



INFORME DE ACTIVIDADES DEL CONTRATO

**CONTRATO NUMERO
2022-0792**

Febrero 01 al 29 de 2024

Contenido

1	INTRODUCCIÓN	5
2	OBJETIVOS	5
3	RESUMEN EJECUTIVO	5
4	SERVICIOS DE CONECTIVIDAD	6
4.1	INTERNET PARA LA GENTE	10
4.2	CANALES SDWAN	10
4.3	Canal de Replicación (Triara – Megacenter)	10
4.4	Señalética (Internet para la gente)	11
4.5	CONCLUSIONES DEL SERVICIO DE CONECTIVIDAD	11
4.6	RECOMENDACIONES DEL SERVICIO DE CONECTIVIDAD	11
5	SERVICIOS CENTROS DE COMPUTO	12
5.1	Datacenter Principal	12
5.1.1	Disponibilidad de Servicios – Datacenter Principal	13
5.1.2	Disponibilidad TRIARA para los servicios de página web	15
5.1.3	Backup Servidores Triara	16
5.2	Datacenter Alterno	17
5.2.1	Hosting Virtual (IaaS)	17
5.2.2	Dataguard BBDD Megacenter	18
5.2.3	Replicación Servicios OnPremise de Icetex a Megacenter	20
5.2.4	Disponibilidad de Servicios de Housing – Datacenter Alterno	20
6	SEGURIDAD	20
6.1	Servicios de Endpoint	20
6.2	ESTADÍSTICAS PORTALES	21
6.3	Estado General de las Plataformas	22
6.4	Estado de Salud de los Equipos de Seguridad	22
6.5	Servicio de centro de Operaciones de Seguridad (SOC)	23
6.5.1	Monitoreo de Marca (SOC)	23
6.6	Eventos Relevantes	24
6.7	RECOMENDACIONES	25
6.8	CONCLUSIONES	25
7	GESTION DE SERVICIO	26
7.1	ACTIVIDADES DE OPERACIÓN	26
7.2	Profesionales Especializados	26
7.2.1	Especialista en Base de Datos DBA	26
7.2.2	Especialista web master	26
7.2.3	Administrador de Soluciones	27
7.2.4	Especialista en Networking	27
7.2.5	Especialista Integrador de nube	27
7.2.6	Especialista en seguridad	28
8	SERVICIO DE COLABORACIÓN	28
8.1	Disponibilidad del servicio – sedes Bogotá (aguas - ángel)	29

8.2	<i>Gestión de incidencias y requerimientos – sedes regionales</i>	29
8.3	<i>Gestión de incidencias y requerimientos – Bogotá (Aguas - Angel)</i>	30
9	Visita a VISE	31
10	CALCULO DE CONCILIACIÓN DE LOS SERVICIOS DEL MES DE FEBRERO	33
	EJECUCIÓN PRESUPUESTAL	33

INDICE DE TABLAS

Tabla 1	Disponibilidad de canales	8
Tabla 2	Canales pendientes por instalar	9
Tabla 3	Canales ampliados febrero 2024	9
Tabla 4	Canales pendientes por ampliar	9
Tabla 5	Disponibilidad canales “Internet para la gente”	10
Tabla 6	Disponibilidad canales “SDWAN”	10
Tabla 7	Estado de la instalación de la señalética de Wifi	11
Tabla 8	Códigos relacionados Disponibilidad Servicios en Housing – Datacenter Principal Sitescope	14
Tabla 9	Códigos relacionados Disponibilidad Servicios en Housing – Datacenter Principal ELK	15
Tabla 10	Disponibilidad de Servicios de Housing – Datacenter Principal	15
Tabla 11	Servicios replicados – Datacenter MEGACENTER	18
Tabla 12	Disponibilidad de Servicios de Housing – Datacenter Alterno	20
Tabla 13	Distribución módulos de videoconferencia por sede	28
Tabla 14	Ejecución Presupuestal	33

INDICE DE ILUSTRACIONES

Ilustración 1 Evidencia del Resumen del Monitoreo 13

Ilustración 2 Promedio Disponibilidad Servicios en Housing – Datacenter Principal Sitescope 13

Ilustración 3 Promedio Disponibilidad Servicios en Housing – Datacenter Principal ELK..... 14

Ilustración 4 Disponibilidad Nodo1 Servicios Portal Web Icetex (Dynatrace) 16

Ilustración 5 Disponibilidad Nodo 2 Servicios Portal Web Icetex (Dynatrace) 16

Ilustración 6 Evidencia Backup Servidores 16

Ilustración 7 Reportes de replicación SRM a Sitio Alterno, febrero 2024..... 17

Ilustración 8 Evidencia Dataguard replicado a Megacenter BD..... 19

Ilustración 9 Evidencia replicado servicios On-premise Icetex a Megacenter 20

Ilustración 10 Evidencia Gráfica Estadísticas de Portales 21

Ilustración 11 Evidencia Estado General de las Plataformas 22

Ilustración 12 Evidencia Estado de Salud de los Equipos de Seguridad..... 22

Ilustración 13 Evidencia Imagen Reporte Monitoreo 23

Ilustración 14 Evidencia Imagen Reporte Monitoreo de Marca 24

Ilustración 15 Recomendaciones plataformas de seguridad 25

Ilustración 16 Disponibilidad de servicio videoconferencia sedes regionales – febrero 2024 29

Ilustración 17 Disponibilidad de servicio videoconferencia sedes Bogotá – febrero 2024 29

Ilustración 18 Incidencias/Requerimientos sedes Regionales – febrero 2024 30

Ilustración 19 Visita Vise-Antecedentes..... 31

Ilustración 20 Visita Vise-Actividades previas 32

Ilustración 21 Visita Vise-Asistentes..... 32

Ilustración 22 Resumen Cintas entregadas en custodia externa a CLARO 33



1 INTRODUCCIÓN

Este informe contiene la información relacionada con las actividades ejecutadas por INFOTIC en el periodo comprendido entre el 01 al 29 de febrero de 2024. Así mismo se relacionan los informes de los siguientes servicios:

- Conectividad y red de comunicaciones
- Servicio de Colaboración
- Centro de Datos
- Servicio de Seguridad
- Persona del Proyecto en Sitio
- Servicios Conexos

El informe de febrero describe los servicios realizados durante el periodo por el equipo de personas con las herramientas tecnológicas apropiadas, dispuestas por INFOTIC para desempeñar las funciones y atender los requerimientos del Ministerio de Educación según lo acordado en el contrato.

2 OBJETIVOS

Presentar el informe de actividades ejecutadas por INFOTIC durante el periodo del 01 al 29 de febrero de 2024, con el fin de determinar el estado, la evolución y disponibilidad de cada una de las gestiones en los diferentes servicios prestados al ICETEX en virtud de la ejecución del contrato, para lo cual se han considerado la recolección de mediciones, el análisis y la producción de informes y reportes periódicos sobre cada una de las gestiones y demás informes especiales sobre los servicios prestados.

3 RESUMEN EJECUTIVO

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

Conectividad: Se continuó con la operación de los canales principales a través del operador Claro, con los anchos de canal requeridos por el ICETEX. Para el mes de febrero se continuo con la ampliación de los anchos de banda de los canales donde INFOTIC en su propuesta económica planteo como adicional a lo contractual, todos con sus respectivas pruebas de saturación.

Servicios de Colaboración: Durante este mes se continuó con el correcto funcionamiento en las distintas sedes del país, sin ninguna novedad.

Centro de Datos: Los servicios del centro de datos funcionaron de forma normal; se realizó la actualización del antivirus varias de las maquinas quedando pendiente las maquinas con sistema operativo Linux.

Servicio de Seguridad: Las herramientas de seguridad operaron sin novedad. Se adelantó el escaneo de vulnerabilidades en las máquinas del ICETEX.

Personal del Proyecto en Sitio: El personal del proyecto operó de manera normal. Los informes de las actividades se adjuntan en el presente informe.

Bolsa para servicios por demanda: En el mes de febrero por parte de Icetex no ha se ha tenido respuesta sobre el tema de las cintas de Backup, el operador Claro continúa realizando la toma y custodia de los Backup

y como consecuencia no se está realizando el traslado a custodia externa.

El presente informe evidencia, además:

- El comportamiento de los canales conforme a los casos reportados en Aranda.
- Reporte que evidencia el rendimiento de la conectividad en términos de capacidad de procesamiento y consumo de recursos durante el mes de febrero del 2024 y la correcta operación de los centros de cómputo tanto principal como el alterno
- Presenta el reporte de monitoreo que se realiza desde los diferentes dispositivos de seguridad que se tienen para la protección de la información de ICETEX.
- Presenta un resumen de las solicitudes escaladas a los ingenieros en sitio con sus respectivas recomendaciones

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

4 SERVICIOS DE CONECTIVIDAD

Durante el mes de febrero, los canales principales y backup instalados operaron de manera normal. La herramienta Solar Winds no esta permitiendo la graficación de los canales INFOTIC ha reportado oportunamente al operador esta incidencia y se está haciendo el seguimiento correspondiente teniendo en cuenta que la gestión de estos casos se encuentra en trámite por parte del operador CLARO para dar solución al tema, aclarando que la data no se ha perdido, no se ha podido graficar.

Los informes de disponibilidad de los canales son monitoreados a través de la herramienta Solarwinds, por su parte los informes de consumo se pueden apreciar en el informe semanal que arroja la herramienta Allot, de acuerdo con el siguiente link:

[Graficas de consumo febrero 2024 - ALLOT INFOTIC.pdf](#)

Durante el mes de febrero se realizó monitoreo del servicio de los canales mediante la herramienta Solarwinds, a través de la cual se obtuvieron los reportes de comportamiento de los canales instalados, de acuerdo con el siguiente link:

[ICETEX febrero 2024.pdf](#)

Sede	Categoría	INR	% Mes
BOGOTA D.C.	Principal / FO (Sede Aguas)	INR0037	99.60%
	Backup / FO (Sede Aguas)	INR0036	100.00%
	Principal / IPVPN (Sede Chapinero)	INR0022	99.95%
	Backup / IPVPN (Sede chapinero)	INR0020	99.95%
	Principal / IPVPN (Angel)	INR0272	100.00%
	Backup / IPVPN (Angel)	INR0273	100.00%
IBAGUE	Principal / IPVPN	INR0073	99.92%
	Backup / IPVPN	INR0076	99.57%
LETICIA	Principal / Satelital		0,00%
NEIVA	Principal / IPVPN	INR0039	100.00%

	Backup / IPVPN	INR0041	100.00%
TUNJA	Principal / IPVPN	INR0104	99.29%
	Backup / IPVPN	INR0106	99.32%
VILLAVICENCIO	Principal / IPVPN	INR0085	93.49%
	Backup / IPVPN	INR0084	93.48%
ARMENIA	Principal / IPVPN	INR0074	99.83%
	Backup / IPVPN	INR0072	100.00%
MANIZALES	Principal / IPVPN	INR0088	100.00%
	Backup / IPVPN	INR0087	99.89%
MEDELLIN	Principal / IPVPN	INR0133	100.00%
	Backup / IPVPN	INR0132	100.00%
APARTADO	Principal / IPVPN	INR0144	99.97%
PEREIRA	Principal / IPVPN	INR0079	97.75%
	Backup / IPVPN	INR0077	98.37%
QUIBDO	Principal / IPVPN	INR0014	99.94%
	Backup / IPVPN		0,00%
BARRANQUILLA	Principal / IPVPN	INR0103	100.00%
	Backup / IPVPN	INR0100	99.89%
CARTAGENA	Principal / IPVPN	INR0109	92.05%
	Backup / IPVPN	INR0107	99.67%
MONTERIA	Principal / IPVPN	INR0080	100.00%
	Backup / IPVPN	INR0081	100.00%
RIOHACHA	Principal / IPVPN	INR0164	99.11%
	Backup / IPVPN	INR0162	99.07%
SANTA MARTA	Principal / IPVPN	INR0154	99.66%
	Backup / IPVPN	INR0152	100.00%
SINCELEJO	Principal / IPVPN	INR0095	100.00%
	Backup / IPVPN	INR0097	100.00%
SAN ANDRES	Principal / IPVPN		0,00%
BARRANCABERMEJA	Principal / IPVPN		0,00%
SAN GIL	Principal / IPVPN		0,00%
BUCARAMANGA	Principal / IPVPN	INR0062	100.00%
	Backup / IPVPN	INR0061	99.93%
CUCUTA	Principal / IPVPN	INR0044	99.94%
	Backup / IPVPN	INR0047	98.94%
VALLEDUPAR	Principal / IPVPN	INR0091	99.83%
	Backup / IPVPN	INR0090	99.83%
YOPAL	Principal / IPVPN	INR0121	99.25%
	Backup / IPVPN	INR0123	100.00%
ARAUCA	Principal / IPVPN	INR0110	99.94%
CALI	Principal / IPVPN	INR0151	97.65%
	Backup / IPVPN	INR0153	100.00%
BUENAVENTURA	Principal / IPVPN	INR0051	100.00%

MOCO A	Principal / IPVPN	INR0135	93.08%
	Backup / Satelital	INR0136	99.38%
PASTO	Principal / IPVPN	INR0130	99.99%
	Backup / IPVPN	INR0131	100.00%
POPAYAN	Principal / IPVPN	INR0035	99.16%
	Backup / IPVPN	INR0032	99.36%
TUMACO	Principal / IPVPN	INR0147	97.15%
WAN general (concentrador total red)	Principal /IPVPN	INR0266	100.00%
WAN general (concentrador total red)	Backup / IPVPN	INR0171	100%
Conectividad dedicada a funciones de réplica para eventos de DRP.	DWDM	INR0224	100%
Canal entre Sitio principal e Ictetex - Dirección General - Aguas	Principal /IPVPN		0%
	Backup / IPVPN		0%
Salida Internet contingencia - Dirección General - Aguas	Ubicado en sede AGUAS interconectado a través de red MPLS		100,00%
Canal entre Sitio contingencia Ictetex - Dirección General - Aguas	Conectividad brindada a través de la red MPLS, con acceso a los dos Datacenter		100,00%
Salida a Internet para toda la WAN desde Bogotá EN CENTRO DE COMPUTO principal	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0034	99.95 %
Salida a Internet para toda la WAN desde Bogotá en CENTRO DE COMPUTO DE CONTINGENCIA	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0230	100.00%
Banco de la Republica hasta Edificio Dirección General ICETEX	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0221	100.00%
DECEVAL hasta Edificio de ICETEX Dirección General.	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0268	23.09%
DECEVAL hasta Edificio de ICETEX Dirección General.	Ubicado en Datacenter Principal, interconectado a través de red MPLS (Backup)	INR0000289	99.84%
Salida del portales https://portal.ictetex.gov.co/portal y www.ictetex.gov.co hacia internet en centro de cómputo principal	Internet Reverso para Portales	INR0000317	99.46%
Salida de los portales https://portal.ictetex.gov.co/portal y www.ictetex.gov.co hacia internet en centro de cómputo de contingencia	Internet Reverso para Portales		0%

Tabla 1 Disponibilidad de canales

A continuación, se listan las sedes sin instalar:

SERVICIO	OBSERVACIONES
Leticia	Sin Sede
Barrancabermeja	Sin sede

San Gil	Sin sede
San Andrés	Canal Principal
Quibdó	Canal de Backup

Tabla 2 Canales pendientes por instalar

En conclusión, se prestó el servicio en las sedes del Ictex brindando conectividad y sin interrumpir la operación del Instituto. Durante el mes de febrero se realizaron 5 ampliaciones y quedan pendientes 13, lo cual significa un 72.34% de las ampliaciones efectivas, en las tablas a continuación se presenta los servicios de conectividad contratados con sus respectivas capacidades ofrecidas y se compara con las cargas prestadas, en el link [Pruebas Saturación Ampliaciones](#) se encuentran las evidencias de las ampliaciones:

CIUDAD	Enlace - Tipo medio	Código Servicio	BW- Mínimo Requerido (MBPS)	Ancho de Banda Ofrecido	Ancho de Banda Prestado	Diferencia (MBPS)
BOGOTA D.C.	Principal / FO (Sede Aguas)	INR0037	370	400	370	30
	Backup / FO (Sede Aguas)	INR0036	160	200	160	40
IBAGUE	Principal / IPVPN	INR0073	18	20	18	2
PEREIRA	Principal / IPVPN	INR0079	18	20	18	2
YOPAL	Principal / IPVPN	INR0121	18	20	18	2

Tabla 3 Canales ampliados febrero 2024

CIUDAD	Enlace - Tipo medio	Código Servicio	BW- Mínimo Requerido (MBPS)	Ancho de Banda Ofrecido	Ancho de Banda Prestado	Diferencia (MBPS)
BOGOTA D.C.	Principal / IPVPN (Sede Chapinero)	INR0022	38	40	38	2
CARTAGENA	Backup / IPVPN	INR0107	8	10	8	2
IBAGUE	Backup / IPVPN	INR0076	8	10	8	2
PEREIRA	Backup / IPVPN	INR0077	8	10	8	2
NEIVA	Principal / IPVPN	INR0039	18	20	18	2
MEDELLIN	Principal / IPVPN	INR0133	63	100	63	37
	Backup / IPVPN	INR0132	15	20	15	5
QUIBDO	Backup / IPVPN	INR0014	18	20	18	2
	Principal / IPVPN	INR0016	8	10	8	2
RIOHACHA	Principal / IPVPN	INR0164	18	20	18	2
BUCARAMANGA	Principal / IPVPN	INR0062	26	30	26	4
CALI	Principal / IPVPN	INR0151	63	100	63	37
	Backup / IPVPN	INR0153	15	20	15	5

Tabla 4 Canales pendientes por ampliar

4.1 INTERNET PARA LA GENTE

Durante el mes de febrero el servicio de Internet para la gente se prestó sin interrupciones en doce de las catorce sedes contratadas, estas son:

Sede	Categoría	INR	% Mes
BARRANQUILLA	INTERNET PARA LA GENTE	INR0094	100.00%
BUCARAMANGA	INTERNET PARA LA GENTE	INR0057	99.93%
CALI	INTERNET PARA LA GENTE	INR0160	97.66%
AGUAS	INTERNET PARA LA GENTE	INR0029	100.00%
CHAPINERO	INTERNET PARA LA GENTE	INR0015	100.00%
MEDELLIN	INTERNET PARA LA GENTE	INR0022	100.00%
APARTADO	INTERNET PARA LA GENTE	INR0140	99.96%
ARAUCA	INTERNET PARA LA GENTE	INR0115	99.90%
LETICIA	INTERNET PARA LA GENTE		0.00%
QUIBDO	INTERNET PARA LA GENTE	INR0021	100.00%
RIOHACHA	INTERNET PARA LA GENTE	INR0159	99.11%
SAN ANDRES	INTERNET PARA LA GENTE		0.00%
YOPAL	INTERNET PARA LA GENTE	INR0127	99.97%
MOCOA	INTERNET PARA LA GENTE	INR0141	93.40%

Tabla 5 Disponibilidad canales "Internet para la gente"

Quedan pendientes 2 instalaciones que son: San Andrés la cual se encuentra en gestión desde que Ictetex informó que ya se cuenta con sede y Leticia donde no se ha podido instalar por falta de sede.

4.2 CANALES SDWAN

Durante el mes de febrero se inició la instalación el servicio de los canales SDWAN con Bogotá y Mocoa, las pruebas de saturación y correspondientes actas de entrega se encuentra en [Pruebas de Saturación-Actas Entrega SDWAN](#)

Sede	Categoría	INR	% Mes
SD WAN AGUAS	SD WAN	INR0033 / 000334	99.94%
SD WAN MOCOA	SD WAN	INR0139 / 000333	99.94%

Tabla 6 Disponibilidad canales "SDWAN"

Está contemplada la instalación de canales SDWAN en las sedes de Leticia y San Andres, San Andrés se encuentra en gestión desde que Ictetex informó que ya se cuenta con sede y Leticia no se ha podido instalar por falta de sede.

4.3 Canal de Replicación (Triara – Megacenter)

Corresponde a los canales de nivel 2 que comunican al Datacenter Principal con el Datacenter Secundario con un ancho de banda de 2Gbps, el cual, durante el mes de febrero, funcionó sin ningún contratiempo.

La evidencia se encuentra en el informe [Replicacion febrero 2024.pdf](#)

4.4 Señalética (Internet para la gente)

Se tiene el siguiente estado en la instalación de la señalética para el uso de la red WIFI en las oficinas:

Ciudad	Fecha Entrega
Barranquilla	14-feb-24
Bucaramanga	14-feb-24
Cali	Pendiente
Bogotá (Aguas)	Pendiente
Bogotá (Chapi)	Pendiente
Medellín	Pendiente
Apartado	29-feb-24
Arauca	20-feb-24
San Andres	Pendiente
Riohacha	20-feb-24
Yopal	21-feb-24
Mocoa	26-feb-24
Quibdó	26-feb-24
Leticia*	Pendiente

Tabla 7 Estado de la instalación de la señalética de Wifi

Leticia* teniendo en cuenta que no hay oficina esta señalética se recibirá en la Oficina de Bogotá sede Aguas.

4.5 CONCLUSIONES DEL SERVICIO DE CONECTIVIDAD

En la operación del mes de febrero:

- Se lograron atender todos los casos y se cerraron en los tiempos establecidos, identificando con respecto al mes anterior una disminución del 70% de los casos escalados lo cual muestra una mayor estabilidad en el servicio.
- Se encuentran pendiente la instalación del canal de Backup de Quibdó y de las 4 sedes donde no había oficina, ya se cuenta con la Oficina de San Andres por lo que se inicia el proceso de instalación de los canales principal, Backup, Internet para la gente y SDWAN.
- Se tiene un avance del 60% de la instalación de las señaléticas.

4.6 RECOMENDACIONES DEL SERVICIO DE CONECTIVIDAD

- De acuerdo con la normatividad vigente se recomienda realizar la renovación de equipos de red de la identidad los cuales en este momento se encuentran obsoletos y sin soporte del fabricante.
- Se recomienda hacer la renovación o cambio de cableado en los diferentes puntos de la identidad ya

que el cableado es muy antiguo y en lo posible hacer una certificación de este.

- Teniendo en cuenta lo que se ha evidenciado del estado de la infraestructura de las sedes, se recomienda hacer el mantenimiento de la infraestructura, así como el cableado y su renovación de equipos de red.

Se adjunta en el repositorio un documento en Excel con el análisis del comportamiento de los canales para el mes de febrero. [Conciliación febrero consolidado.xlsx](#)

5 SERVICIOS CENTROS DE COMPUTO

5.1 Datacenter Principal

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

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

Durante todo el periodo se continuó con el seguimiento permanente de todos los servicios y no se presentaron novedades en la operación. Se genera el reporte desde la herramienta dispuesta en el Datacenter. Ver el informe.

[Report INFORME POR DEMANDA DISPONIBILIDAD Y CAPACIDAD ICETEX Febrero 2024.pdf](#)

[Reporte Monitoreo ICETEX febrero 2024-ELK.pdf](#)

INFORME POR DEMANDA DISPONIBILIDAD Y CAPACIDAD ICETEX America/Bogota 2/1/2024 12:00 AM - 3/1/2024 12:00 AM

PROMEDIO CONSUMO DE CPU

View: month

From: 2/1/2024 12:00 AM

To: 3/1/2024 12:00 AM

America/Bogota

Sample type: ss_hr_t

Nombre de destino	Nombre del monitor	Valor mínimo	Valor máximo	Valor promedio
iceteboglxdarumatest	CPU	0.00	61.00	2.07
icetexbogliferaynfs	CPU	0.00	71.00	1.09
icetexboglxdarumasrv1	CPU	1.00	98.00	4.88
icetexboglxdarumasrv2	CPU	1.00	100.00	2.29
icetexboglxxroad1	CPU	1.00	77.00	3.01
icetexboglxxroad2n	CPU	0.00	12.00	1.44
icetexboglxxroad3	CPU	0.00	13.00	0.66
icetexboglxxroadtest	CPU	1.00	7.00	1.45
ictxprusisgapp	CPU	0.00	82.00	21.34
ictxsisgesapp	CPU	0.00	66.00	14.05
ictxsisgesbd	CPU	0.00	59.00	2.61
inr0233_icetexboglxxorfeo1.localdomain	CPU	0.00	7.00	0.54
inr0237_icetexboglobserver1-r	CPU	0.00	10.00	2.77
inr0239_icetexbogelasticserver1	CPU	0.00	100.00	3.05
inr0241_icetexbogelasticserver3	CPU	0.00	22.00	0.74
inr0242_icetexbogliferayserver2	CPU	0.00	100.00	11.00
inr0243_icetexbogliferayserver1	CPU	1.00	98.00	13.91
inr0262_icetexboglxxorfeo2.localdomain	CPU	0.00	76.00	2.17
inr0276_cxvodaprodn011	CPU	2.00	100.00	64.27
inr0277_cxvodaprodn021	CPU	3.00	100.00	27.48
inr0278_cxvodacontg011	CPU	0.00	61.00	8.75

Ilustración 1 Evidencia del Resumen del Monitoreo

5.1.1 Disponibilidad de Servicios – Datacenter Principal

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

PROMEDIO DE DISPONIBILIDAD		
View: month		
From: 2/1/2024 12:00 AM	To: 3/1/2024 12:00 AM	America/Bogota
Sample type: ss_hr_t		
Nombre de destino	Nombre del monitor	Disponibilidad
iceteboglxdarumatest	Ping	100.00
icetexbogliferafnfs	Ping	99.99
icetexboglxdarumasrv1	Ping	100.00
icetexboglxdarumasrv2	Ping	100.00
icetexboglxroad1	Ping	99.99
icetexboglxroad2n	Ping	100.00
icetexboglxroad3	Ping	100.00
icetexboglxroadtest	Ping	100.00
ictxprusisgapp	Ping	99.81
ictxisgesapp	Ping	99.28
ictxisgesbd	Ping	99.99
inr0233_icetexboglxorfeo1.localdomain	Ping	100.00
inr0237_icetexbogbalsrv1-r	Ping	99.93
inr0239_icetexbogelasticserver1	Ping	100.00
inr0241_icetexbogelasticserver3	Ping	90.70
inr0242_icetexbogliferaysrv2	Ping	99.93
inr0243_icetexbogliferaysrv1	Ping	99.80
inr0262_icetexboglxorfeo2.localdomain	Ping	99.89
inr0276_cxvodaprodn011	Ping	99.43
inr0277_cxvodaprodn021	Ping	99.71
inr0278_cxvodacontg011	Ping	98.94

Ilustración 2 Promedio Disponibilidad Servicios en Housing – Datacenter Principal Sitescope

Cod Servicio	Hostname	Disponibilidad
INR0246	iceteboglxdarumatest	100%
INR0238	icetexbogliferafnfs	99.99%
INR0244	icetexboglxdarumasrv1	100%
INR0245	icetexboglxdarumasrv2	100%
INR0249	icetexboglxroad1	99.99%
INR0247	icetexboglxroad2n	100%
INR0248	icetexboglxroad3	100%
INR0250	icetexboglxroadtest	100%
INR0234	ictxprusisgapp	99.81%
INR0229	ictxisgesapp	99.28%
INR0228	ictxisgesbd	99.99%
INR0233	icetexboglxorfeo1	100%
INR0237	icetexbogbalsrv1	99.93%
INR0239	icetexbogelasticserver1	100%
INR0241	icetexbogelasticserver3	90.70
INR0242	icetexbogliferaysrv2_R	99.93%
INR0243	icetexbogliferaysrv1_R	99.80%
INR0262	icetexboglxorfeo2	99.89%
INR0276	cxvodaprodn011	99.43%

INR0277	cxvodaprodn021	99.71%
INR0278	cxvodacontn011	98.94%

Tabla 8 Códigos relacionados Disponibilidad Servicios en Housing – Datacenter Principal Sitescope

REPORTE DISPONIBILIDAD SERVIDORES		
Last 30 days rounded to the day		
HOSTNAME	DISPONIBILIDAD	
cxvodaprodn011	100.00%	
cxvodaprodn021	100.00%	
icetexboglobserver1-r	100.00%	
icetexbogelasticserver1	100.00%	
icetexbogelasticserver2	100.00%	
icetexbogelasticserver3	100.00%	
icetexbogliferaynfs	100.00%	
icetexbogliferayserver1	100.00%	
icetexbogliferayserver2	100.00%	
icetexbogldarumasrv1	100.00%	
icetexbogldarumasrv2	100.00%	
icetexbogldarumatest	100.00%	
icetexboglxorfeo1.localdomain	100.00%	
icetexboglxorfeo2.localdomain	100.00%	
icetexboglxroad3	100.00%	
icetexosbognfs1	100.00%	
icetexosbognfs2	100.00%	
ictxbogsvpt1	100.00%	
ictxbogsvpt2	100.00%	

Ilustración 3 Promedio Disponibilidad Servicios en Housing – Datacenter Principal ELK

#	Cod Servicio	Hostname	Disponibilidad
1	INR0276	cxvodaprodn011	100%
2	INR0277	cxvodaprodn021	100%
3	INR0237	icetexboglobserver1-r	100%
4	INR0239	icetexbogelasticserver1	100%
5	INR0242	icetexbogliferayserver2	100%
6	INR0241	icetexbogelasticserver3	100%
7	INR0238	icetexbogliferaynfs	100%
8	INR0239	icetexbogelasticserver1	100%
9	INR0242	icetexbogliferayserver2	100%
10	INR0244	icetexbogldarumasrv1	100%
11	INR0245	icetexbogldarumasrv2	100%
12	INR0246	icetebogldarumatest	100%
13	INR0233	icetexboglxorfeo1	100%
14	INR0262	icetexboglxorfeo2	100%
15	INR0248	icetexboglxroad3	100%
16	INR0260	icetexbogosbognfs1	100%
17	INR0252	icetexbogosbognfs2	100%
18	INR0236	ictxbogsvpt1	100%
19	INR0235	ictxbogsvpt2	100%
20	INR000322	ictxcontroldoc	99.90%
21	INR0234	ictxprusisgapp	100%
22	INR0229	ictxisisgesapp	100%
23	INR0228	ictxisisgesbd	100%
24	INR0226	mira	100%

25	INR0247	preprodsec-icetexboglxroad2n	100%
26	INR0250	qasec-icetexboglxroadtest	100%
27	INR0249	xroadsec-icetexboglxroad1	100%

Tabla 9 Códigos relacionados Disponibilidad Servicios en Housing – Datacenter Principal ELK

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

Tabla 10 Disponibilidad de Servicios de Housing – Datacenter Principal

5.1.2 Disponibilidad TRIARA para los servicios de página web

A continuación, se evidencia que la disponibilidad de los servicios del Portal Web estuvo en un 100 % Nodo1 y 99.4% Nodo2 del sitio durante el mes de febrero [ReportDynatracePortal_Febrero2024.pdf](#)

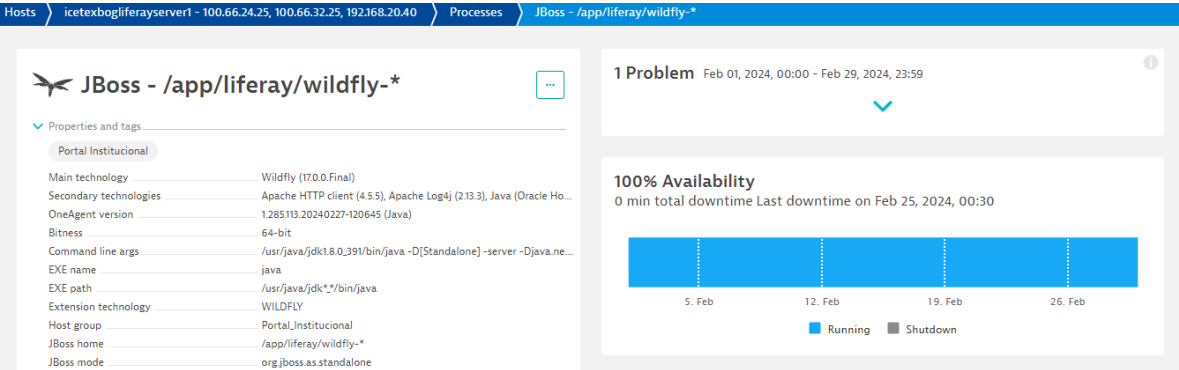


Ilustración 4 Disponibilidad Nodo1 Servicios Portal Web Icetex (Dynatrace)

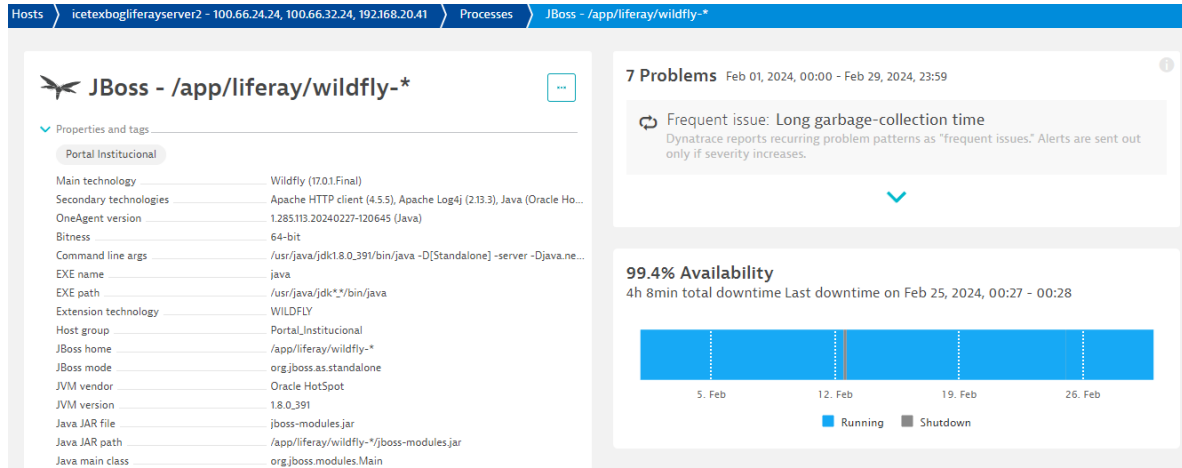


Ilustración 5 Disponibilidad Nodo 2 Servicios Portal Web Icetex (Dynatrace)

5.1.3 Backup Servidores Triara

Durante el periodo de febrero se realizó el backup de acuerdo con la política definida por el Icetex y la cual se implementó en el Datacenter. Se puede verificar en el documento, [Reporte backup mes de febrero 2024.pdf](#) el cual se genera automáticamente desde la herramienta que se utiliza para realizar las copias.

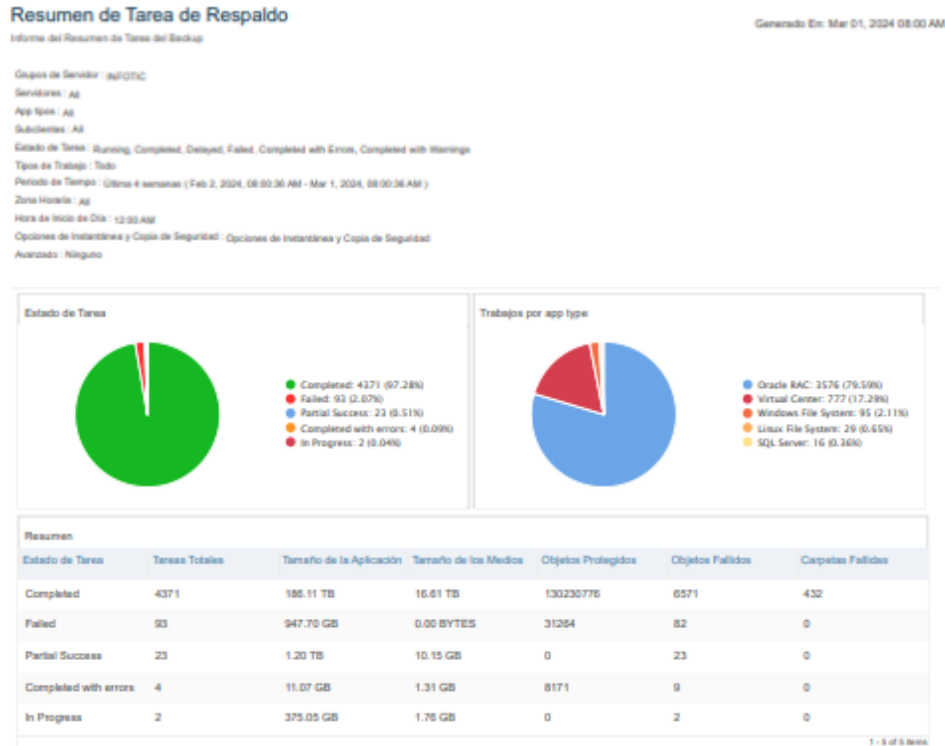


Ilustración 6 Evidencia Backup Servidores

5.2 Datacenter Alterno

5.2.1 Hosting Virtual (IaaS)

En el transcurso del mes de febrero se mantuvieron en constante replicación las máquinas, 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 [Informe mensual replicacion febrero 2024.pdf](#), el cual corresponde al último reporte diario del mes y refleja el consolidado de los informes que se están enviando diariamente desde el 15 de febrero.

ite Recovery Manager - Estado Replicas INFOTIC

tualmente el SRM (vcsatriara-ext.datacenterdhs.local -> vcmegacenter.datacenterdhs.local)
uenta con 13 replicas

General				
Name		Count		
OK		12		
Error		1		
Grupo de protección: PG_INFOTIC_7 (2)				
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	RPO
INR0226_INFOTIC_REP	OK	5 of 5	Feb 29, 2024	5 minutes
INR0228_INFOTIC_REP	OK	1 of 1	Feb 29, 2024	1 hour
Grupo de protección: PG_INFOTIC_6 (1)				
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	RPO
INR0229_INFOTIC_REP	OK	3 of 3	Feb 29, 2024	1 hour
Grupo de protección: PG_INFOTIC_1 (2)				
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	RPO
INR0233_INFOTIC_REP	OK	6 of 6	Feb 29, 2024	30 minutes
INR0262_INFOTIC_REP	OK	1 of 1	Feb 29, 2024	1 hour
Grupo de protección: PG_INFOTIC_5 (1)				
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	RPO
INR0236_INFOTIC_REP	OK	2 of 2	Feb 29, 2024	2 hours
Grupo de protección: PG_INFOTIC_4 (4)				
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	RPO
INR0237_INFOTIC_REP	OK	2 of 2	Feb 29, 2024	5 minutes
INR0238_INFOTIC_REP	Error	2 of 2	Feb 29, 2024	5 minutes
INR0239_INFOTIC_REP	OK	2 of 2	Feb 29, 2024	1 hour

Ilustración 7 Reportes de replicación SRM a Sitio Alterno, febrero 2024

A continuación, se detallan los servidores con sus correspondientes servicios los cuales están siendo replicados a MEGACENTER :

INR Replicación	Host name	Servicio	VirtualMachine MEGACENTER
INR0204	icetexbogwsmira	Portal Web	INR0226_INFOTIC_REP
INR0207	ictxisgesbd	Sisgestion	INR0228_INFOTIC_REP

INR Replicación	Host name	Servicio	VirtualMachine MEGACENTER
INR0206	ictxisgesapp	Sisgestion	INR0229_INFOTIC_REP
INR0220	icetexboglxorfeo1	ORFEO	INR0233_INFOTIC_REP
INR0219	icetexboglxorfeo2	ORFEO	INR0262_INFOTIC_REP
INR0208	ICTXBOGSRVPT1	Portal Transaccional	INR0236_INFOTIC_REP
INR0209	icetexbogbalsever1	Portal productivo (liferay)	INR0237_INFOTIC_REP
INR0210	icetexbogliferaynfs	Portal productivo (liferay)	INR0238_INFOTIC_REP
INR0217	icetexbogelasticserver1	Portal productivo (liferay)	INR0239_INFOTIC_REP
INR0218	icetexbogliferayserver1	Portal productivo (liferay)	INR0243_INFOTIC_REP
INR0215	icetexboglxdarumasrv1	DARUMA	INR0244_INFOTIC_REP
INR0213	icetexboglxdarumasrv2	DARUMA	INR0245_INFOTIC_REP
INR0214	icetexboglxroad1	XROAD	INR0249_INFOTIC_REP

Tabla 11 Servicios replicados – Datacenter MEGACENTER

5.2.2 Dataguad BBDD Megacenter

Durante el mes de febrero de 2024 se continuo con la replicación permanente de las BD Oracle al Datacenter alerno 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. Ver las evidencias en el documento [INFOTIC ICETEX - Evidencias Dataguad Megacenter.pdf](#)

```
oracle@cxvodacontg011:~  
#-----  
cd /home/oracle/script  
find . -name '*.log' -type f -mtime +2 -exec rm {} \;  
sh /home/oracle/script/borradormanAPLICATD.sh  
sh /home/oracle/script/borradormanAPOTEOSD.sh  
sh /home/oracle/script/borradormanAPOTNEWD.sh  
sh /home/oracle/script/borradormanICETEXD.sh  
sh /home/oracle/script/borradormanICTXCYCD.sh  
sh /home/oracle/script/borradormanLANDICTD.sh  
sh /home/oracle/script/borradormanLIFERAYD.sh  
sh /home/oracle/script/borradormanVIGIADTG.sh  
  
[oracle@cxvodacontg011 ~]$ cat /home/oracle/script/borradormanICTXCYCD.sh  
#!/bin/bash  
  
export ORACLE_BASE=/oracle/app/oracle/product  
export ORACLE_HOME=/oracle/app/oracle/product/product/11.2.0/dbhome_1  
export BASE_PATH=/usr/sbin:$PATH  
export PATH=$ORACLE_HOME/bin:$BASE_PATH  
export ORACLE_SID=ICTXCYCD  
export LD_LIBRARY_PATH=$ORACLE_HOME/lib:/lib:/usr/lib  
export CLASSPATH=$ORACLE_HOME/JRE:$ORACLE_HOME/jlib:$ORACLE_HOME/rdbms/jlib  
export PATH  
export DATE=$(date +"%Y %m %d %H")  
export LogFull=/home/oracle/script/log_crontab_${ORACLE_SID}_${DATE}.log  
  
#-----  
# Ejecucion  
#-----  
$ORACLE_HOME/bin/rman target / msglog $LogFull append << EOF  
crosscheck archivelog all;  
delete noprompt force archivelog until time 'sysdate-1';  
#delete noprompt obsolete;  
exit  
EOF  
[oracle@cxvodacontg011 ~]$  
  
[oracle@cxvodacontg011 ~]$ ps -fealgrep pmon  
grid      10449      1 0 Feb24 ?        00:03:16 asm_pmon_+ASM  
oracle    10792      1 0 Feb25 ?        00:07:50 ora_pmon_ ICTXCYCD  
oracle    11336      1 0 Feb25 ?        00:07:35 ora_pmon_ APOTEOSD  
oracle    11715      1 0 Feb25 ?        00:04:14 ora_pmon_ VIGIADTG  
oracle    12044      1 0 Feb25 ?        00:04:08 ora_pmon_ LIFERAYD  
oracle    12307      1 0 Feb25 ?        00:04:12 ora_pmon_ LANDICTD  
oracle    12566      1 0 Feb25 ?        00:07:11 ora_pmon_ APPLICATD  
oracle    12732      1 0 Feb25 ?        00:07:20 ora_pmon_ APOTNEWD  
oracle    12918      1 0 Feb25 ?        00:07:30 ora_pmon_ ICETEXD  
oracle    17537 16920  0 11:07 pts/0    00:00:00 grep  --color=auto pmon  
[oracle@cxvodacontg011 ~]$ sqlplus / as sysdba  
  
SQL*Plus: Release 11.2.0.4.0 Production on Thu Mar 21 11:07:29 2024  
Copyright (c) 1982, 2013, Oracle. All rights reserved.  
  
Connected to:  
Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production  
With the Partitioning, Automatic Storage Management, OLAP, Data Mining  
and Real Application Testing options  
  
SQL> sta fapplyb.sql  


| Thread | Last Sequence | Received | Last Sequence | Applied | TIME_RECEIVED    | TIME_APPLIED     |
|--------|---------------|----------|---------------|---------|------------------|------------------|
| 1      |               | 46821    | 46821         |         | 29/02/2024 09:43 | 29/02/2024 09:43 |
| 2      |               | 37258    | 37257         |         | 29/02/2024 10:43 | 29/02/2024 10:24 |

  
SQL> sta uapply  


| Thread | Last Sequence | Received | Last Sequence | Applied | Difference |
|--------|---------------|----------|---------------|---------|------------|
| 1      |               | 46821    | 46821         |         | 0          |
| 2      |               | 37258    | 37258         |         | 0          |

  
SQL>
```

Ilustración 8 Evidencia Dataguard replicado a Megacenter BD

Se generó la consulta de los archivos recibidos y aplicados de la base de datos de ICTXCYCD a fecha 29/02/2024

19:43 con diferencia cero (0) archivos sin aplicar, lo cual es evidencia que la replicación se encuentra sincronizada.

5.2.3 Replicación Servicios OnPremise de Icetex a Megacenter

A continuación, se presentan la gráfica de la replicación realizada de los servicios on-premise en Icetex hacia el Datacenter alternativo Megacenter (Medellín).

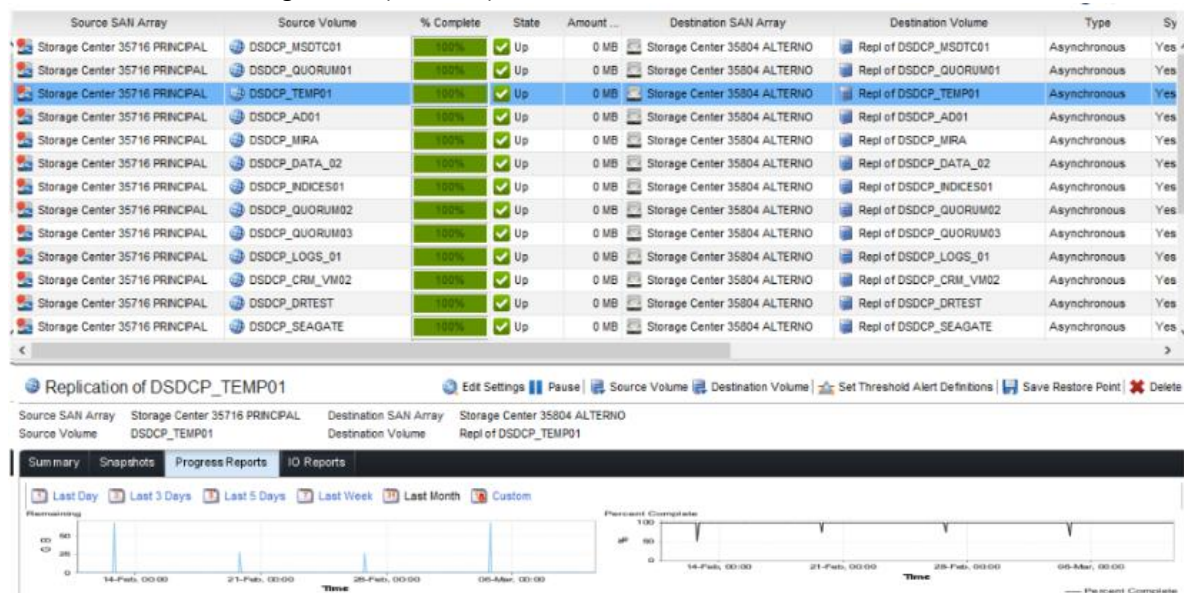


Ilustración 9 Evidencia replicado servicios On-premise Icetex a Megacenter

5.2.4 Disponibilidad de Servicios de Housing – Datacenter Alternativo

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

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

Tabla 12 Disponibilidad de Servicios de Housing – Datacenter Alternativo

6 SEGURIDAD

En este capítulo se hará referencia a las diferentes actividades que se realizaron durante el mes de febrero, en materia de seguridad.

6.1 Servicios de Endpoint

Posterior a la activación del módulo de “Filtrado Web” del antivirus SOPHOS se identificó la necesidad de deshabilitar en protocolo QUIC para que se pueda realizar el Filtrado web, sin embargo, se requiere que se realicen las pruebas de “web filter” en los equipos de mesa de ayuda deshabilitando el protocolo QUIC y dependiendo del resultado funcional se valide con el ICETEX su implementación a nivel de toda la red y las condiciones de dicha implementación.

Actualmente continúa habilitado y funcionando correctamente es el módulo de acceso a USB que se relaciona en las actividades mensuales, la protección XDR y EDR, la protección de virus y el despliegue de políticas centralizadas.

En Endpoints el porcentaje de avance de instalación y configuración es del 90% teniendo en cuenta que existen equipos en bodega.

6.2 ESTADÍSTICAS PORTALES

Durante el mes de febrero se realizó un monitoreo permanente a los portales sobre los que opera el ICETEX, manteniendo, las alertas y reportes a tiempo en caso de que se presentara algún evento que pudiera ocasionar una interrupción en la prestación de los servicios que se ofrecen a través de los portales, este informe se encuentra detallado en el documento [Reporte febrero seguridad 2024.pdf](#) en el capítulo *PORTALES PROTEGIDOS POR EL WAF*

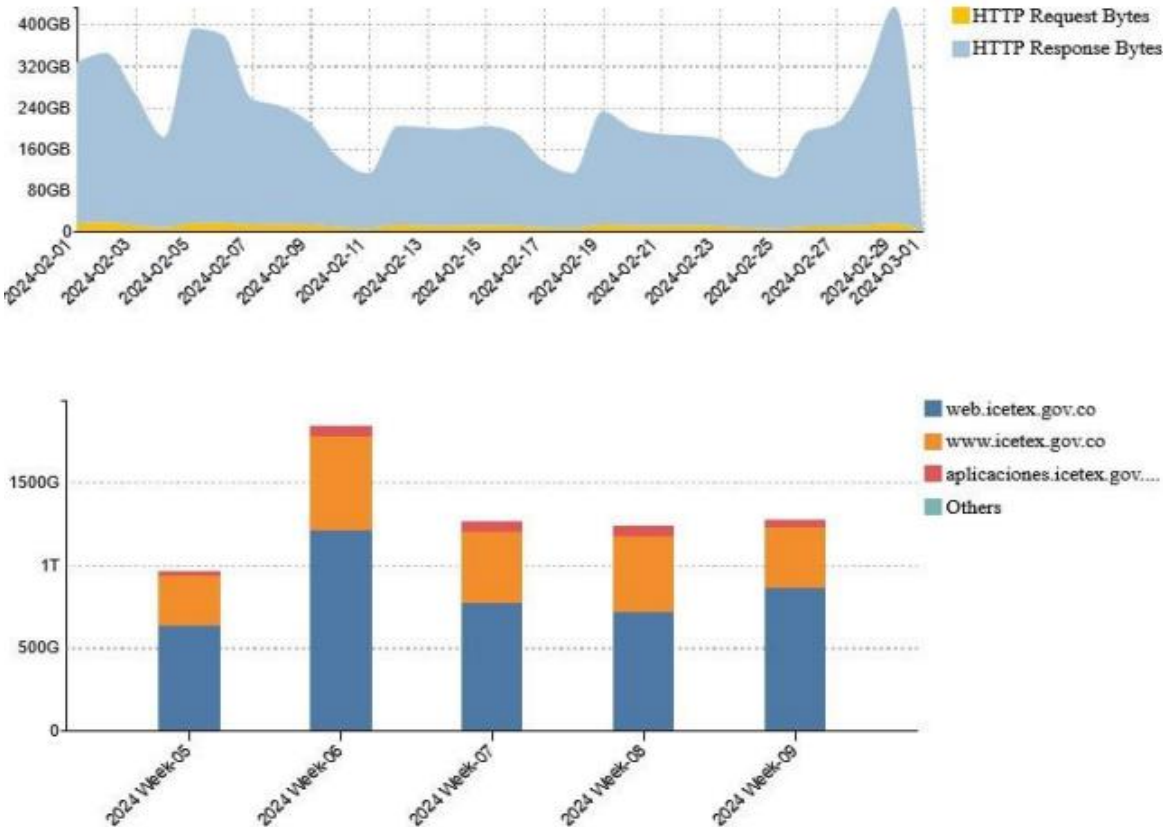


Ilustración 10 Evidencia Gráfica Estadísticas de Portales

En el periodo de tiempo analizado se presenta un promedio de 200 Gb de tráfico general hacia los portales FortiWeb lo cual es un comportamiento normal para este tipo de transacciones de acuerdo con la actividad de los usuarios.

6.3 Estado General de las Plataformas

En el documento [Reporte febrero seguridad 2024.pdf](#) se puede encontrar el Informe de Gestión Mensual que contiene información relevante de seguridad para el mes de febrero en lo concerniente a la Administración Plataformas incluidas las que son de propiedad del ICETEX y las IaaS



Ilustración 11 Evidencia Estado General de las Plataformas

6.4 Estado de Salud de los Equipos de Seguridad

En el transcurso del mes de febrero se mantuvo el monitoreo en el tráfico WAN hacia la MPLS, revisando permanentemente el estado de estas el cual tuvo un comportamiento normal, esto se puede ver en el capítulo 4 ESTADO DE SALUD DE LOS EQUIPOS DE SEGURIDAD del documento [Reporte febrero seguridad 2024.pdf](#)



Ilustración 12 Evidencia Estado de Salud de los Equipos de Seguridad

6.5 Servicio de centro de Operaciones de Seguridad (SOC)

Durante el mes de febrero se continuó con el monitoreo a través del SOC, cumpliendo con todos los requerimientos exigidos por el ICETEX. Durante este mes se hicieron todos los ajustes y afinamientos para el correcto funcionamiento de este servicio. El SOC ha continuado en su adaptación y evolución conforme al cambio en las necesidades del ICETEX por lo cual de manera permanente se mantiene actualizado de acuerdo con la nueva realidad. El detalle se puede ver en el siguiente link [Informe Mensual SOC ICETEX febrero 2024.pdf](#)

TLP:ROJO		INFORME MENSUAL MONITOREO SOC	Página	6 de 61
----------	--	-------------------------------	--------	---------

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

3.1.1 Casos de Uso Seguridad

Se encuentran definidas **1.326** 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.

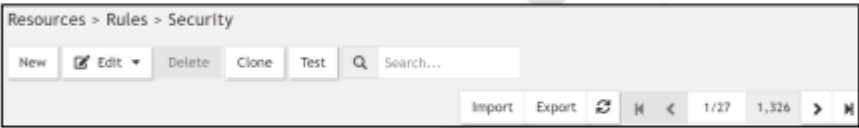


Ilustración: Cantidad de reglas de seguridad

3.1.2 Casos de Uso Disponibilidad

Para los casos de uso de disponibilidad se cuenta con **157** reglas, que tienen como función principal alertar algún tipo de falla o indisponibilidad de los equipos de la entidad y hacer la respectiva notificación a el área encarga.

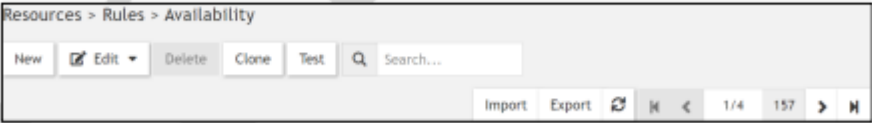


Ilustración: Cantidad de reglas de Disponibilidad

3.1.3 Casos de Uso Rendimiento

De las reglas de rendimiento, se han especificado **231** reglas, que identifican el performance de los equipos de la entidad a nivel de consumo de memoria, CPU y disco, entre otras métricas establecidas de acuerdo con el Core de negocio.

Ilustración 13 Evidencia Imagen Reporte Monitoreo

6.5.1 Monitoreo de Marca (SOC)

Para el mes de febrero y de acuerdo con lo programado se continuó con el servicio de monitoreo de marca. Durante el transcurso del mes se fueron incluyendo parámetros de acuerdo con lo requerido por el ICETEX, cabe anotar que como los métodos de utilización fraudulenta de marca cambian también nuestro sistema evoluciona. El detalle se puede ver en el siguiente link [Informe Marca ICETEX febrero 2024.pdf](#)

4. ANÁLISIS DE MONITOREO DE MARCA

Durante el periodo evaluado, la plataforma de monitoreo de marca – AXUR, reporta un total de **231** posibles amenazas de las 119k que fueron encontradas y analizadas automáticamente por la plataforma de monitoreo. A estas **231** posibles amenazas se les realizó una revisión y análisis interno, de sus características, datos e información. Adicionalmente dada la gestión realizada por la entidad en el período evaluado, se resolvió **02** casos en la plataforma de monitoreo.



A continuación, se presentan los incidentes detectados durante el periodo evaluado de acuerdo con el tipo de categoría:



Ilustración 14 Evidencia Imagen Reporte Monitoreo de Marca

6.6 Eventos Relevantes

- Dada la integración de las plataformas de seguridad desplegadas en la entidad le permite al Icetex prevenir ataques de Ciberseguridad que comprometan la continuidad del negocio.

- Durante el mes de febrero no se presentaron eventos relevantes, que afectaran la disponibilidad de los servicios de la entidad a nivel de la solución de Seguridad.

6.7 RECOMENDACIONES

Recomendación	Estado	Criticidad
Se debe realizar la validación si los usuarios conectados a la VPN y los que hacen uso de la VPN punto a punto, es necesario que naveguen a través del ICETEX.	En evaluación por ICETEX.	Media
Se debe segmentar las políticas de acuerdo con la necesidad y no otorgar acceso de toda una red o todos los servicios.	Se está trabajando como inicio con tesorería, se presenta plan de trabajo y se involucra a redes, seguridad y el equipo de Windows.	Media
Se debe trabajar en el perfilamiento de la navegación de acuerdo con lo entregado por ICETEX.	Se espera por parte de ICETEX la definición de los grupos.	Media-alta
Validar la autenticación de doble factor para todas las plataformas misionales del ICETEX.	En evaluación por parte de ICETEX.	Alta
Realizar autenticación a través del LDAP, para la gestión de las plataformas de seguridad.	Se integra el FortiGate de Triara, se evalúa la posibilidad con las otras plataformas.	Media
Validar la posibilidad de la integración de la consola Sophos con SIEM.	Se debe ampliar la capacidad del SIEM.	Baja
Validar la posibilidad de la integración de una VPN para la gestión desde DT alterno Medellín.	En evaluación por parte de seguridad.	Baja
Realizar la contención automática de equipos que se identifiquen en la red como maliciosos.	En evaluación por parte de ICETEX.	Media

Ilustración 15 Recomendaciones plataformas de seguridad

Cada reporte generado o emitido desde el área del SOC, se le realizó su respectivo informe describiendo el análisis aplicado en cada uno y se reportó por correo, además se realizó un control de las alertas presentadas y un seguimiento a los casos.

6.8 CONCLUSIONES

- La segmentación de la red permite tener una mejor administración y control en caso de un incidente informático.
- El analizador de la red permite identificar que ocurre transversalmente en la red.
- El robustecimiento en cuanto a la posición de seguridad de la información de ICETEX permite estar mejor preparado frente a un incidente de seguridad.

- Evitar usuarios y claves configurados en texto plano en las aplicaciones, protegería la infraestructura por si un incidente informático se lleva a cabo.
- Evitar compartir los accesos previene los incidentes informáticos y ayuda a una identificación en caso de que ocurra.

7 GESTION DE SERVICIO

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

7.1 ACTIVIDADES DE OPERACIÓN

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

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

7.2 Profesionales Especializados.

El detalle de las actividades realizadas por cada uno de los ingenieros especialistas se encuentran el [INFORME ACTIVIDADES FEBRERO.pdf](#)

7.2.1 Especialista en Base de Datos DBA

Profesional en ingeniería de sistemas o afines con experiencia mínima de cuatro (4) años certificado ORACLE, OCP y ORACLE 11G,12C o 19C.

Responsable de garantizar la integridad y disponibilidad de la información, sistemas eficientes, seguros y confiables.

Funciones principales:

- Planificación y diseño de bases de datos
- Configuración y mantenimiento de bases de datos
- Monitoreo y optimización del rendimiento de bases de datos

7.2.2 Especialista web master

Ingeniero de sistemas con mínimo 3 años de experiencia en administración técnica y de contenido de portales de Internet, con experiencia comprobada en gestores de contenido tales como: SiteFinity, SharePoint, Liferay, WordPress, así como conocimientos en Scripting, json, e introducción al desarrollo.

Responsable del diseño, desarrollo y mantenimiento de sitios web y aplicaciones web.

Funciones principales:

- Diseño y desarrollo web
- Mantenimiento y actualización de sitios web
- Pruebas y resolución de problemas

7.2.3 Administrador de Soluciones

Dos (2) profesionales en Ingeniería de sistemas o afines con Tarjeta profesional, con mínimo 7 años de experiencia específica en administración de soluciones tecnológicas

Responsable de administrar y mantener soluciones de software empresarial.

Funciones principales:

- Identificación de soluciones tecnológicas
- Mantenimiento y actualización de soluciones
- Diagnóstico y resolución de problemas

7.2.4 Especialista en Networking

Profesional en Ingeniería de Sistemas, electrónica, telecomunicaciones y afines, con mínimo 3 años de experiencia, conocimientos en soluciones de VoIP y Networking, certificado Cisco CCNP.

Responsable de la planificación, diseño, implementación y mantenimiento de redes de computadoras y sistemas de comunicación.

Funciones principales:

- Diseño y planificación de redes
- Mantenimiento y soporte de redes
- Configuración de servicios de red

7.2.5 Especialista Integrador de nube

Un Profesionales en Ingeniería de sistema o afines con Tarjeta profesional, con mínimo 5 años en experiencia general y mínimo dos (2), con experiencia específica en acompañamiento, despliegues, integración, migración y configuración de servicios en las Nubes Públicas y privadas

Responsable de integrar aplicaciones y sistemas empresariales en la nube.

Funciones principales:

- Diseño de soluciones en la nube
- Configuración e implementación de soluciones en la nube
- Mantenimiento y actualización de soluciones en la nube

7.2.6 Especialista en seguridad

Dos (2) profesionales con Título Profesional con Tarjeta profesional en Ingeniero de sistemas o afines con mínimo 5 años de experiencia específica en administración de servicios de seguridad perimetral.

Responsable de proteger la información y los sistemas informáticos de una empresa contra amenazas internas y externas.

Funciones principales:

- Evaluación de riesgos de seguridad
- Análisis y monitoreo de seguridad
- Configuración y mantenimiento de herramientas de seguridad

8 SERVICIO DE COLABORACIÓN

A continuación, se relacionan las 10 soluciones de videoconferencia o salas virtuales y su distribución:

ÍTEM	SERVICIO	CIUDAD	DIRECCIÓN	CANTIDAD
1	Sala de video conferencia o sala virtual (Tamaño 65")	Bogotá - Aguas	Carrera 3 No. 18-32	3
2	Sala de video conferencia o sala virtual (Tamaño 65")	Bogotá - Ángel	Cl. 19 #6-68 piso 17	1
3	Sala de video conferencia o sala virtual (Tamaño 55")	Bogotá - Aguas	Carrera 3 No. 18-32	1
SEDES REGIONALES				
4	Sala de video conferencia o 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 13 Distribución módulos de videoconferencia por sede

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

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

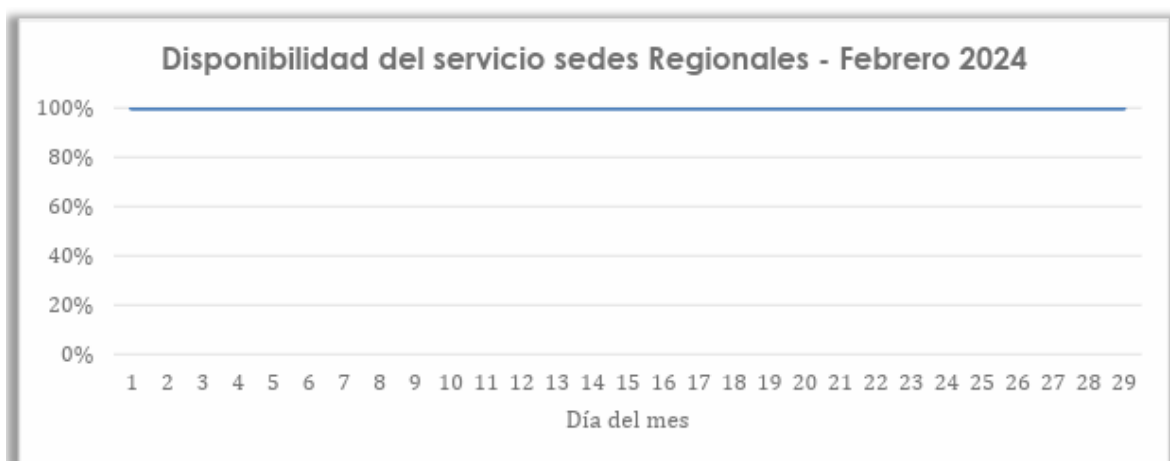


Ilustración 16 Disponibilidad de servicio videoconferencia sedes regionales – febrero 2024

8.1 Disponibilidad del servicio – sedes Bogotá (aguas - ángel)

En la verificación realizada para el mes de febrero del 2024 sobre la solución de videoconferencia distribuida en las sedes Aguas y Angel en la ciudad de Bogotá, se encuentra una disponibilidad del 100%, la solución completa, a fecha del presente informe, en estado activo, además es importante resaltar que se cuenta con todos los requerimientos realizados en las especificaciones técnicas del contrato.

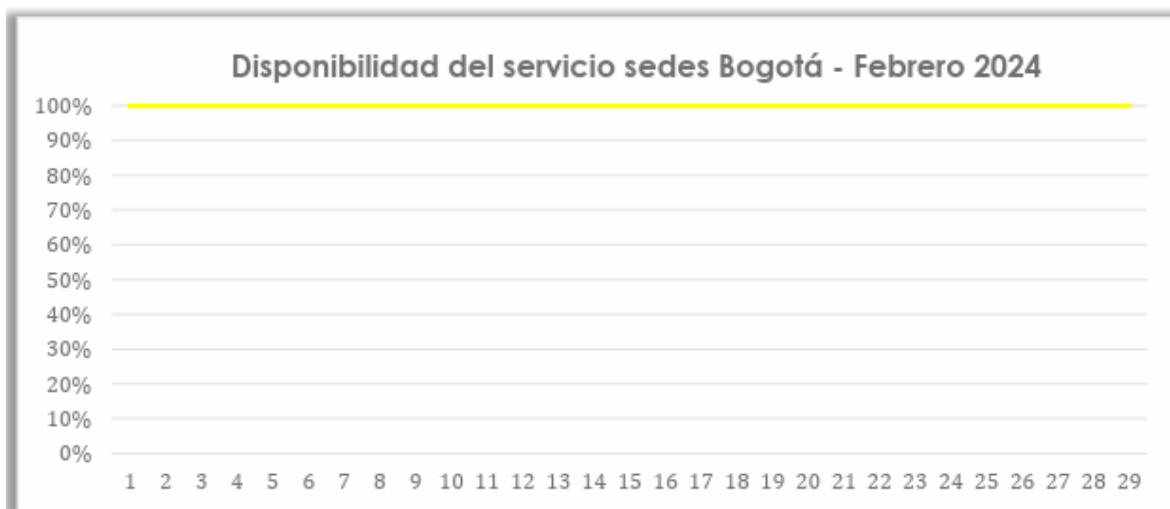


Ilustración 17 Disponibilidad de servicio videoconferencia sedes Bogotá – febrero 2024

8.2 Gestión de incidencias y requerimientos – sedes regionales

Para el mes de febrero, entre el 1 y el 29 del mes, no se presentaron requerimientos, ni fallas en la prestación del servicio.

Se realizan pruebas de la pantalla, wifi, touch, sonido, calidad de imagen y se evidencia que queda

funcionando correctamente. Se realiza nuevamente las recomendaciones en la sede, para mantener el módulo conectado a la red de corriente regulada, con el fin de poder apagar el módulo de manera controlada, debido a que apagados repentinos del módulo por manejo inadecuado, por factores externos o cortes de fluido eléctrico reiterados, generalmente causan errores de inicio de este o incluso daños físicos de los dispositivos que lo componen.



Ilustración 18 Incidencias/Requerimientos sedes Regionales – febrero 2024

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

Para el mes de febrero, a la fecha del presente informe no se generaron requerimientos especiales para las sedes de Bogotá Aguas y Angel; tampoco se reportaron incidencias a nivel del servicio para estas sedes durante el periodo, sin embargo, se continúa al tanto para recibir cualquier solicitud de soporte o apoyo concerniente a la solución de videoconferencia desplegada.

- Durante el mes de febrero se prestó un servicio de calidad conforme a los requerimientos contractuales y se ha brindado el soporte de acuerdo con las necesidades realizadas por el cliente. El servicio presentó continuidad durante el transcurso del mes del presente informe.
- En la infraestructura a nivel del servicio se presenta un nivel de disponibilidad acorde a lo establecido en el contrato.
- Se continúa con disponibilidad continua para atender todas solicitudes de soporte técnico para estas plataformas.
- Los requerimientos del mes fueron atendidos en el mismo momento que se recibieron, con el fin de solventar con prioridad y no afectar la prestación y continuidad del servicio.

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

9 Visita a VISE

Dentro de 2 - actividades realizadas en el mes de febrero de 2024, se realizó el acompañamiento a la visita del centro de almacenamiento y custodia de las cintas de backup que se tiene para el proyecto por parte de CLARO, quien envió las cintas a la empresa VISE, de acuerdo con la siguiente información:

INFORME DE VISITA		
Proyecto:	ICETEX	
Fecha y Hora:	Del: 16-Feb-2024 (09:00 am)	Al: 16-Feb-2024 (10:30 am)
Sede:	VISE	
Responsable:	Oscar Alberto Viuche Tellez	
Rol/ Responsabilidad	Gerente Implementación ICETEX	
Objetivo del Período:	Verificar el estado de las cintas de backup entregadas para almacenamiento externo a CLARO.	

ANTECEDENTES

Dentro del desarrollo del proyecto ICETEX, la entidad entrego para custodia externa 345 cintas de backup de diferentes características a INFOTIC, quien a su vez mediante su aliado estratégico CLARO entregaron la custodia a la empresa VISE, mediante los siguientes documentos: *(se adjunta copia de los documentos)*

No.	Documento	Fecha	Detalle	Nombre
1	Recibo de transporte no. 200815	14-ago-23	264 cintas	Anexo 1
2	Recibo de transporte no. 201099	15-ago-23	61 cintas	Anexo 2
3	Inventario	24-ago-23	345 cintas	Anexo 3

Ilustración 19 Visita Vise-Antecedentes

Para realizar la visita se adelantaron las siguientes actividades previas:

ACTIVIDADES PREVIAS

Para la realización de la visita en la cintoteca de VISE, se realizó:

1. Se solicito la información del estado de la custodia externa de las cintas de Backup a CLARO en la reunión de seguimiento del 13 de febrero de 2024 (08:00 am).
2. CLARO genero un correo con la información requerida a las 10:59 am
3. Se busco el correo de contacto en la página de VISE y se envió la solicitud de información del procedimiento para realizar la visita (custodia@techzone.com.co) a las 11:08 am (*techzone – es otra empresa del grupo ALTUM*)
4. Desde VISE contesto el señor Carlos Guillermo Gonzalez – jefe de medios magnéticos (e) a las 12:01 PM, con la siguiente respuesta:

Ilustración 20 Visita Vise-Actividades previas

La visita se realizó el 16 de febrero de 2024 de las 09:00 am a 10:30 am y asistieron:

ICETEX - Custodia de Medios



Oscar Alberto Viuche Tellez

Para: Carlos Gonzalez <seguridadinformatica@techzone.com.co> Mar 13/02/2024 14:12



Carlos buenas tardes,

Me permito solicitar su colaboración con la autorización de ingreso para la revisión de las cintas en custodia de ICETEX, para:

COMPañÍA (*)	NOMBRE Y APELLIDOS (*)	CEDULA (*)
Icetex	Raul Fernando Gutierrez Tecano	80,874,341
Infotie	Oscar Alberto Viuche Tellez	79,603,394

Fecha de la visita: viernes 16 de febrero de 2024
Hora de la visita: 09:00 am

Cordialmente,

Ilustración 21 Visita Vise-Asistentes

El resultado de la visita fue:

10. El siguiente es el resumen de las cintas entregadas en custodia externa a CLARO:

No.	Detalle	Cintas
1	Entrega (anexo 1 y 2)	325
2	Movimientos (anexo 6 y 7) - salidas	31
3	Saldo actual (anexo 8)	294

Ilustración 22 Resumen Cintas entregadas en custodia externa a CLARO

Se adjunta el link del informe: [Informe visita VISE,custodia cintas](#)

10 CALCULO DE CONCILIACIÓN DE LOS SERVICIOS DEL MES DE FEBRERO

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

EJECUCIÓN PRESUPUESTAL

EJECUCIÓN PRESUPUESTAL					
CONCEPTO					VALOR
VALOR INICIAL DEL CONTRATO					\$ 31.398.996.857,96
VALOR ADICIONES (si aplica, especificar el o los números de adición)					\$ 0,00
VALOR REDUCCIÓN (si aplica)					\$ 0,00
VALOR POR OTRO CONCEPTO (si aplica)					\$ 0,00
VALOR TOTAL DEL CONTRATO					\$ 31.398.996.857,96
VALOR PAGADO					\$ 6.232.541.727,16
Pago No. 1 - mes: Abril de 2023				\$ 537.090.736,00	
Pago No. 2 - mes: Mayo de 2023				\$ 544.104.546,00	
Pago No. 3 - mes: Junio de 2023				\$ 596.978.314,00	
Pago No. 4 - mes: Julio de 2023				\$ 624.431.841,60	
Pago No. 5 - mes: Agosto de 2023				\$ 650.825.466,00	
Pago No. 6 - mes: Septiembre de 2023				\$ 661.959.450,00	
Pago No. 7 - mes: Octubre de 2023				\$ 641.792.285,00	
Pago No. 8 - mes: Noviembre de 2023				\$ 630.348.564,00	
Pago No. 9 - mes: Diciembre de 2023				\$ 663.076.196,00	
Pago No. 10 - mes: Enero de 2024				\$ 681.934.328,00	
VALOR CAUSADO QUE NO SE HA PAGADO (valor a pagar factura) *					\$ 760.734.516,16
VALOR TOTAL EJECUTADO (valor pagado + valor causado no pagado)					\$ 6.993.276.243
SALDO DEL CONTRATO (valor total del contrato – valor total ejecutado)					\$ 24.405.720.615
PORCENTAJE DE EJECUCIÓN					22.27%
* 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 14 Ejecución Presupuestal

