

Orden de pago :
OP2026-111654P



INFORMACIÓN DEL COMPROMISO		Página :	1
Documento	CONTRATO	Fecha :	27/01/2026
Número	22792 CDP CDVF 2026-2022037		

IDENTIFICACIÓN DEL TERCERO			
Nombre :	INFOTIC S.A		
Tipo Doc :	NIT	Número	900068796-1
		Régimen IVA	REGIMEN COMUN

CUENTA ENTIDAD FINANCIERA A EFECTUAR EL PAGO			
Forma Pago :	Transferencia	Código - Nombre Entidad	06 BANCO SANTANDER/ CorpBanca
Tipo Cuenta :	Ahorros	Número cuenta	008016476
Girar a nombre de :	INFOTIC S.A	Núm. Ident.	900068796

CONCEPTO DE LA ORDEN DE PAGO	
Pago de factura FVE 2337- por concepto de servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el icetex. en la ciudad de Bogotá correspondiente a los servicios prestados en el mes de diciembre de 2025	

SubTotal	652,165,854.00	Firmado por: jabecerra 30/01/2026 04:36:10 p. m. JAIME ALEJANDRO BECERRA ACOSTA APROBÓ PAGO
IVA	123,911,512.00	
TOTAL	776,077,366.00	
Legalización Anticipos	0.00	
Rete Renta		
Rete IVA		
Rete ICA		
Otras		
NETO A TRANSFERIR		
Son : SETECIENTOS SETENTA Y SEIS MILLONES SETENTA Y SIETE MIL TRESCIENTOS SESENTA Y SEIS PESOS		

Firmado por: dmora 02/02/2026 02:37:37 p. m.	Firmado por: ctorrijos 02/02/2026 03:23:50 p. m.	Firmado por: evalderrama 02/02/2026 04:42:16 p. m.
PRESUPUESTO	CONTABILIDAD	TESORERÍA



Al contestar cite Radicado 20265000082440-E Id: 7394841
Folios: 5 Fecha: 2026-01-23 09:59:18
Anexos: 0
Remitente: VICEPRESIDENCIA DE OPERACIONES Y TECNOLOGIA
Destinatario: INFOTIC SOLUCIONES INTELIGENTES S.A. -
VICEPRESIDENCIA ADMINISTRATIVA y OTROS

Bogotá, D.C, 22 de enero de 2025

Señor

ADOLFO ANTONIO TEJADA DIAZ

Gerente General

INFOTIC

Correo electrónico: presidencia@infotico.co; vicepresidencia.operaciones@infotico.co;

gerenciaimplementacionicetex@infotico.co

Bogotá D.C.

ASUNTO: CONTRATO N°.2022-0792 Confirmación de valor a facturar mes de DICIEMBRE 2025- Componente base

Cordial saludo.

En el marco de la etapa de ejecución del contrato N°. 2022-0792 cuyo objeto consiste en los “*Servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el ICETEX*”, la supervisión del contrato procede a confirmar el valor de facturación para el mes de **DICIEMBRE de 2025** para los servicios del componente base, conforme con los siguientes antecedentes:

1. MARCO LEGAL PROCEDIMENTAL:

Por remisión contractual al Manual de Contratación de ICETEX, resulta aplicable el aparte contenido en el Manual de Contratación que se transcribe a continuación:

11.3. Elementos de la minuta de contrato. (...)

I. Mecanismos de protección de los derechos e intereses del ICETEX:

(...)

iii. Acuerdo de Nivel de Servicios (ANS) para la adquisición de Bienes y Servicios:

La fijación del descuento que autorice la cláusula se hará siguiendo estrictamente los parámetros que se consignan en el contrato para el efecto, o en su defecto los siguientes pasos:

- Se proyectará, en documento escrito, la cuantía que se planea pagar, discriminando los fundamentos que lo motivan.
- De este escrito se le correrá traslado al contratista para que, dentro del término de tres (3) días hábiles, exprese sus opiniones y comentarios.
- Analizado lo señalado por el contratista, se proyectará el documento definitivo que contendrá la suma que se le reconocerá al contratista como remuneración, incluyendo el decremento que llegare a ocasionarse tras la valoración de lo señalado en los numerales precedentes.

ICETEX

● Carrera 3 # 18-32 Bogota Colombia ● www.icetex.gov.co ● Canal Telefónico / WhatsApp: 333 6025656 ● Nacional: 01 8000 91 68 21
@ icetex_colombia @icetex_oficial @ICETEXTV /icetexcolombia ICETEX in ICETEX @ICETEX

Defensor del Consumidor Financiero

● www.defensoriasernarojas.com ● Carrera 16 A No. 80-63. oficina 601. Edificio Torre Oval. Bogotá, Colombia
✉ defensoria@defensoriasernarojas.com ☎ 601 4898285 Bogotá, Colombia

Revise si es necesario imprimir este documento. Desde el ICETEX aportamos en la implementación de la Política Cero Papel y, a su vez, al cuidado de los recursos naturales.

- El contratista solo podrá presentar factura o cuenta de cobro, o sus equivalentes, por el valor reconocido en el documento definitivo de valoración de la remuneración derivada de la aplicación de los acuerdos de niveles de servicio ANS.

2. CUMPLIMIENTO DEL PROCEDIMIENTO

- Mediante Radicado 20265000078855-E Id: 7386316 del 20 de enero de 2026, ICETEX proyectó y envió a INFOTIC documento escrito indicando la cuantía que se validó a pagar y discriminando los fundamentos que lo motivan, indicando que el traslado se surte por tres (3) días para que se manifieste como corresponda.
- El 21 de enero de 2026, ICETEX recibió comunicación con radicado VOP-005-2026 en el que INFOTIC manifestó lo siguiente:

“ ...

Referencia: Contrato 2022-0792

Asunto: Respuesta al Radicado 20265000078855-E Id: 7386316: Notificación valor a facturar mes de DICIEMBRE DE 2025-Componente base.

Cordial saludo,

De acuerdo con la etapa de ejecución establecida en el contrato 2022-0792, el cual tiene como objeto "Servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el ICETEX", informamos que se ha validado el memorando de facturación correspondiente a la línea base de los servicios prestados en el periodo diciembre 2025.

En virtud de la ejecución del contrato de la referencia, INFOTIC se permite dar respuesta al comunicado con el Radicado 20265000078855-E Id: 7386316, así:

REVISIÓN Y CONCILIACIÓN DE LOS VALORES A PAGAR POR LA LINEA BASE DURANTE EL MES DE DICIEMBRE DE 2025

El memorando de ICETEX en su numeral II, hace referencia al RECuento DE LOS COMPONENTES Y PAGOS A REALIZAR, de acuerdo a los siguientes ítems:

2.1. CONECTIVIDAD Y RED DE COMUNICACIONES. Habiendo revisado los conceptos y dado que se cuenta con el aval del Gerente de Proyecto INFOTIC, se procede a aceptar el valor conciliado en los términos expresados en el memorando:

"Dado lo anterior, para los servicios prestados en conectividad y red de comunicaciones, se realizó el cálculo de acuerdo con la aplicación de los ANS establecidos y la disponibilidad reportada en los canales de comunicaciones, verificando las sedes en operación en la herramienta de monitoreo, determinando que para estos servicios se debe realizar un descuento por aplicación de ANS por valor de VEINTE MILLONES QUINIENTOS TREINTA Y SIETE MIL NOVECIENTOS DOCE PESOS (\$20.537.912) MCTE, y el monto a pagar por este ítem es de CIENTO TREINTA MILLONES OCHOCIENTOS NOVENTA Y DOS MIL SEISCIENTOS NOVENTA Y DOS

ICETEX

● Carrera 3 # 18-32 Bogota Colombia ● www.icetex.gov.co ● Canal Telefónico / WhatsApp: 333 6025656 ● Nacional: 01 8000 91 68 21
@ icetex_colombia @icetex_oficial @ICETEXTV /icetexcolombia ICETEX ICETEX @ICETEX

Defensor del Consumidor Financiero

● www.defensoriasernarojas.com ● Carrera 16 A No. 80-63. oficina 601. Edificio Torre Oval. Bogotá, Colombia
✉ defensoria@defensoriasernarojas.com ☎ 601 4898285 Bogotá, Colombia

Revisa si es necesario imprimir este documento. Desde el ICETEX aportamos en la implementación de la Política Cero Papel y, a su vez, al cuidado de los recursos naturales.



PESOS (\$ 130.892.692) MCTE. El detalle de los valores calculados para cada ítem de este componente se detalla en el archivo anexo "SERVICIOS CALCULO FACTURA DICIEMBRE 2025 VF.XLSX"

2.2. SERVICIO DE COLABORACIÓN. El servicio se prestó sin ninguna novedad por lo cual el memorando no expresa ningún tipo de descuento. INFOTIC procede a aceptar el valor conciliado en los términos expresados en el memorando:

"De acuerdo con lo expuesto, para este servicio no procede descuento alguno, por lo que el valor para facturar es de CINCUENTA Y SIETE MILLONES CIENTO SESENTA MIL SEISCIENTOS VEINTINUEVE PESOS (\$57.160.629) MCTE. El detalle de los valores calculados para cada ítem de este componente se presenta en el archivo anexo SERVICIOS CALCULO FACTURA DICIEMBRE 2025 VF.XLSX."

2.3. CENTRO DE DATOS. Habiendo revisado los conceptos y dado que se cuenta con el aval del Gerente de Proyecto INFOTIC, se procede a aceptar el valor conciliado en los términos expresados en el memorando:

"De acuerdo con lo expuesto, para el subcomponente de CENTRO DE DATOS se realizará un descuento de CUARENTA Y UN MILLONES VEINTIOCHO MIL CIENTO NOVENTA Y SIETE PESOS (\$ 41.028.197) MCTE., valor correspondiente a servicios no prestados y aplicación de ANS por porcentaje de disponibilidad. En consecuencia, el valor a facturar por este componente es de CIENTO CINCUENTA Y CUATRO MILLONES OCHOCIENTOS OCHENTA Y TRES MIL SEISCIENTOS SETENTA Y CINCO PESOS (\$ 154.883.675) MCTE., cuyo detalle de valores calculados para cada ítem de este componente se discrimina en el archivo anexo SERVICIOS CALCULO FACTURA DICIEMBRE 2025 VF.XLSX."

2.4. SERVICIO DE SEGURIDAD. Habiendo revisado los conceptos y dado que se cuenta con el aval del Gerente de Proyecto INFOTIC, se procede a aceptar el valor conciliado en los términos expresados en el memorando:

"El valor a facturar para el mes de diciembre de 2025 por este componente es de DOSCIENTOS VEINTICUATRO MILLONES SETECIENTOS CATORCE MIL CIENTO NUEVE PESOS (\$224.714.109) MCTE., cuyo detalle de los valores calculados para cada ítem de este componente se incluye en el archivo anexo SERVICIOS CALCULO FACTURA DICIEMBRE 2025 VF.XLSX"

2.5. SERVICIOS CONEXOS Y PERSONAL DEL PROYECTO. Al respecto INFOTIC acepta los valores conciliados y especificados en el memorando, conforme a lo descrito por el ICETEX para este ítem:

"Realizada la revisión para el periodo objeto de este informe, no se realizarán descuentos para este concepto pues se contó con los recursos y servicios asignados al proyecto. Por tanto, el valor a facturar corresponde a la suma de CIENTO SETENTA MILLONES SEISCIENTOS CINCUENTA Y NUEVE MIL CUATROCIENTOS SETENTA Y CUATRO PESOS (\$170.659.474) MCTE. por concepto de PERSONAL DEL PROYECTO, y VEINTE MILLONES TRESCIENTOS SESENTA Y CINCO MIL SETECIENTOS OCHO PESOS (\$20.365.708) MCTE. por SERVICIOS

ICETEX

● Carrera 3 # 18-32 Bogotá Colombia ● www.icetex.gov.co ● Canal Telefónico / WhatsApp: 333 6025656 ● Nacional: 01 8000 91 68 21
@ icetex_colombia @icetex_oficial @ICETEXTV /icetexcolombia ICETEX ICETEX @ICETEX

Defensor del Consumidor Financiero

● www.defensoriasernarojas.com ● Carrera 16 A No. 80-63, oficina 601. Edificio Torre Oval. Bogotá, Colombia
✉ defensoria@defensoriasernarojas.com ☎ 601 4898285 Bogotá, Colombia

Revisa si es necesario imprimir este documento. Desde el ICETEX aportamos en la implementación de la Política Cero Papel y, a su vez, al cuidado de los recursos naturales.



CONEXOS. Los valores calculados para cada ítem de este componente se detallan en el archivo anexo "SERVICIOS CALCULO FACTURA DICIEMBRE 2025 VF.XLSX."

2.6. PLAN DE IMPLEMENTACIÓN. INFOTIC acepta los valores conciliados y especificados en el memorando, conforme a lo descrito por el ICETEX para este ítem:

"Para este componente no se realizarán descuentos, toda vez que desde junio de 2023 se llevó a cabo la implementación y migración de servicios al nuevo Datacenter, por lo que el valor a facturar es de DIECISIETE MILLONES CUATROCIENTOS UN MIL SETENTA Y NUEVE PESOS (\$17.401.079) MCTE."

Por lo anterior, y conforme al numeral 2.7 VALOR A PAGAR COMPONENTE BASE del comunicado en mención, para el periodo de Diciembre 2025, en los servicios correspondientes, procede un pago por valor total de SETECIENTOS SETENTA Y SEIS MILLONES SETENTA Y SIETE MIL TRESCIENTOS SESENTA Y SEIS PESOS (\$ 776.077.366) MCTE conforme se muestra en la siguiente tabla resumen:

SERVICIO COMPONENTE	UNIDAD DE MEDIDA	VALOR UNITARIO	IMPORTE		
			VALOR DISCONTINUO POR SERVICIO NO PRESTADO	VALOR DISCONTINUO POR SERVICIO NO PRESTADO	VALOR A FACTURAR
Consultoría y análisis de requerimientos	1	\$17.401.079			\$17.401.079
Servicio de Colaboración	1	\$17.401.079			\$17.401.079
Servicio de Datos	1	\$17.401.079			\$17.401.079
Servicio de SEGURIDAD	1	\$17.401.079			\$17.401.079
Reserva del Proyecto en Sitio	1	\$17.401.079			\$17.401.079
Servicio Contable	1	\$17.401.079			\$17.401.079
Plan de implementación	1	\$17.401.079			\$17.401.079
TOTAL					\$17.401.079

INFOTIC acepta por tanto, los cálculos presentados en el anexo **SERVICIOS CALCULO FACTURA DICIEMBRE 2025 VF.XLSX**.

Quedamos atentos a su respuesta a fin de continuar la gestión de facturación de los servicios conciliados.

3. VALOR DEFINITIVO A FACTURAR PARA EL PERIODO POR CONCEPTO DE COMPONENTE BASE

En el estado descrito del trámite, ICETEX procede a indicar que la suma definitiva que se le reconocerá al contratista como remuneración por los servicios prestados en el mes de **DICIEMBRE de 2025**, en lo que respecta al componente base del contrato inicial es de **SETECIENTOS SETENTA Y SEIS MILLONES SETENTA Y SIETE MIL TRESCIENTOS SESENTA Y SEIS PESOS (\$ 776.077.366) MCTE**. MCTE., de acuerdo con la siguiente discriminación:

ICETEX

● Carrera 3 # 18-32 Bogotá Colombia ● www.icetex.gov.co ● Canal Telefónico / WhatsApp: 333 6025656 ● Nacional: 01 8000 91 68 21
 @ icetex_colombia @icetex_oficial @ICETEXTV /icetexcolombia ICETEX in ICETEX @ICETEX

Defensor del Consumidor Financiero

● www.defensoriasernarojas.com ● Carrera 16 A No. 80-63. oficina 601. Edificio Torre Oval. Bogotá, Colombia
 ● defensoria@defensoriasernarojas.com ● 601 4898285 Bogotá, Colombia

Revisa si es necesario imprimir este documento. Desde el ICETEX aportamos en la implementación de la Política Cero Papel y, a su vez, al cuidado de los recursos naturales.

SERVICIO /COMPONENTE	INFOTIC				
	VR SERVICIO CON IVA	VALOR DESCUENTO POR ANS	VALOR DESCUENTO POR SERVICIO NO PRESTADO	DESCUENTO INFOTIC	VALOR A FACTURAR
Conectividad y red de comunicaciones	\$ 151.430.605	\$ 10.239.051	\$ 10.298.861	\$ 20.537.912	\$ 130.892.692
Servicio de Colaboración	\$ 57.160.629	\$ -	\$ -	\$ -	\$ 57.160.629
Centro de Datos	\$ 195.911.872	\$ 41.028.197	\$ -	\$ 41.028.197	\$ 154.883.675
Servicio de SEGURIDAD	\$ 225.311.753	\$ -	\$ 597.644	\$ 597.644	\$ 224.714.109
Persona del Proyecto en Sitio	\$ 170.659.474	\$ -	\$ -	\$ -	\$ 170.659.474
Servicios Conexos	\$ 20.365.708	\$ -	\$ -	\$ -	\$ 20.365.708
Plan de Implementación.	\$ 17.401.079	\$ -	\$ -	\$ -	\$ 17.401.079
TOTALES	\$ 838.241.120	\$ 51.267.249	\$ 10.896.505	\$ 62.163.754	\$ 776.077.366

En virtud de lo anterior, se solicita a INFOTIC proceder a facturar la suma indicada en cumplimiento del procedimiento aplicable, discriminado por componente.

Atentamente,



JAIME ALEJANDRO BECERRA ACOSTA

Supervisor contrato (Memorando 200252200006793-i id: 6206675)

Vicepresidente de Operaciones y Tecnología-ICETEX

Con asignación de funciones de la Dirección de Tecnología mediante memorando 202520000062-I id:6111834

Elaboró:

Jhon Edwin Mican Palacios- Técnico Administrativo 

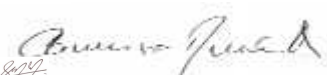
Revisó:

Sandra Milena García Hernández - Contratista Grupo de Infraestructura 

German Augusto Mejia – Coordinador de Infraestructura 

German Manuel Díaz Mejia - Contratista VOT 

Nelson Javier Casallas – Contratista VOT 

Carmenza Duran Alfonso – Contratista VOT 

Armando Castro Molina – Contratista VOT 

ICETEX

● Carrera 3 # 18-32 Bogota Colombia ● www.icetex.gov.co ● Canal Telefónico / WhatsApp: 333 6025656 ● Nacional: 01 8000 91 68 21
 [icetex_colombia](https://www.instagram.com/icetex_colombia)  [@icetex_oficial](https://twitter.com/icetex_oficial)  [@ICETEXTV](https://www.youtube.com/@ICETEXTV)  [/icetexcolombia](https://www.facebook.com/icetexcolombia)  ICETEX  ICETEX  @ICETEX

Defensor del Consumidor Financiero

● www.defensoriasernarojas.com ● Carrera 16 A No. 80-63. oficina 601. Edificio Torre Oval. Bogotá, Colombia
 defensoria@defensoriasernarojas.com  601 4898285 Bogotá, Colombia

Revisa si es necesario imprimir este documento. Desde el ICETEX aportamos en la implementación de la Política Cero Papel y, a su vez, al cuidado de los recursos naturales.

ICETEX 899999035		COMPROBANTE DE CAUSACION No. 149810 Fecha de emisión: 31/01/2026 Página: 1	
Contabilidad: ICETEX NORMA INTERNACIONAL Concepto comprobante: COMPROBANTE DE CAUSACION			
CUENTA	DESCRIPCIÓN	DÉBITOS	CRÉDITOS
25020590	GASTOS ACUMULADOS POR PAGAR SERVICIOS 900068796 INFOTIC S.A 0190 RECURSOS ICETEX Trans. de Entrega No. 111654 - CT No. 2337. Pago de factura FVE 2337- por concepto de servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el icetex. en la ciudad	776,077,366.00	0.00
2503350104	RETENCION IVA 19% 900068796 INFOTIC S.A 0190 RECURSOS ICETEX Base Orig: 652,165,854.00 Base Imp: 123,911,512.00 Trans. de Entrega No. 111654 - CT No. 2337. Pago de factura FVE 2337- por concepto de servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el icetex. en la ciudad	0.00	18,586,727.00
2503050201	SERVICIOS GENERALES DECLARANTES DEL 4% 900068796 INFOTIC S.A 0190 RECURSOS ICETEX Base Orig: 0.00 Base Imp: 652,165,854.00 Trans. de Entrega No. 111654 - CT No. 2337. Pago de factura FVE 2337- por concepto de servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el icetex. en la ciudad	0.00	26,086,634.00
2503100111	RETENCION ICA SERVICIOS 8.66*1000 900068796 INFOTIC S.A 0190 RECURSOS ICETEX Base Orig: 0.00 Base Imp: 652,165,854.00 Trans. de Entrega No. 111654 - CT No. 2337. Pago de factura FVE 2337- por concepto de servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el icetex. en la ciudad	0.00	5,647,756.00
25110501	ADQUISICIÓN DE BIENES Y SERVICIOS 900068796 INFOTIC S.A 0190 RECURSOS ICETEX CT VOT 2337 1 27/01/2026 27/01/2026 DSA: Trans. de Entrega No. 111654 - CT No. 2337. Pago de factura FVE 2337- por concepto de servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el icetex. en la ciudad	0.00	725,756,249.00
Realizado por: CTORRIJOS CRISTIAN DAVID TORRIJOS 02/02/2026 16:26:16		Aprobado por: Fecha:	

899999035

Fecha de emisión: 31/01/2026

Contabilidad: ICETEX NORMA INTERNACIONAL
Concepto comprobante: COMPROBANTE DE CAUSACION

CUENTA	DESCRIPCIÓN	DÉBITOS	CRÉDITOS
	TOTALES:	776,077,366.00	776,077,366.00

Realizado por: CTORRIJOS
CRISTIAN DAVID TORRIJOS
02/02/2026 15:22:10

Aprobado por:
Fecha:



7020-1 Actividad Principal 8.66% 6202 Otras Actividades 6.9%
8299 Actividad Secundaria 9.66% 6209 Otras Actividades 9.66%
Responsables de IVA - No Somos Autorretenedores
Sociedad de economía mixta con participación del 51% de Infanzonales
Gran contribuyente de Industria y Comercio Secretaría de hacienda de Bogotá según la
Resolución DDI 029334 de 31 de octubre de 2025

INFOTIC S.A

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

Tel: 7466000 Fax: 7466000

Bogotá, D.C.

Factura Electrónica De Venta

FVE-2337



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: 1/23/2026 12:56:56 PM
Forma de pago: CREDITO 30 DIAS
Moneda: COP
Fecha vcto: 2/23/2026 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 DICIEMBRE DE 2025. SERVICIOS OPERACIÓN MES DE DICIEMBRE 2025 (INCLUIDO IVA): \$838.241.120 (-) DESCUENTOS INCLUIDO IVA: CONECTIVIDAD Y RED DE COMUNICACIONES: -\$20.537.912 CENTRO DE DATOS: -\$41.028.197 SERVICIO DE SEGURIDAD: \$597.644 TOTAL DESCUENTO CON IVA: -\$62.163.754 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	\$ 652,165,854.00	\$652,165,854.00	\$ 776,077,366.00

IMPUESTOS	BASE	TASA	TOTAL
IVA	\$652,165,854	19 %	\$123,911,512

SETECIENTOS SETENTA Y SEIS MILLONES SETENTA Y SIETE MIL TRESCIENTOS SESENTA Y SEIS PESOS M/CTE *****

Notas

facturacion_electronica@icetex.gov.co

RESPONSABLE: MONICA MARIA VILLAMIZAR SANCHEZ

VALOR BRUTO	\$652,165,854.00
DESCUENTO	\$0.00
SUBTOTAL	\$652,165,854.00
IVA	\$123,911,512.00
TOTAL FACTURA	\$776,077,366.00

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 4ffa6be56cadea8c67c8391de9797c9e300f2182d7e6418310e9635016867b7461e31e8177dea5d88ea2d94d9326b50c

FIRMA DIGITAL:

hRg4GVgUt3+3mTTLrtiVWqyDEf5kww4JqOgfl3Z7DgV3lCL5Ojjez4thaB0a2yDtbHPEAGl2xhxhda9MciDpHnOR6olP1YFPYiUTy+MgmjxjtAiO5OVh0oUJRT
ewFMSSbBef8lVeF+4cu3FqFXTnrLMxJo+NZy9RjMlaNyEKqqfoF5y6R9G76Cmng/V42DoflXjhZ8hCOLGSp3ZSCdQXOHQt/tHVUWWMMmo5oF9vMofO5Fr206Ubd5zKo
MJO/q3wC377os+ocpP6ZlShq9F/og4Hh9uD9Q3AR6AnSWznrcclcc+fd38T0h7ozWfxkl64a8cUxjlmvYdWCUv8XbtlQQ==

FECHA DIAN: 2026-01-23 13:01:36-05:00

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

DATOS GENERALES DEL APORTANTE								
Identificación	dv	Razon Social	Clase Aportante	Sucursal Principal	Dirección	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
2025-11	2025-12	1979313796	9495769349	E	2025/12/23	2025/12/03	BANCO DE BOGOTA	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	

**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 tres (03) de diciembre de 2025, para los aportes correspondientes a salud del mes de diciembre de 2025 y para pensión, riesgos laborales y aportes parafiscales del mes de noviembre de 2025 mediante la planilla No. 9495769349, 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 y el artículo 114-1 del ET, 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 cuatro (04) días del mes de diciembre 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
2025-12	2026-01	2054028739	9497081997	E	2026/01/26	2026/01/02	BANCO DE BOGOTA	0	\$4,743,600

RESUMEN DE PAGO									
RIESGO	CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES	VALOR A PAGAR	
AFP (ADMINISTRADORAS: 2)				3	\$3,149,900	\$0	\$0	\$3,149,900	
COLPENSIONES	25-14	900,336,004	7	2	\$2,594,600	\$0	\$0	\$2,594,600	
PORVENIR	230301	800,224,808	8	1	\$555,300	\$0	\$0	\$555,300	
ARL (ADMINISTRADORAS: 1)				3	\$94,700	\$0	\$0	\$94,700	
ARL SURA	14-11	890,903,790	5	3	\$94,700	\$0	\$0	\$94,700	
CCF (ADMINISTRADORAS: 1)				3	\$749,500	\$0	\$0	\$749,500	
COMFACUNDI	CCF26	860,045,904	7	3	\$749,500	\$0	\$0	\$749,500	
EPS (ADMINISTRADORAS: 2)				3	\$749,500	\$0	\$0	\$749,500	
NUEVA E.P.S.	EPS037	900,156,264	2	1	\$231,700	\$0	\$0	\$231,700	
SANITAS	EPS005	800,251,440	6	2	\$517,800	\$0	\$0	\$517,800	
TOTAL				3	\$4,743,600	\$0	\$0	\$4,743,600	

**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

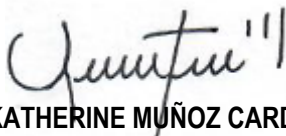
1. A la fecha se encuentra en curso mi examen sobre los estados financieros de la Compañía por el año que terminará el 31 de diciembre de 2025.
2. El último pago se realizó el día dos (02) de enero de 2026, para los aportes correspondientes a salud del mes de enero de 2025 y para pensión, riesgos laborales y aportes parafiscales del mes de diciembre de 2025 mediante la planilla No. 9497081997, 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 y el artículo 114-1 del ET, 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 seis (06) días del mes de enero de 2026, 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.**

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**

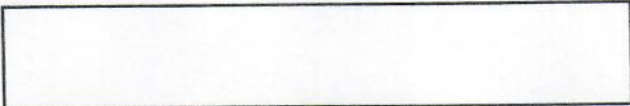
Identificación Plástica S.A. 180942/0119

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



INFORME DE ACTIVIDADES DEL CONTRATO

**CONTRATO NUMERO
2022-0792**

Diciembre 01 al 31 de 2025

versión	Observaciones	Fecha	Responsable
1.0	Versión Inicial	05/01/2026	Francisco Javier Pulido

Tabla de contenido

1.	INTRODUCCIÓN	9
2.	OBJETIVO DEL INFORME	9
3.	ALCANCE	10
4.	AVANCE TÉCNICO	11
4.1.	Conectividad y Red de Comunicaciones	11
4.1.1.	Canales instalados en el mes y entregables	13
4.1.2.	Despliegue de direcciones IP V6	14
4.1.3.	Implementación canales SDWAN	15
4.1.4.	Recomendaciones	16
4.2.	Centro de Datos	17
4.2.1.	Centro de Datos Principal	17
4.2.1.1.	Aplicaciones	17
4.2.1.2.	Bases de Datos	20
4.2.1.3.	Sitio Web	23
4.2.2.	Centro de Datos Alterno	26
4.2.2.1.	Hosting Virtual (IaaS)	26
4.2.2.2.	DataGuard Bases de Datos Megacenter	28
4.2.2.3.	Servicios de Housing – Datacenter Alterno	29
4.2.2.4.	Servicios de DRP	30
4.3.	Seguridad informática	30
4.3.1.	Plataformas Administradas	33
4.3.1.1.	FortiGate Triara	34
4.3.1.2.	FortiGate Aguas	37
4.3.1.3.	FortiGate Medellín	38
4.3.1.4.	FortiWeb 2000F	39
4.3.1.5.	FortiWeb 2000E	39
4.3.1.6.	FortiWebCloud DRP	40
4.3.1.7.	FortiSandBox	40
4.3.1.8.	FortiSIEM	41

4.3.1.9. Sophos EndPoint	41
4.3.2. Recomendaciones de Seguridad para el ICETEX.	42
4.3.3. Servicio de centro de Operaciones de Seguridad (SOC)	44
4.3.3.1. Alertas o Incidentes de Seguridad Detectados	45
4.3.3.1.1. Categoría Seguridad	45
4.3.3.1.2. Categoría Disponibilidad	47
4.3.3.1.3. Amenazas de Ciberseguridad	48
4.3.3.2. Threat Hunting	51
4.3.3.3. Análisis de Marca OSINT	52
4.3.4. Análisis de Vulnerabilidades ICETEX	52
4.3.4.1. Gestión de Vulnerabilidades	54
4.3.4.2. Actividades de PENTEST	55
4.3.4.3. Actividades de PENTEST WEB	55
4.3.4.4. Actividades de PENTEST SERVIDORES	56
4.3.5. Reporte De IPS	58
4.3.6. Arquitectura de Seguridad	58
4.3.7. Plan de Continuidad	59
4.4. Servicios de nube	59
5. GESTION DE LA EJECUCIÓN CONTRACTUAL	60
6. GESTION PRESUPUESTAL	61
7. GESTION ADMINISTRATIVA	63
7.1. Profesionales	63
8. SERVICIO DE COLABORACIÓN	64
9. GESTION DE RIESGOS Y PROBLEMAS	65
10. INDICADORES CLAVE DE DESEMPEÑO	67
10.1. ANS por Disponibilidad de canales de comunicaciones	67
10.1.1. Canal de Replicación (Triara – Megacenter)	70
10.2. ANS por Disponibilidad de servidores	70
10.2.1. Disponibilidad TRIARA para los servicios de página web	72
10.2.2. Análisis componente Liferay Producción	77

10.2.3. Backup Servidores Triara	78
11. CONTROL DE CAMBIOS	80
12. PLAN DE TRABAJO DE LOS PROXIMOS MESES	81
13. PLAN DE ENTREGA	82
14. RECOMENDACIONES DEL CONTRATISTA AL ICETEX	82
14.1. Networking	82
14.2. Aplicaciones	83
14.3. Seguridad	84
14.4. Bases De Datos	85
14.5. Integrador De Nube	85
15. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC	85
15.1. Aumento de la capacidad de Ancho de Banda en algunas de las sedes de la Entidad	86
15.2. Una capacitación al año de seguridad Informática y servicios conexos	86
15.3. TB de capacidad de almacenamiento	86
15.4. "Wifi" para la gente en 19 sedes	87
16. CONCLUSIONES	88
17. ANEXOS	89

TABLA 1 CASOS ATENDIDOS NETWORKING COMPARATIVO MES ANTERIOR	13
TABLA 2 LISTADO DE DIRECCIONES IP V6 ASIGNADAS A LAS OFICINAS	15
TABLA 3 VIGENCIA DE LOS CERTIFICADOS DIGITALES.....	18
TABLA 4 INVENTARIO PRINCIPALES SERVIDORES PRODUCCIÓN	19
TABLA 5 ESTADO BD ORACLE	20
TABLA 6 CRECIMIENTO DE LAS BASES DE DATOS EN LOS ÚLTIMOS 7 MESES	23
TABLA 7 TOP 10 PORTALES MÁS UTILIZADOS.....	25
TABLA 8 ESTADO LICENCIAMIENTO PORTAL WEB ICETEX	26
TABLA 9 SERVICIOS REPLICADOS – DATACENTER MEGACENTER	27
TABLA 10 TOP 5 MÁQUINAS MAYOR TASA DE TRANSFERENCIA	27
TABLA 11 TOP 4 MÁQUINAS MENOR TASA DE TRANSFERENCIA	27
TABLA 12 DISPONIBILIDAD DE SERVICIOS DE HOUSING – DATA CENTER ALTERNO	30
TABLA 13 DETALLE PLATAFORMAS SEGURIDAD ADMINISTRADAS INFOTIC	33
TABLA 14 LICENCIAMIENTO FORTIGATE	34
TABLA 15 LICENCIAMIENTO FORTIWEB	39
TABLA 16 CONFIGURACIÓN FORTISANDBOX 1000D.....	41
TABLA 17 RECOMENDACIONES DE SEGURIDAD	44
TABLA 18 COMPARATIVO – INDICADORES DE COMPROMISO	45
TABLA 19 COMPARATIVO ALERTAS DE SEGURIDAD	46
TABLA 20 RESULTADO ESCANEOS VULNERABILIDADES URL'S	55
TABLA 21 RESULTADO ESCANEOS VULNERABILIDADES SERVIDORES	57
TABLA 22 PLAN DE TRABAJO-ARQUITECTURA DE SEGURIDAD.....	58
TABLA 23 EJECUCIÓN PRESUPUESTAL.....	63
TABLA 24 PERFILES Y ACTIVIDADES.....	64
TABLA 25 GRUPO ADMINISTRATIVO	64
TABLA 26 DISTRIBUCIÓN MÓDULOS DE VIDEOCONFERENCIA POR SEDE	64
TABLA 27 NIVEL DE RIESGO	66
TABLA 28 GRADO DE RIESGO	67
TABLA 29 DISPONIBILIDAD DE CANALES.....	69
TABLA 30 DISPONIBILIDAD CANALES “INTERNET PARA LA GENTE”	70
TABLA 31 CÓDIGOS RELACIONADOS DISPONIBILIDAD SERVICIOS EN HOUSING – DATACENTER PRINCIPAL.....	71
TABLA 32 DISPOSITIVOS EN HOUSING – DATACENTER PRINCIPAL.....	72
TABLA 33 DISTRIBUCIÓN TRIMESTRAL DE ACCESO POR USUARIOS	73
TABLA 34 CINTAS BACKUPS ICETEX.....	78
TABLA 35 CONTROLES DE CAMBIO DICIEMBRE	81
TABLA 36 PLANES DE TRABAJO	82
TABLA 37 CAPACIDADES DE ALMACENAMIENTO CONTRATADO	86
TABLA 38 CAPACIDADES DE ALMACENAMIENTO APROVISIONADO	87
TABLA 39 PRUEBAS DE RESTAURACIONES DE BACKUPS DE DICIEMBRE	87
TABLA 40 WIFI PARA LA GENTE INSTALADOS	87
TABLA 41 WIFI PARA LA GENTE PENDIENTES.....	88
TABLA 42 ANEXOS	91

ILUSTRACIÓN 1 TOPOLOGÍA APROBADA SDWAN	15
ILUSTRACIÓN 2 PLAN DE TRABAJO REIMPLEMENTACIÓN SDWAN	16
ILUSTRACIÓN 3 DISPONIBILIDAD DEL CLUSTER	21
ILUSTRACIÓN 4 DISPONIBILIDAD DE LAS BASES DE DATOS PRINCIPALES ICTXCYC Y APOTEOSYS.....	21
ILUSTRACIÓN 5 CASOS DEL PROYECTO GESTIONADOS ARANDA BASES DE DATOS	22
ILUSTRACIÓN 6 UPTIME: PORTAL WEB WEB.ICETEX.GOV.CO [99,823%]	24
ILUSTRACIÓN 7 TRÁFICO GENERAL DE LOS PORTALES	25
ILUSTRACIÓN 8 REPORTES DE REPLICACIÓN SRM A SITIO ALTERNO – DICIEMBRE2025	26
ILUSTRACIÓN 9 FECHAS CON MAYOR REPLICACIÓN	28
ILUSTRACIÓN 10 EVIDENCIA DATAGUARD REPLICADO A MEGACENTER BD.....	29
ILUSTRACIÓN 11 DIAGRAMA DE LA ARQUITECTURA DE SEGURIDAD	30
ILUSTRACIÓN 12 TOPOLOGÍA DE WAF CLOUD USADO EN PORTALES DE MEDELLÍN	31
ILUSTRACIÓN 13 CONSUMO CANAL MPLS - PROMEDIO 1200G [INR0185 CLARO(MPLS_DC)].....	34
ILUSTRACIÓN 14 CONSUMO CANAL INTERNET SEDES - PROMEDIO 1100 GB WAN-SEDES-ICETEX [INR0264 (INTE_SEDES_ICTX)]	35
ILUSTRACIÓN 15 CONSUMO CANAL INTERNET DATA CENTER- INTERNET DATACENTER [INTERNET_DC_INR0000320 (INET_CLARO)]	35
ILUSTRACIÓN 16 FILTRADO – WEB – (FORTIGATE – TRIARA).....	36
ILUSTRACIÓN 17 INSPECCIÓN – SSL – (FORTIGATE – TRIARA).....	36
ILUSTRACIÓN 18 ANTIVIRUS Y ANTIMALWARE – PERIMETRAL (FORTIGATE – TRIARA).....	37
ILUSTRACIÓN 19 CONSUMO CANAL MPLS AGUAS - PROMEDIO 800 GB	37
ILUSTRACIÓN 20 FILTRADO-WEB-(FORTIGATE-AGUAS).....	38
ILUSTRACIÓN 21 INSPECCIÓN-SSL-(FORTIGATE-AGUAS)	38
ILUSTRACIÓN 22 ANTIVIRUS Y ANTIMALWARE-PERIMETRAL-(FORTIGATE-AGUAS).....	38
ILUSTRACIÓN 23 CONSUMO CANAL MPLS MEDELLÍN	39
ILUSTRACIÓN 24 TRÁFICO GENERAL DE LOS PORTALES	40
ILUSTRACIÓN 25 TRÁFICO GENERAL DE LOS PORTALES	40
ILUSTRACIÓN 26 DESEMPEÑO POR PROCESOS.....	41
ILUSTRACIÓN 27 ESTADO SEGURIDAD SOPHOS	41
ILUSTRACIÓN 28 TOTAL DE ALERTAS DE SEGURIDAD	46
ILUSTRACIÓN 29 TOP 5 DE ALERTAS DE SEGURIDAD ALTAS.....	46
ILUSTRACIÓN 30 TOP 5 DE ALERTAS DE SEGURIDAD MEDIAS.....	47
ILUSTRACIÓN 31 TOP 10 DE ALERTAS DE DISPONIBILIDAD ALTAS	47
ILUSTRACIÓN 32 ATAQUES IPS PERMITIDOS	48
ILUSTRACIÓN 33 ATAQUES IPS DENEGADOS	49
ILUSTRACIÓN 34 PUERTOS ENTRANTES DE PÚBLICO A PRIVADO (PERMITIDOS)	49
ILUSTRACIÓN 35 TOP DE ACCESOS FALLIDOS PLATAFORMA WINDOWS	50
ILUSTRACIÓN 36 CUENTAS BLOQUEADOS	51
ILUSTRACIÓN 37 INCIDENTES POR TIPO DE AMENAZA	52
ILUSTRACIÓN 38 ESTADO DE REMEDIACIÓN COMPLETA DE VULNERABILIDADES.....	53
ILUSTRACIÓN 39 ESTADO DE REMEDIACIÓN PARCIAL DE VULNERABILIDADES.	54
ILUSTRACIÓN 40 BALANCE FINAL DE GESTIÓN DE VULNERABILIDADES.	54
ILUSTRACIÓN 41 SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO	59
ILUSTRACIÓN 42 MATRIZ DE RIESGOS	66
ILUSTRACIÓN 43 UPTIME – PORTAL WEB WEB.ICETEX.GOV.CO	72
ILUSTRACIÓN 44 MÉTRICA DE VISITANTES PORTAL WEB WEB.ICETEX.GOV.CO	73

ILUSTRACIÓN 45 MÉTRICA ADQUISICIÓN USUARIOS PORTAL WEB WEB.ICETEX.GOV.CO	74
ILUSTRACIÓN 46 MÉTRICA DE USUARIO POR PAÍS - PORTAL WEB WEB.ICETEX.GOV.CO.....	74
ILUSTRACIÓN 47 MÉTRICA DE CIUDADES DE COLOMBIA- PORTAL WEB WEB.ICETEX.GOV.CO.....	75
ILUSTRACIÓN 48 NODO 1 CPU	76
ILUSTRACIÓN 49 NODO 1 MEMORIA	77
ILUSTRACIÓN 50 NODO 1 ALMACENAMIENTO.....	77
ILUSTRACIÓN 51 EVIDENCIA BACKUP SERVIDORES RESUMEN GENERAL BACKUPS.....	79
ILUSTRACIÓN 52 EVIDENCIA BACKUP SERVIDORES RESUMEN BACKUPS Y SU ESTADO	79
ILUSTRACIÓN 53 HISTÓRICO CONSOLIDADO USO DE DISCOS SERVIDOR ICTXSRVNETCOR01.....	84

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 diciembre 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 92 % que representa los 33 meses que lleva dentro de la fase de Operación el proyecto.

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

➤ **Conectividad y red de comunicaciones**

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

➤ **Centro de datos**

El informe presenta el estado de los dos (2) Centros de Datos que contempla el proyecto ICETEX: un (01) centro de cómputo principal (TRIARA) y un (01) centro de cómputo secundario o 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 13 solicitudes, con respecto al mes anterior hubo un incremento de 5 casos ya que se atendieron 8 solicitudes en el mes anterior.

[Registro Aranda Diciembre 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.

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**.

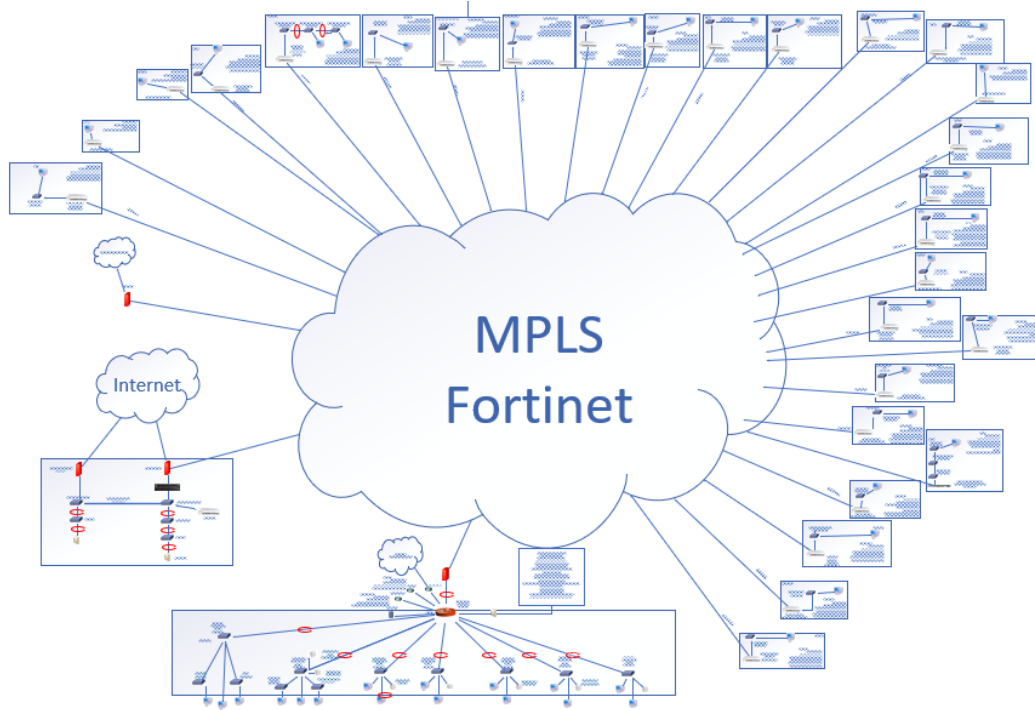
La gestión de dispositivos de red es el proceso mediante el cual se gestionan y controlan los dispositivos de red, desde computadoras, servidores y teléfonos móviles hasta conmutadores y máquinas virtuales.

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

[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

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>

A fin de garantizar un adecuado funcionamiento, se ha previsto que el equipo de especialistas de seguridad procederá a configurar reglas 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.

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 Diciembre 2025.pdf](#)

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 Enero 2026.

Los casos atendidos durante el mes están disponibles en el siguiente enlace:
[Registro Aranda Diciembre 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
Octubre	8
Noviembre	16
Diciembre	13

Tabla 1 Casos atendidos Networking comparativo mes anterior

4.1.2. Despliegue de direcciones IP V6

Se efectuó el despliegue de dirección IPv6 sede y se adelantaron pruebas de navegación empleando un PC de un funcionario en la sede respectiva. A la fecha las sedes realizadas son:

Consecutivo	Sede	Pruebas seguridad	Horario	Observación
1	Aguas	27/08/2025	0:00	Realizadas
2	Chapinero Bogotá	9/09/2025	0:00	Realizadas
3	Cali Prueba 2	29/09/2025	0:00	Realizadas
4	Medellín	2/10/2025	0:00	Realizadas
5	Buenaventura	3/10/2025	0:00	Realizadas
6	Quibdó	7/10/2025	0:00	Realizadas
7	Riohacha	9/10/2025	0:00	Realizadas
8	Montería	10/10/2025	0:00	Realizadas
9	Bucaramanga	16/10/2025	0:00	Realizadas
10	Popayán	17/10/2025	0:00	Realizadas
11	Pereira	20/10/2025	0:00	Realizadas
12	Valledupar	21/10/2025	0:00	Realizadas
13	Santa Marta	23/10/2025	0:00	Realizadas
14	Barranquilla	24/10/2025	0:00	Realizadas
15	Sincedejo	28/10/2025	0:00	Realizadas
16	Tumaco	30/10/2025	0:00	Realizadas
17	Cúcuta	4/11/2025	0:00	Realizadas
18	Villavicencio	6/11/2025	0:00	Realizadas
19	Tunja	7/11/2025	0:00	Realizadas
20	Cartagena	11/11/2025	0:00	Realizadas
21	Armenia	13/11/2025	0:00	Realizadas
22	Arauca	14/11/2025	0:00	Realizadas
23	Pasto	18/11/2025	0:00	Realizadas
24	Ibagué	20/11/2025	0:00	Realizadas
25	Apartado	21/11/2025	0:00	Realizadas
26	Mocoa	24/11/2025	0:00	Realizadas
27	Yopal	26/11/2025	0:00	Realizadas
28	Manizales	1/12/2025	0:00	Realizadas
29	Neiva	1/12/2025	0:00	Realizadas
30	Ocaña	3/12/2025	0:00	No realizar pruebas de ipv6
31	Puerto Inírida	3/12/2025	0:00	No realizar pruebas de ipv6
32	Puerto Carreño	3/12/2025	0:00	No realizar pruebas de ipv6
33	Florencia	5/12/2025	0:00	No realizar pruebas de ipv6

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

Consecutivo	Sede	Pruebas seguridad	Horario	Observación
34	Leticia	5/12/2025	0:00	No realizar pruebas de ipv6
35	Sincelejo	5/12/2025	0:00	Realizadas
36	San Andrés	No se realizará	0:00	No realizar pruebas de ipv6
37	Ángel Bogotá	Pendiente	0:00	Realizadas

Tabla 2 Listado de direcciones IP V6 asignadas a las oficinas

4.1.3. Implementación canales SDWAN

La topología, aprobada, para la solución de SD-WAN en la que se traslada el punto central a Triara es la siguiente:

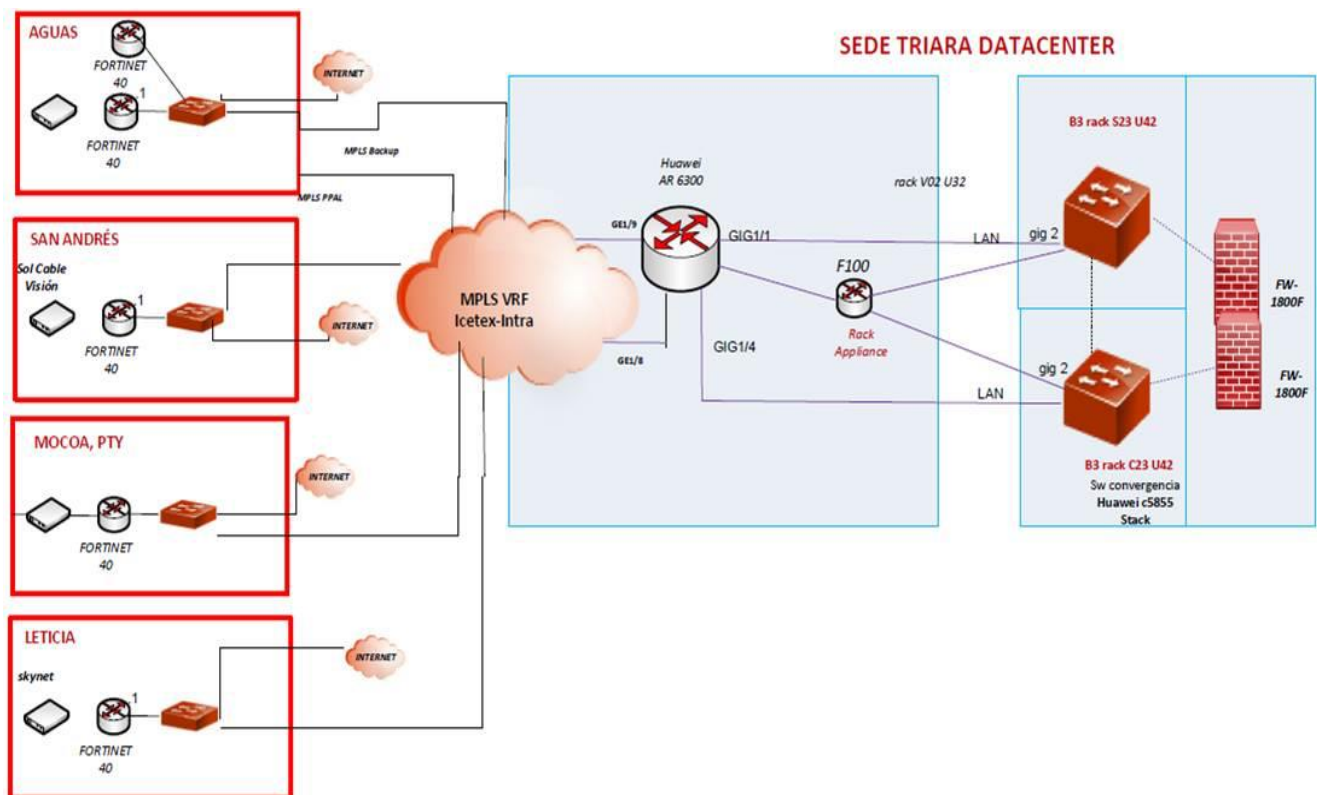


Ilustración 1 Topología aprobada SDWAN

En este escenario se conserva la topología de las 4 sedes:

- Aguas
- San Andrés
- Mocoa

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

- Leticia

A continuación, se presenta el estado actual del plan de trabajo:

Gerente del proyecto:		Arley Vargas					
Inicio del proyecto:		23-oct-25					
Nombre del proyecto:		INFOTIC					
		Semana Inicio:					
#	Actividad	Asignado a	Inicio	Fin	Duración	Estado	% Ejecutado
1	KickOff con Cliente	Claro - Infotíc	23-oct-25	23-oct-25	1	Terminada	100%
2	Adquisición de Equipos	Proyectos - Compras	23-oct-25	28-oct-25	4	Terminada	100%
3	Levantamiento de información Técnica	Claro - Infotíc	28-oct-25	28-oct-25	1	Terminada	100%
4	Elaboración Plan técnico / Sow	Líder Técnico	28-oct-25	12-nov-25	12	Terminada	100%
5	Presentación Plan técnico/ Sow	Líder Técnico	24-nov-25	24-nov-25	1	Terminada	100%
6	Solicitud espacio y carga	Claro	4-dic-25	15-dic-25	8	Terminada	50%
7	Instalación Equipos Triara	Claro	15-dic-25	19-dic-25	5	Terminada	0%
8	Cxc en Triara	Claro	22-dic-25	23-dic-25	2	Asiganda	0%
9	Definición de estrategia plan de migración	Claro - Infotíc	29-dic-25	30-dic-25	2	En curso	50%
10	Pruebas finales y estabilización Triara	Claro	8-ene-26	12-ene-26	3	Asiganda	0%
11	Instalación y pruebas sedes remotas	Claro	15-ene-26	19-ene-26	3	Asiganda	0%
12	Pruebas finales y estabilización	Claro	22-ene-26	26-ene-26	3	Asiganda	0%
13	Paso a operación	Claro	29-ene-26	30-ene-26	2	Asiganda	0%
14	Cierre	Gerente de Proyecto	31-ene-26	31-ene-26	0	Asiganda	0%

Ilustración 2 Plan de trabajo reimplementación SDWAN

El cronograma avanza y se espera entregar los canales configurados el próximo 31 de enero de 2026.

4.1.4. Recomendaciones

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: se debe notificar a ICETEX que actualmente no hay disponibilidad de equipos de red 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.

4.2. Centro de Datos

4.2.1. Centro de Datos Principal

4.2.1.1. Aplicaciones

Durante el mes de diciembre de 2025, se atendieron un total de un total de 13 solicitudes, todas documentadas con sus respectivas evidencias. A continuación, se presenta el detalle de estas:

Las acciones desarrolladas se concentraron principalmente en tres líneas de trabajo:

- **Actualizaciones y despliegues tecnológicos**
 - Actualización de componentes Backend y Frontend del Portal Transaccional e interfaces críticas (Cambios 1225 y 1229).
 - Despliegue de aplicaciones y servicios en servidores específicos, incluyendo entornos preproductivos y de producción (ej. ICTXSRVAPPMIX1).
 - Instalación de RabbitMQ en infraestructura corporativa para servicios de mensajería.
- **Soporte y continuidad operativa**
 - Atención y resolución de incidentes de caída de servicio en la plataforma C&CTEX, asegurando restablecimiento ágil y estabilidad.
 - Gestión de fallas en aplicaciones institucionales, mitigando impactos operativos.
- **Ajustes funcionales y mejoras puntuales**
 - Modificación de enlaces y rutas de acceso a servicios como Gestor de Servicios, Administrador de requerimientos y servicios web relacionados.
 - Actualización de configuraciones asociadas a integración con pasarela de pagos Kushki.

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 1236 y 1237 con el fin de proceder a efectuar las actualizaciones respectivas.

En cuanto al desempeño de los servidores, se sigue identificado que 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 del 96% 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.

El resto de los servidores administrados 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 Diciembre2025.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.

Además, con base a los registros de los últimos tres meses (octubre a diciembre de 2025), el consumo de memoria RAM y CPU en los servidores administrados en producción se ha mantenido dentro de los parámetros normales y controlados, por lo que en general los niveles registrados no representan riesgo de saturación ni alertas críticas.

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, en donde destacan vencimiento de dos certificados en el mes de diciembre:

Sitio Web	URL	Fecha creación	Fecha revocación	Tipo SSL Asignado
Pasareladepagos	https://webhook.icetex.gov.co/swagger/index.html	16/10/2024	25/10/2026	RapidSSL RSA CA
Web Service RNEC	https://rnc.icetex.gov.co/swagger/index.html	18/11/2025	18/11/2026	*.icetex.gov.co
Colección de Aplicaciones	https://aplicaciones.icetex.gov.co/	18/12/2025	18/12/2026	Secure Site Pro EV SSL
Portal Institucional	https://web.icetex.gov.co	18/12/2025	18/12/2026	Secure Site Pro EV SSL
Portal DECEVAL - Pagaré	pagare.icetex.gov.co	18/12/2025	18/12/2026	Secure Site Pro SSL
Portal C&CETEX	https://www.icetex.gov.co	18/12/2025	18/12/2026	Secure Site Pro EV SSL
Colección de Web Services Internos	https://appwebservices.icetex.gov.co	18/12/2025	18/12/2026	Secure Site Pro SSL
Wildcard	*.icetex.gov.co	18/11/2025	18/11/2026	*.icetex.gov.co

Tabla 3 Vigencia de los certificados digitales

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 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 CustomWindowsSe rvviceNovacion	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 al día.

En el informe de los especialistas de soluciones, se presenta un resumen detallado de los hallazgos por

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

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	4,996
ICETEX	11.0.2.0.4	207
APLICATI	11.0.2.0.4	244
APOTEOSY	11.0.2.0.4	481
VIGIAPRD	19.16.0.0	188
LIFERAY LIFERAYPDB	19.16.0.0	8.20
LANDICTX	19.16.0.0	584
SGDEA	19.16.0.0	147

Tabla 5 Estado BD Oracle

Resultado del proceso de administración se destacan las siguientes actividades:

- Se continuo con la replicación permanente de las BD Oracle al Datacenter alternativo de acuerdo con las políticas establecidas, utilizando el Oracle Active DataGuard el cual garantiza una alta disponibilidad, protección de datos y recuperación ante desastres.
- 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 archive log, Backups incrementales y Backups completos o full.
- Se valido la replicación de las bases de datos del Datacenter Bogotá a centro alternativo 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 diciembre 2025 fue del 100% como se evidencia en la siguiente ilustración:

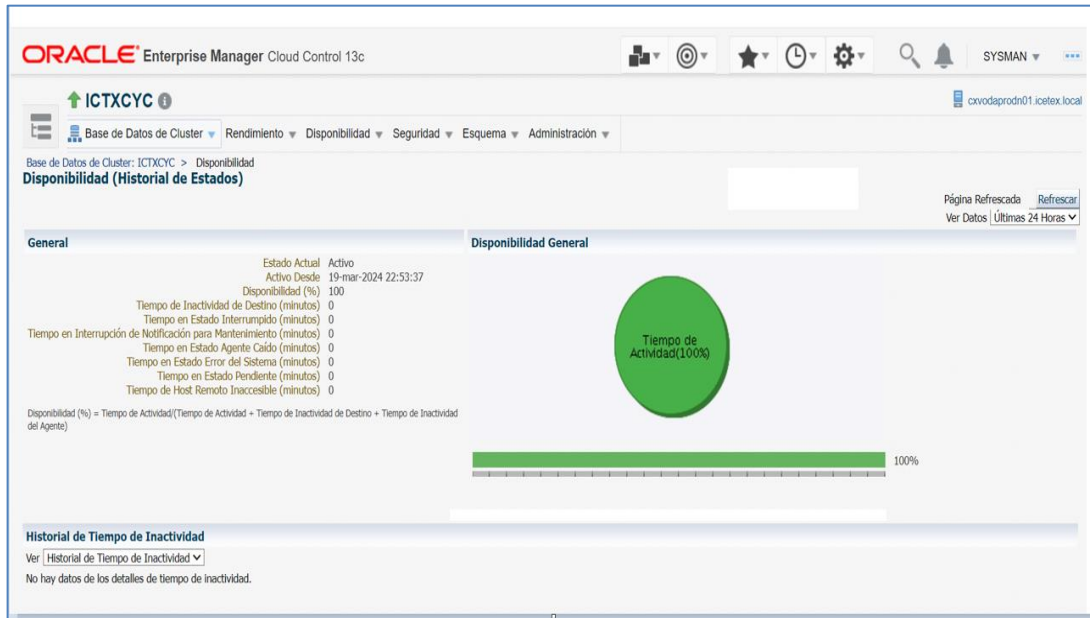


Ilustración 3 Disponibilidad del cluster

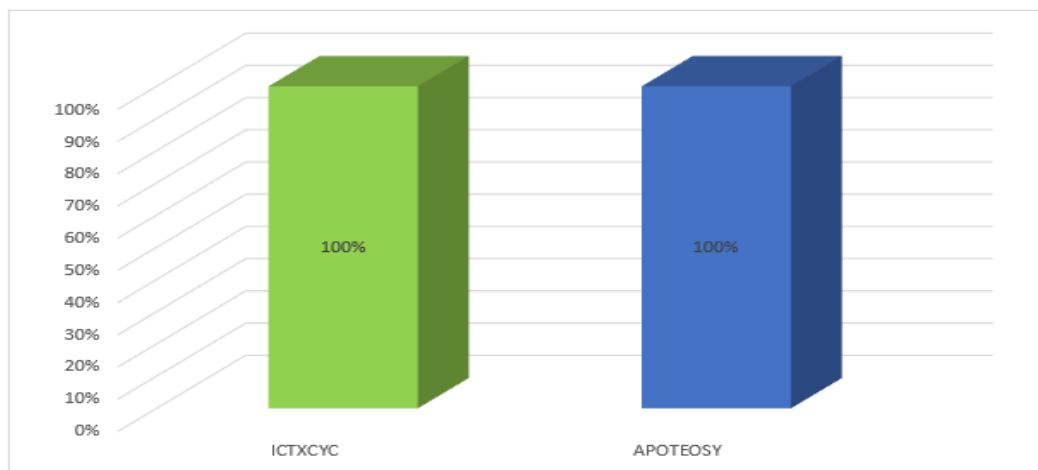


Ilustración 4 Disponibilidad de las Bases de Datos principales ICTXCYC y APOTEOSY

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.

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 en el mes de agosto y hemos apoyado en las tareas que se adelantan con respecto a CICETEX.

➤ Casos del proyecto Gestionados por Bases de datos:



Ilustración 5 Casos del proyecto Gestionados Aranda Bases de datos

Desde Bases de datos se tienen las siguientes recomendaciones:

- Se debe aumentar los espacios de Megacenter del DataGuard por la apertura de las bases de datos para consulta.
- Sólo quedan 120G disponibles, recurso que podría alcanzar sólo para un mes de actividad.
- Se deben crear las tareas y cronologías para migrar las bases de datos que se encuentran en versión 11G fuera de soporte a la versión 19C o mayor.

Almacenamiento:

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

BASE DE DATOS	"MAYO 2025"	"JUNIO 2025"	"JULIO 2025"	"AGO 2025"	"SEPT 2025"	"OCT-2025"	"NOV 2025"	"DICIEMBRE 2025"
ICTXCYC	4,590	4,641	4,683	4,766	4,774	4,923	4,925	4,996
ICETEX	202	203	206	206	206	206	207	207
APLICATI	243	243	243	243	243	243	243	244
APOTEOSY	458	459	460	460	480	481	481	481
VIGIAPRD	133	137	143	143	166	175	178	188
LIFERAY LIFERAYPDB	8.20	8	8	8	8	8	8	8
LANDICTX	529	529	529	529	529	529	554	584
SGDEA	112	120	124	124	136	140	143	147
TOTAL==>	6,274.90	6,340.20	6,396.00	6,479.00	6,542.00	6,705.00	6,738.56	6,855.06

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.

Virus:

- Se iniciaron las acciones para el cambio del antivirus en las bases de datos.

Replicación

- Durante el mes de diciembre de 2025 se continuo con la replicación permanente de las BD Oracle al Datacenter alternativo 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.

4.2.1.3. Sitio Web

Durante el mes de diciembre se continuo con el monitoreo permanente a los portales sobre los que opera el ICETEX, manteniendo, las alertas y reportes a tiempo en caso de que se presentara algún evento que pudiera ocasionar una interrupción en la prestación de los servicios que se ofrecen a través de los portales, este informe se encuentra detallado en el documento [Informe Mensual InfoTIC Seguridad Diciembre2025.pdf](#)

En cuanto a la disponibilidad del portal web de la entidad se presentan unos uptime superiores al 99.823% como se evidencia en la siguiente gráfica:

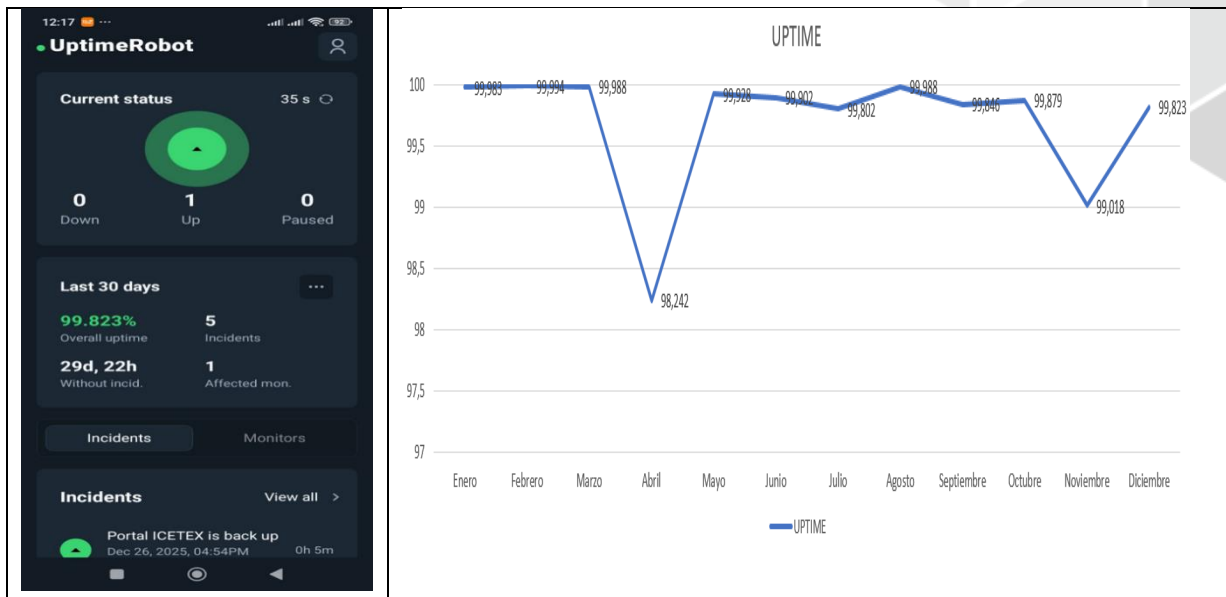


Ilustración 6 UPTIME: Portal WEB web.icetex.gov.co [99,823%]

En relación con los requerimientos, aumentó en un 100%, aumentando a 6 en el presente periodo, debido a que se brindó apoyo a la OCM.

Los incidentes disminuyeron en un 28,57%, los casos reportados corresponden a caídas del servicio Elasticsearch, se reporta 1 caso escalado por error.

En cuanto a los casos de gestión de cambios disminuyeron en un 100%, debido a que no se efectuaron en el transcurso del mes de diciembre.

Por último, los casos SD Claro aumentaron en un 100%, los casos que se reportaron corresponden a los acompañamientos con los especialistas de Claro para cumplir con el plan de reinicios controlados solicitados por el ICETEX, además de redireccionamientos de URLs por parte de la OCM.

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.

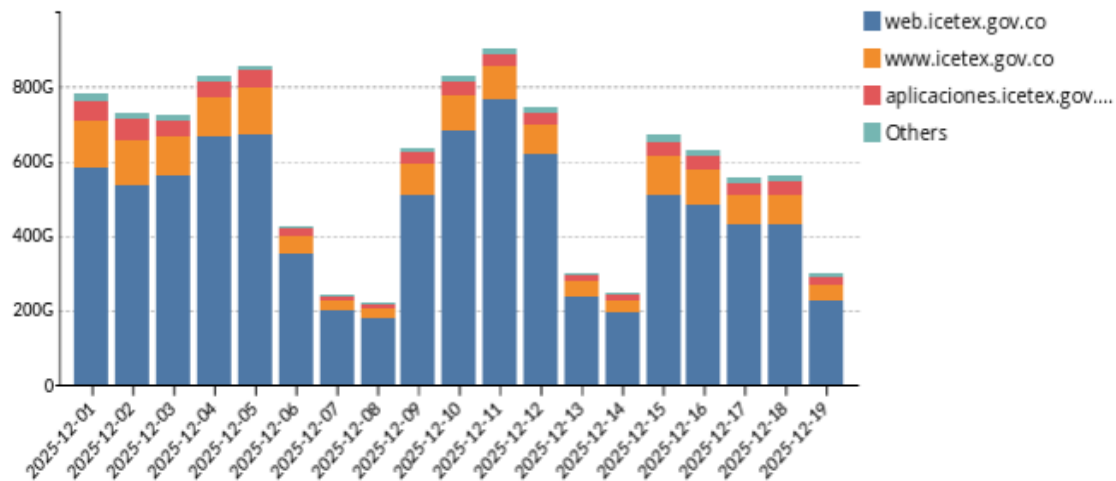


Ilustración 7 Tráfico General De Los Portales

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	529.66 GB	8.05 TB
2	www.icetex.gov.co	38.53 GB	1.37 TB
3	aplicaciones.icetex.gov.co	133.52 GB	563.36 GB
4	appwebsites.icetex.gov.co	313.70 MB	128.51 GB
5	comunidad.icetex.gov.co	654.89 MB	36.73 GB
6	gestordeservicios.icetex.gov.co	3.63 GB	11.36 GB
7	web.icetex.gov.co:443	4.07 MB	132.96 MB
8	186.84.73.163	902.52 KB	115.08 MB
9	186.84.73.157	991.81 KB	109.55 MB
10	186.84.73.155	1.11 MB	108.09 MB

Tabla 7 Top 10 Portales más utilizados

El estado del licenciamiento es el siguiente:

SERVICIO	LICENCIAMIENTO	
	FECHA DE INICIO	FECHA DE EXPIRACIÓN
Liferay 7 .3.10 GA1 – Nodo 1	18 de septiembre de 2025 a las 19:00 horas	17 de octubre de 2026 a las 19:00 horas
Liferay 7 .3.10 GA1 – Nodo 2	18 de septiembre de 2025 a las 19:00 horas	17 de octubre de 2026 a las 19:00 horas
Liferay 7.3.10 GA1 – Ambiente de pruebas	18 de septiembre de 2025 a las 19:00 horas	17 de octubre de 2026 a las 19:00 horas
NFS	Licencia Open Source.	Licencia Open Source.

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

SERVICIO	LICENCIAMIENTO	
	FECHA DE INICIO	FECHA DE EXPIRACIÓN
Elasticsearch – Nodo 1	14 de agosto de 2025 a las 00:00 horas	31 de octubre de 2026 a las 23:59:59 horas
Elasticsearch – Nodo 2	14 de agosto de 2025 a las 00:00 horas	31 de octubre de 2026 a las 23:59:59 horas
Elasticsearch – Nodo 3	14 de agosto de 2025 a las 00:00 horas	31 de octubre de 2026 a las 23:59:59 horas

Tabla 8 Estado Licenciamiento Portal Web Icetex

4.2.2. Centro de Datos Alterno

4.2.2.1. Hosting Virtual (IaaS)

En el transcurso del mes de diciembre, se mantuvo en constante replicación las máquinas virtuales configuradas, estos servidores se replicaron desde el origen en Triara hasta Megacenter usando la herramienta nativa de VMware, Site Recovery Manager (SRM) el detalle de las máquinas virtuales replicadas se puede evidenciar en el [Informe mensual replicacion Diciembre 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 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	Dec 31, 2025	423.93 MB	5 minutes
Grupo de protección: PG_INFOTIC_6 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0228_INFOTIC_REP	OK	1 of 1	Dec 31, 2025	81.67 MB	1 hour
INR0229_INFOTIC_REP	OK	1 of 1	Dec 31, 2025	59.81 MB	1 hour
Grupo de protección: PG_INFOTIC_4 (3)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0238_INFOTIC_REP	OK	2 of 2	Dec 31, 2025	14.38 MB	1 hour
INR0239_INFOTIC_REP	OK	2 of 2	Dec 31, 2025	76.48 MB	1 hour
INR0243_INFOTIC_REP	OK	2 of 2	Dec 31, 2025	39.56 MB	1 hour
Grupo de protección: PG_INFOTIC_3 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0244_INFOTIC_REP	OK	1 of 1	Dec 31, 2025	76.53 MB	1 hour
INR0245_INFOTIC_REP	OK	1 of 1	Dec 31, 2025	7.57 MB	5 minutes
Grupo de protección: PG_INFOTIC_2 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0249_INFOTIC_REP	OK	2 of 2	Dec 31, 2025	8.24 MB	5 minutes

Ilustración 8 Reportes de replicación SRM a Sitio Alterno – diciembre2025

En la siguiente tabla se detallan los servidores con sus correspondientes servicios los cuales están siendo replicados a Megacenter:

#	INR Replicación	Host Name	Servicio	Virtual Machine Megacenter
1	INR0204	icetexbogwsmira	Portal Web	INR0226_INFOTIC_REP
2	INR0207	ictxisgesbd	Sisgestion	INR0228_INFOTIC_REP
3	INR0206	ictxisgesapp	Sisgestion	INR0229_INFOTIC_REP
4	INR0220 ***	icetexboglxorfeo1	ORFEO	INR0233_INFOTIC_REP
5	INR0219 ***	icetexboglxorfeo2	ORFEO	INR0262_INFOTIC_REP
6	INR0208 *	ICTXBOGSRVPT1	Portal Transaccional	INR0236_INFOTIC_REP
7	INR0209 **	icetexbogbalsrver1	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 INR0208 que replica la Maquina INR0236- ICTXBOGSRVPT1, los recursos de esta última se distribuyen en 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- icetexbogbalsrver1, corresponde al antiguo balanceador que fue deshabilitado en TRIARA.

***Por solicitud de ICETEX se detiene la replicación INR0219 y INR0220 que replica las máquinas virtuales INR0233 e INR0262 icetexboglxorfeo1 y icetexboglxorfeo2 respectivamente, las maquinas virtuales siguen en producción en TRIARA, durante este mes Icetex solicita nuevamente habilitar la replicación de INR0233 por que en este servidor se habilitó el espacio para pruebas de restauración, por lo tanto el proximo mes volverá a incluirse en el reporte diario de replicación dicho servidor.

En el caso del balanceador CITRIX, se presentó una indisponibilidad en el segundo equipo afectando la solución prevista, generandose una tasa final del 59,9%, incumpliendo los umbrales previstos, y que nos conduce a un descuento total de este item en la conciliación total.

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

INR	HOSTNAME	MB
INR0243	icetexbogliferayserver1	108429,28
INR0239	icetexbogelasticserver1	8141,04
INR0228	ictxisgesbd	7334,33
INR0229	ictxisgesapp	6851,99

INR	HOSTNAME	MB
INR0245	icetexboglxdarumasrv2	183,98
INR0249	icetexboglxroad1	608,12
INR0244	icetexboglxdarumasrv1	2036,13
INR0238	icetexbogliferaynfs	3085,93

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

Durante el mes de diciembre 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 Diciembre2025.pdf](#)

10.1.18.120 - Conexión a Escritorio remoto

```
[oracle@cxvodacontg011 ~]$ ps -fea |grep pmon
oracle 4684 1 0 Dec19 ? 00:02:40 ora_pmon_LIFERAYD
oracle 6503 6325 0 11:37 pts/0 00:00:00 grep --color=auto pmon
grid 7907 1 0 Aug23 ? 00:19:41 asm_pmon_+ASM
oracle 9290 1 0 Aug23 ? 00:44:08 ora_pmon_ICETEXD
oracle 9630 1 0 Aug23 ? 00:43:58 ora_pmon_APLICATD
oracle 10280 1 0 Aug23 ? 00:44:18 ora_pmon_APOTNEWD
oracle 14591 1 0 Dec26 ? 00:00:53 ora_pmon_LANDICTD
oracle 21179 1 0 Dec19 ? 00:02:51 ora_pmon_VIGIADTG
oracle 26920 1 0 Dec02 ? 00:10:21 ora_pmon_DBPIVOT
oracle 27315 1 0 Nov29 ? 00:12:05 ora_pmon_ICTXCYCD
oracle 30715 1 0 Dec29 ? 00:00:28 ora_pmon_APOTEOSD
oracle 32479 1 0 Dec01 ? 00:07:04 ora_pmon_SGDEAD
[oracle@cxvodacontg011 ~]$ sqlplus / as sysdba
-bash: sqlplus: command not found
[oracle@cxvodacontg011 ~]$ . oraenv
ORACLE_SID = [oracle] ? ICTXCYCD
ORACLE_BASE environment variable is not being set since this
information is not available for the current user ID oracle.
You can set ORACLE_BASE manually if it is required.
Resetting ORACLE_BASE to its previous value or ORACLE_HOME
The Oracle base has been set to /oracle/app/oracle/product/product/11.2.0/dbhome_1
[oracle@cxvodacontg011 ~]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.4.0 Production on Tue Dec 30 11:37:56 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 fapply

  Thread Last Sequence Received Last Sequence Applied TIME_RECEIVED TIME_APPLIED
  -----
1          176275          176275 30/12/2025 11:34 30/12/2025 11:34
2          128933          128933 30/12/2025 11:34 30/12/2025 11:34

SQL> sta uapply

  Thread Last Sequence Received Last Sequence Applied Difference
  -----
1          176275          176275          0
2          128933          128933          0
```

Ilustración 10 Evidencia DataGuard replicado a Megacenter BD

Se generó la consulta de los archivos recibidos y aplicados de la base de datos de ICTXCYCD a 31/12/2025 con diferencia cero(0) archivos sin aplicar, lo anterior indica que las BD y su replicación se encuentran sincronizadas.

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 diciembre al 100%:

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

Tabla 12 Disponibilidad de Servicios de Housing – Data Center Alterno

4.2.2.4. Servicios de DRP

En el mes de diciembre se entregaron los Informes de la prueba de DRP realizada el 29 de noviembre de 2025.

[Informe prueba Aislada DRP Ictex 20251129.pdf](#)

[Anexo1 Evidencias InformePruebaDRPIctex 20251129.pdf](#)

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.

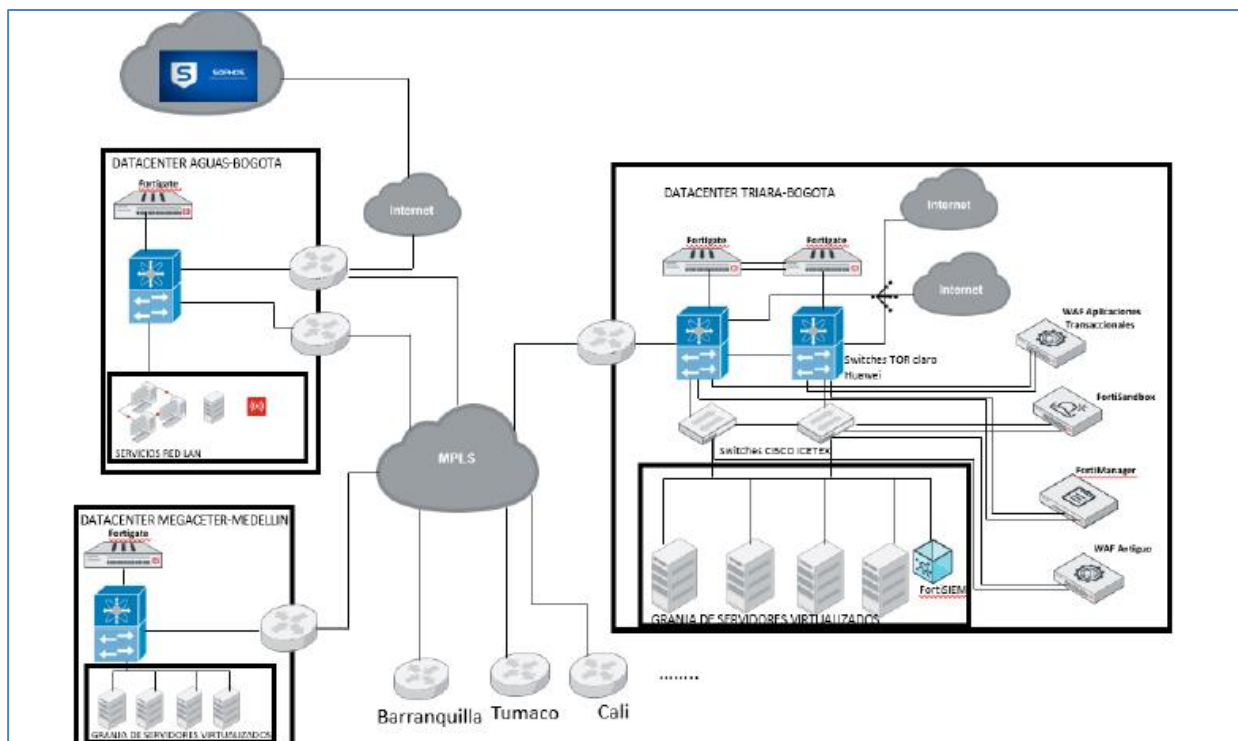


Ilustración 11 Diagrama de la Arquitectura de Seguridad

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

En la ilustración 11, 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.

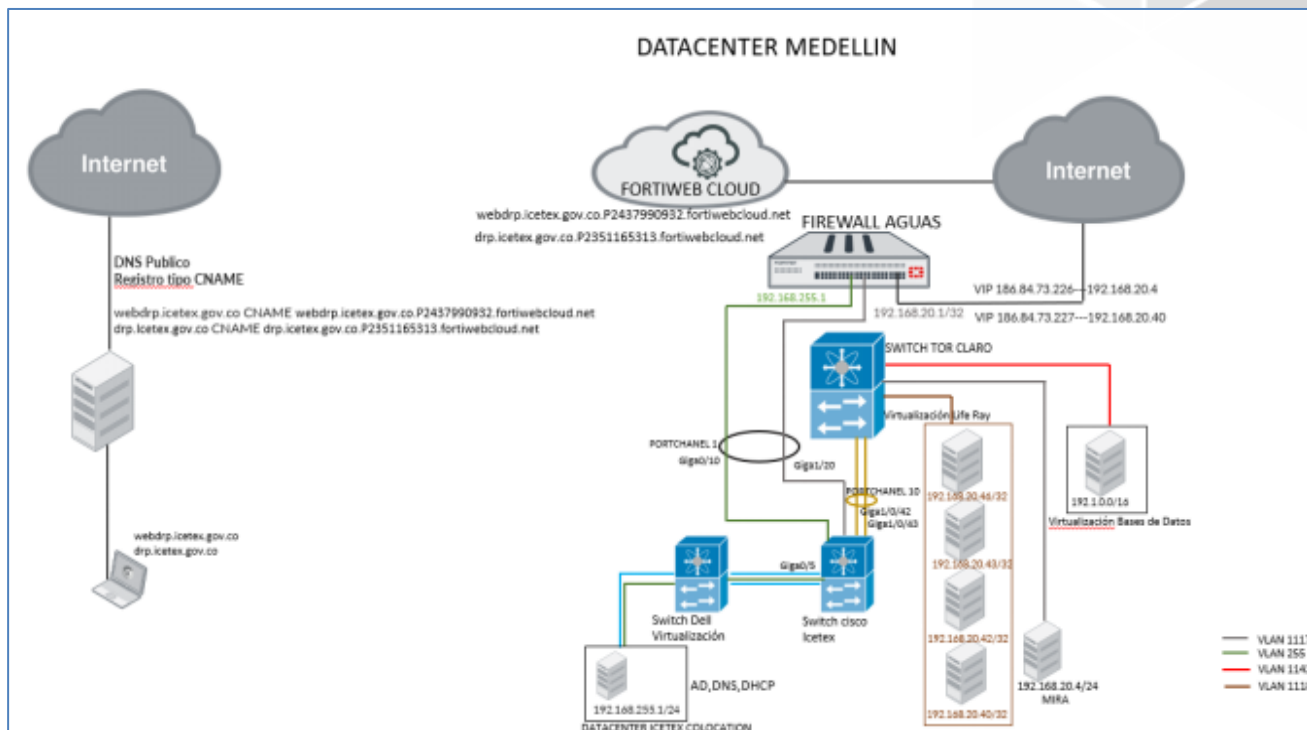


Ilustración 12 Topología de WAF Cloud usado en portales de Medellín

En el ámbito de la gestión de políticas de seguridad, se realizaron configuraciones sobre IPv6, permitiendo el tráfico para la prueba de las sedes.

Se realizó la configuración de VPN Site To Site para el análisis de vulnerabilidades Infotíc.

Se realiza configuración de VPN SSL para ayudar a la conexión del web máster a el ambiente de pruebas.

Se realiza el ajuste a nivel del CPU para el FortiSIEM.

Respecto al firewall de la red de Aguas, se mantienen actualmente 541 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 diciembre, link: [Informe Mensual InfoTIC Seguridad Diciembre2025.pdf](#)

Durante el mes de diciembre 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 Diciembre 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 múltiples eventos de seguridad, dentro de los cuales se incluyeron intentos de acceso no autorizado a los servicios institucionales, detectados por el SOC. A través de FortiSIEM se identificaron diversas direcciones IP maliciosas que intentaron establecer conexiones hacia los servicios web desde diferentes puertos.
- Ajuste permisos bases de datos producción.
- Validación del canal de conexión en el core bancario en la sede de Medellín, asegurando la correcta configuración y cumplimiento de los estándares de seguridad.
- Aplicación de restricciones en las bases de datos de producción y habilitación de accesos únicamente a réplicas, garantizando la protección de la información crítica.
- Recomendaciones sobre fallas en la publicación interna de aplicaciones sin pasar por el WAF, identificando riesgos como SQL Injection, Cross-Site Scripting y robo de datos, entre otros, que podrían comprometer la seguridad.
- Restricción del uso de WhatsApp Web, debido a que representa un riesgo significativo: con un solo clic, el equipo podría ser infectado y posteriormente propagar malware o facilitar un ataque cibernético.
- Configuración de la encriptación de la comunicación entre aguas y Datacenter por medio de la MPLS.

- **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.

- **Gestión Operativa y soporte de seguridad**

Se gestionaron y resolvieron oportunamente los casos reportados a través de la plataforma Aranda, así como las solicitudes recibidas por correo electrónico. El detalle de estas atenciones está documentado en el informe mensual de seguridad.

Se brindó acompañamiento a diversas áreas de la organización en la atención de requerimientos específicos, incluyendo publicaciones en IPv6, configuración de certificados, bloqueos por parte del WAF, etc.

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
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 13 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
FW Fortigate 1800F (MST)	10.0.0.53	Si	18/05/2026	Triara
FW Fortigate 1800F (SLV)	10.0.0.53	Si	18/05/2026	Triara
FW FortiGate 600F	10.0.0.30	Si	1/06/2026	Megacenter
FW FortiGate 600F	10.1.100.33	Si	11/05/2026	Aguas

Tabla 14 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; se adelantó la actualización a la versión de FortiOS 7.4.9.

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:

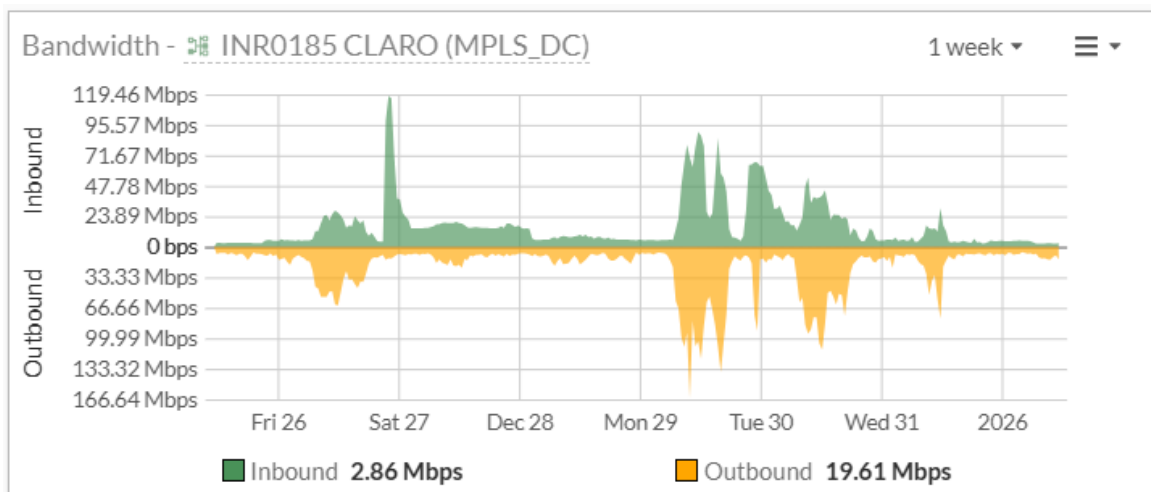


Ilustración 13 Consumo canal MPLS - promedio 1200G [INR0185 CLARO(MPLS_DC)]

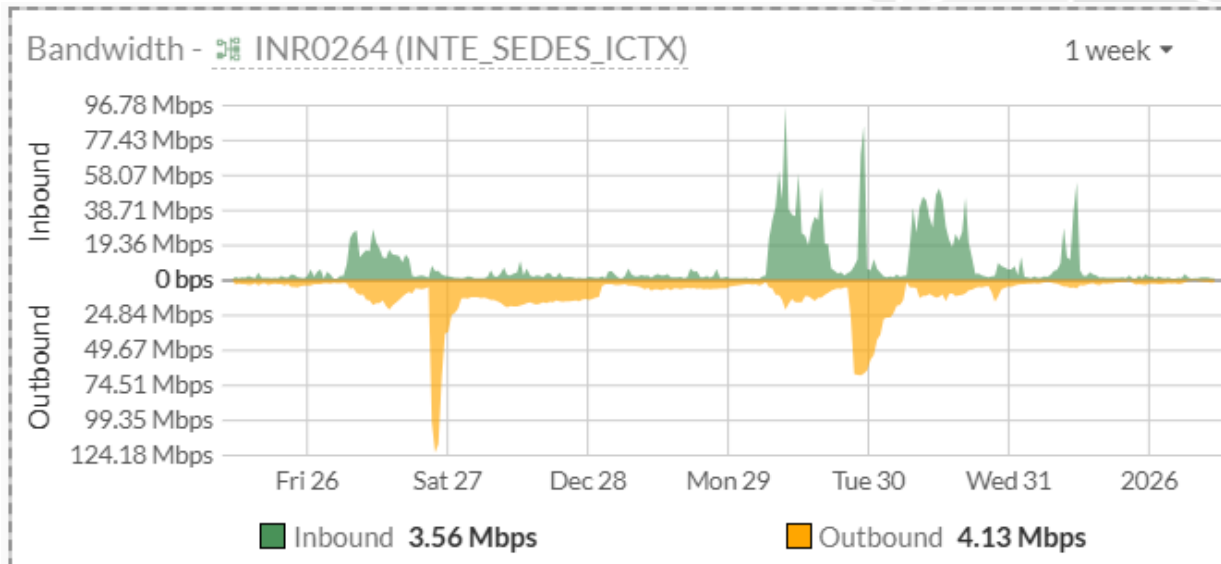


Ilustración 14 Consumo canal Internet Sedes - Promedio 1100 GB WAN-SEDES-ICETEX [INR0264 (INTE_SEDES_ICTX)]

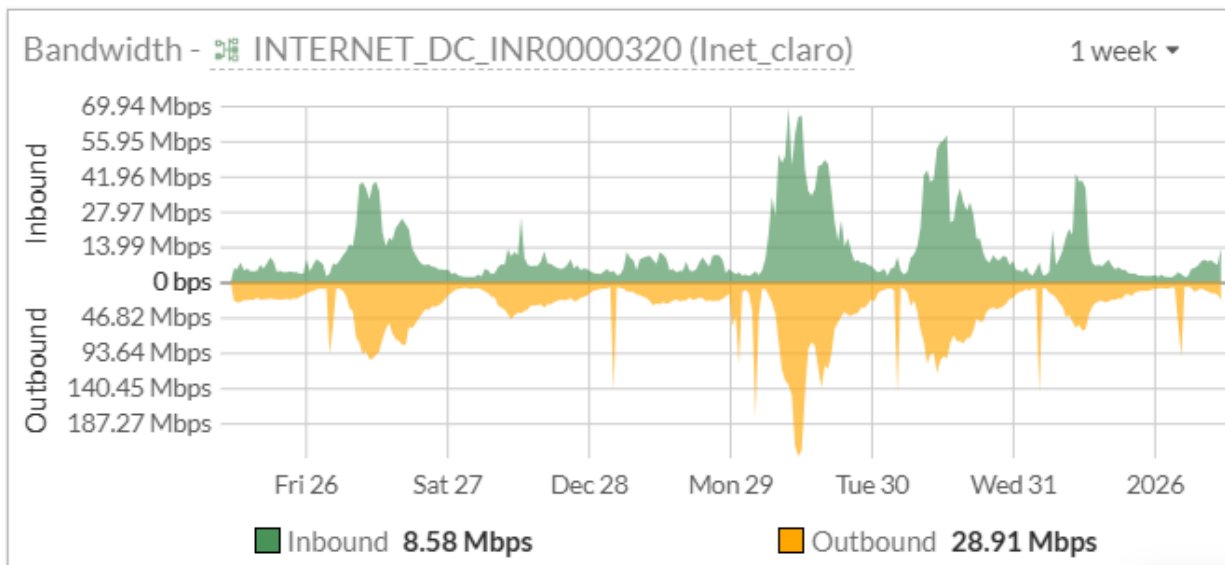


Ilustración 15 Consumo Canal Internet Data Center- INTERNET DATACENTER [INTERNET_DC_INR0000320 (Inet_claro)]

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:

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

	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 16 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 17 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 18 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 7.4.9.

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:

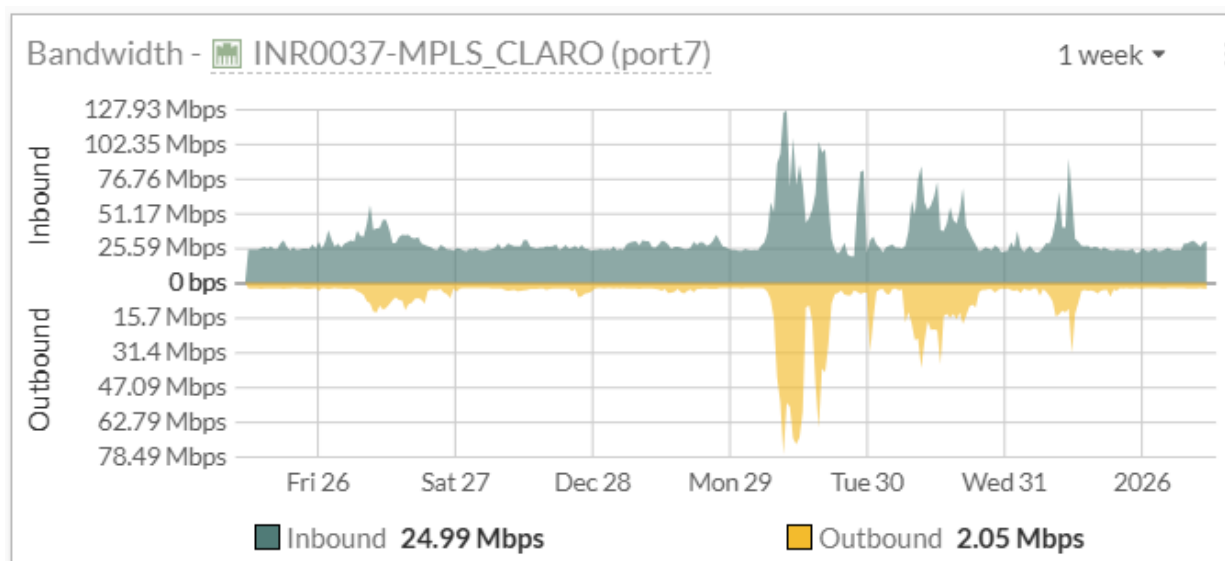


Ilustración 19 Consumo Canal MPLS Aguas - promedio 800 GB

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 20 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 21 Inspección-SSL-(FortiGate-Aguas)

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

Ilustración 22 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 7.4.9.

Se observa en la Ilustración 24, que la interfaz de la MPLS del Data Center de Medellín no presenta tráfico debido a que este se tiene como Data Center Alterno.



#	HTTP Host	HTTP Request Bytes	HTTP Response Bytes
1	web.icetex.gov.co	529.66 GB	8.05 TB
2	www.icetex.gov.co	38.53 GB	1.37 TB
3	aplicaciones.icetex.gov.co	133.52 GB	563.36 GB
4	appwebsites.icetex.gov.co	313.70 MB	128.51 GB
5	comunidad.icetex.gov.co	654.89 MB	36.73 GB
6	gestordeservicios.icetex.gov.co	3.63 GB	11.36 GB
7	web.icetex.gov.co:443	4.07 MB	132.96 MB
8	186.84.73.163	902.52 KB	115.08 MB
9	186.84.73.157	991.81 KB	109.55 MB
10	186.84.73.155	1.11 MB	108.09 MB

Ilustración 24 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.

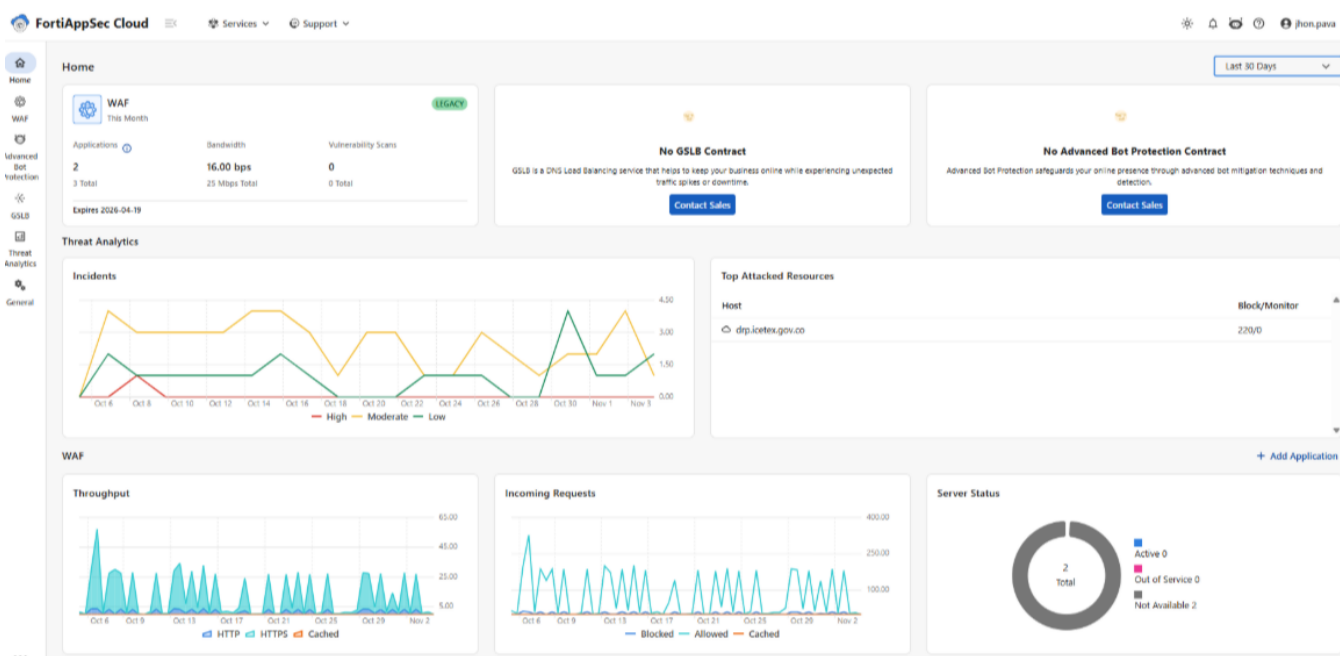


Ilustración 25 Tráfico General de los portales

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).

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

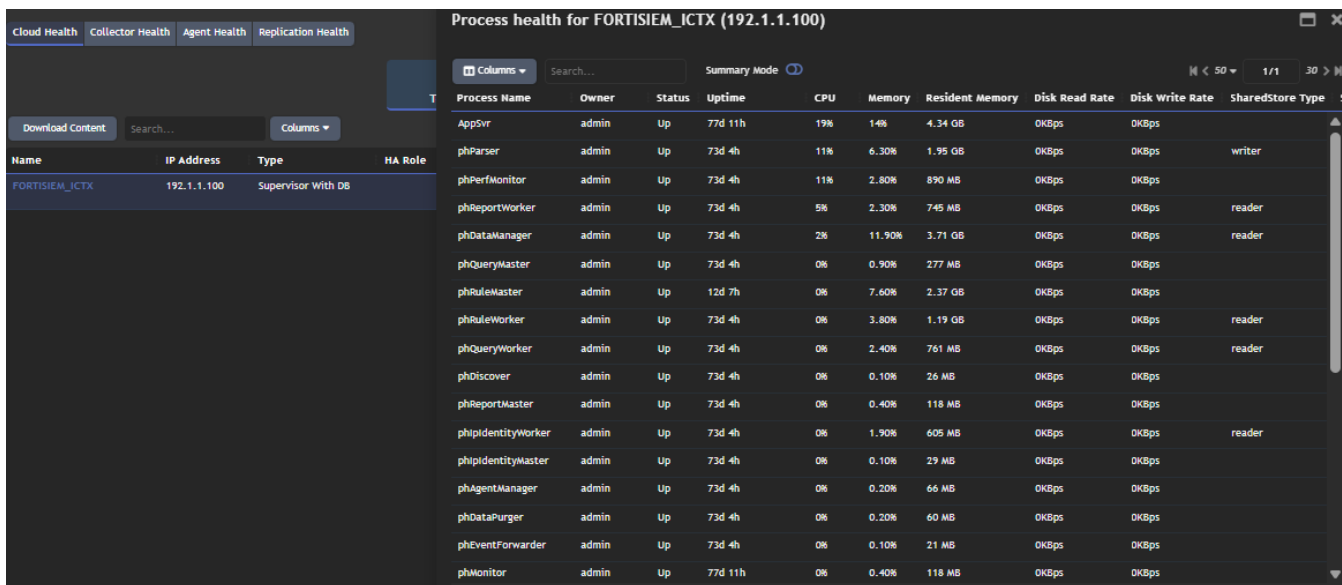
Sede Manizales, Colombia
 Cra. 24 No. 53ª-26 Arboleda
 Alta.
 NIT: 900.068.796-1
 Teléfono: (+606) 88612612

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 16 Configuración FortiSandBox 1000D

4.3.1.8. FortiSIEM

A continuación, se presenta el desempeño por procesos:



Process Name	Owner	Status	Uptime	CPU	Memory	Resident Memory	Disk Read Rate	Disk Write Rate	SharedStore Type
AppSvr	admin	Up	77d 11h	19%	14%	4.34 GB	OKBps	OKBps	
phParser	admin	Up	73d 4h	11%	6.30%	1.95 GB	OKBps	OKBps	writer
phPerfMonitor	admin	Up	73d 4h	11%	2.80%	890 MB	OKBps	OKBps	
phReportWorker	admin	Up	73d 4h	5%	2.30%	745 MB	OKBps	OKBps	reader
phDataManager	admin	Up	73d 4h	2%	11.90%	3.71 GB	OKBps	OKBps	reader
phQueryMaster	admin	Up	73d 4h	0%	0.90%	277 MB	OKBps	OKBps	
phRuleMaster	admin	Up	12d 7h	0%	7.60%	2.37 GB	OKBps	OKBps	
phRuleWorker	admin	Up	73d 4h	0%	3.80%	1.19 GB	OKBps	OKBps	reader
phQueryWorker	admin	Up	73d 4h	0%	2.40%	761 MB	OKBps	OKBps	reader
phDiscover	admin	Up	73d 4h	0%	0.10%	26 MB	OKBps	OKBps	
phReportMaster	admin	Up	73d 4h	0%	0.40%	118 MB	OKBps	OKBps	
phIdentityWorker	admin	Up	73d 4h	0%	1.90%	605 MB	OKBps	OKBps	reader
phIdentityMaster	admin	Up	73d 4h	0%	0.10%	29 MB	OKBps	OKBps	
phAgentManager	admin	Up	73d 4h	0%	0.20%	66 MB	OKBps	OKBps	
phDataPurger	admin	Up	73d 4h	0%	0.20%	60 MB	OKBps	OKBps	
phEventForwarder	admin	Up	73d 4h	0%	0.10%	21 MB	OKBps	OKBps	
phMonitor	admin	Up	77d 11h	0%	0.40%	118 MB	OKBps	OKBps	

Ilustración 26 Desempeño por procesos

4.3.1.9. Sophos EndPoint

En la ilustración 27, 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.

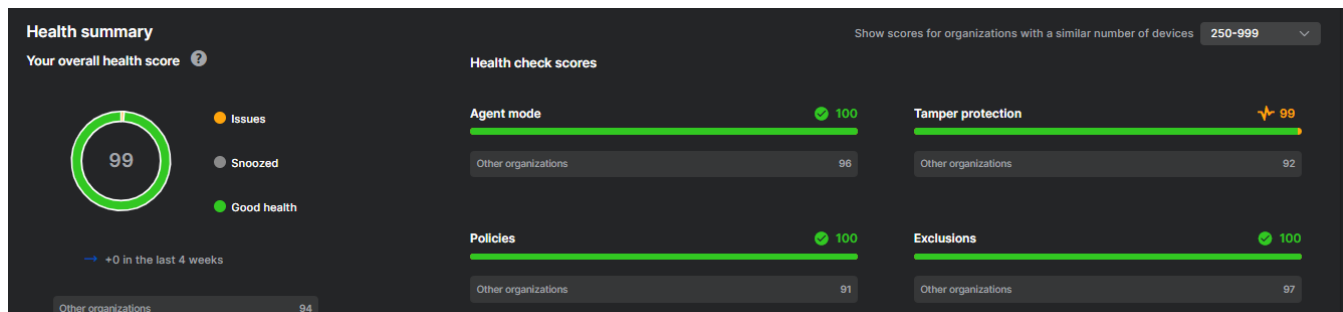


Ilustración 27 Estado Seguridad Sophos

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

Los cuatro equipos que se encuentran no protegidos son: BOGARRIENDO88, BOGIMAC01, BOGVFAPC502 y COWORKING11, los cuales tienen más de 9 meses en algunos casos de no conectarse, recomendamos que la mesa de servicio revise dichos equipos.

En la sección 6.6.1 del informe de seguridad [Informe Mensual InfoTIC Seguridad Diciembre2025.pdf](#) se detallan las amenazas contenidas por la herramienta el Sophos instalado en los equipos ordenadores y servidores.

4.3.2. Recomendaciones de Seguridad para el ICETEX.

Recomendación	Estado	Criticidad	Fuente	Asunto	Personal de ICETEX a quien se notificó
Garantizar la segmentación de la red que permita claramente definir qué servicios deben ser alcanzados por cada usuario.	Como parte de las pruebas de IPv6, se están realizando pruebas de DHCPv6 en la red para que el servidor entregue direccionamiento IPv6 a las redes de la Entidad y que esta segmentación cumpla los estándares del protocolo IPv6.	Media	Informes Mensuales - sesiones	Segmentación Red ICETEX (Sesión Teams) / Segmentación de la red "Tesorería y Cartera" (Sesión Teams) / Validación de topología y segmentación Tesorería (Sesión Teams)	Grupo Coordinación de Infraestructura Tecnológica / Grupo Coordinación de Infraestructura Tecnológica / Especialista de seguridad
Se recomienda una tecnología que permita realizar análisis de tráfico de la red (NTA- Network Traffic Analysis).	En evaluación por parte de ICETEX.	Alta	N/A	N/A	N/A
Se recomienda una tecnología que permita la gestión o validación de privilegios de accesos (IAM). Evitar configurar usuarios y claves dentro de las aplicaciones de ICETEX.	En evaluación por parte de ICETEX.	Alta	N/A	N/A	N/A
Adquirir un equipo Firewall para correo para prevenir brechas de seguridad asociadas al uso del correo electrónico y	En evaluación por parte de ICETEX.	Alta	Informes Mensuales - sesiones	Reunión de pares de seguridad	Grupo Coordinación de Infraestructura Tecnológica / Grupo Coordinación de Infraestructura Tecnológica

Recomendación	Estado	Criticidad	Fuente	Asunto	Personal de ICETEX a quien se notificó
que este es susceptible a muchos tipos de amenazas.					
Validar a nivel de punto final, los equipos que se han visto involucrados con comportamiento malicioso.	Se evalúa por parte de ICETEX. Se hace seguimiento por parte del SOC quien reporta comportamiento malicioso. Sin embargo, es necesario establecer políticas de conexión de equipos externos BYOD debido a que muchos de los casos reportados por el SOC vienen de equipos personales que no hacen parte de la Entidad.	Critica	Informes Mensuales	N/A	N/A
Integrar los equipos que hacen parte del proceso de pagos con el SIEM.	Se debe evaluar la capacidad del SIEM, se espera plan de mejora.	Media	Informes Mensuales - sesiones	Recursos de FORTISIEM CPU, Memoria y disco / Recomendaciones de arquitectura de FortiSIEM Icetex	Líder infraestructura / Especialista Desarrollo / Especialista de seguridad / Especialista de seguridad / Grupo de Coordinación de Infraestructura Tecnológica / Profesional de tecnología
Evaluar los riesgos sobre las plataformas en la nube y considerar aplicar plataformas de seguridad para los ambientes cloud que cuenta la entidad ya que estos contienen servicios críticos para la misma.	En evaluación por parte de ICETEX.	Alta	N/A	N/A	N/A
Se debe realizar la integración de los activos críticos de la compañía a la plataforma de SIEM, no se ha podido lograr por la falta de recursos de este.	En evaluación por parte de ICETEX.	Alta	Informes Mensuales - sesiones	Recursos de FORTISIEM CPU, Memoria y disco / Recomendaciones de arquitectura de FortiSIEM Icetex	Líder infraestructura / Especialista Desarrollo / Especialista de seguridad / Especialista de seguridad / Grupo de Coordinación de Infraestructura

Recomendación	Estado	Criticidad	Fuente	Asunto	Personal de ICETEX a quien se notificó	
					Tecnológica Profesional tecnología	/ de

Tabla 17 Recomendaciones de Seguridad

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 [Informe Mensual SOC-TH ICETEX Diciembre 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)	Diciembre	Noviembre	Octubre	Septiembre
IOC – Malware DOMINIOS	6.047	6.047	6.047	6.047
IOC – Malware IPs	11.076	11.119	11.119	11.121
IOC – Malware HASH	1.627	1.627	1.627	1.627
IOC – Malware URL	4.564	4.564	4.564	4.564

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 Diciembre 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 28 Total de alertas de seguridad

Durante el período evaluado de 52.758 alertas de seguridad identificadas, se presentaron con criticidad ALTA un total de 856 equivalentes al 1,6% 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 Diciembre	Alertas de Seguridad Noviembre	Alertas de Seguridad Octubre	Alertas de Seguridad Septiembre	Alertas de Seguridad Agosto	Alertas de Seguridad Julio
High	1.198	1.862	2.599	4.450	3.949	1.536
Medium	50.794	178.911	250.034	312.033	199.433	9.711
Low	856	1.076	2.556	3.310	2.224	193

Tabla 19 comparativo Alertas de Seguridad

Durante el período evaluado se presentaron 1.198 alertas de seguridad con criticidad MEDIA, un disminuyó con relación a periodos anteriores. En el documento [Informe Mensual SOC-TH ICETEX Diciembre 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 4 se presenta a continuación:

Chart	Event Name	Criticidad	Criticidad	Tactica	Cantidad de Alertas
☒	Concurrent Failed Authentications To Same Account From Multiple Countries	High	9	Credential Access	619
☒	Critical large Outbound Transfer To Outside My Country ICETEX - WX N3	High	9		294
☒	Brute Force Host Login Success CUSTOM 8/10/2021	High	9		118
☒	System Exploit Detected by Network IPS	High	9		50
☒	Repeated Multiple Logon Failures: Server	High	9	Credential Access	27

Ilustración 29 Top 5 de Alertas de Seguridad Altas

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

Durante el período evaluado se presentaron 50.794 alertas de seguridad con criticidad MEDIA, 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 o que requieran una indagación más exacta.

Chart	Event Name	Criticidad	Criticidad	Tactica	Cantidad de Alertas
☒	Alerta Domain Controller Hora Oficina	Medium	8		1,376
☒	Large Inbound Transfer From Outside My Country	Medium	8	Command And Control	885
☒	Large Outbound Transfer To Outside My Country ICETEX	Medium	8		832
☒	Large Outbound Transfer	Medium	8	Exfiltration	172
☒	Account Locked: Server	Medium	8	Credential Access	165

Ilustración 30 Top 5 de Alertas de Seguridad Medias

4.3.3.1.2. Categoría Disponibilidad

Durante el período evaluado se presentaron 72.953 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
☒	Network Device Down: no ping response - WX N3	High	10	Impact	43
☒	FortiSIEM EventDB event store failed	High	10		7
☒	System Collector is down	High	9		24
☒	Network Device Hardware Critical	High	9		18
☒	WMI or OMI Service Unavailable	High	9	Impact	12
☐	EventDB: Event Retention Policy Violation	High	9		9
☐	Excessive Clock Skew Between Collector and Supervisor nodes	High	9		8
☐	FortiSIEM Agent Operational Error WXN2	High	9		7
☐	SNMP Service Unavailable	High	9	Impact	5
☐	Scheduled Report Send Error	High	9		5
☐	No logs from a device in 8 hours - WX N3	High	9		3
☐	FortiSIEM EPS License Exceeded	High	9		2
☐	Excessive External Event Dropped By License	High	9		2
☐	Windows Cluster Service Startup Error	High	9		1

Ilustración 31 Top 10 de Alertas de Disponibilidad Altas

A continuación, se presentan los análisis efectuados:

- “FortiSIEM EventDB Event store failed” – Esta alerta se genera cuando se detecta que el módulo DataManager no puede crear un directorio en NFS para escribir archivos de eventos, incluso después de varios reintentos. Se perderán los datos. Es decir que el sistema intentó guardar eventos en el

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

almacenamiento de red (NFS), pero no tiene permisos, espacio o conectividad para hacerlo. Como no pudo crear la carpeta necesaria, los eventos que deberían guardarse ahí no se van a conservar.

- “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 colector y el supervisor; esto provocará que las reglas en tiempo real no se activen para los eventos recibidos de ese recopilador.
- “EventDB: Event Retention Policy Violation” – Esta alerta 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.
- “Excessive External Event Dropped By License” – Esta alerta se genera cuando detecta que los eventos se descartan debido a una licencia inadecuada.
- “FortiSIEM EPS License Exceeded” – Esta alerta se genera cuando detecta que se excede la licencia global de EPS incluso con una redistribución elástica de EPS. Los eventos se eliminarán a menos que se actualice la licencia.

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 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					
3.1.1 FortiGate: Top IPS Ataques Permitidos - WX Last 1 mon ⚙️ ✕					
Reporting Device	Attack Name	Signature Id	Severity	Firewall Action	COUNT(Match...
DC_FG_MST_ICETEX	React.Server.Components.react-flight...	59644	High	detected	9
DC_FG_MST_ICETEX	DNS.PTR.Records.Scan	51391	Low	detected	12,626
DC_FG_MST_ICETEX	SSL.Anonymous.Ciphers.Negotiation	43544	Low	detected	33

Ilustración 32 ataques IPS permitidos

3.1.1 FortiGate: Top IPS Ataques Denegados - WX						Last 1 mon
Reporting Device	Attack Name	Signature Id	Severity	Firewall Action	COUNT(Match...	
DC_FG_MST_ICETEX	Nmap.Script.Scanner	45360	Medium	dropped	1,641	
DC_FG_MST_ICETEX	ALFA.TEaM.Web.Shell	53229	Medium	dropped	1,616	
DC_FG_MST_ICETEX	Apache.Log4j.Error.Log.Remote.Code...	51006	Medium	dropped	1,481	
DC_FG_MST_ICETEX	ZGrab.Scanner	48805	Medium	dropped	736	
DC_FG_MST_ICETEX	WordPress.REST.API.Username.Enumer...	48072	Medium	dropped	356	
DCAGUAS_FG_MST_ICETEX	Remcos.Botnet	47360	Medium	dropped	305	
DC_FG_MST_ICETEX	PHPUnit.Eval-stdin.PHP.Remote.Code...	45765	Medium	dropped	272	
DC_FG_MST_ICETEX	Kubernetes.Ingress.NGINX.Controller...	57679	Medium	dropped	258	
DC_FG_MST_ICETEX	Censys.io.Scanner	50899	Medium	dropped	210	
DC_FG_MST_ICETEX	MS.IIS.ShortName.Vulnerability.Scanner	47145	Medium	dropped	199	
DCAGUAS_FG_MST_ICETEX	TCP.Split.Handshake	26339	Medium	dropped	191	
DC_FG_MST_ICETEX	Linux.Kernel.TCP.SACK.Panic.DoS	48103	Medium	dropped	105	
DC_FG_MST_ICETEX	Apache.HTTP.Server.cgi-bin.Path.Trav...	50825	Medium	dropped	79	
DC_FG_MST_ICETEX	PTZOptics.PT30X.param.Authenticatio...	56827	Medium	dropped	63	
DC_FG_MST_ICETEX	React.Server.Components.react-flight...	59644	Medium	dropped	58	

Ilustración 33 ataques IPS denegados

➤ **Top Perímetro:** A continuación se 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).

Source IP	Destination IP	IP Protocol	Destination TCP/UDP Port	COUNT(Matched Events)	SUM(Sent Bytes64)	SUM(Received Bytes64)	SUM(Total Bytes64)
2801:192:2:18::10:65	2801:192:2:51::65	17 (UDP)	53 (DOMAIN)	473,688	9.09 GB	15.76 GB	24.85 GB
2801:192:1:108:8559:93f4:84b:34c2	2001:4860:4860::8888	17 (UDP)	53 (DOMAIN)	127,271	20.27 MB	36.16 MB	56.44 MB
200.3.192.203	192.168.91.15	6 (TCP)	443 (HTTPS)	74,609	7.28 TB	3.32 TB	10.6 TB
200.3.192.205	192.168.91.15	6 (TCP)	443 (HTTPS)	71,035	2.82 TB	1.48 TB	4.31 TB
2801:192:2:18::16	2801:192:2:51::65	17 (UDP)	53 (DOMAIN)	50,979	4.19 MB	7.67 MB	11.87 MB
200.3.192.204	192.168.91.15	6 (TCP)	443 (HTTPS)	37,129	4.42 TB	2.4 TB	6.83 TB
192.178.11.96	192.168.91.17	6 (TCP)	443 (HTTPS)	27,674	1.38 GB	38.54 GB	39.92 GB
2801:192:2:51::65	2801:192:2:18::10:65	6 (TCP)	49672	26,224	2.68 GB	4.18 GB	6.86 GB
2801:192:2:20::4	2801:192:2:51::65	17 (UDP)	53 (DOMAIN)	25,826	2.65 MB	4.99 MB	7.65 MB
2801:192:2:18::10:65	2801:192:2:51::65	6 (TCP)	49667	25,708	2.34 GB	3.46 GB	5.8 GB
192.178.11.97	192.168.91.17	6 (TCP)	443 (HTTPS)	24,343	1.51 GB	42.41 GB	43.92 GB
192.178.11.98	192.168.91.17	6 (TCP)	443 (HTTPS)	24,039	1.42 GB	39.61 GB	41.03 GB
2801:192:6:e2:c9d0:493f:d77d:1fd5	2a03:2880:f351:3:face:b00c::4c63	6 (TCP)	443 (HTTPS)	22,899	592 B	1.36 KB	1.94 KB
190.242.43.83	192.168.91.15	6 (TCP)	443 (HTTPS)	21,115	3.14 GB	8.49 GB	11.64 GB
2801:192:6:e2:91f5:5d8f:1196:54eb	2a03:2880:f362:3:face:b00c::4c63	6 (TCP)	443 (HTTPS)	20,033	0B	0B	0B
190.157.218.113	192.168.91.15	6 (TCP)	443 (HTTPS)	18,185	1.95 GB	21 GB	22.95 GB
66.249.77.9	192.168.91.15	6 (TCP)	443 (HTTPS)	17,662	15.96 GB	164.39 GB	180.36 GB
66.249.77.10	192.168.91.15	6 (TCP)	443 (HTTPS)	17,483	17.67 GB	180.96 GB	198.64 GB
66.249.77.11	192.168.91.15	6 (TCP)	443 (HTTPS)	16,263	12.93 GB	132.45 GB	145.39 GB
181.143.30.106	192.168.91.15	6 (TCP)	443 (HTTPS)	15,549	135.63 GB	77.39 GB	213.03 GB
2801:192:6:e2:644b:468e:1088:d56d	2a03:2880:f32f:1:face:b00c::4c63	6 (TCP)	443 (HTTPS)	15,252	15.27 KB	212.22 KB	227.5 KB
2801:192:6:e2:750f:943a:a8f4:183	2a03:2880:f32f:1:face:b00c::4c63	6 (TCP)	443 (HTTPS)	14,684	5.46 KB	18.31 KB	23.77 KB
66.249.77.12	192.168.91.15	6 (TCP)	443 (HTTPS)	14,279	6.43 GB	65.15 GB	71.58 GB

Ilustración 34 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), 389 (LDAP) los cuales en su mayoría son utilizados en entornos LAN o privados.

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

Puertos salientes de público a privado (Permitidos): Debido a las limitantes de recursos de la herramienta FortiSIEM no se puede realizar la extracción de información de este componente.

Failed Windows Login Last 1 hr			
Source IP	User	Server	COUNT(Match...
192.168.53.10	90 goanywhere	ictxsrfs.icetex.local	33,053
10.2.254.104	jcperez	ictxsrfs.icetex.local	1,770
192.168.20.29	gestiondoc	70 ICTXSRVAD001.icet...	1,685
10.2.254.1	jpforero	ictxsrfs.icetex.local	1,108
172.16.224.24	asotoc	ictxsrfs.icetex.local	1,095
192.168.53.10	90 goanywhere	70 ICTXSRVAD001.icet...	944
10.200.176.33	Administrador	70 ICTXSRVAD001.icet...	850
10.2.254.6	jpforero	ictxsrfs.icetex.local	829
10.2.254.118	Administrador	ictxsrfs.icetex.local	780
10.2.254.2	jpforero	ictxsrfs.icetex.local	667
10.2.254.105	jcperez	ictxsrfs.icetex.local	645
172.16.224.204	lmejiac	ictxsrfs.icetex.local	590
10.1.6.42	Icetex	ictxsrfs.icetex.local	587
172.16.224.185	mgalindo	ictxsrfs.icetex.local	564
10.2.254.5	jpforero	ictxsrfs.icetex.local	469

Ilustración 35 Top de Accesos Fallidos plataforma Windows

Account Lockouts		Last
Server	User	COUNT(/
70 ICTXSRVAD001.icetex.local	ad.kmorenoa	1,205
70 ICTXSRVAD001.icetex.local	jdelgado	865
70 ICTXSRVAD001.icetex.local	mmedina	802
70 ICTXSRVAD001.icetex.local	jbarrera	754
68 ICTXSRVAD000.icetex.local	ad.kmorenoa	657
70 ICTXSRVAD001.icetex.local	mmedinamon	517
70 ICTXSRVAD001.icetex.local	37 22823906	484
70 ICTXSRVAD001.icetex.local	dilesh	424
70 ICTXSRVAD001.icetex.local	vacosta	402
70 ICTXSRVAD001.icetex.local	mriascos	323
68 ICTXSRVAD000.icetex.local	mmedina	209
70 ICTXSRVAD001.icetex.local	Administrator	187
70 ICTXSRVAD001.icetex.local	15 jladinos	177
70 ICTXSRVAD001.icetex.local	caucique	150
70 ICTXSRVAD001.icetex.local	yrojasme	129

Ilustración 36 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 de sesión VPN y de Inicio de sesión Unix.

4.3.3.2. 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 Diciembre 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 [Informe Mensual SOC-TH ICETEX Diciembre 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.

4.3.3.3. Análisis de Marca OSINT

Durante el periodo evaluado, la plataforma de monitoreo de protección de marca y OSINT – AXUR, reporta un total de 151 posibles amenazas de las 33,3k que fueron encontradas y analizadas automáticamente por la plataforma de monitoreo. A estas 151 posibles amenazas se les realizó una revisión y análisis interno, de sus características, datos e información.

Durante el periodo evaluado se detectó 9 incidentes de los cuales 4 están relacionados con phishing, 2 con Perfil falso en red social, 1 con uso fraudulento de marca y 1 con otros datos confidenciales.



Ilustración 37 Incidentes por Tipo de Amenaza

En cuanto a casos relacionados a Fraudes digitales y fuga de información, se presentó un total de 30 casos, de los cuales 24 casos fueron descartados, teniendo en cuenta que algunos no tenían relación y otros solo mencionaban la marca, 06 casos fueron reportados a la entidad y se encuentran en estado de tratamiento.

Estos se encuentran detallados en el [Informe Mensual MARCA-OSINT ICETEX Diciembre 2025.pdf](#)

4.3.4. Análisis de Vulnerabilidades ICETEX

Durante diciembre de 2025 se ejecutó satisfactoriamente el análisis de vulnerabilidades correspondiente a la Fase 9 del plan de trabajo. En esta etapa se evaluaron 85 activos: 76 equipos de usuario final (en línea con la planificación mensual) y 9 Servidores atendidos por requerimiento para verificación de remediación de

vulnerabilidades. Esta actividad forma parte del avance progresivo definido para cubrir el entorno completo por bloques, manteniendo la continuidad con las fases anteriores.

Entre los hallazgos más relevantes se encuentran:

Bloque mensual Diciembre — Equipos de usuario final (síntesis)

- **Servicios con configuración por defecto para inicio de sesión:** Se identificó un equipo con un servicio HP con credenciales por defecto
- **Problemas de seguridad a nivel de versión insegura de FTP:** una detección de conexión por versión de vsftpd insegura en un servicio FTP

Conclusión: el bloque mensual revela problemas de uso de servicios con vulnerabilidades conocidas y configuraciones por defecto en servicios en endpoints que los hacen vulnerables — requiere acciones de parcheo/segmentación y hardening

Tres (3) Equipos evaluados (192.168.51.161, 192.168.51.163, 10.1.18.134)

Fecha de solicitud: 1 de diciembre de 2025

Objetivo: Identificar y documentar las vulnerabilidades SSL Medium Strength Cipher Suites Supported (SWEET32)

Estado de remediación de vulnerabilidades: remediación completa por parte de ICETEX:

Severidad	Vulnerabilidad	Dispositivos afectados	Estado de remediación
Alta	SSL Medium Strength Cipher Suites Supported (SWEET32)	192.168.51.161	Remediada
Alta	SSL Medium Strength Cipher Suites Supported (SWEET32)	192.168.51.163	Remediada
Alta	SSL Medium Strength Cipher Suites Supported (SWEET32)	10.1.18.134	Remediada

Ilustración 38 Estado de Remediación completa de vulnerabilidades

Cinco (5) Equipos evaluados (192.168.51.161, 192.168.51.163, 10.1.18.134, 192.1.1.4, 192.168.20.57, 192.168.20.4.)

Fecha de solicitud: 12 de diciembre de 2025

Objetivo: Identificar y documentar vulnerabilidades de seguridad presentes en los activos tecnológicos dentro del alcance de la evaluación.

Estado de de remediación de vulnerabilidades: remediación parcial por parte de ICETEX:

Severidad	Vulnerabilidad	Dispositivos afectados	Estado de remediación
Critical	Detección del protocolo SSL versión SSLv2 y SSLv3	192.168.20.4	Remediada
Critical	Unsupported Web Server Detection	192.168.20.4	Sin remediar
Alta	SSL Certificate Signed Using Weak Hashing Algorithm	192.168.20.4 192.168.20.57	Sin remediar
Medium	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	192.168.20.4	Sin remediar
Medium	Web Server HTTP Header Information Disclosure	192.168.20.4	Sin remediar
Medium	Conjuntos de cifrado SSL de intensidad media compatibles (SWEET32)	192.168.20.4	Remediada
Medium	TLS Version 1.0 Deprecated Protocol	192.168.20.4	Sin remediar

Ilustración 39 Estado de Remediación parcial de vulnerabilidades.

4.3.4.1. Gestión de Vulnerabilidades

Para el mes de diciembre quedó un saldo de 1164 vulnerabilidades pendientes por remediar, ya que se remediaron 17 vulnerabilidades más en comparación con el mes de noviembre. Este aumento se vio reflejado gracias a las sesiones que se llevaron a cabo con los especialistas de ICETEX.

El balance final de la gestión se presenta a continuación:

Severidad	Saldo de Vulnerabilidades por Remediar Noviembre	Resultado escaneo Diciembre	Total de Vulnerabilidades a Diciembre	Vulnerabilidades Remediadas en Diciembre	Saldo de Vulnerabilidades por Remediar Diciembre
Critica	79	1	80	2	78
Alta	117	2	119	7	112
Media	667	24	691	4	687
Baja	264	27	291	4	287
Total	1127	54	1181	17	1164

Ilustración 40 Balance final de Gestión de vulnerabilidades.

Actualmente se registra un total de 1201 vulnerabilidades, de las cuales 37 han sido remediadas, lo que representa una efectividad del 3,08 %. Este bajo porcentaje se explica principalmente porque una parte significativa de las vulnerabilidades corresponde a plataformas y tecnologías sin soporte, cuya remediación

requiere procesos de migración. Dichos procesos demandan un plan de trabajo estructurado, que incluya organización, tiempos definidos y actividades de sensibilización, dado que los servidores afectados soportan procesos críticos para la operación.

4.3.4.2. Actividades de PENTEST

Durante el presente periodo, de acuerdo con el otro sí No 3 suscrito, se efectuaron los ejercicios con los siguientes resultados:

4.3.4.3. Actividades de PENTEST WEB

El análisis general de hallazgos [Informe Pentesting URLs ICETEX Diciembre.pdf](#) presenta una visión consolidada de las vulnerabilidades identificadas durante el proceso de pruebas de penetración. En esta sección se agrupan los resultados más relevantes, clasificándolos según su nivel de criticidad y el impacto potencial sobre la confidencialidad, integridad y disponibilidad de la información.

Las URL's, evaluadas, fueron:

- <https://www.icetex.gov.co/nuevalinea/home.asp?modulo=medianoplazo&file=resultados>
- <http://icetexbpmn1/icetexDev/App/inicio/login.aspx?redirect=http://icetexbpmn1/icetexdev/default.aspx>
- <https://web.icetex.gov.co/atencion-al-ciudadano/centros-de-experiencia-presencial-cep>

El escaneo de vulnerabilidades realizada a las URLs detectó un total de 38 vulnerabilidades: 2 de severidad alta, 13 de severidad media y 23 de severidad baja. A continuación, se detallan las vulnerabilidades por URLs.

URL	Criticas	Altas	Medias	Baja
https://www.icetex.gov.co/nuevalinea/home.asp?modulo=medianoplazo&file=resultados	0	1	8	10
http://icetexbpmn1/icetexDev/App/inicio/login.aspx?redirect=http://icetexbpmn1/icetexdev/default.aspx	0	0	1	2
https://web.icetex.gov.co/atencion-al-ciudadano/centros-de-experiencia-presencial-cep	0	1	4	11

Tabla 20 Resultado Escaneo Vulnerabilidades URL's

El balance de estos hallazgos se resume a continuación:

- Los portales de autenticación no tienen una limitación en los intentos de acceso, lo que permite a un atacante probar un número ilimitado de combinaciones de usuario y contraseña en un corto periodo de tiempo.
- Software y complementos desactualizados.
- En los portales de inicio de sesión se identificó que no están sanitizado correctamente las entradas.
- Ausencia de cabeceras de seguridad.
- Pese a que se cuenta con cookies de sesión, estas no están complementadas con atributos como

HttpOnly o Secure.

- Ninguno de los dominios web tiene vulnerabilidades Cross site Scripting, debido a que los mecanismos de seguridad como el WAF, salvaguarda de este tipo de ataques, es importante integridad de los sitios web y los servidores.
- Debilidades en los mecanismos de identificación y autenticación de usuarios en una aplicación web. Esto puede incluir contraseñas débiles, falta de protección contra ataques de fuerza bruta o vulnerabilidades en el proceso de recuperación de contraseñas.
- Se identificó la divulgación de información técnica sensible, incluyendo versiones del servidor, marcas de tiempo Unix y errores de la aplicación que podrían ser aprovechados por atacantes para perfilar los sistemas.
- Se utilizan librerías y frameworks con versiones obsoletas, las cuales tienen vulnerabilidades conocidas que podrían permitir ataques de XSS.

Se recomienda:

- Aplicar cabeceras HTTP de seguridad faltantes (CSP, HSTS, X-Content-Type-Options) configuradas desde el servidor.
- Ocultar rutas, nombres de archivos internos y, sobre todo, sustituir el parámetro cedula por un token de sesión único o un identificador opaco (UUID) que no revele información del usuario en la URL.
- Trasladar el control de tiempo de vida de la sesión exclusivamente al lado del servidor.
- Eliminar el código de detección de navegadores antiguos para permitir la implementación de medidas de seguridad que estos visualizadores no soportan (como TLS 1.3).
- Configurar bloqueos temporales de cuentas tras un número definido de fallos para mitigar ataques de fuerza bruta.
- Integrar CAPTCHA o reCAPTCHA en todos los formularios de inicio de sesión para prevenir accesos automatizados.
- Asegurar el uso estricto de HTTPS para evitar la interceptación de credenciales en tránsito.
- Migrar librerías a sus versiones más recientes y soportadas para corregir vulnerabilidades conocidas.

4.3.4.4. Actividades de PENTEST SERVIDORES

En lo que concierne a ejercicios de PENTEST de servidores se concertaron con el ICETEX, el ataque a los servidores con las siguientes IP's:

- 192.168.51.178
- 192.168.51.175
- 192.168.51.180
- 10.1.18.42

▪ 10.1.18.33

Antes de iniciar el análisis, se llevó a cabo una fase de reconocimiento para mapear la superficie de los servidores, centrándose en la recopilación de información para identificar tecnologías, servicios y posibles vectores de ataque y puertos abiertos.

Destacan patrones comunes en la exposición de riesgos, posibles vectores de ataque recurrentes y áreas de mayor atención dentro de la infraestructura evaluada. Este análisis permite priorizar esfuerzos de mitigación y sirve como base para la toma de decisiones estratégicas en materia de seguridad de la información.

URL	Criticas	Altas	Medias	Baja	Informativa
192.168.51.178	0	0	3	1	37
192.168.51.175	0	0	3	1	35
192.168.51.180	1	0	5	2	41
10.1.18.42	0	0	0	0	35
10.1.18.33	0	0	0	0	27

Tabla 21 Resultado Escaneo Vulnerabilidades Servidores

Los resultados se presentan a continuación:

El análisis refleja que la organización presenta fallas estructurales de seguridad tanto a nivel de infraestructura como de aplicaciones web, con múltiples vulnerabilidades críticas que podrían ser encadenadas por un atacante para lograr un compromiso total del entorno. La falta de cifrado, el uso de versiones de software vulnerables o sin soporte y la inexistencia de controles robustos contra ataques web indican una postura de seguridad débil, que no se alinea con las buenas prácticas ni con marcos de referencia como OWASP Top 10 y NIST. De mantenerse estas condiciones, el impacto potencial incluye pérdida de información confidencial, interrupción de servicios, acceso no autorizado y afectación reputacional.

Se recomienda implementar de manera prioritaria SSL/TLS fuerte, deshabilitando protocolos inseguros y forzando el uso de versiones modernas y certificados válidos. Es fundamental actualizar o parchear FortiOS a una versión no vulnerable y validar la mitigación del CVE-2024-21762, así como migrar o actualizar los sistemas Windows sin soporte a versiones mantenidas por el fabricante. En el ámbito de aplicaciones web, se deben aplicar controles contra CSRF mediante tokens antifalsificación y fortalecer la validación y sanitización de entradas para mitigar XSS, incluyendo políticas Content Security Policy (CSP). Finalmente, se aconseja restringir o filtrar respuestas ICMP, aplicar controles de firewall, realizar pruebas de seguridad periódicas y establecer un plan de gestión de vulnerabilidades continuo que incluya monitoreo, parches y concienciación de seguridad.

En el documento [Informe Pentesting Servidores ICETEX Diciembre.pdf](#) se puede consultar con mayor detalle los hallazgos aquí descritos

4.3.5. Reporte De IPS

En el análisis del informe se identifican dos firmas críticas: `SSL.Anonymous.Ciphers.Negotiation` y `React.Server.Components.react-flight.Remote.Code.Execution`. La primera se observa desde diferentes direcciones IP, pero las asociadas no presentan otros indicadores ni reportes adicionales, lo que podría sugerir un falso positivo.

Se recomienda realizar una verificación del servidor con IP 192.168.51.73 para confirmar si los servicios implementados requieren el uso de cifrados anónimos. En caso de que no sean necesarios, se debe bloquear la firma siguiendo las directrices del fabricante (si se desea bloquear seguir el siguiente documento del fabricante:

<https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-SSL-Anonymous-Ciphers-Negotiation-in-IPS-log/ta-p/317987>).

Esta validación es fundamental para evitar vulnerabilidades relacionadas con cifrados débiles que podrían comprometer la confidencialidad de las comunicaciones.

Por otro lado, la firma `React.Server.Components.react-flight.Remote.Code.Execution` presenta un riesgo alto, está asociada al CVE-2025-55182 (para más información: <https://www.cve.org/CVERecord?id=CVE-2025-55182>) y afecta componentes de React Server que permiten ejecución remota de código. El informe relaciona tres IP públicas (151.115.91.13, 38.54.13.232 y 203.145.44.183) que, aunque muestran indicadores de compromiso negativos, deben ser tratadas como potencialmente maliciosas debido a la criticidad de la vulnerabilidad. Se recomienda validar las publicaciones y servicios expuestos que interactúan con estas IP, y posteriormente bloquearlas en los controles perimetrales. Adicionalmente, se debe aplicar la firma en los perfiles IPS para robustecer la detección y bloqueo de intentos de explotación. Para más detalles sobre la firma: <https://www.fortiguard.com/encyclopedia/ips/59644>

4.3.6. Arquitectura de Seguridad

De conformidad con el plan de trabajo presentado y aprobado el pasado mes de septiembre:

	Actividad	Fecha
1	Planeación y levantamiento de información	9 de septiembre
2	Diagnóstico de la Arquitectura Actual (AS-IS)	3 de Octubre de
3	Definición de la Arquitectura Objetivo (TO-BE)	14 de Noviembre
4	Validación y ajustes	28 de noviembre
5	Socialización y cierre	19 de diciembre

Tabla 22 Plan de Trabajo-Arquitectura de Seguridad

Durante el presente periodo, se efectuó la sesión de socialización y cierre, el pasado 16 de diciembre, ante

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 vicepresidente de operaciones de la entidad y su equipo de apoyo a la supervisión, dando por cerrado todo el plan de trabajo.

4.3.7. Plan de Continuidad

Durante el presente periodo, se adelantaron las fases 4, 5 y 6 del plan previsto, presentando los siguientes entregables:

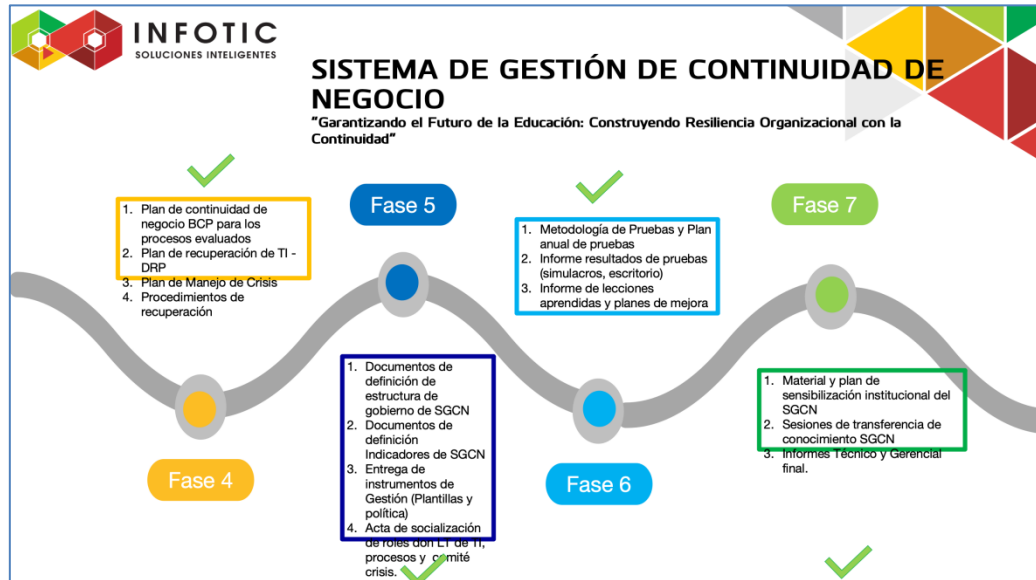


Ilustración 41 Sistema de Gestión de Continuidad de Negocio

El pasado 16 de diciembre, ante el vicepresidente de operaciones de la entidad y su equipo de apoyo a la supervisión, se efectuó la sustentación de dichos entregables y se procedió a dar una explicación gerencial del balance de la consultoría.

Los entregables se encuentran en los siguientes anexos:

- Fase4 Documentacion_Plan_Continuidad_Negocio.zip
- Fase5_Documentacion_Implementacion_Modelo_SGCN.zip
- Fase6_Validacion_Pruebas_Simulacros.zip

4.4. Servicios de nube

Durante diciembre de 2025 se avanzó de manera significativa en la consolidación, aseguramiento y optimización de la infraestructura cloud del ICETEX en Microsoft Azure. Las actividades realizadas se orientaron principalmente a reducir riesgos de seguridad, mejorar la confiabilidad operativa, optimizar recursos existentes y garantizar la correcta puesta en marcha de nuevos entornos.

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 materia de seguridad, se corrigió una vulnerabilidad crítica en reglas de seguridad de red (NSG) que permitía accesos irrestrictos a máquinas virtuales productivas. Esta intervención redujo de forma directa la superficie de exposición del entorno y alineó la operación con buenas prácticas de seguridad recomendadas por Microsoft.

A nivel de continuidad operativa y protección de datos, se optimizaron los servicios de backup, corrigiendo configuraciones que generaban alertas recurrentes sin impacto real, eliminando políticas obsoletas y asegurando la ejecución de respaldos útiles con retención efectiva. Esto permitió mejorar la capacidad de recuperación ante incidentes y disminuir costos asociados a configuraciones inactivas.

Se logró además el despliegue satisfactorio del entorno cloud para el proyecto ABACOS, incluyendo cómputo, seguridad perimetral, base de datos administrada y conectividad controlada, dejando listo el entorno para validaciones y pruebas funcionales. De forma complementaria, se realizaron ajustes sobre el monitoreo centralizado en Azure Monitor y Log Analytics, depurando recursos sin uso y validando configuraciones de retención y SKU para optimizar costos y mejorar visibilidad operativa.

En términos financieros, diciembre evidenció una reducción relevante del gasto mensual en Azure (-57.2 % respecto a noviembre), impulsada por la normalización de cargas de cómputo y la reducción de consumos extraordinarios en máquinas virtuales registrados el mes anterior. El almacenamiento continúa siendo el principal centro de costo, reflejando una operación estable sin comportamientos atípicos.

Finalmente, se dio continuidad al assessment integral del entorno Azure, revisando aspectos clave como seguridad, respaldos, monitoreo, conectividad y arquitectura, proceso que continuará en el siguiente periodo para consolidar un plan de mejoras estructurales.

Impacto del periodo:

- Fortalecimiento de la seguridad perimetral y mitigación de riesgos críticos.
- Mayor estabilidad en continuidad operativa mediante políticas de backup eficaces.
- Optimización del gasto mensual, retornando la suscripción a niveles controlados.
- Despliegue seguro y funcional de nuevos servicios cloud para el negocio.
- Mejor visibilidad operativa y reducción de recursos innecesarios.

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 diciembre del 2025 del proyecto, se encuentra en la fase de operación de los servicios contemplados en el alcance llevando ejecutados 31 meses que equivale al 86,11% de avance,

para lo cual INFOTIC presenta:

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

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 BOLSA NO EJECUTADO 2023	VALOR NO EJECUTADO 2023
\$ 31.398.996.857,96	\$7.856.847.477	\$5,550,653,552.00	\$360,000,000	\$2,700,000	\$357,300,000	\$2,303,493,925.00
	VALOR VIGENCIA 2024	VALOR EJECUTADO 2024	VALOR BOLSA VIGENCIA 2024	VALOR BOLSA EJECUTADO 2024	VALOR BOLSA NO EJECUTADO 2024	VALOR NO EJECUTADO 2024
	\$10,466,332,286.04	\$ 8,888,383,619	\$480,000,000	\$0	\$480,000,000	\$1,587,413,017.00
	VALOR VIGENCIA 2025	VALOR EJECUTADO 2025	VALOR BOLSA VIGENCIA 2025	VALOR BOLSA EJECUTADO 2025	VALOR BOLSA NO EJECUTADO 2025	VALOR NO EJECUTADO 2025
	\$13,237,277,006.00	\$11.403.285.245	\$480,000,000	\$420,000,000	\$60,000,000	\$1.833.991.761,12
	VALOR VIGENCIA 2026	VALOR EJECUTADO 2026	VALOR BOLSA VIGENCIA 2026	VALOR BOLSA EJECUTADO 2026	VALOR BOLSA NO EJECUTADO 2026	VALOR NO EJECUTADO 2026
	\$2,618,949,159.00	0	\$120,000,000	0		0
OTROSI-Adición Servicios	ITEM1 Arquitectura de Seguridad	ITEM2 Gestion de Vulnerabilidades	ITEM3 Pruebas de Pentesting	ITEM4 Continuidad		
\$ 2.761.480.370	\$ 762.253.015	\$275.243.152	\$208.285.884	\$1.515.698.319		Valores Totales
	Fase1: \$85.079.733	\$68.810.788	\$52.071.471	Fase 0: \$79.796.152		
	Fase 2: \$287.192.343			Fase 1: \$94.418.303		
	Fase 3: \$253.506.908			Fase 2: \$ 299.128.428		
	Fase 4: \$85.079.733			Fase 3: \$ 269.884.125		
	Fase 5: \$51.394.298			Fase 4: \$ 240.639.821		
				Fase 5: \$211.395.517		
				Fase 6: \$167.529.063		

				Fase 7: \$152.906.910		
Licenciamiento Liferay	\$420.000.000					Mes de septiembre 2025
CONCEPTO						VALOR
VALOR TOTAL DEL CONTRATO Inicial						\$ 31,398,996,857.96
OTROSI-Adición Servicios						\$ 2.761.480.370
VALOR TOTAL DEL CONTRATO						\$ 34,160,477,227.96
VALOR PAGADO						
Pago No. 1 -	mes:	Abril	de	2023	\$ 537.090.736,00	\$ 20,628,979,988.10
Pago No. 2 -	mes:	Mayo	de	2023	\$ 544.104.546,00	
Pago No. 3 -	mes:	Junio	de	2023	\$ 596.978.314,00	
Pago No. 4 -	mes:	Julio	de	2023	\$ 624.431.841,60	
Pago No. 5 -	mes:	Agosto	de	2023	\$ 650.825.466,00	
Pago No. 6 -	mes:	Septiembre	de	2023	\$ 661.959.450,00	
Pago No. 7 -	mes:	Octubre	de	2023	\$ 641.792.285,00	
Pago No. 8 -	mes:	Noviembre	de	2023	\$ 633,094,717.00	
Pago No. 9 -	mes:	Diciembre	de	2023	\$ 663.076.196,00	
Pago No. 10 -	mes:	Enero	de	2024	\$ 681.934.328,00	
Pago No. 11 -	mes:	Febrero	de	2024	\$ 732,950,102.00	
Pago No. 12 -	mes:	Marzo	de	2024	\$ 733.890.372,09	
Pago No. 13 -	mes:	Abril	de	2024	\$ 730,351,368.00	
Pago No. 14 -	mes:	Mayo	de	2024	\$ 719,104,204.57	
Pago No. 15 -	mes:	Junio	de	2024	\$ 713,673,218.00	
Pago No. 16 -	mes:	Julio	de	2024	\$ 751,372,731.00	
Pago No. 17 -	mes:	Agosto	de	2024	\$755,684,192.00	
Pago No. 18 -	mes:	Septiembre	de	2024	\$ 752,502,515.00	
Pago No. 19 -	mes:	Octubre	de	2024	\$ 770,522,532.00	
Pago No. 20 -	mes:	Noviembre	de	2024	\$ 774,178,154.00	
Pago No. 21 -	mes:	Diciembre	de	2024	\$ 772,219,902.00	
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	
Pago No.30 -	mes:	Septiembre	de	2025	\$ 769,683,313.00	
Pago No. 30 -	mes:	Septiembre	de	2025	\$420,000,000	Contrato Inicial*
Pago No. 1 -	mes:	Septiembre	de	2025	\$120,882,259.89	Bolsa
Pago No. 31 -	mes:	Octubre	de	2025	\$782,805,080.00	OTROSI-Adición Servicios**
Pago No.2 -	mes:	Octubre	de	2025	\$120,882,259.89	Contrato Inicial*
Pago No.32 -	mes:	Noviembre	de	2025	\$ 779,487,583	OTROSI-Adición Servicios**
Pago No. 3 -	mes:	Noviembre	de	2025	\$594,225,142	Contrato Inicial*
Pago No. 4 -	mes:	Diciembre	de	2025	\$1.305.083.859	OTROSI-Adición Servicios**
Pendiente Pago No.33 -	mes:	Diciembre	de	2025	\$ 776.077.366	Contrato Inicial*
VALOR CAUSADO QUE NO SE HA PAGADO (valor a pagar factura) *						\$ 776.077.366
VALOR TOTAL EJECUTADO (valor pagado + valor causado no pagado)						\$ 25.845.022.416
SALDO DEL CONTRATO (valor total del contrato – valor total ejecutado)						\$ 8.315.454.812
PORCENTAJE DE EJECUCIÓN						75,66%

* 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 23 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 Johan Cardozo – Apoyo DBA	Informe Mensual InfoTIC DBA Diciembre2025.pdf
Especialista Web Máster	Juan Carlos Martinez	Informe Mensual InfoTIC Webmaster Diciembre2025.pdf
Especialista Integrador de nube	Carlos Barrera	Informe Mensual InfoTIC Webmaster Diciembre2025.pdf
Especialistas de Seguridad	Jhon Alveiro Pava González Edwin Morales	Informe Mensual InfoTIC Seguridad Diciembre2025.pdf
Especialistas de soluciones	Jose Francisco Escobar Escorcia Davis Alexander Mogollón Fandiño	Informe Mensual InfoTIC Administrador de Soluciones Diciembre2025.pdf
Especialista de Networking	Carlos Alberto Roldan Ríos Victor Manuel Castiblanco Sanchez - Apoyo Networking	Informe Mensual InfoTIC Administrador de Redes Diciembre2025.pdf
Líder Red Team	Luis Alfonso Rodriguez	Informe Pentesting URLs ICETEX Diciembre.pdf Informe Pentesting Servidores ICETEX Diciembre.pdf Plan de Remediación Vulnerabilidades ICETEX V8.pdf Matriz Remediación de Vulnerabilidades ICETEX V3.xlsx Resultados Escaneo de Vulnerabilidades Srv Diciembre 2025.pdf Resumen Gerencial ICETEX Diciembre.pdf
Consultoría Arquitectura de Seguridad	Sonia Constanza Villamil	Arquitectura Seguridad TOBE para el ICETEX 1.4.pdf Presentación Infotoc consultoría ARQ TOBE 1.0.pptx
Consultoría BCP	Mario Cifuentes Zarta	Presentación Fases 5-6-7 ConsultoriaSGCN INFOTIC Dic2025.pptx Fase2 Entregables Fase3 Escenarios y Estrategias de Continuidad Fase5 Documentación Implementación Modelo SGCN

Perfiles	Especialistas	Anexo
		Fase6 Validación Pruebas Simulacros Fase7 GestionProyecto ApropiaciónICETEX

Tabla 24 Perfiles y Actividades

El siguiente es el grupo administrativo que estuvo en el desarrollo de la operación del mes de diciembre 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 25 Grupo Administrativo

8. SERVICIO DE COLABORACIÓN

Durante el mes de diciembre, 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 movible por lo tanto no se puede especificar su piso de ubicación.	1
SEDES REGIONALES				
4	Sala de video conferencia o sala virtual (Tamaño 55")	Bogotá - Chapinero	Calle 57 No. 8-69 Local 46 - 48 y 50	1
5	Sala de video conferencia o sala virtual (Tamaño 55")	Barranquilla	Calle 70 #53-74 piso 3	1
6	Sala de video conferencia o sala virtual (Tamaño 55")	Bucaramanga	CR 29 # 45 - 45, Ofi. 703	1
7	Sala de video conferencia o sala virtual (Tamaño 55")	Cali	Calle 5 No. 66B - 67, Centro Cultural El Capitolio – Piso 3	1
8	Sala de video conferencia o sala virtual (Tamaño 55")	Medellín	Calle 52 No. 47-42 Piso 10 Ofi. 1002	1

Tabla 26 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.

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

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 Ictex.

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 componentes de cada módulo que se encuentra 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.
- Disponibilidad de atención a requerimientos que surjan 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 Diciembre2025.pdf](#)

Para el periodo de diciembre del presente año, comprendido entre el 1 y el 31 del mes, en las sedes Regionales (Cali, Barranquilla, Bucaramanga, Medellín y Chapinero) no se recibieron solicitudes especiales que requirieran atención y gestión de soporte técnico, tampoco se reportaron incidencias a nivel del servicio para estas sedes durante el periodo, sin embargo, como en cada periodo, se contó con la disponibilidad para recibir cualquier solicitud de soporte (Incidencia/requerimiento) o apoyo concerniente a la solución de videoconferencia desplegada y puesta en funcionamiento.

Para el periodo comprendido entre el 1 y el 31 de diciembre, para las sedes de Bogotá Aguas y Ángel, 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. La solicitud de gestión interna de ingreso a la entidad para la visita técnica frecuente se realizó mediante el caso RF-320775-8-24861.

9. GESTION DE RIESGOS Y PROBLEMAS

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

- Matriz de riesgos

Se adjunta la matriz de riesgo y 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 compartida	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 liberada 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 42 Matriz de riesgos

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 [Matriz de riesgos ICETEX.xlsx](#).

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 27 Nivel de Riesgo

➤ Tabla de grado de riesgo

COLOR	NIVEL DE RIESGOS
Verde	Riesgo Aceptable
Amarillo	Riesgo Tolerable
Naranja	Riesgo Alto
Rojo	Riesgo Extremo

Tabla 28 Grado de riesgo

10. INDICADORES CLAVE DE DESEMPEÑO

10.1. ANS por Disponibilidad de canales de comunicaciones

Durante el mes de diciembre 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 Diciembre 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 diciembre: [ANS Diciembre 2025.xlsx](#)

Sede	Categoría	INR	%MES
BOGOTAD.C.	Principal/FO (Sede Aguas)	INR0037	100,00%
	Backup /FO (Sede Aguas)	INR0036	100,00%
	Principal/IPVPN (Sede Chapinero)	INR0022	100,00%
	Backup /IPVPN (Sede chapinero)	INR0020	100,00%
	Principal/IPVPN (Angel)	INR0272	76.37%
	Backup /IPVPN (Angel)	INR0273	98.67%
IBAGUE	Principal/IPVPN	INR0073	100,00%
	Backup/IPVPN	INR0076	100,00%
LETICIA	Principal/Satelital	INR0000373	99,61%
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	99.74%
	Backup/IPVPN	INR0084	100,00%
ARMENIA	Principal/IPVPN	INR0074	99.96%
	Backup/IPVPN	INR0072	99.96%
MANIZALES	Principal/IPVPN	INR0088	99,93%
	Backup/IPVPN	INR0087	99,99%
MEDELLIN	Principal/IPVPN	INR0133	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
	Backup/IPVPN	INR0132	99,95%
APARTADO	Principal/IPVPN	INR0144	99,98%
PEREIRA	Principal/IPVPN	INR0079	99,96%
	Backup/IPVPN	INR0077	99,93%
QUIBDO	Principal/IPVPN	INR0014	99,97%
	Backup/IPVPN		
BARRANQUILLA	Principal/IPVPN	INR0103	100,00%
	Backup/IPVPN	INR0100	99,97%
CARTAGENA	Principal/IPVPN	INR0109	99,37%
	Backup/IPVPN	INR0107	99,37%
MONTERIA	Principal/IPVPN	INR0080	99,95%
	Backup/IPVPN	INR0081	99,97%
RIOHACHA	Principal/IPVPN	INR0164	98,98%
	Backup/IPVPN	INR0162	98,51%
SANTAMARTA	Principal/IPVPN	INR0154	99,68%
	Backup/IPVPN	INR0152	99,96%
SINCELEJO	Principal/IPVPN	INR0095	99,99%
	Backup/IPVPN	INR0097	99,6%
SAN ANDRES	Principal/IPVPN	INR0000367 INR0000369	85,09%
BARRANCABERMEJA	Principal/IPVPN		
SANGIL	Principal/IPVPN		
BUCARAMANGA	Principal/IPVPN	INR0062	100,00%
	Backup/IPVPN	INR0061	100,00%
CUCUTA	Principal/IPVPN	INR0044	99,59%
	Backup/IPVPN	INR0047	99,58%
VALLEDUPAR	Principal/IPVPN	INR0091	99,64%
	Backup/IPVPN	INR0090	99,64%
YOPAL	Principal/IPVPN	INR0121	98,57%
	Backup/IPVPN	INR0123	100,00%
ARAUCA	Principal/IPVPN	INR0110	99,99%
CALI	Principal/IPVPN	INR0151	100,00%
	Backup/IPVPN	INR0153	100,00%
BUENAVENTURA	Principal/IPVPN	INR0051	100,00%
MOCOA	Principal/IPVPN	INR0135	99,99%
	Backup/Satelital	INR0136	99,95%
PASTO	Principal/IPVPN	INR0130	100,00%
	Backup/IPVPN	INR0131	99,71%
POPAYAN	Principal/IPVPN	INR0035	100,00%
	Backup/IPVPN	INR0032	99,84%
TUMACO	Principal/IPVPN	INR0147	99,21%
DCTRIARA	MPLSPP	INR0266	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. 53*-26 Arboleda
 Alta.
 NIT: 900.068.796-1
 Teléfono: (+606) 88612612

Sede	Categoría	INR	%MES
	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		
	Backup/IPVPN		
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	99,99%
DECEVAL hasta Edificio de ICETEX Dirección General	Ubicado en Data center Principal. Interconectado a través de red MPLS (Backup)	INR0000318	100,00%
Salida del portal https://portal.icetex.gov.co/portalywww.icetex.gov.co/haciainternetencentrodecomputoprincipal	Internet Reverso para Portales	INR0000320	100,00 %
Salida del portal https://portal.icetex.gov.co/portalywww.icetex.gov.co/haciainternetencentrodecomputodecontingencia	Internet Reverso para Portales	INR0274	0 %
DCTRIARA	Allot Centralizado 800M Triara(equipo)	INR0270	100,00 %

Tabla 29 Disponibilidad de Canales

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

Sede	Categoría	INR	% Mes
BARRANQUILLA	INTERNET PARA LA GENTE	INR0094	100,00%
BUCARAMANGA	INTERNET PARA LA GENTE	INR0057	100,00%
CALI	INTERNET PARA LA GENTE	INR0160	100,00%
AGUAS	INTERNET PARA LA GENTE	INR0029	100,00%
CHAPINERO	INTERNET PARA LA GENTE	INR0015	100,00%
MEDELLIN	INTERNET PARA LA GENTE	INR0122	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	INTERNET PARA LA GENTE	INR0140	99,97%
ARAUCA	INTERNET PARA LA GENTE	INR0115	99,99%
LETICIA	INTERNET PARA LA GENTE	INR0000378	99,97%
QUIBDO	INTERNET PARA LA GENTE	INR0021	99,97%
RIOHACHA	INTERNET PARA LA GENTE	INR0159	100,00%
SAN ANDRES	INTERNET PARA LA GENTE	INR0000368	85,09%
YOPAL	INTERNET PARA LA GENTE	INR0127	92,67%
MOCOA	INTERNET PARA LA GENTE	INR0141	99,99%

Tabla 30 Disponibilidad canales "Internet para la gente"

10.1.1. Canal de Replicación (Triara – Megacenter)

El proyecto tiene asignado un canal 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 diciembre continúa su funcionamiento correctamente sin novedades que afectaran la prestación del servicio. La evidencia se encuentra en el [Reporte Monitoreo ICETEX Diciembre2025-ELK.pdf](#) y en el archivo de [Disponibilidad Server ELK Diciembre 2025.xlsx](#)

10.2. ANS por Disponibilidad de servidores

La herramienta utilizada para el monitoreo de la disponibilidad de servidores es ELK y el informe correspondiente que permite la revisión de los ANS es la [Disponibilidad Server ELK Diciembre 2025.xlsx](#)

No	COD.	Etiquetas de fila	Disponibilidad
1	INR0000322	ictsrvctrldoc	100,00%
2	INR0226	mira	100,00%
3	INR0228	ictxisgesbd	100,00%
4	INR0229	ictxisgesapp	100,00%
5	INR0233	icetexboglخورف1.localdomain	100,00%
6	INR0234	ictxprusisgapp	100,00%
7	INR0235	ictxbogsrvpt2 **	100,00%
8	INR0236	ictxbogsrvpt1**	100,00%
9	INR0237	icetexboglobserver1-r*	100,00%
10	INR0238	icetexbogliferaynfs	99,88%
11	INR0239	icetexbogelasticserver1	99,97%
12	INR0240	icetexbogelasticserver2	99,97%
13	INR0241	icetexbogelasticserver3	99,97%
14	INR0242	icetexbogliferayserver2	99,97%
15	INR0243	icetexbogliferayserver1	99,97%
16	INR0244	icetexboglxdarumasrv1	100,00%
17	INR0245	icetexboglxdarumasrv2	100,00%
18	INR0246	icetexboglxdarumatest	100,00%
19	INR0247	preprodsec	100,00%

No	COD.	Etiquetas de fila	Disponibilidad
20	INR0248	icetexboglxxroad3	100,00%
21	INR0249	xroadsec	100,00%
22	INR0250	qasec	100,00%
23	INR0251	INR0251_INFOTIC	99,99%
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	99,96%
33	INR0262	icetexboglخورفو2.localdomain	100,00%
34	INR0276	cxvodaprodn011	100,00%
35	INR0277	cxvodaprodn021	100,00%
36	INR0278	cxvodacontg011	100,00%

Tabla 31 Códigos relacionados Disponibilidad Servicios en Housing – Datacenter Principal

******Los servidores (icetxbogsrvpt1 y icetxbogsrvpt2) en el mes de diciembre 2024 se solicitó por parte del ICETEX dar de baja y distribuir sus recursos en los servidores de OPENSIFT, dicha solicitud quedó aplicada la cierre del mes de diciembre, por lo tanto no se visualizaran a partir del mes de enero de 2025 en el Reporte de disponibilidad, sin embargo para efectos de facturación se continúan teniendo en cuenta tal como se acordó, evidencia de la solicitud en el documento: [Baja de servidores - Actualización OpenShift incremento de RAM.pdf](#)

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 2025.

Como resultado de esta medida, este servidor dejó de aparecer en el Reporte de Disponibilidad a partir de agosto, no obstante, el servidor sigue facturándose. En el mes de diciembre se asignaron los recursos de memoria en el servidor Nodo 2 de Portal Icetex.

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

#	Dispositivo	Marca	Modelo
5	FORTISANDBOX	Fortinet	1000D
6	Cisco 3650X	Cisco	WS-C3650-48TQ
7	Cisco 3560X SW	Cisco	WS-C3650-48TQ
8	Switch DELL Networking	Dell	N4032 24 ports
9	Controladora SAN Dell Compellent	Dell	SC8000
10	Controladora SAN Dell Compellent	Dell	SC8000
11	Enclosure Discos SAN	Dell	EN-SC200
12	Enclosure Discos SAN	Dell	EN-SC220
13	Enclosure Discos SAN	Dell	EN-SC200
14	Enclosure Discos SAN	Dell	EN-SC220
15	Enclosure Discos SAN	Dell	EN-SC220
16	Enclosure Discos SAN	Dell	EN-SC200
17	Enclosure Dell Blade – Principal 5 Servidor – Blade M1000, 6 IOM Slot B2 -Tarjeta Enclosure - M1000	Dell	M1000E

Tabla 32 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 diciembre un **UPTIME del [99.823%]** tal como se evidencia en la gráfica a continuación.

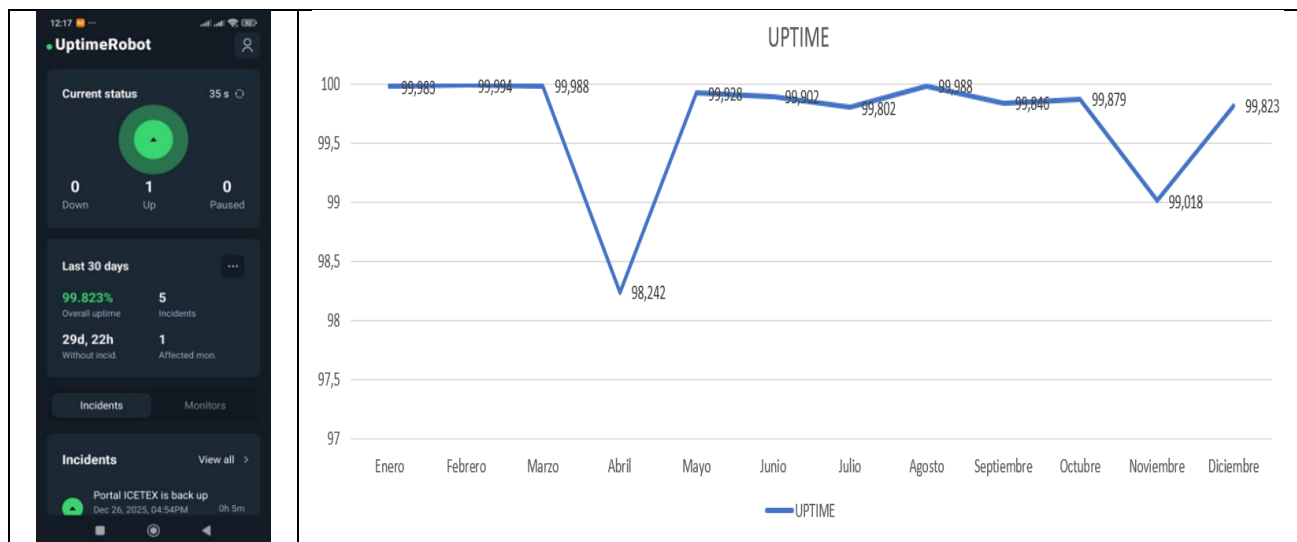


Ilustración 43 UPTIME – Portal WEB web.ICETEX.gov.co

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

	Septiembre	Octubre	Noviembre	Diciembre
Usuarios activos mes	526.000	422.000	408000	565000
Usuarios nuevos	408.000	291.000	283000	393000

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

	Septiembre	Octubre	Noviembre	Diciembre
Tiempo de interacción (seg)	91	65	122	123

Tabla 33 Distribución trimestral de acceso por usuarios

El portal WEB cuenta con un total de 565 mil usuarios, con 393 mil usuarios nuevos. El tiempo de interacción medio es de 1 minutos y 3 segundos, señalando el interés de la audiencia en las diferentes páginas del portal web.icetex.gov.co.

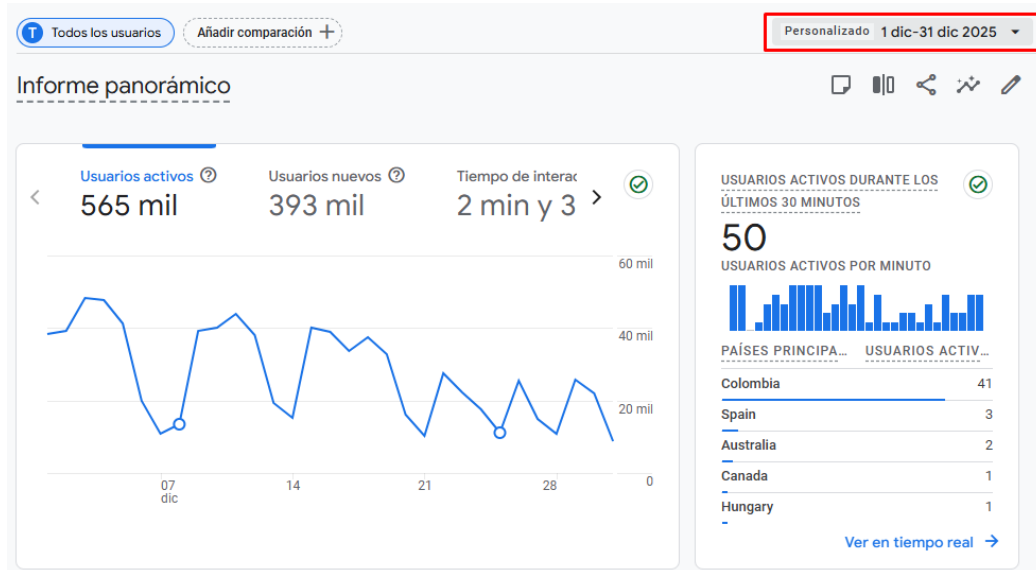


Ilustración 44 Métrica de visitantes Portal WEB web.ICETEX.gov.co

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

Adquisición de usuarios: Primer grupo de canales principal del usuario ... Personalizado 1 dic-31 dic 2025

Incluir en gráfico Q Buscar... Filas por página: 10 Ir a: 1 1-10 de 12

	Primer grupo de...redeterminado	Total de usuarios	Usuarios nuevos	Usuarios recurrentes	Tiempo de interacción medio por usuario activo	Sesiones con interacción por usuario activo	Número de eventos Todos los eventos
☒ Total		594.331 100 % respecto al total	392.686 100 % respecto al total	290.339 100 % respecto al total	2 min y 36 s Media 0 %	1,45 Media 0 %	8.972.219 100 % respecto al total
☒ 1 Organic Search		354.573 (59,66 %)	217.415 (55,37 %)	193.095 (66,51 %)	2 min y 59 s	1,56	5.950.746 (66,32 %)
☒ 2 Direct		207.928 (34,99 %)	145.844 (37,14 %)	86.304 (29,73 %)	2 min y 02 s	1,24	2.655.267 (29,59 %)
☒ 3 Organic Social		20.924 (3,52 %)	19.018 (4,84 %)	3.222 (1,11 %)	43 s	0,72	135.745 (1,51 %)
☒ 4 Referral		13.986 (2,35 %)	9.267 (2,36 %)	6.370 (2,19 %)	2 min y 55 s	1,39	213.782 (2,38 %)
☒ 5 Unassigned		778 (0,13 %)	669 (0,17 %)	164 (0,06 %)	1 min y 27 s	1,02	7.406 (0,08 %)
☐ 6 Email		260 (0,04 %)	189 (0,05 %)	116 (0,04 %)	1 min y 56 s	1,15	3.126 (0,03 %)
☐ 7 Organic Video		156 (0,03 %)	80 (0,02 %)	82 (0,03 %)	2 min y 52 s	1,65	2.547 (0,03 %)
☐ 8 Paid Search		134 (0,02 %)	55 (0,01 %)	69 (0,02 %)	2 min y 41 s	1,22	1.799 (0,02 %)
☐ 9 Paid Social		109 (0,02 %)	90 (0,02 %)	12 (<0,01 %)	21 s	0,29	501 (<0,01 %)
☐ 10 Paid Other		85 (0,01 %)	52 (0,01 %)	43 (0,01 %)	1 min y 09 s	1,40	1.215 (0,01 %)

Ilustración 45 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.

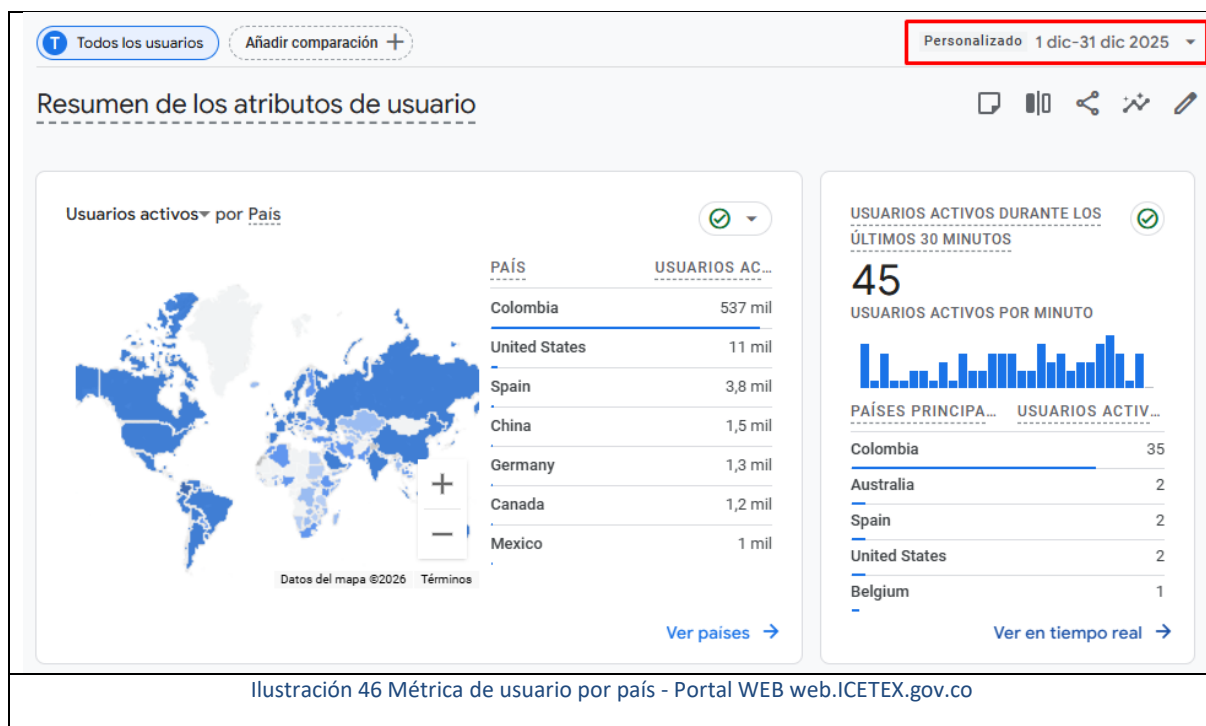
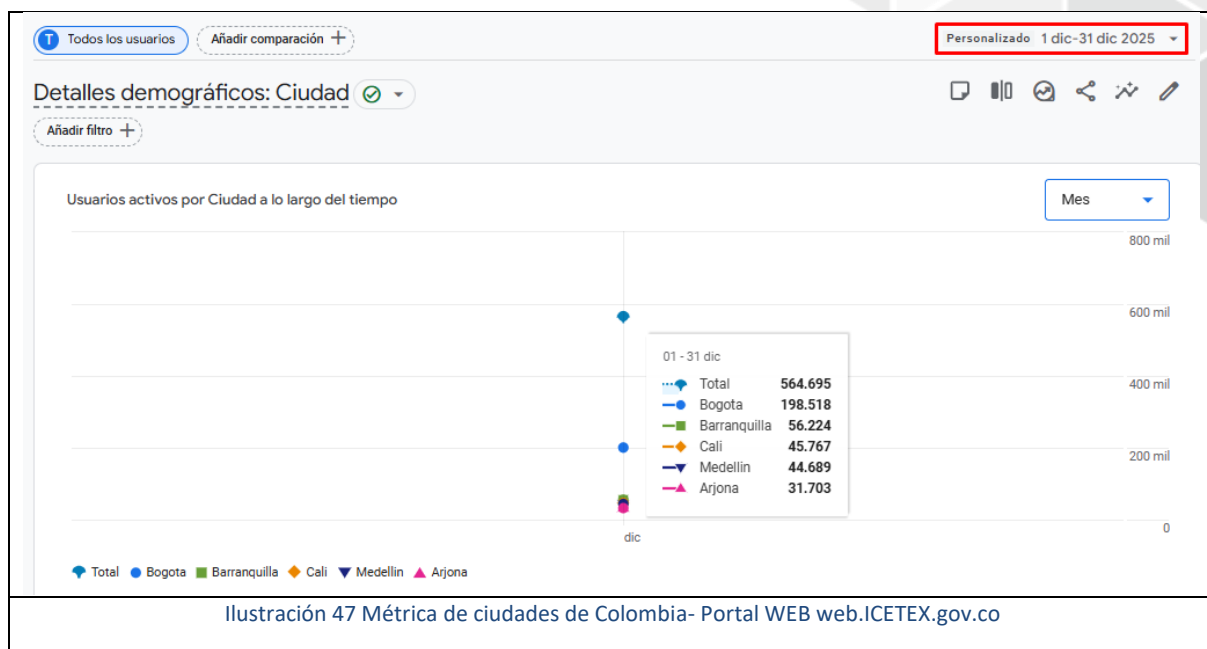


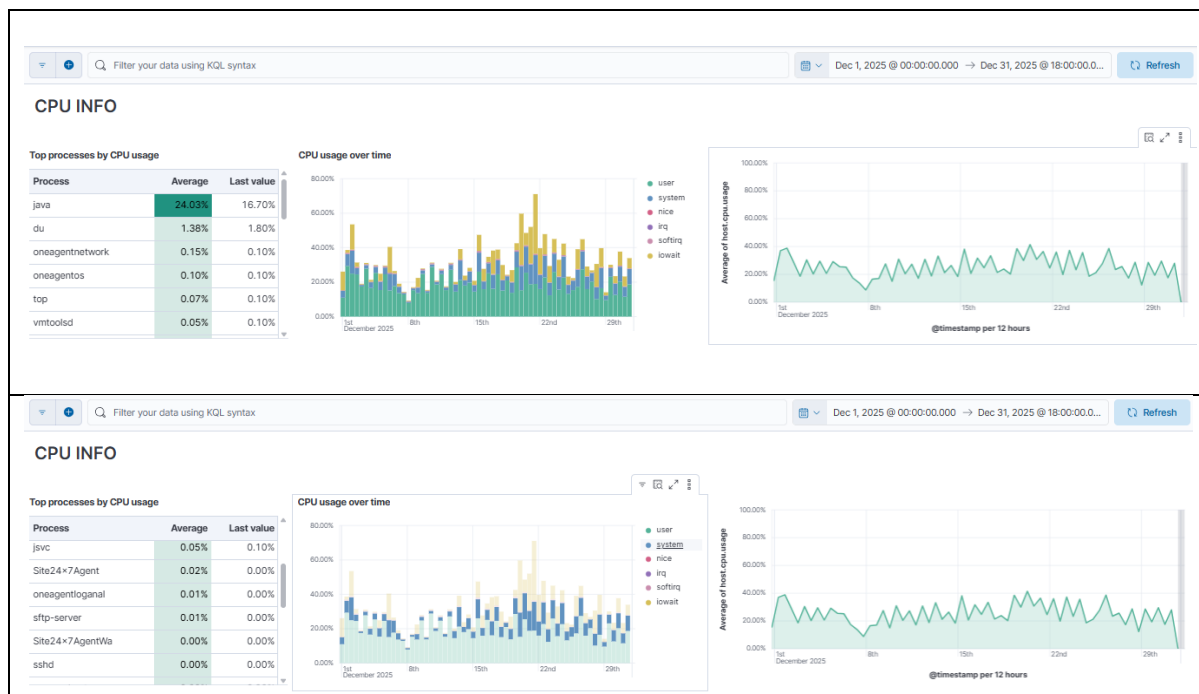
Ilustración 46 Métrica de usuario por país - Portal WEB web.ICETEX.gov.co

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



A continuación, se muestran las gráficas referentes a memoria RAM y almacenamiento en los nodos 1 y 2 del portal ICETEX desde el 1 de diciembre desde las 00:00 horas hasta las 23:59 horas del 31 de diciembre de 2.025



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

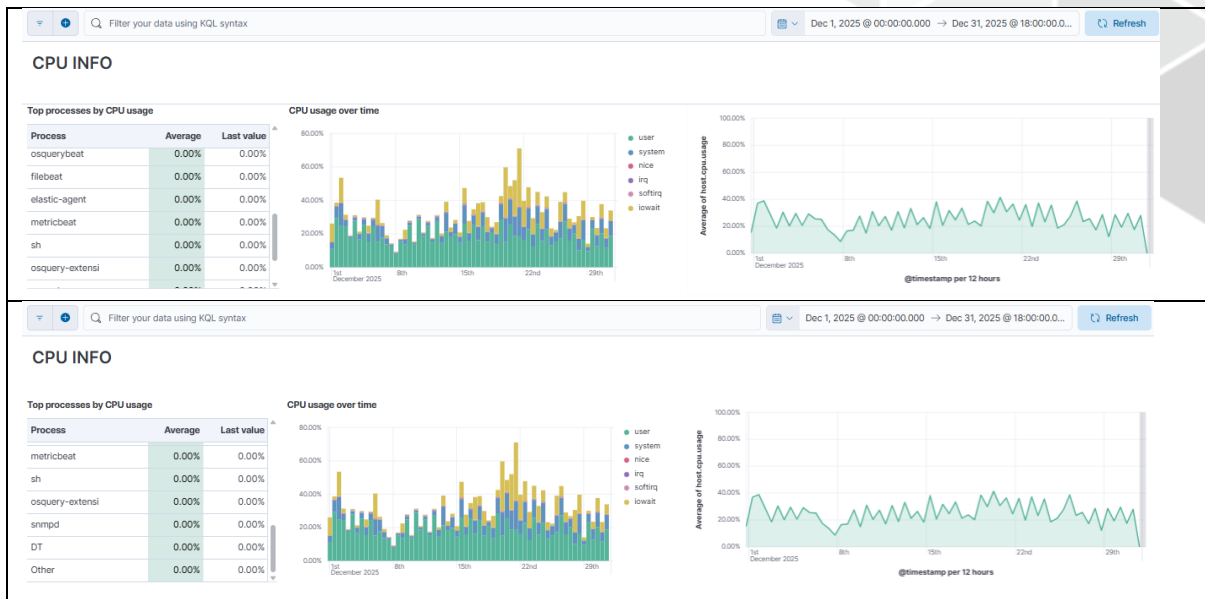


Ilustración 48 NODO 1 CPU

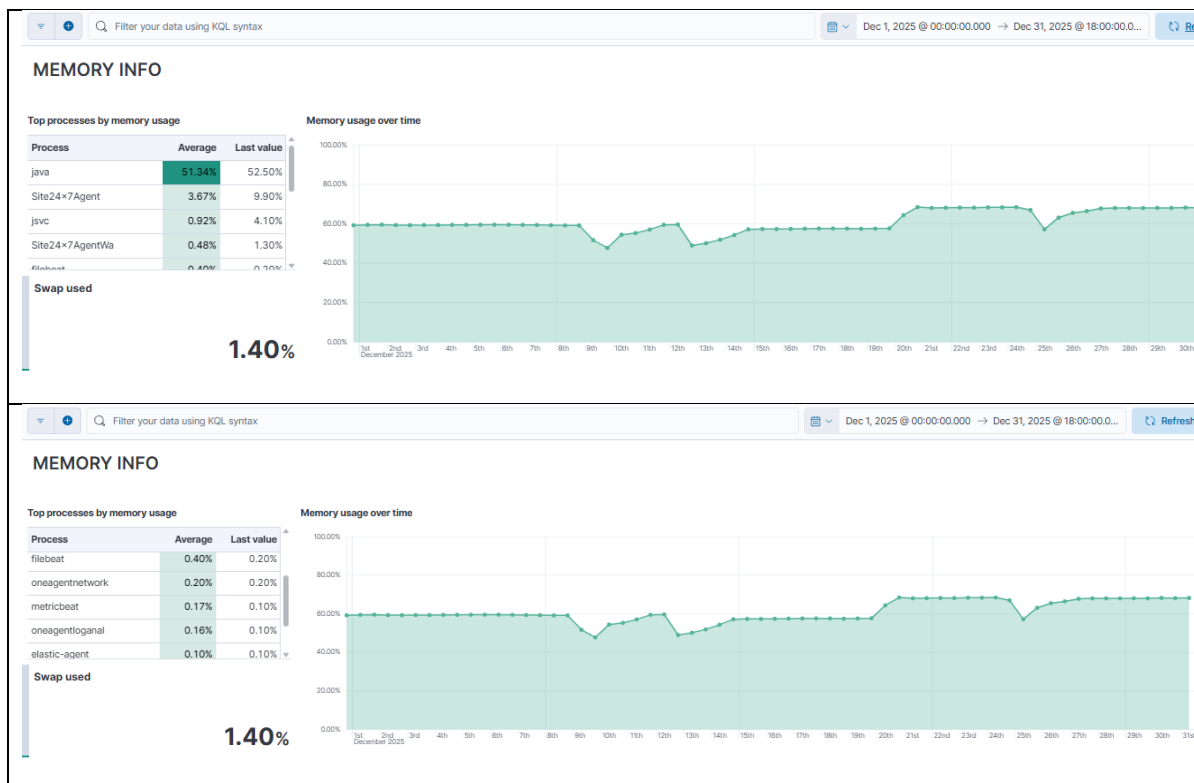




Ilustración 49 NODO 1 Memoria

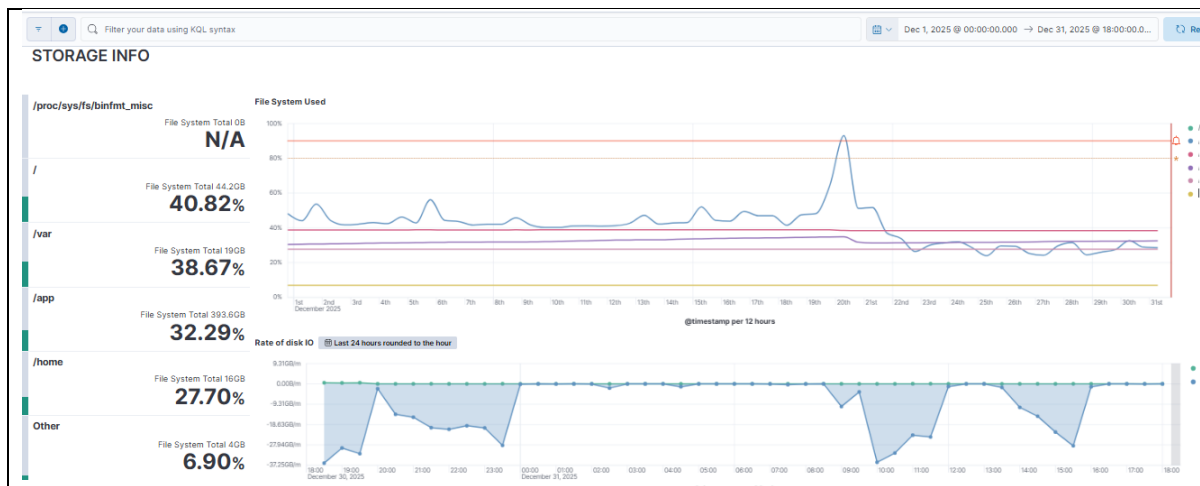


Ilustración 50 NODO 1 Almacenamiento

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 [Informe Mensual InfoTIC Webmaster Diciembre 2025.docx](#).

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.

Se recomienda ampliar el almacenamiento de la partición raíz / de los tres nodos del Elasticsearch debido a identificación en los logs en indisponibilidades presentadas en el servicio indica que se encuentra con un escaso espacio en disco, esta ampliación le daría mayor estabilidad al funcionamiento de los tres nodos de Elasticsearch.

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

10.2.3. Backup Servidores Triara

Durante el periodo de diciembre se realizaron los Backups de acuerdo con las políticas definidas por el ICETEX, las cuales desde su inicio se implementaron en el Datacenter. Se puede verificar en el documento [Informe Backups mes de Diciembre 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 Mensual de Backups diciembre 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 Icetex V3.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 finales del mes, ICETEX realizó la adquisición de cintas de backup necesarias para llevar a cabo el almacenamiento y traslado a custodia externa, se encuentra en proceso la coordinación con el Operador la devolución de 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 Vise	303
Librería	32
Nuevo Custodia	60
Total	395 cintas

Tabla 34 Cintas Backups ICETEX

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

Resumen de Tarea de Respaldo

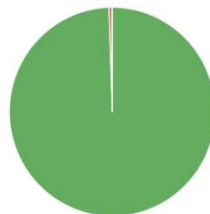
Generated on: Jan 1, 2026, 8:03 am

Informe del Resumen de Tarea del Backup

CommCell	All
Company	All
Server groups	INFOTIC
Servers	All
App types / Workloads	All
Subclients	All
Job status	En ejecución, Completado, Retraso, Fallido, Completado con Errores, Completado con Advertencias
Job types	All
Time frame	Última 4 Semanas (Dec 4, 2025, 08:03:14 AM - Jan 1, 2026, 08:03:14 AM)
Time zone	CommServ
Hora de Inicio de Día	12:00 AM
Snap and Backup Copy options	All
Advanced	All
Agents	All
Número máximo de trabajos a devolver	4000

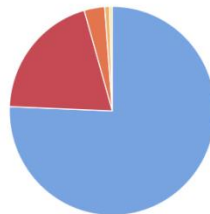
Ilustración 51 Evidencia Backup servidores resumen general Backups

Estado de Tarea



Completed : 3621 (99.51 %)
Failed : 16 (0.44 %)
Completed with errors : 2 (0.05 %)

Tareas por tipo de app / carga de trabajo



Oracle RAC : 2753 (75.65 %)
VMware vCenter : 726 (19.95 %)
Windows Server : 117 (3.22 %)
Linux Server : 28 (0.77 %)
SQL Server : 15 (0.41 %)

Ilustración 52 Evidencia Backup servidores resumen Backups y su estado

El total del tamaño de la información respalda para el mes de diciembre corresponde a 233.96 TB, donde 99.51% se completó en el primer lanzamiento del robot con un total de 233.57 TB de información.

El 75.65% 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 3639 trabajos analizados, el 99,56% se completó con éxito (incluyendo los que tuvieron errores menores). El 99.51% de todos los trabajos se completaron sin ningún error.

- Tasa de éxito: 99.56 % (trabajos completados o completados con errores)
- Tasa de fracaso: 0.44% (trabajos fallidos o cancelados)
- Oracle RAC: El 75.65% de los trabajos de respaldo corresponden a este tipo de servidor, con un total de 2753 trabajos.
- VMware vCenter: El 19.95% de los trabajos pertenecen a este entorno, con 726 trabajos.
- Otros Servidores: Los trabajos de Windows Server, Linux Server y SQL Server representan el 3.22%, 0.77% y 0.41% 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 todos los soportes y evidencias de la ejecución de las políticas de Backup, la política actualizada y vigente de la toma de Backup, se encuentra en el link del repositorio [Backup Diario](#) y el informe de Backups en la carpeta [Informe de Backup](#)

11. CONTROL DE CAMBIOS

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

No. Cambio	Alcance	Fecha De Creación	Fecha De Ejecución	Resultado	Observaciones
1236	El cambio aplica a los siguientes servidores que tienen instalado Windows Server 2019 Standard: ICTXS R VM OODLE (192.168.51.82): aloja la aplicación ComunidadICETEX (https://comunidad.icetex.gov.co/ComunidadicetexFront/inicio), publicada en internet y accedida por usuarios externos. ICTXS R VAPPM IX3 (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.	18/12/2025	20/12/2025	Exitoso	2025-12 Cumulative Update for Windows Server 2019 for x64-based Systems (KB 5071544)
1237	El cambio aplica a los siguientes servidores en entorno de producción: • ICTXS R VNET COR 01 (192.168.51.165) aloja las aplicaciones PS E, Cargue Archivos, Cuentas Abandonadas, Cuentas Inactivas,	18/12/2025	20/12/2025	Exitoso	2025-12 Cumulative Update for Windows Server 2016 for x64-based Systems

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

No. Cambio	Alcance	Fecha De Creación	Fecha De Ejecución	Resultado	Observaciones
	PortalTransaccional y Transunion, las cuales están publicadas en internet y accedidas por usuarios externos. • ICTXS R VAPPM IX1 (192.168.51.134) : aloja las aplicaciones internas Desembolsos, R eporteador, Servicios de Integración MEN, Censo Indígena, S isbén, Vigía e Icfes, utilizadas para procesos institucionales críticos. • I CTXS R VDCVAL01 (192.168.51.170): aloja la aplicación Deceval, esencial para la integración con servicios financieros externos.				(K B 5071543). 2025-12 Cumulative Update for Windows Server 2019 for x64-based Systems (K B 5071544)
1230	Migración SDWAN	15/12/2025	15/01/2026	Pendiente	Fue aprobado en el comité del 17/12/2025 para su ejecución en enero 15 a 22 2026
1257	Implementar filtrado por dirección MAC (MAC Filtering)	15/12/2025	17/12/2025	Exitoso	Se implementa un esquema de filtrado por dirección MAC (MAC Filtering) en el servicio DHCP de Windows Server, con el fin de restringir la asignación de direcciones IP únicamente a dispositivos previamente autorizados.

Tabla 35 Controles de cambio diciembre

12. PLAN DE TRABAJO DE LOS PROXIMOS MESES

A continuación, se presenta el avance de cada uno de los temas y de los que se requiera se definirá un 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	31-03-2026	Esta situación implica riesgos críticos tanto a nivel de seguridad como de continuidad operativa, entre los que se destacan: - Falta de actualizaciones de seguridad críticas. - Mayor exposición a vulnerabilidades y ataques cibernéticos. - Incompatibilidad con software y hardware actualizado. - Ausencia de soporte oficial por parte del

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
				fabricante.
Verificar la configuración de los equipos de LAN y WAN que hace falta para el funcionamiento de IPv6.	ICETEX	01-12-2024	31-03-2026	INFOTIC ha culminado su etapa de pruebas y configuración. El proyecto queda pendiente de las validaciones funcionales por parte del ICETEX. Reanudaremos el seguimiento en cuanto se confirme el inicio de dichas pruebas.
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	31-03-2026	Se programará la desinstalación de Symantec y la migración al antivirus Falcon, conforme a las ventanas de mantenimiento y disponibilidad que defina el ICETEX.

Tabla 36 Planes de trabajo

13. PLAN DE ENTREGA

Mediante el memorando **VOP-463-2025**, radicado el 19 de diciembre, se remite la propuesta del plan de entrega del **Contrato 0792-2022**.

[VOP 463-2025 Asunto- Remisión propuesta plan de entrega – Contrato 0792-2022.pdf](#)

14. RECOMENDACIONES DEL CONTRATISTA AL ICETEX

14.1. 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 Andrés, 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

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

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.

14.2. 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

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

del servidor ICTXSRVNETCOR01, correspondiente a los meses de agosto, septiembre y diciembre de 2025, seguido de observaciones y recomendaciones:

Disco	Métrica	Jul-25	ago-25	sep-25	Observaciones	Recomendaciones
C:	Espacio usado	65% (66.6 GiB)	58% (58.1 GiB)	69% (68.97 GiB)	Se incrementó el uso en almacenamiento en comparación con el mes anterior en aproximadamente 11 GiB.	Considerar mover archivos no esenciales a otro volumen que dispongan desde el lado de infraestructura hacia almacenamiento secundario.
	Espacio libre	33.3 GiB	41.4 GiB	30.54 GiB		
F:	Espacio usado	92% (1.74 TiB)	95% (1.80 TiB)	96% (1.90 TiB)	Altísima ocupación constante (>90%), aunque mejora en septiembre debido al aumento del almacenamiento en 100GB	Urgente implementar políticas de depuración de archivos antiguos o inactivos. Considerar expansión del volumen o migración de datos a almacenamiento secundario.
	Espacio libre	146 GiB	89.4 GiB	72.91 GiB		
E:	Espacio usado	79% (51.7 GiB)	65% (42.5 GiB)	88% (57.08 GiB)	Aún se mantiene en zona de riesgo por encima del 80%.	Considerar mover archivos no esenciales a otro volumen que dispongan desde el lado de infraestructura hacia almacenamiento secundario. Considerar expansión del volumen si requieren almacenar por mucho más tiempo los logs de las aplicaciones
	Espacio libre	13.3 GiB	22.4 GiB	7.92 GiB		

Ilustración 53 Histórico consolidado uso de discos servidor ICTXSRVNETCOR01

14.3. Seguridad

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.

14.4. Bases De Datos

Considerando el aumento en los espacios del área de recuperación del entorno de producción, se requiere escalar de manera equivalente la base de datos de réplica.

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.

14.5. Integrador De Nube

Se recomienda continuar con el plan de depuración de las configuraciones. Desde los últimos 2 meses se ha podido avanzar en estos aspectos.

- Se lograron avances sólidos en la optimización, ordenamiento y fortalecimiento de la infraestructura Microsoft Azure – ICETEX, consolidando un entorno productivo más organizado, seguro y alineado con buenas prácticas Cloud.
- Las actividades ejecutadas fortalecieron la gobernanza mediante la depuración de redes y grupos de recursos huérfanos, el ajuste de reglas NSG y el redimensionamiento de la VNet vm-app-home-vnet.
- La instrumentación de alertas preventivas y el aprovisionamiento de almacenamiento especializado mejoraron la observabilidad, permitiendo monitoreo oportuno de servicios críticos.
- La Reserva de Instancia aplicada a la VM vm-devops-agent representa un avance clave en eficiencia financiera, asegurando ahorros relevantes en el horizonte operativo.
- La documentación técnica consolidada para Datafondos refuerza la trazabilidad y asegura continuidad operativa bajo estándares de seguridad.
- La Solicitud Especial – Microsoft – ÁBACOS marca el inicio formal de la etapa de diseño y dimensionamiento del micrositio y plataforma educativa a migrar hacia ICETEX.
- El mes de diciembre representó un progreso importante hacia la madurez operativa y de gobernanza del entorno Azure institucional, sentando bases para fases futuras de automatización, control de costos y consolidación arquitectónica.

15. EVIDENCIAS DE VALOR AGREGADO ENTREGADO POR INFOTIC

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

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

15.1. 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 diciembre 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.

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

Para el periodo de reporte se reporta, la ejecución de la segunda capacitación de seguridad el pasado **28 de diciembre de 2025**, correspondiente al segundo año del contrato.

Se continuará con la programación de la capacitación correspondiente al año 3 del contrato de acuerdo con la disponibilidad de agenda de los equipos de trabajo del ICETEX, aspecto que se concertará con la supervisión del contrato.

15.3. TB de capacidad de almacenamiento

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

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

Tabla 37 Capacidades de almacenamiento contratado

Aprovisionado se tienen las siguientes capacidades instaladas:

EJECUTADO		
TRIARA	ALMACENAMIENTO APROVISIONADO (TB)	Evidencia
Almacenamiento MVs VMware	49,6	RV Tools
Almacenamiento MVs KMV (BD)	10,9	RF1700669
TOTAL	60,5	
MEGACENTER	ALMACENAMIENTO APROVISIONADO (TB)	Evidencia
Almacenamiento MVs replicación VMware	19,4	RVTools
Almacenamiento MVs KMV (BD)	10,9	RF1700669

TOTAL	30,3	
TOTAL, ALMACENAMIENTO APROVISIONADO	90,8	

Tabla 38 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.

En el almacenamiento aprovisionaron 3 TB como valor agregado de INFOTIC para realizar la prueba de restauración de Backups, durante el mes de diciembre realizaron las siguientes pruebas de restauración:

Código de Servicio	Hostname	Tipo de restauración	Fecha backup restaurado	Fecha restauración	prueba	Resultado	Evidencia
INR0243	icetexbogliferaerver1	full backup	4/12/2025	10/12/2025		Exitoso	INR0243

Tabla 39 Pruebas de Restauraciones de Backups de Diciembre

15.4. “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.

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 40 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 41 WIFI para la gente pendientes

16. 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.

17. ANEXOS

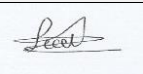
Tema	SubTema	Anexo
Almacenamiento	Backups Diarios	Backups diarios diciembre 2025 (31 reportes) Backup Diario
	Informe de Backups	Consolidado mensual Backups diciembre2025 Consolidado Mensual de Backups diciembre 2025.pdf Informe Backups mes de Diciembre 2025.pdf Politica Backup Ictetex V3.xlsx
Aplicaciones	Informes de actividades	Informe actividades Módulos videoconferencia ICETEX diciembre2025 Informe actividades Módulos videoconferencia ICETEX Diciembre2025.pdf Informe mensual Administrador de Soluciones diciembre2025 Informe Mensual InfoTIC Administrador de Soluciones Diciembre2025.pdf Informe mensual Administrador Web Master diciembre2025 Informe Mensual InfoTIC Webmaster Diciembre 2025.docx Informe mensual Integrador Nube diciembre2025 Informe Mensual InfoTIC Integrador de Nube Diciembre 2025.pdf
Arquitectura de Seguridad		Informe de Arquitectura AS-IS de Seguridad de la Información V. 1.4 Arquitectura Seguridad TOBE para el ICETEX 1.4.pdf Presentación Infotoc consultoría_ARQ_TOBE_1.0 Presentación Infotoc consultoría_ARQ_TOBE 1.0.pptx
Bases De Datos		Informe mensual Administrador de Bases de datos diciembre2025 Informe Mensual InfoTIC DBA Diciembre2025.pdf
Ejecución Presupuestal		Conciliación diciembre consolidado Conciliación Diciembre consolidado.xlsx Informe de Gestión Servicio diciembre2025 Informe de Gestion Servicio Diciembre 2025.pdf Informe de Gestion Servicio Diciembre 2025.docx
Informe Pentest		Informe Pentest Informe Pentesting URLs ICETEX Diciembre.pdf

Tema	SubTema	Anexo
		Informe Pentesting Servidores ICETEX Diciembre.pdf Plan de Remediación Vulnerabilidades ICETEX V8.pdf Matriz Remediación de Vulnerabilidades ICETEX V3.xlsx Resultados Escaneo de Vulnerabilidades Srv Diciembre 2025.pdf Resumen Gerencial ICETEX Diciembre.pdf
Informes Plan de Continuidad		Informes Plan de Continuidad Presentación Fases 5-6-7 ConsultoriaSGCN INFOTIC Dic2025.pptx Fase2_Entregables: 01. Matriz de riesgos consolidada de procesos evaluados.pptx 01. Metodología Evaluación de Riesgos Icetex.docx 02. Informe BIA consolidado procesos priorizados.docx 02. Metodología BIA ICETEX.docx 03. Matriz interdependencias procesos evaluados .xlsx 04. Informe de Impactos potenciales para atender en corto plazo.docx Fase3 Escenarios y Estrategias de Continuidad: 1. Matriz Escenarios de alternativas de Continuidad para procesos priorizados y evaluados.xlsx 2. Informe de recomendación de estrategia de continuidad.docx 3. Documento de la estrategia seleccionada por ICETEX.docx Fase5_Documentación_Implementación_Modelo_SGCN: 1. Documento de definición de estructura de gobierno de SGCN.docx 2. Documento definición de Indicadores.docx 3. Entrega de Instrumentos de Gestión.docx 4. Acta Socialización de roles.docx Fase6_Validación_Pruebas_Simulacros: 1. Metodología de Pruebas y Plan anual de pruebas.docx 2. Informe resultados de pruebas (simulacros - escritorio).docx 3. Informe de lecciones aprendidas y planes de mejora.docx Fase7_GestionProyecto_ApropiaciónICETEX: 1. Material y plan de sensibilización institucional del SGCN.docx 2. Sesiones de transferencia de conocimiento SGCN.docx 3. Informe Técnico Gerencial Final - SGCN.docx
Seguridad		Informe Mensual MARCA-OSINT ICETEX diciembre Informe Mensual MARCA-OSINT ICETEX Diciembre 2025.pdf Informe Mensual Seguridad diciembre2025 Informe Mensual InfoTIC Seguridad Diciembre2025.pdf Informe Mensual SOC - ICETEX diciembre2025 Informe Mensual SOC-TH ICETEX Diciembre 2025.pdf Informe técnico análisis de vulnerabilidades ICETEX diciembre2025 WX INFORME TECNICO AV ICETEX Diciembre.pdf

Tema	SubTema	Anexo
		WX Matriz de Vulnerabilidades ICETEX Diciembre.xlsx Reporte de IPS diciembre2025 Reporte de IPS de Diciembre infotic 2025.pdf
Soporte Y Monitoreo	Canales	ANS diciembre2025 ANS Diciembre 2025.xlsx Informe mensual Administrador de Networking diciembre2025 Informe Mensual InfoTIC Administrador de Redes Diciembre2025.pdf Informe Mensual Disponibilidad diciembre2025 Reporte Mensual Disponibilidad INFOTIC Diciembre 2025.pdf
	Gráficas de consumo	Informe Mensual ALLOT diciembre2025 Graficas de consumo Diciembre 2025 – ALLOT INFOTIC.xls Consumo general mensual 1.1.26 6.00 AM.pdf
Data center Alterno	Replicación	Informe mensual replicación diciembre2025 Informe mensual replicacion Diciembre 2025.pdf Reportes diarios diciembre2025 (27 reportes) Replicaciones
	Prueba DRP	Informes Prueba DRP Informe prueba Aislada DRP Icetex 20251129.pdf Anexo1 Evidencias InformePruebaDRPIcetex 20251129.pdf
Data Center Principal		Reporte Monitoreo ICETEX diciembre2025-ELK Reporte Monitoreo ICETEX Diciembre2025-ELK.pdf Data ELK Disponibilidad Server ELK Diciembre 2025.xlsx
Plan De Entrega De Servicios Al Icetex		Memorando VOP 463-2025 Asunto- Remisión propuesta plan de entrega – Contrato 0792-2022.pdf Plan de Entrega de Servicios PlanEntrega-20251219112923.pdf

Tabla 42 Anexos

Revisión técnica

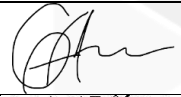
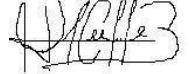
REVISÓ	FIRMAS
SANDRA MILENA GARCIA HERNANDEZ CONTRATISTA GRUPO DE INFRAESTRUCTURA	

 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



INFOTIC
SOLUCIONES INTELIGENTES

JOAO DO NELSON DUCUARA CONTRATISTA GRUPO DE INFRAESTRUCTURA	
GERMAN MANUEL DIAZ CONTRATISTA GRUPO DE INFRAESTRUCTURA	
NELSON JAVIER CASALLAS BELTRAN CONTRATISTA GRUPO DE INFRAESTRUCTURA	
GERMAN AUGUSTO MEJIA CARDONA COORDINADOR DE INFRAESTRUCTURA	

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