



INFORME DE ACTIVIDADES DEL CONTRATO

**CONTRATO NUMERO
2022-0792**

Marzo 01 al 31 de 2024

CONTENIDO

Contenido

1	INTRODUCCIÓN	4
2	OBJETIVOS	4
3	RESUMEN EJECUTIVO	4
4	SERVICIOS DE CONECTIVIDAD	5
4.1	INTERNET PARA LA GENTE	8
4.2	CANALES SDWAN	9
4.3	Canal de Replicación (Triara – Megacenter)	9
4.4	Señalética (Internet para la gente)	9
4.5	CONCLUSIONES DEL SERVICIO DE CONECTIVIDAD	10
4.6	RECOMENDACIONES DEL SERVICIO DE CONECTIVIDAD	10
5	SERVICIOS CENTROS DE COMPUTO	11
5.1	Datacenter Principal	11
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	19
5.2.3	Replicación Servicios OnPremise de Ictex a Megacenter	21
5.2.4	Disponibilidad de Servicios de Housing – Datacenter Alterno	22
6	SEGURIDAD	22
6.1	Servicios de Endpoint	22
6.2	ESTADÍSTICAS PORTALES	23
6.3	Estado General de las Plataformas	23
6.4	Estado de Salud de los Equipos de Seguridad	24
6.5	Servicio de centro de Operaciones de Seguridad (SOC)	24
6.5.1	Monitoreo de Marca-Estrategia OSINT-SOC	25
6.6	Eventos Relevantes	27
6.7	RECOMENDACIONES	27
6.8	CONCLUSIONES	28
7	GESTION DE SERVICIO	29
7.1	ACTIVIDADES DE OPERACIÓN	29
7.2	Profesionales Especializados	29
7.2.1	Especialista en Base de Datos DBA	29
7.2.2	Especialista web master	29
7.2.3	Administrador de Soluciones	30
7.2.4	Especialista en Networking	30
7.2.5	Especialista Integrador de nube	30
7.2.6	Especialista en seguridad	31

8	SERVICIO DE COLABORACIÓN	31
8.1	<i>Disponibilidad del servicio – sedes Bogotá (aguas - ángel)</i>	32
8.2	<i>Gestión de incidencias y requerimientos – sedes regionales</i>	32
8.3	<i>Gestión de incidencias y requerimientos – Bogotá (Aguas - Angel)</i>	33
9	CALCULO DE CONCILIACIÓN DE LOS SERVICIOS DEL MES DE MARZO	34
	EJECUCIÓN PRESUPUESTAL	34

INDICE DE TABLAS

Tabla 1	Disponibilidad de canales	7
Tabla 2	Canales pendientes por instalar	8
Tabla 3	Canales pendientes por ampliar	8
Tabla 4	Disponibilidad canales “Internet para la gente”	9
Tabla 5	Disponibilidad canales “SDWAN”	9
Tabla 6	Estado de la instalación de la señalética de Wifi	10
Tabla 7	Códigos relacionados Disponibilidad Servicios en Housing – Datacenter Principal	15
Tabla 8	Disponibilidad de Servicios de Housing – Datacenter Principal	15
Tabla 9	Servicios replicados – Datacenter MEGACENTER.....	19
Tabla 10	Disponibilidad de Servicios de Housing – Datacenter Alterno	22
Tabla 11	Recomendaciones plataformas de seguridad	27
Tabla 12	Recomendaciones de seguridad para Icetex	28
Tabla 13	Distribución módulos de videoconferencia por sede.....	31
Tabla 14	Ejecución Presupuestal.....	34

INDICE DE ILUSTRACIONES

Ilustración 1	Evidencia del Resumen del Monitoreo	12
Ilustración 2	Promedio Disponibilidad Servicios en Housing – Datacenter Principal	13
Ilustración 3	Disponibilidad Nodo1 Servicios Portal Web Icetex (Dynatrace)	16
Ilustración 4	Disponibilidad Nodo 2 Servicios Portal Web Icetex (Dynatrace)	16
Ilustración 5	Evidencia Backup Servidores.....	17
Ilustración 6	Reportes de replicación SRM a Sitio Alterno, marzo 2024.....	18
Ilustración 7	Evidencia Dataguard replicado a Megacenter BD.....	21
Ilustración 8	Evidencia replicado servicios On-premise Icetex a Megacenter	22
Ilustración 9	Evidencia Gráfica Estadísticas de Portales	23
Ilustración 10	Evidencia Estado General de las Plataformas	24
Ilustración 11	Evidencia Estado de Salud de los Equipos de Seguridad.....	24
Ilustración 12	Evidencia Imagen Reporte Monitoreo	25
Ilustración 13	Evidencia Imagen Reporte Monitoreo OSINT	26
Ilustración 14	Disponibilidad de servicio videoconferencia sedes regionales – marzo 2024	32
Ilustración 15	Disponibilidad de servicio videoconferencia sedes Bogotá – marzo 2024	32
Ilustración 16	Incidencias/Requerimientos sedes Regionales – marzo 2024	33

1 INTRODUCCIÓN

Este informe contiene la información relacionada con las actividades ejecutadas por INFOTIC en el periodo comprendido entre el 01 al 31 de marzo 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 marzo 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 31 de marzo 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 marzo se coordinaron las ampliaciones de anchos de banda pendientes de los canales donde INFOTIC en su propuesta económica planteo como adicional a lo contractual, sin embargo, las implementaciones se proyecta su ejecución en los próximos meses, 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.

Servicio de Seguridad: Las herramientas de seguridad operaron sin novedad. durante este mes no ha habido vulnerabilidades encontradas en los equipos de seguridad perimetral.

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 marzo 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 marzo 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 marzo de 2024.

4 SERVICIOS DE CONECTIVIDAD

Durante el mes de marzo, los canales principales y Backup instalados operaron de manera normal. La herramienta Solar Winds permite la graficación de los canales, pero las descargas de data se generan incompletas para los últimos 3 meses, INFOTIC ha estado haciendo el seguimiento oportunamente al operador de esta incidencia, 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 es un tema a nivel del reporteador.

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 Marzo 2024 - ALLOT INFOTIC.pdf](#)

Durante el mes de marzo 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 marzo 2024.pdf](#)

Sede	Categoría	INR	% Mes
BOGOTA D.C.	Principal / FO (Sede Aguas)	INR0037	100.00%
	Backup / FO (Sede Aguas)	INR0036	99.93%
	Principal / IPVPN (Sede Chapinero)	INR0022	99.05%
	Backup / IPVPN (Sede chapinero)	INR0020	100.00%
	Principal / IPVPN (Angel)	INR0272	100.00%
	Backup / IPVPN (Angel)	INR0273	100.00%
IBAGUE	Principal / IPVPN	INR0073	100.00%
	Backup / IPVPN	INR0076	100.00%
LETICIA	Principal / Satelital		0,00%

NEIVA	Principal / IPVPN	INR0039	100.00%
	Backup / IPVPN	INR0041	99.87%
TUNJA	Principal / IPVPN	INR0104	100.00%
	Backup / IPVPN	INR0106	100.00%
VILLAVICENCIO	Principal / IPVPN	INR0085	99.82%
	Backup / IPVPN	INR0084	100.00%
ARMENIA	Principal / IPVPN	INR0074	100.00%
	Backup / IPVPN	INR0072	99.97%
MANIZALES	Principal / IPVPN	INR0088	100.00%
	Backup / IPVPN	INR0087	100.00%
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	100.00%
CUCUTA	Principal / IPVPN	INR0044	99.84%
	Backup / IPVPN	INR0047	99.76%
VALLEDUPAR	Principal / IPVPN	INR0091	99.71%
	Backup / IPVPN	INR0090	98.30%
YOPAL	Principal / IPVPN	INR0121	99.46%
	Backup / IPVPN	INR0123	99.95%
ARAUCA	Principal / IPVPN	INR0110	100.00%
CALI	Principal / IPVPN	INR0151	100.00%
	Backup / IPVPN	INR0153	100.00%
BUENAVENTURA	Principal / IPVPN	INR0051	99.86%

MOCO A	Principal / IPVPN	INR0135	95.73%
	Backup / Satelital	INR0136	99.82%
PASTO	Principal / IPVPN	INR0130	100.00%
	Backup / IPVPN	INR0131	100.00%
POPAYAN	Principal / IPVPN	INR0035	100.00%
	Backup / IPVPN	INR0032	100.00%
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	INR0034	100,00%
Canal entre Sitio contingencia Ictetex - Dirección General - Aguas	Conectividad brindada a través de la red MPLS, con acceso a los dos Datacenter	INR0230	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	INR0221	99,92%
Internet Dedicado Navegación centralizada Megacenter	Internet Backup	INR0268	100.00%
Banco de la Republica hasta Edificio Dirección General ICETEX	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0000289	99.84%
DECEVAL hasta Edificio de ICETEX Dirección General.	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0000317	99.46%
DECEVAL hasta Edificio de ICETEX Dirección General.	Ubicado en Datacenter Principal, interconectado a través de red MPLS (Backup)	INR0000318	99,92%
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	INR0264	100.00%
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	INR0177	99,97%

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 marzo continúan pendientes 13 ampliaciones de ancho de banda, es decir un 72.34% de las ampliaciones se han culminado, en las tablas a continuación se presenta los servicios de conectividad contratados con sus respectivas capacidades ofrecidas y se compara con las cargas prestadas:

CIUDAD	Enlace - Tipo medio	Código Servicio	BW- Mínimo Requerido (MBPS)	Ancho de Banda Ofrecido	Ancho de Banda Prestado	Diferencia (MBPS)
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 3 Canales pendientes por ampliar

4.1 INTERNET PARA LA GENTE

Durante el mes de marzo 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 4 Disponibilidad canales "Internet para la gente"

Quedan pendientes 2 instalaciones que son: San Andrés la cual se encuentra en factibilidad por parte del operador y Leticia donde no se ha podido instalar por falta de sede.

4.2 CANALES SDWAN

Durante el mes de marzo se culmina la conectividad de los canales SD WAN entre Aguas 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 5 Disponibilidad canales "SDWAN"

Está contemplada la instalación de canales SDWAN en las sedes de Leticia y San Andres, San Andrés se encuentra por el momento en factibilidad por parte del operador y Leticia sólo se podrá iniciar la gestión una vez ICETEX confirme que se cuenta con Sede y se tenga la dirección.

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 marzo, funcionó sin ningún contratiempo.

La evidencia se encuentra en el informe [Replicacion Marzo 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)	15-mar-24
Bogotá (Chapi)	13-mar-24
Medellín	06-mar-24
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*	15-mar-24

Tabla 6 Estado de la instalación de la señalética de Wifi

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

Quedarían Faltando la señalética de Cali que sufrió un pequeño daño durante el transporte y la oficina no la recibió por lo cual se debió devolver para nuevamente volverse a fabricar y San Andres que se entregará una vez se entregue el canal.

4.5 CONCLUSIONES DEL SERVICIO DE CONECTIVIDAD

En la operación del mes de marzo:

- Se lograron atender todos los casos y se cerraron en los tiempos establecidos, identificando con respecto al mes anterior un incremento del 30% de los casos escalados según el análisis se evidencia que obedece a que todos los funcionarios ya se encuentran laborando en la entidad.
- Los casos generados durante el mes fueron cerrados con notificación a los funcionarios del servicio operativo, en cuanto a los casos abiertos con claro presenta un aumento del 20% con respecto al mes anterior dado el inconveniente en la herramienta solar Winds.
- Se tiene un avance del 97% de los canales instalados teniendo pendiente Quibdó Backup
- Se tiene un avance del 90% de la instalación de las señaléticas.
- Se ha realizado un trabajo contante con reuniones diarias de seguimiento para terminar lograr avanzar con el proyecto de Ipv6 con el proveedor durante este mes.
- Se encuentran pendiente la instalación del canal de Backup de Quibdó y de las 4 sedes donde no había oficina, la Oficina de San Andres se encuentra iniciando fase de factibilidad de los canales principal, Backup, Internet para la gente y SDWAN.
- Se está realizando una actualización de la arquitectura de las redes que conforman las sedes y la manera como se están recibiendo los servicios del ISP.
- Se determina la ubicación precisa de todos los componentes que conforman la infraestructura de cada sede, así como su conexión lógica con el proveedor de servicios para acceder a Internet.

4.6 RECOMENDACIONES DEL SERVICIO DE CONECTIVIDAD

- Se recomienda que los canales con SDWAN se puedan tomar como una canal redundante por si llegara a fallar los canales principales y Backup.

- 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 marzo. [Conciliación marzo consolidado.xlsx](#)

5 SERVICIOS CENTROS DE COMPUTO

5.1 Datacenter Principal

Para el mes de marzo 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 las herramientas Sitescope y ELK dispuestas en el Datacenter. Ver los informes.

[INFORME POR DEMANDA DISPONIBILIDAD Y CAPACIDAD ICETEX Marzo 2024.pdf](#)
[Reporte Monitoreo ICETEX Marzo 2024-ELK.pdf](#)

PROMEDIO CONSUMO DE CPU

View: month

From: 3/1/2024 12:00 AM

To: 4/1/2024 12:00 AM

America/Bogota

Sample type: ss_hr_t

Nombre de destino	Nombre del monitor	Valor mínimo	Valor máximo	Valor promedio
iceteboglxdarumatest	CPU	1.00	28.00	1.70
icetexbogliferaynfs	CPU	0.00	42.00	2.40
icetexboglxdarumasrv1	CPU	0.00	100.00	5.61
icetexboglxdarumasrv2	CPU	1.00	39.00	1.95
icetexboglxxroad1	CPU	1.00	33.00	3.28
icetexboglxxroad2n	CPU	0.00	7.00	1.46
icetexboglxxroad3	CPU	0.00	6.00	0.80
icetexboglxxroadtest	CPU	1.00	27.00	1.53
ictxprusisgapp	CPU	0.00	83.00	21.53
ictxisgesapp	CPU	0.00	77.00	13.76
ictxisgesbd	CPU	0.00	66.00	15.95
inr0233_icetexboglxxorfeo1.localdomain	CPU	0.00	13.00	0.69
inr0237_icetexboglserver1-r	CPU	0.00	20.00	4.21
inr0239_icetexbogelasticserver1	CPU	0.00	81.00	2.50
inr0241_icetexbogelasticserver3	CPU	0.00	3.00	0.52
inr0242_icetexbogliferayserver2	CPU	0.00	100.00	11.31
inr0243_icetexbogliferayserver1	CPU	1.00	71.00	9.68
inr0262_icetexboglxxorfeo2.localdomain	CPU	0.00	76.00	1.97
inr0276_cxvodaprodn011	CPU	2.00	100.00	54.27
inr0277_cxvodaprodn021	CPU	9.00	100.00	32.25
inr0278_cxvodacontg011	CPU	3.00	71.00	8.91

Ilustración 1 Evidencia del Resumen del Monitoreo

REPORTE USO DISCOS					
Last 30 days rounded to the day					
HOSTNAME	CODIGO DE S	FILESYSTEM	MAX DISK US	MIN DISK US	AVG DISK US
bastion.locald	INR0253	/mnt	100.00%	100.00%	100.00%
bastion.locald	INR0253	/	88.90%	88.80%	88.90%
bastion.locald	INR0253	/boot	14.00%	14.00%	14.00%
bastion.locald	INR0253	/home	13.10%	13.10%	13.10%
cxvodaprodn0	INR0276	/DAT OS	100.00%	11.80%	61.65%
cxvodaprodn0	INR0276	/grid	94.40%	80.60%	87.45%
cxvodaprodn0	INR0276	/oracle	92.00%	72.10%	80.45%
cxvodaprodn0	INR0276	/opt	81.80%	75.10%	76.10%
cxvodaprodn0	INR0276	/home	46.30%	45.50%	45.89%
cxvodaprodn0	INR0276	/var/crash	29.40%	29.40%	29.40%
cxvodaprodn0	INR0276	/var	20.40%	20.30%	20.30%
cxvodaprodn0	INR0276	/boot	18.00%	18.00%	18.00%
cxvodaprodn0	INR0276	/usr	17.60%	17.60%	17.60%
cxvodaprodn0	INR0276	/tmp	6.40%	0.60%	2.41%
cxvodaprodn0	INR0277	/DAT OS	100.00%	11.80%	61.61%
cxvodaprodn0	INR0277	/oracle	99.00%	73.40%	80.46%
cxvodaprodn0	INR0277	/grid	95.60%	80.30%	87.15%
cxvodaprodn0	INR0277	/opt	84.20%	80.70%	81.18%
cxvodaprodn0	INR0277	/home	52.40%	52.30%	52.34%
cxvodaprodn0	INR0277	/var/crash	22.80%	22.80%	22.80%
cxvodaprodn0	INR0277	/var	20.20%	20.20%	20.20%
cxvodaprodn0	INR0277	/boot	18.00%	18.00%	18.00%

Ilustración 2 Evidencia del Resumen del Monitoreo ELK

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: 3/1/2024 12:00 AM	To: 4/1/2024 12:00 AM	America/Bogota
Sample type: ss_hr_t		
Nombre de destino	Nombre del monitor	Disponibilidad
iceteboglxdarumatest	Ping	100.00
icetexbogliferaynfs	Ping	99.99
icetexboglxdarumasrv1	Ping	99.93
icetexboglxdarumasrv2	Ping	99.96
icetexboglxxroad1	Ping	100.00
icetexboglxxroad2n	Ping	100.00
icetexboglxxroad3	Ping	100.00
icetexboglxxroadtest	Ping	99.93
ictxprusigapp	Ping	99.95
ictxisgesapp	Ping	99.53
ictxisgesbd	Ping	100.00
inr0233_icetexboglxxorfeo1.localdomain	Ping	100.00
inr0237_icetexbogbalserver1-r	Ping	100.00
inr0239_icetexbogelasticserver1	Ping	100.00
inr0241_icetexbogelasticserver3	Ping	100.00
inr0242_icetexbogliferayserver2	Ping	99.99
inr0243_icetexbogliferayserver1	Ping	100.00
inr0262_icetexboglxxorfeo2.localdomain	Ping	99.99
inr0276_cxvodaprodn011	Ping	99.92
inr0277_cxvodaprodn021	Ping	100.00
inr0278_cxvodacontg011	Ping	99.84

Ilustración 3 Promedio Disponibilidad Servicios en Housing – Datacenter Principal

Reporte Disponibilidad Servidores	
Last 30 days rounded to the day	
HOSTNAME	DISPONIBILIDAD
cxvodaprodn011	100.00%
cxvodaprodn021	100.00%
icetexboglserver1-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.jo.caldomain	100.00%
icetexboglxorfeo2.jo.caldomain	100.00%
icetexboglxroad3	100.00%
icetexstog nfs1	100.00%
icetexstog nfs2	100.00%
icetexogsvpt1	100.00%
icetexogsvpt2	100.00%
icetextroldoc	99.89%
icetxprusigapp	100.00%
icetxsisgesapp	100.00%
icetxsisgesbd	100.00%
nfsa	100.00%
preprodsec	100.00%
qasec	100.00%
xroadsec	100.00%

Ilustración 4 Reporte ELK Promedio Disponibilidad Servicios en Housing – Datacenter Principal

Cod Servicio	Hostname	Disponibilidad
INR0246	icetexbogldarumatest	100%
INR0238	icetexbogliferaynfs	99.99%
INR0244	icetexbogldarumasrv1	99.93%
INR0245	icetexbogldarumasrv2	99.96%
INR0249	icetexboglxroad1	100%
INR0247	icetexboglxroad2n	100%
INR0248	icetexboglxroad3	100%
INR0250	icetexboglxroadtest	99.93%
INR0234	icetxprusigapp	99.95%
INR0229	icetxsisgesapp	99.53%
INR0228	icetxsisgesbd	100%
INR0233	icetexboglxorfeo1	100%
INR0237	icetexboglserver1	100%
INR0239	icetexbogelasticserver1	100%
INR0241	icetexbogelasticserver3	100%
INR0242	icetexbogliferayserver2_R	99.99%
INR0243	icetexbogliferayserver1_R	100%
INR0262	icetexboglxorfeo2	99.99%
INR0276	cxvodaprodn011	99.92%
INR0277	cxvodaprodn021	100%

INR0278	cxvodacontn011	98.84%
INR0240	icetexbogelasticserver2	100%
INR0260	icetexbogobognfs1	100%
INR0252	icetexbogobognfs2	100%
INR0236	ictxbogsvrpt1	100%
INR0235	ictxbogsvrpt2	100%
INR0000322	ictxcontroldoc	99.89%
INR0226	mira	100%

Tabla 7 Códigos relacionados Disponibilidad Servicios en Housing – 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 Slot B2 -Tarjeta Enclosure - M1000	Dell	M1000E	99,80%	100%

Tabla 8 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 97.5% Nodo2 del sitio durante el mes de Marzo [ReportDynatracePortal_Marzo2024.pdf](#)

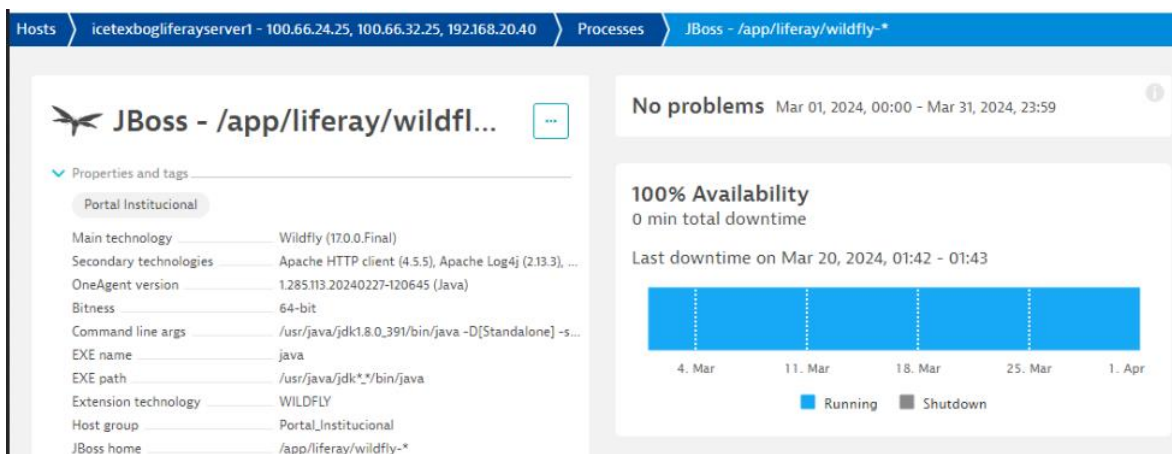


Ilustración 5 Disponibilidad Nodo1 Servicios Portal Web Icetex (Dynatrace)

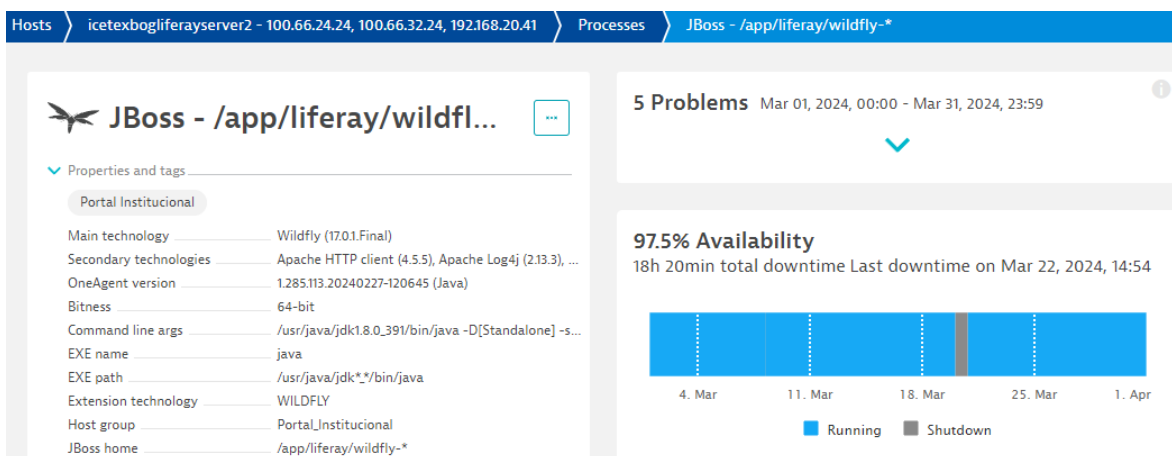


Ilustración 6 Disponibilidad Nodo 2 Servicios Portal Web Icetex (Dynatrace)

5.1.3 Backup Servidores Triara

Durante el periodo de marzo se realizaron los backups de acuerdo con las políticas definidas por el Icetex las cuales desde su inicio se implementaron en el Datacenter. Se puede verificar en el documento, [Reporte backups mes de marzo 2024.pdf](#) el cual se genera automáticamente desde la herramienta que se utiliza para realizar las copias.

Backup job summary

Backup job summary report

Generated on: Apr 01, 2024 08:39 AM

Server groups : INFOTIC
Servers : All
App types : All
Subclients : All
Job status : Running, Completed, Delayed, Failed, Killed, Completed with Errors, Completed with Warnings, Committed
Job Types : All
Time Frame : Last 4 weeks (Mar 4, 2024, 08:39:11 AM - Apr 1, 2024, 08:39:11 AM)
Time zone : GMT+05:30
Day Start Time : 12:00 AM
Snap and Backup Copy options : Snap and Backup Copy options
Advanced : None

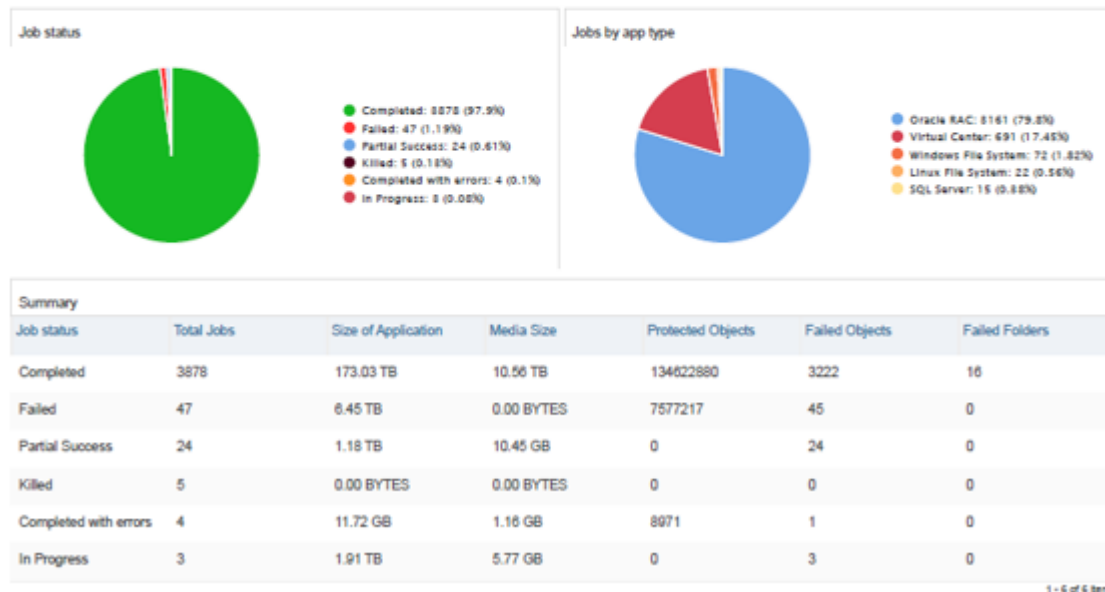


Ilustración 7 Evidencia Backup Servidores

5.2 Datacenter Alterno

5.2.1 Hosting Virtual (IaaS)

En el transcurso del mes de marzo 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 [Replicacion Marzo 2024.pdf](#), el cual corresponde al último reporte diario del mes y refleja el consolidado de los informes que se están periódicamente desde el mes anterior.

Site Recovery Manager - Estado Replicas INFOTIC

Actualmente el SRM (vcsatriars-ext.datacenterdhs.local -> vcmegacenter.datacenterdhs.local)
cuenta con 14 replicas

General				
Name			Count	
OK			13	
Not Active			1	
Grupo de protección: PG_INFOTIC_7 (2)				
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	RPO
INR0226_INFOTIC_REP	OK	5 of 5	Apr 1, 2024	5 minutes
INR0228_INFOTIC_REP	OK	1 of 1	Apr 1, 2024	1 hour
Grupo de protección: PG_INFOTIC_6 (1)				
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	RPO
INR0229_INFOTIC_REP	OK	1 of 1	Apr 1, 2024	1 hour
Grupo de protección: PG_INFOTIC_1 (2)				
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	RPO
INR0233_INFOTIC_REP	OK	6 of 6	Apr 1, 2024	30 minutes
INR0262_INFOTIC_REP	OK	1 of 1	Apr 1, 2024	1 hour
Grupo de protección: PG_INFOTIC_5 (1)				
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	RPO
INR0236_INFOTIC_REP	OK	2 of 2	Apr 1, 2024	2 hours
Grupo de protección: PG_INFOTIC_4 (4)				
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	RPO
INR0237_INFOTIC_REP	OK	2 of 2	Apr 1, 2024	5 minutes
INR0238_INFOTIC_REP	OK	2 of 2	Apr 1, 2024	1 hour
INR0239_INFOTIC_REP	OK	2 of 2	Apr 1, 2024	1 hour
INR0243_INFOTIC_REP	OK	2 of 2	Apr 1, 2024	5 minutes
Grupo de protección: PG_INFOTIC_PRUEBA (1)				
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	RPO
INR0243_INFOTIC_REP_CLON	Not Active	2 of 2	Mar 26, 2024	1 hour
Grupo de protección: PG_INFOTIC_3 (2)				
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	RPO
INR0244_INFOTIC_REP	OK	1 of 1	Apr 1, 2024	1 hour
INR0245_INFOTIC_REP	OK	1 of 1	Apr 1, 2024	5 minutes
Grupo de protección: PG_INFOTIC_2 (1)				
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	RPO
INR0249_INFOTIC_REP	OK	2 of 2	Apr 1, 2024	5 minutes

Ilustración 8 Reportes de replicación SRM a Sitio Alterno, marzo 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
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

INR Replicación	Host name	Servicio	VirtualMachine MEGACENTER
INR0213	icetexboglxdarumasrv2	DARUMA	INR0245_INFOTIC_REP
INR0214	icetexboglxroad1	XROAD	INR0249_INFOTIC_REP

Tabla 9 Servicios replicados – Datacenter MEGACENTER

5.2.2 Dataguard BBDD Megacenter

Durante el mes de marzo de 2024 se continuo con la replicación permanente de las BD Oracle al Datacenter alterno de acuerdo con las políticas establecidas, utilizando el Oracle Active Data Guard el cual garantiza una alta disponibilidad, protección de datos y recuperación ante desastres. Ver las evidencias en el documento [INFOTIC ICETEX - Evidencias Dataguard Megacenter Marzo.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:~  
#-----  
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
[oracle@cxvodacontg011 ~]$ ps -fe|grep pmon
grid      10449      1  0 Feb24 ?        00:04:58 asm_pmon_+ASM
oracle    10792      1  0 Feb25 ?        00:12:04 ora_pmon_ICTXCYCD
oracle    11336      1  0 Feb25 ?        00:11:47 ora_pmon_APOTEOSD
oracle    11715      1  0 Feb25 ?        00:06:33 ora_pmon_VIGIADTG
oracle    12044      1  0 Feb25 ?        00:06:21 ora_pmon_LIFERAYD
oracle    12307      1  0 Feb25 ?        00:06:31 ora_pmon_LANDICTD
oracle    12566      1  0 Feb25 ?        00:11:08 ora_pmon_APLICATD
oracle    12732      1  0 Feb25 ?        00:11:26 ora_pmon_APOTNEWD
oracle    12918      1  0 Feb25 ?        00:11:41 ora_pmon_ICETEXD
oracle    25240 25014  0 21:20 pts/0    00:00:00 grep --color=auto pmon
[oracle@cxvodacontg011 ~]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.4.0 Production on Tue Apr 2 21:20:34 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              48594              48594 31/03/2024 20:32 31/03/2024 20:32
        2              38834              38834 31/03/2024 20:55 31/03/2024 20:55

SQL> sta uapply

  Thread Last Sequence Received Last Sequence Applied Difference
  -----
        1              48594              48594             0
        2              38834              38834             0

SQL>
SQL>

```

Ilustración 9 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 31/03/2024 20:32 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).

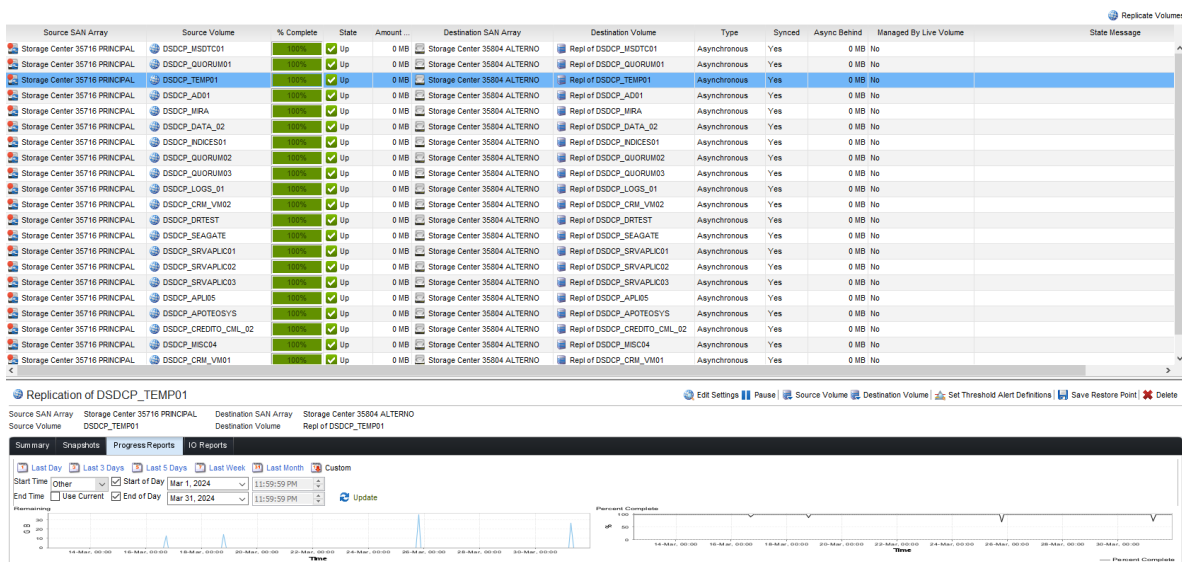


Ilustración 10 Evidencia replicado servicios On-premise Icetex a Megacentre

5.2.4 Disponibilidad de Servicios de Housing – Datacenter Alterno

A continuación, se presentan las máquinas alojadas en el Datacenter alterno en Medellín, las cuales estuvieron disponibles todo el mes de marzo 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 10 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 marzo, en materia de seguridad.

6.1 Servicios de Endpoint

Conforme a la activación del módulo de “Filtrado Web” del antivirus Sophos en los equipos de pruebas y según los resultados de las respectivas pruebas las cuales fueron satisfactorias deshabilitando el módulo QUIC en los respectivos navegadores. Se ha validado con ICETEX los resultados y solicitan realizar una comparación del filtrado web de la plataforma de Sophos con el del Firewall FortiGate. Esto con el fin de ajustar este filtrado web de Sophos a las necesidades de cada área para implementar según las necesidades de estas.

Actualmente continúa habilitado y funcionando correctamente 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 permanece en un 90%, dado que no se puede avanzar más porque este 10% son equipos que se encuentran en bodega.

6.2 ESTADÍSTICAS PORTALES

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

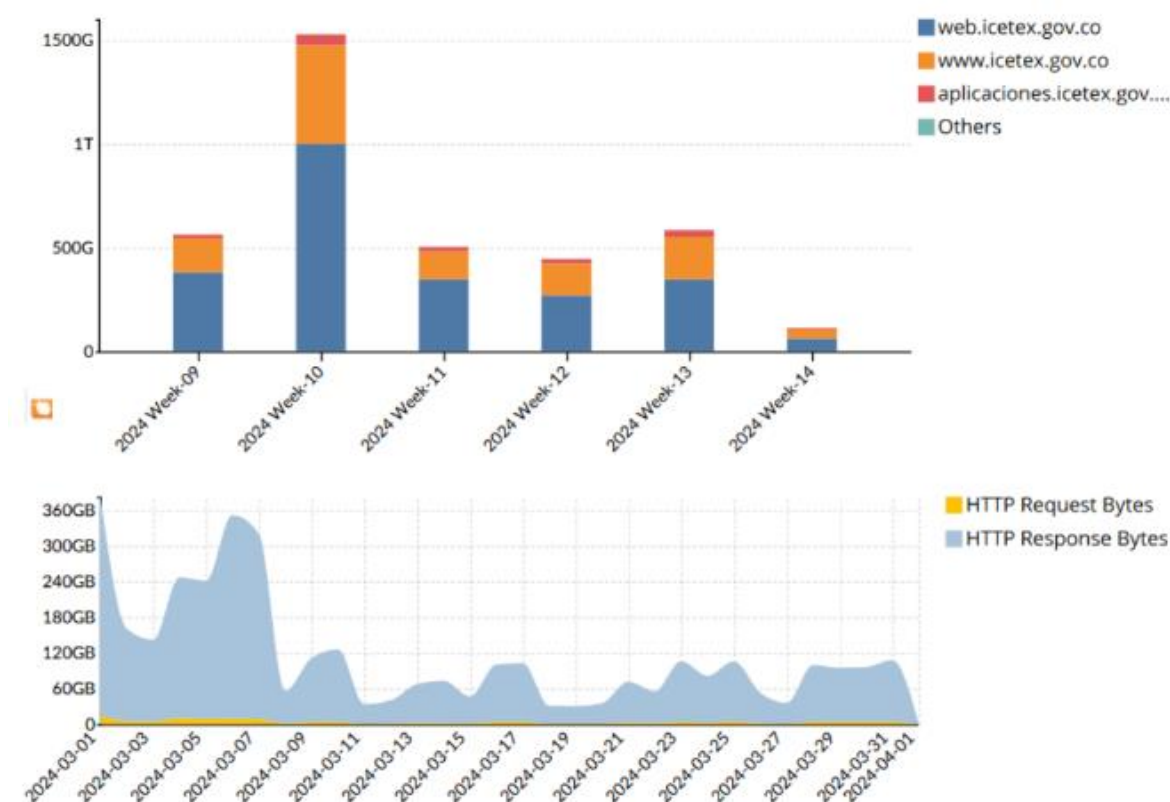


Ilustración 11 Evidencia Gráfica Estadísticas de Portales

En el periodo de tiempo analizado se presenta un promedio de 500 Gb de tráfico general hacia los portales FortiWeb Apps Nuevas, donde el portal de web.icetex.gov.co es el más consultado, 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 marzo seguridad 2024.pdf](#) se puede encontrar el Informe de Gestión Mensual que contiene información relevante de seguridad para el mes de marzo en lo concerniente a la Administración Plataformas incluidas las que son de propiedad del ICETEX y las IaaS

FORTIGATE TRIARA

Imagen 1 Seguridad-Perimetral-DC_Principal (FortiGate-Triara)

System Information

Hostname	DC_FG_MST_ICETEX
Serial Number	FG180FTK22901087 
Firmware	v7.2.7 build1577 (Mature)
Mode	NAT
System Time	2024/04/01 11:37:40
Uptime	24:14:49:48
WAN IP	 186.84.155.234

Ilustración 12 Evidencia Estado General de las Plataformas

6.4 Estado de Salud de los Equipos de Seguridad

En el transcurso del mes de marzo 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 marzo seguridad 2024.pdf](#)

ESTADO DE SALUD DE LOS EQUIPOS-TRAFICO Y SESIONES

FIREWALL AGUAS

Se observa el tráfico hacia la MPLS de la sede de Aguas con un promedio de 38.58 Mbps (Port7) en la última semana.

Imagen 14 Consumo Del Canal

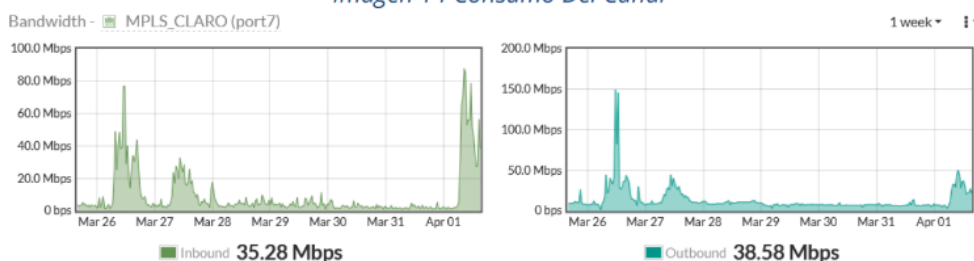


Ilustración 13 Evidencia Estado de Salud de los Equipos de Seguridad

6.5 Servicio de centro de Operaciones de Seguridad (SOC)

Durante el mes de marzo en el ICETEX, 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 Marzo 2024.pdf](#)

TLP:ROJO		INFORME MENSUAL MONITOREO SOC	Página	6 de 67
----------	---	-------------------------------	--------	---------

- 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 **2.411** 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 **167** 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: Cantidad de reglas de Rendimiento

Ilustración 14 Evidencia Imagen Reporte Monitoreo

6.5.1 Monitoreo de Marca-Estrategia OSINT-SOC

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

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

TLP:ROJO

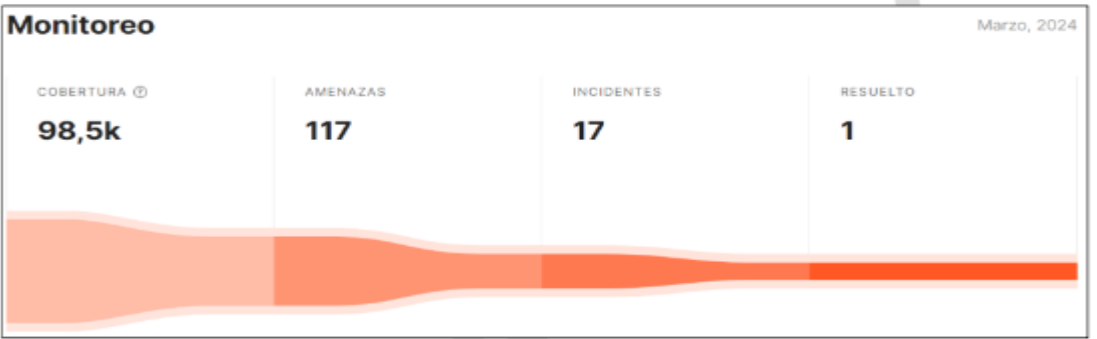
INFORME MENSUAL MONITOREO OSINT

Página

3 de 12

4. ANÁLISIS DE MONITOREO DE OSINT

Durante el periodo evaluado, la plataforma de monitoreo de OSINT – AXUR, reporta un total de **117** posibles amenazas de las 98,5k que fueron encontradas y analizadas automáticamente por la plataforma de monitoreo. A estas **117** 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 **01** caso en la plataforma de monitoreo.



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



Ilustración 15 Evidencia Imagen Reporte Monitoreo OSINT

Durante el periodo evaluado se detectaron 17 incidentes, 15 relacionados con exposición de infraestructura, relacionado con actividad sospechosa en sitio web y uno relacionado con aplicación móvil falsa.

6.6 Eventos Relevantes

En marzo se actualizaron los equipos de seguridad perimetral.

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

Tabla 11 Recomendaciones plataformas de seguridad

Recomendación	Estado	Criticidad
Garantizar la segmentación de la red que permita claramente definir qué servicios deben ser alcanzados por cada usuario.	Se toma a tesorería como área inicial se comparte plan de trabajo involucrando a seguridad, Redes y el equipo de Windows	Media
Se recomienda una tecnología que permita realizar análisis de tráfico de la red (NTA-Network Traffic Analysis).	En evaluación por parte de ICETEX.	Alta
Se recomienda una tecnología que permita la gestión o validación de privilegios de accesos (IAM). Evitar compartir usuarios en la red, (Servidor Orfeo con usuario root). Evitar configurar usuarios y claves dentro de las aplicaciones de ICETEX	En evaluación por parte de ICETEX.	Alta
Establecer un proceso de hardening en los equipos y servidores.	Se propone establecer la política.	Media
Estructuración de análisis y respuesta de incidentes.	Se propone al ICETEX realizar un proceso o política de seguridad de gestión de incidentes, tomando como posible base la ISO 27001	Critica
Estructurar y resguardar los procesos críticos de	Se propone al ICETEX elaborar el	Media

la compañía a nivel de seguridad (ejm: tesorería).	Procedimiento.	
Estructurar la seguridad de perímetro y de endpoint en la nube "Escritorios remotos".	Se evalúa por parte de ICETEX que infraestructura utilizar.	Alta
Validar a nivel de punto final los equipos que se han visto involucrados con comportamiento malicioso.	Se evalúa por parte de ICETEX la elaboración de la política de gestión de incidentes se debe identificar los actores responsables.	Critica
Capturar las IPs a nivel de aplicación, logs de eventos al momento de hacer transacciones por ejemplo en los casos en que se hacen renovaciones.	Se debe validar de parte de desarrollo si esto es posible.	Baja
Cerrar a nivel de aplicación los accesos por geolocalización, por ejemplo, en los casos en que se hacen renovaciones.	Se debe validar de parte de desarrollo si esto es posible.	Baja
Integrar los servidores de Directorio Activo con el SIEM.	Se debe evaluar la capacidad del SIEM, se espera plan de mejora.	Media
Integrar los equipos que hacen parte del proceso de pagos con el SIEM.	Se debe evaluar la capacidad del SIEM, se espera plan de mejora.	Media
Se recomienda la integración de doble factor de autenticación para la plataforma Password Manager Pro.	Se ejecuta por parte del administrador para algunos usuarios como método de prueba.	Alta
Se recomienda que la gestión de procesos o acceso a equipos de misión monetaria se haga a través de VPN y con doble factor de autenticación.	Se evalúa por parte de ICETEX.	Media
Definir línea base para los equipos de punto final tanto pertenecientes al ICETEX como los que no.	Se está elaborando por parte de ICETEX la línea base y se evalúa la creación del procedimiento.	Media

Tabla 12 Recomendaciones de seguridad para Icetex

6.8 CONCLUSIONES

- La segmentación de la red permite tener un mejor control y administración 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 marzo, 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 MENSUAL MARZO.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 MENSUAL MARZO.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 todo el mes de marzo del 2024 sobre la solución de videoconferencia en las sedes regionales, se encuentra una disponibilidad del 100%, la solución completa en estado activo, para el periodo del presente informe, además es importante resaltar que se cuenta con todos los requerimientos realizados en las especificaciones técnicas del contrato.

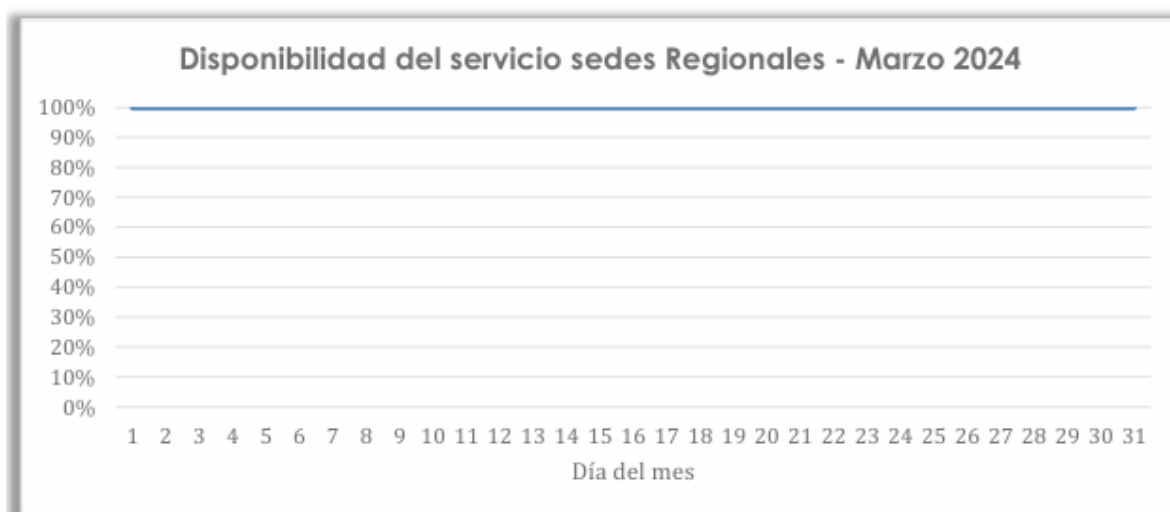


Ilustración 16 Disponibilidad de servicio videoconferencia sedes regionales – marzo 2024

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

En la verificación realizada para el mes de marzo de 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.

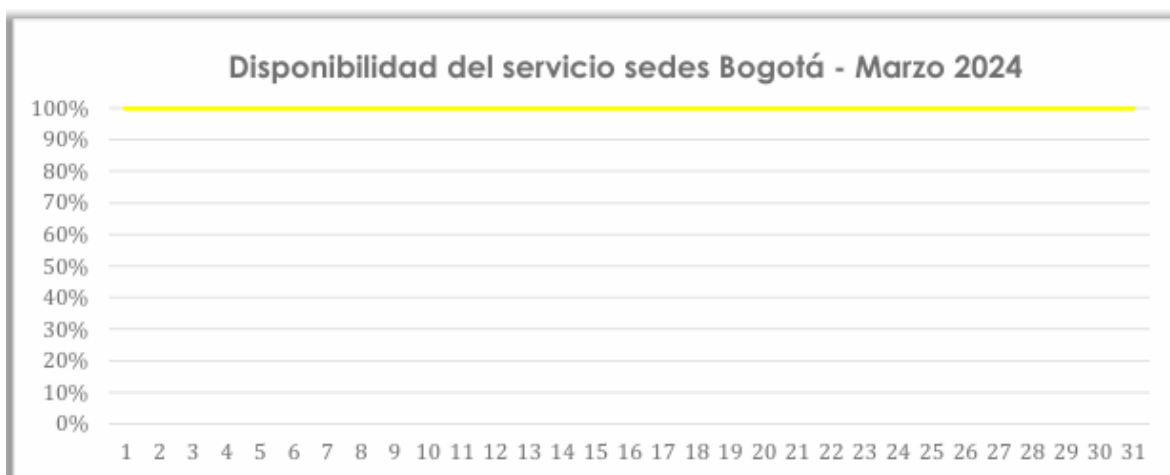


Ilustración 17 Disponibilidad de servicio videoconferencia sedes Bogotá – marzo 2024

8.2 Gestión de incidencias y requerimientos – sedes regionales

Para el mes de marzo, entre el 1 y el 31 del mes, no se generaron requerimientos especiales que requirieran atención y gestión de soporte técnico en las sedes Regionales; tampoco se reportaron incidencias a nivel del servicio para estas sedes durante el mes, sin embargo, se tuvo total disponibilidad para recibir cualquier requerimiento de soporte o solicitud de apoyo concerniente a la solución de videoconferencia desplegada.

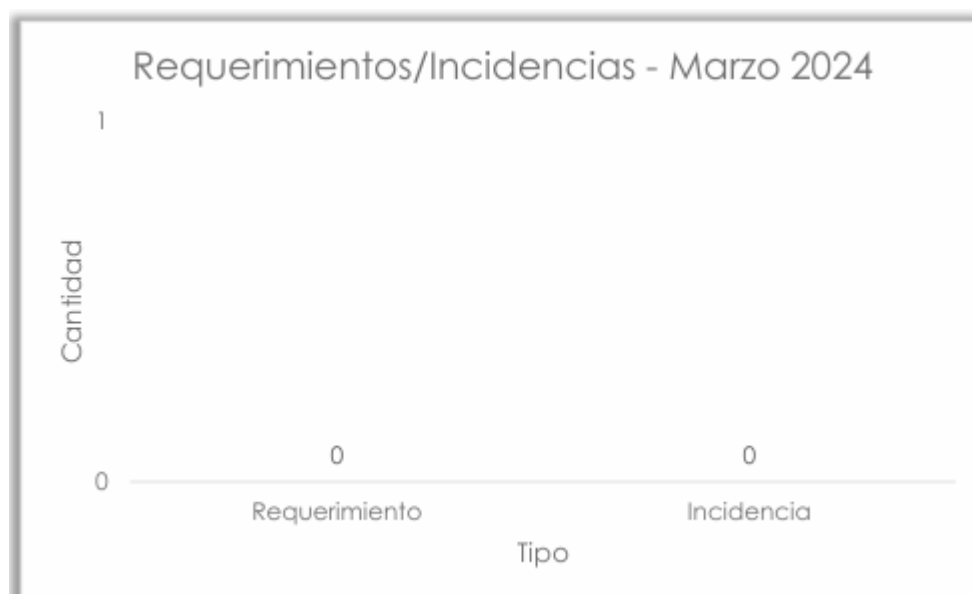


Ilustración 18 Incidencias/Requerimientos sedes Regionales – marzo 2024

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

Para el periodo comprendido entre el 1 y el 31 de marzo, no se recibieron requerimientos especiales que requirieran gestión y atención del soporte técnico para las sedes de Bogotá Aguas y Ángel; tampoco fueron reportadas incidencias a nivel del servicio para estas sedes durante el mes del presente informe, no obstante, se tuvo total disponibilidad para recibir cualquier requerimiento de soporte o solicitud de apoyo concerniente a la solución de videoconferencia desplegada.

Con el fin de facilitar el procedimiento de ingreso para los técnicos que están apoyando la revisión de incidencias, requerimientos, visitas y/o novedades de soporte nivel II en sitio, para los módulos de videoconferencia instalados en las sedes de ICETEX, durante este periodo se realizó la gestión para permitir y agilizar el ingreso frecuente a las instalaciones de la entidad, en aras de responder a los requerimientos de una manera más ágil teniendo en cuenta la disponibilidad de cada técnico del área de TI. Se continúa al tanto para recibir cualquier solicitud de soporte, acompañamiento o apoyo concerniente a la solución de videoconferencia desplegada.

- Durante el mes de marzo 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.

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

9 CALCULO DE CONCILIACIÓN DE LOS SERVICIOS DEL MES DE MARZO

A la fecha la conciliación del mes de marzo con ICETEX se encuentra en proceso, el detalle de conciliación del mes anterior se puede ver en el siguiente link [Conciliación marzo 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) *					\$ 760.438.823,49
VALOR TOTAL EJECUTADO (valor pagado + valor causado no pagado)					\$ 7.753.715.067
SALDO DEL CONTRATO (valor total del contrato – valor total ejecutado)					\$ 23.645.281.791
PORCENTAJE DE EJECUCIÓN					24.69%
* 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