



INFORME DE ACTIVIDADES DEL CONTRATO

**CONTRATO NUMERO
2022-0792**

Mayo 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	8
4.2	Canales SDWAN	9
4.3	Canal de Replicación (Triara – Megacenter)	9
4.4	Señalética (Internet para la gente)	9
4.5	Implementación de IPv6	10
4.6	Normalización de la LAN de IPv4	10
4.7	Gestión de Vulnerabilidades en Networking	10
4.8	CONCLUSIONES DEL SERVICIO DE CONECTIVIDAD	10
4.9	RECOMENDACIONES 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 TRIARA para los servicios de página web	13
5.1.3	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 Icetex a Megacenter	18
5.2.4	Disponibilidad de Servicios de Housing – Datacenter Alterno	19
6	SEGURIDAD	19
6.1	Servicios de Endpoint	19
6.2	ESTADÍSTICAS PORTALES	20
6.3	Estado General de las Plataformas	20
6.4	Estado de Salud de los Equipos de Seguridad	21
6.5	Servicio de centro de Operaciones de Seguridad (SOC)	21
6.5.1	Monitoreo de Marca-Estrategia OSINT-SOC	22
6.6	Eventos Relevantes	23
6.7	RECOMENDACIONES	23
6.7.1	Recomendaciones Generales	24
6.7.2	Recomendaciones Específicas	24
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	27
7.2.3	Administrador de Soluciones	27
7.2.4	Especialista en Networking	27

7.2.5	Especialista Integrador de nube.....	27
7.2.6	Especialista en seguridad	28
8	SERVICIO DE COLABORACIÓN	28
8.1	Disponibilidad del servicio – sedes Bogotá (aguas - ángel)	29
8.2	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 MAYO	30

INDICE DE TABLAS

Tabla 1	Disponibilidad de canales	7
Tabla 2	Disponibilidad de canales Armenia.....	7
Tabla 3	Canales pendientes por instalar	7
Tabla 4	Canales pendientes por ampliar	8
Tabla 5	Disponibilidad canales “Internet para la gente”	8
Tabla 6	Disponibilidad canales “SDWAN”	9
Tabla 7	Estado de la instalación de la señalética de Wifi.....	9
Tabla 8	Códigos relacionados Disponibilidad Servicios en Housing – Datacenter Principal	13
Tabla 9	Disponibilidad de Servicios de Housing – Datacenter Principal	13
Tabla 10	Servicios replicados – Datacenter MEGACENTER.....	17
Tabla 11	Disponibilidad de Servicios de Housing – Datacenter Alterno	19
Tabla 12	Recomendaciones plataformas de seguridad	24
Tabla 13	Recomendaciones de seguridad para Icetex	25
Tabla 14	Distribución módulos de videoconferencia por sede.....	28
Tabla 15	Ejecución Presupuestal.....	31

INDICE DE ILUSTRACIONES

Ilustración 1	Evidencia del Resumen del Monitoreo CPU-Memoria ELK	11
Ilustración 2	Evidencia del Resumen del Monitoreo ELK	12
Ilustración 3	Reporte ELK Promedio Disponibilidad Servicios en Housing – Datacenter Principal... ..	12
Ilustración 4	Disponibilidad Nodo1 Servicios Portal Web Icetex (Dynatrace)	14
Ilustración 5	Disponibilidad Nodo 2 Servicios Portal Web Icetex (Dynatrace)	14
Ilustración 6	UPTIME: Portal WEB web.icetex.gov.co	14
Ilustración 7	Métrica de Visitantes Portal WEB web.icetex.gov.co	15
Ilustración 8	Evidencia Backup Servidores	16
Ilustración 9	Reportes de replicación SRM a Sitio Alterno, mayo 2024.....	17
Ilustración 10	Evidencia Dataguard replicado a Megacenter BD.....	18
Ilustración 11	Evidencia replicado servicios On-premise Icetex a Megacenter.....	19
Ilustración 12	Evidencia Gráfica Estadísticas de Portales	20
Ilustración 13	Evidencia Estado General de las Plataformas	21
Ilustración 14	Evidencia Estado de Salud de los Equipos de Seguridad.....	21
Ilustración 15	Evidencia Imagen Reporte Monitoreo	22
Ilustración 16	Evidencia Imagen Reporte Monitoreo OSINT	23
Ilustración 17	Disponibilidad de servicio videoconferencia sedes regionales – mayo 2024	29
Ilustración 18	Disponibilidad de servicio videoconferencia sedes Bogotá –mayo 2024	29
Ilustración 19	Incidencias/Requerimientos sedes Regionales – mayo 2024	30

1 INTRODUCCIÓN

Este informe contiene la información relacionada con las actividades ejecutadas por INFOTIC en el periodo comprendido entre el 01 al 31 de mayo 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 mayo 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 mayo 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, se avanzó con las ampliaciones pendientes, como parte de las mejoras planteadas por Infotíc se hace la normalización de todas las sedes Lan IPv4 a nivel nacional, fueron resueltas todas las vulnerabilidades de la sede Aguas.

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 presentó la novedad dentro de la operación el servidor controldoc debió ser reinstalado en otra máquina virtual quedando pendiente la actividad de activar el monitoreo de ELK en la nueva máquina virtual.

Servicio de Seguridad: Las herramientas de seguridad han operado sin incidentes durante el mes de mayo, no se detectaron vulnerabilidades en los dispositivos de seguridad perimetral debido a que los firmware se encuentran en las últimas versiones estables entregadas por el fabricante.

La implementación del filtro web de Sophos en los equipos de la Entidad proporciona una solución eficiente para controlar el acceso a Internet como primera capa de seguridad. Esta implementación, organizada por áreas, permite una administración centralizada de categorías y excepciones para sitios o categorías

específicos. Este enfoque no solo refuerza la seguridad, sino que también incrementa la eficiencia operativa al facilitar una gestión más efectiva de los recursos de red y una respuesta rápida a las necesidades de cada área. La optimización constante de la herramienta FortiSIEM en relación con las políticas de monitoreo de servicios de la Entidad ha sido importante para mejorar la gestión de la seguridad en la red de la Entidad. A través de la revisión y ajuste de estas políticas, se va corrigiendo y mejorando la detección de eventos relevantes, incrementa la capacidad de respuesta ante incidentes. Esto nos permite un monitoreo más preciso y centrado en los servicios críticos de la Entidad.

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 mayo por parte de Icetex se continua pendiente de la 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 mayo del 2024 y la correcta operación de los centros de cómputo tanto principal como alterno.
- Reportes que evidencia la disponibilidad de los servidores y demás equipos de Infraestructura en el centro de datos principal.
- Reporte que evidencia la replicación de las máquinas virtuales desde el centro de datos principal al centro de datos 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 mayo de 2024.

4 SERVICIOS DE CONECTIVIDAD

Durante el mes de mayo, los canales principales y Backup instalados operaron de manera normal. La herramienta Solar Winds permite la graficación de los canales.

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 Mayo 2024 - ALLOT INFOTIC.pdf](#)

Durante el mes de mayo 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 MAYO 2024.pdf](#)

Sede	Categoría	INR	% Mes
BOGOTA D.C.	Principal / FO (Sede Aguas)	INR0037	99.98%
	Backup / FO (Sede Aguas)	INR0036	99.98%
	Principal / IPVPN (Sede Chapinero)	INR0022	99.97%
	Backup / IPVPN (Sede chapinero)	INR0020	97.58%
	Principal / IPVPN (Angel)	INR0272	99.98%
	Backup / IPVPN (Angel)	INR0273	99.90%
IBAGUE	Principal / IPVPN	INR0073	99.88%
	Backup / IPVPN	INR0076	99.92%
LETICIA	Principal / Satelital		0.00%
NEIVA	Principal / IPVPN	INR0039	100.00%
	Backup / IPVPN	INR0041	99.98%
TUNJA	Principal / IPVPN	INR0104	99.98%
	Backup / IPVPN	INR0106	99.89%
VILLAVICENCIO	Principal / IPVPN	INR0085	99.93%
	Backup / IPVPN	INR0084	99.88%
ARMENIA	Principal / IPVPN	INR0074	72.82%
	Backup / IPVPN	INR0072	72.75%
MANIZALES	Principal / IPVPN	INR0088	99.89%
	Backup / IPVPN	INR0087	99.98%
MEDELLIN	Principal / IPVPN	INR0133	99.98%
	Backup / IPVPN	INR0132	99.98%
APARTADO	Principal / IPVPN	INR0144	99.99%
PEREIRA	Principal / IPVPN	INR0079	99.63%
	Backup / IPVPN	INR0077	100.00%
QUIBDO	Principal / IPVPN	INR0014	99.98%
	Backup / IPVPN		0.00%
BARRANQUILLA	Principal / IPVPN	INR0103	99.97%
	Backup / IPVPN	INR0100	99.96%
CARTAGENA	Principal / IPVPN	INR0109	99.96%
	Backup / IPVPN	INR0107	99.90%
MONTERIA	Principal / IPVPN	INR0080	100.00%
	Backup / IPVPN	INR0081	99.98%
RIOHACHA	Principal / IPVPN	INR0164	99.93%
	Backup / IPVPN	INR0162	98.85%
SANTA MARTA	Principal / IPVPN	INR0154	99.98%
	Backup / IPVPN	INR0152	100.00%
SINCELEJO	Principal / IPVPN	INR0095	99.41%
	Backup / IPVPN	INR0097	99.40%
SAN ANDRES	Principal / IPVPN		0.00%
BARRANCABERMEJA	Principal / IPVPN		0.00%
SAN GIL	Principal / IPVPN		0.00%
BUCARAMANGA	Principal / IPVPN	INR0062	99.99%
	Backup / IPVPN	INR0061	99.99%
CUCUTA	Principal / IPVPN	INR0044	99.98%
	Backup / IPVPN	INR0047	99.71%
VALLEDUPAR	Principal / IPVPN	INR0091	99.69%
	Backup / IPVPN	INR0090	92.66%
YOPAL	Principal / IPVPN	INR0121	99.96%
	Backup / IPVPN	INR0123	99.96%
ARAUCA	Principal / IPVPN	INR0110	99.80%
CALI	Principal / IPVPN	INR0151	99.93%
	Backup / IPVPN	INR0153	99.98%
BUENAVENTURA	Principal / IPVPN	INR0051	99.97%
MOCOA	Principal / IPVPN	INR0135	99.83%

	Backup / Satelital	INR0136	99.85%
PASTO	Principal / IPVPN	INR0130	99.12%
	Backup / IPVPN	INR0131	99.70%
POPAYAN	Principal / IPVPN	INR0035	99.98%
	Backup / IPVPN	INR0032	99.98%
TUMACO	Principal / IPVPN	INR0147	95.64%
WAN general (concentrador total red)	MPLS PP	INR0266	99.97%
WAN general (concentrador total red)	MPLS Backup	INR0171	100.00%
Conectividad dedicada a funciones de réplica para eventos de DRP.	DWDM	INR0224	100.00%
Canal entre Sitio principal e Icetex - 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	99.99%
Canal entre Sitio contingencia Icetex - Dirección General - Aguas	Conectividad brindada a través de la red MPLS, con acceso a los dos Datacenter	INR0230	99.98%
Salida a Internet para toda la WAN desde Bogotá EN CENTRO DE COMPUTO principal	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0264	100.00%
Internet Dedicado Navegación centralizada Megacenter	Internet Backup	INR0268	99.99%
Banco de la Republica hasta Edificio Dirección General ICETEX	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0000289	99.96%
DECEVAL hasta Edificio de ICETEX Dirección General.	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0000317	100.00%
DECEVAL hasta Edificio de ICETEX Dirección General.	Ubicado en Datacenter Principal, interconectado a través de red MPLS (Backup)	INR0000318	99.98%
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	INR0177	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	INR0221	99.99%

Tabla 1 Disponibilidad de canales

- Para los canales de Armenia se debe tener en cuenta la disponibilidad siguiente:

Sede	Categoría	INR	% Mes
ARMENIA	Principal / IPVPN	INR0074	99.99%
	Backup / IPVPN	INR0072	99.84%

Tabla 2 Disponibilidad de canales Armenia

Las disponibilidades presentadas en el mes están por debajo del 90%, sin embargo, esta disponibilidad no debe ser tenida en cuenta por que por razones de racionamiento en la sede de Armenia están apagando los equipos generando esta indisponibilidad por lo tanto solicitamos se tenga en cuenta la disponibilidad del mes anterior que es el comportamiento normal de estos canales, como soporte se encuentran el caso de Aranda #76024.

A continuación, se listan las sedes sin instalar o en proceso de instalación:

SERVICIO	OBSERVACIONES
Leticia ppal.	En Fase de viabilidad
Barrancabermeja ppal.	Sin sede
San Gil ppal.	Sin sede
San Andrés ppal.	En fase de instalación
Quibdó bk	En fase de instalación

Tabla 3 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 mayo se está trabajando en las ampliaciones de Cartagena Backup y Riohacha principal, queda pendiente las Saturaciones de los canales para poder dar el cierre y recibir a satisfacción las ampliaciones, 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
NEIVA	Principal / IPVPN	INR0039	18	20	18	2
MEDELLIN	Principal / IPVPN	INR0133	63	100	63	37
	Backup / IPVPN	INR0132	15	20	15	5
QUIBDO	Principal / IPVPN	INR0014	18	20	18	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

Tabla 4 Canales pendientes por ampliar

4.1 INTERNET PARA LA GENTE

Durante el mes de mayo 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	99.96%
BUCARAMANGA	INTERNET PARA LA GENTE	INR0057	99.96%
CALI	INTERNET PARA LA GENTE	INR0160	99.95%
AGUAS	INTERNET PARA LA GENTE	INR0029	99.99%
CHAPINERO	INTERNET PARA LA GENTE	INR0015	99.95%
MEDELLIN	INTERNET PARA LA GENTE	INR0022	99.98%
APARTADO	INTERNET PARA LA GENTE	INR0140	99.71%
ARAUCA	INTERNET PARA LA GENTE	INR0115	93.28%
LETICIA	INTERNET PARA LA GENTE		0.00%
QUIBDO	INTERNET PARA LA GENTE	INR0021	99.98%
RIOHACHA	INTERNET PARA LA GENTE	INR0159	98.97%
SAN ANDRES	INTERNET PARA LA GENTE		0.00%
YOPAL	INTERNET PARA LA GENTE	INR0127	99.96%
MOCOA	INTERNET PARA LA GENTE	INR0141	99.83%

Tabla 5 Disponibilidad canales "Internet para la gente"

El canal de San Andres queda instalado el mes de mayo, pero no se tiene todavía gestión de la sede ya que está pendiente por parte del operador la configuración de la Lan, estos temas se retrasaron porque el Switch que se encuentra en sede presenta falla en su Software, por lo tanto se procede a enviar un equipo de reemplazo para la sede y así poder hacer el cambio correspondiente de equipos para poder avanzar con la puesta en marcha con las correspondientes pruebas de saturación y el acta de entrega, las cuales serán subidas al SharePoint.

De igual forma el canal Backup de Quibdó sigue pendiente de instalación por parte del operador, la instalación de este canal se ha retrasado por gestiones administrativas en el sitio donde se debe instalar ya se solventaron lo correspondiente a Ictex y continúan las gestiones correspondientes al operador que son requeridas para obtener el permiso de instalación en las instalaciones del centro comercial donde está ubicada la oficina de Ictex.

4.2 Canales SDWAN

Durante el mes de mayo, la conectividad SDWAN entre Aguas y Mocoa, presenta la siguiente disponibilidad:

Sede	Categoría	INR	% Mes
SD WAN AGUAS	SD WAN	INR0033 / 000334	100.00%
SD WAN MOCOA	SD WAN	INR0139 / 000333	71.82%

Tabla 6 Disponibilidad canales "SDWAN"

La indisponibilidad del SDWAN de Mocoa aún este mes obedece al equipo que se reemplazó por un nuevo equipo por haberse quemado por temas concernientes a la entidad.

SDWAN en las sedes de Leticia y San Andrés, San Andrés se encuentra por el momento en proceso de implementación por parte del operador y Leticia se inicia la fase de viabilidad dado que ICETEX ya confirmó que se cuenta con Sede y remitió 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 mayo, funcionó sin ningún contratiempo.

La evidencia se encuentra en el [Informe mensual replicacion mayo 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 7 Estado de la instalación de la señalética de Wifi

La señalética de wifi para la gente, continúan pendientes por entregar las sedes de San Andres y Cali.

4.5 Implementación de IPv6

Durante el mes se tuvieron avances en las siguientes actividades:

- Se determinaron las direcciones IPv6 que llevarán las VLAN en todas las sedes.
- Se definió el mapa del direccionamiento de los servidores que están en la nube.
- Se está desarrollando la actividad para el cambio del sistema autónomo de ICETEX. Esto permitirá que ICETEX sea reconocido como su propio sistema autónomo en el ámbito internacional, en lugar de ser identificado como parte del sistema autónomo de Claro.

Las siguientes actividades que están pendientes de realizar:

- Finalizar el cambio del sistema autónomo de ICETEX.
- Documentar los avances y las lecciones aprendidas.

El direccionamiento IPv6 para las VLAN se puede encontrar en el repositorio como [PLAN DIRECCIONAMIENTO IPV6](#)

4.6 Normalización de la LAN de IPv4

Como parte de las mejoras planteadas por Infotec se hace la normalización de todas las sedes Lan a nivel nacional, el direccionamiento como quedo se puede revisar en el siguiente documento: [DIRECCIONAMIENTO LAN ACTUAL IPV4 - IPV6 2024.xlsx](#)

4.7 Gestión de Vulnerabilidades en Networking

A la fecha se han resuelto las vulnerabilidades sobre el servidor 192.168.151.199 el cual es el encargado de almacenar todos los backups de los equipos de redes tales como routers y switchings de la identidad, por parte de networking se queda pendiente de un nuevo escaneo de vulnerabilidades por parte de la entidad tanto para confirmar si todas las vulnerabilidades quedaron remediadas como para atender las que se reporten sobre los equipos administrados de networking.

4.8 CONCLUSIONES DEL SERVICIO DE CONECTIVIDAD

- La implementación de IPv6 en ICETEX está progresando según lo previsto en cronograma de actividades que se tiene para la implementación del Direccionamiento.
- Se han superado varios desafíos y se han logrado avances importantes.
- ICETEX está comprometido a completar la implementación de IPv6 para mejorar la seguridad, la redundancia y la eficiencia de su red.
- La información sobre el entorno de pruebas de DHCP estará disponible a medida que avance el proyecto.
- Se comunicarán los detalles sobre el cambio del sistema autónomo de ICETEX una vez que se finalice la actividad.
- En el escaneo de vulnerabilidades realizado el día 17/05/23 en la sede Aguas sobre los equipos de networking, se evidencia que todas las vulnerabilidades reportadas de la sede Aguas fueron remediadas satisfactoriamente.
- Todos los casos fueron atendidos por la herramienta Aranda, no se atendió ningún caso por ningún otro medio, con respecto al mes anterior se identificó un aumento del 25% lo cual obedece a la normal presencia de los funcionarios en la identidad.
- Los casos abiertos con el operador presentaron un aumento del 28% con respecto al mes anterior, porque se tuvo inconvenientes con canales y ajustes sobre la herramienta de solar Winds.
- Se continua con el 97% de avance en los canales instalados teniendo pendiente Quibdó Backup San

- Andres y Leticia.
- Se continua con el 90% de avance de la instalación de las señaléticas.

4.9 RECOMENDACIONES DEL SERVICIO DE CONECTIVIDAD

- De acuerdo con la normatividad vigente se recomienda realizar la renovación de equipos de red de la identidad los cuales en este momento se encuentran obsoletos y sin soporte del fabricante.
- Se recomienda hacer la renovación o cambio de cableado en los diferentes puntos de la identidad ya que el cableado es muy antiguo y en lo posible hacer una certificación de este.
- Teniendo en cuenta lo que se ha evidenciado del estado de la infraestructura de las sedes, se recomienda hacer el mantenimiento de la infraestructura, así como el cableado y su renovación de equipos de red.

Se adjunta en el repositorio un documento en Excel con el análisis del comportamiento de los canales para el mes de mayo [ANS canales Mayo 2024 v1.xlsx](#)

5 SERVICIOS CENTROS DE COMPUTO

5.1 Datacenter Principal

Para el mes de mayo 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 continua con el monitoreo de los servidores en la herramienta ELK el cual entra a reemplazar el monitoreo que se hace con Sitescope.

Sin embargo, se continuará por un tiempo con el monitoreo desde las dos herramientas, se adjunta el Reporte desde ELK:

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

REPORTE USO CPU					REPORTE USO MEMORIA				
Last 30 days rounded to the day					Last 30 days rounded to the day				
HOSTNAME	CODIGO DE SER	MAX CPU USAG	MIN CPU USAGE	AVG CPU USAGI	HOSTNAME	CODIGO DE SER	MAX MEMORY L	MIN MEMORY U:	AVG MEMORY U
bastion.localdom	INR0253	16.30%	0.20%	0.32%	bastion.localdom	INR0253	56.00%	26.90%	47.49%
cxvodacontg011	INR0278	70.80%	2.90%	5.32%	cxvodacontg011	INR0278	87.80%	81.30%	87.12%
cxvodaprodn011	INR0276	99.90%	11.37%	42.77%	cxvodaprodn011	INR0276	99.50%	83.70%	94.42%
cxvodaprodn021	INR0277	99.90%	11.48%	32.20%	cxvodaprodn021	INR0277	99.30%	74.30%	94.49%
icetexboglobserv	INR0237	26.10%	0.30%	13.43%	icetexboglobserv	INR0237	50.10%	9.30%	38.55%
icetexbogelastic	INR0239	79.10%	0.30%	1.54%	icetexbogelastic	INR0239	34.70%	31.80%	32.59%
icetexbogelastic	INR0240	0.60%	0.10%	0.21%	icetexbogelastic	INR0240	29.70%	28.70%	29.14%
icetexbogelastic	INR0241	17.10%	0.19%	0.37%	icetexbogelastic	INR0241	54.60%	14.10%	16.47%
icetexbogliferayr	INR0238	15.80%	0.20%	4.64%	icetexbogliferayr	INR0238	89.40%	26.00%	57.27%
icetexbogliferayr	INR0243	98.13%	0.50%	18.82%	icetexbogliferayr	INR0243	99.50%	3.80%	56.53%
icetexbogliferayr	INR0242	79.20%	0.40%	6.60%	icetexbogliferayr	INR0242	99.40%	3.10%	81.99%
icetexboglxdarur	INR0244	53.20%	1.10%	3.45%	icetexboglxdarur	INR0244	98.00%	82.60%	91.35%
icetexboglxdarur	INR0245	51.40%	1.00%	1.48%	icetexboglxdarur	INR0245	95.10%	51.80%	82.09%

Ilustración 1 Evidencia del Resumen del Monitoreo CPU-Memoria ELK

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%	88.87%
bastion.locald	INR0253	/var/lib/contain	88.90%	88.80%	88.80%
bastion.locald	INR0253	/boot	14.00%	14.00%	14.00%
bastion.locald	INR0253	/home	13.10%	13.10%	13.10%
cxvodacontg0	INR0278	/oracle	75.00%	74.80%	74.84%
cxvodacontg0	INR0278	/grid	68.40%	68.20%	68.28%
cxvodacontg0	INR0278	/opt	48.50%	45.30%	46.15%
cxvodacontg0	INR0278	/tmp	28.10%	28.10%	28.10%
cxvodacontg0	INR0278	/boot	26.20%	26.20%	26.20%
cxvodacontg0	INR0278	/var/crash	22.80%	22.80%	22.80%
cxvodacontg0	INR0278	/usr	22.10%	22.10%	22.10%
cxvodacontg0	INR0278	/var	21.30%	21.30%	21.30%

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:

REPORTE DISPONIBILIDAD SERVIDORES	
Last 30 days rounded to the day	
HOSTNAME	DISPONIBILIDAD
bastion.localdomain	100.00%
cxvodacontg011	100.00%
cxvodaprodn011	100.00%
cxvodaprodn021	100.00%
icetexboglobserver1-r	100.00%
icetexbogelasticserver1	100.00%
icetexbogelasticserver2	100.00%
icetexbogelasticserver3	100.00%
icetexbogliferaynfs	100.00%
icetexbogliferayserver1	100.00%
icetexbogliferayserver2	100.00%
icetexboglxdarumasrv1	100.00%
icetexboglxdarumasrv2	100.00%

Ilustración 3 Reporte ELK Promedio Disponibilidad Servicios en Housing – Datacenter Principal

#	Cod Servicio	Hostname	Disponibilidad
1	INR0228	ictxisgesbd	100%
2	INR0229	ictxisgesapp	100%
3	INR0233	icetexboglخورفو1	100%
4	INR0234	ictxprusigapp	100%
5	INR0237	icetexboglobserver1-r	100%
6	INR0238	icetexbogliferaynfs	100%
7	INR0239	icetexbogelasticserver1	100%
8	INR0241	icetexbogelasticserver3	100%
9	INR0242	icetexbogliferayserver2	100%
10	INR0243	icetexbogliferayserver1	100%

11	INR0244	icetexboglxdarumasrv1	100%
12	INR0245	icetexboglxdarumasrv2	100%
13	INR0246	iceteboglxdarumatest	100%
14	INR0247	preprodsec-icetexboglxroad2n	100%
15	INR0248	icetexboglxroad3	100%
16	INR0249	xroadsec-icetexboglxroad1	100%
17	INR0250	qasec-icetexboglxroadtest	100%
18	INR0262	icetexboglxorfeo2	100%
19	INR0276	cxvodaprodn011	100%
20	INR0277	cxvodaprodn021	100%
21	INR0278	cxvodacontn011	100%
22	INR0240	icetexbogelasticserver2	100%
23	INR0260	icetexbogobognfs1	100%
24	INR0252	icetexbogobognfs2	100%
25	INR0236	ictxbogsvpt1	100%
26	INR0235	ictxbogsvpt2	100%
27	INR000322	ictxcontroldoc	0%
28	INR0226	mira	100%
29	INR0253	bastion	100%

Tabla 8 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 9 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 nodos donde se encuentran los servicios del Portal Web institucional web.icetex.gov.co, los cuales estuvieron en un 100 % tanto en el Nodo1 como en el Nodo2 durante el mes de mayo [ReportDynatracePortal Mayo2024.pdf](#)

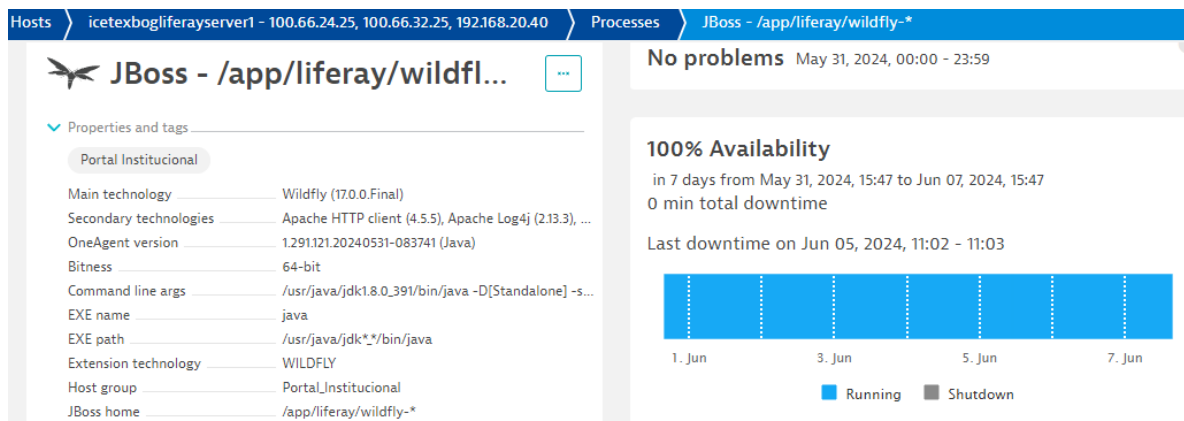


Ilustración 4 Disponibilidad Nodo1 Servicios Portal Web Icetex (Dynatrace)

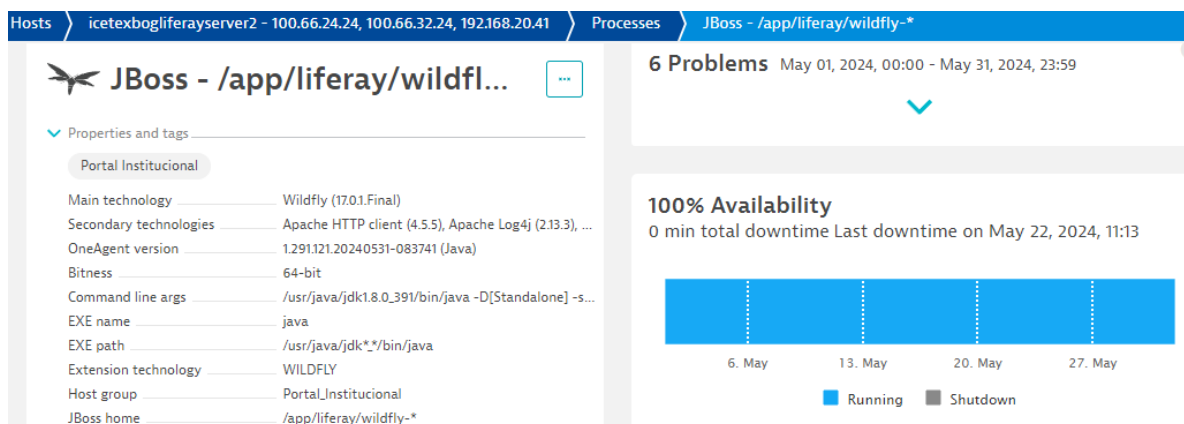


Ilustración 5 Disponibilidad Nodo 2 Servicios Portal Web Icetex (Dynatrace)

Portal WEB web.icetex.gov.co [99,94%]

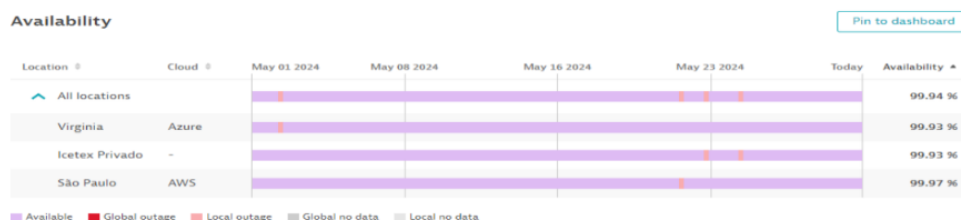
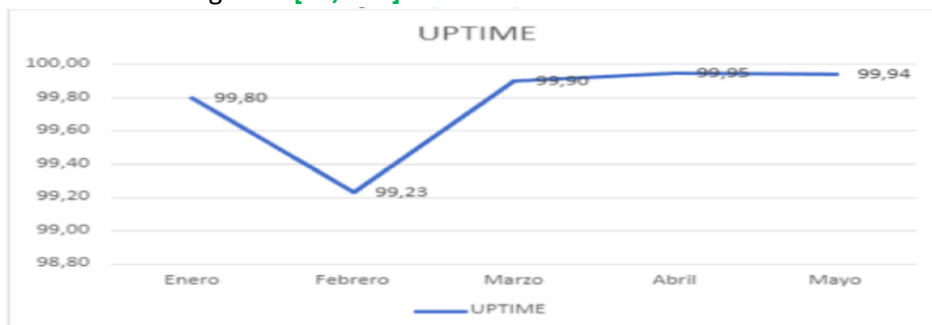


Ilustración 6 UPTIME: Portal WEB web.icetex.gov.co

Durante el mes de mayo se evidenció un comportamiento estable del portal WEB institucional y se cumplió con el porcentaje de disponibilidad de este con un porcentaje del 99,94% adicional en este informe mensual se incluyeron métricas e indicadores que contribuyen al entendimiento y al comportamiento del servicio, tales como número de visitantes donde se evidencia que el portal WEB cuenta con un total de 539 mil usuarios, con 393 mil usuarios nuevos. El tiempo de interacción medio es de 2 minutos 56 segundos, señalando el interés de la audiencia en las diferentes páginas del portal web.icetex.gov.co

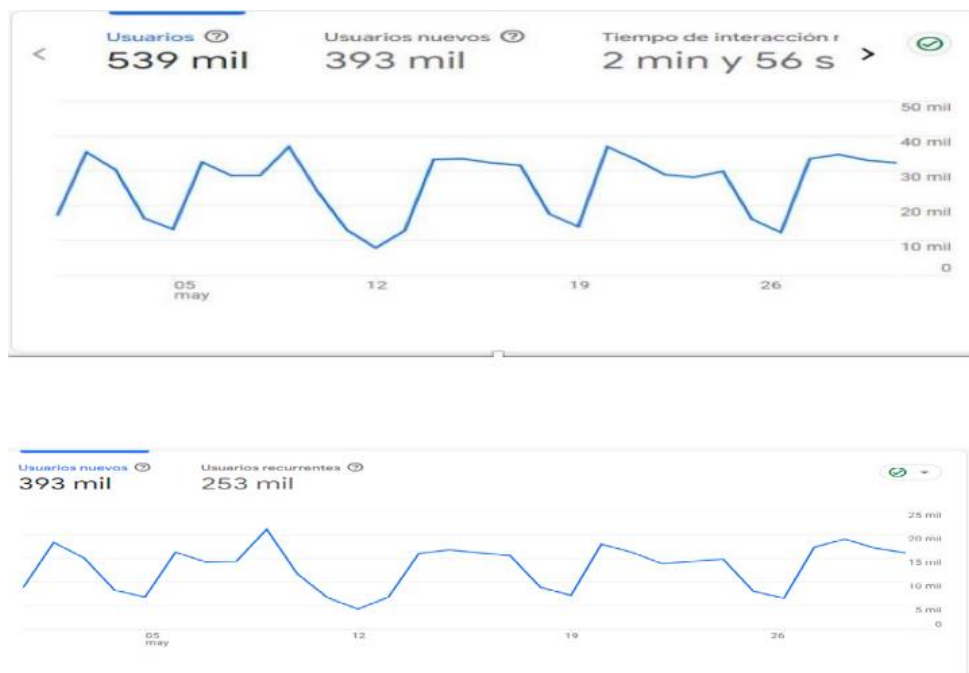


Ilustración 7 Métrica de Visitantes Portal WEB web.icetex.gov.co

La mejora continua tanto en la presentación del informe como en la atención del servicio generan valor al cliente haciendo que evidencie un aumento en la satisfacción en la prestación del servicio.

5.1.3 Backup Servidores Triara

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

Backup job summary

Backup job summary report

Generated on: Jun 01, 2024 08:39 AM

Server group : BgOTIC
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 (May 4, 2024, 08:39:15 AM - Jun 1, 2024, 08:39:15 AM)
Time zone : ComenServ
Day Start Time : 12:00 AM
Snap and Backup Copy options : Snap and Backup Copy options
Advanced : None

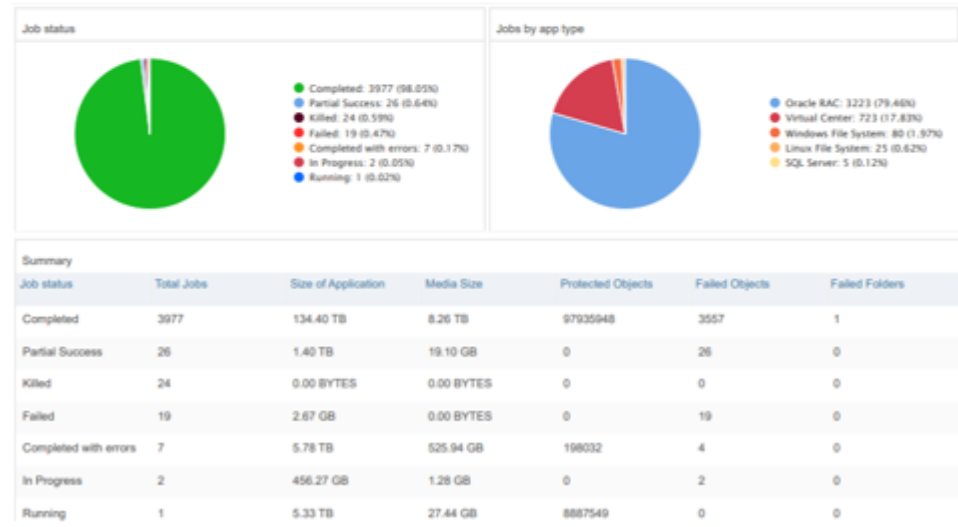


Ilustración 8 Evidencia Backup Servidores

5.2 Datacenter Alterno

5.2.1 Hosting Virtual (IaaS)

En el transcurso del mes de mayo 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 mensual replicacion mayo 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 (vcsatriara-ext.datacenterdhs.local -> vmegacenter.datacenterdhs.local) cuenta con 14 replicas

General					
Name			Count		
OK			13		
Paused			1		
Grupo de protección: PG_INFOTIC_7 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0226_INFOTIC_REP	OK	5 of 5	May 31, 2024	4.84 MB	5 minutes
Grupo de protección: PG_INFOTIC_6 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0228_INFOTIC_REP	OK	1 of 1	May 31, 2024	9.55 MB	1 hour
INR0229_INFOTIC_REP	OK	1 of 1	May 31, 2024	65.11 MB	1 hour
Grupo de protección: PG_INFOTIC_1 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0233_INFOTIC_REP	OK	6 of 6	May 31, 2024	3.6 MB	30 minutes
INR0262_INFOTIC_REP	OK	1 of 1	May 31, 2024	1.66 MB	1 hour
Grupo de protección: PG_INFOTIC_5 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0236_INFOTIC_REP	OK	2 of 2	May 31, 2024	34.17 MB	2 hours
Grupo de protección: PG_INFOTIC_4 (4)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0237_INFOTIC_REP	OK	2 of 2	May 31, 2024	9.51 MB	5 minutes
INR0238_INFOTIC_REP	Buscar...			14.98 MB	1 hour
INR0239_INFOTIC_REP				15.48 MB	1 hour
INR0243_INFOTIC_REP				19.73 MB	1 hour

Ilustración 9 Reportes de replicación SRM a Sitio Alterno, mayo 2024

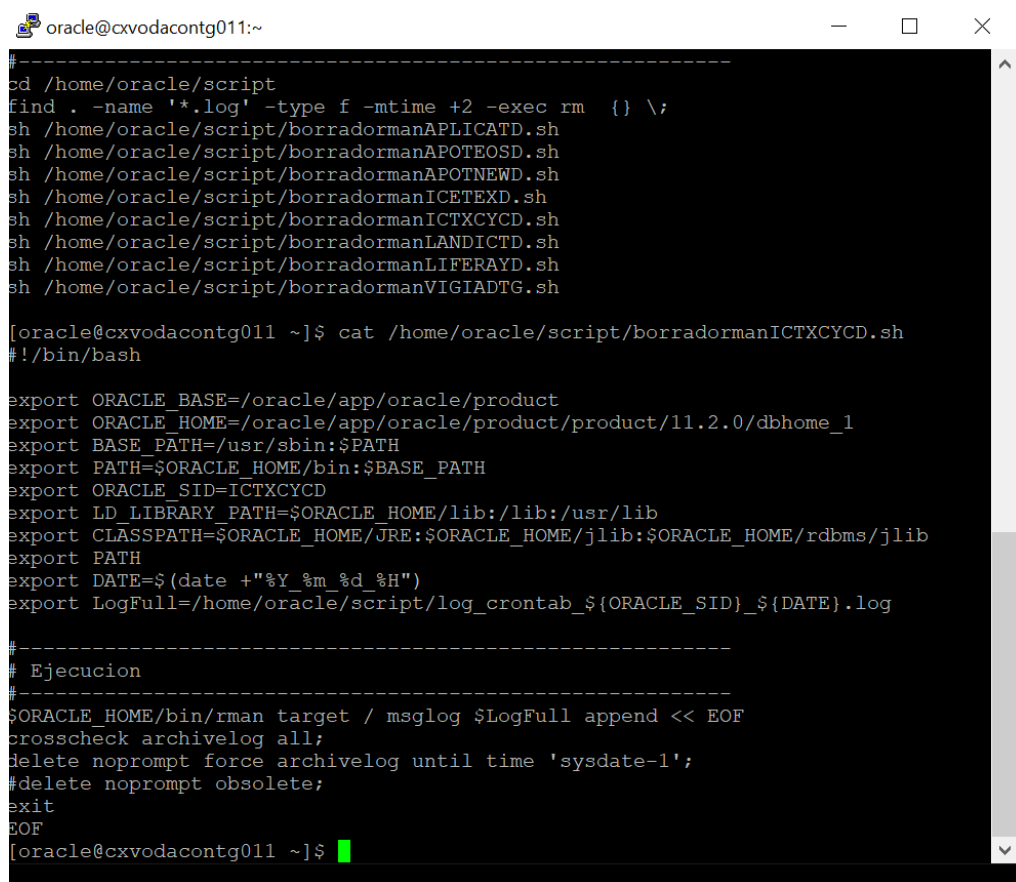
A continuación, se detallan los servidores con sus correspondientes servicios los cuales están siendo replicados a MEGACENTER :

#	INR Replicación	Host name	Servicio	VirtualMachine MEGACENTER
1	INR0204	icetexbogswwmira	Portal Web	INR0226_INFOTIC_REP
2	INR0207	ictxisgesbd	Sisgestion	INR0228_INFOTIC_REP
3	INR0206	ictxisgesapp	Sisgestion	INR0229_INFOTIC_REP
4	INR0220	icetexboglxorfeo1	ORFEO	INR0233_INFOTIC_REP
5	INR0219	icetexboglxorfeo2	ORFEO	INR0262_INFOTIC_REP
6	INR0208	ICTXBOGSRVPT1	Portal Transaccional	INR0236_INFOTIC_REP
7	INR0209	icetexbogbalserv1	Portal productivo (liferay)	INR0237_INFOTIC_REP
8	INR0210	icetexbogliferaynfs	Portal productivo (liferay)	INR0238_INFOTIC_REP
9	INR0217	icetexbogelasticserver1	Portal productivo (liferay)	INR0239_INFOTIC_REP
10	INR0218	icetexbogliferayserver1	Portal productivo (liferay)	INR0243_INFOTIC_REP
11	INR0215	icetexboglxdarumasrv1	DARUMA	INR0244_INFOTIC_REP
12	INR0213	icetexboglxdarumasrv2	DARUMA	INR0245_INFOTIC_REP
13	INR0214	icetexboglxroad1	XROAD	INR0249_INFOTIC_REP

Tabla 10 Servicios replicados – Datacenter MEGACENTER

5.2.2 Dataguard BBDD Megacenter

Durante el mes de mayo 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 Mayo.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 $LogFull append << EOF
crosscheck archivelog all;
delete noprompt force archivelog until time 'sysdate-1';
#delete noprompt obsolete;
exit
EOF
[oracle@cxvodacontg011 ~]$
```

Ilustración 10 Evidencia Dataguard replicado a Megacenter BD

Se genero la consulta de los archivos recibidos y aplicados de la base de datos de ICTXCYCD a 31/05/2024 10:18 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 alterno Megacenter (Medellín).

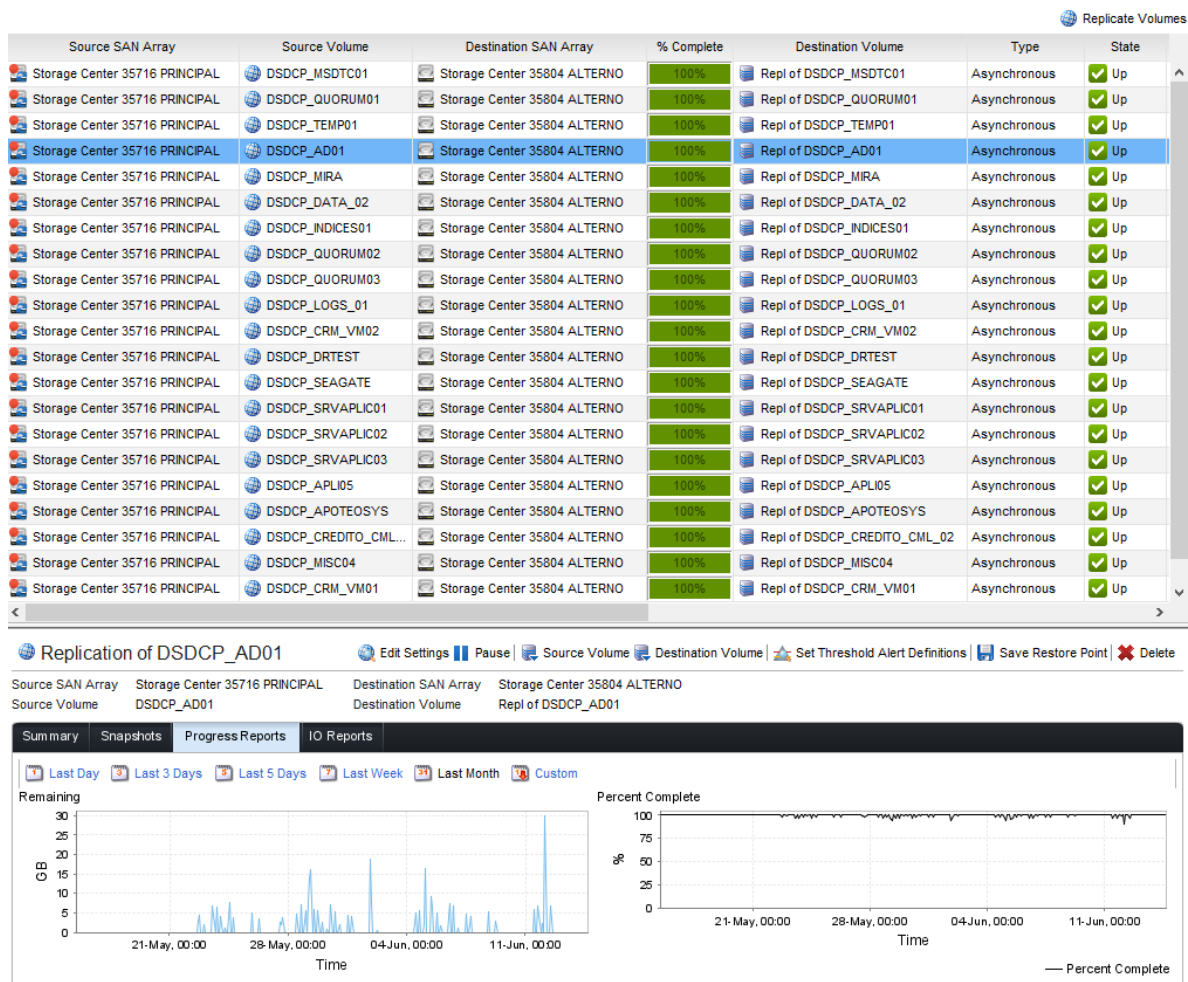


Ilustración 11 Evidencia replicado servicios On-premise Ictetex a Megacenter

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 mayo 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 11 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 mayo, en materia de seguridad.

6.1 Servicios de Endpoint

Con respecto a Filtrado Web del antivirus Sophos, se ha terminado de realizar el comparativo entre los filtrados web que tienen los equipos de seguridad perimetral (Firewall FortiGate) de la Entidad. Queda pendiente una sesión con ICETEX para exponer este comparativo y definir los parámetros de configuración para empezar con la planeación y ejecución de esta actividad.

Actualmente se continúa habilitado y actualizado el módulo de acceso a USB a los equipos de la Entidad y los cuales se relacionan en las actividades mensuales al igual de la protección XDR y EDR, amenazas y despliegue de políticas centralizadas.

En Endpoints, el porcentaje de avance de instalación y configuración permanece al 90%, dado que no se ha podido avanzar más porque el 10% restante son equipos que se encuentran en bodega.

6.2 ESTADÍSTICAS PORTALES

Durante el mes de mayo 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 mayo seguridad 2024.pdf](#) en el capítulo *PORTALES PROTEGIDOS POR EL WAF*

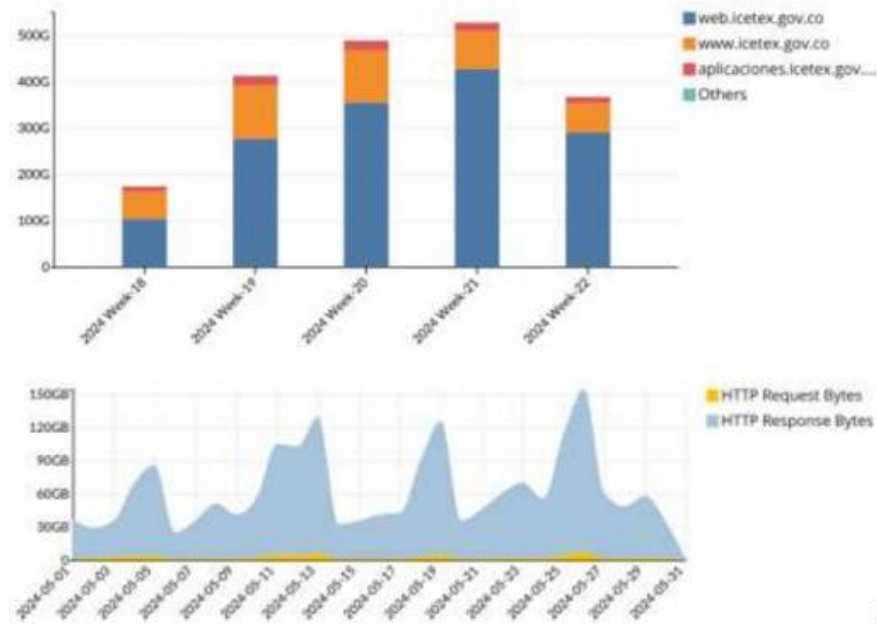


Ilustración 12 Evidencia Gráfica Estadísticas de Portales

En el periodo de tiempo analizado se presenta un promedio de 450 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 mayo seguridad 2024.pdf](#) se puede encontrar el Informe de Gestión Mensual que contiene información relevante de seguridad para el mes de mayo 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	2024/06/04 14:30:23
Uptime	88:17:42:20
WAN IP	186.84.155.234

Ilustración 13 Evidencia Estado General de las Plataformas

6.4 Estado de Salud de los Equipos de Seguridad

En el transcurso del mes de mayo 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 capítulo4 ESTADO DE SALUD DE LOS EQUIPOS DE SEGURIDAD del documento [Reporte mayo 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 35.84 Mbps (Port7) en la última semana.

Imagen 14 Consumo Del Canal

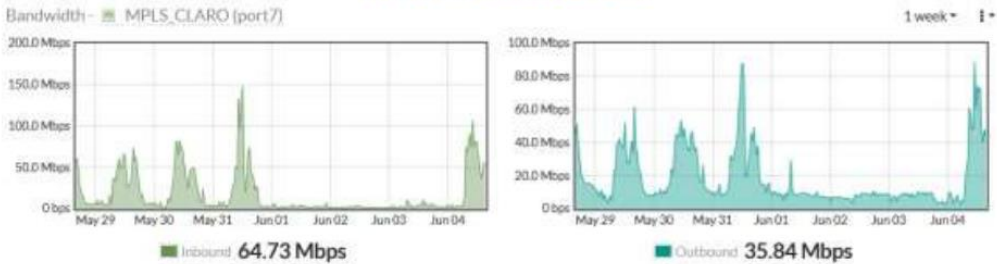


Ilustración 14 Evidencia Estado de Salud de los Equipos de Seguridad

6.5 Servicio de centro de Operaciones de Seguridad (SOC)

Durante el mes de mayo en el ICETEX 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 Mayo 2024.pdf](#)

3.1.1 Casos de Uso Seguridad

Se encuentran definidas **2.423** 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 15 Evidencia Imagen Reporte Monitoreo

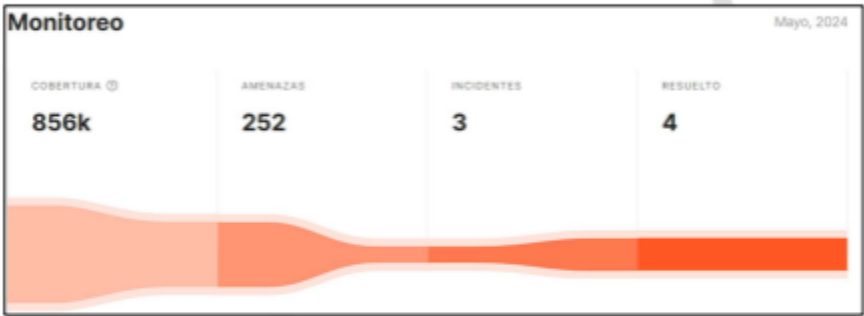
6.5.1 Monitoreo de Marca-Estrategia OSINT-SOC

Para el mes de mayo 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 Mensual MARCA-OSINT ICETEX Mayo 2024.pdf](#)

ANÁLISIS DE MONITOREO DE PROTECCIÓN DE MARCAR Y OSINT

Durante el periodo evaluado, la plataforma de monitoreo de protección de marca y OSINT – AXUR, reporta un total de **252** posibles amenazas de las 856k que fueron encontradas y analizadas automáticamente por la plataforma de monitoreo. A estas **252** posibles amenazas se les realizó una revisión y análisis interno, de sus características, datos e información.



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



Ilustración 16 Evidencia Imagen Reporte Monitoreo OSINT

Durante el periodo evaluado se detectaron 03 incidentes, 01 relacionado con aplicación móvil falsa, 01 relacionado con actividad sospechosa en sitio web y 01 relacionado con otros datos confidenciales.

6.6 Eventos Relevantes

Dada la integración de las plataformas de seguridad desplegadas en la entidad, le permite al ICETEX prevenir ataques de ciberseguridad que comprometan la continuidad del negocio.

- De los ataques reportados en este informe se hizo un bloqueo del 100%.
- Se realiza la protección de puntos finales y servidores con la herramienta de AV Sophos.
- Se realiza la restricción de la conexión VPN-SSL a países no autorizados.

6.7 RECOMENDACIONES

6.7.1 Recomendaciones Generales

- Verificar y aumentar los recursos del FortiSIEM, como se ha solicitado desde meses anteriores, en razón a que se están presentando alertas críticas de almacenamiento de logs o eventos y de CPU que impiden el correcto desarrollo de reportes mensuales.
- Verificar los dispositivos que están presentando errores para la lectura de eventos desde el FortiSIEM a través de los protocolos WMI y VM_SDK.
- 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 las alertas y reportes enviados y en lo posible dar respuesta o retroalimentar al SOC con el actualizar cada uno casos y realizar las correspondientes excepciones o filtros con el fin de disminuir las alertas y falsos positivos.
- 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.

6.7.2 Recomendaciones Específicas

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 12 Recomendaciones plataformas de seguridad

Recomendación	Estado	Criticidad
Garantizar la segmentación de la red que permita claramente definir qué servicios deben ser	Se toma a tesorería como área inicial se comparte plan de trabajo involucrando a	Media

alcanzados por cada usuario.	seguridad, Redes y el equipo de Windows	
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 la compañía a nivel de seguridad (ejm: tesorería).	Se propone al ICETEX elaborar el Procedimiento.	Media
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 13 Recomendaciones de seguridad para Ictetex

6.8 CONCLUSIONES

- La implementación de medidas adicionales de control de acceso contribuye a la mitigación de riesgos en incidentes de seguridad, fortaleciendo la postura de seguridad de la Entidad ante posibles amenazas y ataques.

- La utilización de herramientas de monitoreo permite una optimización en la detección y respuesta ante eventos anómalos o potencialmente maliciosos, mejorando la capacidad de identificación temprana y reduciendo los tiempos de respuesta frente a posibles incidentes de seguridad.
- La adopción de buenas prácticas en la gestión de credenciales de usuario disminuye el riesgo de materialización de eventos críticos o de alto impacto en la seguridad de la infraestructura, al garantizar la autenticación segura y la gestión adecuada de privilegios de acceso.
- La implementación de políticas y controles específicos para el BYOD (Bring Your Own Device) refuerza la postura de seguridad de la entidad al facilitar la integración segura de dispositivos personales en el entorno corporativo. Esto permite mitigar riesgos asociados a la pérdida de datos, accesos no autorizados y vulnerabilidades inherentes a la diversidad de dispositivos utilizados dentro de la infraestructura de la organización.

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 mayo, 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 MAYO 2024 .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 MENSUAL MAYO 2024 .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 14 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 mayo 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.

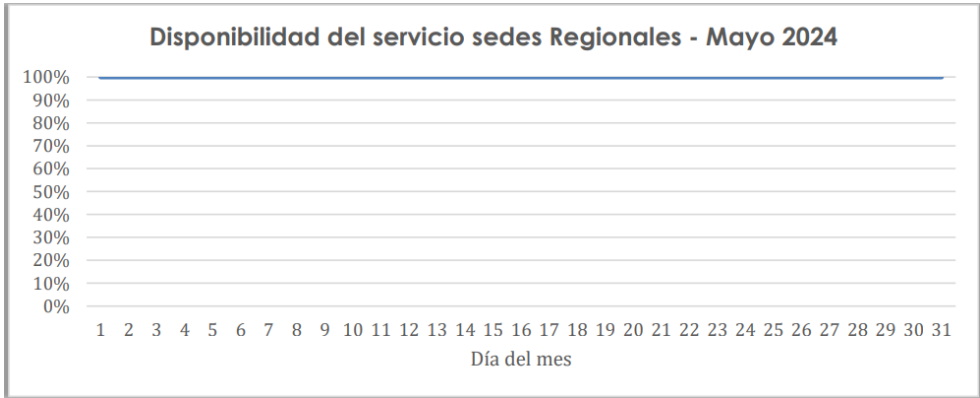


Ilustración 17 Disponibilidad de servicio videoconferencia sedes regionales – mayo 2024

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

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

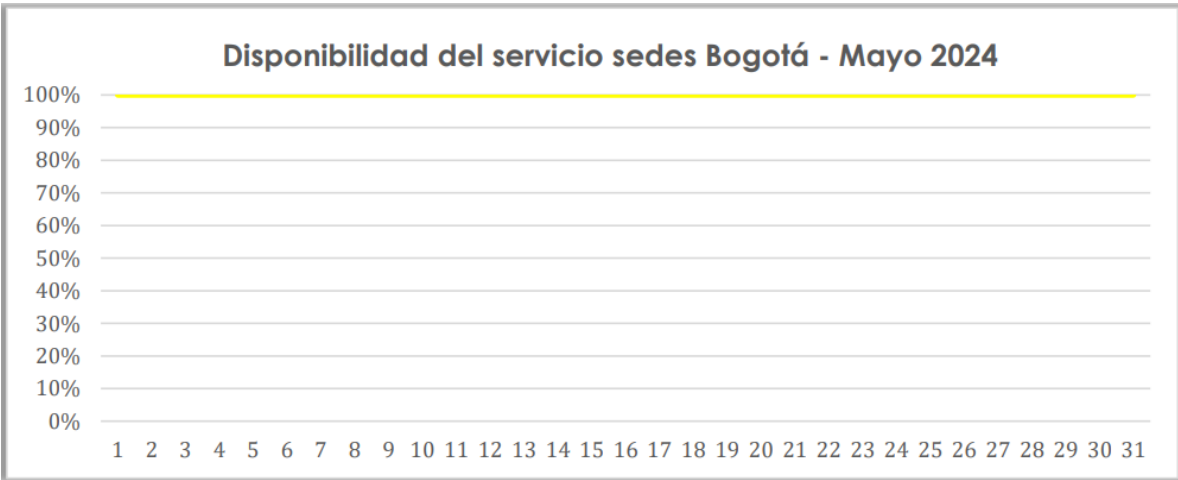


Ilustración 18 Disponibilidad de servicio videoconferencia sedes Bogotá – mayo 2024

8.2 Gestión de incidencias y requerimientos – sedes regionales

Para el periodo comprendido entre el 1 y el 31 de mayo, no se generaron requerimientos especiales o

solicitudes de soporte técnico que requirieran atención y gestión en las sedes Regionales; Tampoco se reportaron incidencias a nivel del servicio para estas sedes durante el mes del presente informe, sin embargo, se tuvo total disponibilidad para recibir cualquier requerimiento de soporte o solicitud de apoyo concerniente a la solución de videoconferencia desplegada y en funcionamiento.

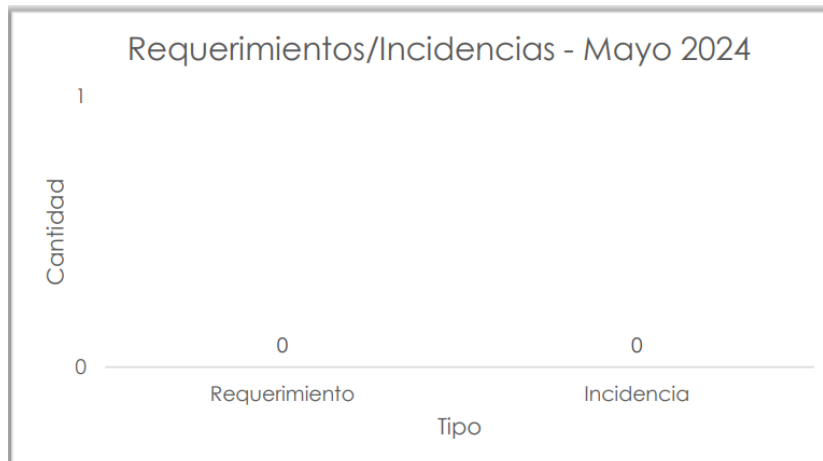


Ilustración 19 Incidencias/Requerimientos sedes Regionales – mayo 2024

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

Para el periodo comprendido entre el 1 y el 31 de mayo, no se recibieron solicitudes 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. Por lo tanto, durante este periodo no se presentaron novedades y los módulos se encuentran funcionando de manera correcta y con la regularidad requerida.

Se continúa al tanto para recibir cualquier solicitud de soporte, acompañamiento o apoyo concerniente a la solución de videoconferencia desplegada.

- Durante el mes de mayo 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 Mayo 2024.pdf](#)

9 CALCULO DE CONCILIACIÓN DE LOS SERVICIOS DEL MES DE MAYO

A la fecha la conciliación del mes de mayo con ICETEX se encuentra en proceso, el detalle de conciliación del mes anterior se puede ver en el siguiente link [Conciliación mayo 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				\$ 7.699.382.200,80
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	
Pago No. 11 - mes:	Febrero	de	2024	
			\$ 732.950.101,55	
Pago No. 12 - mes:	Marzo	de	2024	
			\$ 733.890.372,09	
VALOR CAUSADO QUE NO SE HA PAGADO (valor a pagar factura) *				\$ 732.771.085,82
VALOR TOTAL EJECUTADO (valor pagado + valor causado no pagado)				\$ 9.161.889.263
SALDO DEL CONTRATO (valor total del contrato – valor total ejecutado)				\$ 22.237.107.595
PORCENTAJE DE EJECUCIÓN				29.18%%
* 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 15 Ejecución Presupuestal