PARA LA GENTE | INR0115    | 99.80%  |
| LETICIA    | INTERNET PARA LA GENTE | INR0000378 | 99.43%  |
| QUIBDO     | INTERNET PARA LA GENTE | INR0021    | 96.94%  |
| RIOHACHA   | INTERNET PARA LA GENTE | INR0159    | 100.00% |
| SAN ANDRES | INTERNET PARA LA GENTE | INR0000368 | 97.76%  |
| YOPAL      | INTERNET PARA LA GENTE | INR0127    | 100.00% |
| MOCOA      | INTERNET PARA LA GENTE | INR0141    | 98.96%  |

*Tabla 25 Disponibilidad canales "Internet para la gente"*

### 9.1.1. Canal de Replicación (Triara – Megacenter)

El proyecto tiene asignado dos (2) canales de comunicación con un ancho de banda de 2 Gbps, el cual se comunica en forma bidireccional entre los data centers de Triara y Megacenter, permitiendo generar la replicación de la información de los equipos de ICETEX, para el mes de julio continúa su funcionamiento correctamente sin novedades que afectaran la prestación del servicio. La evidencia se encuentra en el [Informe mensual replicacion Julio 2025.pdf](#)

### 9.2. ANS por Disponibilidad de servidores:

La herramienta utilizada para el monitoreo de la disponibilidad de servidores es ELK, y el informe correspondiente permite la revisión de los ANS en los documentos [Reporte Monitoreo ICETEXJulio 2025-ELK.pdf](#) y [Disponibilidad Server ELK Julio2025.xlsx](#)

| No | COD.       | Etiquetas de fila            | Disponibilidad |
|----|------------|------------------------------|----------------|
| 1  | INR0000322 | ictsrvctrldoc                | 99.15%         |
| 2  | INR0226    | mira                         | 99.99%         |
| 3  | INR0228    | ictxisgesbd                  | 100.00%        |
| 4  | INR0229    | ictxisgesapp                 | 100.00%        |
| 5  | INR0233    | icetexboglخورفو1.localdomain | 100.00%        |
| 6  | INR0234    | ictxprusisgapp               | 100.00%        |
| 7  | INR0235*   | ictxbogsvrpt2                | 100.00%        |
| 8  | INR0236*   | ictxbogsvrpt1                | 100.00%        |
| 9  | INR0237**  | icetexbogbalserv1-r          | 1.21%          |
| 10 | INR0238    | icetexbogliferaynfs          | 100.00%        |
| 11 | INR0239    | icetexbogelasticserv1        | 100.00%        |
| 12 | INR0240    | icetexbogelasticserv2        | 100.00%        |
| 13 | INR0241    | icetexbogelasticserv3        | 100.00%        |
| 14 | INR0242    | icetexbogliferayserver1      | 99.99%         |
| 15 | INR0243    | icetexbogliferayserver2      | 99.99%         |
| 16 | INR0244    | icetexboglxdarumasrv1        | 100.00%        |
| 17 | INR0245    | icetexboglxdarumasrv2        | 100.00%        |
| 18 | INR0246    | icetexboglxdarumatest        | 100.00%        |
| 19 | INR0247    | preprodsec                   | 100.00%        |
| 20 | INR0248    | icetexboglxroad3             | 100.00%        |

|    |         |                               |         |
|----|---------|-------------------------------|---------|
| 21 | INR0249 | xroadsec                      | 100.00% |
| 22 | INR0250 | qasec                         | 100.00% |
| 23 | INR0251 | INR0251_INFOTIC               | 100.00% |
| 24 | INR0252 | icetexosbognfs2               | 100.00% |
| 25 | INR0253 | bastion.localdomain           | 100.00% |
| 26 | INR0254 | INR0254_INFOTIC               | 100.00% |
| 27 | INR0255 | INR0255_INFOTIC               | 100.00% |
| 28 | INR0256 | INR0256_INFOTIC               | 100.00% |
| 29 | INR0257 | INR0257_INFOTIC               | 100.00% |
| 30 | INR0258 | INR0258_INFOTIC               | 99.98%  |
| 31 | INR0259 | INR0259_INFOTIC               | 100.00% |
| 32 | INR0260 | icetexosbognfs1               | 100.00% |
| 33 | INR0262 | icetexboglxorfeo2.localdomain | 100.00% |
| 34 | INR0276 | cxvodaprodn011                | 100.00% |
| 35 | INR0277 | cxvodaprodn021                | 100.00% |
| 36 | INR0278 | cxvodacontg011                | 100.00% |

*Tabla 26 Códigos relacionados Disponibilidad Servicios en Housing – Datacenter Principal*

El servidor **\*icetexbogsbalserver1-r**, que corresponde al antiguo balanceador de carga, fue deshabilitado a principios del mes de julio. Esta acción se llevó a cabo debido a la puesta en producción de un nuevo balanceador en el mes de junio.

Como resultado de esta medida, la disponibilidad del servidor antiguo disminuyó lógicamente y dejará de aparecer en el Reporte de Disponibilidad a partir del próximo mes. No obstante, el servidor sigue facturándose. Estaremos a la espera de la distribución de estos recursos en los servidores que el ICETEX considere pertinentes.

Por otro lado, con respecto a los servidores **\*\* ictxbogsrvpt1** e **ictxbogsrvpt2**, les recordamos que a finales de diciembre de 2024 el ICETEX solicitó su baja y la distribución de sus recursos en los servidores de **OpenShift**.

Esta solicitud se hizo efectiva al cierre de ese mismo mes, por lo que a partir de enero de 2025 estos servidores ya no se muestran en el Reporte de Disponibilidad mensual. Sin embargo, para efectos de facturación, se siguen teniendo en cuenta tal como se acordó previamente. La evidencia de dicha solicitud se encuentra en el documento: [Baja de servidores - Actualización OpenShift incremento de RAM.pdf](#)

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

| #  | Dispositivo                      | Marca    | Modelo         |
|----|----------------------------------|----------|----------------|
| 1  | FORTIWEB01                       | Fortinet | 2000E          |
| 2  | FORTIWEB02                       | Fortinet | 2000E          |
| 3  | FORTIAUTH01                      | Fortinet | 1000D          |
| 4  | FORTIAUTH02                      | Fortinet | 1000D          |
| 5  | FORTISANDBOX                     | Fortinet | 1000D          |
| 6  | Cisco 3650X                      | Cisco    | WS-C3650-48TQ  |
| 7  | Cisco 3560X SW                   | Cisco    | WS-C3650-48TQ  |
| 8  | Switch DELL Networking           | Dell     | N4032 24 ports |
| 9  | Controladora SAN Dell Compellent | Dell     | SC8000         |
| 10 | Controladora SAN Dell Compellent | Dell     | SC8000         |
| 11 | Enclosure Discos SAN             | Dell     | EN-SC200       |

| #  | Dispositivo                                                                                         | Marca | Modelo   |
|----|-----------------------------------------------------------------------------------------------------|-------|----------|
| 12 | Enclosure Discos SAN                                                                                | Dell  | EN-SC220 |
| 13 | Enclosure Discos SAN                                                                                | Dell  | EN-SC200 |
| 14 | Enclosure Discos SAN                                                                                | Dell  | EN-SC220 |
| 15 | Enclosure Discos SAN                                                                                | Dell  | EN-SC220 |
| 16 | Enclosure Discos SAN                                                                                | Dell  | EN-SC200 |
| 17 | Enclosure Dell Blade – Principal 5 Servidor – Blade M1000, 6 IOM Slot B2 -Tarjeta Enclosure - M1000 | Dell  | M1000E   |

Tabla 27 Dispositivos en Housing – Datacenter Principal

### 9.2.1. Disponibilidad TRIARA para los servicios de página web

A continuación, se evidencia que la disponibilidad del Portal Web institucional web.ICETEX.gov.co, el cual presentó en el mes de julio un **UPTIME del [99,902%]** tal como se evidencia en la gráfica a continuación.

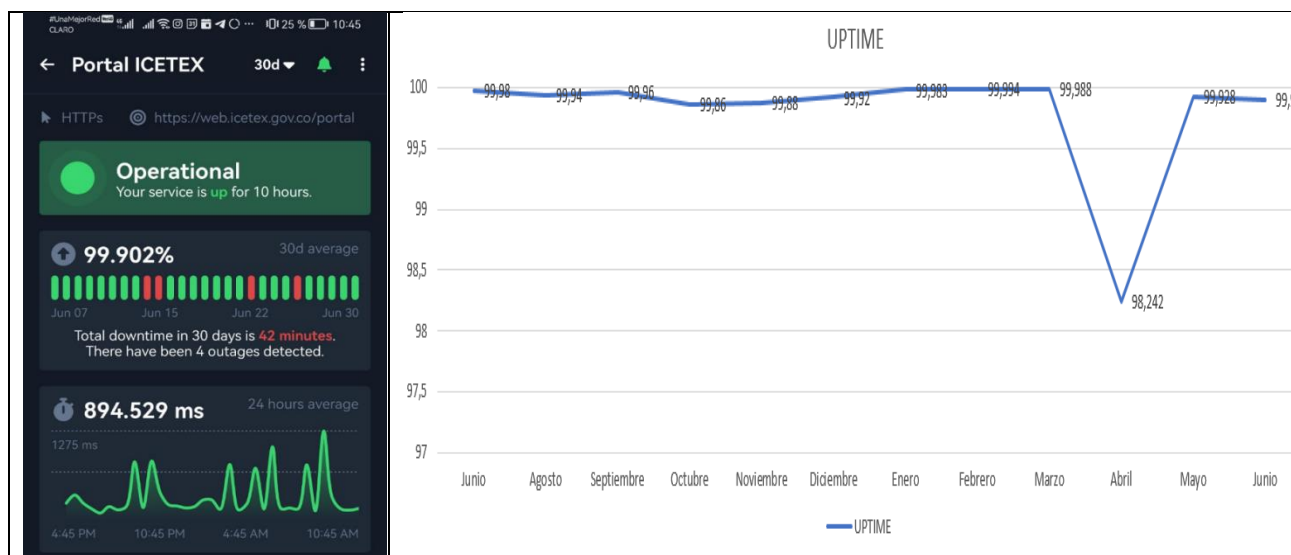


Ilustración 40 UPTIME – Portal WEB web.ICETEX.gov.co

Durante el mes de julio se evidenció un comportamiento estable del portal WEB institucional y se cumplió con el porcentaje de disponibilidad de este con un porcentaje del **99,902%**.

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

|                             | Mayo    | Junio   | Julio   |
|-----------------------------|---------|---------|---------|
| Usuarios activos mes        | 463.000 | 595.000 | 511.000 |
| Usuarios nuevos             | 329.000 | 417.000 | 344.000 |
| Tiempo de interacción (seg) | 129     | 124     | 140     |

Tabla 28 Distribución trimestral de acceso por usuarios

El portal WEB cuenta con un total de 511 mil usuarios, con 344 mil usuarios nuevos. El tiempo de interacción medio es de 2 minutos y 20 segundos, señalando el interés de la audiencia en las diferentes páginas del portal web.icetex.gov.co.

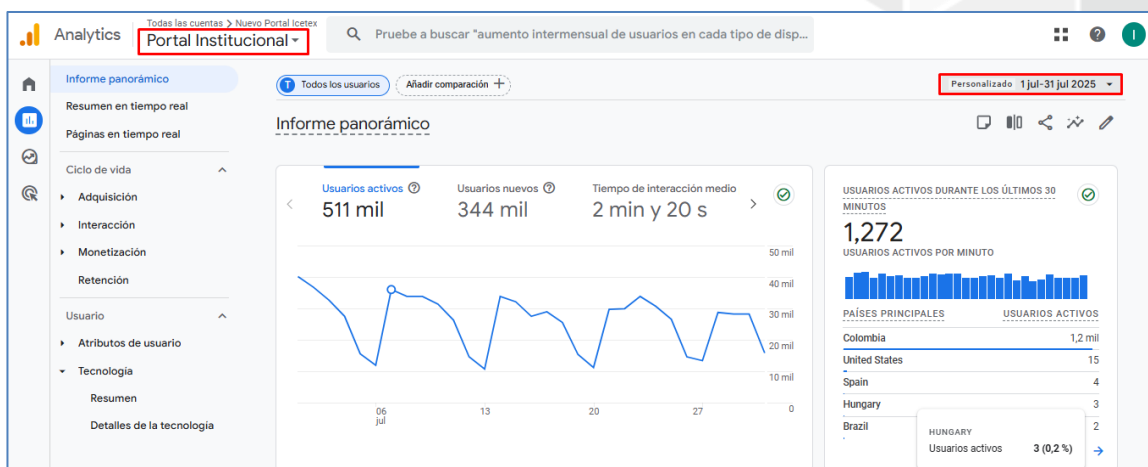


Ilustración 41 Métrica de visitantes Portal WEB web.ICETEX.gov.co

**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:



Ilustración 42 Métrica adquisición usuarios Portal WEB web.ICETEX.gov.co

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

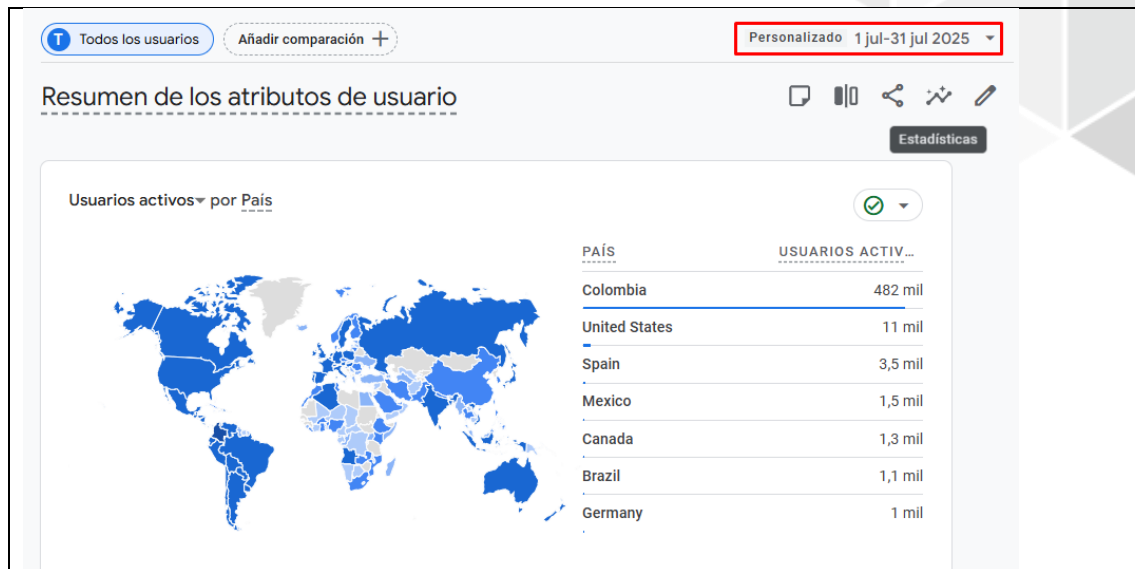


Ilustración 43 Métrica de usuario por país - Portal WEB web.ICETEX.gov.co

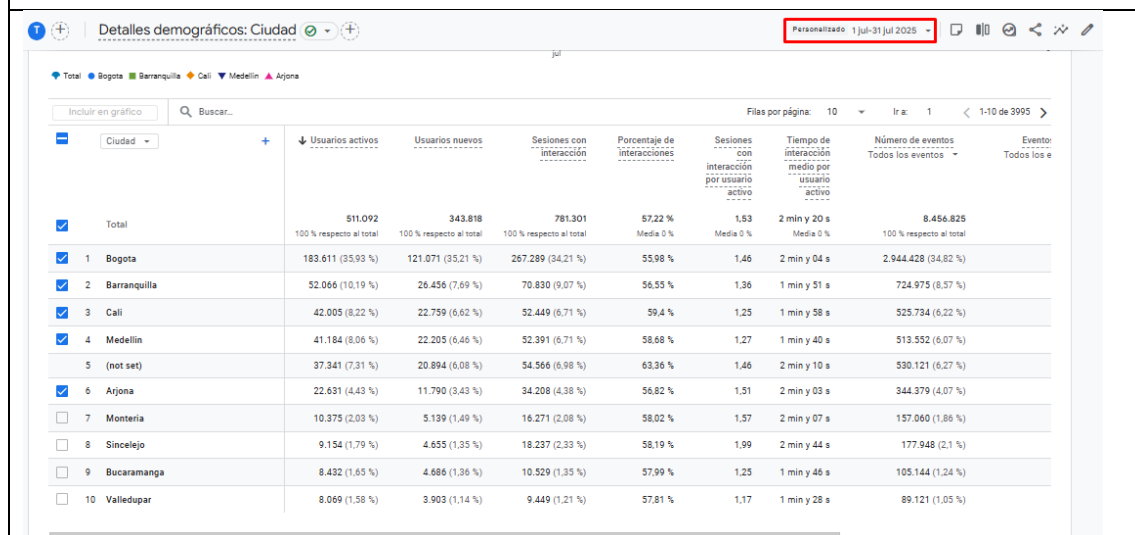


Ilustración 44 Métrica de ciudades de Colombia- Portal WEB web.ICETEX.gov.co

A continuación, se muestran las gráficas referentes a CPU, memoria RAM y almacenamiento en los nodos 1 y 2 del portal ICETEX desde el 1 de julio desde las 0:00 am hasta las 10:30 horas del 31 de julio de 2025.

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

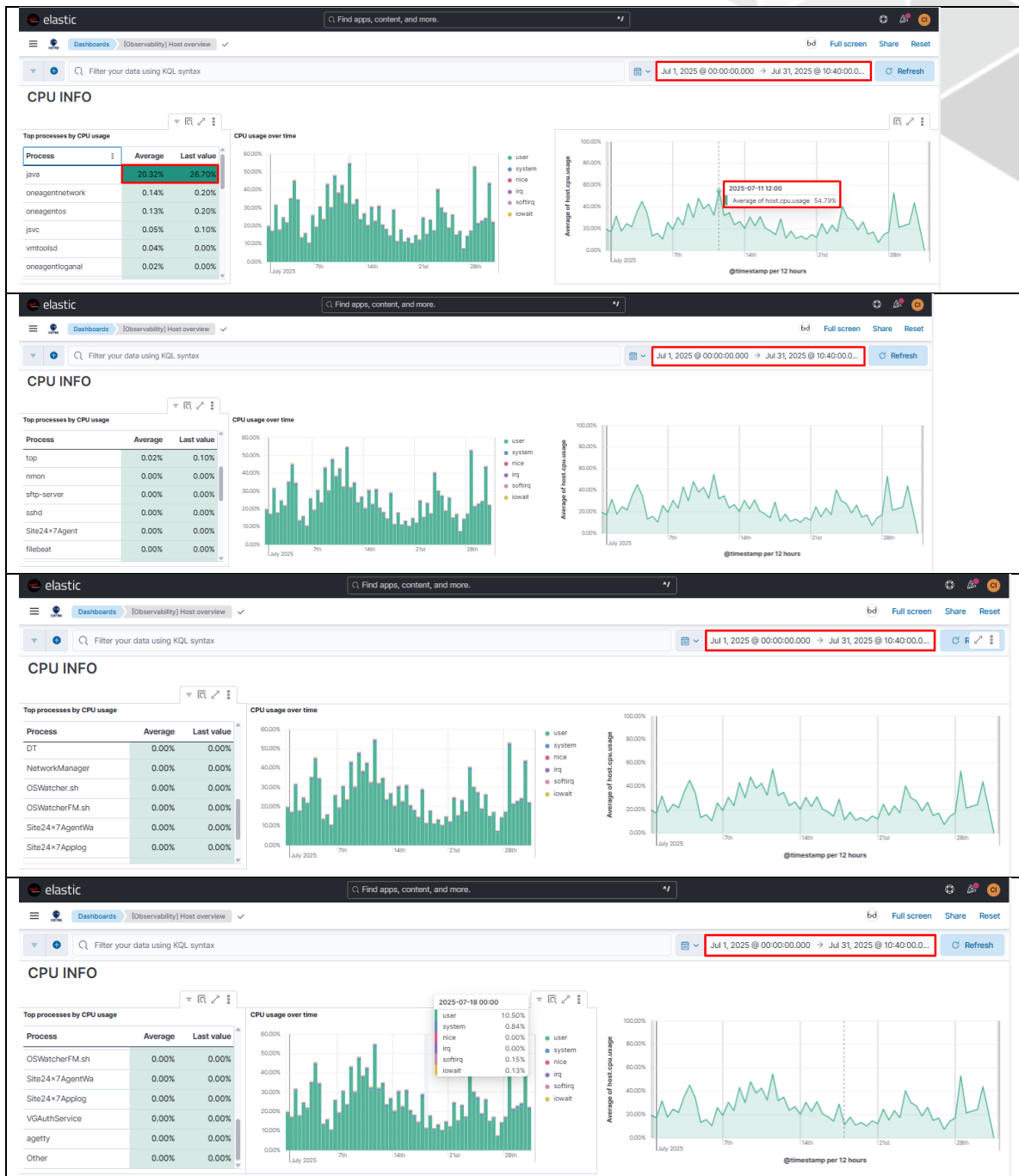
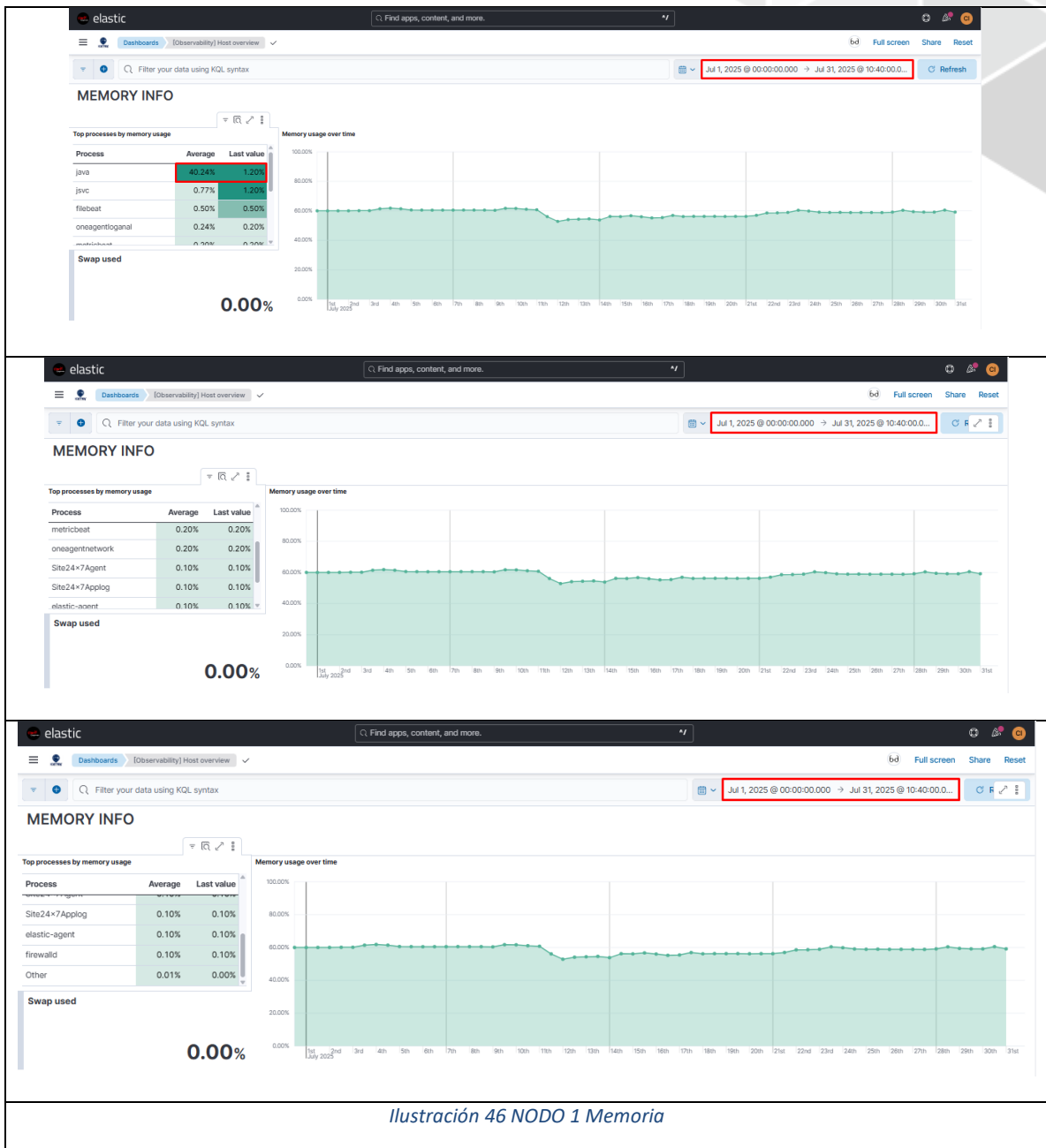


Ilustración 45 NODO 1 CPU

Sede principal-Bogotá, Colombia  
Calle 93B # 13-44, Segundo piso  
NIT:900.068.796-1  
Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
Cra. 24 No. 53ª-26 Arboleda  
Alta.  
NIT: 900.068.796-1  
Teléfono: (+606) 88612612



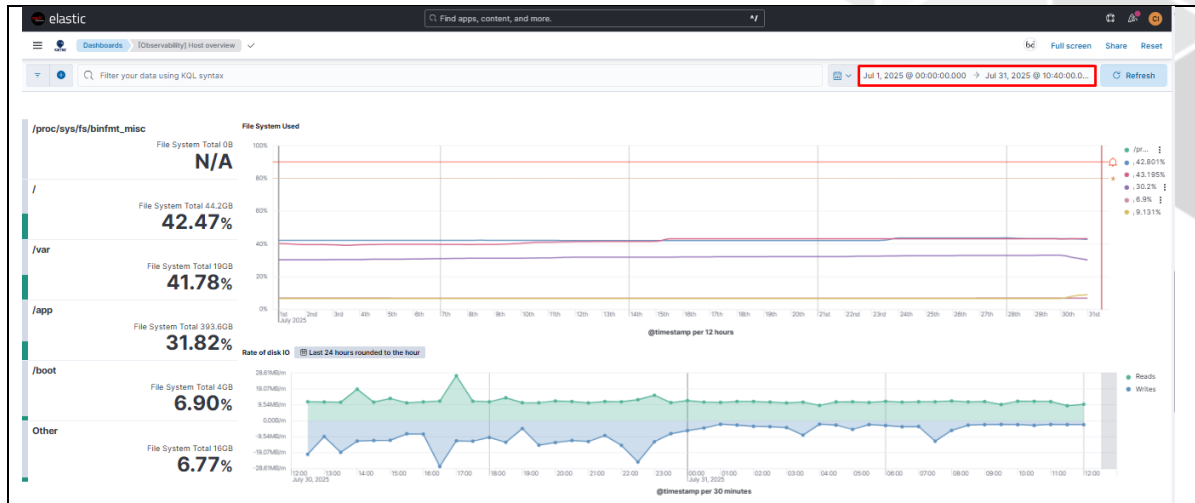


*Ilustración 47 NODO 1 Almacenamiento*

Estos mismos recursos, para el nodo 2 se monitorean de igual manera. El detalle de los consumos y sus umbrales puede ser consultado en el informe de nuestro especialista web master.

### 9.2.2. Análisis componente Liferay Producción

Como parte de las actividades desarrolladas por el Web máster se realiza una revisión de la infraestructura tecnológica y el entorno de software del portal Liferay, abordando aspectos fundamentales para su óptimo rendimiento y seguridad sin encontrarse Hallazgos significativos.

### 9.2.3. Backup Servidores Triara

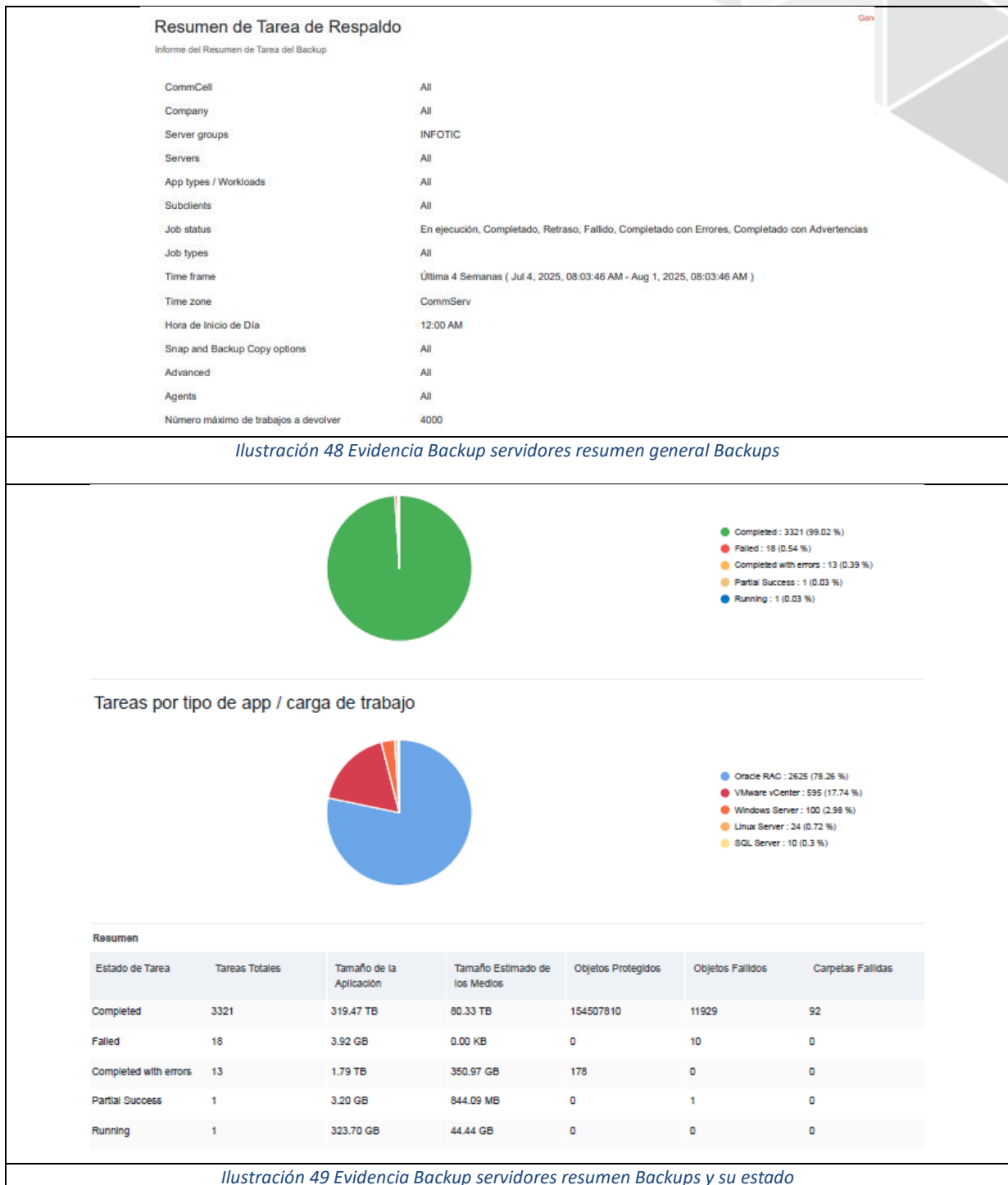
Durante el periodo de julio de 2025 se realizaron los Backups de acuerdo con las políticas definida por el ICETEX, las cuales desde su inicio se implementaron en el Datacenter. Se puede verificar en el documento [Informe Backups mes de Julio 2025.pdf](#) que se genera con el análisis del comportamiento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

Dentro de las actividades del proyecto de servicios tecnológicos para ICETEX, se tiene la toma de copias de respaldo de la información creada, actualizada, reutilizada y procesada dentro de las diferentes actividades de la entidad la cual requiere para el desarrollo de sus actividades diarias, para lo cual se tiene como lineamiento principal la aplicación del anexo 22 donde se contempla las diferentes variables para la toma de Backups y la política de Backups la cual se encuentra actualizada con la operación actual: [Política Backup Ictex V1.xlsx](#)

Actualmente, se cuenta con la custodia externa de 294 cintas en las instalaciones de VISE, correspondientes a la información histórica entregada a partir del 23 de agosto de 2023.

A la fecha, el ICETEX, no ha entregado las cintas de backup necesarias para llevar a cabo el almacenamiento y traslado a custodia externa, lo que permitiría devolver todas las cintas que actualmente se encuentran en calidad de préstamo.

Para el mes de julio de 2025 el resultado de la ejecución de los Backups fue el siguiente:



El total del tamaño de la información respalda para el mes de julio corresponde a 321.6 TB, donde 99.02% se completó en el primer lanzamiento del robot con un total de 319.47 TB de información.

El 78.26% está representado en el respaldo dado a la información del Oracle RAC.

En el caso de los Backups que no fueron exitosos o que presentan algún tipo de problema son revisados de

forma interna, subsanados y nuevamente tomados por el área correspondiente.

El Rendimiento general del sistema de backups está funcionando de manera bastante eficiente en la mayoría de los meses, con una alta tasa de tareas completadas.

La evidencia se genera diariamente en el reporte que se entrega de forma automática a los correos que el ICETEX solicitó y en el informe mensual se anexan todas los soportes y evidencias de la ejecución de las políticas de Backup, la política actualizada y vigente de la toma de Backup, se encuentra en el link del repositorio [Backups Diarios](#) y el informe de Backups en la carpeta [Informe de Backups](#).

A la fecha ICETEX no ha realizado la entrega de las cintas de Backup para devolver las cintas que se están usando en calidad de préstamo para realizar el almacenamiento y traslado a custodia externa.

## 10. CONTROL DE CAMBIOS

Durante el mes de julio 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 |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|--------------------|-----------------------|---------------|
| 1168       | Actualizaciones de Seguridad Servidores Windows<br><b>ICTXSRVAPPMIX1 (192.168.51.134);</b><br><b>ICTXSRVNETCOR01 (192.168.51.165);</b><br><b>ICTXSRVDCVAL01 (192.168.51.170)</b> | 25/06/2025        | 06/07/2025         | Exitoso               | N/A           |
| 1170       | Despliegue de componente Java (.jar) para borrado de caché en el nodo 1 y 2 del portal ICETEX.                                                                                   | 27/06/2025        | 11/07/2025         | No aprobado en el CAB |               |
| 1173       | Despliegue de componente Java (.jar) para borrado de caché en el nodo 1 y 2 del portal ICETEX.                                                                                   | 16/07/2025        | 17/07/2025         | Exitoso               | N/A           |
| 1179       | Actualización a la versión 7.4.0 FortiSIEM                                                                                                                                       | 28/07/2025        | 31/07/2025         | Exitoso               | N/A           |

*Tabla 29 Controles de cambio julio*

## 11. PLAN DE TRABAJO DE LOS PROXIMOS MESES

Se adjunta la tabla del plan de trabajo:

| Actividades                                                                                                               | Responsables     | Fecha Inicio | Fecha fin  | Verificación                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------|------------------|--------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Revisar las alternativas de solución respecto al licenciamiento de las herramientas de seguridad (perimetral y antivirus) | ICETEX           | 01-06-2025   | 31-12-2025 | Esta situación implica riesgos críticos tanto a nivel de seguridad como de continuidad operativa, entre los que se destacan:<br>- Falta de actualizaciones de seguridad críticas.<br>- Mayor exposición a vulnerabilidades y ataques cibernéticos.<br>- Incompatibilidad con software y hardware actualizado.<br>- Ausencia de soporte oficial por parte del fabricante. |
| Se debe realizar mesa técnica conjunta entre ICETEX e INFOTIC para revisar las alternativas de solución frente a la       | INFOTIC – ICETEX | 01-12-2024   | 31-08-2025 | Infotic seguirá enviando los insumos para el comité de vulnerabilidad, se coordina sesión con la especialista de seguridad de ICETEX para definir el proceso de tratamiento de                                                                                                                                                                                           |

| Actividades                                                                                                                                     | Responsables     | Fecha Inicio | Fecha fin  | Verificación                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------|------------------|--------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| gestión de vulnerabilidades.                                                                                                                    |                  |              |            | vulnerabilidades.                                                                                                                                                                                                                                                                    |
| Actualización de Liferay de la versión 7.3 a la 7.4                                                                                             | ICETEX           | 01-12-2024   | 31-08-2025 | Depende de la contratación del soporte de LIFERAY, por parte del ICETEX.                                                                                                                                                                                                             |
| Verificar la configuración de los equipos de LAN y WAN que hace falta para el funcionamiento de IPv6.                                           | INFOTIC - ICETEX | 01-12-2024   | 30-09-2025 | Se está haciendo seguimiento a estos temas de implementación de IPV6 en las sesiones semanales. Ver avances en la última acta de seguimiento del mes de julio de 2025.                                                                                                               |
| Gestión de la administración Azure nube                                                                                                         | INFOTIC - ICETEX | 01-12-2024   | 31-08-2025 | Para efectos de poder avanzar en la este frente, se requiere la designación del personal, por parte de ICETEX, para retomar las sesiones de trabajo y así, definir el plan a seguir.                                                                                                 |
| Políticas e inventarios de las creaciones en la nube                                                                                            | INFOTIC - ICETEX | 01-12-2024   | 31-08-2025 | Para efectos de poder avanzar en la este frente, se requiere la designación del personal, por parte de ICETEX, para retomar las sesiones de trabajo y así, definir el plan a seguir.                                                                                                 |
| Capacitación en seguridad al grupo de especialistas de seguridad del ICETEX                                                                     | INFOTIC - ICETEX | 01-12-2024   | 31-10-2025 | Se realizó la primera capacitación de temas de ciberseguridad al ICETEX el 03/04/2025. Se continuará coordinando con ICETEX las capacitaciones previstas para cada año                                                                                                               |
| Monitoreo de los diferentes servicios realizados por el SOC. Revisión conjunta entre ICETEX – INFOTIC                                           | INFOTIC - ICETEX | 01-12-2024   | 31-12-2025 | Se envió el mes pasado al ICETEX un informe sobre los dispositivos que están siendo monitoreados por el SOC, con el fin de que sean validados por dicha entidad. Actualmente, estamos a la espera de su respuesta. El correo tiene como asunto: Dispositivos monitoreados FortiSIEM. |
| Revisar la parametrización de restricción y los problemas ocasionados a la conexión, para activar el agente de antivirus en las bases de datos. | INFOTIC - ICETEX | 01-12-2024   | 31-12-2025 | Se realizó una primera sesión con los ingenieros de CLARO e INFOTIC para revisar y está en curso la identificación de la causa para poder generar la solución.                                                                                                                       |
| Solicitud de instalación de (5) Internet para la gente en las Oficinas ICETEX de Manizales, Armenia, Cartagena, Sinclejo y Pasto.               | INFOTIC - ICETEX | 01-12-2024   | 30-06-2025 | Se entregó la propuesta comercial a ICETEX de los internet solicitados.                                                                                                                                                                                                              |

Tabla 30 Planes de trabajo

## 12. RECOMENDACIONES DEL CONTRATISTA AL ICETEX

### 12.1. Licenciamiento De Software

Se recomienda efectuar la renovación del soporte de LIFERAY, el cual estuvo activo hasta el pasado 31 de diciembre de 2024 y se prorrogó, por garantía, hasta el 31 de enero de 2025. Es imperativo actualizar el soporte para garantizar la colaboración del fabricante en varios procesos tales como: La obtención de nuevos instaladores, parches de seguridad, claves de licencia para el entorno productivo, así como para pruebas y desarrollo (localhost), y posteriormente llevar a cabo la migración a la nueva versión Liferay 7.4 GA125.

## 12.2. Networking

**Renovación de Equipos:** Se sugiere llevar a cabo la actualización de los equipos de la entidad, ya que muchos de ellos se encuentran obsoletos y carecen de soporte por parte del fabricante, lo que podría afectar el rendimiento y la seguridad de la infraestructura.

**Reemplazo de Equipos Dañados:** Luego del daño del equipo en la sede de San Andres, se informa a ICETEX que actualmente no hay disponibilidad de equipos adicionales para reemplazos futuros en caso de que surjan nuevos daños.

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

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

**Aprovisionamiento de espacio.** Se ha reportado el espacio empleado en la unidad F del servidor ICTXSRVNETCOR01, el cual llega a unos umbrales cercanos al 94% poniendo en riesgo la disponibilidad de dicho servidor. Se recomienda, al ICETEX, validar las políticas de respaldo que se aplican sobre la información allí almacenada así como evaluar la posibilidad de disponer de información histórica en otros medios de almacenamiento permitiendo liberar este espacio.

## 12.3. Aplicaciones

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

Existen aplicaciones que operan sobre el Framework .Net Classic, se recomienda que sean migradas a un Framework más actual y que cuente con soporte vigente. En la actualidad los ambientes de pruebas cuentan con Framework actualizado, lo que permite que las actualizaciones puedan validarse en estos ambientes controlados.

Existen aplicaciones que están implementadas en sistemas operativos obsoletos sean migradas a Servidores con sistemas operativos de versiones actuales y con soporte de Microsoft.

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

Se sigue identificado que el servidor ICTXSRVNETCOR01 presenta una situación crítica relacionada con el espacio en disco en la unidad F:\ la cual dispone únicamente de 69.4 GB libres de un total de 1.79 TB. Este espacio se encuentra comprometido principalmente por archivos antiguos de la aplicación CargueArchivos, almacenados desde el año 2019, por lo que se recomienda aplicar el aumento del almacenamiento en la ruta identificada o que se depuren archivos obsoletos por parte de los responsables de la aplicación, en dado caso que no se realicen estas dos sugerencias existe el riesgo de que el servidor quede sin espacio suficiente en esa partición, afectando gravemente el rendimiento, la estabilidad del sistema y la disponibilidad de la aplicación CargueArchivos, con posibles interrupciones en el servicio.

Se sigue identificado que el servidor ICTXSRVNETCOR01 presenta una situación crítica relacionada con el espacio en disco en la unidad E:\ la cual dispone únicamente de 4.82 GB libres de un total de 65 GB. Este espacio se encuentra comprometido principalmente por archivos antiguos que contienen todos los logs de las aplicaciones configuradas, por lo que se recomienda aplicar el aumento del almacenamiento en la ruta identificada, en dado caso que no se realice esta sugerencia existe el riesgo de que el servidor quede sin espacio suficiente en esa partición, afectando que no se registren más logs.

A continuación, se presenta un cuadro histórico consolidado del uso del almacenamiento en los discos del servidor ICTXSRVNETCOR01, correspondiente a los meses de mayo, junio y julio de 2025, seguido de recomendaciones de observaciones y recomendaciones:

| Disco | Métrica       | may-25         | jun-25         | jul-25         | Observaciones                                                                                             | Recomendaciones                                                                                                                        |
|-------|---------------|----------------|----------------|----------------|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| C:    | Espacio usado | 58% (58.2 GiB) | 61% (61.7 GiB) | 65% (66.6 GiB) | Se incrementa el uso mensual del disco en aproximadamente 3-4 GiB.                                        | Considerar mover archivos no esenciales a otro volumen que dispongan desde el lado de infraestructura hacia almacenamiento secundario. |
|       | Espacio libre | 41.7 GiB       | 38.3 GiB       | 33.3 GiB       | Si continúa esta tendencia, se alcanzará el 80% de uso en los próximos 4 meses.                           |                                                                                                                                        |
| F:    | Espacio usado | 94% (1.69 TiB) | 95% (1.71 TiB) | 92% (1.74 TiB) | Altísima ocupación constante (>90%), aunque mejora en julio debido al aumento del almacenamiento en 100GB | Urgente implementar políticas de depuración de archivos antiguos o inactivos.                                                          |
|       | Espacio libre | 109 GiB        | 86.5 GiB       | 146 GiB        |                                                                                                           | Considerar expansión del volumen o migración de datos a almacenamiento secundario.                                                     |
| E:    | Espacio usado | 87% (56.3 GiB) | 88% (57.2 GiB) | 79% (51.7 GiB) | Notable mejoría en julio con liberación archivos logs de aproximadamente 5.5 GiB.                         | Considerar mover archivos no esenciales a otro volumen que dispongan desde el lado de infraestructura hacia almacenamiento secundario. |
|       | Espacio libre | 8.7 GiB        | 7.82 GiB       | 13.3 GiB       | Aún se mantiene en zona de riesgo por encima del 75%.                                                     | Considerar expansión del volumen si requieren almacenar por mucho más tiempo los logs de las aplicaciones                              |

*Ilustración 50 consolidado del uso del almacenamiento en los discos del servidor ICTXSRVNETCOR01*

## 12.4. Seguridad

En cuanto a la gestión de las bases de datos se recomienda retirar permiso de SUDO a los usuarios INFOTIC, GAWUSER y DCSCAF pues, con esto usuarios, podrían realizar actividades administrativas que no van con su rol. Para ello se debe analizar la razón de estos privilegios con los equipos que realizan mantenimientos a las aplicaciones y verificar el cambio a un rol más apropiado a sus labores.

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

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

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

- Se debe trabajar en el perfilamiento de la navegación de acuerdo con lo entregado por ICETEX.
- Validar la autenticación de doble factor para todas las plataformas misionales del ICETEX.
- Realizar autenticación a través del LDAPS, para la gestión de las plataformas de seguridad.
- Realizar la contención automática de equipos que se identifiquen en la red como maliciosos.
- Realizar el aumento de recursos a la plataforma de FortiSIEM (CPU, Memoria y disco) y hacer un cambio de arquitectura con el objetivo de mejorar.
- Se debe realizar la integración de los activos críticos de la compañía a la plataforma de SIEM, no se ha podido lograr por la falta de recursos de este.

- Adquirir un equipo Firewall para correo para prevenir brechas de seguridad asociadas al uso del correo electrónico y que este es susceptible a muchos tipos de amenazas.
- Integrar los servidores de Directorio Activo con el SIEM.
- Garantizar la segmentación de la red que permita claramente definir qué servicios deben ser alcanzados por cada usuario.
- Se recomienda, que el ICETEX, adquiera una herramienta que permita realizar análisis de tráfico de la red (NTA- Network Traffic Analysis).
- Se recomienda una tecnología que permita la gestión o validación de privilegios de accesos (IAM). Evitar configurar usuarios y claves dentro de las aplicaciones de ICETEX.
- Validar a nivel de punto final, los equipos que se han visto involucrados con comportamiento malicioso.
- Integrar los equipos que hacen parte del proceso de pagos con el SIEM.
- Evaluar los riesgos sobre las plataformas en la nube y considerar aplicar plataformas de seguridad para los ambientes Cloud que cuenta la entidad ya que estos contienen servicios críticos para la misma.

### **12.5. Bases De Datos**

Se deben aumentar los espacios del área de recuperación de las bases de datos productivas de 1TB a 5TB para tener una retención de 10 días o más, con el TB de almacenamiento aprovisionado solo se puede mantener 2 días por BD.

Se debe aprovisionar más almacenamiento para las bases de datos de producción ya que se encuentra en estado crítico, solo queda disponibles 329Gb.

### **12.6. Integrador De Nube**

Configuraciones y malas prácticas permanentes (usuarios identificables por convención de la entidad nombre y apellido, hay usuarios que se conectan con cuentas administradoras de office 365 que al ser administradores hacen imposible su identificación dentro de la compañía).

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

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

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

Se envió un reporte con la lista de máquinas Windows 10 encontradas en la nube de Azure como respuesta al riesgo de seguridad notificado mediante el correo con el asunto “Boletín de seguridad COLCERT Fin del Soporte de Windows 10” para su socialización y escalamiento, a la fecha no hemos informado del funcionario delegado, por el ICETEX, para atender este aspecto.

### 13. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC

Con respecto a los valores agregados indicados contractualmente, se relaciona el estado:

#### 13.1. Aumento de la capacidad de Ancho de Banda en algunas de las sedes de la Entidad

El proceso de ampliación de las sedes de la entidad se completó en el mes de noviembre de 2024 , permitiendo un aumento en la capacidad de ancho de banda conforme a lo establecido en el ANEXO # 2. esta información se puede evidenciar a través de la herramienta de monitoreo Solar Winds y se verifica mensualmente en la facturación de ICETEX.

#### 13.2. Una capacitación al año de seguridad Informática y servicios conexos

Para el periodo de reporte no se presentan avances, dado que la capacitación, que se debe realizar, es una vez al año, la cual se ejecutó el pasado **3 de abril de 2025**, en el horario de **2:00 p.m. a 4:00 p.m.**

Se continuará con la programación de las capacitaciones pendientes de acuerdo con la disponibilidad de agenda de los equipos de trabajo del ICETEX, aspecto que se concertará con la supervisión del contrato.

#### 13.3. TB de capacidad de almacenamiento

El almacenamiento definido contractualmente fue entregado en la fase de implementación por **Contrato** ingresaron las siguientes capacidades:

| CONTRATADO   |            |                                            |                |
|--------------|------------|--------------------------------------------|----------------|
| Cod Servicio | CIUDAD     | ALCANCE                                    | CAPACIDAD (TB) |
| INR0194      | TRIARA     | Almacenamiento Centralizado 23 TB Tier 2   | 35             |
| INR0193      | TRIARA     | Almacenamiento Centralizado 12 TB Tier 2.5 |                |
| INR0192      | MEGACENTER | Almacenamiento Centralizado 15 TB Tier 2   | 25             |
| INR0191      | MEGACENTER | Almacenamiento Centralizado 10 TB Tier 2.5 |                |
|              |            |                                            | <b>60</b>      |

*Tabla 31 Capacidades de almacenamiento contratado*

Aprovisionado se tienen las siguientes capacidades instaladas:

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

*Tabla 32 Capacidades de almacenamiento provisionado*

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

que consumen espacio.

### 13.4. Se oferta Ítem de “Wifi” para la gente en 19 sedes

Se ha estado llevando a cabo el cumplimiento contractual y hasta la fecha, se dispone de conexión wifi en las 14 sedes donde ICETEX tiene oficinas.

INFOTIC envió el 23 de abril propuesta comercial a ICETEX de 5 Canales Internet Para la gente, en respuesta a la solicitud de instalación de cinco puntos de Internet para las sedes de Manizales, Armenia, Cartagena, Sincelejo y Pasto, sin tener una respuesta a la fecha.

La oferta se puede consultar en el link: [Oferta Wifi para la gente](#)

| Enlace - Tipo medio | INR        | BW- Mínimo Requerido (MBPS) | Ancho de Banda actual |
|---------------------|------------|-----------------------------|-----------------------|
| BARRANQUILLA        | INR0094    | 10                          | 10                    |
| BUCARAMANGA         | INR0057    | 10                          | 10                    |
| CALI                | INR0160    | 10                          | 10                    |
| AGUAS               | INR0029    | 20                          | 20                    |
| CHAPINERO           | INR0015    | 20                          | 20                    |
| MEDELLIN            | INR0122    | 10                          | 10                    |
| APARTADO            | INR0140    | 10                          | 10                    |
| ARAUCA              | INR0115    | 10                          | 10                    |
| LETICIA             | INR0000378 | 10                          | 10                    |
| QUIBDO              | INR0021    | 10                          | 10                    |
| RIOHACHA            | INR0159    | 10                          | 10                    |
| SAN ANDRES          | INR0000368 | 10                          | 10                    |
| YOPAL               | INR0127    | 10                          | 10                    |
| MOCOA               | INR0141    | 10                          | 10                    |

*Tabla 33 WIFI para la gente instalados*

| Enlace - Tipo medio | INR     | BW- Mínimo Requerido (MBPS) |
|---------------------|---------|-----------------------------|
| Manizales           | INR0088 | 10                          |
| Armenia             | INR0074 | 10                          |
| Cartagena           | INR0109 | 10                          |
| Sincelejo           | INR0095 | 10                          |
| Pasto               | INR0130 | 10                          |

*Tabla 34 WIFI para la gente pendientes*

## 14. CONCLUSIONES

- El uso de autenticación de doble factor en las conexiones VPN de los funcionarios ayudaría a proteger mejor la información sensible y evitar accesos no autorizados.
- Administrar adecuadamente las contraseñas y permisos garantiza que solo las personas autorizadas accedan a información importante, reduciendo riesgos de seguridad.
- Configurar controles de acceso a la red basados en los servidores de la entidad permite restringir el acceso a ciertas áreas, evitando que los usuarios lleguen a sitios peligrosos.
- Optimizar los recursos del FortiSIEM facilitaría el monitoreo de sistemas clave como bases de datos,

aplicaciones internas y equipos, permitiendo detectar problemas rápidamente y responder de forma oportuna.

- Ajustar las reglas de seguridad en la red ha permitido un mejor control sobre los recursos clave, asegurando que solo lo necesario esté disponible y fortaleciendo la protección.
- Implementar soluciones para gestionar quién puede conectarse a la red mejoraría la seguridad y reduciría el impacto de posibles incidentes.
- Los reportes del SOC han sido clave para detectar y corregir vulnerabilidades, evitando que amenazas afecten la infraestructura crítica de la entidad.
- Es fundamental contar con una persona desde ICETEX en temas de nube que pueda auditar y revisar autorizaciones, ya que su apoyo es crucial para abordar y resolver los hallazgos reportados, lo que permitirá avanzar en los proyectos relacionados con recursos en la nube. La falta de un responsable limita la capacidad de gestión y solución de problemas en este ámbito.

## 15. ANEXOS

| Tema                          | SubTema                 | Anexo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Almacenamiento</b>         | Backups Diarios         | Backups diarios julio 2025 (30 reportes)<br><a href="#">Backups Diarios</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                               | Informe de Backups      | Consolidado mensual Backups Julio 2025<br><a href="#">Consolidado Diario de Backup julio 2025.pdf</a><br><a href="#">Informe Backups mes de Julio 2025.pdf</a>                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Aplicaciones</b>           | Informes de actividades | Informe actividades Módulos videoconferencia ICETEX julio2025<br><a href="#">Informe actividades Módulos videoconferencia ICETEX Julio2025.pdf</a><br>Informe mensual Administrador de Soluciones julio 2025<br><a href="#">Informe Mensual InfoTIC Administrador de Soluciones Julio 2025.pdf</a><br>Informe mensual Administrador Web Master julio 2025<br><a href="#">Informe Mensual InfoTIC Webmaster Julio 2025.pdf</a><br>Informe mensual Integrador Nube julio 2025<br><a href="#">Informe Mensual InfoTIC Integrador de Nube Julio 2025.pdf</a> |
| <b>Bases De Datos</b>         |                         | Informe mensual Administrador de Bases de datos julio 2025<br><a href="#">Informe Mensual InfoTIC DBA Julio 2025.pdf</a>                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Ejecución Presupuestal</b> |                         | Conciliación julio consolidado <a href="#">Conciliación Julio consolidado.xlsx</a><br>Consolidado informe mensual especialistas julio 2025<br><a href="#">Informe Mensual Julio 2025.pdf</a><br>Informe de Gestión Servicio julio 2025 <a href="#">Informe de Gestion Servicio Julio 2025.pdf</a>                                                                                                                                                                                                                                                        |
| <b>Seguridad</b>              |                         | Informe Mensual y Anexo MARCA-OSINT ICETEX julio 2025<br><a href="#">Informe Mensual MARCA-OSINT ICETEX Julio 2025.pdf</a><br><a href="#">Anexo Informe Mensual MARCA-OSINT ICETEX Julio 2025.xlsx</a><br><br>Informe Mensual Seguridad julio 2025<br><a href="#">Informe Mensual InfoTIC Seguridad Julio 2025.pdf</a><br><br>Informe Mensual SOC - ICETEX julio 2025                                                                                                                                                                                    |

| Tema                         | SubTema                                        | Anexo                                                                                                                                                                                                                                                                                                               |
|------------------------------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              |                                                | <a href="#">Informe Mensual SOC-TH ICETEX Julio 2025.pdf</a><br>Informe técnico análisis de vulnerabilidades ICETEX julio 2025<br><a href="#">Informe Técnico Análisis De Vulnerabilidades ICETEX Julio2025.pdf</a><br>Reporte de IPS julio 2025<br><a href="#">Reporte de IPS de Julio infotic 2025.pdf</a>        |
|                              | <b>Reporte total de ataques recibidos-SIEM</b> | Denegados julio 1-15 <a href="#">Denegados Julio1-15.pdf</a><br>Denegados julio 16-31 <a href="#">Denegados Julio16-31.pdf</a>                                                                                                                                                                                      |
| <b>Soporte Y Monitoreo</b>   | <b>Canales</b>                                 | ANS julio 2025 <a href="#">ANS Julio 2025.xlsx</a><br>Informe mensual Administrador de Networking julio 2025<br><a href="#">Informe Mensual InfoTIC Administrador de Redes Julio 2025.pdf</a><br>Informe Mensual Disponibilidad julio 2025<br><a href="#">Reporte Mensual Disponibilidad INFOTIC Julio 2025.pdf</a> |
|                              | <b>Gráficas de consumo</b>                     | Informe Mensual ALLOT julio 2025<br><a href="#">Informe Mensual ALLOT Julio 2025.xls</a>                                                                                                                                                                                                                            |
| <b>Data center Alterno</b>   | <b>Replicación</b>                             | Informe mensual replicación julio 2025<br><a href="#">Informe mensual replicacion Julio 2025.pdf</a><br>Reportes diarios julio 2025 (28 reportes)<br><a href="#">Replicación</a>                                                                                                                                    |
| <b>Data Center Principal</b> |                                                | Reporte Monitoreo ICETEX julio 2025-ELK<br><a href="#">Reporte Monitoreo ICETEXJulio 2025-ELK.pdf</a><br>Data ELK <a href="#">Disponibilidad Server ELK Julio2025.xlsx</a>                                                                                                                                          |

Tabla 35 Anexos

## Revisión técnica

| REVISÓ                                                                 | FIRMAS                                                                                |
|------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| SANDRA MILENA GARCIA HERNANDEZ<br>CONTRATISTA GRUPO DE INFRAESTRUCTURA |  |
| RAUL FERNANDO GUTIERREZ TECANO<br>ANALISTA 2                           | Raul Gutierrez Tecano                                                                 |



# **INFORME DE ACTIVIDADES DEL CONTRATO**

**CONTRATO NUMERO  
2022-0792**

**Agosto 01 al 31 de 2025**

| versión | Observaciones   | Fecha      | Responsable             |
|---------|-----------------|------------|-------------------------|
| 1.0     | Versión Inicial | 01/09/2025 | Francisco Javier Pulido |

## Tabla de contenido

|                                                                |           |
|----------------------------------------------------------------|-----------|
| <b>1. INTRODUCCIÓN .....</b>                                   | <b>9</b>  |
| <b>2. OBJETIVO DEL INFORME .....</b>                           | <b>9</b>  |
| <b>3. ALCANCE .....</b>                                        | <b>10</b> |
| <b>4. AVANCE TÉCNICO.....</b>                                  | <b>11</b> |
| <b>4.1. Conectividad y Red de Comunicaciones .....</b>         | <b>11</b> |
| <b>4.1.1. Canales instalados en el mes y entregables.....</b>  | <b>13</b> |
| <b>4.1.1.1. Solicitudes Nuevas Instalación de canales.....</b> | <b>14</b> |
| <b>4.1.2. Pruebas de Saturación Bidireccionales .....</b>      | <b>14</b> |
| <b>4.2. Centro de Datos.....</b>                               | <b>14</b> |
| <b>4.2.1. Centro de Datos Principal .....</b>                  | <b>14</b> |
| 4.2.1.1. Aplicaciones .....                                    | 14        |
| 4.2.1.2. Bases de Datos .....                                  | 17        |
| 4.2.1.3. Sitio web .....                                       | 20        |
| <b>4.2.2. Centro de Datos Alterno .....</b>                    | <b>23</b> |
| 4.2.2.1. Hosting Virtual (IaaS) .....                          | 23        |
| 4.2.2.2. Dataguard Bases de Datos Megacenter .....             | 25        |
| 4.2.2.3. Servicios de Housing – Datacenter Alterno .....       | 26        |
| 4.2.2.4. Servicios de DRP .....                                | 26        |
| <b>4.3. Seguridad informática .....</b>                        | <b>27</b> |
| <b>4.3.1.1. FortiGate Triara .....</b>                         | <b>30</b> |
| <b>4.3.1.2. FortiGate Aguas.....</b>                           | <b>33</b> |
| <b>4.3.1.3. FortiGate Medellín .....</b>                       | <b>34</b> |
| <b>4.3.1.4. FortiWeb 2000F .....</b>                           | <b>35</b> |
| <b>4.3.1.5. FortiWeb 2000E .....</b>                           | <b>35</b> |
| <b>4.3.1.6. FortiWebCloud DRP .....</b>                        | <b>36</b> |
| <b>4.3.1.7. FortiSandBox .....</b>                             | <b>36</b> |
| <b>4.3.1.7. FortiSIEM.....</b>                                 | <b>36</b> |
| <b>4.3.1.8. Sophos EndPoint .....</b>                          | <b>37</b> |

|                                                                        |           |
|------------------------------------------------------------------------|-----------|
| <b>4.3.3.1. Alertas o Incidentes de Seguridad Detectados .....</b>     | <b>39</b> |
| <b>4.3.3.1.1. Categoría Seguridad .....</b>                            | <b>39</b> |
| <b>4.3.3.1.2. Categoría Disponibilidad .....</b>                       | <b>41</b> |
| <b>4.3.3.1.2. Amenazas de Ciberseguridad .....</b>                     | <b>41</b> |
| <b>4.3.3.1.4. Threat Hunting.....</b>                                  | <b>45</b> |
| 4.3.4.1. Resumen de Vulnerabilidades .....                             | 47        |
| 4.3.4.2. Conclusiones Vulnerabilidades .....                           | 48        |
| <b>4.3.5. Reporte De IPs .....</b>                                     | <b>50</b> |
| <b>5. GESTION DE LA EJECUCIÓN CONTRACTUAL.....</b>                     | <b>50</b> |
| <b>6. GESTION PRESUPUESTAL.....</b>                                    | <b>51</b> |
| <b>7. GESTION ADMINISTRATIVA.....</b>                                  | <b>52</b> |
| <b>7.1. Profesionales.....</b>                                         | <b>52</b> |
| <b>8. SERVICIO DE COLABORACIÓN.....</b>                                | <b>53</b> |
| <b>9. GESTION DE RIESGOS Y PROBLEMAS .....</b>                         | <b>54</b> |
| <b>10. INDICADORES CLAVE DE DESEMPEÑO .....</b>                        | <b>56</b> |
| <b>10.1. ANS por Disponibilidad de canales de comunicaciones:.....</b> | <b>56</b> |
| 10.1.1. Canal de Replicación (Triara – Megacenter) .....               | 59        |
| <b>10.2. ANS por Disponibilidad de servidores: .....</b>               | <b>59</b> |
| 10.2.1. Disponibilidad TRIARA para los servicios de página web.....    | 61        |
| 10.2.2. Análisis componente Liferay Producción .....                   | 66        |
| 10.2.3. Backup Servidores Triara .....                                 | 66        |
| <b>11. CONTROL DE CAMBIOS .....</b>                                    | <b>69</b> |
| <b>12. PLAN DE TRABAJO DE LOS PROXIMOS MESES.....</b>                  | <b>69</b> |
| <b>13. RECOMENDACIONES DEL CONTRATISTA AL ICETEX .....</b>             | <b>71</b> |
| <b>13.1. Licenciamiento De Software .....</b>                          | <b>71</b> |
| <b>13.2. Networking .....</b>                                          | <b>71</b> |
| <b>13.3. Aplicaciones .....</b>                                        | <b>71</b> |
| <b>13.4. Seguridad.....</b>                                            | <b>72</b> |
| <b>13.5. Bases De Datos.....</b>                                       | <b>73</b> |
| <b>13.6. Integrador De Nube.....</b>                                   | <b>73</b> |

|                                                                                                    |           |
|----------------------------------------------------------------------------------------------------|-----------|
| <b>14. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC .....</b>                                | <b>74</b> |
| <b>14.1. Aumento de la capacidad de Ancho de Banda en algunas de las sedes de la Entidad .....</b> | <b>74</b> |
| <b>14.2. Una capacitación al año de seguridad Informática y servicios conexos .....</b>            | <b>74</b> |
| <b>14.3. TB de capacidad de almacenamiento .....</b>                                               | <b>74</b> |
| <b>14.4. Se oferta Ítem de “Wifi” para la gente en 19 sedes .....</b>                              | <b>75</b> |
| <b>15. CONCLUSIONES.....</b>                                                                       | <b>76</b> |
| <b>16. ANEXOS.....</b>                                                                             | <b>77</b> |

## Listado de Tablas

|                                                                                                |    |
|------------------------------------------------------------------------------------------------|----|
| TABLA 1 ESTADO NUEVAS SOLICITUDES CANALES .....                                                | 11 |
| TABLA 2 NORMALIZACIÓN DE DIRECCIONES .....                                                     | 13 |
| TABLA 3 CASOS ATENDIDOS NETWORKING COMPARATIVO MES ANTERIOR .....                              | 14 |
| TABLA 4 VIGENCIA DE LOS CERTIFICADOS DIGITALES .....                                           | 16 |
| TABLA 5 INVENTARIO PRINCIPALES SERVIDORES PRODUCCIÓN .....                                     | 17 |
| TABLA 6 ESTADO BD ORACLE .....                                                                 | 17 |
| TABLA 7 CRECIMIENTO DE LAS BASES DE DATOS EN LOS ÚLTIMOS 7 MESES .....                         | 19 |
| TABLA 8 TOP 10 PORTALES MÁS UTILIZADOS.....                                                    | 23 |
| TABLA 9 SERVICIOS REPLICADOS – DATACENTER MEGACENTER .....                                     | 24 |
| TABLA 10 TOP 5 MÁQUINAS MAYOR TASA DE TRANSFERENCIA .....                                      | 24 |
| TABLA 11 TOP 5 MÁQUINAS MENOR TASA DE TRANSFERENCIA .....                                      | 24 |
| TABLA 12 FECHAS CON MAYOR REPLICACIÓN.....                                                     | 25 |
| TABLA 13 DISPONIBILIDAD DE SERVICIOS DE HOUSING – DATA CENTER ALTERNO.....                     | 26 |
| TABLA 14 DETALLE PLATAFORMAS SEGURIDAD ADMINISTRADAS INFOTIC.....                              | 30 |
| TABLA 15 LICENCIAMIENTO FORTIGATE .....                                                        | 30 |
| TABLA 16 LICENCIAMIENTO FORTIWEB .....                                                         | 35 |
| TABLA 17 CONFIGURACIÓN FORTISANDBOX 1000D .....                                                | 36 |
| TABLA 18 COMPARATIVO – INDICADORES DE COMPROMISO .....                                         | 39 |
| TABLA 19 COMPARATIVO ALERTAS DE SEGURIDAD .....                                                | 40 |
| TABLA 20 EJECUCIÓN PRESUPUESTAL .....                                                          | 52 |
| TABLA 21 PERFILES Y ACTIVIDADES .....                                                          | 52 |
| TABLA 22 GRUPO ADMINISTRATIVO.....                                                             | 53 |
| TABLA 23 DISTRIBUCIÓN MÓDULOS DE VIDEOCONFERENCIA POR SEDE .....                               | 53 |
| TABLA 24 NIVEL DE RIESGO .....                                                                 | 55 |
| TABLA 25 GRADO DE RIESGO .....                                                                 | 56 |
| TABLA 26 DISPONIBILIDAD DE CANALES.....                                                        | 58 |
| TABLA 27 DISPONIBILIDAD CANALES “INTERNET PARA LA GENTE” .....                                 | 59 |
| TABLA 28 CÓDIGOS RELACIONADOS DISPONIBILIDAD SERVICIOS EN HOUSING – DATACENTER PRINCIPAL ..... | 60 |
| TABLA 29 DISPOSITIVOS EN HOUSING – DATACENTER PRINCIPAL.....                                   | 61 |
| TABLA 30 DISTRIBUCIÓN TRIMESTRAL DE ACCESO POR USUARIOS .....                                  | 61 |
| TABLA 31 CINTAS BACKUPS ICETEX.....                                                            | 67 |
| TABLA 32 CONTROLES DE CAMBIO AGOSTO .....                                                      | 69 |
| TABLA 33 PLANES DE TRABAJO.....                                                                | 71 |
| TABLA 34 CAPACIDADES DE ALMACENAMIENTO CONTRATADO .....                                        | 74 |
| TABLA 35 CAPACIDADES DE ALMACENAMIENTO APROVISIONADO .....                                     | 75 |
| TABLA 36 WIFI PARA LA GENTE INSTALADOS.....                                                    | 76 |
| TABLA 37 WIFI PARA LA GENTE PENDIENTES .....                                                   | 76 |
| TABLA 38 ANEXOS.....                                                                           | 78 |

## Listado de Ilustraciones

|                                                                                                              |    |
|--------------------------------------------------------------------------------------------------------------|----|
| ILUSTRACIÓN 1 DISPONIBILIDAD DEL CLÚSTER .....                                                               | 18 |
| ILUSTRACIÓN 2 DISPONIBILIDAD DE LAS BASES DE DATOS PRINCIPALES ICTXCYC Y APOTEOSYS .....                     | 18 |
| ILUSTRACIÓN 3 CASOS DEL PROYECTO GESTIONADOS ARANDA BASES DE DATOS .....                                     | 19 |
| ILUSTRACIÓN 4 UPTIME: PORTAL WEB WEB.ICETEX.GOV.CO [99,802%] .....                                           | 21 |
| ILUSTRACIÓN 5 TRÁFICO GENERAL DE LOS PORTALES .....                                                          | 22 |
| ILUSTRACIÓN 6 REPORTES DE REPLICACIÓN SRM A SITIO ALTERNO – AGOSTO 2025 .....                                | 23 |
| ILUSTRACIÓN 7 EVIDENCIA DATAGUARD REPLICADO A MEGACENTER BD .....                                            | 26 |
| ILUSTRACIÓN 8 DIAGRAMA DE LA ARQUITECTURA DE SEGURIDAD .....                                                 | 27 |
| ILUSTRACIÓN 9 TOPOLOGÍA DE WAF CLOUD USADO EN PORTALES DE MEDELLÍN .....                                     | 28 |
| ILUSTRACIÓN 10 CONSUMO CANAL MPLS - PROMEDIO 1200G [INR0185 CLARO(MPLS_DC)] .....                            | 30 |
| ILUSTRACIÓN 11 CONSUMO INTERNET SEDES - PROMEDIO 1100 GB WAN-SEDES-ICETEX [INR0264 (INTE_SEDES ICTX)] .....  | 31 |
| ILUSTRACIÓN 12 CONSUMO INTERNET DATA CENTER- INTERNET DATACENTER [INTERNET_DC_INR0000320 (INET_CLARO)] ..... | 31 |
| ILUSTRACIÓN 13 FILTRADO – WEB – (FORTIGATE – TRIARA) .....                                                   | 32 |
| ILUSTRACIÓN 14 INSPECCIÓN – SSL – (FORTIGATE – TRIARA) .....                                                 | 32 |
| ILUSTRACIÓN 15 ANTIVIRUS Y ANTIMALWARE – PERIMETRAL (FORTIGATE – TRIARA) .....                               | 33 |
| ILUSTRACIÓN 16 CONSUMO CANAL MPLS AGUAS - PROMEDIO 800 GB .....                                              | 33 |
| ILUSTRACIÓN 17 FILTRADO-WEB-(FORTIGATE-AGUAS) .....                                                          | 34 |
| ILUSTRACIÓN 18 INSPECCIÓN-SSL-(FORTIGATE-AGUAS) .....                                                        | 34 |
| ILUSTRACIÓN 19 ANTIVIRUS Y ANTIMALWARE-PERIMETRAL-(FORTIGATE-AGUAS) .....                                    | 34 |
| ILUSTRACIÓN 20 CONSUMO CANAL MPLS MEDELLÍN .....                                                             | 35 |
| ILUSTRACIÓN 21 TRÁFICO GENERAL DE LOS PORTALES .....                                                         | 35 |
| ILUSTRACIÓN 22 TRÁFICO GENERAL DE LOS PORTALES .....                                                         | 36 |
| ILUSTRACIÓN 23 LICENCIAMIENTO FORTISIEM .....                                                                | 37 |
| ILUSTRACIÓN 24 ESTADO SEGURIDAD SOPHOS .....                                                                 | 37 |
| ILUSTRACIÓN 25 TOTAL DE ALERTAS DE SEGURIDAD .....                                                           | 40 |
| ILUSTRACIÓN 26 TOP 5 DE ALERTAS DE SEGURIDAD ALTAS .....                                                     | 40 |
| ILUSTRACIÓN 27 TOP 5 DE ALERTAS DE DISPONIBILIDAD ALTAS .....                                                | 41 |
| ILUSTRACIÓN 28 ATAQUES IPS PERMITIDOS .....                                                                  | 42 |
| ILUSTRACIÓN 29 ATAQUES IPS DENEGADOS .....                                                                   | 42 |
| ILUSTRACIÓN 30 PUERTOS ENTRANTES DE PÚBLICO A PRIVADO (PERMITIDOS) .....                                     | 43 |
| ILUSTRACIÓN 31 PUERTOS SALIENTE DE PÚBLICO A PRIVADO (PERMITIDOS) .....                                      | 43 |
| ILUSTRACIÓN 32 FALLOS DE INICIO DE SESIÓN VPN .....                                                          | 44 |
| ILUSTRACIÓN 33 FALLOS DE INICIO DE SESIÓN UNIX .....                                                         | 44 |
| ILUSTRACIÓN 34 CUENTAS BLOQUEADOS .....                                                                      | 44 |
| ILUSTRACIÓN 35 ACCESOS DETECTADOS A TRAVÉS DE LA APLICACIÓN ANYDESK .....                                    | 45 |
| ILUSTRACIÓN 36 CANTIDAD TOTAL DE HALLAZGOS IDENTIFICADOS .....                                               | 47 |
| ILUSTRACIÓN 37 VULNERABILIDADES CRITICAS .....                                                               | 48 |
| ILUSTRACIÓN 38 TOP 5 DE MAYORES HALLAZGOS EN EL MES .....                                                    | 48 |
| ILUSTRACIÓN 39 MATRIZ DE RIESGOS .....                                                                       | 55 |
| ILUSTRACIÓN 40 UPTIME – PORTAL WEB WEB.ICETEX.GOV.CO .....                                                   | 61 |
| ILUSTRACIÓN 41 MÉTRICA DE VISITANTES PORTAL WEB WEB.ICETEX.GOV.CO .....                                      | 62 |
| ILUSTRACIÓN 42 MÉTRICA ADQUISICIÓN USUARIOS PORTAL WEB WEB.ICETEX.GOV.CO .....                               | 62 |
| ILUSTRACIÓN 43 MÉTRICA DE USUARIO POR PAÍS - PORTAL WEB WEB.ICETEX.GOV.CO .....                              | 63 |
| ILUSTRACIÓN 44 MÉTRICA DE CIUDADES DE COLOMBIA- PORTAL WEB WEB.ICETEX.GOV.CO .....                           | 63 |
| ILUSTRACIÓN 45 NODO 1 CPU .....                                                                              | 64 |

|                                                                                                   |           |
|---------------------------------------------------------------------------------------------------|-----------|
| ILUSTRACIÓN 46 NODO 1 MEMORIA.....                                                                | 65        |
| ILUSTRACIÓN 47 NODO 1 ALMACENAMIENTO.....                                                         | 66        |
| ILUSTRACIÓN 48 EVIDENCIA BACKUP SERVIDORES RESUMEN GENERAL BACKUPS.....                           | 67        |
| <i>ILUSTRACIÓN 49 EVIDENCIA BACKUP SERVIDORES RESUMEN BACKUPS Y SU ESTADO .....</i>               | <i>68</i> |
| <i>ILUSTRACIÓN 50 CONSOLIDADO DEL USO ALMACENAMIENTO EN DISCOS SERVIDOR ICTXSRVNETCOR01 .....</i> | <i>72</i> |

## 1. INTRODUCCIÓN

Este informe contiene la información relacionada con las actividades ejecutadas por INFOTIC con ocasión de la celebración del contrato 2022-0792, durante el periodo comprendido entre el 01 al 31 de Agosto de 2025. Para tal fin se cuenta con la información generada por el grupo de 10 especialistas y 3 profesionales administrativos con los cuales se soportan y garantizan la atención de servicios especializados descritos en el alcance del proyecto como son:

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

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

- Firma del Acta de Inicio suscrita el 30 de diciembre del 2022, con fecha de iniciación del 19 de enero del 2023. Cumplida al 100%.
- Fase de Transición. Que comprendió desde el 19 de enero hasta el 31 de marzo de 2023. Esta fase se encuentra cumplida al 100%.
- Fase de operación. Inició desde el 1 de abril de 2023, cuenta con un avance en la ejecución del 75 % que representa los 27 meses que lleva dentro de la fase de Operación el proyecto.

El presente informe, correspondiente al mes de agosto del 2025, describe los servicios realizados durante el periodo por el equipo de profesionales y las herramientas tecnológicas asignadas y dispuestas por INFOTIC para desempeñar las funciones y atender los requerimientos del ICETEX según lo establecido en el contrato.

## 2. OBJETIVO DEL INFORME

Presentar las actividades ejecutadas por INFOTIC durante el periodo del 01 al 31 de Agosto de 2025, con el fin de determinar el estado, la gestión, evolución y la disponibilidad de los servicios especializados prestados al ICETEX en virtud de la ejecución del contrato, para lo cual se han considerado la recolección de mediciones desde las herramientas de monitoreo, el análisis y la producción de informes y reportes periódicos sobre cada una de las gestiones y demás informes especiales sobre los servicios prestados.

El presente informe comprende:

- **Administración de Seguridad, Redes y Telecomunicaciones:**  
Descripción de las acciones ejecutadas en la gestión de redes y telecomunicaciones, con énfasis en la estabilidad, disponibilidad y optimización de la infraestructura.

Reporte de incidentes de seguridad, su impacto y las medidas correctivas implementadas.

➤ **Conectividad y Red de comunicaciones:**

Estado de las redes LAN/WAN, su desempeño y disponibilidad.

Indicadores de tráfico, calidad de servicio (QoS) y balanceo de cargas.

➤ **Centro de Datos:**

Estado de operación de los centros de datos, incluyendo disponibilidad, desempeño de servidores, almacenamiento y virtualización.

Acciones de mantenimiento preventivo y correctivo realizadas.

➤ **Seguridad Informática:**

Medidas implementadas para proteger la información y la infraestructura, como monitoreo, control de acceso, actualizaciones y parches de seguridad.

➤ **Servicios de Nube:**

Reporte de uso de servicios en la nube, desempeño y cumplimiento de niveles de servicio (SLA).

Descripción de servicios implementados o integrados en el entorno 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. ALCANCE

El alcance comprende la descripción de las actividades de los servicios especializados durante el periodo del 01 al 31 de Agosto conforme a los frentes definidos por el ICETEX, así:

➤ **Conectividad y red de comunicaciones**

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

➤ **Centro de datos**

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

➤ **Seguridad informática**

El presente informe describe las actividades del periodo que se realizaron con el fin de proveer el servicio de seguridad informática a nivel de administración y gestión para los equipos de seguridad de propiedad

del ICETEX, para los servicios on-premise y para la implementación de controles de seguridad especificados por el modelo de seguridad digital de la Entidad, conforme a los lineamientos legales u otros a fin de fortalecer la seguridad informática de la Entidad.

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

➤ **Servicios de nube**

El informe presenta el estado y detalle de los Servicios de Data Center Principal y Alterno los cuales se encuentra bajo la modalidad de Housing y todos los servicios requeridos para nube privada, dejando claro que a través del contrato se busca integrar servicios de nube pública e híbrida. A la fecha todos los recursos actuales se están usando sin sobre dimensionamientos.

➤ **Servicios conexos**

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

## 4. AVANCE TÉCNICO

### 4.1. Conectividad y Red de Comunicaciones

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

Durante el presente periodo y a fin de destacar se atendieron un total de 38 solicitudes, con respecto al mes anterior hubo un incremento de 23 casos ya que se atendieron 15 solicitudes en el mes anterior.

[Registro Aranda agosto 2025.xlsx](#)

En cuanto a la gestión de vulnerabilidades, todas las detectadas en el último escaneo han sido corregidas. Estamos a la espera de los resultados de un nuevo escaneo para atender cualquier vulnerabilidad adicional que se identifique. Respecto a la implementación de IPv6, se ha trabajado con los especialistas de seguridad en las pruebas correspondientes. Asimismo, se ha avanzado en la documentación y entrega de informes conforme a los lineamientos periódicos de ICETEX.

Referente a las solicitudes efectuadas por parte del ICETEX y canales que se encuentran pendientes se relacionan los pendientes:

| Sede           | Observación                                       |
|----------------|---------------------------------------------------|
| Puerto Carreño | A la espera de la definición por parte del ICETEX |
| Puerto Inírida | A la espera de la definición por parte del ICETEX |

*Tabla 1 Estado nuevas solicitudes canales*

Los casos escalados durante el mes, así como el estado del canal pendiente por instalar, se encuentra descrito

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

#### en el numeral 4.1.1. Canales instalados en el mes y entregables.

La gestión de dispositivos de red es el proceso mediante el cual se gestionan y controlan los dispositivos de red, desde computadoras, servidores y teléfonos móviles hasta conmutadores y máquinas virtuales.

Esto incluye la implementación, la operación y el mantenimiento de todos los dispositivos físicos y virtuales que conforman la infraestructura de red. Actualmente los equipos de red están en buen estado, pero se encuentran en EOL and EOS (End-of-Sale and End-of-Life) esto quiere decir que los equipos ya no cuentan con garantía por parte del fabricante y tampoco son vendidos por los mismos se recomienda al Ictetex adquirir equipos nuevos ya que la infraestructura actual cuenta con más de 15 años de antigüedad

[inventario de equipos.xlsx](#)

[https://icetex.sharepoint.com/:x/r/sites/Infraestructura/\\_layouts/15/Doc.aspx?sourcedoc=%7BD8EB1425-7A43-4FA2-8B11-38665423B9B3%7D&file=inventario%20de%20equipos.xlsx&action=default&mobileredirect=true](https://icetex.sharepoint.com/:x/r/sites/Infraestructura/_layouts/15/Doc.aspx?sourcedoc=%7BD8EB1425-7A43-4FA2-8B11-38665423B9B3%7D&file=inventario%20de%20equipos.xlsx&action=default&mobileredirect=true)

La topología actualizada, a la fecha, se encuentra en el siguiente enlace: [TOPOLOGIAS DE AGUAS](#)

<https://icetex.sharepoint.com/sites/Infraestructura/Documentos%20compartidos/Forms/AllItems.aspx?id=%2Fsites%2FInfraestructura%2FDocumentos%20compartidos%2FTOPOLOGIAS%20DE%20AGUAS&viewid=2cd2befc%2D9f50%2D42c3%2Db53a%2D74e0122a42e3>

Con el fin de garantizar conectividad con el protocolo IPV6, hemos adelantado un plan de trabajo, cuyo estado a la fecha se presenta a continuación:

| SEDE             | Segmento IPv4  | Segmento IPv6      |
|------------------|----------------|--------------------|
| Aguas            | 10.255.0.0/24  | 2801:192:6:E0::/64 |
| Chapinero Bogotá | 10.255.1.0/24  | 2801:192:6:E1::/64 |
| Ángel Bogotá     | 10.255.2.0/24  | 2801:192:6:E2::/64 |
| Cali             | 10.255.3.0/24  | 2801:192:6:E3::/64 |
| Medellín         | 10.255.4.0/24  | 2801:192:6:E4::/64 |
| Buenaventura     | 10.255.5.0/24  | 2801:192:6:E5::/64 |
| Quibdó           | 10.255.6.0/24  | 2801:192:6:E6::/64 |
| Riohacha         | 10.255.7.0/24  | 2801:192:6:E7::/64 |
| Montería         | 10.255.8.0/24  | 2801:192:6:E8::/64 |
| Pereira          | 10.255.9.0/24  | 2801:192:6:E9::/64 |
| Bucaramanga      | 10.255.10.0/24 | 2801:192:6:EA::/64 |
| Popayán          | 10.255.11.0/24 | 2801:192:6:EB::/64 |
| Valledupar       | 10.255.12.0/24 | 2801:192:6:EC::/64 |
| Santa Marta      | 10.255.13.0/24 | 2801:192:6:ED::/64 |
| Barranquilla     | 10.255.14.0/24 | 2801:192:6:EE::/64 |
| Sincelejo        | 10.255.15.0/24 | 2801:192:6:EF::/64 |
| Tumaco           | 10.255.16.0/24 | 2801:192:6:F0::/64 |
| Cúcuta           | 10.255.17.0/24 | 2801:192:6:F1::/64 |
| Villavicencio    | 10.255.18.0/24 | 2801:192:6:F2::/64 |

| SEDE           | Segmento IPv4  | Segmento IPv6      |
|----------------|----------------|--------------------|
| Aguas          | 10.255.0.0/24  | 2801:192:6:E0::/64 |
| Tunja          | 10.255.19.0/24 | 2801:192:6:F3::/64 |
| Cartagena      | 10.255.20.0/24 | 2801:192:6:F4::/64 |
| San Andrés     | 10.255.21.0/24 | 2801:192:6:F5::/64 |
| Armenia        | 10.255.22.0/24 | 2801:192:6:F6::/64 |
| Arauca         | 10.255.23.0/24 | 2801:192:6:F7::/64 |
| Pasto          | 10.255.24.0/24 | 2801:192:6:F8::/64 |
| Ibagué         | 10.255.25.0/24 | 2801:192:6:F9::/64 |
| Apartado       | 10.255.26.0/24 | 2801:192:6:FA::/64 |
| Mocoa          | 10.255.27.0/24 | 2801:192:6:FB::/64 |
| Yopal          | 10.255.28.0/24 | 2801:192:6:FC::/64 |
| Manizales      | 10.255.29.0/24 | 2801:192:6:FD::/64 |
| Neiva          | 10.255.30.0/24 | 2801:192:6:FE::/64 |
| Angel          | 10.255.31.0/24 |                    |
| Leticia        | 10.255.32.0/24 | 2801:192:6:FF::/64 |
| Mocoa SD WAN   | 10.255.61.0/24 |                    |
| Aguas SD_WAN   |                |                    |
| Leticia SD_WAN | 10.255.70.0/24 |                    |

*Tabla 2 Normalización de direcciones.*

A fin de garantizar un adecuado funcionamiento, se ha previsto que el equipo de especialistas de seguridad procederá a configurar reglas de seguridad, en los firewalls, para las direcciones IPV6, empleando como guía las que se encuentran productivas a la fecha con direccionamiento IPV4. El plan de trabajo previsto puede ser consultado en el informe de nuestro especialista de Networking.

En lo concerniente a las pruebas de los aplicativos del ICETEX, se adelantaron pruebas de acceso a las aplicaciones web de la entidad utilizando NAT64, dado que el portal web.icetex.gov.co, que incluye aplicaciones web no compatibles con IPv6, requiere este tipo de traducción de direcciones para asegurar el acceso. Este proceso de conversión de IPv6 a IPv4 es gestionado por el firewall de Triara, permitiendo así la comunicación con el WAF y las aplicaciones web en el servidor.

#### **4.1.1. Canales instalados en el mes y entregables**

Durante el periodo de reporte no se han adelantado instalación de canales tanto principales como de backups.

**Canales Principales.** A la fecha, se ha instalado un total de 40 de los 43 canales MPLS principales previstos en la línea base. De los tres canales restantes, uno corresponde al canal entre el Sitio principal e ICETEX - Dirección General – Aguas, cuya instalación fue descartada por ICETEX. Los otros dos canales faltantes están relacionados con sedes donde ICETEX aún no dispone de oficinas, específicamente en Barrancabermeja y San Gil.

En resumen, hasta la fecha se ha completado la instalación del 100% de los canales principales de comunicación en las sedes especificadas en la línea base del contrato.

**Canales de Backup.** De los 32 canales de Backups previstos en la línea base, se han instalado 30, lo que representa un avance del 96,55%. Actualmente, queda pendiente la instalación del canal de Backup para la oficina en Quibdó, así como un canal entre el sitio principal e ICETEX - Dirección General - Aguas, cuya instalación ya fue descartada por ICETEX.

**Canales de internet para la gente.** El servicio de "internet para la gente" ha sido implementado en las 14 sedes solicitadas según el anexo técnico, logrando así un cumplimiento del 100% de lo previsto.

**Anchos de banda.** Los canales instalados cuentan con el 100% del ancho de banda contratado. Se lleva a cabo un monitoreo mensual de la disponibilidad de estos canales mediante la herramienta SolarWinds, generando un informe correspondiente que está disponible en el siguiente enlace: [Reporte Mensual Disponibilidad INFOTIC Agosto 2025.pdf](#)

#### 4.1.1.1. Solicitudes Nuevas Instalación de canales

En el periodo no se han recibido solicitud de instalación de nuevos canales, pero si se adelantaron mesas técnicas, al interior de la operación, con el fin de entregar configurados los canales SD-WAN de acuerdo a los requerimientos del ICETEX, labor que se espera finalizar en el mes de septiembre.

Los casos atendidos durante el mes están disponibles en el siguiente enlace: [Registro Aranda agosto 2025.xlsx](#)

Todos los casos fueron gestionados exclusivamente a través de la herramienta Aranda, sin que se registrara atención por otros medios.

| Mes    | No. Casos |
|--------|-----------|
| Junio  | 23        |
| Julio  | 15        |
| Agosto | 38        |

*Tabla 3 Casos atendidos Networking comparativo mes anterior*

#### 4.1.2. Pruebas de Saturación Bidireccionales

A la fecha no hay pruebas de saturación que se encuentren pendientes.

### 4.2. Centro de Datos

#### 4.2.1. Centro de Datos Principal

##### 4.2.1.1. Aplicaciones

Durante el mes de Agosto de 2025, se atendieron un total de 15 solicitudes (13 Tareas de Cambio y 2 requerimientos), todas documentadas con sus respectivas evidencias. A continuación, se presenta el detalle de estas:

- **Actualización de archivos en servidores C&CTEX y MIRA**  
Se realizaron cuatro intervenciones orientadas a la modificación y ajuste de archivos ASP, garantizando la continuidad y el correcto funcionamiento de las aplicaciones institucionales.
- **Optimización de la integración PSE (recaptcha)**  
Se ejecutaron tareas tanto en el **Frontend** como en el **Backend** del sistema de pagos, fortaleciendo los mecanismos de validación y seguridad para los usuarios.

- **Acceso a servidores de pruebas**

Se habilitaron accesos a distintos servidores (10.1.18.65 y 10.1.18.124), asegurando la disponibilidad de entornos de validación y pruebas para el equipo de desarrollo.

- **Desarrollo y actualización de aplicaciones institucionales**

- Creación e implementación de la aplicación Simulador de Crédito Educativo, junto con su posterior actualización.
- Copia y actualización de plantillas asociadas a la aplicación WsDesembolsos, garantizando su alineación con los procesos operativos.

- **Gestión de accesos y permisos FTP**

Se configuraron y ajustaron permisos para usuarios VF y OCM, asegurando un control adecuado en la transferencia de archivos y la gestión de información.

Con el fin de garantizar el funcionamiento de las soluciones de manera eficiente y segura, se han revisado el estado de actualización de los parches de los sistemas operativos, y durante el mes se presentaron dos controles de cambio, el 1182 y 1183 con el fin de proceder a efectuar las actualizaciones respectivas.

En cuanto al desempeño de los servidores, reiteramos nuestra preocupación sobre el servidor ICTXSRNSTCOR01 en donde se aloja la aplicación (es) CargueArchivos, ConciliacionesIES, Condonaciones, TransunionAPI, VotoElectronico, WebServiceServicioPasarelaKushki, WebSiteCondonacion, WebSitePortalTransaccional, WebsitePSE, WsApiSolicitudes, WsConciliacionesIES, WsCuentasAbandonaadasAPI, WsDynamics, WsPasarela y WsPortalTransaccional presenta, en su unidad F, un espacio de uso cercano al 97% generando un riesgo para el adecuado funcionamiento de la misma, por lo cual se recomienda al ICETEX revisar las políticas de respaldo sobre esa información, si se están ejecutando y alternativas para optimizar dicho espacio.

Con respecto al resto de servidores administrados, estos se encuentran en estado estable, sin eventos críticos, únicamente registros informativos normales. El detalle de los consumos de los principales recursos puede ser consultado en el informe de especialistas de soluciones.

Se continua con la actualización del inventario de los servidores con los servicios que allí se prestan, el cual puede ser consultado en el siguiente enlace [Revision\\_IIS\\_Agosto2025.xlsx](#)

En cuanto a las actividades de validación de logs, se procedió a efectuar una revisión del visor de eventos en los servidores identificando que:

- Los registros analizados corresponden principalmente a eventos informativos, relacionados con operaciones normales del sistema y de las aplicaciones hospedadas.
- No se detectaron eventos críticos ni errores que comprometan la estabilidad, seguridad o el rendimiento de los servicios en los servidores evaluados.
- Se identificaron eventos habituales como:
  - Inicios y cierres de sesión.
  - Tareas programadas completadas.
  - Validaciones exitosas de servicios.
  - Estados normales de servicios de red y aplicaciones web.

De acuerdo con esta revisión podemos concluir que la infraestructura de servidores se encuentra en estado estable, sin indicios de fallas críticas ni anomalías relevantes en el periodo revisado. Este resultado refleja un funcionamiento adecuado de los sistemas, sin necesidad de acciones correctivas inmediatas.

Durante el mes de Agosto de 2025, se continuó con la revisión técnica de parámetros clave del sistema operativo, servicios de red, protocolos de comunicación, y servicios como IIS y Apache Tomcat, conforme a lineamientos establecidos en guías de seguridad de Microsoft y CIS Benchmarks. Todos los grupos de parámetros se reportaron al equipo de apoyo a la supervisión y nos encontramos a la espera de directrices, por parte del ICETEX, para proseguir esta tarea.

Con el objetivo de asegurar la protección de la información y la confidencialidad de las comunicaciones realizadas a través de los diferentes servicios web de la entidad, se lleva a cabo un control detallado sobre los certificados SSL asignados a los subdominios bajo el dominio institucional icetex.gov.co. A continuación se presenta el estado de estos:

| No | Sitio Web                          | Subdominio (icetex.gov.co)   | Fecha creación | Fecha revocación | Tipo SSL Asignado         |
|----|------------------------------------|------------------------------|----------------|------------------|---------------------------|
| 1  | Colección de Aplicaciones          | aplicaciones.icetex.gov.co   | 4/12/2024      | 4/12/2025        | Secure Site Pro EV SSL    |
| 2  | Portal Institucional               | web.icetex.gov.co            | 4/12/2024      | 4/12/2025        | Secure Site Pro EV SSL    |
| 3  | Portal DECEVAL - Pagaré            | pagare.icetex.gov.co         | 3/12/2024      | 3/12/2025        | Secure Site Pro SSL       |
| 4  | Portal C&CETEX                     | www.icetex.gov.co            | 4/12/2024      | 4/12/2025        | Secure Site Pro EV SSL    |
| 5  | Colección de Web Services Internos | appwebservices.icetex.gov.co | 3/12/2024      | 3/12/2025        | Secure Site Pro SSL       |
| 6  | Pasareladepagos                    | webhook.icetex.gov.co        | 16/10/2024     | 16/10/2025       | RapidSSL                  |
| 7  | Web Service RNEC                   | rniec.icetex.gov.co          | 16/10/2024     | 16/10/2025       | RapidSSL                  |
| 8  | Wildcard                           | *.icetex.gov.co              | 17/11/2024     | 17/11/2025       | Wildcard Rapid SSL RSA CA |

*Tabla 4 Vigencia de los certificados digitales*

Este control es fundamental para garantizar la disponibilidad y seguridad de los servicios ofrecidos a los usuarios, cumpliendo con las políticas institucionales de ciberseguridad y buenas prácticas en la administración de infraestructura tecnológica. Se recomienda al ICETEX contra con los contratos con las entidades que expiden dichos certificados.

Esta información permite una supervisión efectiva del ciclo de vida de los certificados, facilitando la planeación de renovaciones y la mitigación de riesgos asociados a certificados expirados o mal gestionados. El detalle del estado de los certificados y sus fechas de expiración puede ser consultado en el informe de nuestros especialistas de soluciones.

La siguiente tabla detalla las características técnicas de los principales servidores en producción, especificando información clave como: nombre del servidor, dirección IP, sistema operativo, tipo de servidor web utilizado, así como los recursos de hardware disponibles (memoria RAM, capacidad de procesamiento – CPU, y almacenamiento).

Esta información es esencial para la toma de decisiones relacionadas con la administración de recursos, optimización de cargas de trabajo, y cumplimiento de políticas de seguridad y disponibilidad.

| SERVIDOR        | IP             | SISTEMA OPERATIVO                        | SERVIDOR WEB                                  | MEMORIA RAM | CPU    | ALMACENAMIENTO |
|-----------------|----------------|------------------------------------------|-----------------------------------------------|-------------|--------|----------------|
| ICTXSRVNETCOR01 | 192.168.51.165 | Windows Server 2016 Standard 64-bit      | IIS                                           | 27GB        | 16VCPU | 2TB            |
| ICTXSRVAPPSMIX1 | 192.168.51.135 | Windows Server 2019 Standard 64-bit      | IIS                                           | 12GB        | 4VCPU  | 200GB          |
| ICTXSRVDCVAL01  | 192.168.51.17  | Windows Server 2016 Standard 64-bit      | Apache Tomcat                                 | 8GB         | 4VCPU  | 140GB          |
| MIRA            | 192.168.20.4   | Windows Server 2008 R2 Enterprise 64-bit | IIS                                           | 32GB        | 12VCPU | 1,6TB          |
| KIOSKODIGITAL   | 192.1.1.22     | Windows Server 2008 R2 Enterprise 64-bit | IIS                                           | 16GB        | 4VCPU  | 650GB          |
| SRV_APLIC       | 192.1.1.4      | Windows Server 2003 R2 Standard Edition  | IIS                                           | 4GB         | 6VCPU  | 550GB          |
| ICTXSRVMOODLE   | 192.168.51.82  | Windows Server 2019 Standard 64-bit      | IIS                                           | 12GB        | 6VCPU  | 250GB          |
| ICTXSRVAPPSMIX2 | 192.168.51.139 | Windows Server 2019 Standard 64-bit      | Tarea programada CustomWindowsServiceNovacion | 8GB         | 4VCPU  | 150GB          |

*Tabla 5 Inventario principales servidores producción*

Se realizó la verificación de las actualizaciones instaladas en los servidores Windows ICTXSRVNETCOR01, ICTXSRVAPPSMIX1, ICTXSRVDCVAL01, ICTXSRVMOODLE y ICTXSRVAPPSMIX2, identificando que se encuentran al día.

En el informe de los especialistas de soluciones, se presenta un resumen detallado de los hallazgos por servidor, identificando los puntos cumplidos, las áreas de mejora y las recomendaciones correspondientes para asegurar el cumplimiento de estándares mínimos de protección en cada entorno revisado.

#### 4.2.1.2. Bases de Datos

A continuación se presenta un cuadro resumen con el estado actual de las bases de datos administradas:

*Tabla 6*

| BASES DE DATOS     | VERSION     | TAMAÑO |
|--------------------|-------------|--------|
| ASMn user grid     | 19.13.0.0.0 | GB     |
| ICTXCYC            | 11.0.2.0.4  | 4,766  |
| ICETEX             | 11.0.2.0.4  | 206    |
| APLICATI           | 11.0.2.0.4  | 243    |
| APOTEOSY           | 11.0.2.0.4  | 460    |
| VIGIAPRD           | 19.16.0.0   | 143    |
| LIFERAY LIFERAYPDB | 19.16.0.0   | 8.20   |
| LANDICTX           | 19.16.0.0   | 529    |
| SGDEA              | 19.16.0.0   | 124    |

*Estado BD Oracle*

Resultado del proceso destacan las siguientes

- Se continuo con la las BD Oracle al acuerdo con las utilizando el cual garantiza una protección de desastres.
- Se resolvieron los administradores de base de datos en los tiempos estipulados por prioridad.
- Se atendieron todas las reuniones solicitadas por el ICETEX.
- Se realizaron los mantenimientos de los espacios de los filesystem /oracle /grid /opt /DATOS de las

de administración se actividades:

replicación permanente de Datacenter alterno de políticas establecidas, Oracle Active DataGuard el alta disponibilidad, datos y recuperación ante

casos asignados a los

- maquinas donde se encuentran alojadas las bases de datos para su correcto funcionamiento.
- Se validaron los respaldos de las bases de datos de los archivelog, backups incrementales y backup completos o full.
- Se valido la replicación de las bases de datos del Datacenter Bogotá a centro alterno de Medellín Megacenter.
- Se realizaron las restauraciones solicitadas por ICETEX de ambiente de producción a ambiente de desarrollo.
- Se realizaron actividades de tuning base de datos SGDEA (Control Doc)
- Se realizaron los mantenimientos de los espacios de los filesystem /oracle /grid /opt /DATOS de las maquinas donde se encuentran alojadas las bases de datos para su correcto funcionamiento.
- La disponibilidad del Clusterware BD para el mes de Agosto 2025 fue del 100% como se evidencia en la siguiente ilustración:

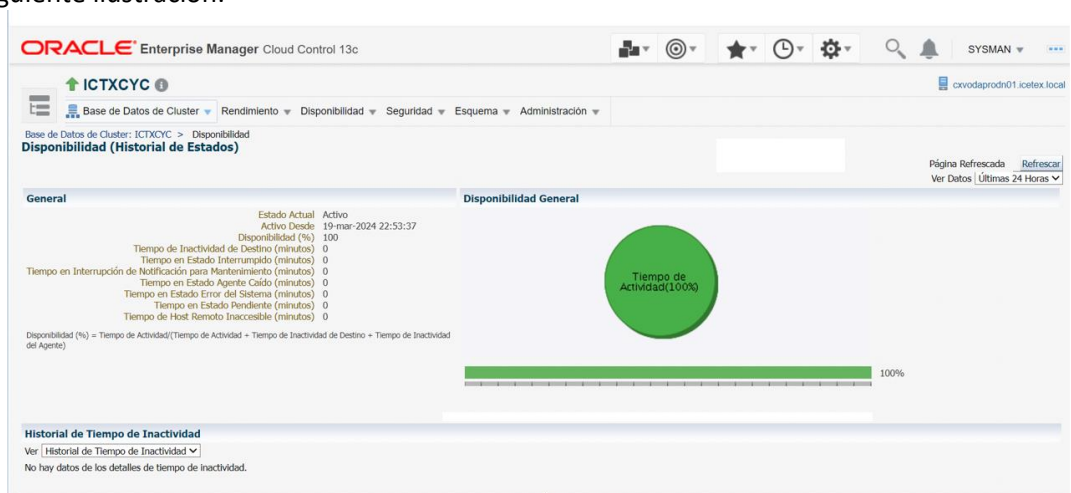


Ilustración 1 Disponibilidad del clúster

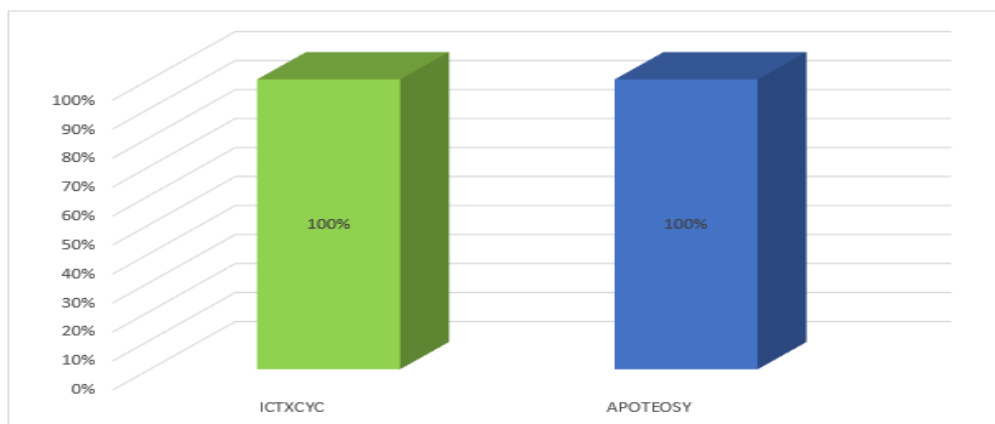


Ilustración 2 Disponibilidad de las Bases de Datos principales ICTXCYC y APOTEOSY

Se ha informado al ICETEX la carencia de recursos en el server de BD 10.1.4.95 para igualar los recursos del ambiente de pruebas a los de producción ya que en estos momentos la BD SICCI se encuentra funcionando con menos de  $\frac{1}{4}$  de los recursos que el ambiente presenta en producción y los usuarios ya han escalado el tema en varias ocasiones, a nivel de BD se generó el análisis para el crecimiento de los recursos que se requieren sean asignados a nivel de S.O para posteriormente asignar estos a la BD SICCI.

Sede principal-Bogotá, Colombia  
Calle 93B # 13-44, Segundo piso  
NIT:900.068.796-1  
Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
Cra. 24 No. 53ª-26 Arboleda Alta.  
NIT: 900.068.796-1  
Teléfono: (+606) 88612612

En periodos pasados se elaboró una propuesta para el control de accesos a nivel de BD, sin tener respuesta por parte del ICETEX. A la fecha se tiene evidencia, por medio de consultas a la auditoría, que hay usuarios realizando DML's y DDL's en la BD empleando usuarios de aplicación sin ningún tipo de solicitud o control de cambio.

La versión de base de datos 11 G ya no tiene soporte por Oracle la versión que en este momento tiene soporte es 19C y, en la actualidad, se cuentan con 5 base de datos operando en esta versión. Se ha brindado soporte, al equipo de sistemas de información del ICETEX, en el proceso de migración a la versión 19c, siendo la base de datos con la que se dio inicio APOTEOSYS.

➤ **Casos del proyecto Gestionados por Bases de datos:**

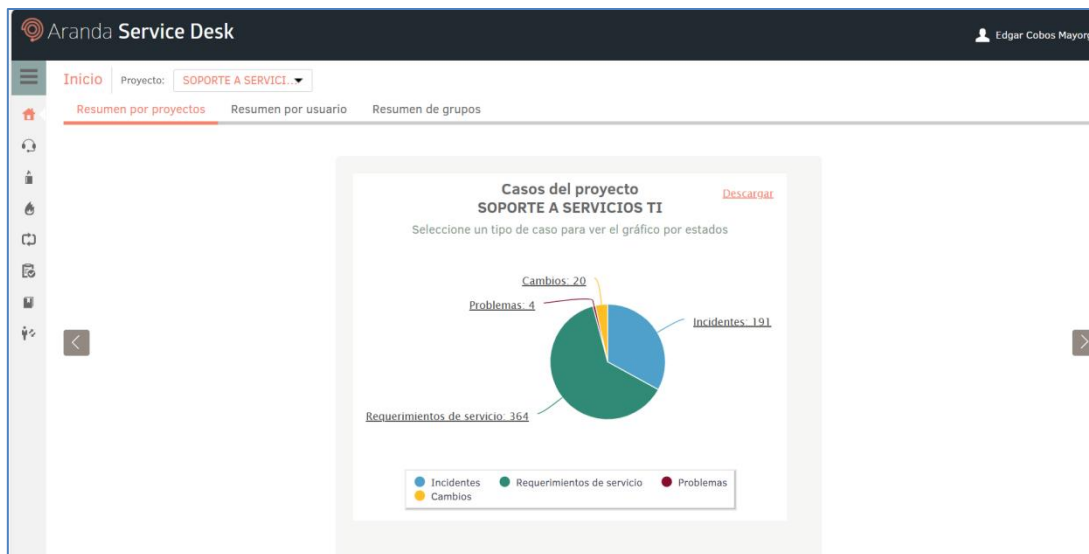


*Ilustración 3 Casos del proyecto Gestionados Aranda Bases de datos*

Desde Bases de datos se tienen las siguientes recomendaciones:

**Almacenamiento:**

A continuación, se presenta el consumo del almacenamiento disponible, por cada una de las bases de datos administradas:

| BASE DE DATOS      | "ENERO - 2025" | "FEB-2025" | MARZO 2025" | ABRIL 2025" | "MAYO 2025" | "JUNIO 2025" | "JULIO 2025" | "AGOSTO 2025" |
|--------------------|----------------|------------|-------------|-------------|-------------|--------------|--------------|---------------|
| ICTXCYC            | 4,561.42       | 4,590      | 4,620       | 4,652       | 4,590       | 4,641        | 4,683        | 4,766         |
| ICETEX             | 203.00         | 204        | 204         | 204         | 202         | 203          | 206          | 206           |
| APLICATI           | 247.00         | 247        | 247         | 247         | 243         | 243          | 243          | 243           |
| APOTEOSY           | 475.00         | 483        | 485         | 485         | 458         | 459          | 460          | 460           |
| VIGIAPRD           | 111.20         | 114        | 116         | 120         | 133         | 137          | 143          | 143           |
| LIFERAY LIFERAYPDB | 8.2            | 8.20       | 8.20        | 8.20        | 8.20        | 8            | 8            | 8             |
| LANDICTX           | 533.5          | 533.5      | 533.5       | 533.5       | 529         | 529          | 529          | 529           |
| SGDEA              | 94             | 108        | 108         | 108         | 112         | 120          | 124          | 124           |
| TOTAL==>           | 6,233.32       | 6287.7     | 6321.7      | 6357.7      | 6,274.90    | 6,340.20     | 6,396.00     | 6,479.00      |

*Tabla 7 Crecimiento de las bases de datos en los últimos 7 meses*

- Se aumentó el espacio del área de recuperación de las bases de datos productivas de 1TB a 2TB para tener una retención de 10 días o más.

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

- Se aprovisionó 1TB más de almacenamiento para las bases de datos de producción de las 8TB adicionales al cluster de producción. Esto implica que hay capacidad para un periodo de un año más, quedando pendiente por distribuir 16 TB.

#### **Seguridad AntVirus:**

- El antivirus de Symantec en las bases de datos sigue inactivo. Nos encontramos adelantando sesiones necesarias para lograr una adecuada configuración que no genere indisponibilidad de los servicios de bases de datos.

#### **Permisos de usuarios en las bases de datos:**

- Se debe restringir a los usuarios de desarrollo a las bases de datos de producción ya que se conectan a través del usuario dueño de los objetos de Core ICETEX\_NUEVO.

#### **Replicación**

- Durante el mes de Agosto de 2025 se continuo con la replicación permanente de las BD Oracle al Datacenter alterno de acuerdo con las políticas establecidas, utilizando el Oracle Active DataGuard el cual garantiza una alta disponibilidad, protección de datos y recuperación ante desastres.

#### **4.2.1.3. Sitio web**

Durante el mes de Agosto se continuo con el monitoreo permanente a los portales sobre los que opera el ICETEX, manteniendo, las alertas y reportes a tiempo en caso de que se presentara algún evento que pudiera ocasionar una interrupción en la prestación de los servicios que se ofrecen a través de los portales, este informe se encuentra detallado en el documento [Informe Mensual InfoTIC Seguridad Agosto 2025.pdf](#)

A fin de mejorar la disponibilidad de los portales, nuestro web master continuó con la automatización de la tarea de administración de borrado de cache. Dicho despliegue se efectuó sobre los nodos 1 y 2 del portal ICETEX.

En cuanto a la disponibilidad del portal web de la entidad se presentan unos uptime superiores al 99,988% como se evidencia en la siguiente gráfica:



Ilustración 4 UPTIME: Portal WEB web.icetex.gov.co [99,802%]

Sin embargo, en la semana comprendida entre el 25 al 31 de agosto, se presentaron inconvenientes en la operación del sitio web del ICETEX, en particular en la visualización de algunas imágenes y descarga de archivos (documentos, plantillas, etc) por parte de los usuarios.

Como medidas administrativas y técnicas, esta gerencia en compañía de nuestra gerente de servicios, los especialistas Web master, de soluciones y de seguridad, realizamos una revisión exhaustiva, durante varias sesiones de trabajo a lo largo de la semana, donde se analizaron los siguientes puntos:

- ◆ Registros de transacciones (logs).
- ◆ Estado de los servidores (nodos de Liferay, Elasticsearch y NFS).
- ◆ Permisos de acceso a las carpetas de descarga.
- ◆ Contención de bloqueos (locks).

Una vez finalizadas las sesiones, nos llevaron a concluir que el problema radica en la indexación de archivos que emplea la herramienta Elasticsearch.

Dicho diagnóstico fue presentado en la sesión de seguimiento semanal del contrato, el pasado 28 de agosto.

Posteriormente, el 29 de agosto, con la colaboración del Ing. German Diaz, contratista de la Vicepresidencia de operaciones del ICETEX, nos reunimos con expertos de la compañía Entelgy. La reunión entre otros aspectos confirmó que la causa raíz del inconveniente es la expiración de la licencia de Elasticsearch. Esta situación impide que el proceso de indexación funcione correctamente, a pesar de que los nodos estén configurados.

La renovación del soporte de Liferay, que se mantuvo activo hasta el 31 de diciembre de 2024, es esencial para garantizar la colaboración del fabricante en varios procesos. Esto incluye la obtención de nuevos

instaladores, parches de seguridad, claves de licencia para el entorno productivo, así como para pruebas y desarrollo en localhost. Además, es fundamental para llevar a cabo la actividad de migración a la nueva versión Liferay 7.4 DXP como otras actividades que requiere con urgencia el equipo de trabajo de la OCM como el posicionamiento por SEO de los contenidos web publicados.

Por otra parte, se recomienda la actualización del licenciamiento de los nodos de Elasticsearch para un óptimo funcionamiento. Para la versión de Liferay 7.4 DXP es necesario cambiar de versión 8.19 o superior.

En cuanto al uso de recursos, estos se encuentran dentro de los umbrales normales, presentándose altos consumos en periodos particulares que corresponden a las solicitudes de actualizaciones y publicaciones de contenido en el portal web, incluye contenidos web, imágenes, banners, displays, videos, ADTs, fragmentos, actualización de URLs a través de la plantilla, redireccionamientos URL.

En el mes, se presenta un promedio de 1200GB de tráfico general hacia los portales protegidos por el FortiWeb donde el portal de [web.icetex.gov.co](http://web.icetex.gov.co) y [www.icetex.gov.co](http://www.icetex.gov.co) fueron los más utilizados en este periodo, lo cual es un comportamiento normal para este tipo de transacciones de acuerdo con la actividad de los usuarios y las convocatorias vigentes.

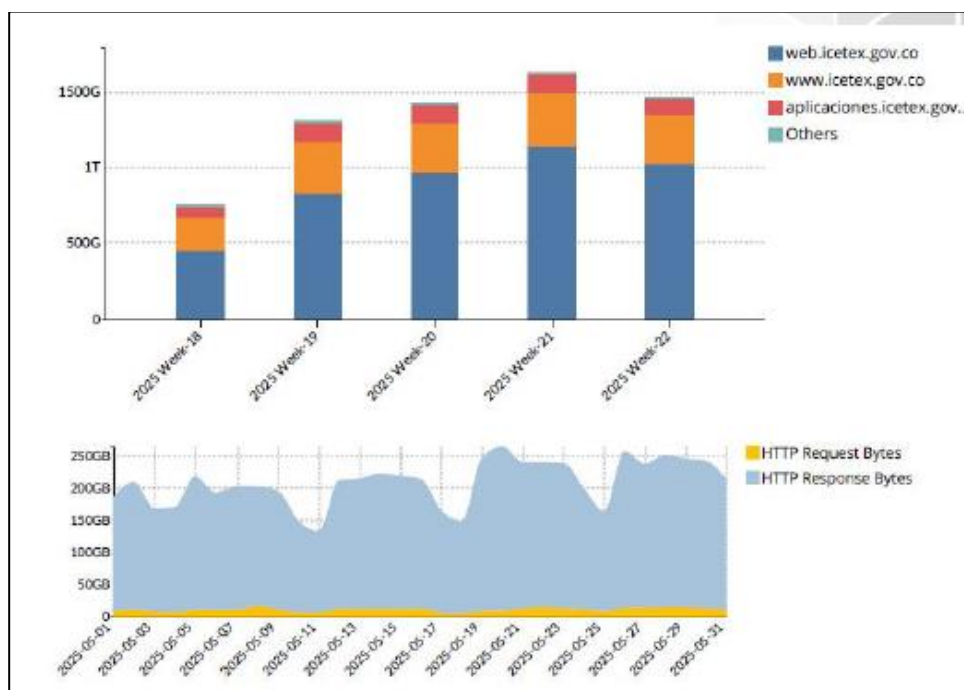


*Ilustración 5 Tráfico General De Los Portales*

En cuanto a los portales más utilizados, la estadística del presente mes es la siguiente:

| #  | HTTP Host                   | HTTP Request Bytes | HTTP Response Bytes |
|----|-----------------------------|--------------------|---------------------|
| 1  | web.icetex.gov.co           | 264.76 GB          | 4.01 TB             |
| 2  | www.icetex.gov.co           | 28.46 GB           | 1.44 TB             |
| 3  | aplicaciones.icetex.gov.co  | 36.87 GB           | 504.84 GB           |
| 4  | comunidad.icetex.gov.co     | 367.37 MB          | 26.19 GB            |
| 5  | portal.icetex.gov.co        | 675.65 MB          | 15.57 GB            |
| 6  | comunidad.icetex.gov.co:443 | 3.18 MB            | 403.22 MB           |
| 7  | web.icetex.gov.co:443       | 4.37 MB            | 235.40 MB           |
| 8  | identidad.icetex.gov.co     | 5.63 MB            | 129.57 MB           |
| 9  | web.icetex.gov.co:80        | 1.23 MB            | 121.79 MB           |
| 10 | www.icetex.gov.co:443       | 7.92 MB            | 117.60 MB           |

Tabla 8 Top 10 Portales más utilizados

Reiteramos nuestra solicitud relacionado con el soporte, por parte del fabricante, de la herramienta Liferay, aspecto que se ha informado en lo corrido del año 2025.

## 4.2.2. Centro de Datos Alterno

### 4.2.2.1. Hosting Virtual (IaaS)

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

## Site Recovery Manager - Estado Replicas INFOTIC

Actualmente el SRM (vcsatriara-ext.datacenterdhs.local -> vomeqacenter.datacenterdhs.local) cuenta con 9 replicas

| General                               |        |                 |                       |              |           |  |
|---------------------------------------|--------|-----------------|-----------------------|--------------|-----------|--|
| Name                                  |        |                 | Count                 |              |           |  |
| OK                                    |        |                 | 9                     |              |           |  |
| Grupo de protección: PG_INFOTIC_7 (1) |        |                 |                       |              |           |  |
| VirtualMachine                        | Status | ConfiguredDisks | LastInstanceSyncPoint | LastSyncSize | RPO       |  |
| INR0226_INFOTIC_REP                   | OK     | 5 of 5          | Aug 31, 2025          | 155.63 MB    | 5 minutes |  |
| Grupo de protección: PG_INFOTIC_6 (2) |        |                 |                       |              |           |  |
| VirtualMachine                        | Status | ConfiguredDisks | LastInstanceSyncPoint | LastSyncSize | RPO       |  |
| INR0228_INFOTIC_REP                   | OK     | 1 of 1          | Aug 31, 2025          | 52.38 MB     | 1 hour    |  |
| INR0229_INFOTIC_REP                   | OK     | 1 of 1          | Aug 31, 2025          | 181.02 MB    | 1 hour    |  |
| Grupo de protección: PG_INFOTIC_4 (3) |        |                 |                       |              |           |  |
| VirtualMachine                        | Status | ConfiguredDisks | LastInstanceSyncPoint | LastSyncSize | RPO       |  |
| INR0238_INFOTIC_REP                   | OK     | 2 of 2          | Aug 31, 2025          | 36.66 MB     | 1 hour    |  |
| INR0239_INFOTIC_REP                   | OK     | 2 of 2          | Aug 31, 2025          | 27.81 MB     | 1 hour    |  |
| INR0243_INFOTIC_REP                   | OK     | 2 of 2          | Aug 31, 2025          | 59.28 MB     | 1 hour    |  |
| Grupo de protección: PG_INFOTIC_3 (2) |        |                 |                       |              |           |  |
| VirtualMachine                        | Status | ConfiguredDisks | LastInstanceSyncPoint | LastSyncSize | RPO       |  |
| INR0244_INFOTIC_REP                   | OK     | 1 of 1          | Aug 31, 2025          | 53.07 MB     | 1 hour    |  |
| INR0245_INFOTIC_REP                   | OK     | 1 of 1          | Aug 31, 2025          | 6.43 MB      | 5 minutes |  |
| Grupo de protección: PG_INFOTIC_2 (1) |        |                 |                       |              |           |  |
| VirtualMachine                        | Status | ConfiguredDisks | LastInstanceSyncPoint | LastSyncSize | RPO       |  |
| INR0249_INFOTIC_REP                   | OK     | 2 of 2          | Aug 31, 2025          | 7.36 MB      | 5 minutes |  |

Ilustración 6 Reportes de replicación SRM a Sitio Alterno – Agosto 2025

En la siguiente tabla se detallan los servidores con sus correspondientes servicios los cuales están

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

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 ***     | icetexboglخورfeo1       | ORFEO                       | INR0233_INFOTIC_REP        |
| 5  | INR0219 ***     | icetexboglخورfeo2       | ORFEO                       | INR0262_INFOTIC_REP        |
| 6  | INR0208 *       | ICTXBOGSRVPT1           | Portal Transaccional        | INR0236_INFOTIC_REP        |
| 7  | INR0209 **      | icetexboglobserver1     | 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 9 Servicios replicados – Datacenter Megacenter*

\*Se detiene la replicación identificada con el código INR0208 que replica la máquina INR0236- ICTXBOGSRVPT1. Los recursos de esta última se distribuyen, en el centro de datos TRIARA, entre los servidores OPENSIFT identificados con los códigos de servicio INR0259, INR0258 e INR0251.

\*\* Se detiene la replicación INR0209 que replica la máquina virtual INR0237- icetexboglobserver1, corresponde al antiguo balanceador, NGIX, que fue deshabilitado en TRIARA

\*\*\*Por solicitud de ICETEX se detiene la replicación INR0219 y INR0220 que replica las máquinas virtuales INR0233 e INR0262 icetexboglخورfeo1 y icetexboglخورfeo2 respectivamente, las máquinas virtuales siguen en producción en TRIARA.

A continuación se presentan las máquinas con mayores y menores tasas de transferencia:

| INR     | HOSTNAME                | MB       |
|---------|-------------------------|----------|
| INR0238 | icetexbogliferaynfs     | 15515.44 |
| INR0228 | ictxisgesbd             | 7879.12  |
| INR0226 | icetexbogwsmira         | 4804.14  |
| INR0243 | icetexbogliferayserver1 | 3628.59  |
| INR0229 | ictxisgesapp            | 3366.91  |

*Tabla 10 TOP 5 máquinas mayor tasa de transferencia*

| INR     | HOSTNAME                | MB      |
|---------|-------------------------|---------|
| INR0245 | icetexboglxdarumasrv2   | 209.54  |
| INR0249 | icetexboglxroad1        | 316.44  |
| INR0262 | icetexboglخورfeo2       | 338.6   |
| INR0233 | icetexboglخورfeo1       | 878.75  |
| INR0239 | icetexbogelasticserver1 | 1448.25 |

*Tabla 11 TOP 5 máquinas menor tasa de transferencia*

En cuanto a las fechas con mayor replicación presentada podemos observar el siguiente comportamiento:

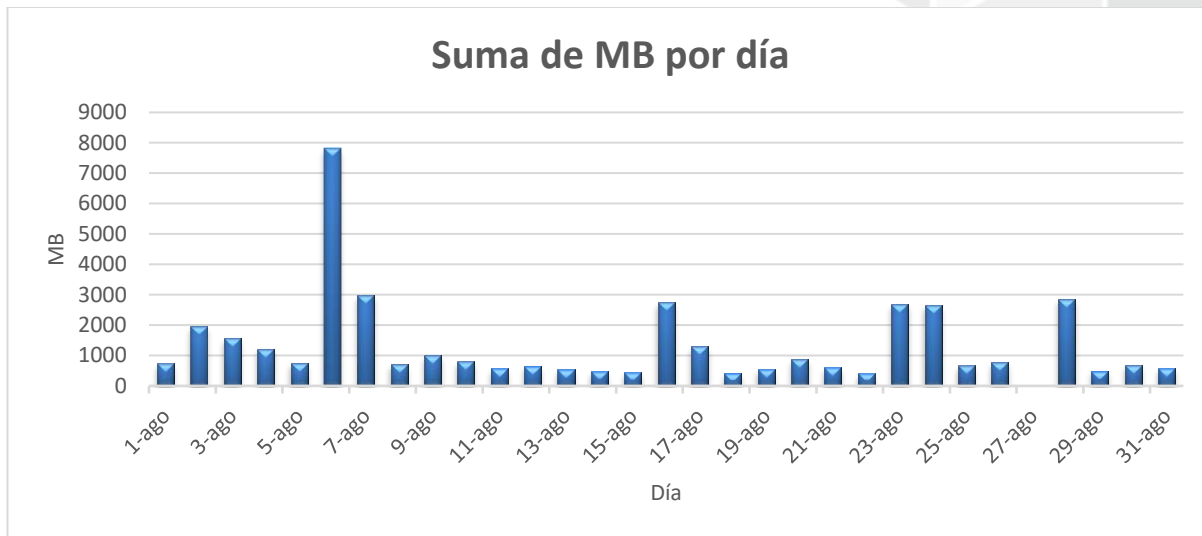


*Tabla 12 Fechas con mayor replicación*

En agosto, las mayores transferencias de datos ocurrieron durante los días laborales de la semana, fue notable el volumen de transferencia del 6 de agosto, que tuvo un mayor volumen con 7814.38 MB, más del doble que el siguiente pico.

La tendencia semanal indica una disminución significativa de la transferencia de datos después de la primera semana, seguida de fluctuaciones.

La primera semana (01-ago al 07-ago) tuvo la mayor cantidad de datos replicados, con **17.04 GB**. Esto es más del doble de la cantidad transferida en cualquier otra semana completa del mes.

INR0233 y INR0262: Estas VMs tienen una transferencia de datos muy constante y baja, lo que indica que tienen un cambio de datos mínimo. Es importante notar que la replicación se detuvo para estas VMs a partir del 20 de agosto, como se indica en la falta de datos.

Los datos muestran que el proceso de replicación incremental está funcionando correctamente. Las variaciones en las cantidades de datos transferidos en las semanas posteriores reflejan la cantidad de cambios (nuevos datos o modificaciones) que se produjeron en el entorno de las máquinas virtuales durante esos períodos.

#### 4.2.2.2. Dataguad Bases de Datos Megacenter

Durante el mes de Agosto de 2025 se continuo con la replicación permanente de las BD Oracle al Datacenter alterno de acuerdo con las políticas establecidas, utilizando el Oracle Active DataGuard el cual garantiza una alta disponibilidad, protección de datos y recuperación ante desastres. Ver las evidencias en el documento [Informe Mensual InfoTIC DBA Agosto 2025.pdf](#)

```

oracle@cxvodacontg011:~$ ps -fea |grep pmon
grid      7907      1  0 Aug23 ?        00:01:13 asm_pmon_+ASM
oracle    9005      1  0 Aug23 ?        00:03:16 ora_pmon_ICTXCYCD
oracle    9290      1  0 Aug23 ?        00:03:23 ora_pmon_ICETEXD
oracle    9630      1  0 Aug23 ?        00:03:22 ora_pmon_APLICATD
oracle    9922      1  0 Aug23 ?        00:03:24 ora_pmon_APOTEOSD
oracle   10280      1  0 Aug23 ?        00:03:24 ora_pmon_APOTNEWD
oracle   10592      1  0 Aug23 ?        00:02:07 ora_pmon_VIGIADTG
oracle   10990      1  0 Aug23 ?        00:02:07 ora_pmon_LANDICTD
oracle   11427      1  0 Aug23 ?        00:02:03 ora_pmon_LIFERAYD
oracle   29262 29080  0 10:51 pts/1    00:00:00 grep --color=auto pmon

[oracle@cxvodacontg011 ~]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.4.0 Production on Tue Sep 2 10:51:09 2025

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

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

SQL> sta faplyb.sql

   Thread Last Sequence Received Last Sequence Applied TIME_RECEIVED   TIME_APPLIED
-----
1          122381          122381 31/08/2025 10:51 31/08/2025 10:51
2           88059           88059 31/08/2025 10:51 31/08/2025 10:51

SQL>

```

*Ilustración 7 Evidencia Dataguard replicado a Megacenter BD*

Se generó la consulta de los archivos recibidos y aplicados de la base de datos de ICTXCYCD a 02/07/2025 con diferencia cero (0) archivos sin aplicar, lo que evidencia la sincronización a nivel de Bases de datos Oracle.

#### 4.2.2.3. Servicios de Housing – Datacenter Alterno

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

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

*Tabla 13 Disponibilidad de Servicios de Housing – Data Center Alterno*

#### 4.2.2.4. Servicios de DRP

Nos encontramos a la espera de la definición del alcance de la prueba y de la fecha prevista de la misma, por parte del ICETEX.

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

### 4.3. Seguridad informática

Se presenta el diagrama de red que se tiene actualmente a nivel de los dispositivos de seguridad perimetral y el componente de antivirus Sophos.

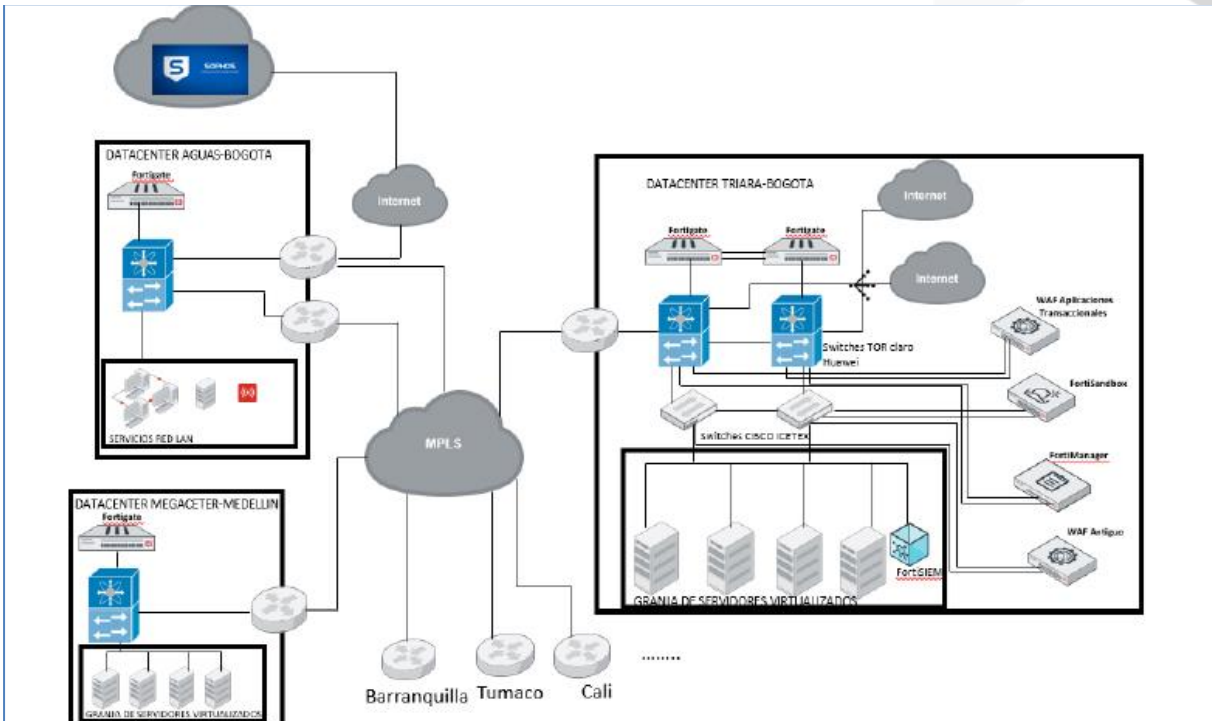


*Ilustración 8 Diagrama de la Arquitectura de Seguridad*

En la ilustración 9, se observa la implementación del WAF Cloud donde se utilizaron dos aplicaciones web para el DRP los cuales tienen como dominios: webdrp.icetex.gov.co y drp.icetex.gov.co.

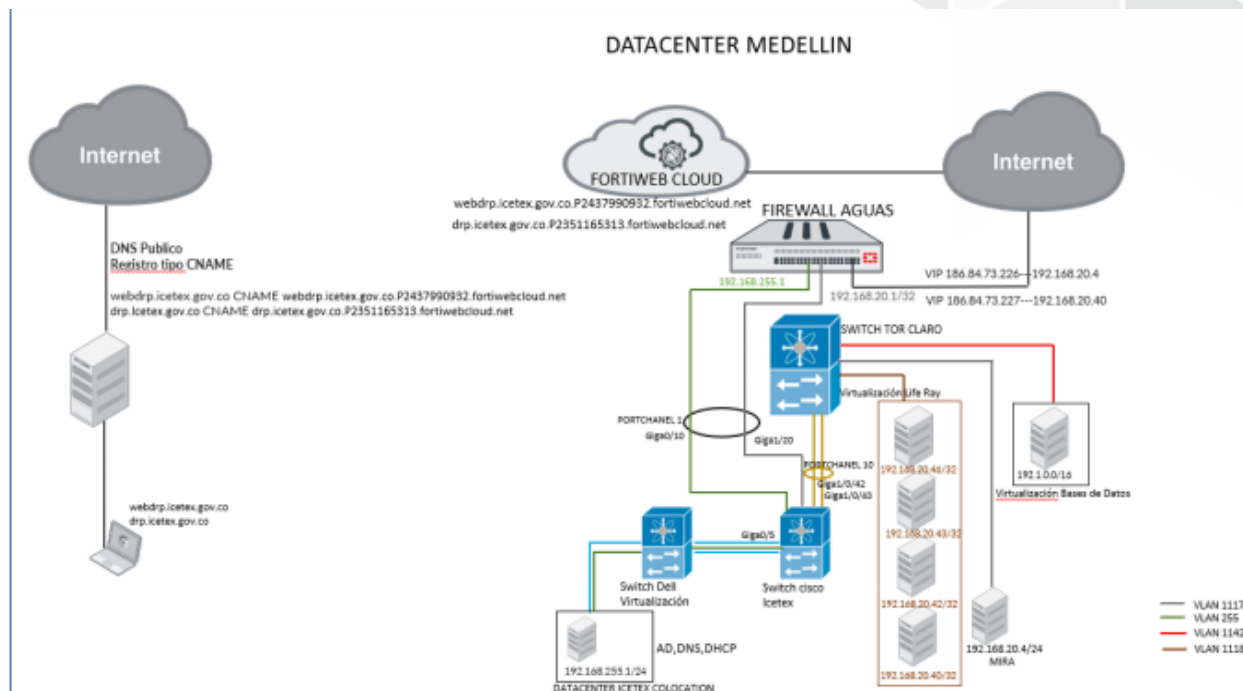


Ilustración 9 Topología de WAF Cloud usado en portales de Medellín

Durante el mes de Agosto de 2025, se llevaron a cabo diversas actividades relacionadas con la administración y gestión de la seguridad perimetral de la entidad.

En particular, se brindó apoyo en la identificación de un sitio fraudulento ([pagocreditoicetex.com/WebsitePSE/login.php](http://pagocreditoicetex.com/WebsitePSE/login.php)) y se trabajó en conjunto con el equipo de desarrollo para fortalecer los portales institucionales del SENA, con el fin de mitigar riesgos de plagio y suplantación.

En el ámbito de la gestión de políticas de seguridad, se realizaron configuraciones sobre IPv6, habilitando las reglas Policy\_web.icetex.gov.co\_IPV6 y Policy\_Intranet\_IPV6, asegurando la correcta protección del tráfico en dichos entornos.

Respecto al firewall de la red de Aguas, se mantienen actualmente 536 políticas activas, las cuales continúan en proceso de evaluación con el propósito de consolidar configuraciones, eliminar reglas innecesarias y optimizar la operación de la red.

Las evidencias de esta gestión fueron incluidas en el numeral 6.2 del informe mensual de especialistas de seguridad del mes de Agosto, link: [Informe Mensual InfoTIC Seguridad Agosto 2025.pdf](#)

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

### Gestión y fortalecimiento de la seguridad perimetral.

Durante el mes de Agosto se mantuvo una gestión activa de la seguridad perimetral y Endpoint, evidenciada en la atención de incidentes, requerimientos y tareas, así como en el monitoreo continuo de alertas mediante FortiSIEM, FortiGate, FortiWeb, Sophos y otros componentes del ecosistema de seguridad.

Sede principal-Bogotá, Colombia  
Calle 93B # 13-44, Segundo piso  
NIT:900.068.796-1  
Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
Cra. 24 No. 53ª-26 Arboleda Alta.  
NIT: 900.068.796-1  
Teléfono: (+606) 88612612

## Monitoreo de seguridad y respuesta ante incidentes

### Detección Oportuna de Amenazas

Se identificaron múltiples eventos de seguridad como intentos de acceso no autorizado a través de VPNs desde el extranjero, tráfico hacia indicadores de compromiso (IoC) y ataques de denegación de servicio (DoS). La oportuna intervención del equipo permitió contener las amenazas, minimizar el riesgo y ajustar las configuraciones para prevenir eventos futuros.

### Ajustes y Afinamientos en Políticas de Seguridad

Se realizaron labores de depuración y optimización en las reglas de firewall, eliminando políticas obsoletas, duplicadas o sin tráfico, especialmente en el firewall de Aguas, mejorando la eficiencia y mantenibilidad de las reglas. También se fortalecieron las configuraciones IPv6.

### Plataformas Actualizadas y con Buen Rendimiento

Los dispositivos FortiGate, FortiWeb y FortiSandbox se encuentran operativos con versiones estables de firmware y dentro de los parámetros normales de rendimiento (uso de CPU, memoria y sesiones). No obstante, se detectaron dispositivos con licenciamiento vencido o en etapa de fin de vida útil, como el FortiWeb 2000E y el FortiSandbox 1000D, lo cual requiere acciones próximas.

### Cobertura y Contención con Sophos Endpoint

Se bloquearon múltiples amenazas, en su mayoría variantes de malware HTML y troyanos, desde diversas fuentes, especialmente del dominio “crearfuturo.co” y sitios externos maliciosos. A pesar de la buena cobertura, se identificaron equipos sin conexión al sistema de protección durante más de 9 meses, recomendándose su revisión y eventual retiro.

#### 4.3.1. Plataformas Administradas

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

| SERIAL           | MODELO            | UBICACIÓN FÍSICA                | OBSERVACIONES                                             |
|------------------|-------------------|---------------------------------|-----------------------------------------------------------|
| FG6H0FTB22902021 | FortiGate 600F    | Aguas                           | Funciona como Firewall - Prestación como servicio INFOTIC |
| FG180FTK22901087 | FortiGate 1800F   | Data Center Triara              | Funciona como Firewall - Prestación como servicio INFOTIC |
| FG180FTK22901182 | FortiGate 1800F   | Backup Data Center Triara       | Funciona como Firewall - Prestación como servicio INFOTIC |
| FG6H0FTB22902086 | FortiGate 600F    | Data Center Megacenter Medellín | Funciona como Firewall - Prestación como servicio INFOTIC |
| FV-2KFTE21000029 | FortiWeb 2000F    | Data Center Triara              | Función como WAF - Prestación como servicio INFOTIC       |
| FMG2HGTA22000550 | FortiManager 200G | Data Center Triara              | Prestación como servicio INFOTIC                          |

| SERIAL           | MODELO                   | UBICACIÓN FÍSICA                  | OBSERVACIONES                                                          |
|------------------|--------------------------|-----------------------------------|------------------------------------------------------------------------|
| FSMP000000001340 | FortiSIEM                | Máquina Virtual VMware de cliente | Funciona como correlacionador de eventos - En VMware de Icetex         |
| FV-2KE3117000046 | FortiWeb 2000E           | Data Center Triara                | Función como WAF - Propiedad de Icetex                                 |
| FV-2KE3117000032 | FortiWeb 2000E           | Data Center Triara                | Función como WAF - Propiedad de Icetex                                 |
| FSA1KD3A17000156 | FortiSandbox 1000D       | Data Center Triara                | Funciona como Escaneo de archivos - Propiedad de Icetex                |
| FAC1KD3A17000020 | FortiAuthenticator 1000D | Data Center Triara                | Funciona para autenticación y CA de certificados - Propiedad de Icetex |
| FAC1KD3A17000036 | FortiAuthenticator 1000D | Data Center Triara                | Propiedad de Icetex                                                    |

*Tabla 14 Detalle plataformas Seguridad administradas INFOTIC*

A continuación, se presenta el estado actual de los tiempos de soporte y vigencias de los dispositivos FortiGate administrados:

| Dispositivo                     | IP          | Licenciamiento | Fin Licenciamiento | Datacenter |
|---------------------------------|-------------|----------------|--------------------|------------|
| <b>FW Fortigate 1800F (MST)</b> | 10.0.0.53   | Si             | 18/05/2026         | Triara     |
| <b>FW Fortigate 1800F (SLV)</b> | 10.0.0.53   | Si             | 18/05/2026         | Triara     |
| <b>FW FortiGate 600F</b>        | 10.0.0.30   | Si             | 1/06/2026          | Megacenter |
| <b>FW FortiGate 600F</b>        | 10.1.100.33 | Si             | 11/05/2026         | Aguas      |

*Tabla 15 Licenciamiento FortiGate*

#### 4.3.1.1. FortiGate Triara

A nivel de sistema, el firewall de Triara (FortiGate 1800F), no presenta afectaciones en cuanto a licenciamiento o performance; actualmente se encuentra en la versión de FortiOS 7.4.8. la cual fue actualizada en el mes de Agosto.

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

A continuación se presentan los consumos en el presente mes:

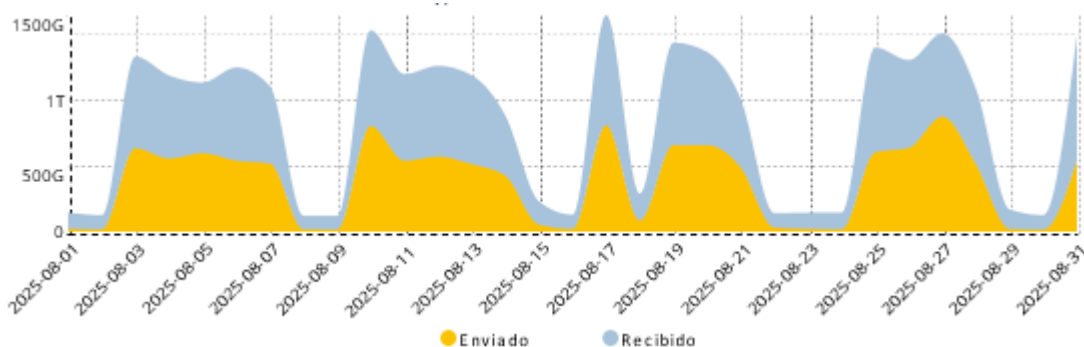


*Ilustración 10 Consumo canal MPLS - promedio 1200G [INR0185 CLARO(MPLS\_DC)]*

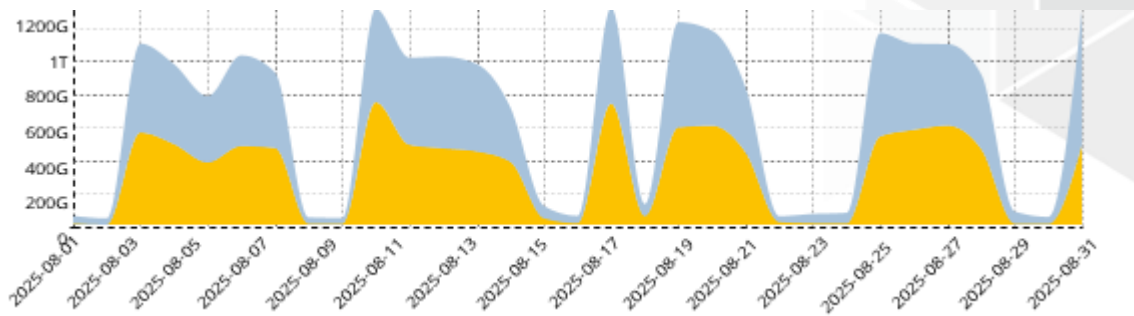


*Ilustración 11 Consumo Internet Sedes - Promedio 1100 GB WAN-SEDES-ICETEX [INR0264 (INTE\_SEDES\_ICTX)]*

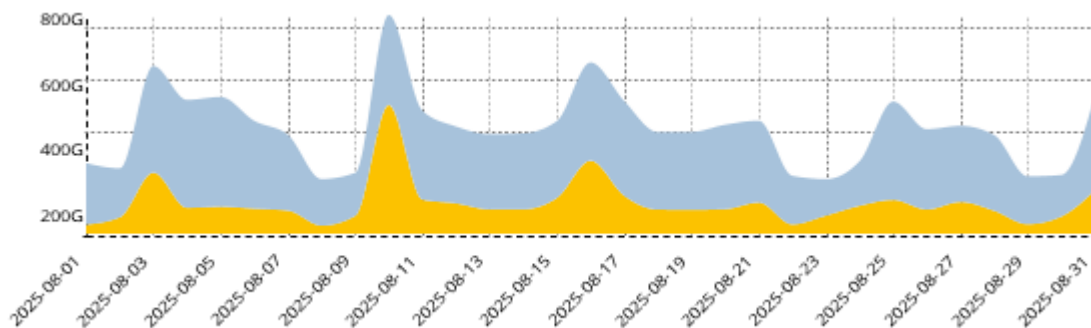


*Ilustración 12 Consumo Internet Data Center- INTERNET DATACENTER [INTERNET\_DC\_INR0000320 (Inet\_claro)]*

A nivel de perfiles de UTM (UTM son fragmentos de texto que se añaden al final de la URL y que sirven para rastrear, con mayor precisión, el origen de las visitas a una web), se tienen los siguientes perfiles para Web Filter, Antivirus y SSL Inspection actualmente:

|     | Name                            | Comments                                                           | Ref. |
|-----|---------------------------------|--------------------------------------------------------------------|------|
| WEB | default                         | Perfil con las mínimas restricciones                               | 0    |
| WEB | Navegacionpcs_Comware           | Perfil con restricciones                                           | 2    |
| WEB | Navegacionpcs_Comware_con_redes | Perfil con restricciones                                           | 1    |
| WEB | WF-Avanzado                     | Perfil para FSSO Navegación Avanzada                               | 31   |
| WEB | WF-Comunicaciones               | Perfil para FSSO comunicaciones                                    | 2    |
| WEB | WF-General                      | Perfil para todos                                                  | 5    |
| WEB | WF-General_Sedes                | Perfil para todos                                                  | 1    |
| WEB | WF-Sede_Ibague_YT               | 27022025/InfoTIC/Tarea Aranda 517214 (17458) Se solicita el acc... | 1    |
| WEB | WF-Tesoreria                    | Perfil con restricciones específicas por auditoria.                | 4    |
| WEB | WF-VIP                          | Perfil para FSSO Navegación_VIP                                    | 16   |
| WEB | WF-wetransfer                   | Perfil para FSSO Navegación Avanzada                               | 1    |
| WEB | wifi-default                    | Perfil de FULL acceso para pruebas                                 | 1    |

Ilustración 13 Filtrado – WEB – (FortiGate – Triara)

|     | Name                          | Comments                                    | Ref. |
|-----|-------------------------------|---------------------------------------------|------|
| SSL | custom-deep-inspection        | Customizable deep inspection profile.       | 0    |
| SSL | deep-inspection               | Read-only deep inspection profile.          | 0    |
| SSL | certificate-inspection_2780   | Read-only SSL handshake inspection profile. | 1    |
| SSL | certificate-inspection_IPv6   | Read-only SSL handshake inspection profile. | 1    |
| SSL | Prueba certificate-inspection | Read-only SSL handshake inspection profile. | 12   |
| SSL | certificate-inspection_ICETEX | SSL para BUS de servicios                   | 31   |
| SSL | no-inspection                 | Read-only profile that does no inspection.  | 230  |
| SSL | certificate-inspection        | Read-only SSL handshake inspection profile. | 400  |

Ilustración 14 Inspección – SSL – (FortiGate – Triara)

|    | Name         | Comments              | Ref. |
|----|--------------|-----------------------|------|
| AV | AV-FSB       | HTTP,SMTP FULL FSB    | 73   |
| AV | AV-HTTP      | HTTP con FSB          | 25   |
| AV | AV-HTTP&CIFS | HTTP,CIFS con FSB     | 4    |
| AV | AV-SMTP      | SMTP FULL FSB         | 1    |
| AV | default      | ALL con FSB           | 40   |
| AV | ICETEX       |                       | 65   |
| AV | prueba2      |                       | 57   |
| AV | wifi-default | ALL monitoreo sin FSB | 1    |

Ilustración 15 Antivirus y Antimalware – Perimetral (FortiGate – Triara)

#### 4.3.1.2. FortiGate Aguas

A nivel de sistema, el firewall de Aguas (FortiGate 600F), no presenta afectaciones en cuanto a licenciamiento o performance; actualmente se encuentra en la versión de FortiOS 7.4.8.

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

A continuación se presentan los consumos en el presente mes:

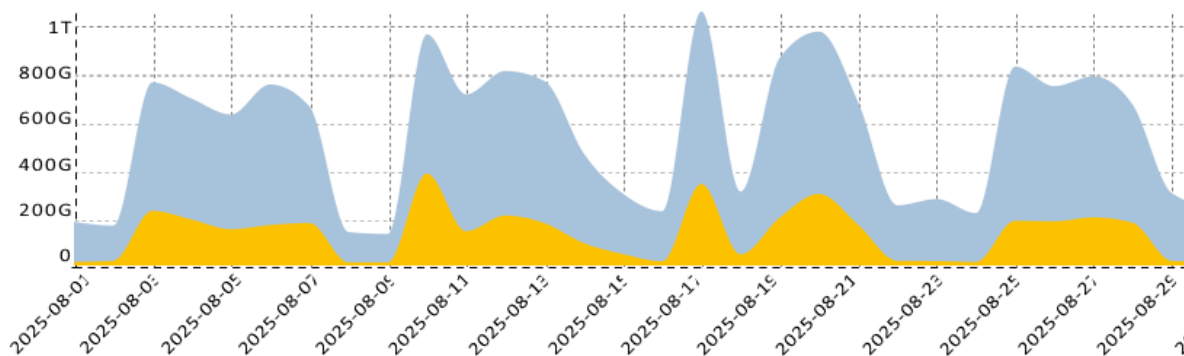


Ilustración 16 Consumo Canal MPLS Aguas - promedio 800 GB

A nivel de perfiles de UTM, se tienen los siguientes perfiles para Web Filter, Antivirus y SSL Inspección actualmente:

|     | Name             | Comments                                           | Ref. |
|-----|------------------|----------------------------------------------------|------|
| WEB | default          | Default web filtering.                             | 0    |
| WEB | General_Icetex   |                                                    | 51   |
| WEB | monitor-all      | Monitor and log all visited URLs, flow-based.      | 0    |
| WEB | VIP_FUNCIONARIOS |                                                    | 3    |
| WEB | wifi-default     | Default configuration for offloading WiFi traffic. | 1    |

Ilustración 17 Filtrado-Web-(FortiGate-Aguas)

|     | Name                          | Comments                                    | Ref. |
|-----|-------------------------------|---------------------------------------------|------|
| SSL | certificate-inspection        | Read-only SSL handshake inspection profile. | 275  |
| SSL | certificate-inspection_WX     | Read-only SSL handshake inspection profile. | 2    |
| SSL | custom-deep-inspection        | Customizable deep inspection profile.       | 0    |
| SSL | custom-deep-inspection_icetex | Customizable deep inspection profile.       | 0    |
| SSL | deep-inspection               | Read-only deep inspection profile.          | 0    |
| SSL | no-inspection                 | Read-only profile that does no inspection.  | 239  |

Ilustración 18 Inspección-SSL-(FortiGate-Aguas)

|     | Name                          | Comments                                    | Ref. |
|-----|-------------------------------|---------------------------------------------|------|
| SSL | certificate-inspection        | Read-only SSL handshake inspection profile. | 275  |
| SSL | certificate-inspection_WX     | Read-only SSL handshake inspection profile. | 2    |
| SSL | custom-deep-inspection        | Customizable deep inspection profile.       | 0    |
| SSL | custom-deep-inspection_icetex | Customizable deep inspection profile.       | 0    |
| SSL | deep-inspection               | Read-only deep inspection profile.          | 0    |
| SSL | no-inspection                 | Read-only profile that does no inspection.  | 239  |

Ilustración 19 Antivirus y Antimalware-Perimetral-(FortiGate-Aguas)

#### 4.3.1.3. FortiGate Medellín

A nivel de sistema, el firewall de Medellín (FortiGate 600F), no presenta afectaciones en cuanto a licenciamiento o performance; actualmente se encuentra en la versión de FortiOS 7.4.8. Para más información validar el portal del fabricante <https://docs.fortinet.com/product/fortigate/7.6>

Se observa en la Ilustración 18, que la interfaz de la MPLS del Data Center de Medellín no presenta tráfico debido a que este se tiene como Data Center Alterno.

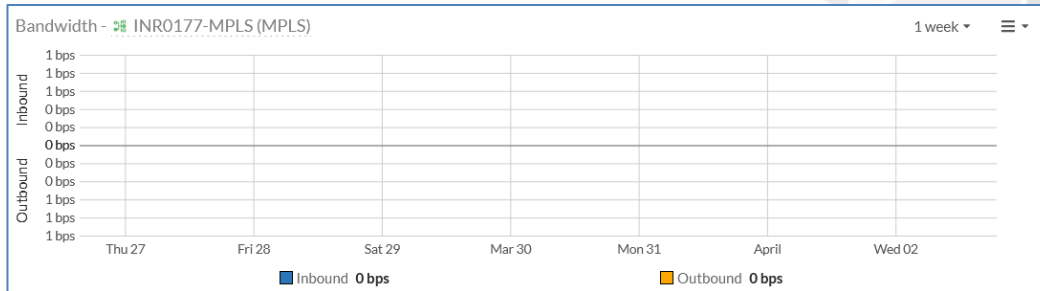


Ilustración 20 Consumo Canal MPLS Medellín

#### 4.3.1.4. FortiWeb 2000F

A nivel de sistema del FortiWeb su versión de firmware está en la 7.6.4 la cual es una de las versiones actuales más estables.

#### 4.3.1.5. FortiWeb 2000E

A nivel de sistema, el FortiWeb presenta su configuración actual y su versión de Firmware que actualmente se encuentra en la 7.6.4. Sin embargo, cabe aclarar que, a nivel de licenciamiento, los equipos no tienen un licenciamiento vigente en este momento.

| Dispositivo                 | IP            | Propiedad Icetex | Licenciamiento | Fin Licenciamiento | DC     | End Of Order | Last Service Extension | End of support |
|-----------------------------|---------------|------------------|----------------|--------------------|--------|--------------|------------------------|----------------|
| Fortiweb1 2000E (WAF) (MST) | 10.0.0.251    | SI               | No             | 20/06/2023         | Triara | 13/01/2022   | 13/01/2026             | 13/01/2027     |
| Fortiweb2 2000E (WAF) (SLV) | 10.0.0.251    | SI               | No             | 20/06/2023         | Triara | 13/01/2022   | 13/01/2026             | 13/01/2027     |
| Fortiweb1 2000F (WAF)       | 192.168.91.10 | No               | Si             | 1/06/2026          | Triara | N/A          | N/A                    | N/A            |

Tabla 16 Licenciamiento FortiWeb

En el mes, se presenta un promedio de 1200GB de tráfico general hacia los portales protegidos por el FortiWeb donde el portal de web.icetex.gov.co y www.icetex.gov.co fueron los más utilizados en este periodo, lo cual es un comportamiento normal para este tipo de transacciones de acuerdo con la actividad de los usuarios y las convocatorias vigentes.

| 2.2.Top Hosts per Response Bytes |                                |                     |
|----------------------------------|--------------------------------|---------------------|
| #                                | HTTP Host                      | HTTP Response Bytes |
| 1                                | web.icetex.gov.co              | 29.68 GB            |
| 2                                | www.icetex.gov.co              | 7.36 GB             |
| 3                                | aplicaciones.icetex.gov.co     | 2.61 GB             |
| 4                                | comunidad.icetex.gov.co        | 153.42 MB           |
| 5                                | identidad.icetex.gov.co        | 1.97 MB             |
| 6                                | web.icetex.gov.co:443          | 1.83 MB             |
| 7                                | comunidad.icetex.gov.co:443    | 1.35 MB             |
| 8                                | appsitiospruebas.icetex.gov.co | 822.69 KB           |
| 9                                | 186.84.73.163                  | 650.76 KB           |
| 10                               | 186.84.73.154                  | 643.16 KB           |

Ilustración 21 Tráfico General de los portales

#### 4.3.1.6. FortiWebCloud DRP

A nivel de sistema, el FortiWeb que se tienen en nube presenta su configuración la versión actual es 25.3.a, se encuentran pasando dos portales.

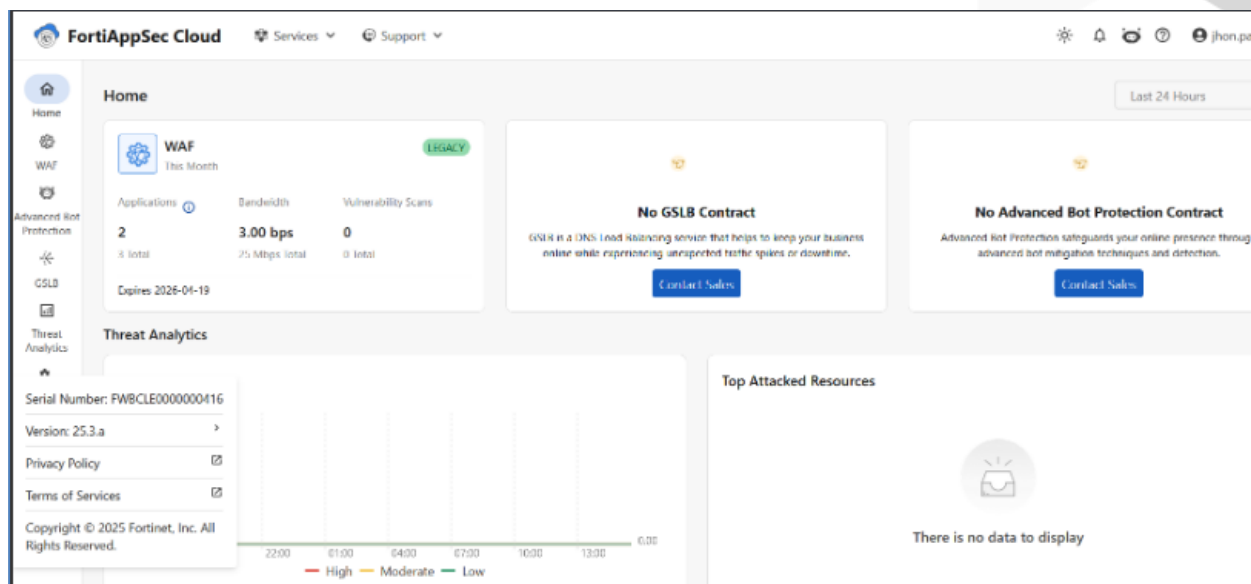


Ilustración 22 Tráfico General de los portales

#### 4.3.1.7. FortiSandBox

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

| Dispositivo        | IP         | Propiedad Ictetex | Licenciamiento | Fin Licenciamiento | DC     | End Of Order | Last Service Extension | End of support |
|--------------------|------------|-------------------|----------------|--------------------|--------|--------------|------------------------|----------------|
| FortiSandbox 1000D | 10.0.0.249 | Si                | No             | 1/06/2023          | Triara | 2/04/2019    | 2/04/2023              | 2/04/2024      |

Tabla 17 Configuración FortiSandBox 1000D

#### 4.3.1.7. FortiSIEM

Debido a problemas de rendimiento en la plataforma FortiSIEM ocasionados principalmente por la falta de recursos de hardware, en particular de CPU, la cual se ha mantenido con un uso sostenido del 100% por más de 7 días y que ha sido reportada en reiteradas ocasiones por el SOC, se presentan inconvenientes para consultar información sobre este dispositivo. Se reitera la necesidad de renovar el soporte y las capacidades de este dispositivo, aspectos que se encuentran a cargo del ICETEX.

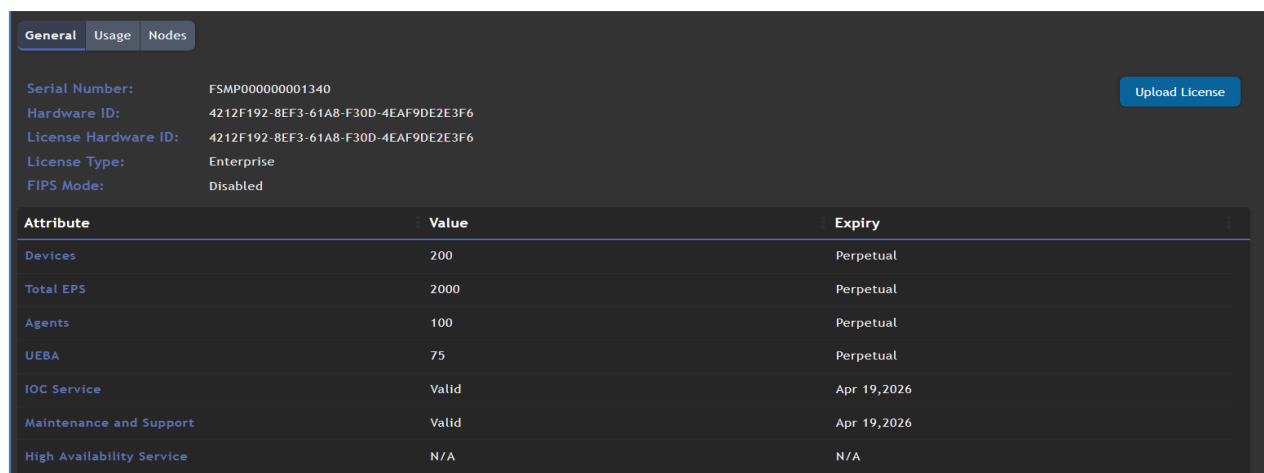
Resultado de esta situación, no ha sido posible realizar las siguientes acciones esenciales para el funcionamiento del SOC:

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

- Generación del informe mensual: No es posible generar el informe de manera completa debido a los errores continuos en la plataforma, lo que impide procesar adecuadamente la información necesaria para su elaboración.
- Monitoreo diario de eventos: La incapacidad para procesar los eventos en tiempo real afecta la visibilidad de las alertas y eventos críticos, limitando la capacidad de monitoreo y respuesta oportuna.

Es importante señalar que esta situación está afectando gravemente la calidad y disponibilidad del servicio de monitoreo.



| General Usage Nodes            |                                      |              |
|--------------------------------|--------------------------------------|--------------|
| Serial Number:                 | FSMP000000001340                     |              |
| Hardware ID:                   | 4212F192-8EF3-61A8-F30D-4EAF9DE2E3F6 |              |
| License Hardware ID:           | 4212F192-8EF3-61A8-F30D-4EAF9DE2E3F6 |              |
| License Type:                  | Enterprise                           |              |
| FIPS Mode:                     | Disabled                             |              |
| <a href="#">Upload License</a> |                                      |              |
| Attribute                      | Value                                | Expiry       |
| Devices                        | 200                                  | Perpetual    |
| Total EPS                      | 2000                                 | Perpetual    |
| Agents                         | 100                                  | Perpetual    |
| UEBA                           | 75                                   | Perpetual    |
| IOC Service                    | Valid                                | Apr 19, 2026 |
| Maintenance and Support        | Valid                                | Apr 19, 2026 |
| High Availability Service      | N/A                                  | N/A          |

Ilustración 23 Licenciamiento FortiSIEM

#### 4.3.1.8. Sophos Endpoint

En la ilustración 21, se observa un resumen del estado de Seguridad del Endpoint donde actualmente se están cumpliendo en un 100% los puntos de seguridad de la plataforma de Sophos indicando protección de equipos, políticas y exclusiones.



Ilustración 24 Estado Seguridad Sophos

En cuanto al licenciamiento se cuenta con una vigencia hasta el 26 de junio de 2026.

Los cuatro equipos de la ilustración 41, que se encuentran no protegido son: BOGARRIENDO88, BOGIMAC01, BOGVFAPC502, COWORKING11 y llevan más de 9 meses en algunos casos de con no

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

conectarse, recomendamos que la mesa revise los equipos.

En la sección 6.6.1 del informe de seguridad [Informe Mensual InfoTIC Seguridad Agosto 2025.pdf](#) se detallan las amenazas contenidas por la herramienta el Sophos instalado en los equipos ordenadores y servidores.

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

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. Actualmente el motor de búsqueda de amenazas está distribuido en cuatro criterios de búsqueda y correlación, los cuales son: compromiso del sistema, explotación e instalación de agentes maliciosos, entrega y ataque, reconocimiento y sondeo y finalmente advertencia ambiental o anomalías detectadas sobre el rendimiento de la máquina. Dichos criterios distribuyen los alertas e incidentes de esta manera de acuerdo con el match que el sistema ejecute y categorice dentro de sus reglas de correlación previamente configuradas o implementadas por defecto. Las cuales detectan alertas e incidentes de tipo:

- Descarga de ejecutables sospechosos provenientes de un sitio de mala reputación
- Actividad de escaneo en la red, en función de descubrimiento de puertos
- Violación, infracción y vulneración de políticas de seguridad
- Detección de malware
- Detección de ataques (Fuerza Bruta, puerta trasera (Shell), Botnet o kit de explotación de un sitio malicioso, XSS, Inyección de SQL, DoS.
- Monitoreo de alertas de autenticación
- Monitoreo de alertas de sistema
- Monitoreo de alarmas y alertas de seguridad
- Monitoreo de accesibilidad
- Monitoreo de bases de datos
- Alertas e incidentes de tráfico y navegación
- Alertas de acceso permitido a páginas web maliciosas o de baja reputación

A la fecha de presentación de este informe se encuentran definidas 2.382 reglas de seguridad, las cuales, tienen como fin reconocer cualquier posible vector de ataque, así como verificar que los equipos de seguridad perimetral (Firewall, IPS, NAC, etc.), estén bien configurados a nivel de sus políticas de seguridad.

Para los casos de uso de disponibilidad se cuenta con 174 reglas, que tienen como función principal alertar algún tipo de falla o indisponibilidad de los equipos de la entidad y hacer la respectiva notificación, en caso de requerirse, al ICETEX.

Para cualquier detalle relacionado con las reglas puede consultarse en el siguiente enlace [Informe Mensual SOC-TH ICETEX Agosto 2025.pdf](#)

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

#### **Indicadores de compromiso (Thread Hunting):**

Un indicador de compromiso puede venir dado bajo la forma de un nombre de archivo, el nombre de un proceso en el administrador de tareas, una URL o dirección IP, comportamiento anómalo en el tráfico web,

intentos de inicio de sesión fallidos, entre otros tantos más.

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

| Indicadores de compromiso (IOC) | Agosto | Julio  | Junio | Mayo  |
|---------------------------------|--------|--------|-------|-------|
| IOC – Malware DOMINIOS          | 6.047  | 6.047  | 3.919 | 3.919 |
| IOC – Malware IPs               | 11.189 | 11.031 | 8.483 | 5.278 |
| IOC – Malware HASH              | 1.627  | 1.627  | 1.621 | 1.612 |
| IOC – Malware URL               | 4.564  | 4.564  | 780   | 780   |

*Tabla 18 Comparativo – Indicadores de Compromiso*

Después de efectuado el registro de alertas se considera y diseña la generación de alertas y niveles de criticidad, acorde con la experiencia del equipo consultor, aplicación de buenas prácticas y reuniones de trabajo efectuadas a nivel de infraestructura tecnológica alineado con el proceso de levantamiento de riesgos.

De acuerdo con las conexiones y las reglas configuradas sobre la herramienta de monitoreo SOC FortiSIEM, el cual analiza las alertas en busca de patrones de comportamiento inusuales; estas reglas estudian y conectan las alertas para evaluar su prioridad y confiabilidad.

En el Informe del SOC se presentan gráficas y tablas de los tipos de alertas presentados durante el periodo monitoreado de: Seguridad – Disponibilidad – Rendimiento, donde estos a su vez se encuentran distribuidos con niveles de severidad con tres colores:

- Rojo: severidad o criticidad ALTO (10-9)
- Amarillo: severidad o criticidad MEDIO (6-8)
- Verde: severidad o criticidad BAJO (1-5)

#### **4.3.3.1. Alertas o Incidentes de Seguridad Detectados**

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

##### **4.3.3.1.1. Categoría Seguridad**

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

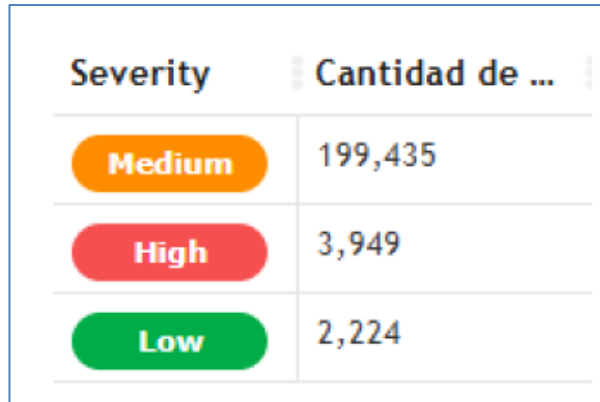


Ilustración 25 Total de alertas de seguridad

Durante el período evaluado de 205.609 alertas de seguridad identificadas, se presentaron con criticidad ALTA un total de 3.949 , equivalentes al 1,9% del periodo. En el informe mensual del SOC, se puede observar la cantidad según el tipo de alerta y se realiza una descripción de los tipos de alertas que mayor cantidad de registros o que requieran una indagación más exacta. El comparativo, en los últimos 5 meses, se presenta a continuación:

| Severidad | Alertas de Seguridad Agosto | Alertas de Seguridad Julio | Alertas de Seguridad junio | Alertas de Seguridad mayo | Alertas de Seguridad abril |
|-----------|-----------------------------|----------------------------|----------------------------|---------------------------|----------------------------|
| High      | 3.949                       | 1.536                      | 825                        | 740                       | 2.897                      |
| Medium    | 199.433                     | 9.711                      | 12.459                     | 9.806                     | 10.710                     |
| Low       | 2.224                       | 193                        | 174                        | 198                       | 210                        |

Tabla 19 comparativo Alertas de Seguridad

Durante el período evaluado se presentaron 199.435 alertas de seguridad con criticidad MEDIA, un incremento bastante elevado con relación a periodos anteriores. En el En el documento [Informe Mensual SOC-TH ICETEX Agosto 2025.pdf](#) se presenta la cantidad según el tipo de alerta y se realiza una descripción de los tipos de alertas que mayor cantidad de registros o que requieran una indagación más exacta.

En cuanto a las alertas altas, el top 5 se presenta a continuación:

| Chart                               | Event Name                                                                    | Criticidad | Criticidad | Tactica           | Cantidad de Alertas |
|-------------------------------------|-------------------------------------------------------------------------------|------------|------------|-------------------|---------------------|
| <input checked="" type="checkbox"/> | Concurrent Failed Authentications To Same Account From Multiple Countries     | High       | 9          | Credential Access | 1,182               |
| <input checked="" type="checkbox"/> | Website access policy violation: High volume WYN2                             | High       | 9          |                   | 595                 |
| <input checked="" type="checkbox"/> | Repeated Multiple Logon Failures: Domain                                      | High       | 9          | Credential Access | 444                 |
| <input checked="" type="checkbox"/> | Website access policy violation: Multiple categories                          | High       | 9          |                   | 399                 |
| <input checked="" type="checkbox"/> | Concurrent Successful Authentications To Same Account From Multiple Countries | High       | 9          | Credential Access | 384                 |

Ilustración 26 Top 5 de Alertas de Seguridad Altas

NOTA: Debido a las limitantes de recursos de la herramienta FortiSIEM no se puede realizar un análisis preciso de las alertas.

#### 4.3.3.1.2. Categoría Disponibilidad

Durante el período evaluado se presentaron 944 alertas de disponibilidad con criticidad ALTA, a continuación, se puede observar la cantidad según el tipo de alerta y se realiza una descripción de los tipos de alertas que mayor cantidad de registros presentaron y se realiza una descripción de los tipos de alertas que mayor cantidad de registros presentaron:

| Chart                               | Event Name                                                  | Criticidad | Criticidad | Tactica | Cantidad de Alertas |
|-------------------------------------|-------------------------------------------------------------|------------|------------|---------|---------------------|
| <input checked="" type="checkbox"/> | Network Device Down: no ping response - WX N3               | High       | 10         | Impact  | 613                 |
| <input checked="" type="checkbox"/> | Server Down: No Ping Response ICETEX                        | High       | 10         |         | 2                   |
| <input checked="" type="checkbox"/> | WMI or OMI Service Unavailable                              | High       | 9          | Impact  | 184                 |
| <input checked="" type="checkbox"/> | Network Device Hardware Critical                            | High       | 9          |         | 17                  |
| <input checked="" type="checkbox"/> | SNMP Service Unavailable                                    | High       | 9          | Impact  | 15                  |
| <input type="checkbox"/>            | FortiSIEM Agent Operational Error WXN2                      | High       | 9          |         | 10                  |
| <input type="checkbox"/>            | EventDB: Event Retention Policy Violation                   | High       | 9          |         | 6                   |
| <input type="checkbox"/>            | Excessive Clock Skew Between Collector and Supervisor nodes | High       | 9          |         | 2                   |
| <input type="checkbox"/>            | Windows Cluster Service Startup Error                       | High       | 9          |         | 2                   |
| <input type="checkbox"/>            | Windows Cluster Service Quorum Error                        | High       | 9          |         | 1                   |
| <input type="checkbox"/>            | Service Down: No Response PSE ICETEX                        | High       | 9          | Impact  | 1                   |

*Ilustración 27 Top 5 de Alertas de Disponibilidad Altas*

A continuación, se presentan los análisis efectuados:

- “Network Device Down: no ping response - WX N3” – se genera cuando Detecta que un dispositivo no responde al ping. Se pierden 10 de cada 10 paquetes de ping. Esto puede deberse a que el host está inactivo o a un problema de enrutamiento.
- “EventDB: Event Retention Policy Violation” – se genera cuando Detecta violaciones de la política de retención de eventos. Esto podría indicar que se están eliminando, modificando o reteniendo logs de manera parcial, incumpliendo las políticas definidas por la entidad.
- “WMI or OMI Service Unavailable” – Esta alerta se genera cuando Detecta que el servicio WMI u OMI no está disponible. Nota: Se recomienda verificar el estado de los protocolos WMI de los dispositivos relacionados, los cuales se utilizan para enviar eventos de seguridad al SIEM; de lo contrario informar al SOC si el dispositivo se encuentra fuera de servicio con el fin de depurar y actualizar la base de datos del FortiSIEM – CMDB.
- “FortiSIEM Agent Operational Error WXN2” – Esta alerta se genera cuando se detectan errores operativos del agente FortiSIEM Linux/Windows: se desinstala, se detiene y no responde.

#### 4.3.3.1.2. Amenazas de Ciberseguridad

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

- **Top Ataques IPS:** Se representa el Top de los ataques IPS permitidos y denegados detectados por los dispositivos de ciberseguridad perimetral. Se recomienda el bloqueo de los ataques de severidad alta detectados por el IPS y verificar los eventos o alertas de severidad media.

| Top de Ataques IPS Permitidos    |                      |              |          |                |                 |
|----------------------------------|----------------------|--------------|----------|----------------|-----------------|
| Reporting Device                 | Attack Name          | Signature Id | Severity | COUNT(Match... | Firewall Action |
| 39 DC_FG_MST_ICETEX.icetex.local | DNS PTR Records Scan | 51391        | Low      | 5,357          | detected        |
| 1 DCAGUAS_FG_MST_ICETEX          | TCP Split Handshake  | 26339        | Medium   | 199            | detected        |

Ilustración 28 ataques IPS permitidos

| Reporting Device                | Attack Name                                | Signature Id | Severity | COUNT(Matched Events) | Firewall Action |
|---------------------------------|--------------------------------------------|--------------|----------|-----------------------|-----------------|
| 7 DC_FG_MST_ICETEX.icetex.local | Nmap Script Scanner                        | 45360        | Medium   | 1,593                 | dropped         |
| 7 DC_FG_MST_ICETEX.icetex.local | ZGrab Scanner                              | 48805        | Medium   | 572                   | dropped         |
| 7 DC_FG_MST_ICETEX.icetex.local | PHPUnit Eval-stdin PHP Remote Code Exec... | 45765        | Medium   | 442                   | dropped         |
| 7 DC_FG_MST_ICETEX.icetex.local | ALFA TEaM Web Shell                        | 53229        | Medium   | 262                   | dropped         |
| 7 DC_FG_MST_ICETEX.icetex.local | WordPress REST API Username Enumeratio...  | 48072        | Medium   | 217                   | dropped         |
| 7 DC_FG_MST_ICETEX.icetex.local | Bash Function Definitions Remote Code E... | 39294        | Medium   | 80                    | dropped         |
| 7 DC_FG_MST_ICETEX.icetex.local | Apache HTTP Server cgi-bin Path Traversal  | 50825        | Medium   | 75                    | dropped         |
| 7 DC_FG_MST_ICETEX.icetex.local | Mirai Botnet                               | 43191        | Medium   | 69                    | dropped         |
| 7 DC_FG_MST_ICETEX.icetex.local | Linux Kernel TCP SACK Panic DoS            | 48103        | Medium   | 66                    | dropped         |
| 7 DC_FG_MST_ICETEX.icetex.local | SystemBC Botnet                            | 49827        | Medium   | 62                    | dropped         |
| 7 DC_FG_MST_ICETEX.icetex.local | Multiple Routers GPON formLogin Remote...  | 52588        | Medium   | 53                    | dropped         |
| 7 DC_FG_MST_ICETEX.icetex.local | Masscan Scanner                            | 44778        | Medium   | 40                    | dropped         |
| 7 DC_FG_MST_ICETEX.icetex.local | AndroXGh0st Malware                        | 52567        | Medium   | 33                    | dropped         |
| 7 DC_FG_MST_ICETEX.icetex.local | PHP Malicious Shell                        | 44580        | Medium   | 32                    | dropped         |
| 7 DC_FG_MST_ICETEX.icetex.local | PHP CGI Argument Injection                 | 31752        | Medium   | 31                    | dropped         |

Ilustración 29 ataques IPS denegados

- **Top Perímetro:** A continuación de presentan el TOP de los eventos o tráfico de red organizado por los puertos TCP/UDP que más recibieron o enviaron bytes hacia Internet. Principales Puertos Entrantes por Conexiones (Tráfico Permitido).

| IP Protocol | Destination TCP/UDP Port | COUNT(Matched Events) | SUM(Sent Bytes64) | SUM(Received Bytes64) | SUM(Total Bytes64) |
|-------------|--------------------------|-----------------------|-------------------|-----------------------|--------------------|
| 6 (TCP)     | 443 (HTTPS)              | 1,905,995             | 196.7 GB          | 408.89 GB             | 605.59 GB          |
| 17 (UDP)    | 443                      | 43,174                | 3.01 GB           | 4.9 GB                | 7.92 GB            |
| 1 (ICMP)    | 0                        | 23,633                | 1.78 MB           | 1.78 MB               | 3.57 MB            |
| 6 (TCP)     | 80 (HTTP)                | 18,286                | 103.04 MB         | 3.01 GB               | 3.11 GB            |
| 17 (UDP)    | 53 (DOMAIN)              | 3,699                 | 7.32 MB           | 15.34 MB              | 22.67 MB           |
| 6 (TCP)     | 440 (SGCP)               | 3,012                 | 11.7 MB           | 94.62 MB              | 106.32 MB          |
| 6 (TCP)     | 458 (APPLEQTC)           | 2,889                 | 4.84 GB           | 202.77 MB             | 5.04 GB            |
| 17 (UDP)    | 123 (NTP)                | 2,024                 | 177.27 KB         | 92.59 KB              | 269.87 KB          |
| 6 (TCP)     | 5228                     | 1,521                 | 19.97 MB          | 33.21 MB              | 53.19 MB           |
| 17 (UDP)    | 547 (DHCPv6-SERVER)      | 1,293                 | 3.66 MB           | 18.98 KB              | 3.68 MB            |
| 6 (TCP)     | 5222                     | 842                   | 195.92 MB         | 456.44 MB             | 652.36 MB          |
| 17 (UDP)    | 389 (LDAP)               | 772                   | 225.33 KB         | 176.3 KB              | 401.63 KB          |
| 17 (UDP)    | 3478                     | 688                   | 2.91 MB           | 3.68 MB               | 6.6 MB             |
| 17 (UDP)    | 500 (IPSec1)             | 495                   | 588.69 KB         | 682.16 KB             | 1.24 MB            |
| 17 (UDP)    | 3480                     | 277                   | 7.34 GB           | 15.55 GB              | 22.9 GB            |

*Ilustración 30 Puertos entrantes de público a privado (Permitidos)*

Se recomienda verificar si es necesario mantener expuestos a internet de los siguientes puertos conocidos como el 53 (DOMAIN), 123 (NTP) los cual comúnmente son autorizados como puertos de salida y no de entrada, así mismo confirmar otros puertos conocidos como el 440 (SGCP), 458 (APPLEQTC), 547 (DHCP) 447 (DDM-DFM), 389 (LDAP) los cuales en su mayoría son utilizados en entornos LAN o privados.

#### Principales Puertos Salientes por Conexiones (Tráfico Permitido)

| IP Protocol | Destination TCP/UDP Port | COUNT(Matched Events) | SUM(Sent Bytes64) | SUM(Received Bytes64) | SUM(Total Bytes64) |
|-------------|--------------------------|-----------------------|-------------------|-----------------------|--------------------|
| 6 (TCP)     | 443 (HTTPS)              | 25,777,958            | 9.66 TB           | 5.24 TB               | 14.91 TB           |
| 17 (UDP)    | 53 (DOMAIN)              | 3,535,172             | 1.13 GB           | 2.26 GB               | 3.39 GB            |
| 17 (UDP)    | 443                      | 2,599,292             | 342.83 GB         | 571.08 GB             | 1013.91 GB         |
| 6 (TCP)     | 80 (HTTP)                | 1,539,747             | 108.82 GB         | 419.68 GB             | 528.5 GB           |
| 6 (TCP)     | 5228                     | 617,790               | 19.48 GB          | 27.97 GB              | 47.45 GB           |
| 6 (TCP)     | 25 (SMTP)                | 501,765               | 375.2 MB          | 751.49 MB             | 1.1 GB             |
| 6 (TCP)     | 4001 (Moxa.Modbus.RTU)   | 184,078               | 46.02 MB          | 49.27 MB              | 95.29 MB           |
| 6 (TCP)     | 587 (SUBMISSION)         | 167,771               | 298.59 MB         | 289.7 MB              | 588.3 MB           |
| 6 (TCP)     | 8810                     | 167,303               | 36.33 GB          | 34.38 GB              | 70.71 GB           |
| 17 (UDP)    | 123 (NTP)                | 155,631               | 86.52 GB          | 86.42 GB              | 172.95 GB          |
| 6 (TCP)     | 5222                     | 128,798               | 12.23 GB          | 31.45 GB              | 43.68 GB           |
| 17 (UDP)    | 3478                     | 123,258               | 102.17 GB         | 556.67 GB             | 658.84 GB          |
| 6 (TCP)     | 8812                     | 97,277                | 351.03 GB         | 577.96 GB             | 928.99 GB          |
| 17 (UDP)    | 4000 (ICQ)               | 95,412                | 405.26 MB         | 832.89 MB             | 1.2 GB             |
| 6 (TCP)     | 8445                     | 64,338                | 39.25 GB          | 1.83 TB               | 1.87 TB            |

*Ilustración 31 Puertos saliente de público a privado (Permitidos)*

Se recomienda verificar si es necesario mantener tráfico hacia internet a través de los siguientes puertos conocidos como: 4001(Moxa Modbus RTU – Protocolo usado en entornos industriales/SCADA), 25(SMTP – Envío de correo electrónico no seguro), 5228(Google Play Services – Utilizado por dispositivos Android para

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

actualizaciones), 4000(Mensajería ICQ, obsoleta y desactualizada)

Top de Accesos Fallidos plataforma Windows:

| Reporting Device       | User         | ▼ COUNT(Matched Events) |
|------------------------|--------------|-------------------------|
| 61 DC_FG_MST_ICETEX... | 31 apineda   | 80                      |
| 61 DC_FG_MST_ICETEX... | 45 ldiaza    | 77                      |
| 61 DC_FG_MST_ICETEX... | 34 mramireza | 59                      |
| 61 DC_FG_MST_ICETEX... | aropero      | 58                      |
| 61 DC_FG_MST_ICETEX... | nmercado     | 54                      |
| 61 DC_FG_MST_ICETEX... | account      | 48                      |
| 61 DC_FG_MST_ICETEX... | 62 yarguello | 47                      |
| 61 DC_FG_MST_ICETEX... | scan         | 41                      |
| 61 DC_FG_MST_ICETEX... | scanner      | 40                      |
| 61 DC_FG_MST_ICETEX... | 21 asotoc    | 38                      |
| 61 DC_FG_MST_ICETEX... | nalzate      | 36                      |

Ilustración 32 Fallos de Inicio de sesión VPN

| Failed Unix Login |          |                   |         | Last 1 |
|-------------------|----------|-------------------|---------|--------|
| Source IP         | User     | Server            | COUNT(A |        |
| 90 192.1.1.100    | pghauser | 90 FORTISIEM ICTX | 2       |        |

Ilustración 33 Fallos de Inicio de sesión Unix

| Server                    | User    | COUNT(Mat... |
|---------------------------|---------|--------------|
| 51 ictxsrvfs.icetex.local | Soporte | 4            |

Ilustración 34 Cuentas bloqueados

Debido a las limitantes de recursos de la herramienta FortiSIEM no se puede realizar la extracción de información de los intentos de logon fallidos en Windows.

#### 4.3.3.1.4. Threat Hunting

Se lleva a cabo el proceso de "Threat Hunting" de manera proactiva mediante la realización de boletines de ciber amenazas y la utilización de la plataforma MISP (Malware Information Sharon Platform) del First (Forum of Incident Response Team), los boletines pueden ser consultado en el numeral 4.4 Boletines del [Informe Mensual SOC-TH ICETEX Agosto 2025.pdf](#)

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

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

Los indicadores de compromiso - IoC fueron recopilados por intercambio de información con algunas instituciones del Estado Colombiano, inteligencia de amenazas en plataformas públicas o privadas, como el FIRST, CISA, CSIRT'S y caza de amenazas en plataformas de ciberseguridad. Los análisis de dichos indicadores, así como sus recomendaciones se encuentran consignados en el documento [Informe Mensual SOC-TH ICETEX Agosto 2025.pdf](#), **es importante resaltar que Todo el tráfico fue bloqueado**, sin embargo, se recomienda la verificación de los equipos con las direcciones IP origen privada.

Además se detectaron accesos a través de la aplicación Anydesk, software de acceso remoto de escritorio que permite a los usuarios controlar y acceder a computadoras y dispositivos de forma remota y utilizar en su lugar conexiones VPN. Se recomienda revisar el uso de dicho software.

| Source IP     | Destination IP | Event Action | COUNT(i |
|---------------|----------------|--------------|---------|
| 172.16.222.51 | 46.246.14.13   | 1 (Deny)     | 32      |
| 172.16.222.26 | 46.246.14.13   | 0 (Permit)   | 10      |
| 172.16.222.26 | 46.246.14.13   | 1 (Deny)     | 10      |
| 172.16.222.51 | 46.246.14.13   | 0 (Permit)   | 8       |
| 172.16.222.26 | 46.246.14.13   | 0 (Permit)   | 6       |
| 172.16.222.26 | 46.246.14.13   | 1 (Deny)     | 6       |
| 172.16.222.26 | 46.246.14.13   | 0 (Permit)   | 4       |

*Ilustración 35 Accesos detectados a través de la aplicación Anydesk*

#### 4.3.4. Análisis de Vulnerabilidades ICETEX

Durante el mes de agosto de 2025, se ejecutó satisfactoriamente el análisis de vulnerabilidades correspondiente a la Fase 6 del plan de trabajo, abordando el segundo bloque de activos planificados para

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

este ciclo. En esta etapa se evaluaron 76 activos, compuestos por 28 bases de datos y 48 equipos de usuario final en línea con la planificación mensual establecida para avanzar progresivamente en la cobertura del entorno completo.

Cabe destacar que la Fase 5 (abril) cubrió el 100% de los activos definidos inicialmente, lo cual sirvió como base para establecer una línea de referencia. A partir de la Fase 6 (mayo-junio), el enfoque se centró en revisar segmentos parciales del entorno en función del plan mensual, estimando una cobertura del 50% del total de activos durante esta fase.

El balance de toda esta fase se resume a continuación:

- Mayo: Se ejecutaron pruebas sobre 76 servidores.
- Junio: Se evaluaron 65 servidores adicionales y 11 dispositivos de red (switches).
- Julio: Se evaluaron 23 dispositivos de red (switches), 8 dispositivos de seguridad perimetral, 43 aplicaciones o portales web internos y 2 bases de datos Oracle.
- Agosto: Se evaluaron 28 bases de datos y 48 equipos de usuario final

Durante el análisis no se identificaron vulnerabilidades críticas; sin embargo, se reportaron hallazgos de severidad alta, media y baja, principalmente asociados a configuraciones criptográficas inseguras, tales como: PROCESO DE CONSULTORÍA Formato de informe técnico Código Versión F. Aprobación Página WX-IINFR-06 01 02/06/2023 5 de 46.

Protocolos inseguros expuestos en servicios críticos, incluyendo soporte de TLS 1.0 y TLS 1.1, obsoletos y sin soporte oficial desde 2020.

Cifrados de mediana y baja fortaleza habilitados, entre ellos 3DES y CBC, lo que expone los servicios a ataques criptográficos conocidos como SWEET32.

Se mantiene un alto nivel de obsolescencia tecnológica en componentes clave, lo que incrementa el riesgo general de la infraestructura. Los hallazgos actuales respaldan la necesidad de priorizar acciones correctivas y mejoras en configuración y actualización de sistemas.

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

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

A 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 Analisis De Vulnerabilidades ICETEX Agosto2025.pdf](#)

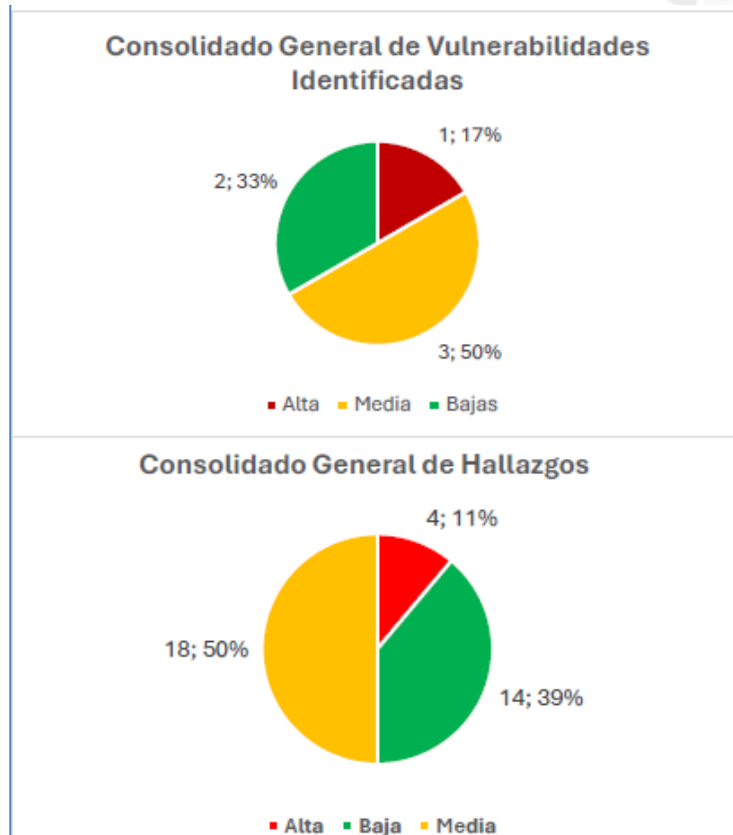


*Ilustración 36 Cantidad Total de Hallazgos identificados*

#### 4.3.4.1. Resumen de Vulnerabilidades

La recomendación fundamental es desarrollar e implementar un plan de mitigación de vulnerabilidades, priorizando la actualización tecnológica, el fortalecimiento de protocolos y la migración a versiones de la plataforma base (sistemas operativos, bases de datos, etc.). Para efectos de apoyar el cierre de vulnerabilidades, según requerimientos de ICETEX, se sugiere realizar una mesa técnica para revisar las alternativas de solución.

El resumen de las vulnerabilidades se puede revisar a más detalle en el numeral 11. Resumen de vulnerabilidades del [Informe Tecnico Analisis De Vulnerabilidades ICETEX Agosto2025.pdf](#)

Destacan en los hallazgos las siguientes vulnerabilidades:

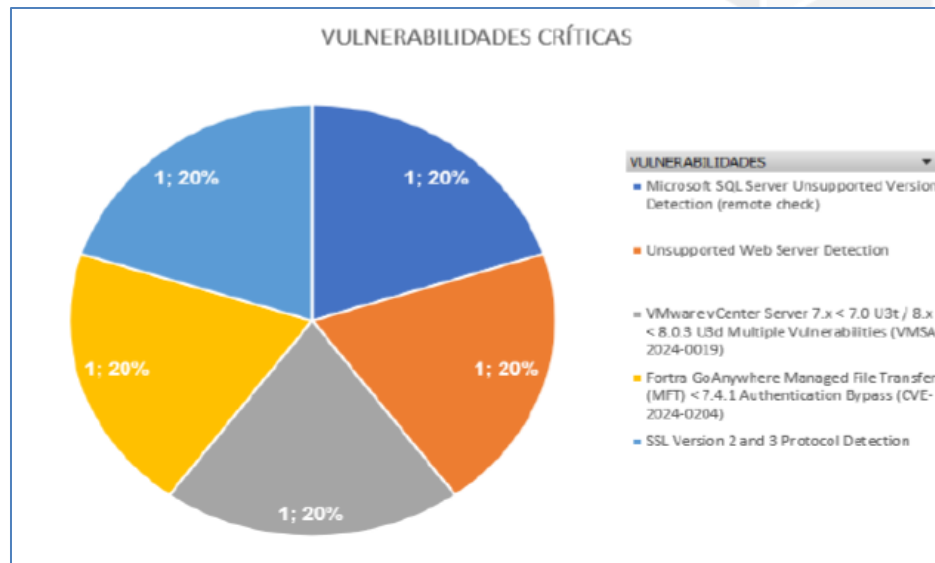


Ilustración 37 Vulnerabilidades Críticas

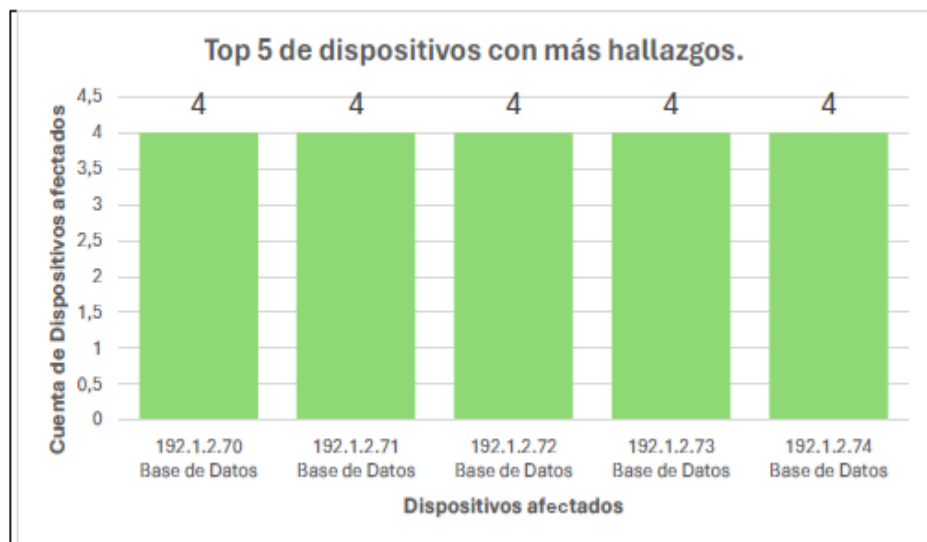


Ilustración 38 Top 5 de mayores hallazgos en el mes

#### 4.3.4.2. Conclusiones Vulnerabilidades

La evaluación de vulnerabilidades correspondiente a la Fase 6, evidencia que, si bien existen avances puntuales, persisten riesgos críticos que afectan directamente la seguridad y disponibilidad de los activos tecnológicos. La presencia de sistemas sin soporte, configuraciones débiles en SMB, RDP y servicios web, y el uso de componentes criptográficos obsoletos, confirma una superficie de ataque amplia y explotable.

Esta situación se ve agravada por la proximidad del fin de soporte de varios sistemas utilizados, lo que pone en evidencia la necesidad urgente de acciones correctivas. En este contexto, se concluye que es necesario adoptar un enfoque técnico y estratégico, que incluya medidas inmediatas de remediación y una planificación estructurada de modernización tecnológica.

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

- **Actualizar y migrar sistemas sin soporte:** Reemplazar sistemas Windows sin soporte (VULN-001) y servidores web no compatibles (VULN-002) por versiones actualizadas que reciban mantenimiento de seguridad activo.
- **Aplicar Parches críticos.** Priorizar la mitigación de la vulnerabilidad BlueKeep (VULN-003 / CVE-2019-0708) mediante la instalación de parches oficiales, desactivación de RDP si no es necesario, y segmentación de red para limitar el alcance.
- **Endurecer configuraciones de red y servicios**
  - SMB: Deshabilitar SMBv1 y habilitar la firma de SMB.
  - Restringir métodos HTTP peligrosos como TRACE / TRACK (VULN-007).
  - Inhabilitar el listado de directorios web navegables (VULN-009) en servidores públicos o expuestos
- **Mejorar la seguridad de los servicios de escritorio remoto:**
  - Configurar Network Level Authentication (NLA) obligatoria (VULN-012).
  - Elevar el nivel de cifrado en RDP a FIPS-140 o equivalente (VULN-010, VULN-013).
  - Corregir vulnerabilidades relacionadas con ataques Man-in-the-Middle (VULN-005).
- **Fortalecer la gestión de certificados y cifrado**
  - Renovar certificados SSL cercanos a expiración (VULN-008).
  - Sustituir algoritmos de hashing débiles (VULN-006), como MD5 o SHA-1, por SHA-256 o superior.
- **Monitorear y gestionar activamente la seguridad:**
  - Implementar herramientas de detección y respuesta ante incidentes (SIEM).
  - Establecer un plan de gestión de vulnerabilidades con revisiones periódicas y correcciones priorizadas.

La implementación de estas medidas permitirá reducir significativamente la exposición a amenazas, mejorar la seguridad de la infraestructura tecnológica y minimizar el impacto de posibles ataques. Como parte del otro sí No 3, firmado en el presente periodo, nos encontramos en la preparación del plan para la mitigación

de estas vulnerabilidades que requiere el acompañamiento del equipo de la Dirección de tecnología del ICETEX.

#### 4.3.5. Reporte De IPs

Del reporte de IPS [Reporte de IPS de Agosto infotic 2025.docx](#) se observan para el mes de agosto algunos eventos permitidos por el IPS de TCP.Split.Handshake con orígenes desde redes internas eso debido a que se ha venido ajustando los perfiles de IPS pero aún falta hacerlo para esta firma como visualiza en el reporte.

Si bien se han aplicado las recomendaciones del fabricante para el bloqueo de la firma TCP.Split.Handshake en el firewall de Aguas, no se ha habilitado la funcionalidad de Deep Inspection. Esta decisión tiene como objetivo validar si los bloqueos efectuados por el módulo UTM son efectivos y están respaldados por el fabricante únicamente cuando se encuentra habilitada dicha funcionalidad. Por lo tanto, se recomienda iniciar el despliegue de Deep Inspection, el cual puede implementarse inicialmente utilizando un certificado auto firmado. Para ello, se sugiere seguir la guía técnica proporcionada en el siguiente enlace: Technical Tip - How to distribute a Fortinet CA SSL certificate.

#### 4.4. Servicios de nube

Con el fin de elaborar recomendaciones de migración a la nube se requiere, por parte del ICETEX, del inventario de aplicaciones y máquinas virtuales que se planean migrar a la nube con el fin de efectuar un análisis y proceder a proponer alternativas tendientes a optimizar los recursos en el ICETEX.

Con el propósito de dar solución al boletín de seguridad titulado "**Boletín de seguridad COLCERT Fin del Soporte de Windows 10**", remitido el pasado mes de Febrero y, tras socializar la lista de máquinas virtuales con Windows 10 existentes en Azure se recomienda, como indican las mejores prácticas proporcionadas por el fabricante Microsoft, la creación de estas máquinas en su versión de Windows 11 descartando la actualización directa de Windows 10 a Windows 11 en la misma máquina, pues es excesiva en costos.

Microsoft ha extendido el plazo hasta Octubre 14 del 2025 para realizar estas actualizaciones, por lo que se recomienda de forma urgente, al ICETEX, adelantar esta labor.

### 5. GESTION DE LA EJECUCIÓN CONTRACTUAL

El contrato 2022-0792 con fecha de perfeccionamiento del acta de inicio del 30 de diciembre del 2022, donde se establece un plazo del contrato de 39 meses, el cual se compone de una fase de transición de 3 meses y una fase de operación de 36 meses, el plazo comenzó a contar a partir de la firma del acta de inicio que fue el 12 de enero del 2023, y la ejecución de los servicios en fase de operación el 1 de abril de 2024, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato, es de aclarar que la fase de transición no es facturable.

En el presente informe del mes de Agosto del 2025 del proyecto, se encuentra en la fase de operación de los servicios contemplados en el alcance llevando ejecutados 28 meses que equivale al 77,7% de avance, para lo cual INFOTIC presenta:

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

A finales del mes, se suscribió el otro si No3 en donde se incluyeron 3 nuevos componentes a cargo de

INFOTIC, los cuales se señalan a continuación:

- ◆ Arquitectura de Seguridad
- ◆ Gestión de vulnerabilidades
- ◆ Pruebas de pentest
- ◆ Desarrollo de un plan de continuidad de negocio.

En el mes de septiembre se presentará el equipo de trabajo que desarrollará dichas funciones así como los respectivos planes de trabajo.

## 6. GESTION PRESUPUESTAL

A continuación, se relacionan los pagos realizados por ICETEX a INFOTIC durante la ejecución del proyecto, de acuerdo con los informes presentados con la evidencia de las actividades realizadas:

| EJECUCIÓN PRESUPUESTAL           |                     |                      |                           |                            |                             |
|----------------------------------|---------------------|----------------------|---------------------------|----------------------------|-----------------------------|
| VALOR INICIAL DEL CONTRATO       | VALOR VIGENCIA 2023 | VALOR EJECUTADO 2023 | VALOR BOLSA VIGENCIA 2023 | VALOR BOLSA EJECUTADO 2023 | VALOR NO EJECUTADO 2023     |
| <b>\$31.398.996.857,96</b>       | \$ 7,849,749,214.53 | \$5,550,607,398.6    | \$360,000,000             | \$2.700.000                | \$1,936,441,815.93          |
|                                  | VALOR VIGENCIA 2024 | VALOR EJECUTADO 2024 | VALOR BOLSA VIGENCIA 2024 | VALOR BOLSA EJECUTADO 2024 | VALOR NO EJECUTADO 2024     |
|                                  | \$10,466,332,286.04 | \$8,116,163,716.21   | \$480,000,000             | \$0                        | \$ 1,870,168,569.83         |
|                                  | VALOR VIGENCIA 2025 | VALOR EJECUTADO 2025 | VALOR BOLSA VIGENCIA 2025 | VALOR BOLSA EJECUTADO 2025 | VALOR NO EJECUTADO 2025     |
|                                  | \$13,227,812,656.04 | \$ 6,187,242,817     | \$480,000,000             | \$0                        | \$7,040,569,838.94          |
| OTROSI-Adición Servicios         | ITEM1               | ITEM2                | ITEM3                     | ITEM4                      |                             |
| <b>\$ 2.761.480.370</b>          | \$ 762.253.015      | \$275.243.152        | \$208.285.884             | 1.515.698.319              |                             |
| CONCEPTO                         |                     |                      |                           |                            |                             |
| CONCEPTO                         |                     |                      |                           |                            | VALOR                       |
| VALOR TOTAL DEL CONTRATO Inicial |                     |                      |                           |                            | <b>\$ 31,398,996,857.96</b> |
| OTROSI-Adición Servicios         |                     |                      |                           |                            | <b>\$ 2.761.480.370</b>     |
| <b>VALOR TOTAL DEL CONTRATO</b>  |                     |                      |                           |                            | <b>\$ 34,160,477,227.96</b> |
| VALOR PAGADO                     |                     |                      |                           |                            | \$ 19,851,678,888.71        |
| 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:                | Agosto               | de                        | 2023                       | \$ 624.431.841,60           |
| Pago No. 5                       | mes:                | Agosto               | de                        | 2023                       | \$ 650.825.466,00           |
| Pago No. 6                       | mes:                | Septiembre           | de                        | 2023                       | \$ 661.959.450,00           |
| Pago No. 7                       | mes:                | Octubre              | de                        | 2023                       | \$ 641.792.285,00           |
| Pago No. 8                       | mes:                | Noviembre            | de                        | 2023                       | \$ 633.094.717,00           |
| Pago No. 9                       | mes:                | Diciembre            | de                        | 2023                       | \$ 663.076.196,00           |
| Pago No. 10                      | mes:                | Enero                | de                        | 2024                       | \$ 681.934.328,00           |
| Pago No. 11                      | mes:                | Febrero              | de                        | 2024                       | \$ 732,950,102.00           |
| Pago No. 12                      | mes:                | Marzo                | de                        | 2024                       | \$ 733.890.372,09           |
| Pago No. 13                      | mes:                | Abril                | de                        | 2024                       | \$ 730,351,368.00           |
| Pago No. 14                      | mes:                | Mayo                 | de                        | 2024                       | \$ 719,104,204.57           |

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

|                                                                                                                                                           |      |            |    |      |                   |                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------|------------|----|------|-------------------|-------------------|
| Pago No. 15 -                                                                                                                                             | mes: | Junio      | de | 2024 | \$ 713,673,218.00 |                   |
| Pago No. 16 -                                                                                                                                             | mes: | Agosto     | de | 2024 | \$ 751,372,731.00 |                   |
| Pago No. 17 -                                                                                                                                             | mes: | Agosto     | de | 2024 | \$755,684,192.00  |                   |
| Pago No. 18 -                                                                                                                                             | mes: | Septiembre | de | 2024 | \$ 752,502,515.00 |                   |
| Pago No. 19 -                                                                                                                                             | mes: | Octubre    | de | 2024 | \$ 770,522,532.00 |                   |
| Pago No. 20 -                                                                                                                                             | mes: | Noviembre  | de | 2024 | \$ 774,178,154.00 |                   |
| Pago No. 21 -                                                                                                                                             | mes: | Diciembre  | de | 2024 | \$ 772,219,902.00 |                   |
| Pago No. 22 -                                                                                                                                             | mes: | Enero      | de | 2025 | \$ 740,982,385.00 |                   |
| Pago No. 23 -                                                                                                                                             | mes: | Febrero    | de | 2025 | \$ 771,789,618.00 |                   |
| Pago No. 24 -                                                                                                                                             | mes: | Marzo      | de | 2025 | \$ 786,219,135.00 |                   |
| Pago No. 25 -                                                                                                                                             | mes: | Abril      | de | 2025 | \$ 778,320,320.00 |                   |
| Pago No. 26 -                                                                                                                                             | mes: | Mayo       | de | 2025 | \$ 778,015,139.00 |                   |
| Pago No. 27 -                                                                                                                                             | mes: | Junio      | de | 2025 | \$ 776,103,223.00 |                   |
| Pago No. 28 -                                                                                                                                             | mes: | Julio      | de | 2025 | \$ 778,511,897.08 |                   |
| Pago No. 29 *-                                                                                                                                            | mes: | Agosto     | de | 2025 | \$ 777,301,100.40 |                   |
| VALOR CAUSADO QUE NO SE HA PAGADO (valor a pagar factura) *                                                                                               |      |            |    |      |                   | \$ 777,301,100.40 |
| VALOR TOTAL EJECUTADO (valor pagado + valor causado no pagado)                                                                                            |      |            |    |      |                   | \$ 20,628,979,988 |
| SALDO DEL CONTRATO (valor total del contrato – valor total ejecutado)                                                                                     |      |            |    |      |                   | \$ 13,531,497,240 |
| PORCENTAJE DE EJECUCIÓN                                                                                                                                   |      |            |    |      |                   | 60.39%            |
| * 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 20 Ejecución Presupuestal

## 7. GESTION ADMINISTRATIVA

### 7.1. Profesionales

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

| Perfiles                        | Especialistas                                                       | Anexo                                                                               |
|---------------------------------|---------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Especialista Bases de datos DBA | Edgar Cobos Mayorga<br>Johan Cardozo - Apoyo                        | <a href="#">Informe Mensual InfoTIC DBA Agosto 2025.pdf</a>                         |
| Especialista Web Máster         | Juan Carlos Martínez Sierra                                         | <a href="#">Informe Mensual InfoTIC Webmaster Agosto 2025.pdf</a>                   |
| Especialista Integrador de nube | Jose Luis Mantilla Guiza                                            | <a href="#">Informe Mensual InfoTIC Integrador de Nube Agosto 2025.pdf</a>          |
| Especialistas de Seguridad      | Jhon Alveiro Pava González<br>Edwin Morales                         | <a href="#">Informe Mensual InfoTIC Seguridad Agosto 2025.pdf</a>                   |
| Especialistas de soluciones     | Jose Francisco Escobar Escorcía<br>Davis Alexander Mogollón Fandiño | <a href="#">Informe Mensual InfoTIC Administrador de Soluciones Agosto 2025.pdf</a> |
| Especialista de Networking      | Carlos Alberto Roldan Ríos<br>Cristian Salgado - Apoyo              | <a href="#">Informe Mensual InfoTIC Administrador de Redes Agosto 2025.pdf</a>      |

Tabla 21 Perfiles y Actividades

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

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

| NOMBRE COMPLETO                 | ROL RESPONSABLE             |
|---------------------------------|-----------------------------|
| María Victoria Suárez Osorio    | Gerente de Servicio         |
| Angie Paola Parra Bustos        | Documentadora               |
| Francisco Javier Pulido Fajardo | Gerente de Implementaciones |

*Tabla 22 Grupo Administrativo*

El pasado 27 de agosto hemos recibido la aceptación de la hoja de vida del ingeniero Carlos Barrera quien, a partir del mes de septiembre, asumirá el rol de especialista integrador nube.

## 8. SERVICIO DE COLABORACIÓN

Durante el mes de Agosto, el servicio de módulos de videoconferencia en las distintas sedes de la entidad se mantuvo operativo sin interrupciones ni problemas. Se aseguró el correcto funcionamiento de cada módulo y se dispuso de apoyo técnico para garantizar su operatividad. A lo largo de este periodo, no se registraron reportes de falta de disponibilidad del servicio en ninguna de las sedes.

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

*Tabla 23 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.

Con el fin de evitar fallos, asegurar un rendimiento óptimo y prolongar la vida útil de los equipos, se llevan a cabo revisiones periódicas y mantenimientos preventivos necesarios para garantizar la continuidad del servicio y el correcto funcionamiento de cada módulo instalado en las sedes de Icetex.

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

- Visita en sitio en sedes de Bogotá, para realizar pruebas de funcionamiento, inspección de los módulos y posterior limpieza interna y externa de los módulos instalados en la sede Aguas, Ángel y Chapinero, para garantizar la prestación continua del servicio y validar que no se estén presentando novedades y/o incidencias.
- Visita en sitio en sedes Bogotá con el fin de realizar ejercicio para gestión de vulnerabilidades para los módulos de videoconferencia.
- Atención y solución de requerimientos para revisión de novedades presentadas.
- Informe mensual de operación del servicio y reporte técnico de visitas a sedes Regionales, el cual se puede consultar en el link [Informe actividades Módulos videoconferencia ICETEX agosto 2025.pdf](#)

En la verificación realizada para el pasado mes de agosto del 2025 sobre la solución de videoconferencia en las sedes regionales, se encontró que la solución completa presentó estado activo para los 31 días del periodo, con disponibilidad del 100%, además, es importante resaltar que se cuenta con todos los requerimientos realizados en las especificaciones técnicas del contrato..

Adicionalmente, No se recibieron requerimientos para gestión y atención del soporte técnico; tampoco fueron reportadas incidencias a nivel del servicio para estas sedes durante el mes del presente informe, no obstante, como cada periodo, se contó con la disponibilidad técnica para recibir cualquier requerimiento de soporte o solicitud de apoyo en lo concerniente a la solución de videoconferencia desplegada.

## 9. GESTION DE RIESGOS Y PROBLEMAS

Se construyó una tabla de nivel riesgo que contiene los factores a analizar cómo son severidad y probabilidad otorgando un rango de valor que representa cada uno de los niveles de ocurrencia, con los cuales se determina el nivel de riesgo. Cabe destacar que la determinación de estos valores no sigue una regla estricta, y puede ser ajustada de acuerdo con las necesidades del proyecto.

- Matriz de riesgos Se presenta la matriz de riesgo y se deja la evidencia del documento generado.

| No. | Actividad                                                                        | Peligro                                                                                                               | Consecuencia Riesgo                                                            | Medidas de control                                                                                        | Evaluación del riesgo |                  |       | Medidas de control a implementar                                                                                                      | Responsable      |
|-----|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|-----------------------|------------------|-------|---------------------------------------------------------------------------------------------------------------------------------------|------------------|
|     |                                                                                  |                                                                                                                       |                                                                                |                                                                                                           | Severidad (S)         | Probabilidad (P) | S x P |                                                                                                                                       |                  |
| 1   | Sin acceso a los servidores con los usuarios y contraseñas entregados            | No poder gestionar los servicios requeridos por el ICETEX                                                             | Perdida de tiempo y dinero                                                     | Realizar pruebas mensualmente para confirmar el acceso a los servidores                                   | 3                     | 8                | 24    | Verificar con CLARO los cambios que realicen a nivel de la gestión corporativa                                                        | INFOTIC          |
| 2   | Instalación de agente de antivirus en los servidores de ICETEX                   | Sufrir ataques que pueden dañar la información o no permitir el desarrollo de los servicios instalados en los equipos | Fallas de seguridad                                                            | Inventario de los servidores identificando cuales tienen instalado y actualizado la versión del antivirus | 2                     | 6                | 12    | Mensualmente revisar los servidores asignados al proyecto revisando el estado del antivirus                                           | INFOTIC          |
| 3   | Parches de actualización de los sistemas operativos de los servidores del ICETEX | Se presentan vulnerabilidades a nivel de los servidores                                                               | Fallas de seguridad                                                            | Inventario de los servidores identificando la última versión de parches actualizada                       | 3                     | 6                | 18    | Verificación con los fabricantes sobre la última versión libre y funcionando comparada con la instalada actualmente en los servidores | INFOTIC          |
| 4   | Actualización de servidores que son 2008 y 2012                                  | Se presentan vulnerabilidades a nivel de los servidores                                                               | Fallas de seguridad                                                            | Inventario de los servidores                                                                              | 4                     | 8                | 32    | Verificación semanal del estado de los servidores                                                                                     | ICETEX - INFOTIC |
|     |                                                                                  | Fallas en el funcionamiento de las aplicaciones instaladas en estos equipos                                           | Reprocesos y altos costos ya que estos equipos no tienen soporte de fabricante | Inventario de las aplicaciones                                                                            |                       |                  |       | Verificación semanal del estado de las aplicaciones                                                                                   | ICETEX - INFOTIC |

Ilustración 39 Matriz de riesgos

### Matriz de riesgos ICETEX.xlsx

A partir de la identificación del nivel de riesgo relacionado al proyecto ICETEX, se pueden implementar estrategias que permitan mitigarlo o, incluso, eliminar los posibles obstáculos a los que se pueda enfrentar el ICETEX.

Durante la ejecución de un proyecto, existen una gran cantidad de factores que pueden determinar el nivel de riesgo, por lo que es importante diferenciar dos tipos:

- **Factores internos:** son aquellos que hacen parte esencial del desarrollo de la operación que se realiza en ICETEX y que tienen que ver con el alcance del proyecto, como lo pueden ser los servidores, aplicaciones, canales de comunicaciones, data center principal y externo.
- **Factores externos:** son aquellos que se encuentran fuera del alcance de la empresa, y son de difícil identificación, tales como los fenómenos naturales o fenómenos económicos.

Para lo cual, se tiene:

- Tabla de nivel de riesgo

|                |   | PROBABILIDAD |         |           |          |           |
|----------------|---|--------------|---------|-----------|----------|-----------|
|                |   | IMPROBABLE   | POSIBLE | OCASIONAL | MODERADA | CONSTANTE |
| SEVERIDAD      |   | 2            | 4       | 6         | 8        | 10        |
| INSIGNIFICANTE | 1 | 2            | 4       | 6         | 8        | 10        |
| MENOR          | 2 | 4            | 8       | 12        | 16       | 20        |
| MODERADO       | 3 | 6            | 12      | 18        | 24       | 30        |
| CRITICO        | 4 | 8            | 16      | 24        | 32       | 40        |
| CATASTROFICO   | 5 | 10           | 20      | 30        | 40       | 50        |

Tabla 24 Nivel de Riesgo

- Tabla de grado de riesgo

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

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

*Tabla 25 Grado de riesgo*

## 10. INDICADORES CLAVE DE DESEMPEÑO

### 10.1. ANS por Disponibilidad de canales de comunicaciones:

Durante el mes de Agosto de 2025, los canales principales y Backup instalados operaron de manera normal, se realizó monitoreo del servicio de los canales mediante la herramienta SolarWinds, el informe de disponibilidad es el que permite la revisión de los ANS y se tiene la línea base de los canales instalados con sus anchos de banda iniciales la cual se actualizando con las ampliaciones de las canales acordadas contractualmente, se tiene el reporte: [Reporte Mensual Disponibilidad INFOTIC Agosto 2025.pdf](#)

También se puede consultar en el repositorio un documento en Excel con el análisis del comportamiento de los canales para el mes de agosto [ANS agosto 2025.xlsx](#)

| Sede          | Categoría                        | INR        | %MES     |
|---------------|----------------------------------|------------|----------|
| BOGOTAD.C.    | Principal/FO (Sede Aguas)        | INR0037    | 99,93 %  |
|               | Backup /FO (Sede Aguas)          | INR0036    | 100,00 % |
|               | Principal/IPVPN (Sede Chapinero) | INR0022    | 99,71 %  |
|               | Backup /IPVPN (Sede chapinero)   | INR0020    | 99,98 %  |
|               | Principal/IPVPN (Angel)          | INR0272    | 89,78 %  |
|               | Backup /IPVPN (Angel)            | INR0273    | 100,00 % |
| IBAGUE        | Principal/IPVPN                  | INR0073    | 99,95 %  |
|               | Backup/IPVPN                     | INR0076    | 99,95 %  |
| LETICIA       | Principal/Satelital              | INR0000373 | 97,97 %  |
| NEIVA         | Principal/IPVPN                  | INR0039    | 89,65 %  |
|               | Backup/IPVPN                     | INR0041    | 90,66 %  |
| TUNJA         | Principal/IPVPN                  | INR0104    | 87,75 %  |
|               | Backup/IPVPN                     | INR0106    | 87,72 %  |
| VILLAVICENCIO | Principal/IPVPN                  | INR0085    | 100%     |
|               | Backup/IPVPN                     | INR0084    | 100,00 % |
| ARMENIA       | Principal/IPVPN                  | INR0074    | 100,00 % |
|               | Backup/IPVPN                     | INR0072    | 99,68 %  |
| MANIZALES     | Principal/IPVPN                  | INR0088    | 97,66 %  |
|               | Backup/IPVPN                     | INR0087    | 99,80 %  |
| MEDELLIN      | Principal/IPVPN                  | INR0133    | 100,00 % |
|               | Backup/IPVPN                     | INR0132    | 100,00 % |

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

| Sede            | Categoría        | INR                      | %MES     |
|-----------------|------------------|--------------------------|----------|
| APARTADO        | Principal/IPVPN  | INR0144                  | 98,95 %  |
| PEREIRA         | Principal/IPVPN  | INR0079                  | 99,40 %  |
|                 | Backup/IPVPN     | INR0077                  | 99,98 %  |
| QUIBDO          | Principal/IPVPN  | INR0014                  | 90,10 %  |
|                 | Backup/IPVPN     |                          | 0%       |
| BARRANQUILLA    | Principal/IPVPN  | INR0103                  | 97,03 %  |
|                 | Backup/IPVPN     | INR0100                  | 96,83 %  |
| CARTAGENA       | Principal/IPVPN  | INR0109                  | 98,92 %  |
|                 | Backup/IPVPN     | INR0107                  | 98,95 %  |
| MONTERIA        | Principal/IPVPN  | INR0080                  | 99,54 %  |
|                 | Backup/IPVPN     | INR0081                  | 99,54 %  |
| RIOHACHA        | Principal/IPVPN  | INR0164                  | 99,49 %  |
|                 | Backup/IPVPN     | INR0162                  | 99,88 %  |
| SANTAMARTA      | Principal/IPVPN  | INR0154                  | 96,23 %  |
|                 | Backup/IPVPN     | INR0152                  | 99,35 %  |
| SINCELEJO       | Principal/IPVPN  | INR0095                  | 99,79 %  |
|                 | Backup/IPVPN     | INR0097                  | 100,00 % |
| SAN ANDRES      | Principal/IPVPN  | INR0000367<br>INR0000369 | 100%     |
| BARRANCABERMEJA | Principal/IPVPN  |                          | 0        |
| SANGIL          | Principal/IPVPN  |                          | 0        |
| BUCARAMANGA     | Principal/IPVPN  | INR0062                  | 100,00 % |
|                 | Backup/IPVPN     | INR0061                  | 100,00 % |
| CUCUTA          | Principal/IPVPN  | INR0044                  | 99,99 %  |
|                 | Backup/IPVPN     | INR0047                  | 99,99 %  |
| VALLEDUPAR      | Principal/IPVPN  | INR0091                  | 99,99 %  |
|                 | Backup/IPVPN     | INR0090                  | 99,95 %  |
| YOPAL           | Principal/IPVPN  | INR0121                  | 47%      |
|                 | Backup/IPVPN     | INR0123                  | 99,99 %  |
| ARAUCA          | Principal/IPVPN  | INR0110                  | 94,70 %  |
| CALI            | Principal/IPVPN  | INR0151                  | 100,00 % |
|                 | Backup/IPVPN     | INR0153                  | 100,00 % |
| BUENAVENTURA    | Principal/IPVPN  | INR0051                  | 99,70 %  |
| MOCOA           | Principal/IPVPN  | INR0135                  | 82,11 %  |
|                 | Backup/Satelital | INR0136                  | 94,60 %  |
| PASTO           | Principal/IPVPN  | INR0130                  | 100,00 % |
|                 | Backup/IPVPN     | INR0131                  | 100,00 % |
| POPAYAN         | Principal/IPVPN  | INR0035                  | 99,87 %  |
|                 | Backup/IPVPN     | INR0032                  | 99,87 %  |

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

| Sede                                                                                                                | Categoría                                                              | INR        | %MES     |
|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|------------|----------|
| TUMACO                                                                                                              | Principal/IPVPN                                                        | INR0147    | 92,12 %  |
| DCTRIARA                                                                                                            | MPLSPP                                                                 | INR0266    | 100.00%  |
|                                                                                                                     | MPLS Backup                                                            | INR0171    | 100.00%  |
| DCTRIARA                                                                                                            | INTERNET BK                                                            | INR0221    | 100.00%  |
|                                                                                                                     | INTERNET PP                                                            | INR0264    | 100.00%  |
| DCTRIARA                                                                                                            | NOC claro de dedicado (DWDM)2GTriaramegacentro                         | INR0224    | 100.00%  |
| Canal entre Sitio principal Icetex- Dirección General-Aguas                                                         | Principal/IPVPN                                                        |            | 0        |
|                                                                                                                     | Backup/IPVPN                                                           |            | 0        |
| BOGOTAD.C.                                                                                                          | Internet (Sede Aguas)                                                  | INR0034    | 100.00%  |
| DC Megacentro                                                                                                       | DCMEGACENTER–CONTIGENCIA–MPLSPPAL                                      | INR0177    | 100.00%  |
| DCTRIARA                                                                                                            | DCMEGACENTER–CONTIGENCIA–MPLS BK                                       | INR0230    | 100.00%  |
| DC Megacentro                                                                                                       | Internet                                                               | INR0268    | 100.00%  |
| Banco de la Republica hasta Edificio Dirección General ICETEX                                                       | Ubicado en Data center Principal. Interconectado a través de red MPLS  | INR0000289 | 100.00%  |
| DECEVAL hasta Edificio de ICETEX Dirección General                                                                  | Ubicado en Data center Principal. Interconectado a través de red MPLS  | INR0000317 | 99,92 %  |
| DECEVAL hasta Edificio de ICETEX Dirección General                                                                  | Ubicado enDatacenter Principal.interconectado atravesderedMPLS(Backup) | INR0000318 | 100.00%  |
| Salidadelportaleshttps://portal.icetex.gov.co/portalywww.icetex.gov.cohaciainternetencentrodecó mputoprincipal      | Internet Reverso para Portales                                         | INR0000320 | 100.00%  |
| Salidadelportaleshttps://portal.icetex.gov.co/portalywww.icetex.gov.cohaciainternetencentrodecó mputodecontingencia | Internet Reverso para Portales                                         | INR0274    | 100,00 % |
| DCTRIARA                                                                                                            | Allot Centralizado 800M Triara(equipo)                                 | INR0270    | 100,00 % |

*Tabla 26 Disponibilidad de Canales*

Durante el mes de Agosto de 2025 el servicio de Internet para la gente se prestó sin interrupciones en todas las catorce sedes contratadas donde ICETEX cuenta con oficina, las cuales se relacionan a continuación:

| Sede         | Categoría              | INR        | % Mes    |
|--------------|------------------------|------------|----------|
| BARRANQUILLA | INTERNET PARA LA GENTE | INR0094    | 97,04 %  |
| BUCARAMANGA  | INTERNET PARA LA GENTE | INR0057    | 100,00 % |
| CALI         | INTERNET PARA LA GENTE | INR0160    | 100,00 % |
| AGUAS        | INTERNET PARA LA GENTE | INR0029    | 99,93 %  |
| CHAPINERO    | INTERNET PARA LA GENTE | INR0015    | 99,70 %  |
| MEDELLIN     | INTERNET PARA LA GENTE | INR0122    | 100,00 % |
| APARTADO     | INTERNET PARA LA GENTE | INR0140    | 98,95 %  |
| ARAUCA       | INTERNET PARA LA GENTE | INR0115    | 94,70 %  |
| LETICIA      | INTERNET PARA LA GENTE | INR0000378 | 97,92 %  |

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

| Sede       | Categoría              | INR        | % Mes   |
|------------|------------------------|------------|---------|
| QUIBDO     | INTERNET PARA LA GENTE | INR0021    | 90,09 % |
| RIOHACHA   | INTERNET PARA LA GENTE | INR0159    | 99,49 % |
| SAN ANDRES | INTERNET PARA LA GENTE | INR0000368 | 98,84 % |
| YOPAL      | INTERNET PARA LA GENTE | INR0127    | 85,99 % |
| MOCOA      | INTERNET PARA LA GENTE | INR0141    | 82,07 % |

*Tabla 27 Disponibilidad canales "Internet para la gente"*

### 10.1.1. Canal de Replicación (Triara – Megacenter)

El proyecto tiene asignado dos (2) canales de comunicación con un ancho de banda de 2 Gbps, el cual se comunica en forma bidireccional entre los data centers de Triara y Megacenter, permitiendo generar la replicación de la información de los equipos de ICETEX, para el mes de agosto continúa su funcionamiento correctamente sin novedades que afectaran la prestación del servicio. La evidencia se encuentra en el [Informe mensual replicacion Agosto 2025.pdf](#)

### 10.2. ANS por Disponibilidad de servidores:

La herramienta utilizada para el monitoreo de la disponibilidad de servidores es ELK, y el informe correspondiente permite la revisión de los ANS en los documentos [Reporte Monitoreo ICETEX agosto 2025-ELK.pdf](#) y [Disponibilidad Server ELK Agosto2025.xlsx](#)

| No | COD.       | Etiquetas de fila            | Disponibilidad |
|----|------------|------------------------------|----------------|
| 1  | INR0000322 | ictsrvctrlidoc               | 100.00%        |
| 2  | INR0226    | mira                         | 100.00%        |
| 3  | INR0228    | ictxisgesbd                  | 99.97%         |
| 4  | INR0229    | ictxisgesapp                 | 100.00%        |
| 5  | INR0233    | icetexboglxfefo1.localdomain | 99.19%         |
| 6  | INR0234    | ictxprusigapp                | 100.00%        |
| 7  | INR0235*   | ictxbogsrvpt2                | 100.00%        |
| 8  | INR0236*   | ictxbogsrvpt1                | 100.00%        |
| 9  | INR0237**  | icetexboglserver1-r          | 100.00%        |
| 10 | INR0238    | icetexbogliferaynfs          | 99.17%         |
| 11 | INR0239    | icetexbogelasticserver1      | 99.11%         |
| 12 | INR0240    | icetexbogelasticserver2      | 99.19%         |
| 13 | INR0241    | icetexbogelasticserver3      | 99.60%         |
| 14 | INR0242    | icetexbogliferayserver1      | 99.44%         |
| 15 | INR0243    | icetexbogliferayserver2      | 99.52%         |
| 16 | INR0244    | icetexboglxdarumasrv1        | 98.79%         |
| 17 | INR0245    | icetexboglxdarumasrv2        | 99.19%         |
| 18 | INR0246    | icetexboglxdarumatest        | 99.19%         |
| 19 | INR0247    | preprodsec                   | 99.19%         |
| 20 | INR0248    | icetexboglxxroad3            | 99.19%         |

|    |         |                               |         |
|----|---------|-------------------------------|---------|
| 21 | INR0249 | xroadsec                      | 98.79%  |
| 22 | INR0250 | qasec                         | 98.79%  |
| 23 | INR0251 | INR0251_INFOTIC               | 100.00% |
| 24 | INR0252 | icetexosbognfs2               | 100.00% |
| 25 | INR0253 | bastion.localdomain           | 0%      |
| 26 | INR0254 | INR0254_INFOTIC               | 100.00% |
| 27 | INR0255 | INR0255_INFOTIC               | 100.00% |
| 28 | INR0256 | INR0256_INFOTIC               | 100.00% |
| 29 | INR0257 | INR0257_INFOTIC               | 100.00% |
| 30 | INR0258 | INR0258_INFOTIC               | 99.98%  |
| 31 | INR0259 | INR0259_INFOTIC               | 99.99%  |
| 32 | INR0260 | icetexosbognfs1               | 100.00% |
| 33 | INR0262 | icetexboglxfefeo2.localdomain | 99.19%  |
| 34 | INR0276 | cxvodaprodn011                | 98.39%  |
| 35 | INR0277 | cxvodaprodn021                | 98.79%  |
| 36 | INR0278 | cxvodacontg011                | 98.02%  |

*Tabla 28 Códigos relacionados Disponibilidad Servicios en Housing – Datacenter Principal*

El servidor **\*icetexboglobserver1-r**, que corresponde al antiguo balanceador de carga, fue deshabilitado a principios del mes de julio. Esta acción se llevó a cabo debido a la puesta en producción de un nuevo balanceador en el mes de junio.

Como resultado de esta medida, la disponibilidad del servidor antiguo disminuye lógicamente y dejará de aparecer en el Reporte de Disponibilidad a partir del próximo mes. No obstante, el servidor sigue facturándose. Estaremos a la espera de la distribución de estos recursos en los servidores que el ICETEX considere pertinentes.

Por otro lado, con respecto a los servidores **\*\* icetexboglobserver1** e **icetexboglobserver2**, les recordamos que a finales de diciembre de 2024 el ICETEX solicitó su baja y la distribución de sus recursos en los servidores de **OpenShift**.

Esta solicitud se hizo efectiva al cierre de ese mismo mes, por lo que a partir de enero de 2025 estos servidores ya no se muestran en el Reporte de Disponibilidad mensual. Sin embargo, para efectos de facturación, se siguen teniendo en cuenta tal como se acordó previamente. La evidencia de dicha solicitud se encuentra en el documento: [Baja de servidores - Actualización OpenShift incremento de RAM.pdf](#)

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

| # | Dispositivo    | Marca    | Modelo        |
|---|----------------|----------|---------------|
| 1 | FORTIWEB01     | Fortinet | 2000E         |
| 2 | FORTIWEB02     | Fortinet | 2000E         |
| 3 | FORTIAUTH01    | Fortinet | 1000D         |
| 4 | FORTIAUTH02    | Fortinet | 1000D         |
| 5 | FORTISANDBOX   | Fortinet | 1000D         |
| 6 | Cisco 3650X    | Cisco    | WS-C3650-48TQ |
| 7 | Cisco 3650X SW | Cisco    | WS-C3650-48TQ |

| #  | Dispositivo                                                                                         | Marca | Modelo         |
|----|-----------------------------------------------------------------------------------------------------|-------|----------------|
| 8  | Switch DELL Networking                                                                              | Dell  | N4032 24 ports |
| 9  | Controladora SAN Dell Compellent                                                                    | Dell  | SC8000         |
| 10 | Controladora SAN Dell Compellent                                                                    | Dell  | SC8000         |
| 11 | Enclosure Discos SAN                                                                                | Dell  | EN-SC200       |
| 12 | Enclosure Discos SAN                                                                                | Dell  | EN-SC220       |
| 13 | Enclosure Discos SAN                                                                                | Dell  | EN-SC200       |
| 14 | Enclosure Discos SAN                                                                                | Dell  | EN-SC220       |
| 15 | Enclosure Discos SAN                                                                                | Dell  | EN-SC220       |
| 16 | Enclosure Discos SAN                                                                                | Dell  | EN-SC200       |
| 17 | Enclosure Dell Blade – Principal 5 Servidor – Blade M1000, 6 IOM Slot B2 -Tarjeta Enclosure - M1000 | Dell  | M1000E         |

Tabla 29 Dispositivos en Housing – Datacenter Principal

### 10.2.1. Disponibilidad TRIARA para los servicios de página web

A continuación, se evidencia que la disponibilidad del Portal Web institucional web.ICETEX.gov.co, el cual presentó en el mes de agosto un **UPTIME del [99,902%]** tal como se evidencia en la gráfica a continuación.

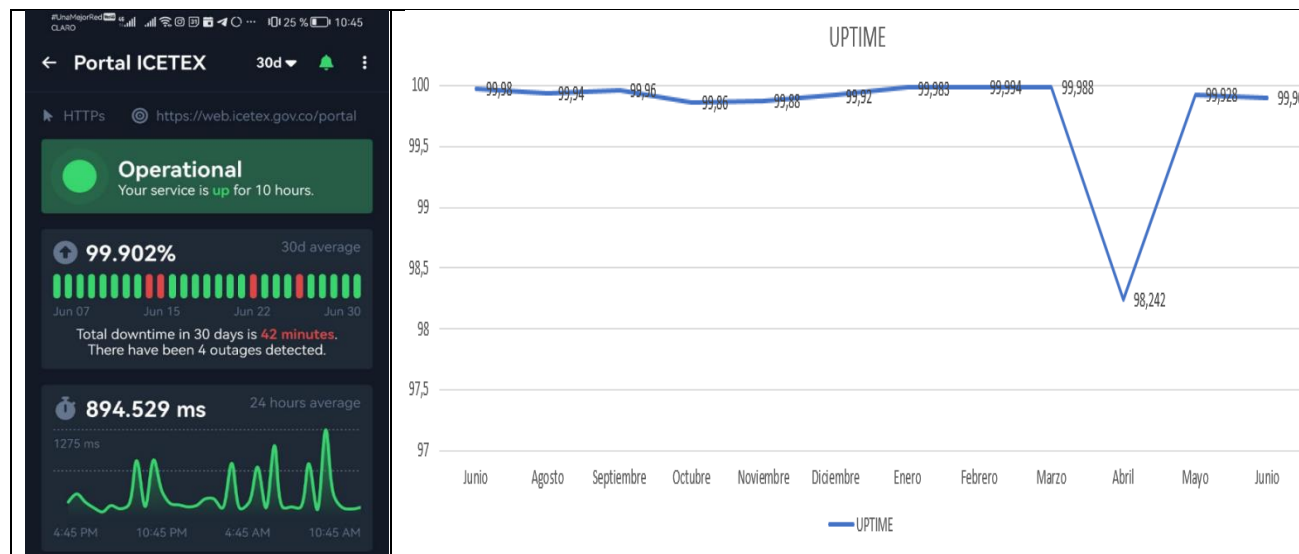


Ilustración 40 UPTIME – Portal WEB web.ICETEX.gov.co

Durante el mes de Agosto se evidenció un comportamiento estable del portal WEB institucional y se cumplió con el porcentaje de disponibilidad de este con un porcentaje del **99,902%**.

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

|                                    | Junio   | Julio   | Agosto  |
|------------------------------------|---------|---------|---------|
| <b>Usuarios activos mes</b>        | 595.000 | 511.000 | 511.000 |
| <b>Usuarios nuevos</b>             | 417.000 | 344.000 | 344.000 |
| <b>Tiempo de interacción (seg)</b> | 124     | 140     | 140     |

Tabla 30 Distribución trimestral de acceso por usuarios

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

El portal WEB cuenta con un total de 511 mil usuarios, con 344 mil usuarios nuevos. El tiempo de interacción medio es de 2 minutos y 20 segundos, señalando el interés de la audiencia en las diferentes páginas del portal web.icetex.gov.co.

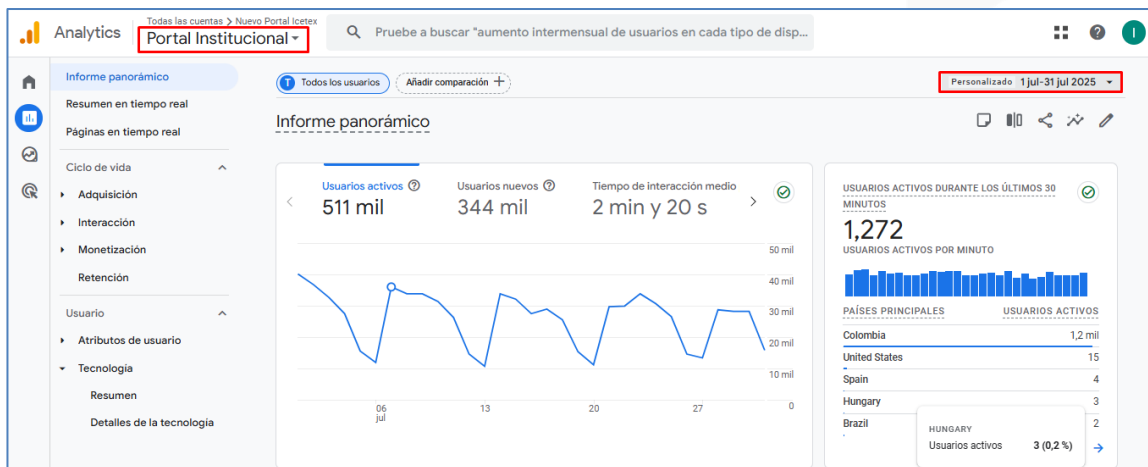


Ilustración 41 Métrica de visitantes Portal WEB web.ICETEX.gov.co

**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:



Ilustración 42 Métrica adquisición usuarios Portal WEB web.ICETEX.gov.co

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

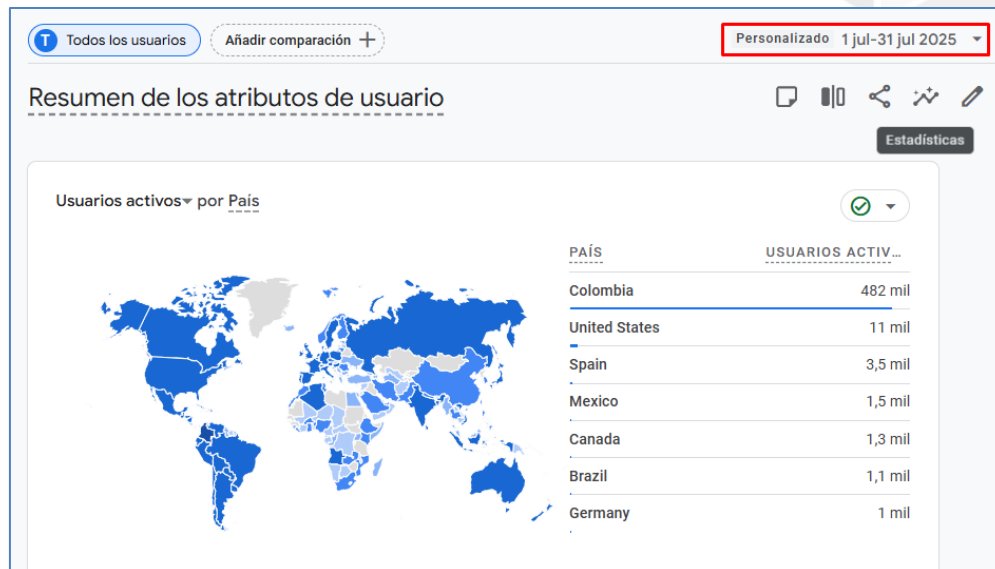


Ilustración 43 Métrica de usuario por país - Portal WEB web.ICETEX.gov.co

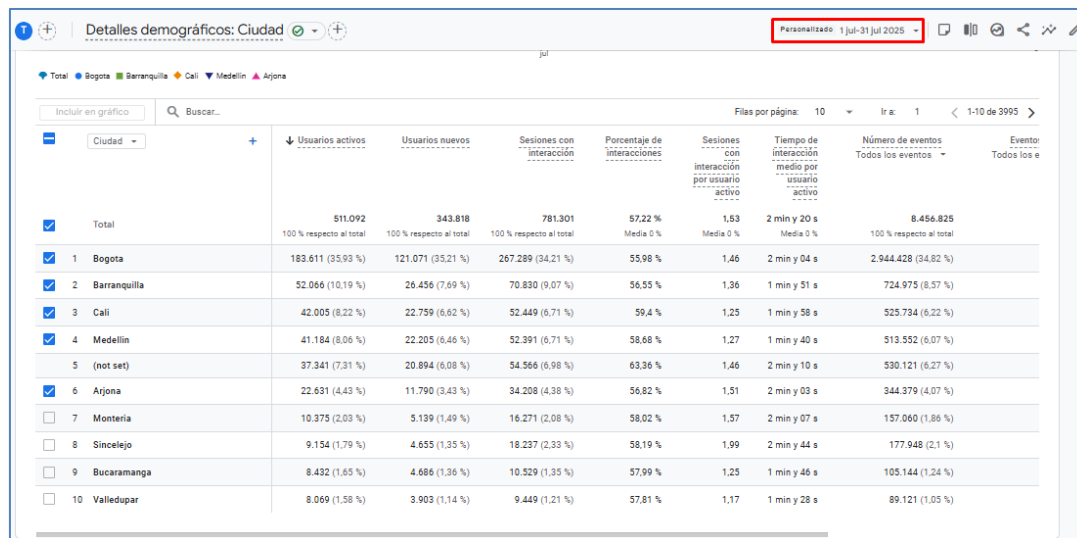


Ilustración 44 Métrica de ciudades de Colombia- Portal WEB web.ICETEX.gov.co

A continuación, se muestran las gráficas referentes a CPU, memoria RAM y almacenamiento en los nodos 1 y 2 del portal ICETEX desde el 1 de Agosto desde las 0:00 am hasta las 10:30 horas del 31 de Agosto de 2025.

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

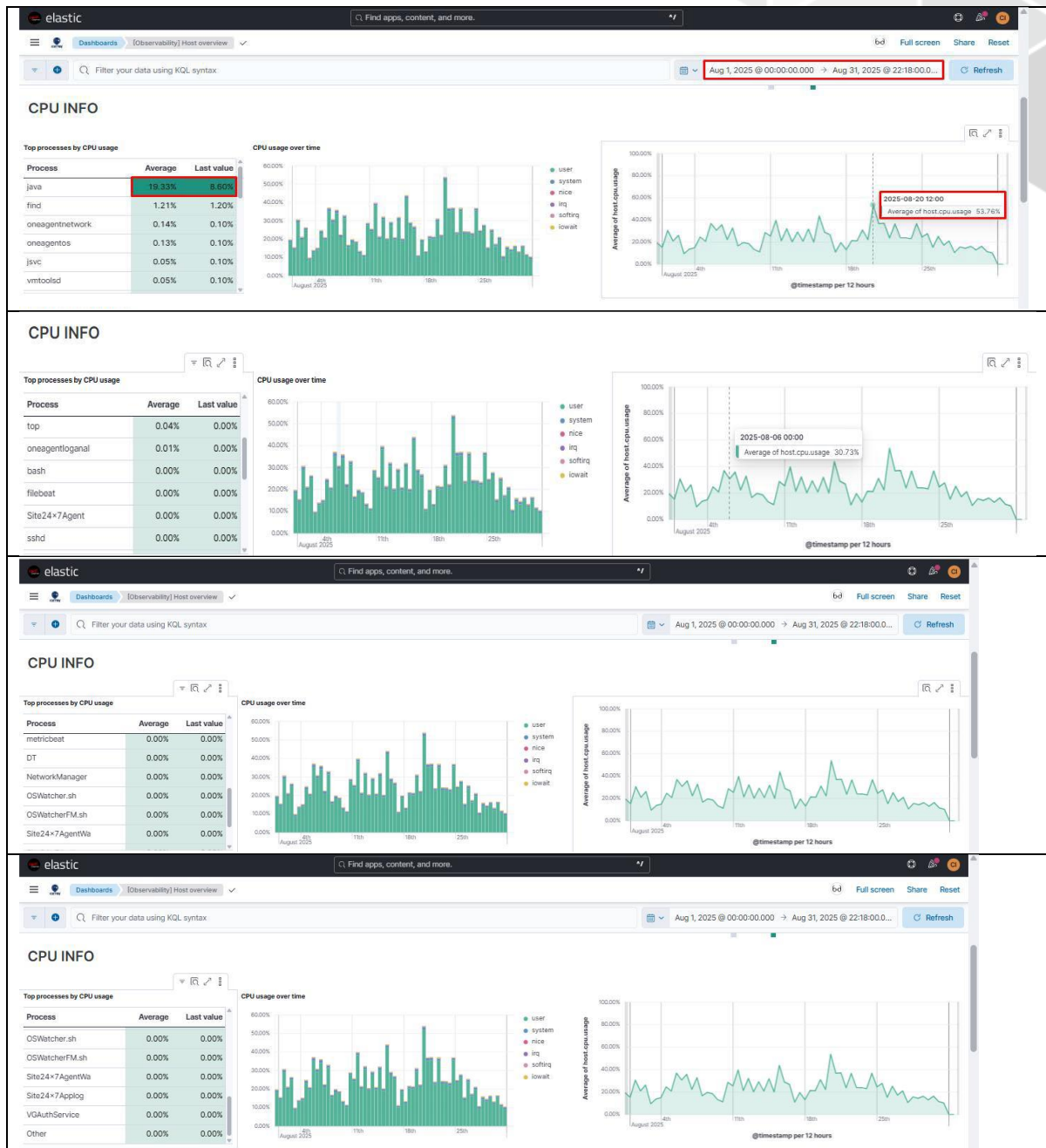


Ilustración 45 NODO 1 CPU

Sede principal-Bogotá, Colombia  
Calle 93B # 13-44, Segundo piso  
NIT:900.068.796-1  
Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
Cra. 24 No. 53ª-26 Arboleda Alta.  
NIT: 900.068.796-1  
Teléfono: (+606) 88612612

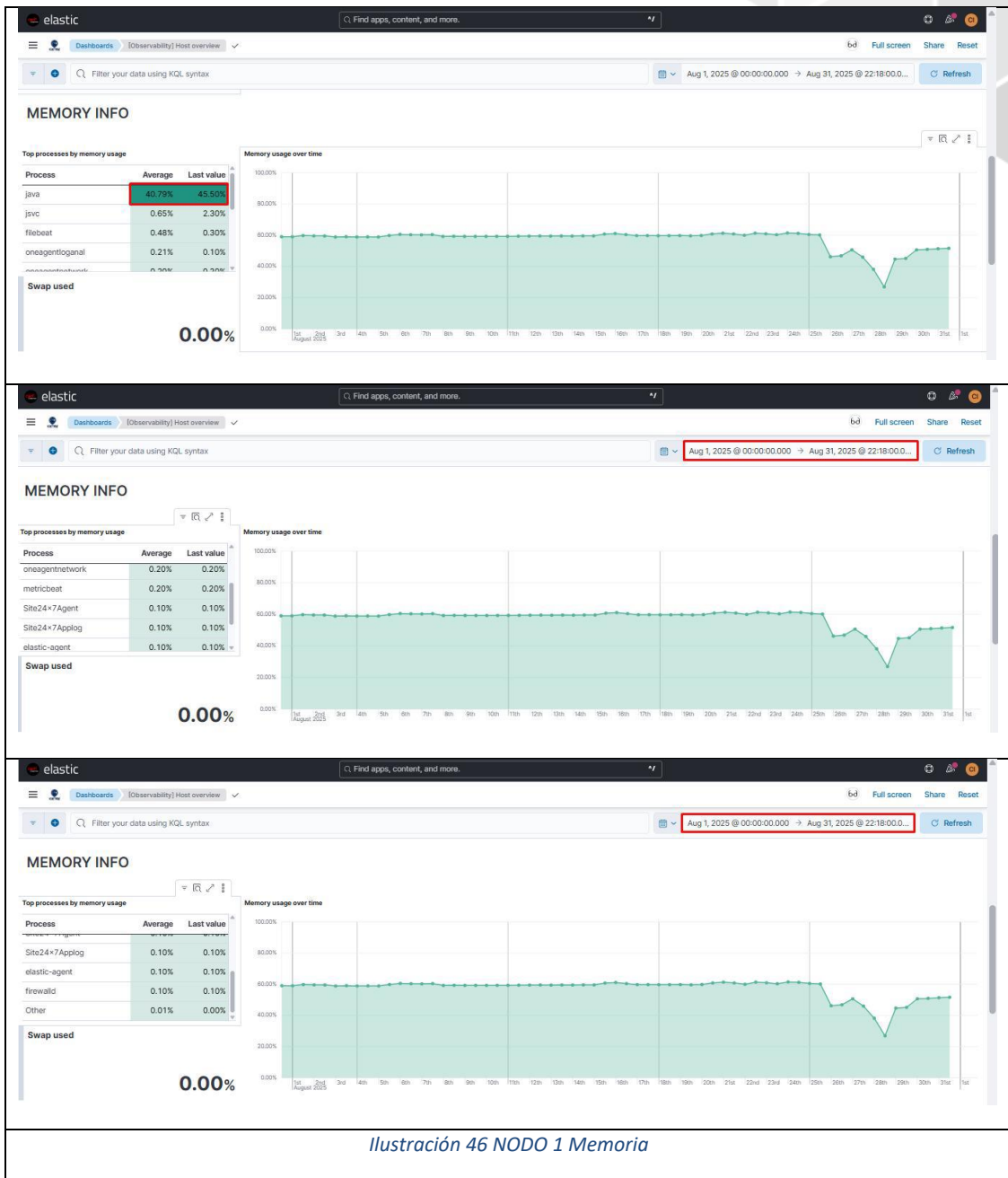


*Ilustración 46 NODO 1 Memoria*

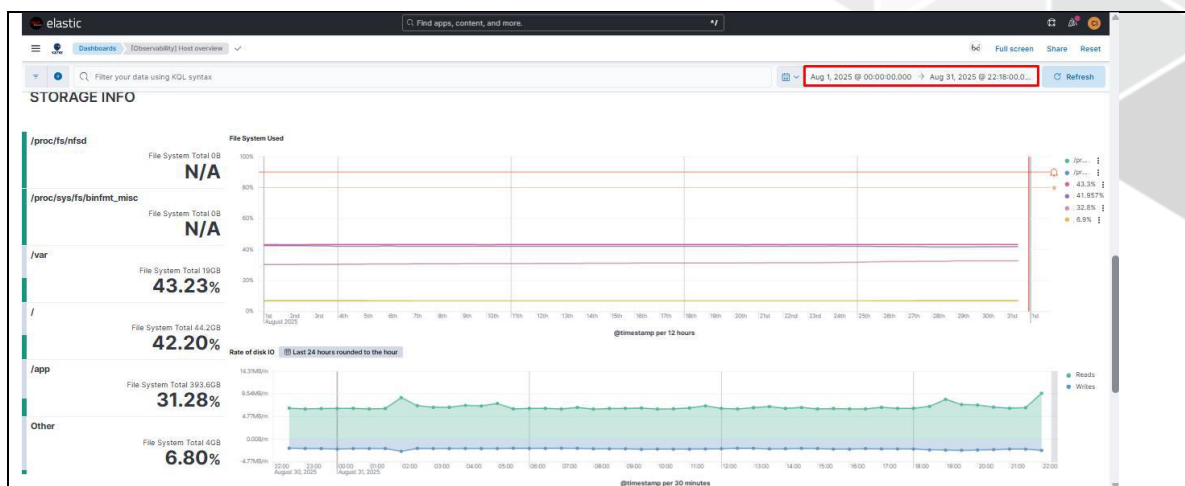


*Ilustración 47 NODO 1 Almacenamiento*

Estos mismos recursos, para el nodo 2 se monitorean de igual manera. El detalle de los consumos y sus umbrales puede ser consultado en el informe de nuestro especialista web master.

### 10.2.2. Análisis componente Liferay Producción

Como parte de las actividades desarrolladas por el Web máster se realiza una revisión de la infraestructura tecnológica y el entorno de software del portal Liferay, abordando aspectos fundamentales para su óptimo rendimiento y seguridad sin encontrarse Hallazgos significativos.

### 10.2.3. Backup Servidores Triara

Durante el periodo de agosto se realizaron los Backups de acuerdo con las políticas definida por el ICETEX, las cuales desde su inicio se implementaron en el Datacenter. Se puede verificar en el documento [Informe Backups mes de Agosto 2025.pdf](#) que se genera con la guía de los diferentes reportes de backups disponibles durante el mes y se adjunta el reporte de los backups que se genera automáticamente desde la herramienta de backups [Consolidado Diario de Backups agosto 2025.pdf](#)

Dentro de las actividades del proyecto de servicios tecnológicos para ICETEX, se tiene la toma de copias de respaldo de la información creada, actualizada, reutilizada y procesada dentro de las diferentes actividades de la entidad la cual requiere para el desarrollo de sus actividades diarias, para lo cual se tiene como lineamiento principal la aplicación del anexo 22 donde se contempla las diferentes variables para la toma de Backups y la política de Backups la cual se encuentra actualizada con la operación actual: [Politica Backup Ictex V2.xlsx](#)

Actualmente, se cuenta con la custodia externa de 294 cintas en las instalaciones de VISE, correspondientes a la información histórica entregada a partir del 23 de agosto de 2023.

A la fecha, el ICETEX, no ha entregado las cintas de backup necesarias para llevar a cabo el almacenamiento y traslado a custodia externa, lo que permitiría devolver todas las cintas que actualmente se encuentran en

calidad de préstamo.

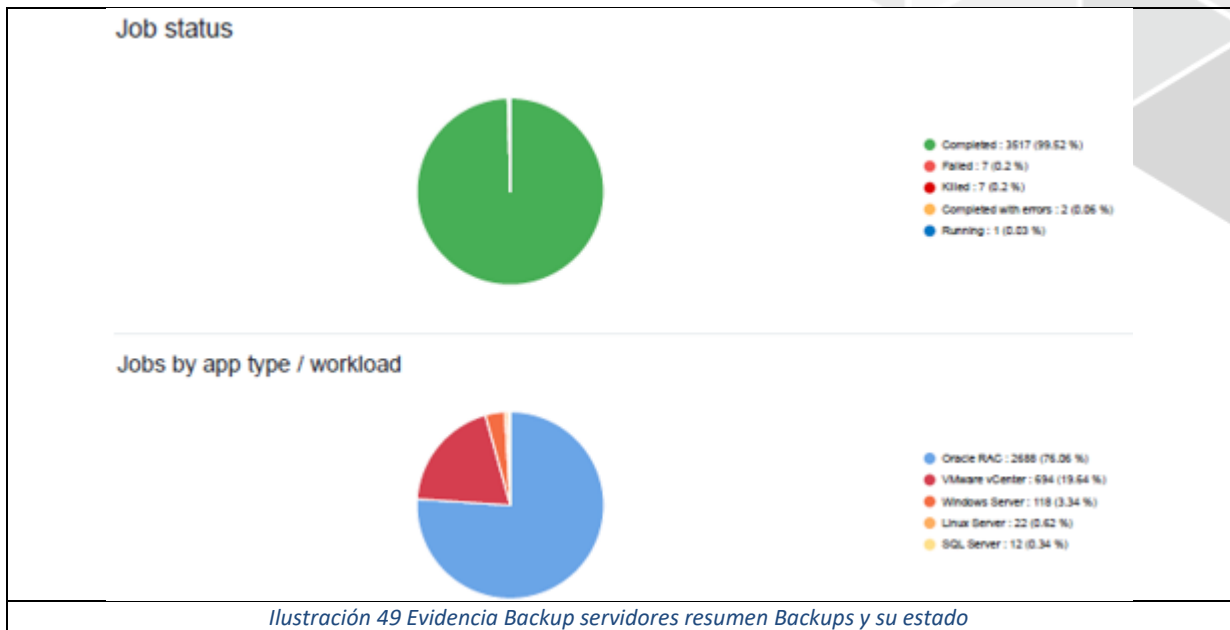
El consolidado de las cintas utilizadas hasta la fecha son las siguientes:

| Ubicación    | Cantidad de Cintas ICETEX |
|--------------|---------------------------|
| Custodia     | 274                       |
| Librería     | 35                        |
| WISE         | 60                        |
| <b>Total</b> | <b>369 cintas</b>         |

*Tabla 31 Cintas Backups ICETEX*

Para el mes de Agosto el resultado de la ejecución de los Backups fue el siguiente:

| Backup job summary                                                        |                                                                                                        | Generated on: Sep 1, 2025, 8:39 am |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|------------------------------------|
| Backup job summary report                                                 |                                                                                                        |                                    |
| CommCell                                                                  | All                                                                                                    |                                    |
| Company                                                                   | All                                                                                                    |                                    |
| Server groups                                                             | INFOTIC                                                                                                |                                    |
| Servers                                                                   | All                                                                                                    |                                    |
| App types / Workloads                                                     | All                                                                                                    |                                    |
| Subclients                                                                | All                                                                                                    |                                    |
| Job status                                                                | Running, Completed, Delayed, Failed, Killed, Completed with Errors, Completed with Warnings, Committed |                                    |
| Job types                                                                 | All                                                                                                    |                                    |
| Time frame                                                                | Last 4 Weeks ( Aug 4, 2025, 08:39:12 AM - Sep 1, 2025, 08:39:12 AM )                                   |                                    |
| Time zone                                                                 | Afghanistan Standard Time                                                                              |                                    |
| Day start time                                                            | 12:00 AM                                                                                               |                                    |
| Snap and Backup Copy options                                              | All                                                                                                    |                                    |
| Advanced                                                                  | All                                                                                                    |                                    |
| Agents                                                                    | All                                                                                                    |                                    |
| Max number of jobs to return                                              | 4000                                                                                                   |                                    |
| <i>Ilustración 48 Evidencia Backup servidores resumen general Backups</i> |                                                                                                        |                                    |



El total del tamaño de la información respalda para el mes de agosto corresponde a 433.78 TB, donde 99.52% se completó en el primer lanzamiento del robot con un total de 432.36 TB de información.

El 76.06% está representado en el respaldo dado a la información del Oracle RAC.

En el caso de los Backups que no fueron exitosos o que presentan algún tipo de problema son revisados de forma interna, subsanados y nuevamente tomados por el área correspondiente.

El análisis y conclusiones del comportamiento de los Backups para este mes es el siguiente:

De un total de 3534 trabajos analizados, el 99.58% se completó con éxito (incluyendo los que tuvieron errores menores). El 99.52% de todos los trabajos se completaron sin ningún error.

- Tasa de éxito: 99.58% (trabajos completados o completados con errores)
- Tasa de fracaso: 0.40% (trabajos fallidos o cancelados)
- Trabajo en curso: 1 trabajo se encuentra en ejecución.
- Oracle RAC: El 76.06% de los trabajos de respaldo corresponden a este tipo de servidor, con un total de 2688 trabajos.
- VMware vCenter: El 19.64% de los trabajos pertenecen a este entorno, con 694 trabajos.
- Otros Servidores: Los trabajos de Windows Server, Linux Server y SQL Server representan el 3.34%, 0.62% y 0.34%, respectivamente.

La evidencia se genera diariamente en el reporte que se entrega de forma automática a los correos que el ICETEX solicitó y en el informe mensual se anexan todas los soportes y evidencias de la ejecución de las políticas de Backup, la política actualizada y vigente de la toma de Backup, se encuentra en el link del repositorio [Backups Diarios](#) y el informe de Backups en la carpeta [Informe de Backups](#)

A la fecha ICETEX no ha realizado la entrega de las cintas de Backup para devolver las cintas que se están usando en calidad de préstamo para realizar el almacenamiento y traslado a custodia externa.

## 11. CONTROL DE CAMBIOS

Durante el mes de agosto 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                                                       |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|--------------------|-----------|---------------------------------------------------------------------|
| 1182       | El cambio aplica a los siguientes servidores que tienen instalado Windows Server 2019 Standard:<br>-ICTXSRVMOODLE (192.168.51.82): aloja la aplicación ComunidadICETEX ( <a href="https://comunidad.icetex.gov.co/ComunidadIcetexFront/inicio">https://comunidad.icetex.gov.co/ComunidadIcetexFront/inicio</a> ), publicada en internet y accedida por usuarios externos.<br>-ICTXSRVAPPMIX3 (192.168.51.139): aloja el servicio CustomWindowsServiceNovacion, crítico para procesos internos. Ambos servidores serán actualizados con los últimos parches de seguridad y estabilidad de Windows. No se verán afectadas otras máquinas o servicios fuera de estos entornos.                                                                                                                                                                                                 | 31/07/2025        | 09/08/2025         | Exitoso   | N/A                                                                 |
| 1183       | El cambio aplica a los siguientes servidores en entorno de producción:<br>-ICTXSRVNETCOR01 (192.168.51.165) aloja las aplicaciones PSE, Cargue Archivos, Cuentas Abandonadas, Cuentas Inactivas, Portal Transaccional y Transunion, las cuales están publicadas en internet y accedidas por usuarios externos.<br>-ICTXSRVAPPMIX1 (192.168.51.134): aloja las aplicaciones internas Desembolsos, Reportador, Servicios de Integración MEN, Censo Indígena, Sisbén, Vigía e Icfes, utilizadas para procesos institucionales críticos.<br>-ICTXSRVDCVAL01 (192.168.51.170): aloja la aplicación Deceval, esencial para la integración con servicios financieros externos. Los tres servidores serán actualizados con los últimos parches de seguridad y estabilidad del sistema operativo Windows. No se verán afectadas otras máquinas ni servicios fuera de estos entornos. | 05/08/2025        | 09/08/2025         | Exitoso   | N/A                                                                 |
| 1185       | Actualización servidor Oracle contingencia-INR0278                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 21/08/2025        | 22/08/2025         | Exitoso   | N.A                                                                 |
| 1186       | Despliegue de componente Java para borrado de caché cada 20 minutos.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 20/08/2025        | 21/08/2025         | Exitoso   | El equipo OCM reporta mejoría en el desempeño en las publicaciones. |
| 1189       | Reinicio controlado para restablecer imágenes en el portal ICETEX.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 26/08/2025        | 26/08/2025         | Ejecutado | N.A                                                                 |
| 1190       | Reinicio controlado para restablecer imágenes en el portal ICETEX con servicio NFS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 27/08/2025        | 27/08/2025         | Ejecutado | N.A                                                                 |
| 1192       | Ejecución de dos scripts Groovy para reindexado del portal ICETEX únicamente en nodo 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 28/08/2025        | 28/08/2025         | Ejecutado | N.A                                                                 |

*Tabla 32 Controles de cambio agosto*

## 12. PLAN DE TRABAJO DE LOS PROXIMOS MESES

Se adjunta la tabla del plan de trabajo:

| Actividades                                                            | Responsables | Fecha Inicio | Fecha fin  | Verificación                                                                             |
|------------------------------------------------------------------------|--------------|--------------|------------|------------------------------------------------------------------------------------------|
| Monitoreo de disponibilidad de balanceador en la herramienta ELK.      | INFOTIC      | 25-08-2025   | 31-10-2025 | En gestión con el Aliado para incluir en la herramienta ELK el balanceador implementado. |
| Revisar las alternativas de solución respecto al licenciamiento de las | ICETEX       | 01-06-2025   | 31-12-2025 | Esta situación implica riesgos críticos tanto a                                          |

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

| Actividades                                                                                                                                      | Responsables     | Fecha Inicio | Fecha fin  | Verificación                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------|------------------|--------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| herramientas de seguridad (perimetral y antivirus)                                                                                               |                  |              |            | nivel de seguridad como de continuidad operativa, entre los que se destacan: <ul style="list-style-type: none"> <li>Falta de actualizaciones de seguridad críticas.</li> <li>Mayor exposición a vulnerabilidades y ataques cibernéticos.</li> <li>Incompatibilidad con software y hardware actualizado.</li> <li>Ausencia de soporte oficial por parte del fabricante.</li> </ul> |
| Se debe realizar mesa técnica conjunta entre ICETEX e INFOTIC para revisar las alternativas de solución frente a la gestión de vulnerabilidades. | INFOTIC – ICETEX | 01-12-2024   | 31-08-2025 | Infotic seguirá enviando los insumos para el comité de vulnerabilidad, se coordina sesión con la especialista de seguridad de ICETEX para definir el proceso de tratamiento de vulnerabilidades.                                                                                                                                                                                  |
| Actualización de Liferay de la versión 7.3 a la 7.4                                                                                              | ICETEX           | 01-12-2024   | 31-08-2025 | Depende de la contratación del soporte de LIFERAY, por parte del ICETEX.                                                                                                                                                                                                                                                                                                          |
| Verificar la configuración de los equipos de LAN y WAN que hace falta para el funcionamiento de IPV6.                                            | INFOTIC - ICETEX | 01-12-2024   | 30-09-2025 | Se está haciendo seguimiento a estos temas de implementación de IPV6 en las sesiones semanales. Ver avances en la última acta de seguimiento del mes de agosto.                                                                                                                                                                                                                   |
| Gestión de la administración Azure nube                                                                                                          | INFOTIC - ICETEX | 01-12-2024   | 31-08-2025 | Para efectos de poder avanzar en la este frente, se requiere la designación del personal, por parte de ICETEX, para retomar las sesiones de trabajo y así, definir el plan a seguir.                                                                                                                                                                                              |
| Políticas e inventarios de las creaciones en la nube                                                                                             | INFOTIC - ICETEX | 01-12-2024   | 31-08-2025 | Para efectos de poder avanzar en la este frente, se requiere la designación del personal, por parte de ICETEX, para retomar las sesiones de trabajo y así, definir el plan a seguir.                                                                                                                                                                                              |
| Capacitación en seguridad al grupo de especialistas de seguridad del ICETEX                                                                      | INFOTIC - ICETEX | 01-12-2024   | 31-10-2025 | Se realizó la primera capacitación de temas de ciberseguridad al ICETEX el 03/04/2025. Se continuará coordinando con ICETEX las capacitaciones previstas para cada año                                                                                                                                                                                                            |
| Monitoreo de los diferentes servicios realizados por el SOC. Revisión conjunta entre ICETEX – INFOTIC                                            | INFOTIC - ICETEX | 01-12-2024   | 31-12-2025 | Se envió el mes pasado al ICETEX un informe sobre los dispositivos que están siendo monitoreados por el SOC, con el fin de que sean validados por dicha entidad. Actualmente, estamos a la espera de su respuesta. El correo tiene como asunto: Dispositivos monitoreados FortiSIEM.                                                                                              |
| Revisar la parametrización de restricción y los problemas ocasionados a la conexión, para activar el agente de antivirus en las bases de datos.  | INFOTIC - ICETEX | 01-12-2024   | 31-12-2025 | Se realizó una primera sesión con los ingenieros de CLARO e INFOTIC para revisar y está en curso la identificación de la causa para poder generar la solución.                                                                                                                                                                                                                    |
| Solicitud de instalación de (5)                                                                                                                  | INFOTIC -        | 01-12-2024   | 30-06-2025 | Se entregó la propuesta comercial a                                                                                                                                                                                                                                                                                                                                               |

| Actividades                                                                                        | Responsables | Fecha Inicio | Fecha fin | Verificación                        |
|----------------------------------------------------------------------------------------------------|--------------|--------------|-----------|-------------------------------------|
| Internet para la gente en las Oficinas ICETEX de Manizales, Armenia, Cartagena, Sincelejo y Pasto. | ICETEX       |              |           | ICETEX de los internet solicitados. |

*Tabla 33 Planes de trabajo*

### 13. RECOMENDACIONES DEL CONTRATISTA AL ICETEX

#### 13.1. Licenciamiento De Software

Se recomienda efectuar la renovación del soporte de LIFERAY, el cual estuvo activo hasta el pasado 31 de diciembre de 2024 y se prorrogó, por garantía, hasta el 31 de enero de 2025. Es imperativo actualizar el soporte para garantizar la colaboración del fabricante en varios procesos tales como: La obtención de nuevos instaladores, parches de seguridad, claves de licencia para el entorno productivo, así como para pruebas y desarrollo (localhost), y posteriormente llevar a cabo la migración a la nueva versión Liferay 7.4 GA125.

#### 13.2. Networking

**Renovación de Equipos:** Se sugiere llevar a cabo la actualización de los equipos de la entidad, ya que muchos de ellos se encuentran obsoletos y carecen de soporte por parte del fabricante, lo que podría afectar el rendimiento y la seguridad de la infraestructura.

**Reemplazo de Equipos Dañados:** Luego del daño del equipo en la sede de San Andres, se informa a ICETEX que actualmente no hay disponibilidad de equipos adicionales para reemplazos futuros en caso de que surjan nuevos daños.

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

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

**Aprovisionamiento de espacio.** Se ha reportado el espacio empleado en la unidad F del servidor ICTXSRVNETCOR01, el cual llega a unos umbrales cercanos al 94% poniendo en riesgo la disponibilidad de dicho servidor. Se recomienda, al ICETEX, validar las políticas de respaldo que se aplican sobre la información allí almacenada así como evaluar la posibilidad de disponer de información histórica en otros medios de almacenamiento permitiendo liberar este espacio.

#### 13.3. Aplicaciones

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

Existen aplicaciones que operan sobre el Framework .Net Classic, se recomienda que sean migradas a un Framework más actual y que cuente con soporte vigente. En la actualidad los ambientes de pruebas cuentan con Framework actualizado, lo que permite que las actualizaciones puedan validarse en estos ambientes controlados.

Existen aplicaciones que están implementadas en sistemas operativos obsoletos sean migradas a Servidores con sistemas operativos de versiones actuales y con soporte de Microsoft.

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

Se sigue identificado que el servidor ICTXSRVNETCOR01 presenta una situación crítica relacionada con el espacio en disco en la unidad F:\ la cual dispone únicamente de 69.4 GB libres de un total de 1.79 TB. Este espacio se encuentra comprometido principalmente por archivos antiguos de la aplicación CargueArchivos, almacenados desde el año 2019, por lo que se recomienda aplicar el aumento del almacenamiento en la ruta identificada o que se depuren archivos obsoletos por parte de los responsables de la aplicación, en dado caso que no se realicen estas dos sugerencias existe el riesgo de que el servidor quede sin espacio suficiente en esa partición, afectando gravemente el rendimiento, la estabilidad del sistema y la disponibilidad de la aplicación CargueArchivos, con posibles interrupciones en el servicio.

Se sigue identificado que el servidor ICTXSRVNETCOR01 presenta una situación crítica relacionada con el espacio en disco en la unidad E:\ la cual dispone únicamente de 4.82 GB libres de un total de 65 GB. Este espacio se encuentra comprometido principalmente por archivos antiguos que contienen todos los logs de las aplicaciones configuradas, por lo que se recomienda aplicar el aumento del almacenamiento en la ruta identificada, en dado caso que no se realice esta sugerencia existe el riesgo de que el servidor quede sin espacio suficiente en esa partición, afectando que no se registren más logs.

A continuación, se presenta un cuadro histórico consolidado del uso del almacenamiento en los discos del servidor ICTXSRVNETCOR01, correspondiente a los meses de junio, julio y Agosto de 2025, seguido de recomendaciones de observaciones y recomendaciones:

| Disco | Métrica       | jun-25         | jul-25         | ago-25         | Observaciones                                                                                             | Recomendaciones                                                                                                                        |
|-------|---------------|----------------|----------------|----------------|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| C:    | Espacio usado | 61% (61.7 GiB) | 65% (66.6 GiB) | 58% (58.1 GiB) | Se incrementa el uso mensual del disco en aproximadamente 3-4 GiB.                                        | Considerar mover archivos no esenciales a otro volumen que dispongan desde el lado de infraestructura hacia almacenamiento secundario. |
|       | Espacio libre | 38.3 GiB       | 33.3 GiB       | 41.4 GiB       | Si continúa esta tendencia, se alcanzará el 80% de uso en los próximos 4 meses.                           |                                                                                                                                        |
| F:    | Espacio usado | 95% (1.71 TiB) | 92% (1.74 TiB) | 95% (1.80 TiB) | Altísima ocupación constante (>90%), aunque mejora en julio debido al aumento del almacenamiento en 100GB | Urgente implementar políticas de depuración de archivos antiguos o inactivos.                                                          |
|       | Espacio libre | 86.5 GiB       | 146 GiB        | 89.4 GiB       |                                                                                                           | Considerar expansión del volumen o migración de datos a almacenamiento secundario.                                                     |
| E:    | Espacio usado | 88% (57.2 GiB) | 79% (51.7 GiB) | 65% (42.5 GiB) | Notable mejora en julio con liberación archivos logs de aproximadamente 5.5 GiB.                          | Considerar mover archivos no esenciales a otro volumen que dispongan desde el lado de infraestructura hacia almacenamiento secundario. |
|       | Espacio libre | 7.82 GiB       | 13.3 GiB       | 22.4 GiB       | Aún se mantiene en zona de riesgo por encima del 75%.                                                     | Considerar expansión del volumen si requieren almacenar por mucho más tiempo los logs de las aplicaciones                              |

*Ilustración 50 consolidado del uso almacenamiento en discos servidor ICTXSRVNETCOR01*

### 13.4. Seguridad

En cuanto a la gestión de las bases de datos se recomienda retirar permiso de SUDO a los usuarios INFOTIC, GAWUSER y DCSCAF pues, con estos usuarios, podrían realizar actividades administrativas que no van con su rol. Para ello se debe analizar la razón de estos privilegios con los equipos que realizan mantenimientos a las aplicaciones y verificar el cambio a un rol más apropiado a sus labores.

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

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

Analizar el inventario de aplicaciones en la entidad para darle un mejor uso a la nube Azure, este inventario

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

debe tener versiones de lenguajes de programación, aun cuando el alcance es sólo Azure y sus políticas con mejores prácticas (gobernanza), es una oportunidad para que las buenas prácticas de la nube se apliquen también en los Datacenter de la entidad.

- Se debe trabajar en el perfilamiento de la navegación de acuerdo con lo entregado por ICETEX.
- Validar la autenticación de doble factor para todas las plataformas misionales del ICETEX.
- Realizar autenticación a través del LDAPS, para la gestión de las plataformas de seguridad.
- Realizar la contención automática de equipos que se identifiquen en la red como maliciosos.
- Realizar el aumento de recursos a la plataforma de FortiSIEM (CPU, Memoria y disco) y hacer un cambio de arquitectura con el objetivo de mejorar.
- Se debe realizar la integración de los activos críticos de la compañía a la plataforma de SIEM, no se ha podido lograr por la falta de recursos de este.
- Adquirir un equipo Firewall para correo para prevenir brechas de seguridad asociadas al uso del correo electrónico y que este es susceptible a muchos tipos de amenazas.
- Integrar los servidores de Directorio Activo con el SIEM.
- Garantizar la segmentación de la red que permita claramente definir qué servicios deben ser alcanzados por cada usuario.
- Se recomienda, que el ICETEX, adquiera una herramienta que permita realizar análisis de tráfico de la red (NTA- Network Traffic Analysis).
- Se recomienda una tecnología que permita la gestión o validación de privilegios de accesos (IAM). Evitar configurar usuarios y claves dentro de las aplicaciones de ICETEX.
- Validar a nivel de punto final, los equipos que se han visto involucrados con comportamiento malicioso.
- Integrar los equipos que hacen parte del proceso de pagos con el SIEM.
- Evaluar los riesgos sobre las plataformas en la nube y considerar aplicar plataformas de seguridad para los ambientes Cloud que cuenta la entidad ya que estos contienen servicios críticos para la misma.

### **13.5. Bases De Datos**

Se deben aumentar los espacios del área de recuperación de las bases de datos productivas de 1TB a 5TB para tener una retención de 10 días o más, con el TB de almacenamiento aprovisionado solo se puede mantener 2 días por BD.

Las versiones disponibles del sistema manejador de base de datos ORACLE son Oracle Database 23 ai, Oracle Database 21c y Oracle Database 19c. No obstante que se dio inicio, al plan de migración de las bases de datos que se encuentran en versiones anteriores, se recomienda al ICETEX, que analice la posibilidad de efectuar la migración sobre versiones más recientes con el fin de evitar ejecutar planes de migración con demasiada frecuencia.

### **13.6. Integrador De Nube**

Configuraciones y malas prácticas permanentes (usuarios identificables por convención de la entidad nombre y apellido, hay usuarios que se conectan con cuentas administradoras de office 365 que al ser administradores hacen imposible su identificación dentro de la compañía).

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

Sede principal-Bogotá, Colombia  
Calle 93B # 13-44, Segundo piso  
NIT:900.068.796-1  
Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
Cra. 24 No. 53ª-26 Arboleda  
Alta.  
NIT: 900.068.796-1  
Teléfono: (+606) 88612612

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

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

Se envió un reporte con la lista de máquinas Windows 10 encontradas en la nube de Azure como respuesta al riesgo de seguridad notificado mediante el correo con el asunto “Boletín de seguridad COLCERT Fin del Soporte de Windows 10” para su socialización y escalamiento, a la fecha no hemos informado del funcionario delegado, por el ICETEX, para atender este aspecto.

#### 14. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC

Con respecto a los valores agregados indicados contractualmente, se relaciona el estado:

##### 14.1. Aumento de la capacidad de Ancho de Banda en algunas de las sedes de la Entidad

El proceso de ampliación de las sedes de la entidad se completó en el mes de noviembre de 2024 , permitiendo un aumento en la capacidad de ancho de banda conforme a lo establecido en el ANEXO # 2. esta información se puede evidenciar a través de la herramienta de monitoreo Solar Winds y se verifica mensualmente en la facturación de ICETEX.

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

Para el periodo de reporte no se presentan avances, dado que la capacitación, que se debe realizar, es una vez al año, la cual se ejecutó el pasado **3 de abril de 2025**, en el horario de **2:00 p.m. a 4:00 p.m.**

Se continuará con la programación de las capacitaciones pendientes de acuerdo con la disponibilidad de agenda de los equipos de trabajo del ICETEX, aspecto que se concertará con la supervisión del contrato.

##### 14.3. Capacidad de almacenamiento en TB

El almacenamiento definido contractualmente fue entregado en la fase de implementación por **Contrato** ingresaron las siguientes capacidades:

| CONTRATADO   |            |                                            |                |
|--------------|------------|--------------------------------------------|----------------|
| Cod Servicio | CIUDAD     | ALCANCE                                    | CAPACIDAD (TB) |
| INR0194      | TRIARA     | Almacenamiento Centralizado 23 TB Tier 2   | 35             |
| INR0193      | TRIARA     | Almacenamiento Centralizado 12 TB Tier 2.5 |                |
| INR0192      | MEGACENTER | Almacenamiento Centralizado 15 TB Tier 2   | 25             |
| INR0191      | MEGACENTER | Almacenamiento Centralizado 10 TB Tier 2.5 |                |
|              |            |                                            | <b>60</b>      |

*Tabla 34 Capacidades de almacenamiento contratado*

Aprovisionado se tienen las siguientes capacidades instaladas:

Sede principal-Bogotá, Colombia  
 Calle 93B # 13-44, Segundo piso  
 NIT:900.068.796-1  
 Teléfono (+601) 7466000- 3185214505

Sede Manizales, Colombia  
 Cra. 24 No. 53ª-26 Arboleda  
 Alta.  
 NIT: 900.068.796-1  
 Teléfono: (+606) 88612612

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

*Tabla 35 Capacidades de almacenamiento aprovisionado*

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

#### 14.4. Se oferta Ítem de “Wifi” para la gente en 19 sedes

Se ha estado llevando a cabo el cumplimiento contractual y hasta la fecha, se dispone de conexión wifi en las 14 sedes donde ICETEX tiene oficinas.

INFOTIC envió el 23 de abril propuesta comercial a ICETEX de 5 Canales Internet Para la gente, en respuesta a la solicitud de instalación de cinco puntos de Internet para las sedes de Manizales, Armenia, Cartagena, Sincelejo y Pasto, sin tener una respuesta a la fecha.

La oferta se puede consultar en el link: [Oferta Wifi para la gente](#)

| Enlace - Tipo medio | INR        | BW- Mínimo<br>Requerido (MBPS) | Ancho de Banda<br>actual |
|---------------------|------------|--------------------------------|--------------------------|
| BARRANQUILLA        | INR0094    | 10                             | 10                       |
| BUCARAMANGA         | INR0057    | 10                             | 10                       |
| CALI                | INR0160    | 10                             | 10                       |
| AGUAS               | INR0029    | 20                             | 20                       |
| CHAPINERO           | INR0015    | 20                             | 20                       |
| MEDELLIN            | INR0122    | 10                             | 10                       |
| APARTADO            | INR0140    | 10                             | 10                       |
| ARAUCA              | INR0115    | 10                             | 10                       |
| LETICIA             | INR0000378 | 10                             | 10                       |
| QUIBDO              | INR0021    | 10                             | 10                       |
| RIOHACHA            | INR0159    | 10                             | 10                       |
| SAN ANDRES          | INR0000368 | 10                             | 10                       |
| YOPAL               | INR0127    | 10                             | 10                       |
| MOCOA               | INR0141    | 10                             | 10                       |

*Tabla 36 WIFI para la gente instalados*

| Enlace - Tipo medio | INR     | BW- Mínimo<br>Requerido (MBPS) |
|---------------------|---------|--------------------------------|
| Manizales           | INR0088 | 10                             |
| Armenia             | INR0074 | 10                             |
| Cartagena           | INR0109 | 10                             |
| Sincelejo           | INR0095 | 10                             |
| Pasto               | INR0130 | 10                             |

*Tabla 37 WIFI para la gente pendientes*

## 15. CONCLUSIONES

- El uso de autenticación de doble factor en las conexiones VPN de los funcionarios ayudaría a proteger mejor la información sensible y evitar accesos no autorizados.
- Administrar adecuadamente las contraseñas y permisos garantiza que solo las personas autorizadas accedan a información importante, reduciendo riesgos de seguridad.
- Configurar controles de acceso a la red basados en los servidores de la entidad permite restringir el acceso a ciertas áreas, evitando que los usuarios lleguen a sitios peligrosos.
- Optimizar los recursos del FortiSIEM facilitaría el monitoreo de sistemas clave como bases de datos, aplicaciones internas y equipos, permitiendo detectar problemas rápidamente y responder de forma oportuna.
- Ajustar las reglas de seguridad en la red ha permitido un mejor control sobre los recursos clave, asegurando que solo lo necesario esté disponible y fortaleciendo la protección.
- Implementar soluciones para gestionar quién puede conectarse a la red mejoraría la seguridad y reduciría

el impacto de posibles incidentes.

- Los reportes del SOC han sido clave para detectar y corregir vulnerabilidades, evitando que amenazas afecten la infraestructura crítica de la entidad.
- Es fundamental contar con una persona desde ICETEX en temas de nube que pueda auditar y revisar autorizaciones, ya que su apoyo es crucial para abordar y resolver los hallazgos reportados, lo que permitirá avanzar en los proyectos relacionados con recursos en la nube. La falta de un responsable limita la capacidad de gestión y solución de problemas en este ámbito.

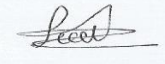
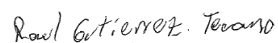
## 16. ANEXOS

| Tema                          | SubTema                                        | Anexo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Almacenamiento</b>         | Backups Diarios                                | Backups diarios Agosto 2025 (30 reportes)<br><a href="#">Backups Diarios</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                               | Informe de Backups                             | Consolidado mensual Backups Agosto 2025<br><a href="#">Consolidado Diario de Backups agosto 2025.pdf</a><br><a href="#">Informe Backups mes de Agosto 2025.pdf</a><br><a href="#">Politica Backup Icetex V2.xlsx</a>                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Aplicaciones</b>           | Informes de actividades                        | Informe actividades Módulos videoconferencia ICETEX agosto 2025<br><a href="#">Informe actividades Módulos videoconferencia ICETEX agosto 2025.pdf</a><br>Informe mensual Administrador de Soluciones Agosto 2025<br><a href="#">Informe Mensual InfoTIC Administrador de Soluciones Agosto 2025.pdf</a><br>Informe mensual Administrador Web Master Agosto 2025<br><a href="#">Informe Mensual InfoTIC Webmaster Agosto 2025.pdf</a><br>Informe mensual Integrador Nube agosto 2025<br><a href="#">Informe Mensual InfoTIC Integrador de Nube Agosto 2025.pdf</a>                                  |
| <b>Bases De Datos</b>         |                                                | Informe mensual Administrador de Bases de datos Agosto 2025<br><a href="#">Informe Mensual InfoTIC DBA Agosto 2025.pdf</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Ejecución Presupuestal</b> |                                                | Conciliación agosto consolidado<br><a href="#">Conciliación Agosto consolidado.xlsx</a><br>Consolidado informe mensual especialistas agosto 2025<br><a href="#">Informe Mensual Agosto 2025.pdf</a><br>Informe de Gestión Servicio agosto 2025<br><a href="#">Informe de Gestion Servicio Agosto 2025.pdf</a>                                                                                                                                                                                                                                                                                       |
| <b>Seguridad</b>              |                                                | Informe Mensual MARCA-OSINT ICETEX agosto 2025<br><a href="#">Informe Mensual MARCA-OSINT ICETEX Agosto 2025.pdf</a><br>Informe Mensual Seguridad agosto 2025<br><a href="#">Informe Mensual InfoTIC Seguridad Agosto 2025.pdf</a><br>Informe Mensual SOC - ICETEX agosto 2025<br><a href="#">Informe Mensual SOC-TH ICETEX Agosto 2025.pdf</a><br>Informe técnico análisis de vulnerabilidades ICETEX agosto 2025<br><a href="#">Informe Tecnico Analisis De Vulnerabilidades ICETEX Agosto2025.pdf</a><br>Reporte de IPS Agosto 2025<br><a href="#">Reporte de IPS de Agosto_infotc_2025.docx</a> |
|                               | <b>Reporte total de ataques recibidos-SIEM</b> | Denegados agosto 1-15<br><a href="#">Denegados Agosto1-15.pdf</a><br>Denegados agosto 16-31                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Tema                         | SubTema                    | Anexo                                                                                                                                                                                                                                                                                                                     |
|------------------------------|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              |                            | <a href="#">Denegados Agosto16-31.pdf</a>                                                                                                                                                                                                                                                                                 |
| <b>Soporte Y Monitoreo</b>   | <b>Canales</b>             | ANS agosto 2025 <a href="#">ANS_agosto_2025.xlsx</a><br>Informe mensual Administrador de Networking agosto 2025<br><a href="#">Informe Mensual InfoTIC Administrador de Redes Agosto 2025.pdf</a><br>Informe Mensual Disponibilidad agosto 2025<br><a href="#">Reporte Mensual Disponibilidad INFOTIC Agosto 2025.pdf</a> |
|                              | <b>Gráficas de consumo</b> | Informe Mensual ALLOT Agosto 2025<br><a href="#">Informe Mensual ALLOT Agosto 2025.xls</a>                                                                                                                                                                                                                                |
| <b>Data center Alterno</b>   | <b>Replicación</b>         | Informe mensual replicación agosto 2025<br><a href="#">Informe mensual replicacion Agosto 2025.pdf</a><br>Reportes diarios agosto 2025 (30 reportes)<br><a href="#">Replicacion</a>                                                                                                                                       |
| <b>Data Center Principal</b> |                            | Reporte Monitoreo ICETEX agosto 2025-ELK<br><a href="#">Reporte Monitoreo ICETEX agosto 2025-ELK.pdf</a><br>Data ELK<br><a href="#">Disponibilidad Server ELK Agosto2025.xlsx</a><br>Controles de Cambios agosto<br><a href="#">Control de Cambios</a>                                                                    |

Tabla 38 Anexos

#### Revisión técnica

| REVISÓ                                                                 | FIRMAS                                                                                |
|------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| SANDRA MILENA GARCIA HERNANDEZ<br>CONTRATISTA GRUPO DE INFRAESTRUCTURA |   |
| JOAO DO NELSON DUCUARA<br>CONTRATISTA GRUPO DE INFRAESTRUCTURA         |  |
| RAUL FERNANDO GUTIERREZ TECANO<br>ANALISTA 2                           |  |