



INFORME DE ACTIVIDADES DEL CONTRATO

**CONTRATO NUMERO
2022-0792**

Enero 01 al 31 de 2024

Contenido

1	INTRODUCCIÓN	4
2	OBJETIVOS	4
3	RESUMEN EJECUTIVO	4
4	SERVICIOS DE CONECTIVIDAD	5
4.1	INTERNET PARA LA GENTE	10
4.2	Canal de Replicación (Triara – Megacenter)	10
4.3	CONCLUSIONES DEL SERVICIO DE CONECTIVIDAD	11
5	SERVICIOS CENTROS DE COMPUTO	11
5.1	Datacenter Principal	11
5.1.1	Disponibilidad de Servicios – Datacenter Principal	12
5.1.2	Disponibilidad de Servicios de Housing – Datacenter Principal	14
5.1.3	Disponibilidad TRIARA para los servicios de página web	15
5.1.4	Backup Servidores Triara	15
5.2	Datacenter Alterno	16
5.2.1	Hosting Virtual (IaaS)	16
5.2.2	Dataguard BBDD Megacenter	18
5.2.3	Replicación Servicios OnPremise de Ictetex a Megacenter	19
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	27
8	SERVICIO DE COLABORACIÓN	28
8.1	Disponibilidad del servicio – sedes Bogotá (aguas - ángel)	29
8.2	Gestión de incidencias y requerimientos – sedes regionales	29
8.3	Gestión de incidencias y requerimientos – Bogotá (Aguas - Angel)	30

9 CALCULO DE CONCILIACIÓN DE LOS SERVICIOS DEL MES DE DICIEMBRE	31
EJECUCIÓN PRESUPUESTAL	31

INDICE DE TABLAS

Tabla 1 Disponibilidad de canales	8
Tabla 2 Canales pendientes por instalar	8
Tabla 3 Canales ampliados enero 2024.....	9
Tabla 4 Canales pendientes por ampliar	10
Tabla 5 Disponibilidad canales “Internet para la gente”	10
Tabla 6 Disponibilidad de Servicios de Housing – Datacenter Principal	15
Tabla 7 Disponibilidad de Servicios de Housing – Datacenter Alterno	20
Tabla 8 Distribución módulos de videoconferencia por sede.....	28
Tabla 9 Requerimientos sedes regionales.....	30
Tabla 10 Ejecución Presupuestal.....	31

INDICE DE ILUSTRACIONES

Ilustración 1 INR0268 - // MEDELLÍN // DC MEGACENTER ICETEX	5
Ilustración 2 INR0230 // MEDELLÍN // DC MEGACENTER ICETEX // BACKUP	5
Ilustración 3 Evidencia del canal de replicación entre Triara y Megacenter	11
Ilustración 4 Evidencia del Resumen del Monitoreo	12
Ilustración 5 Evidencia Disponibilidad Servicio Datacenter Principal	13
Ilustración 6 Disponibilidad Servidores OPENSIFT– Datacenter Principal.....	14
Ilustración 7 Disponibilidad Servicios Portal Web Ictex (Dynatrace)	15
Ilustración 8 Evidencia Backup Servidores	16
Ilustración 9 Evidencia replicación SRM a Sitio Alterno, ENERO-2024	17
Ilustración 10 Reportes de replicación SRM a Sitio Alterno, ENERO 2024	17
Ilustración 11 Evidencia Dataguard replicado a Megacenter BD.....	19
Ilustración 12 Evidencia replicado servicios On-premise Ictex a Megacenter.....	20
Ilustración 13 Evidencia Gráfica Estadísticas de Portales	21
Ilustración 14 Evidencia Estado General de las Plataformas	22
Ilustración 15 Evidencia Estado de Salud de los Equipos de Seguridad.....	22
Ilustración 16 Evidencia Imagen Reporte Monitoreo	23
Ilustración 17 Evidencia Imagen Reporte Monitoreo de Marca	24
Ilustración 18 Disponibilidad de servicio videoconferencia sedes regionales – Enero 2024.....	29
Ilustración 19 Disponibilidad de servicio videoconferencia sedes Bogotá – enero 2024	29
Ilustración 20 Incidencias/Requerimientos sedes Regionales – enero 2024.....	30

1 INTRODUCCIÓN

Este informe contiene la información relacionada con las actividades ejecutadas por INFOTIC en el periodo comprendido entre el 1 al 31 de enero 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 diciembre 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 1 al 31 de enero 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 sobrecada 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 enero se inició 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 conmutación, así como sus actas de entrega, para Wifi para la gente, durante el mes de enero se hicieron los ajustes sobre los Aps para las sedes de Yopal, Chapinero, Mocoa, Apartadó y Arauca.

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 una prueba de restauración granular y fue exitosa, 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. Se presento el cambio del Web Master quien realizo el

empalme, entrega de la información y actividades realizadas y pendientes de ejecutar.

Bolsa para servicios por demanda: Durante el periodo de enero se presentaron la Icetex la propuesta económica de las cintas de backup.

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 enero 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 enero de 2024.

4 SERVICIOS DE CONECTIVIDAD

Durante el mes de enero, los canales principales y backup instalados operaron de manera normal. Se realizó el traslado del APP de la sede de Arauca todos con sus respectivas pruebas de conmutación, así como sus actas de entrega, los cuales están en el siguiente link:

[Actas](#)

El canal INR0268 - // MEDELLÍN // DC MEGACENTER ICETEX se factura a partir de la fecha en que aparece en el monitoreo de SolarWinds de acuerdo con la evidencia de la siguiente imagen:

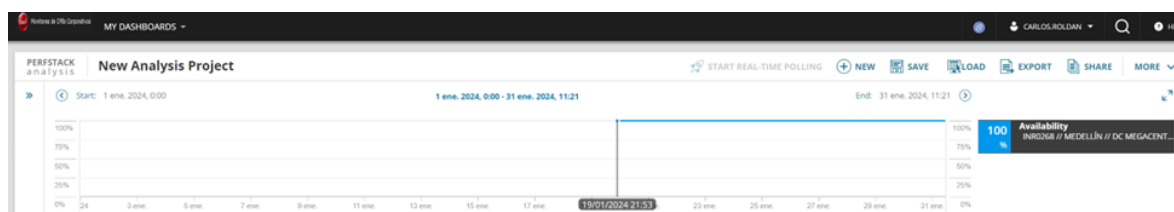


Ilustración 1 INR0268 - // MEDELLÍN // DC MEGACENTER ICETEX

El canal INR0230 // MEDELLÍN // DC MEGACENTER ICETEX // BACKUP se factura a partir de la fecha en que aparece en el monitoreo de SolarWinds de acuerdo con la evidencia de la siguiente imagen:



Ilustración 2 INR0230 // MEDELLÍN // DC MEGACENTER ICETEX // BACKUP

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 enero 2024-ALLOT INFOTIC.pdf](#)

Durante el mes de enero 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 Enero 2024.pdf](#)

Sede	Categoría	INR	% Mes
BOGOTA D.C.	Principal / FO (Sede Aguas)	INR0037	100.00%
	Backup / FO (Sede Aguas)	INR0221	100.00%
	Principal / IPVPN (Sede Chapinero)	INR0022	100.00%
	Backup / IPVPN (Sede chapinero)	INR0020	99.45%
	Principal / IPVPN (Angel)	INR0272	99.96%
	Backup / IPVPN (Angel)	INR0273	98.34%
IBAGUE	Principal / IPVPN	INR0073	99.92%
	Backup / IPVPN	INR0076	99.57%
LETICIA	Principal / Satelital		0,00%
NEIVA	Principal / IPVPN	INR0039	86.71%
	Backup / IPVPN	INR0041	86.71%
TUNJA	Principal / IPVPN	INR0104	93.69%
	Backup / IPVPN	INR0106	99.29%
VILLAVICENCIO	Principal / IPVPN	INR0084	99.94%
	Backup / IPVPN	INR0085	100.00%
ARMENIA	Principal / IPVPN	INR0072	99.96%
	Backup / IPVPN	INR0074	100.00%
MANIZALES	Principal / IPVPN	INR0088	100.00%
	Backup / IPVPN	INR0087	99.96%
MEDELLIN	Principal / IPVPN	INR0133	100.00%
	Backup / IPVPN	INR0132	100.00%
APARTADO	Principal / IPVPN	INR0144	100.00%
PEREIRA	Principal / IPVPN	INR0079	100.00%
	Backup / IPVPN	INR0077	99.90%
QUIBDO	Principal / IPVPN	INR0014	99.94%
	Backup / IPVPN		0,00%
BARRANQUILLA	Principal / IPVPN	INR0103	99.92%
	Backup / IPVPN	INR0100	99.97%
CARTAGENA	Principal / IPVPN	INR0109	99.76%
	Backup / IPVPN	INR0107	99.96%
MONTERIA	Principal / IPVPN	INR0080	100.00%
	Backup / IPVPN	INR0081	99.80%

RIOHACHA	Principal / IPVPN	INR0164	98.94%
	Backup / IPVPN	INR0162	98.54%
SANTA MARTA	Principal / IPVPN	INR0154	100.00%
	Backup / IPVPN	INR0152	99.82%
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	100.00%
CUCUTA	Principal / IPVPN	INR0044	100.00%
	Backup / IPVPN	INR0047	99.68%
VALLEDUPAR	Principal / IPVPN	INR0091	99.96%
	Backup / IPVPN	INR0090	99.96%
YOPAL	Principal / IPVPN	INR0121	100.00%
	Backup / IPVPN	INR0123	99.98%
ARAUCA	Principal / IPVPN	INR0110	96.68%
CALI	Principal / IPVPN	INR0151	100.00%
	Backup / IPVPN	INR0153	100.00%
BUENAVENTURA	Principal / IPVPN	INR0051	99.98%
MOCOA	Principal / IPVPN	INR0135	99.97%
	Backup / Satelital	INR0136	100.00%
PASTO	Principal / IPVPN	INR0130	94.55%
	Backup / IPVPN	INR0131	99.98%
POPAYAN	Principal / IPVPN	INR0035	99.30%
	Backup / IPVPN	INR0032	100.00%
TUMACO	Principal / IPVPN	INR0147	88.98%
WAN general (concentrador total red)	Principal /IPVPN	INR0266	100,00%
WAN general (concentrador total red)	Backup / IPVPN	INR0171	89,89%
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	100.00%

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	100.00%
DECEVAL hasta Edificio de ICETEX Dirección General.	Ubicado en Datacenter Principal, interconectado a través de red MPLS (Backup)	INR0000289	100.00%
Salida del portales https://portal.icetex.gov.co/portal y www.icetex.gov.co hacia internet en centro de cómputo principal	Internet Reverso para Portales	INR0000317	100.00%
Salida de los portales https://portal.icetex.gov.co/portal y www.icetex.gov.co hacia internet en centro de cómputo de contingencia	Internet Reverso para Portales		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	Sin sede
Quibdó	Canal de backup

Tabla 2 Canales pendientes por instalar

En conclusión, se prestó el servicio en las sedes del Icetex brindando conectividad y sin interrumpir la operación del Instituto. Durante el mes de enero se realizaron 29 ampliaciones y quedan pendientes 19, es decir van un 60.4% 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.	Backup / IPVPN (Sede chapinero)	INR0020	22	25	25	0
NEIVA	Backup / IPVPN	INR0041	8	10	10	0
CUCUTA	Principal / IPVPN	INR0044	18	20	20	0
	Backup / IPVPN	INR0047	8	10	10	0
BUCARAMANGA	Backup / IPVPN	INR0061	12	20	20	0
ARMENIA	Principal / IPVPN	INR0074	15	20	20	0

	Backup / IPVPN	INR0072	8	10	10	0
MONTERIA	Principal / IPVPN	INR0080	18	20	20	0
	Backup / IPVPN	INR0081	8	10	10	0
VILLAVICENCIO	Principal / IPVPN	INR0084	18	20	20	0
	Backup / IPVPN	INR0085	8	10	10	0
TUNJA	Principal / IPVPN	INR0104	18	20	20	0
MANIZALES	Principal / IPVPN	INR0088	18	20	20	0
	Backup / IPVPN	INR0087	8	10	10	0
APARTADO	Principal / IPVPN	INR0144	15	20	20	0
BARRANQUILLA	Principal / IPVPN	INR0103	63	100	100	0
	Backup / IPVPN	INR0100	15	20	20	0
CARTAGENA	Principal / IPVPN	INR0109	18	20	20	0
RIOHACHA	Backup / IPVPN	INR0162	8	10	10	0
SANTA MARTA	Principal / IPVPN	INR0154	18	20	20	0
	Backup / IPVPN	INR0152	8	10	10	0
SINCELEJO	Principal / IPVPN	INR0095	15	20	20	0
VALLEDUPAR	Principal / IPVPN	INR0091	18	20	20	0
	Backup / IPVPN	INR0090	8	10	10	0
YOPAL	Backup / IPVPN	INR0123	8	10	10	0
ARAUCA	Principal / IPVPN	INR0110	15	20	20	0
PASTO	Principal / IPVPN	INR0130	18	20	20	0
	Backup / IPVPN	INR0131	8	10	10	0
TUMACO	Principal / IPVPN	INR0147	18	20	20	0

Tabla 3 Canales ampliados enero 2024

CIUDAD	Enlace - Tipo medio	Código Servicio	BW- Mínimo Requerido (MBPS)	Ancho de Banda Ofrecido	Ancho de Banda Prestado	Diferencia (MBPS)
QUIBDO	Principal / IPVPN	INR0014	18	20	18	2
BOGOTA D.C.	Principal / FO (Sede Aguas)	INR0037	370	400	370	30
	Backup / FO (Sede Aguas)	INR0036	160	200	160	40
	Principal / IPVPN (Sede Chapinero)	INR0022	38	40	38	2
YOPAL	Principal / IPVPN	INR0121	18	20	18	2
CARTAGENA	Backup / IPVPN	INR0107	8	10	8	2
IBAGUE	Principal / IPVPN	INR0073	18	20	18	2
	Backup / IPVPN	INR0076	8	10	8	2
PEREIRA	Principal / IPVPN	INR0079	18	20	18	2
	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 enero 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	99.95%
BUCARAMANGA	INTERNET PARA LA GENTE	INR0057	100.00%
CALI	INTERNET PARA LA GENTE	INR0160	100.00%
AGUAS	INTERNET PARA LA GENTE	INR0034	100.00%
CHAPINERO	INTERNET PARA LA GENTE	INR0015	100.00%
MEDELLIN	INTERNET PARA LA GENTE	INR0022	100.00%
APARTADO	INTERNET PARA LA GENTE	INR0140	100.00%
ARAUCA	INTERNET PARA LA GENTE	INR0115	96.80%
LETICIA	INTERNET PARA LA GENTE		0.00%
QUIBDO	INTERNET PARA LA GENTE	INR0021	100.00%
RIOHACHA	INTERNET PARA LA GENTE	INR0159	98.94%
SAN ANDRES	INTERNET PARA LA GENTE		0.00%
YOPAL	INTERNET PARA LA GENTE	INR0127	99.99%
MOCOA	INTERNET PARA LA GENTE	INR0141	99.96%

Tabla 5 Disponibilidad canales "Internet para la gente"

Quedan pendientes 2 instalaciones que son: Leticia y San Andrés por falta de sede.

4.2 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 enero, funcionó sin ningún contratiempo.

La evidencia se encuentra en el informe [Informe Técnico replicación INFOTIC v.1.pdf](#)

The screenshot shows the VMware Site Recovery Manager (SRM) interface. The top navigation bar includes 'Site Recovery' and 'Replicaciones'. The main content area displays a list of replication channels between 'vmegacenter.datacenterdhs.local' and 'vcsatriara-ext.datacenterdhs.local'. The table below represents the data shown in the interface.

Máquina virtual	Estado	RPO	Origen	Servidor de replicación
INR0226_INFOTIC_REP	✓ Correcto	1 hora	vcsatriara-ext.datacenterdhs.local	TFM3837_CLARO_VRA
INR0228_INFOTIC_REP	✓ Correcto	1 hora	vcsatriara-ext.datacenterdhs.local	TFM3837_CLARO_VRA
INR0229_INFOTIC_REP	✓ Correcto	1 hora	vcsatriara-ext.datacenterdhs.local	TFM3837_CLARO_VRA
INR0233_INFOTIC_REP	✓ Correcto	1 hora	vcsatriara-ext.datacenterdhs.local	TFM3837_CLARO_VRA
INR0236_INFOTIC_REP	✓ Correcto	1 hora	vcsatriara-ext.datacenterdhs.local	TFM3837_CLARO_VRA
INR0237_INFOTIC_REP	✓ Correcto	1 hora	vcsatriara-ext.datacenterdhs.local	TFM3837_CLARO_VRA
INR0238_INFOTIC_REP	✓ Correcto	1 hora	vcsatriara-ext.datacenterdhs.local	TFM3837_CLARO_VRA
INR0239_INFOTIC_REP	✓ Correcto	1 hora	vcsatriara-ext.datacenterdhs.local	TFM3837_CLARO_VRA
INR0243_INFOTIC_REP	✓ Correcto	1 hora	vcsatriara-ext.datacenterdhs.local	TFM3837_CLARO_VRA
INR0244_INFOTIC_REP	✓ Correcto	1 hora	vcsatriara-ext.datacenterdhs.local	TFM3837_CLARO_VRA
INR0245_INFOTIC_REP	✓ Correcto	1 hora	vcsatriara-ext.datacenterdhs.local	TFM3837_CLARO_VRA
INR0249_INFOTIC_REP	✓ Correcto	1 hora	vcsatriara-ext.datacenterdhs.local	TFM3837_CLARO_VRA
INR0262_INFOTIC_REP	✓ Correcto	1 hora	vcsatriara-ext.datacenterdhs.local	TFM3837_CLARO_VRA

Ilustración 3 Evidencia del canal de replicación entre Triara y Megacenter

4.3 CONCLUSIONES DEL SERVICIO DE CONECTIVIDAD

En la operación del mes de enero:

- Se cuenta con el 100% de los canales principales instalados a nivel nacional en los cuales Icetex tiene sede.
- Se han implementado 28 de 29 canales, el 96.5% de los canales Backup.
- Se implementó el 100% de los canales “Internet para la gente” donde Icetex tiene sede.
- Se lograron atender todos los casos y se cerraron en los tiempos establecidos.

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

5 SERVICIOS CENTROS DE COMPUTO

5.1 Datacenter Principal

Para el mes de enero 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

PROMEDIO CONSUMO DE MEMORIA

View: month

From: 1/1/2024 12:00 AM

To: 2/1/2024 12:00 AM

America/Bogota

Sample type: ss_hr_t

Nombre de destino	Nombre del monitor	Valor mínimo	Valor máximo	Valor promedio
iceteboglxdarumatest	Memory	35.00	98.00	85.70
icetexbogliferaynfs	Memory	34.00	98.00	96.77
icetexboglxdarumasrv1	Memory	52.00	97.00	83.60
icetexboglxdarumasrv2	Memory	52.00	97.00	89.60
icetexboglxroad1	Memory	63.00	98.00	95.75
icetexboglxroad2n	Memory	97.00	98.00	97.23
icetexboglxroad3	Memory	66.00	97.00	83.89
icetexboglxroadtest	Memory	81.00	89.00	85.68
ictxprusisgapp	Memory	60.00	80.00	63.52
ictxisgesapp	Memory	25.00	54.00	44.17
ictxisgesbd	Memory	86.00	88.00	86.93
inr0233_icetexboglxorfeo1.localdomain	Memory	13.00	21.00	18.10
inr0237_icetexbogbalserver1-r	Memory	4.00	11.00	5.04
inr0239_icetexbogelasticserver1	Memory	2.00	17.00	15.78
inr0241_icetexbogelasticserver3	Memory	31.00	31.00	31.00
inr0242_icetexbogliferayserv2	Memory	2.00	87.00	79.77
inr0243_icetexbogliferayserv1	Memory	7.00	56.00	50.14
inr0262_icetexboglxorfeo2.localdomain	Memory	5.00	13.00	5.93
inr0276_cxvodaprodn011	Memory	58.00	71.00	59.91
inr0277_cxvodaprodn021	Memory	60.00	65.00	61.97
inr0278_cxvodacontg011	Memory	45.00	47.00	46.29

Ilustración 4 Evidencia del Resumen del Monitoreo

5.1.1 Disponibilidad de Servicios – Datacenter Principal

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

PROMEDIO DE DISPONIBILIDAD		
View: month		
From: 1/1/2024 12:00 AM	To: 2/1/2024 12:00 AM	America/Bogota
Sample type: ss_hr_t		
Nombre de destino	Nombre del monitor	Disponibilidad
iceteboglxdarumatest	Ping	100.00
icetexbogliferaynfs	Ping	100.00
iceteboglxdarumasrv1	Ping	100.00
iceteboglxdarumasrv2	Ping	100.00
iceteboglxroad1	Ping	100.00
iceteboglxroad2n	Ping	100.00
iceteboglxroad3	Ping	100.00
iceteboglxroadtest	Ping	100.00
ictxprusigapp	Ping	99.84
ictxsisgesapp	Ping	99.84
ictxsisgesbd	Ping	99.91
inr0233_iceteboglxorfeo1.localdomain	Ping	99.98
inr0237_iceteboglbserver1-r	Ping	99.92
inr0239_icetebogelasticserver1	Ping	100.00
inr0241_icetebogelasticserver3	Ping	100.00
inr0242_icetebogliferayserver2	Ping	99.98
inr0243_icetebogliferayserver1	Ping	99.77
inr0262_iceteboglxorfeo2.localdomain	Ping	100.00
inr0276_cxvodaprodn011	Ping	100.00
inr0277_cxvodaprodn021	Ping	100.00
inr0278_cxvodacontg011	Ping	99.98

Ilustración 5 Evidencia Disponibilidad Servicio Datacenter Principal

A continuación, se muestra la evidencia del estado activo de las 11 máquinas virtuales que forman parte del OPENSIFT(INR251-INR252-INR253-INR254-INR255-INR256-INR257-INR258-INR259-INR260-INR261) en el Datacenter Principal, se aclara que esta evidencia en una excepción aceptada por ICETEX durante este mes y el mes anterior:

CLT314_TRI_COM_OCTADECACORE09_ACL_ADD

ACCIONES

Resumen

Supervisar

Configurar

Permisos

Hosts

Máquinas virtuales

Almacenes de datos

Redes

Actualizaciones

Máquinas virtuales

Plantillas de máquina virtual

vApps

INR02

☐	Nombre	Estado	Condición	Espacio aprovisionado	Espacio utilizado	CPU de host	Memoria de host
☐	 INR0242_INFOTIC_CLON	Encendido	 Normal	954,66 GB	954,66 GB	91 MHz	7,06 GB
☐	 INR0242_NEW	Encendido	 Normal	365,09 GB	365,09 GB	0 Hz	5,96 GB
☐	 INR0233_INFOTIC_REP	Encendido	 Normal	11,26 TB	11,26 TB	137 MHz	15,98 GB
☐	 INR0262_INFOTIC_REP	Encendido	 Normal	319,3 GB	319,3 GB	68 MHz	32,03 GB
☐	 INR0261_INFOTIC	Encendido	 Normal	107,08 GB	107,08 GB	0 Hz	2,3 GB
☐	 INR0260_INFOTIC	Encendido	 Normal	830,23 GB	830,23 GB	849 MHz	7,97 GB
☐	 INR0252_INFOTIC	Encendido	 Normal	830,25 GB	830,25 GB	114 MHz	7,96 GB
☐	 INR0258_INFOTIC_OLD	Encendido	 Normal	168,24 GB	168,24 GB	2,18 GHz	15,86 GB
☐	 INR0259_INFOTIC_OLD	Encendido	 Normal	152,24 GB	152,24 GB	2,27 GHz	16,08 GB
☐	 INR0257_INFOTIC_OLD	Encendido	 Normal	184,3 GB	184,3 GB	1,29 GHz	31,87 GB
☐	 INR0256_INFOTIC_OLD	Encendido	 Normal	184,55 GB	184,55 GB	2,32 GHz	31,91 GB
☐	 INR0255_INFOTIC_OLD	Encendido	 Normal	184,28 GB	184,28 GB	2,02 GHz	32,13 GB
☐	 INR0254_INFOTIC_OLD	Encendido	 Normal	184,25 GB	184,25 GB	1,33 GHz	32,12 GB
☐	 INR0251_INFOTIC_OLD	Encendido	 Normal	152,21 GB	152,21 GB	2,64 GHz	16,07 GB
☐	 INR0236_INFOTIC_REP	Encendido	 Normal	235,24 GB	235,24 GB	436 MHz	23,36 GB
☐	 INR0235_INFOTIC	Encendido	 Normal	235,35 GB	235,35 GB	413 MHz	18,68 GB

EXPORTAR

Elementos por página

35

26 ele

CLT310_TRI_COM_OCTADECACORE06_ACI

ACCIONES

Resumen

Supervisar

Configurar

Permisos

Hosts

Máquinas virtuales

Almacenes de datos

Redes

Actualizaciones

Máquinas virtuales

Plantillas de máquina virtual

vApps

inr0253

☐	Nombre	Estado	Condición	Espacio aprovisionado	Espacio utilizado	CPU de host	Memoria de host
☐	 INR0253_INFOTIC	Encendido	 Normal	308,09 GB	274,01 GB	25 MHz	5,18 GB

 EXPORTAR

Elementos por página 35 1 elemento

	Detalles	Iniciador	En cola por	Hora de inicio	Hora de finalización	Servidor
20 %	Migrando el estado activo d...	System	3 ms	25/04/2024, 10:28:41		vcsatriara-ext...

1-25 de 39 elementos 1 / 2

Ilustración 6 Disponibilidad Servidores OPENSIFT– Datacenter Principal

5.1.2 Disponibilidad de Servicios de Housing – Datacenter Principal

El siguiente cuadro presenta el porcentaje de disponibilidad de los servidores en Datacenter principal:

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

	Slot B2 -Tarjeta Enclosure - M1000				
--	------------------------------------	--	--	--	--

Tabla 6 Disponibilidad de Servicios de Housing – Datacenter Principal

5.1.3 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 % Nodo 1 y 99.9% Nodo 2 del sitio durante el mes de Enero [ReportDynatracePortal Enero2024.pdf](#)

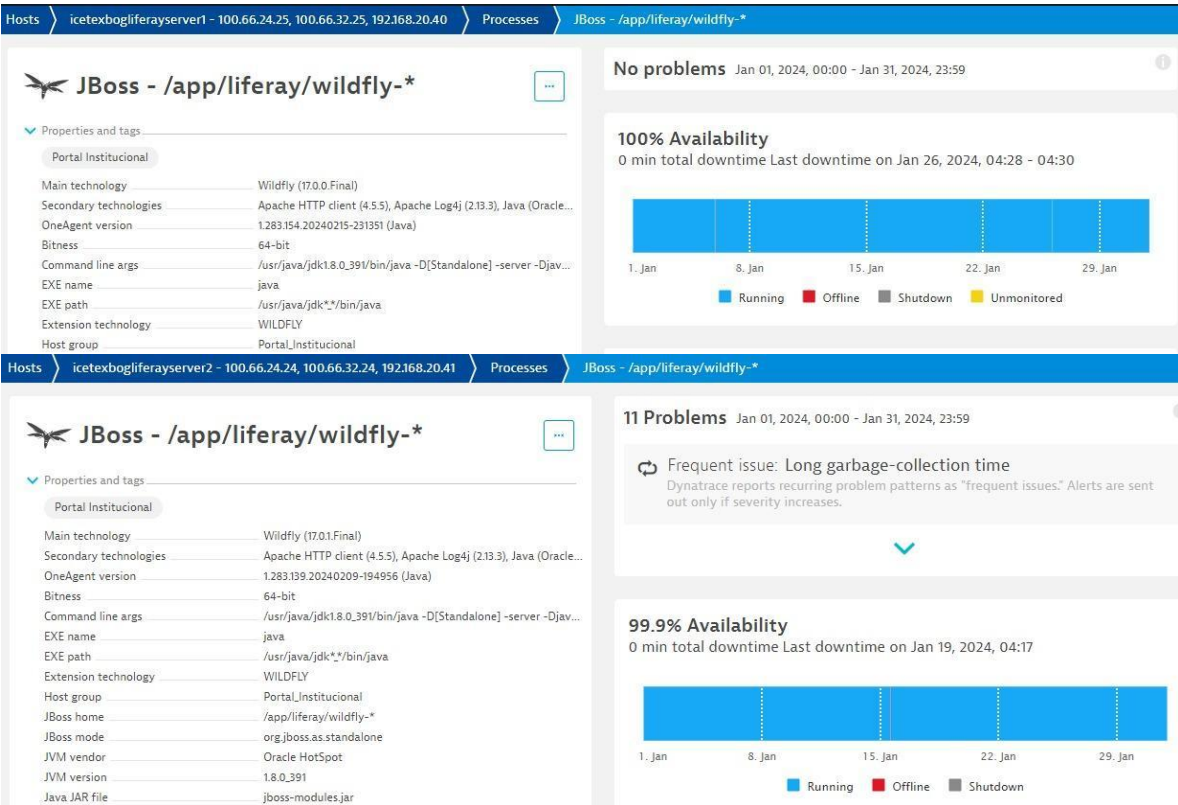


Ilustración 7 Disponibilidad Servicios Portal Web Ictex (Dynatrace)

5.1.4 Backup Servidores Triara

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



Ilustración 8 Evidencia Backup Servidores

5.2 Datacenter Alterno

5.2.1 Hosting Virtual (IaaS)

En el transcurso del mes de enero 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 Técnico replicación INFOTIC v.1.pdf](#)

Topología del Servicio

A continuación, se muestra la topología del servicio implementado:

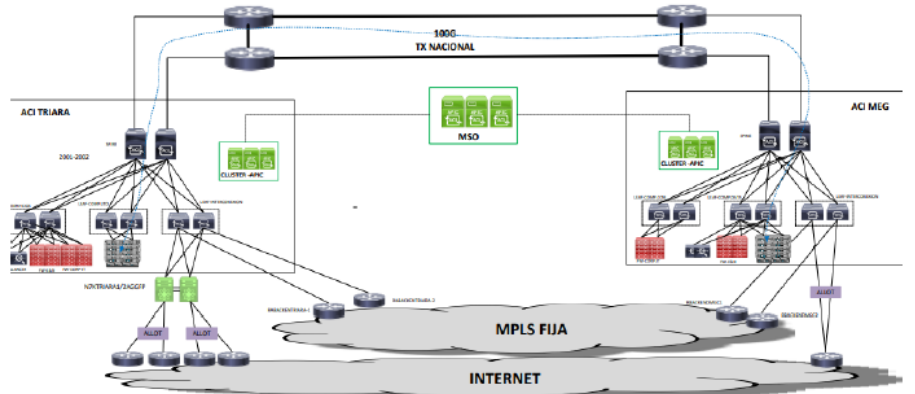


Ilustración 9 Evidencia replicación SRM a Sitio Alterno, ENERO-2024

 Informe técnico

Enero 15 de 2024

The screenshot shows a Windows 10 desktop with a taskbar at the bottom. The active application is Microsoft Excel, displaying a spreadsheet titled "2024-05-24-08-26.gsm_3026h_Mega". The spreadsheet has a header row with columns labeled A through H. The data rows show network connection information for various VMs.

A	B	C	D	E	F	G	H
VM	Connection state	Band state	Bandwidth	Creation date	Change events	CPU%	Memory
WIN2028-WFOVTC-BGP	connected	not running	gray	2024/01/14 08:07:33	2024/04/17 03:10:42	12	32.76%
WIN2028-WFOVTC-BGP	connected	not running	gray	2024/01/19 18:38:02	2024/02/17 03:10:42	4	8.39%
WIN2029-WFOVTC-BGP	connected	not running	gray	2024/01/13 19:51:24	2024/02/12 19:56:23	4	8.39%
WIN2033-WFOVTC-BGP	connected	not running	gray	2023/11/17 14:08:19	2024/03/12 16:58:54	6	8.39%
WIN2036-WFOVTC-BGP	connected	not running	gray	2023/11/19 16:05:50	2024/03/17 03:10:42	10	32.76%
WIN2037-WFOVTC-BGP	connected	not running	gray	2023/11/19 16:04:50	2024/02/12 18:02:50	6	32.76%
WIN2038-WFOVTC-BGP	connected	not running	gray	2024/01/09 16:22:17	2024/04/12 18:02:50	4	8.39%
WIN2040-WFOVTC-BGP	connected	not running	gray	2024/01/22 15:33:04	2024/02/12 15:33:04	6	8.39%
WIN2042-WFOVTC-BGP	connected	not running	gray	2023/11/19 16:04:49	2024/02/12 18:02:50	6	40.86%
WIN2044-WFOVTC-BGP	connected	not running	gray	2024/01/22 15:26:07	2024/04/12 15:26:08	2	5.34%
WIN2045-WFOVTC-BGP	connected	not running	gray	2023/11/14 08:03:01	2023/11/28 03:10:42	4	5.34%
WIN2046-WFOVTC-BGP	connected	not running	gray	2023/11/14 08:02:29	2023/11/17 19:58:54	6	8.39%
WIN2050-WFOVTC-BGP	connected	not running	gray	2023/11/17 08:01:03	2024/02/12 16:58:54	4	32.76%

Enero 31 de 2024

The screenshot shows the Microsoft Excel application window. The title bar indicates the file name is "2024-01-31-00-Wg-mg_AvSofts_Mega". The ribbon is set to "Formulas", and the "AutoSum" dropdown is visible. The spreadsheet contains data for various VMs, with columns for VM, Connection state, Config state, Download, Creation date, Cleanup (days), Cpu%, and Memory. The data is organized into rows, with the first row (row 1) serving as the header. The data rows start from row 2 and continue down to row 25. The data includes IP addresses, connection states (connected, not running), and various numerical values representing cleanup days, CPU usage, and memory usage.

VM	Connection state	Config state	Download	Creation date	Cleanup (days)	Cpu%	Memory
14 1949228_1MORTC_REPO	connected	not running	gruy	2023/11/14 08:07:51	2024/01/31 85:39:43	13	252.566
15 1949228_1MORTC_REPO	connected	not running	gruy	2024/01/15 18:28:01	2024/01/31 82:39:42	4	8.392
16 1949229_1MORTC_REPO	connected	not running	gruy	2024/01/12 18:31:24	2024/01/29 84:40:34	4	8.392
17 1949229_1MORTC_REPO	connected	not running	gruy	2023/11/17 14:08:19	2024/01/29 12:12:04	6	3.384
18 1949228_1MORTC_REPO	connected	not running	gruy	2023/12/19 15:03:56	2024/01/31 83:03:15	16	32.768
19 1949228_1MORTC_REPO	connected	not running	gruy	2023/11/19 18:04:30	2024/01/29 12:04:30	8	32.768
20 1949228_1MORTC_REPO	connected	not running	gruy	2023/11/09 18:02:17	2024/01/29 12:04:34	4	8.392
21 1949228_1MORTC_REPO	connected	not running	gruy	2024/01/08 18:02:48	2024/01/29 12:04:34	6	3.384
22 1949243_1MORTC_REPO	connected	not running	gruy	2023/11/19 18:04:48	2024/01/29 12:04:34	6	40.864
23 1949244_1MORTC_REPO	connected	not running	gruy	2024/01/22 15:38:07	2024/01/31 30:48:47	2	6.344
24 1949245_1MORTC_REPO	connected	not running	gruy	2023/11/14 08:03:01	2024/01/31 30:48:47	2	6.344
25 1949245_1MORTC_REPO	connected	not running	gruy	2023/11/14 08:02:26	2024/01/29 17:06:48	4	6.344
26 1949245_1MORTC_REPO	connected	not running	gruy	2023/11/17 08:01:41	2024/01/31 21:12:03	4	32.768

Ilustración 10 Reportes de replicación SRM a Sitio Alterno, ENERO 2024

5.2.2 Dataguard BBDD Megacenter

En el periodo del mes de enero se realizó la réplica permanente de las BD Oracle al Datacenter alternativo de acuerdo con las políticas establecidas, utilizando el Dataguard. Ver las evidencias en el documento [INFOTIC ICETEX - Evidencias Dataguard 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/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 -fe|grep pmon
grid      8511      1 0 Feb18 ?        00:00:10 asm_pmon +ASM
oracle    8988  8595  0 19:52 pts/2    00:00:00 grep --color=auto pmon
oracle    9456      1 0 Feb18 ?        00:00:29 ora_pmon APOTEOSED
oracle    9707      1 0 Feb18 ?        00:00:27 ora_pmon ICTXCXCD
oracle    9961      1 0 Feb18 ?        00:00:16 ora_pmon VIGIADTG
oracle   10210      1 0 Feb18 ?        00:00:16 ora_pmon LIFERAYD
oracle   10455      1 0 Feb18 ?        00:00:16 ora_pmon LANDICTD
oracle   10688      1 0 Feb18 ?        00:00:28 ora_pmon APPLICATD
oracle   10876      1 0 Feb18 ?        00:00:28 ora_pmon APOTNEWD
oracle   11068      1 0 Feb18 ?        00:00:28 ora_pmon ICETEXD

[oracle@cxvodacontg011 ~]$ . oraenv
ORACLE_SID = [ICTXCXCD] ?
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 Remains unchanged with value /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 Mon Feb 19 19:52:32 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 faplyb

      Thread Last Sequence Received Last Sequence Applied TIME RECEIVED      TIME APPLIED
-----
          1             41903             41903 31/01/2024 19:42 31/01/2024 19:42
          2             33131             33131 31/01/2024 19:25 31/01/2024 19:25

SQL> sta uaplyb

      Thread Last Sequence Received Last Sequence Applied Difference
-----
          1             41903             41903             0
          2             33131             33131             0

SQL>

```

Ilustración 11 Evidencia Dataguard replicado a Megacenter BD

Se generó la consulta de los archivos recibidos y aplicados de la base de datos de ICTXCXCD a 31/01/2024 19:42 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).

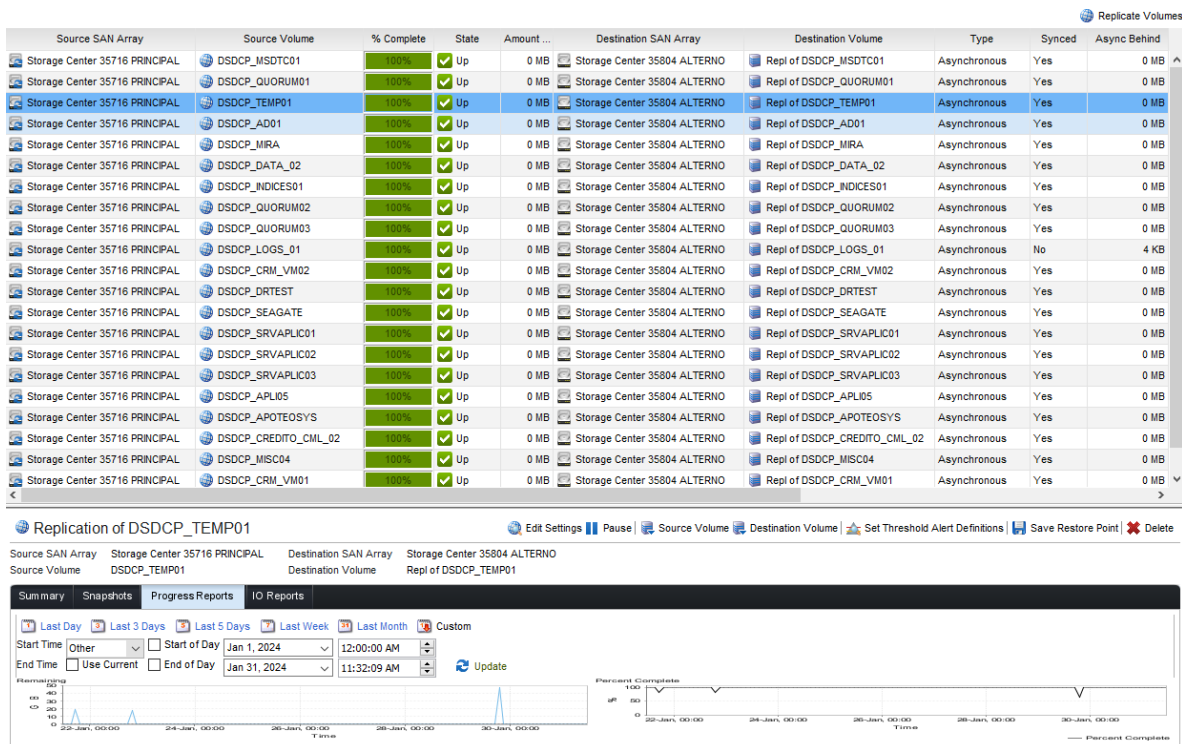


Ilustración 12 Evidencia replicado servicios On-premise Icetex a Megacenter

5.2.4 Disponibilidad de Servicios de Housing – Datacenter Alterno

A continuación, se presentan las máquinas alojadas en el Datacenter alternativo en Medellín, las cuales estuvieron disponibles todo el mes 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 7 Disponibilidad de Servicios de Housing – Datacenter Alterno

6 SEGURIDAD

En este capítulo se hará referencia a las diferentes actividades que se realizaron durante el mes de enero, 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 diciembre 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 [Informe enero 2024 seguridad.pdf](#) en el capítulo PORTALES PROTEGIDOS POR EL WAF

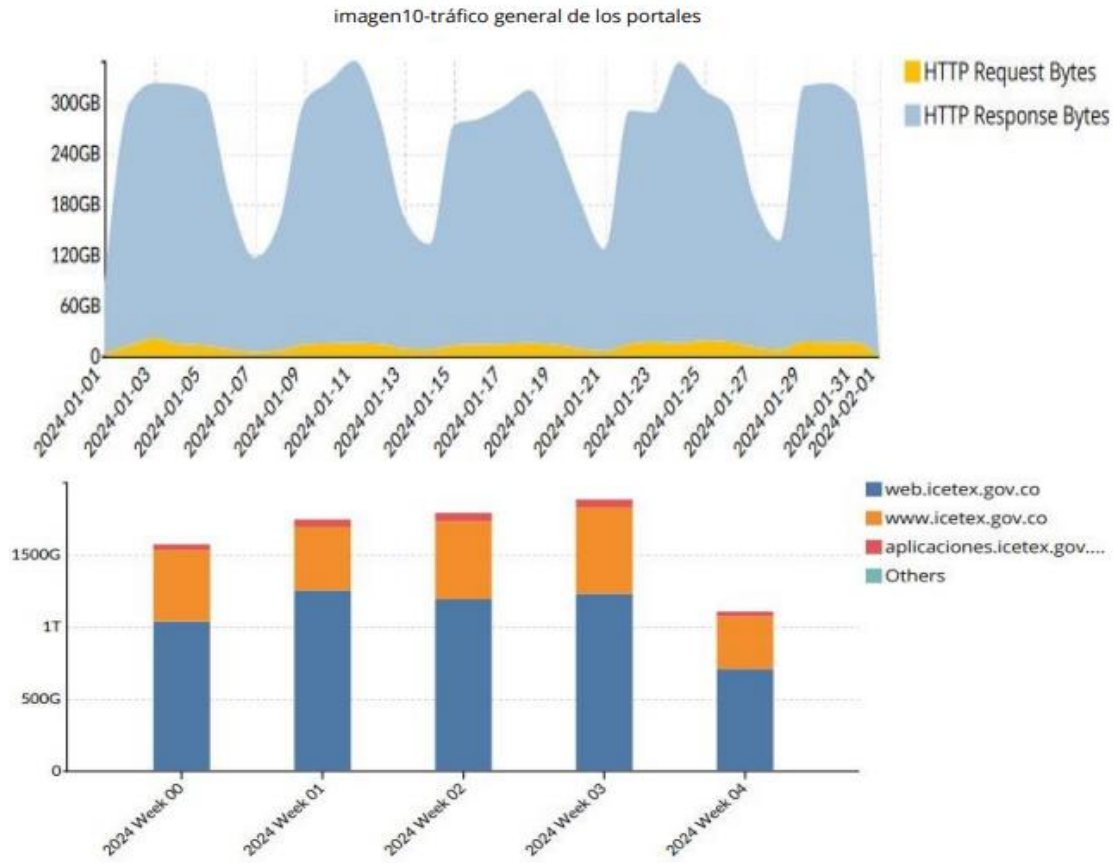


Ilustración 13 Evidencia Gráfica Estadísticas de Portales

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



Ilustración 14 Evidencia Estado General de las Plataformas

6.4 Estado de Salud de los Equipos de Seguridad

En el transcurso del mes de diciembre 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 [Informe enero 2024 seguridad.pdf](#)



Ilustración 15 Evidencia Estado de Salud de los Equipos de Seguridad

6.5 Servicio de centro de Operaciones de Seguridad (SOC)

Durante el mes de enero 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 [240131 Informe Mensual SOC ICETEX Enero 2024.pdf](#)

TLP:ROJO

INFORME MENSUAL MONITOREO SOC

Página

6 de 62

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.

Resources > Rules > Security

New

Edit

Delete

Clone

Test

Search...

Import

Export

1/27

1,326

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.

Resources > Rules > Availability

New

Edit

Delete

Clone

Test

Search...

Import

Export

1/4

157

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.

Resources > Rules > Performance

New

Edit

Delete

Clone

Test

Search...

Import

Export

1/5

231

Ilustración: Cantidad de reglas de Rendimiento

Ilustración 16 Evidencia Imagen Reporte Monitoreo

6.5.1 Monitoreo de Marca (SOC)

Para el mes de Enero 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 [240201 Informe Marca - OSINT ICETEX Enero 2024.pdf](#)

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

23





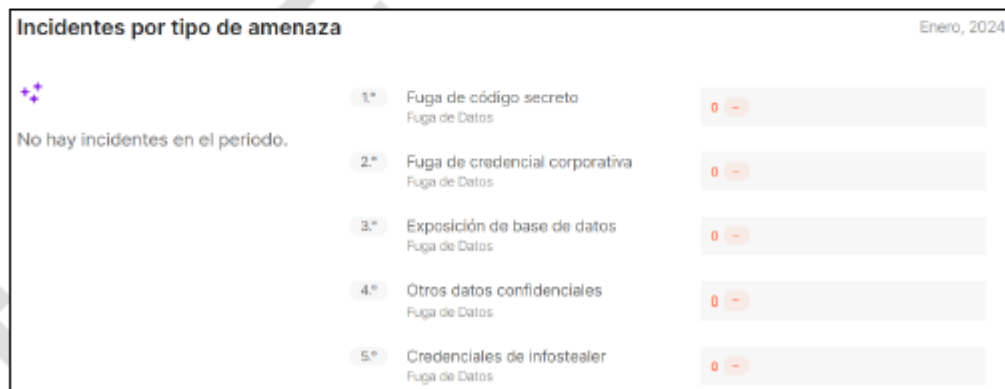
CO-SC-CER921046

4. ANÁLISIS DE MONITOREO DE MARCA

Durante el periodo evaluado, la plataforma de monitoreo de marca – AXUR, reporta un total de **83** posibles amenazas de las 58,1k que fueron encontradas y analizadas automáticamente por la plataforma de monitoreo. A estas **83** 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 periodo evaluado, se resolvió **04** casos en la plataforma de monitoreo.



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



Durante el periodo de tiempo evaluado no se detectaron incidentes.

Ilustración 17 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 Ictetex prevenir ataques de Ciberseguridad que comprometan la continuidad del negocio.

- Durante el mes de enero 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

- Verificar las alertas reportadas en este informe de mayor cantidad, e informar al SOC si estos comportamientos o actividades son normales o autorizadas, con el fin de realizar excepciones, filtros o modificación de umbrales para reducir la cantidad de alertas y falsos positivos, como las siguientes:
-FortiWeb: Permitted Inbound Attack Detected
- Realizar bloqueo de las direcciones IP origen o destinos identificadas como maliciosas en indicadores de compromisos- IoC.
- Verificar en otros, con software antimalware, los equipos con direcciones IP origen relacionados en la alerta “Tráfico Permitido o Denegado Hacia IoC Maliciosas – WX” la cual detecta tráfico hacia direcciones IP “maliciosas”. Lo anterior puede indicar que el equipo con IP Origen probablemente está infectado por malware y está intentando conexiones a servidores de comando y control (C&C) o está tratando de iniciar una infección, independientemente si fue negado o permitido el tráfico.
- Informar al SOC, respecto a alertas de disponibilidad (No Ping Response) cuales dispositivos se deben depurar en el SIEM, con el fin de evitar estas alertas y reducir los falsos positivos.
- Verificar y aumentar los recursos del FortiSIEM, en razón a que se están presentando alertas críticas de consumo de CPU que impiden el correcto desarrollo de reportes mensuales, igualmente el SIEM presenta espacio en disco del 100%.
- Revisar los dispositivos que se encuentran en las alertas de rendimiento y si es posible aumentar la capacidad de recursos que en ellos se usan para evitar demoras y/o retrasos de servicio. Por ahora ningún servicio se ha visto indisponible a causa de recursos internos de los dispositivos que se usan para llevar a cabo dichos servicios.

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

- 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.
- 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 de la posición de la seguridad de la información de la entidad ICETEX, permite estar mejor posicionado frente a un incidente informático o de ciberseguridad.

7 GESTIÓN 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 enero, 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 ENERO.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 en el [INFORME ACTIVIDADES ENERO.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:

ÍTEMS	SERVICIO	CIUDAD	DIRECCIÓN	CANTIDAD
1	Sala de video conferencia o sala virtual (Tamaño 65")	Bogotá - Aguas	Carrera 3 No. 18-32	3
2	Sala de video conferencia o sala virtual (Tamaño 65")	Bogotá - Ángel	Cl. 19 #6-68 piso 17	1
3	Sala de video conferencia o sala virtual (Tamaño 55")	Bogotá - Aguas	Carrera 3 No. 18-32	1
SEDES REGIONALES				
4	Sala de video conferencia o 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 8 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 enero 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.

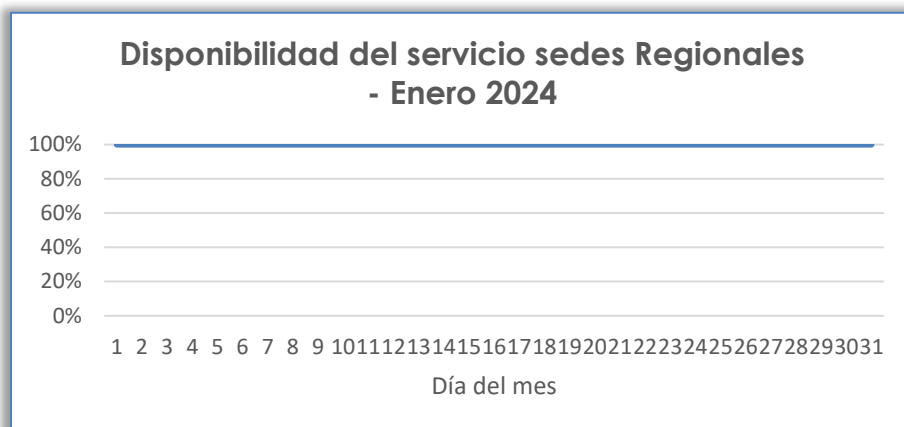


Ilustración 18 Disponibilidad de servicio videoconferencia sedes regionales – Enero 2024

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

En la verificación realizada para el mes de enero 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.

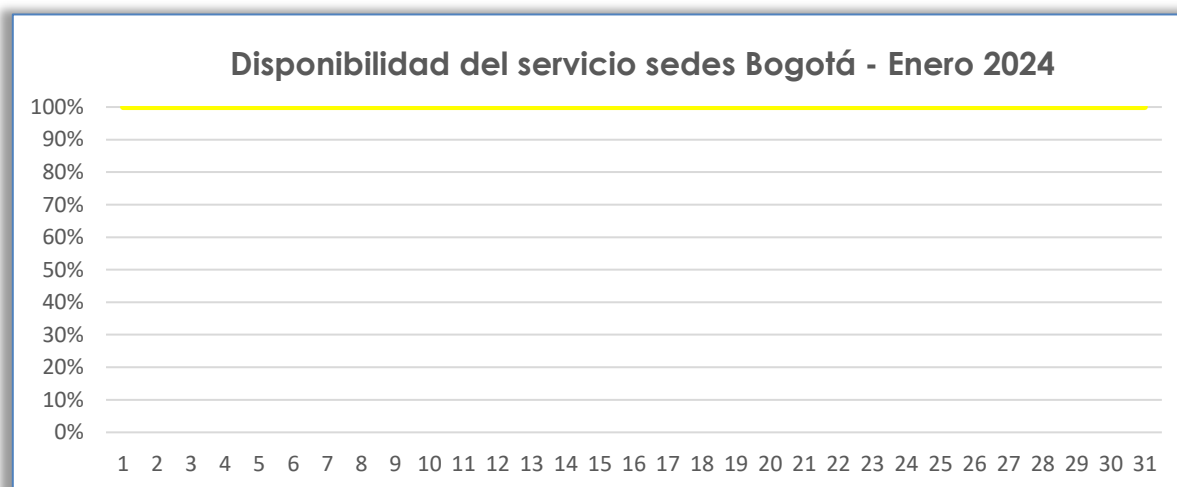


Ilustración 19 Disponibilidad de servicio videoconferencia sedes Bogotá – enero 2024

8.2 Gestión de incidencias y requerimientos – sedes regionales

Para el mes de enero, entre el 1 y el 31 del mes, se generó un (1) requerimiento, como se muestra en la Tabla 8. Su distribución corresponde a revisión y mantenimiento soporte del módulo de videoconferencia de chapinero, con el fin de evitar incidencias de bloqueo en el encendido o en el reinicio cuando se presentan cortes de energía inesperados.

Ítem	Tipo	Requerimiento	Severidad	Estado
1	Requerimiento	soporte técnico de OPS de la sede chapinero: Mantenimiento preventivo y correctivo, con el objetivo de corregir y evitar fallos en el encendido del módulo cuando se reinicia o se presentan cortes de energía no controlados	Media	Cerrado

Tabla 9 Requerimientos sedes regionales

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.

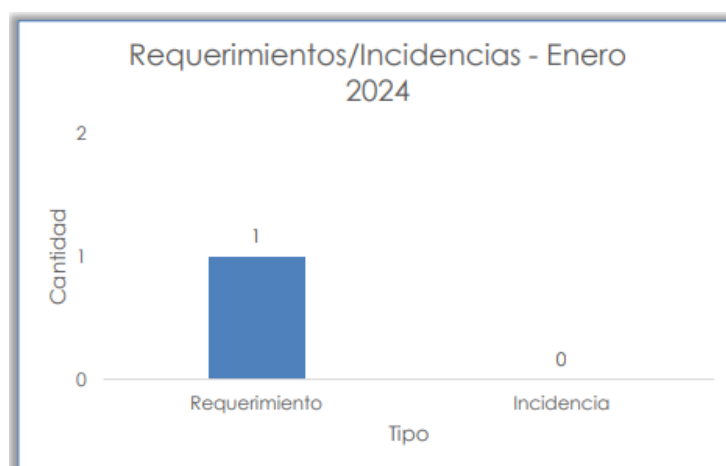


Ilustración 20 Incidencias/Requerimientos sedes Regionales – enero 2024

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

Para el mes de enero, 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 enero 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 Enero 2024.pdf](#)

9 CALCULO DE CONCILIACIÓN DE LOS SERVICIOS DEL MES DE DICIEMBRE

A la fecha la conciliación del mes de enero con ICETEX se encuentra en proceso, el detalle de conciliación del mes anterior se puede ver en el siguiente link [Conciliación enero 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				\$ 5.582.644.616	
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
VALOR CAUSADO QUE NO SE HA PAGADO (valor a pagar factura) *00				\$ 728.801.311,96	
VALOR TOTAL EJECUTADO (valor pagado + valor causado no pagado)				\$ 6.344.575.596	
SALDO DEL CONTRATO (valor total del contrato – valor total ejecutado)				\$ 25.054.421.262	
PORCENTAJE DE EJECUCIÓN				20.21%	
* 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 10 Ejecución Presupuestal