



INFORME DE ACTIVIDADES DEL CONTRATO

**CONTRATO NUMERO
2022-0792**

Agosto 01 al 31 de 2024

CONTENIDO

Contenido

1	INTRODUCCIÓN	5
2	OBJETIVOS	5
3	RESUMEN EJECUTIVO	5
4	SERVICIOS DE CONECTIVIDAD	6
4.1	INTERNET PARA LA GENTE	10
4.2	Canales SDWAN	10
4.3	Canal de Replicación (Triara – Megacenter)	10
4.4	Señalética (Internet para la gente)	11
4.5	Implementación de IPv6	11
4.6	Gestión de Vulnerabilidades en Networking	12
4.7	CONCLUSIONES DEL SERVICIO DE CONECTIVIDAD	12
4.8	RECOMENDACIONES DEL SERVICIO DE CONECTIVIDAD	12
5	SERVICIOS CENTROS DE COMPUTO	13
5.1	Datacenter Principal	13
5.1.1	Disponibilidad de Servicios – Datacenter Principal	15
5.1.2	Disponibilidad TRIARA para los servicios de página web	18
5.1.3	Análisis componente Liferay	20
5.1.4	Backup Servidores Triara	21
5.2	Datacenter Alterno	22
5.2.1	Hosting Virtual (IaaS)	22
5.2.2	Dataguard BBDD Megacenter	25
5.2.3	Replicación Servicios OnPremise de Icetex a Megacenter	26
5.2.4	Disponibilidad de Servicios de Housing – Datacenter Alterno	26
5.2.5	Servicios de DRP	26
6	SEGURIDAD	27
6.1	Servicios de Endpoint	27
6.2	ESTADÍSTICAS PORTALES	28
6.3	Estado General de las Plataformas	28
6.4	Estado de Salud de los Equipos de Seguridad	32
6.5	Servicio de centro de Operaciones de Seguridad (SOC)	32
6.5.1	Monitoreo de Marca-Estrategia OSINT-SOC	33
6.6	Eventos Relevantes	36
6.7	RECOMENDACIONES	37
6.7.1	Recomendaciones Generales	37
6.7.2	Recomendaciones Específicas	38
6.8	CONCLUSIONES	39
7	GESTION DE SERVICIO	40
7.1	ACTIVIDADES DE OPERACIÓN	40
7.2	Profesionales Especializados	40

7.2.1	Especialista en Base de Datos DBA	40
7.2.2	Especialista web master	40
7.2.3	Administrador de Soluciones	41
7.2.4	Especialista en Networking.....	41
7.2.5	Especialista Integrador de nube	41
7.2.6	Especialista en seguridad.....	42
8	SERVICIO DE COLABORACIÓN	42
8.1	<i>Disponibilidad del servicio – sedes Bogotá (aguas - ángel)</i>	43
8.2	<i>Gestión de incidencias y requerimientos – sedes regionales</i>	43
8.3	<i>Gestión de incidencias y requerimientos – Bogotá (Aguas - Angel)</i>	44
9	CALCULO DE CONCILIACIÓN DE LOS SERVICIOS DEL MES DE AGOSTO	48

INDICE DE TABLAS

Tabla 1	Disponibilidad de canales	9
Tabla 2	Canales pendientes por instalar	9
Tabla 3	Canales pendientes por ampliar agosto	10
Tabla 4	Disponibilidad canales “Internet para la gente”	10
Tabla 5	Disponibilidad canales “SDWAN”	10
Tabla 6	Estado de la instalación de la señalética de Wifi	11
Tabla 7	Ejemplo de Direccionamiento IPv6	12
Tabla 8	Códigos relacionados Disponibilidad Servicios en Housing – Datacenter Principal	18
Tabla 9	Disponibilidad de Servicios de Housing – Datacenter Principal.....	18
Tabla 10	Resumen-Análisis componente Liferay agosto	21
Tabla 11	Servicios replicados – Datacenter MEGACENTER	24
Tabla 12	Recursos-Datacenter Alterno Anexo #3. EC-Alternos_IAS	24
Tabla 13	Disponibilidad de Servicios de Housing – Datacenter Alterno.....	26
Tabla 14	Recomendaciones plataformas de seguridad	38
Tabla 15	Recomendaciones de seguridad para Ictetex.....	39
Tabla 16	Distribución módulos de videoconferencia por sede	42
Tabla 17	Ejecución Presupuestal.....	49

INDICE DE ILUSTRACIONES

Ilustración 1	Evidencia del Resumen del Monitoreo CPU-Memoria ELK.....	13
Ilustración 2	Evidencia del Resumen del Monitoreo CPU-Memoria servidores Openshift ELK	14
Ilustración 3	Evidencia del Resumen del Monitoreo ELK	15
Ilustración 4	Reporte ELK Promedio Disponibilidad Servicios en Housing – Datacenter Principal ...	16
Ilustración 5	Reporte ELK Promedio Disponibilidad servidores Open shift en Housing – Datacenter Principal.....	17
Ilustración 6	UPTIME: Portal WEB web.ictetex.gov.co	19
Ilustración 7	Métrica de Visitantes Portal WEB web.ictetex.gov.co	19
Ilustración 8	Evidencia Backup Servidores.....	22
Ilustración 9	Reportes de replicación SRM a Sitio Alterno, agosto 31 2024	23

Ilustración 10 Evidencia Dataguard replicado a Megacenter BD	25
Ilustración 11 Evidencia replicado servicios OnPremise Icetex a Megacenter.....	26
Ilustración 12 Evidencia Gráfica Estadísticas de Portales	28
Ilustración 13 Estado General de las Plataformas- Seguridad-Perimetral-DC_Principal (FortiGate-Triara)	29
Ilustración 14 Estado General de las Plataformas- Seguridad-Perimetral-DC-Alterno- (FortiGate-Aguas)	29
Ilustración 15 Estado General de las Plataformas- Seguridad-Perimetral- DC-Alterno-(FortiGate-Megacenter).....	30
Ilustración 16 Estado General de las Plataformas WAF-(FortiWeb_Triara_APPS_Nuevas)	30
Ilustración 17 Estado General de las Plataformas WAF-(FortiWeb-Triara-APPS_Viejas)	31
Ilustración 18 Estado General de las Plataformas seguridad-Local-(FortiSandBox)	32
Ilustración 19 Evidencia Estado de Salud de los Equipos de Seguridad	32
Ilustración 20 Evidencia Imagen Reporte Monitoreo	33
Ilustración 21 Evidencia Imagen Reporte Monitoreo OSINT	35
Ilustración 22 Disponibilidad de servicio videoconferencia sedes regionales – agosto 2024.....	43
Ilustración 23 Disponibilidad de servicio videoconferencia sedes Bogotá –agosto 2024	43
Ilustración 24 Incidencias/Requerimientos sedes Regionales – agosto 2024	44
Ilustración 25 Evidencia primera visita módulo funcional sede Aguas 65”, piso 2 – agosto 2024... 45	45
Ilustración 26 Prueba de funcionamiento OPS Backup módulo 65” sede Aguas, piso 4 – agosto 2024.....	46
Ilustración 27 Módulo sede Aguas piso 4 – agosto 2024.....	46
Ilustración 28 Verificación sede Aguas, piso 6 (módulo móvil) agosto 2024	47
Ilustración 29 Verificación sede Aguas, piso 8 - agosto 2024	47
Ilustración 30 Verificación módulo sede Ángel - agosto 2024.....	48

1 INTRODUCCIÓN

Este informe contiene la información relacionada con las actividades ejecutadas por INFOTIC en el periodo comprendido entre el 01 al 31 de agosto 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 agosto 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 Ictex según lo acordado en el contrato.

2 OBJETIVOS

Presentar el informe de actividades ejecutadas por INFOTIC durante el periodo del 01 al 31 de agosto 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: La operación de los canales de conectividad se mantuvo estable, garantizando los anchos de banda requeridos por ICETEX realizando gestión sobre los casos reportados que afectan directamente los canales o sobre la herramienta de monitoreo de los mismos, se han venido coordinando con el operador la instalación de los canales pendientes.

En cuanto a la gestión de vulnerabilidades se encuentran remediadas las vulnerabilidades reportadas en el último escaneo de vulnerabilidades y nos encontramos atentos de los resultados de una nueva ejecución de escaneo de vulnerabilidades para proceder a su atención; en cuanto a la implementación de IPV6 se ha venido trabajando con los especialistas de Seguridad realizando las pruebas de implementación de IPV6 donde se han configurado las interfaces de MPLS de los firewalls de Aguas, Triara y Megacenter para la comunicación entre sedes a través de IPV6 y avanzando en los temas de documentación de acuerdo con los lineamientos que va indicando Ictex periódicamente.

De igual forma se ha estado trabajando tanto con el equipo interno como con Ictex en la próxima prueba de DRP, realizando las actividades requeridas a nivel de Networking en las pruebas del pretest realizado.

Servicios de Colaboración: Durante este mes 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 comparten este mes los cronogramas de los mantenimientos programados para los equipos de infraestructura tales como

UPS y sistemas eléctricos, tanto en el Datacenter principal como en el Datacenter alterno.

Servicio de Seguridad: Durante agosto de 2024 se llevaron a cabo las actividades relacionadas con la administración y gestión de la seguridad perimetral. Estas actividades incluyeron la resolución de las alertas de tráfico de la red que genera el SOC. En el FortiSIEM se detectaron durante el mes múltiples eventos relacionados con tráfico permitido desde direcciones IP enmarcadas en listas de amenazas (6 de agosto, 15 de agosto, 21 de agosto, 22 de agosto, 26 de agosto y 29 de agosto). Se revisaron y analizaron los eventos para asegurar que no representaran una amenaza para la seguridad de la red y se tomaron las respectivas acciones para contener posibles amenazas. También durante el mes, se evidenciaron a través del FortiSIEM alertas de uso de protocolos inseguros o sin cifrar (IMAP), las cuales fueron realizadas por usuarios de la entidad a través de las redes inalámbricas y quienes no pudieron ser validados (8 de agosto y 14 de agosto). Se implementaron medidas de seguridad adicionales para prevenir accesos no autorizados y se realizó seguimiento continuo. Dentro de los alertamientos recibidos durante el mes se presentaron eventos de cambio de estado activo a no responder a la sonda de monitoreo, esto se debe a una aplicación tercerizada que no está licenciada y por esto falla constantemente. Se solicita al SOC realizar una excepción sobre estas aplicaciones mientras se solucionan estas fallas (21 de agosto).

Personal del Proyecto en Sitio: El personal del proyecto operó de manera normal. Los informes de las actividades se adjuntan en el presente informe. El ingeniero de seguridad (Jhon Pava) ha manifestado desde el mes de febrero 2024 el deseo de no continuar desempeñando sus funciones para el ICETEX, para esto se han remitido varias hojas de vida para ser evaluadas y generar el concepto de aprobado, es de aclarar que desde INFOTIC se ha realizado el acercamiento con el ingeniero, para que desista de la opción de retirarse pero la respuesta ha sido que sigue en firme la opción de retirarse del proyecto por proyectos personales.

Bolsa para servicios por demanda: En el mes de agosto por parte de ICETEX continua pendiente de la respuesta sobre el tema de las cintas de Backup, se alerta al ICETEX que no se cuenta con espacio para seguir realizando el almacenamiento de los Backups realizados a la información de acuerdo a la programación establecida y es urgente contar con las cintas de backups para generar el procedimiento de traslado de la información que reposa en los servidores del proveedor tecnológico y enviarlos a custodia externa como es debido.

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 agosto 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 agosto de 2024.

4 SERVICIOS DE CONECTIVIDAD

Durante el mes de agosto, los canales principales y Backup instalados operaron de manera normal.

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 Agosto 2024 - ALLOT INFOTIC.pdf](#)

Durante el mes de agosto 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:

[Reporte Mensual Disponibilidad Canales ICETEX Agosto 2024.pdf](#)

Sede	Categoría	INR	% Mes
BOGOTA D.C.	Principal / FO (Sede Aguas)	INR0037	100.00%
	Backup / FO (Sede Aguas)	INR0036	100.00%
	Principal / IPVPN (Sede Chapinero)	INR0022	100.00%
	Backup / IPVPN (Sede chapinero)	INR0020	99.98%
	Principal / IPVPN (Angel)	INR0272	100.00%
	Backup / IPVPN (Angel)	INR0273	100.00%
IBAGUE	Principal / IPVPN	INR0073	99.91%
	Backup / IPVPN	INR0076	99.46%
LETICIA	Principal / Satelital		0.00%
NEIVA	Principal / IPVPN	INR0039	99.98%
	Backup / IPVPN	INR0041	99.82%
TUNJA	Principal / IPVPN	INR0104	100.00%
	Backup / IPVPN	INR0106	100.00%
VILLAVICENCIO	Principal / IPVPN	INR0085	95.15%
	Backup / IPVPN	INR0084	99.93%
ARMENIA	Principal / IPVPN	INR0074	100.00%
	Backup / IPVPN	INR0072	99.24%
MANIZALES	Principal / IPVPN	INR0088	99.80%
	Backup / IPVPN	INR0087	99.77%
MEDELLIN	Principal / IPVPN	INR0133	99.99%
	Backup / IPVPN	INR0132	100.00%
APARTADO	Principal / IPVPN	INR0144	99.97%
PEREIRA	Principal / IPVPN	INR0079	100.00%
	Backup / IPVPN	INR0077	100.00%
QUIBDO	Principal / IPVPN	INR0014	99.97%
	Backup / IPVPN		0.00%
BARRANQUILLA	Principal / IPVPN	INR0103	100.00%
	Backup / IPVPN	INR0100	100.00%
CARTAGENA	Principal / IPVPN	INR0109	99.57%

	Backup / IPVPN	INR0107	99.72%
MONTERIA	Principal / IPVPN	INR0080	100.00%
	Backup / IPVPN	INR0081	99.87%
RIOHACHA	Principal / IPVPN	INR0164	99.61%
	Backup / IPVPN	INR0162	99.58%
SANTA MARTA	Principal / IPVPN	INR0154	95.72%
	Backup / IPVPN	INR0152	99.49%
SINCELEJO	Principal / IPVPN	INR0095	93.50%
	Backup / IPVPN	INR0097	93.38%
SAN ANDRES	Principal / IPVPN	INR0000368	99.94%
BARRANCABERMEJA	Principal / IPVPN		0.00%
SAN GIL	Principal / IPVPN		0.00%
BUCARAMANGA	Principal / IPVPN	INR0062	100.00%
	Backup / IPVPN	INR0061	100.00%
CUCUTA	Principal / IPVPN	INR0044	100.00%
	Backup / IPVPN	INR0047	100.00%
VALLEDUPAR	Principal / IPVPN	INR0091	99.98%
	Backup / IPVPN	INR0090	99.68%
YOPAL	Principal / IPVPN	INR0121	99.98%
	Backup / IPVPN	INR0123	99.89%
ARAUCA	Principal / IPVPN	INR0110	99.63%
CALI	Principal / IPVPN	INR0151	99.02%
	Backup / IPVPN	INR0153	100.00%
BUENAVENTURA	Principal / IPVPN	INR0051	100.00%
MOCOYA	Principal / IPVPN	INR0135	98.12%
	Backup / Satelital	INR0136	90.66%
PASTO	Principal / IPVPN	INR0130	99.85%
	Backup / IPVPN	INR0131	99.85%
POPAYAN	Principal / IPVPN	INR0035	100.00%
	Backup / IPVPN	INR0032	100.00%
TUMACO	Principal / IPVPN	INR0147	83.43%
WAN general (concentrador total red)	MPLS PP	INR0266	100.00%
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 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	INR0177	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	INR0230	100.00%

Internet Dedicado Navegación centralizada Megacenter	Internet Backup		
Banco de la Republica hasta Edificio Dirección General ICETEX	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0000289	100.00%
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	100.00%
Salida de portales https://portal.icetex.gov.co/portal y www.icetex.gov.co hacia internet en centro de cómputo principal	Internet Reverso para Portales	INR0264	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	INR0268	100.00%

Tabla 1 Disponibilidad de canales

A continuación, se listan las sedes que continúan en proceso de instalación:

SERVICIO	OBSERVACIONES
Leticia canal de datos principal.	En fase de instalación
Quibdó canal de datos de Backup	En fase de instalación

Tabla 2 Canales pendientes por instalar

Los canales de datos principales para Barrancabermeja y San Gil, no ha sido posible avanzar teniendo en cuenta que aún el Icetex no tiene oficina en dichas ciudades.

Canal principal de Leticia e Internet para la gente: En proceso de Instalación se hace seguimiento en las sesiones semanales y actualmente se depende de las adecuaciones físicas por parte de Icetex para poder instalar los canales.

Canal de Backup de Quibdó: igualmente el seguimiento se hace en la sesión semanal y según el último seguimiento el operador indica que "Airplane informó que darán inicio a la realización del contrato y que esto puede demorar alrededor de 15 días hábiles", esto porque la demora ha sido este contrato con Airplane que tendría que realizar cualquier operador que requiera instalar un canal en el centro comercial donde se encuentra la oficina.

En conclusión, se prestó el servicio en las sedes del Icetex brindando conectividad y sin interrumpir la operación del Instituto. Durante el mes de agosto no se realizaron 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)
NEIVA	Principal / IPVPN	INR0039	18	20	18	2

Tabla 3 Canales pendientes por ampliar agosto

4.1 INTERNET PARA LA GENTE

Durante el mes de agosto el servicio de Internet para la gente se prestó sin interrupciones en trece 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	100.00%
CALI	INTERNET PARA LA GENTE	INR0160	99.03%
AGUAS	INTERNET PARA LA GENTE	INR0029	100.00%
CHAPINERO	INTERNET PARA LA GENTE	INR0015	100.00%
MEDELLIN	INTERNET PARA LA GENTE	INR0122	100.00%
APARTADO	INTERNET PARA LA GENTE	INR0140	100.00%
ARAUCA	INTERNET PARA LA GENTE	INR0115	99.87%
LETICIA*	INTERNET PARA LA GENTE		0.00%
QUIBDO	INTERNET PARA LA GENTE	INR0021	100.00%
RIOHACHA	INTERNET PARA LA GENTE	INR0159	99.85%
SAN ANDRES	INTERNET PARA LA GENTE	INR0000367/ INR0000369	100.00%
YOPAL	INTERNET PARA LA GENTE	INR0127	100.00%
MOCOA	INTERNET PARA LA GENTE	INR0141	99.50%

Tabla 4 Disponibilidad canales "Internet para la gente"

*El Internet para la gente de Leticia se encuentra en proceso de Instalación.

4.2 Canales SDWAN

Durante el mes de agosto, 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	99.80%

Tabla 5 Disponibilidad canales "SDWAN"

SDWAN en las sedes de Leticia y San Andrés, se encuentra por el momento en proceso de instalación por parte del operador, en San Andrés se ha tardado por capacidad en la troncal la cual debió entrar en un proceso de ampliación por alta demanda de usuarios en la Isla aún sigue en el mismo estado.

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 agosto, funcionó sin ningún contratiempo.

La evidencia se encuentra en el [Informe mensual replicacion agosto 2024.pdf](#)

4.4 Señalética (Internet para la gente)

La señalética para el uso de la red WIFI en las oficinas, se encuentran entregadas trece, continua pendiente la señalética correspondiente a la ciudad de Cali, se encuentra en proceso de elaboración se ha retrasado porque tuvo un problema de avería en el transporte y de esta forma tiene un proceso distinto antes de volver a generar su elaboración que es más dispendioso según explica el operador de Telecomunicaciones.

A continuación se presenta la relación de las señaléticas entregadas y su fecha de entrega y/o instalación en sitio.

Ciudad	Fecha Entrega	Estado
Barranquilla	14-feb-24	Instalada en sitio
Bucaramanga	14-feb-24	Instalada en sitio
Cali	Pendiente	En elaboración
Bogotá (Aguas)	15-mar-24	Instalada en sitio
Bogotá (Chapi)	13-mar-24	Instalada en sitio
Medellín	06-mar-24	Instalada en sitio
Apartado	29-feb-24	Instalada en sitio
Arauca	20-feb-24	Instalada en sitio
San Andrés	18-junio-24	Instalada en sitio
Riohacha	20-feb-24	Instalada en sitio
Yopal	21-feb-24	Instalada en sitio
Mocoa	26-feb-24	Instalada en sitio
Quibdó	26-feb-24	Instalada en sitio
Leticia	15-mar-24	Entregada en Bogotá -aguas

Tabla 6 Estado de la instalación de la señalética de Wifi

4.5 Continuidad a la integración con el protocolo IPV6

Durante el mes de agosto, ICETEX ha llevado a cabo un proceso de normalización de sus redes a nivel nacional, migrando de direcciones ULA a direccionamiento IPV6 nativo. Este cambio ha sido coordinado con el proveedor de servicios Claro, y ha implicado la modificación de las configuraciones en los routers del operador Claro para reflejar las nuevas direcciones IPV6.

A la fecha, las sedes Ángel, Aguas (VLAN 21) y Barranquilla ya se encuentran operando con IPV6 nativo. El plan de direccionamiento adjunto detalla la correspondencia entre las direcciones IPV4 existentes y las nuevas direcciones IPV6 asignadas para cada una de las sedes.

En la siguiente tabla se muestra un ejemplo de Direccionamiento, sin embargo la tabla completa se puede consultar en el link [PLAN direccionamiento IPV6 ICETEX_NEW.xlsx](#):

NUMERAL	SEDE	VLAN	NOMBRE VLAN	Segmento IPv4	Gateway IPv4	Segmento IPv6 Propuesto	Gateway IPv6
3	Angel	6	LAN 6	10.255.3.0	10.255.3.1	2801:192::/64	2801:192::1
1	Aguas	6	LAN 6	10.255.0.0	10.255.0.1	2801:192::/64	2801:192::1
1	Aguas	21	LAN 21	10.255.21.0	10.255.21.1	2801:1E0::/64	2801:1E0::1
16	Barranquilla	6	LAN 6	10.255.15.0	10.255.15.1	2801:19F::/64	2801:19F::1

Tabla 7 Ejemplo de Direccionamiento IPv6

El área de Seguridad y Networking han venido trabajando en conjunto realizando las pruebas de implementación de IPv6 donde se han configurado las interfaces de MPLS de los firewalls de Aguas, Triara y Megacenter para la comunicación entre sedes a través de IPv6.

Se han ido configurando algunas sedes con este direccionamiento según cronograma entregado por el operador de Networking y donde el firewall se encarga del enrutamiento hacia la MPLS y por lo cual a las distintas sedes de la entidad. Se han realizado pruebas de acceso a aplicaciones Web de la Entidad sobre este protocolo haciendo uso de NAT64 ya que el portal web.icetex.gov.co como tiene aplicaciones web embebidas que no son compatibles con IPv6, se hace necesario recurrir a este tipo de NAT para lograr acceder a dichas aplicaciones, este NAT se realiza desde el firewall de Triara y este se encarga de convertir la petición de IPv6 a IPv4 comprensible para el WAF y la aplicación web en el servidor.

4.6 Gestión de Vulnerabilidades en Networking

A la fecha el equipo de Networking queda pendiente del resultado de un nuevo escaneo de vulnerabilidades para su atención.

4.7 CONCLUSIONES DEL SERVICIO DE CONECTIVIDAD

- ✓ 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 una disminución del 65%.
- ✓ Todos los casos fueron cerrados con notificación a los funcionarios del servicio operativo para casos abiertos con el proveedor y presenta una disminución del 30% con respecto al mes anterior.
- ✓ Se encuentran en proceso de instalación el canal de Quibdó Backup y Leticia principal.
- ✓ En señalética sólo falta que se entregue por parte del operador la correspondiente a Cali y se completaría al 100% de las sedes con Internet para la gente.
- ✓ Se continúa trabajando en el proyecto de IPV6 con un seguimiento semanal por parte del Icetex.

4.8 RECOMENDACIONES DEL SERVICIO DE CONECTIVIDAD

- ✓ De acuerdo con la normatividad vigente se recomienda realizar la renovación de equipos 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 agosto [ANS canales Agosto 2024.xlsx](#)

5 SERVICIOS CENTROS DE COMPUTO

5.1 Datacenter Principal

Para el mes de agosto 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 y el otro también se puede ubicar en la misma ruta del repositorio:

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

[Reporte Monitoreo ICETEX Agosto 2024-Sitescope.pdf](#)



REPORTES									
REPORTE USO CPU					REPORTE USO MEMORIA				
Last 30 days rounded to the day					Last 30 days rounded to the day				
HOSTNAME	CODIGO DE SERVICIO	MAX CPU USAGE	MIN CPU USAGE	AVG CPU USAGE	HOSTNAME	CODIGO DE SERVICIO	MAX MEMORY USAGE	MIN MEMORY USAGE	AVG MEMORY USAGE
bastion.localdom	INR0253	0.60%	0.20%	0.30%	bastion.localdom	INR0253	36.30%	34.80%	35.49%
cxvodacontg011	INR0278	75.80%	4.50%	8.39%	cxvodacontg011	INR0278	85.90%	84.70%	85.17%
cxvodaprodn011	INR0276	99.90%	9.50%	29.41%	cxvodaprodn011	INR0276	99.40%	88.20%	95.19%
cxvodaprodn021	INR0277	99.60%	11.60%	41.72%	cxvodaprodn021	INR0277	99.40%	89.30%	93.95%
icetexbogbalserv	INR0237	23.70%	8.50%	13.50%	icetexbogbalserv	INR0237	76.00%	13.70%	36.86%
icetexbogelastic	INR0239	92.40%	0.30%	1.00%	icetexbogelastic	INR0239	30.40%	28.40%	29.23%
icetexbogelastic	INR0240	1.50%	0.10%	0.21%	icetexbogelastic	INR0240	12.70%	11.70%	12.23%
icetexbogelastic	INR0241	92.80%	0.30%	0.93%	icetexbogelastic	INR0241	66.10%	61.60%	63.14%
icetexbogliferayr	INR0238	25.90%	0.20%	7.71%	icetexbogliferayr	INR0238	97.70%	27.10%	58.69%
icetexbogliferayr	INR0243	99.90%	1.00%	30.98%	icetexbogliferayr	INR0243	69.70%	4.10%	56.59%
icetexbogliferayr	INR0242	40.70%	0.50%	4.96%	icetexbogliferayr	INR0242	99.40%	10.50%	86.20%
icetexbogixdarur	INR0244	91.90%	1.50%	3.84%	icetexbogixdarur	INR0244	97.80%	83.30%	91.25%
icetexbogixdarur	INR0245	91.00%	1.00%	1.46%	icetexbogixdarur	INR0245	98.10%	96.80%	97.50%
icetexbogixdarur	INR0246	19.20%	0.80%	1.23%	icetexbogixdarur	INR0246	96.70%	34.00%	73.95%
icetexbogixorfeo	INR0233	4.70%	0.10%	0.32%	icetexbogixorfeo	INR0233	95.30%	47.60%	67.57%
icetexbogixorfeo	INR0262	47.30%	0.20%	0.50%	icetexbogixorfeo	INR0262	97.60%	73.50%	86.84%

Ilustración 1 Evidencia del Resumen del Monitoreo CPU-Memoria ELK

METRICAS MV

📅 Last 30 days rounded to the day

VM NAME	AVG VM CPU.USED.MHZ	MAX VM CPU.USED.MHZ	MIN VM CPU.USED.GHZ
INR0251_INFOTIC_OLD	2,396.29	5,005.00	1,607.00
INR0254_INFOTIC_OLD	960.58	7,094.00	413.00
INR0255_INFOTIC_OLD	2,094.89	9,184.00	826.00
INR0256_INFOTIC_OLD	1,658.65	8,541.00	528.00
INR0257_INFOTIC_OLD	1,094.46	6,727.00	436.00
INR0258_INFOTIC_OLD	1,893.32	3,099.00	1,239.00
INR0259_INFOTIC_OLD	2,137.91	4,316.00	1,216.00

📅 Last 30 days rounded to the day

VM NAME	AVG VM MEM.USED.%	MAX VM MEM.USED.%	MIN VM MEM.USED.%
INR0251_INFOTIC_OLD	38.65%	62.99%	18.99%
INR0254_INFOTIC_OLD	6.47%	24.00%	1.00%
INR0255_INFOTIC_OLD	16.83%	41.00%	3.00%
INR0256_INFOTIC_OLD	11.97%	36.00%	1.00%
INR0257_INFOTIC_OLD	7.88%	30.00%	1.00%
INR0258_INFOTIC_OLD	28.92%	61.00%	15.00%
INR0259_INFOTIC_OLD	30.44%	60.00%	12.00%

Ilustración 2 Evidencia del Resumen del Monitoreo CPU-Memoria servidores Openshift ELK

REPORTE USO DISCOS

📅 Last 30 days rounded to the day

HOSTNAME	CODIGO DE SERVICIO	FILESYSTEM	MAX DISK USAGE	MIN DISK USAGE	AVG DISK USAGE
bastion.locald	INR0253	/	88.90%	88.90%	88.90%
bastion.locald	INR0253	/boot	14.00%	14.00%	14.00%
bastion.locald	INR0253	/home	13.10%	13.10%	13.10%
cxvodacontg0	INR0278	/oracle	75.40%	75.30%	75.37%
cxvodacontg0	INR0278	/grid	68.30%	68.10%	68.24%
cxvodacontg0	INR0278	/opt	50.80%	45.50%	46.38%
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%
cxvodacontg0	INR0278	/var/log	6.60%	5.50%	6.03%
cxvodacontg0	INR0278	/	1.90%	1.90%	1.90%
cxvodaprodn0	INR0276	/grid	100.00%	0.00%	94.81%
cxvodaprodn0	INR0276	/oracle	90.80%	77.80%	82.86%
cxvodaprodn0	INR0276	/opt	87.50%	79.40%	79.91%
cxvodaprodn0	INR0276	/DATOS	60.30%	25.70%	54.04%
cxvodaprodn0	INR0276	/home	48.50%	48.10%	48.26%
cxvodaprodn0	INR0276	/var/crash	29.40%	29.40%	29.40%

Ilustración 3 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	100.00000000%
cxvodacontg011	100.00000000%
cxvodaprodn011	100.00000000%
cxvodaprodn021	100.00000000%
icetexbogbalserv1-r	100.00000000%
icetexbogelasticserver1	100.00000000%
icetexbogelasticserver2	100.00000000%
icetexbogelasticserver3	100.00000000%
icetexbogliferaynfs	100.00000000%
icetexbogliferayserver1	100.00000000%
icetexbogliferayserver2	100.00000000%
icetexboglxdarumasrv1	100.00000000%
icetexboglxdarumasrv2	100.00000000%
icetexboglxdarumatest	100.00000000%
icetexboglxorfeo1.localdomain	100.00000000%
icetexboglxorfeo2.localdomain	100.00000000%
icetexboglxroad3	100.00000000%
icetexosbognfs1	100.00000000%
icetexosbognfs2	100.00000000%

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

📅 Last 30 days rounded to the day

VM NAME	DISPONIBILIDAD
INR0251_INFOTIC_OLD	100.00%
INR0254_INFOTIC_OLD	100.00%
INR0255_INFOTIC_OLD	100.00%
INR0256_INFOTIC_OLD	100.00%
INR0257_INFOTIC_OLD	100.00%
INR0258_INFOTIC_OLD	100.00%
INR0259_INFOTIC_OLD	100.00%

Ilustración 5 Reporte ELK Promedio Disponibilidad servidores Open shift en Housing – Datacenter Principal

#	Cod Servicio	Hostname	Disponibilidad
1	INR0228	ictxisisgesbd	100%
2	INR0229	ictxisisgesapp	100%
3	INR0233	icetexboglxorfeo1	100%
4	INR0234	ictxprusisgapp	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	icetexboglxdarumatest	100%
14	INR0247	preprodsec-icetexboglxroad2n	100%
15	INR0248	icetexboglxroad3	100%
16	INR0249	xroadsec-icetexboglxroad1	99.99%
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	ictxbogsvrpt1	100%
26	INR0235	ictxbogsvrpt2	100%
27	INR0000322	ictxcontroldoc	0%
28	INR0226	mira	100%
29	INR0253	bastion	100%
30	INR251	OpenShift	100%
31	INR254	OpenShift	100%
32	INR255	OpenShift	100%

33	INR256	OpenShift	100%
34	INR257	OpenShift	100%
35	INR258	OpenShift	100%
36	INR259	OpenShift	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

El presente mes se elabora y envía al Icetex un documento que contiene la programación de mantenimiento que se han venido realizando este año en el data center de TRIARA sobre los siguientes elementos de la Infraestructura del proveedor:

1. Aries
2. UPS Emmerson
3. UPS Eaton
4. Cellwatch
5. Alber
6. Generadore

El detalle se puede ver en el siguiente link: [PLAN DE MANTENIMIENTOS DC TRIARA 2024-CRONOGRAMA.pdf](#)

5.1.2 Disponibilidad TRIARA para los servicios de página web

A continuación, se evidencia que la disponibilidad del Portal Web institucional web.icetex.gov.co, los cuales tuvieron un **UPTIME del [99,94%]** tal como se evidencia en la gráfica a continuación.

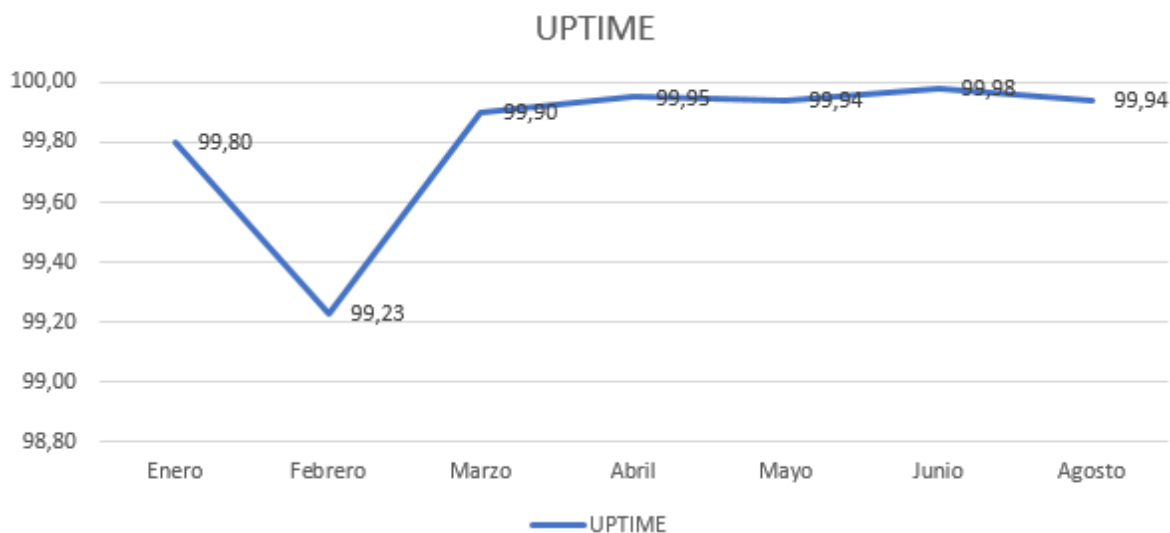


Ilustración 6 UPTIME: Portal WEB web.icetex.gov.co

Durante el mes de agosto 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 para este mes con un total de 438 mil usuarios, con 301 mil usuarios nuevos. El tiempo de interacción medio es de 2 minutos 25 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

Se viene trabajando con una mejora continua en la presentación de informes como en la atención del servicio procurando buscar soluciones de raíz a los temas que se presentan, lo cual generan valor al cliente haciendo que evidencie un aumento en la satisfacción en la prestación del servicio.

5.1.3 Análisis componente Liferay

Como parte de las actividades desarrolladas por el Web master se realiza una revisión de la infraestructura tecnológica y el entorno de software del portal Liferay, abordando aspectos fundamentales para su óptimo rendimiento y seguridad. Desde finales de mes pasado y en lo corrido del mes de agosto se realizó un análisis completo de los componentes principales del sistema, incluyendo la Memoria RAM, Procesador, y Disco Duro, que son esenciales para el funcionamiento del portal. Además, parches de seguridad instalados en Liferay, se evaluará el estado del File System para asegurar que su llenado no comprometa la operatividad del portal.

Adicional incluye un inventario de las librerías instaladas y los desarrollos implementados, se revisa la configuración del archivo portal-ext.properties, el cual es crucial para la personalización y ajuste de Liferay según los requisitos específicos de la organización.

Así como también el análisis del volumen de logs generados, un aspecto vital para el monitoreo y diagnóstico continuo del sistema, asegurando que se mantenga un rendimiento adecuado y se puedan identificar y resolver rápidamente cualquier problema que surja.

A continuación se presenta un cuadro con el resumen con los hallazgos y observaciones:

UNIDAD	HALLAZGO	OBSERVACIONES
MEMORIA RAM	Nodo 1 total de memoria RAM – 65.79 GB. Nodo 2 total de memoria RAM – 41.02 GB	Se solicita a ICETEX la autorización para disponer y configurar la memoria necesaria para que los dos nodos queden iguales.
SISTEMA OPERATIVO	La última versión del UPDATE del Sistema Operativo Red Hat Enterprise 7.2 , donde esta alojada el servidor de Liferay 7.3.10 GA1	Se coordinará con el operador tecnológico (Claro) para la actualización a la última versión del UPDATE del Sistema Operativo Red Hat Enterprise 7.2, donde está alojado el servidor de Liferay 7.3.10 GA1. Ya se creó el control de cambios 1039 que fue aprobado y está por ser ejecutarlo.
DISCO DURO	El espacio en disco utilizado por el CMS Liferay en el nodo 1 es 210 GB . El espacio disponible es de 166 GB. El espacio en disco utilizado por el CMS Liferay en el nodo 2 es 135 GB . El espacio disponible es de 243 GB.	No se está replicando la misma información en ambos nodos, el contenido de la carpeta 64G ./dtstaging/liferay Se procede a escalar con el proveedor LIFERAY para determinar si este archivo debe estar en ambos nodos y realizar las acciones que se indiquen
FILE SYSTEM	El espacio en disco utilizado por el CMS Liferay en el nodo 1 es 210 GB . El espacio en disco utilizado por el CMS Liferay en el nodo 2 es 135 GB .	
PARCHES DE SEGURIDAD	Nodo 1 - activation-key-dxpproduction-7.3-icetex-publicportal 40.xml activation-key-dxpproduction-7.3-	Se valido con el proveedor y confirma que el archivo en mención es la última versión

	icetex-publicportal - icetexbogliferayserver1.xml Nodo 2 - activation-key- dxpproduction-7.3-icetex-publicportal - icetexbogliferayserver2.xml	liberada y que cuenta con todo el soporte para el tema de los hotfixs . Caso #116639
VOLUMEN DE LOGS	Entre el registro histórico del nodo 1 y el nodo 2 , hay una diferencia de 21 días.	La diferencia se presenta por la situación presentada en el mes de diciembre del 2023.

Tabla 10 Resumen-Análisis componente Liferay agosto

Se puede visualizar el informe completo en el link: [Estado actual LIFERAY.pdf](#)

Durante el presente mes también además de atender la solicitud se entregó un informe indica las acciones ejecutada y el análisis de un reporte de lentitud en la página Web, el cual se puede ver mas a detalle en el siguiente link: [Informe página web.pdf](#)

5.1.4 Backup Servidores Triara

Durante el periodo de agosto 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 agosto 2024.pdf](#) donde se adjunta el reporte que se genera automáticamente desde la herramienta que se utiliza para realizar las copias.

Dentro de las actividades del proyecto de servicios tecnológicos para Icetex, se tiene la toma de copias de respaldo de la información creada, manipulada, reutilizada y procesada dentro de las diferentes actividades de la entidad la cual requiere para el desarrollo de sus actividades diarias, para lo cual se tiene como lineamiento principal la aplicación del anexo 22 donde se contempla las diferentes variables para la toma de backups.

Esta información debe ser trasladada a las cintas de Backup que Icetex entregara para proceder a la custodia externa de la información.

En la actualidad se cuenta con la custodia de 294 cintas de forma externa en las instalaciones de VISE, la información que contienen corresponde a la información historia entrega en custodia a partir del 23 de agosto del 2023.

A la fecha ICETEX continua con el pendiente de realizar la entrega de las cintas de Backup para realizar el almacenamiento y traslado a custodia externa, la información desde el año 2023 se encuentra en los equipos del operador de CLARO y **reiteramos ya no se tiene más espacio para continuar con este almacenamiento, por lo tanto se solicita al Icetex provea las cintas para realizar el proceso como se acordó contractualmente.**

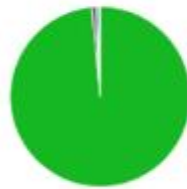
Backup job summary

Backup job summary report

Generated on: Sep 01, 2024 08:39 AM

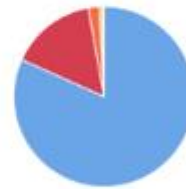
Server groups : BPODC
Servers : All
App types : All
Subclients : All
Job status : Running, Completed, Delayed, Failed, Killed, Completed with Errors, Completed with Warnings, Completed
Job Types : All
Time Frame : Last 4 weeks (Aug 4, 2024, 08:39:18 AM - Sep 1, 2024, 08:39:18 AM)
Time zone : Coordinated
Day Start Time : 12:00 AM
Snap and Backup Copy options : Snap and Backup Copy options
Advanced : None

Job status



Completed: 3861 (98.55%)
Killed: 26 (0.68%)
Partial Success: 22 (0.58%)
Failed: 6 (0.15%)
In Progress: 3 (0.08%)

Jobs by app type



Oracle RAC: 3204 (81.78%)
Virtual Center: 604 (15.42%)
Windows File System: 78 (1.99%)
Linux File System: 21 (0.54%)
SQL Server: 11 (0.28%)

Summary

Job status	Total Jobs	Size of Application	Media Size	Protected Objects	Failed Objects	Failed Folders
Completed	3861	148.65 TB	9.06 TB	105066226	6271	37
Killed	26	5.08 GB	0.00 BYTES	0	2	0
Partial Success	22	1.15 TB	19.92 GB	0	22	0
Failed	6	3.58 GB	0.00 BYTES	0	6	0
In Progress	3	507.38 GB	3.01 GB	0	3	0

1 - 5 of 5 items

Ilustración 8 Evidencia Backup Servidores

5.2 Datacenter Alterno

5.2.1 Hosting Virtual (IaaS)

En el transcurso del mes de agosto se mantuvieron en constante replicación las máquinas virtuales, 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 agosto 2024.pdf](#), el cual corresponde al último reporte diario del mes y refleja el consolidado de los informes que se están entregando periódicamente.

Site Recovery Manager - Estado Replicas INFOTIC

Actualmente el SRM (vcsatriara-ext.datacenterdhs.local -> vcmeagacenter.datacenterdhs.local) cuenta con 13 replicas

General					
Name			Count		
OK			13		
Grupo de protección: PG_INFOTIC_7 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0226_INFOTIC_REP	OK	5 of 5	Aug 31, 2024	7.58 MB	5 minutes
Grupo de protección: PG_INFOTIC_6 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0228_INFOTIC_REP	OK	1 of 1	Aug 31, 2024	34.23 MB	1 hour
INR0229_INFOTIC_REP	OK	1 of 1	Aug 31, 2024	62.91 MB	1 hour
Grupo de protección: PG_INFOTIC_1 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0233_INFOTIC_REP	OK	6 of 6	Aug 31, 2024	7.01 MB	30 minutes
INR0262_INFOTIC_REP	OK	1 of 1	Aug 31, 2024	14.3 MB	1 hour
Grupo de protección: PG_INFOTIC_5 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0236_INFOTIC_REP	OK	2 of 2	Aug 31, 2024	63.24 MB	2 hours
Grupo de protección: PG_INFOTIC_4 (4)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0237_INFOTIC_REP	OK	2 of 2	Aug 31, 2024	7.17 MB	5 minutes
INR0238_INFOTIC_REP	OK	2 of 2	Aug 31, 2024	23.8 MB	1 hour
INR0239_INFOTIC_REP	OK	2 of 2	Aug 31, 2024	14.61 MB	1 hour
INR0243_INFOTIC_REP	OK	2 of 2	Aug 31, 2024	25.46 MB	1 hour
Grupo de protección: PG_INFOTIC_3 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0244_INFOTIC_REP	OK	1 of 1	Aug 31, 2024	50.77 MB	1 hour
INR0245_INFOTIC_REP	OK	1 of 1	Aug 31, 2024	3.28 MB	5 minutes
Grupo de protección: PG_INFOTIC_2 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0249_INFOTIC_REP	OK	2 of 2	Aug 31, 2024	4.2 MB	5 minutes

Ilustración 9 Reportes de replicación SRM a Sitio Alterno, agosto 31 2024

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

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

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



#	INR Replicación	Host name	Servicio	Virtual Machine MEGACENTER
1	INR0204	icetexbogwsmira	Portal Web	INR0226_INFOTIC_REP
2	INR0207	ictxisgesbd	Sisgestion	INR0228_INFOTIC_REP
3	INR0206	ictxisgesapp	Sisgestion	INR0229_INFOTIC_REP
4	INR0220	icetexboglxorfeo1	ORFEO	INR0233_INFOTIC_REP
5	INR0219	icetexboglxorfeo2	ORFEO	INR0262_INFOTIC_REP
6	INR0208	ICTXBOGSRVPT1	Portal Transaccional	INR0236_INFOTIC_REP
7	INR0209	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 11 Servicios replicados – Datacenter MEGACENTER

Teniendo en cuenta que Icetex ha solicitado realizar la replicación de más máquinas virtuales, se realizó con el operador Claro el análisis del consumo tanto de CPU, memoria y disco duro de las máquinas virtuales replicadas frente a las acordadas según el Anexo #3 - Parte 6 Alterno IAS, encontrando que las 13 Máquinas virtuales que se están replicando tenemos:

- 9 máquinas que superaron la capacidad de Almacenamiento.
- 10 máquinas que superaron la capacidad de memoria.

En conclusión, 9 Máquinas Virtuales de las 13 replicadas en el Datacenter alterno están utilizando un almacenamiento mayor al aprovisionado inicialmente para cada uno de los servidores según el Anexo 3 y que las 13 máquinas virtuales replicadas están ocupando el **94.5%** de almacenamiento total definido en el Anexo #3 - Parte 6 Alterno IAS.

Almacenamiento Anexo #3 - Parte 6 Alterno IAS TB	Almacenamiento Utilizado actualmente TB	Diferencia (TB)	VM replicada
11.0	11.3	0.26	icetexboglxorfeo1.localdomain
0.3	0.3	0.01	icetexboglxorfeo2.localdomain
0.3	0.5	0.20	ICTXSISGESBD.icetex.local
0.1	0.2	0.08	xroadsec
0.3	0.9	0.59	icetexbogbalserv1-r
0.9	0.9	0.03	icetexbogliferayserver1
0.9	0.9	0.03	icetexbogelasticserver1
0.2	0.2	0.02	ICTXBOGSRVPT1.icetex.local
0.2	1.6	1.37	MIRA
14.3	16.9	2.6	

Tabla 12 Recursos-Datacenter Alterno Anexo #3. EC-Altern_o_IAS

El presente mes se elabora y envía al Ictex un documento que contiene la programación de mantenimiento que se han venido realizando este año en el data center de MEGACENTER sobre los siguientes elementos de la Infraestructura del proveedor:

- 1. Aries
- 2. UPS
- 3. Generadores

El detalle se puede ver en el siguiente link: [PLAN DE MANTENIMIENTOS DC MEGACENTER 2024-CRONOGRAMA.pdf](#)

5.2.2 Dataguard BBDD Megacenter

Durante el mes de agosto 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 DataGuard el cual garantiza una alta disponibilidad, protección de datos y recuperación ante desastres. Ver las evidencias en el documento [INFOTIC ICETEX - Evidencias Dataguard Megacenter Agosto.pdf](#)

```
oracle@cxvodacontg011:~$ ps -fealgrep pmon
grid      6046      1 0 Jul27 ?        00:06:03 asm_pmon +ASM
oracle    6341      1 0 Jul27 ?        00:14:52 ora_pmon ICTXCYCD
oracle    7047      1 0 Jul27 ?        00:13:19 ora_pmon ICETEXD
oracle    7343      1 0 Jul27 ?        00:13:31 ora_pmon APOTEOSD
oracle    7736      1 0 Jul27 ?        00:13:26 ora_pmon APOTNEWD
oracle    8246      1 0 Jul27 ?        00:07:20 ora_pmon VIGIADTG
oracle    8572      1 0 Jul27 ?        00:07:20 ora_pmon LANDICTD
oracle    9297      1 0 Jul27 ?        00:13:30 ora_pmon APLICATD
oracle    9681      1 0 Jul27 ?        00:07:19 ora_pmon LIFERAYD
oracle    15166 14847 0 11:09 pts/1    00:00:00 grep --color=auto pmon

[oracle@cxvodacontg011 ~]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.4.0 Production on Thu Sep 5 11:09:11 2024

Copyright (c) 1982, 2013, Oracle. All rights reserved.

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production
With the Partitioning, Automatic Storage Management, OLAP, Data Mining
and Real Application Testing options

SQL> sta faplyb.sql

  Thread Last Sequence Received Last Sequence Applied TIME_RECEIVED    TIME_APPLIED
-----
1          66619          66619 31/08/2024 10:20 31/08/2024 10:20
2          49937          49937 31/08/2024 10:14 31/08/2024 10:14

SQL> sta uapply

  Thread Last Sequence Received Last Sequence Applied Difference
-----
1          66619          66619          0
2          49937          49937          0

SQL>
```

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 31/08/2024 10:20 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 OnPremise en Icetex hacia el Datacenter alternativo Megacenter (Medellín).

Source SAN Array	Source Volume	Destination SAN Array	% Complete	Destination Volume	Type	State
Storage Center 35716 PRINCIPAL	DSDCP_MSOTC01	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_MSOTC01	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_QUORUM01	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_QUORUM01	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_TEMP01	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_TEMP01	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_AD01	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_AD01	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_MIRA	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_MIRA	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_DATA_02	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_DATA_02	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_INDICES01	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_INDICES01	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_QUORUM02	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_QUORUM02	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_QUORUM03	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_QUORUM03	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_LOGS_01	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_LOGS_01	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_CRM_VM02	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_CRM_VM02	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_DRTEST	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_DRTEST	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_SEAGATE	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_SEAGATE	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_SRVAPLIC01	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_SRVAPLIC01	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_SRVAPLIC02	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_SRVAPLIC02	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_SRVAPLIC03	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_SRVAPLIC03	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_APLI05	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_APLI05	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_APOTEOSYS	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_APOTEOSYS	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_CREDITO_CML...	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_CREDITO_CML_02	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_MISC04	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_MISC04	Asynchronous	Up
Storage Center 35716 PRINCIPAL	DSDCP_CRM_VM01	Storage Center 35804 ALTERNO	100%	Repl of DSDCP_CRM_VM01	Asynchronous	Up

Ilustración 11 Evidencia replicado servicios OnPremise Icetex a Megacenter

5.2.4 Disponibilidad de Servicios de Housing – Datacenter Alternativo

A continuación, se presentan las máquinas alojadas en el Datacenter alternativo en Medellín, las cuales estuvieron disponibles todo el mes de agosto 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 13 Disponibilidad de Servicios de Housing – Datacenter Alternativo

5.2.5 Servicios de DRP

Se continua con las sesiones semanales tanto internas (Infotex-Claro) como con el Icetex con el fin de coordinar y/o realizar las pruebas preliminares y ajustar el minutograma para la prueba definitiva, la cual aún no se tiene confirmada la fecha por parte de Icetex tentativamente sería para el mes de octubre.

En el mes del presente informen se han realizado al Ictetex las siguientes solicitudes y requerimientos:

- Solicitud de aprobación de la cotización del traslado del WAF físico del Datacenter Triara al Datacenter alternativo Megacenter.
- Solicitud de aprobación de la cotización de la configuración de WAF Virtual.
- Se dio respuesta y se presentaron las observaciones al correo remitido con el objeto y el alcance del DRP del segundo semestre del 2024.

A nivel de documentación se entregó el Informe que se puede encontrar en el siguiente link: [Informe prueba pre test.pdf](#)

6 SEGURIDAD

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

6.1 Servicios de Endpoint

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

Para el despliegue de Web Filter de Sophos, se solicita por parte de infraestructura de ICETEX realizar un informe de cómo va el proceso de implementación de esta característica, donde se indican las pruebas realizadas y los perfiles que se tienen configurados actualmente en el firewall de Triara y como estos pueden ser homologados en el control web de la consola de Sophos y el cual ya fue entregado para su validación.

Se continua a la espera de la sesión con el área de riesgos e infraestructura Ictetex para socializar este comparativo y decidir cómo se hará la implementación en base a las pruebas realizadas y sobre esto se recomienda realizarlo segmentado por áreas para controlar accesos y las respectivas excepciones.

Se informó oportunamente a Ictetex que en la gestión de la consola de antivirus Sophos, presenta una notificación de caducidad de la licencia de **Mayor compatibilidad con Windows**, la cual caducó el pasado **30 de agosto de 2024**. Esta licencia permite la compatibilidad con versiones del sistema operativo Windows (Server 2008, 2012, Windows 7 y Windows 8, etc.) con el agente de antivirus de Sophos. De no renovarse este licenciamiento, se puede presentar incompatibilidad y falta de elementos de protección que brinda el agente Sophos a estos sistemas operativos y que representaría una brecha de seguridad importante.

Durante este mes se realizó la actualización del firmware de los equipos de seguridad perimetral FortiGate, FortiWeb y FortiManager. Esta actividad se realiza como parte de los mantenimientos preventivos sobre estos equipos y adicionalmente para prevenir la vulnerabilidad reportada CVE-2024-36505 y la cual afectaba la versión anterior de los dispositivos. Se dejan en las versiones más estables y actuales que reciben todos los componentes de servicio y actualización de UTM por FortiGuard y no presenta inconvenientes con ninguno de los componentes y configuraciones actuales en los equipos de la entidad, al igual que como se indica, esta versión del Firmware no es afectada por la vulnerabilidad CVE-2024-36505. Se efectuaron las respectivas pruebas de funcionamiento de todos los servicios de la organización y se encuentran en funcionamiento correcto.

6.2 ESTADÍSTICAS PORTALES

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

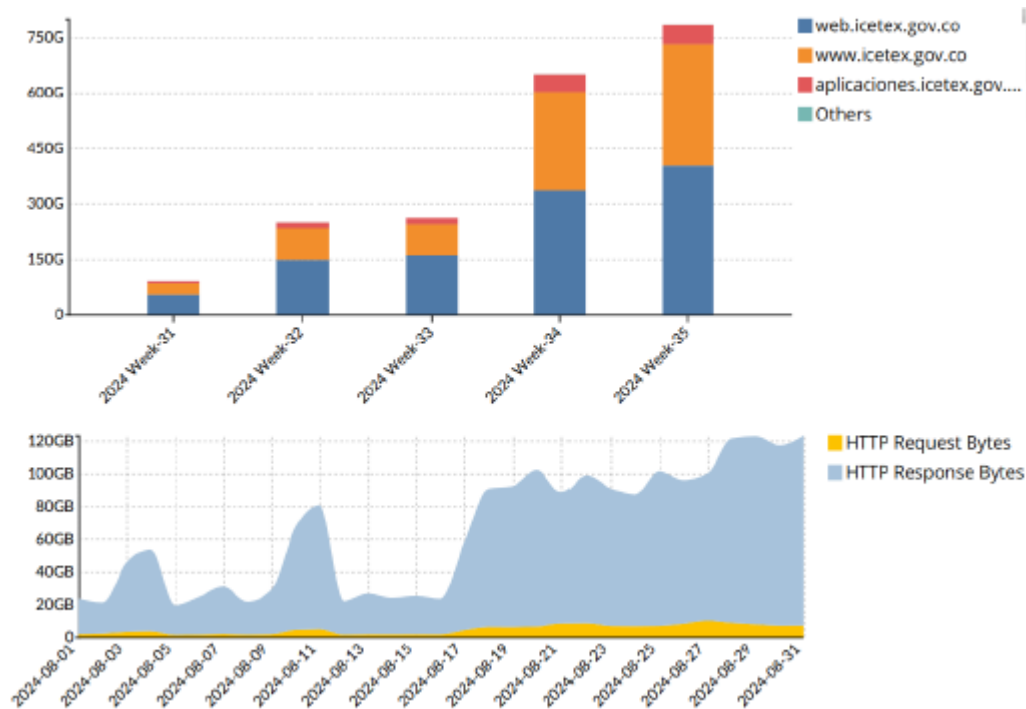


Ilustración 12 Evidencia Gráfica Estadísticas de Portales

En el periodo de tiempo analizado se presenta un promedio de 750 GB de tráfico general hacia los portales FortiWeb Apps Nuevas donde el portal de web.icetex.gov.co y www.icetex.gov.co fueron los más consultados sobre todo en la semana 35 (25 de agosto a 31 de agosto de 2024), lo cual es un comportamiento normal para este tipo de transacciones de acuerdo con la actividad de los usuarios y las convocatorias vigentes.

6.3 Estado General de las Plataformas

Se elabora y entrega a Icetex un Informe que contiene información relevante para evidenciar el estado actual de las plataformas de seguridad perimetral de la entidad conforme a los compromisos adquiridos en el contrato entre las partes, el cual se puede consultar en el link: [Estado de Infraestructura Seguridad ICETEX.pdf](#)

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

System Information	
Hostname	DC_FG_SLV_ICETEX
Serial Number	FG180FTK22901182 
Firmware	v7.2.9 build1688 (Mature)
Mode	NAT
System Time	2024/09/02 11:27:39
Uptime	15:13:35:05
WAN IP	 2801:192:0:dd::8c

Ilustración 13 Estado General de las Plataformas- Seguridad-Perimetral-DC_Principal (FortiGate-Triara)

System

Hostname	DCAGUAS_FG_MST_ICETEX
Serial Number	FG6H0FTB22902021 
Firmware	v7.2.9 build1688 (Mature)
Mode	NAT
System Time	2024/09/02 11:40:44
Uptime	15:14:00:32
WAN IP	 2801:192:0:dd::8c

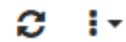
Ilustración 14 Estado General de las Plataformas- Seguridad-Perimetral-DC-Alterno-(FortiGate-Aguas)

System Information

Hostname	DCB_FG_MST_ICETEX
Serial Number	FG6H0FTB22902086 
Firmware	v7.2.9 build1688 (Mature)
Mode	NAT
System Time	2024/09/02 11:42:39
Uptime	15:13:24:55
WAN IP	 190.145.153.186

Ilustración 15 Estado General de las Plataformas- Seguridad-Perimetral- DC-Alterno-(FortiGate-Megacenter)

System Information



HA Status	Standalone
Host Name	FortiWeb_ICETEX
Serial Number	FV-2KFTE21000029
Operation Mode	Reverse Proxy
System Time	Mon Sep 2 11:44:05 2024
Firmware Version	FortiWeb-2000F 7.4.4,build0649(GA),240628
System Uptime	[15 day(s) 13 hour(s) 6 min(s)]
Administrative Domain	 Disabled
Threat Analytics 	Start Trial
Advanced Bot Protection 	 Disabled

Ilustración 16 Estado General de las Plataformas WAF-(FortiWeb_Triara_APPS_Nuevas)

System Information



HA Status	Active-Passive
Cluster Name	Icetex
Cluster Members	ICTX_FORTIWEB1/ FV-2KE3117000046 (Primary) ICTX_FORTIWEB2/ FV-2KE3117000032 (Secondary)
Serial Number	FV-2KE3117000046
Operation Mode	Reverse Proxy
System Time	Mon Sep 2 11:45:24 2024
Firmware Version	FortiWeb-2000E 7.4.4,build0649(GA),240628
System Uptime	[15 day(s) 12 hour(s) 51 min(s)]
Administrative Domain	Disabled

[Threat Analytics](#)

Start Trial

Ilustración 17 Estado General de las Plataformas WAF-(FortiWeb-Triara-APPs_Viejas)

System Information			
Unit Type	Standalone		
Host Name	fsa.icetex.gov.co [Change]		
Serial Number	FSA1KD3A17000156		
System Time	Mon Sep 2 11:46:55 2024 -05 [Change]		
Firmware Version	v3.2.4,build0279 (GA) [All firmwares 👁]		
System Configuration	Last Backup: 2024-03-07 21:04 [Backup/Restore]		
Current User	jairo.acevedo		
Uptime	178 day(s) 14 hour(s) 7 minute(s)		
Windows VM	✓ [Upload License]		
Microsoft Office	✓ [Upload License]		
VM Internet Access	✓		
FDN Download Server	✓		
Community Cloud Server	✓		
Web Filtering Server	✓		

Ilustración 18 Estado General de las Plataformas seguridad-Local-(FortiSandBox)

6.4 Estado de Salud de los Equipos de Seguridad

En el transcurso del mes de agosto 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 **16. ESTADO DE SALUD DE LOS EQUIPOS-TRAFICO Y SESIONES** del documento [Reporte Agosto seguridad 2024.pdf](#)

16. ESTADO DE SALUD DE LOS EQUIPOS-TRAFICO Y SESIONES

16.1. FIREWALL AGUAS

Se observa el tráfico hacia la MPLS de la sede de Aguas con un promedio de 43.51Mbps (Port7) en la última semana.

Imagen 12 Consumo Del Canal

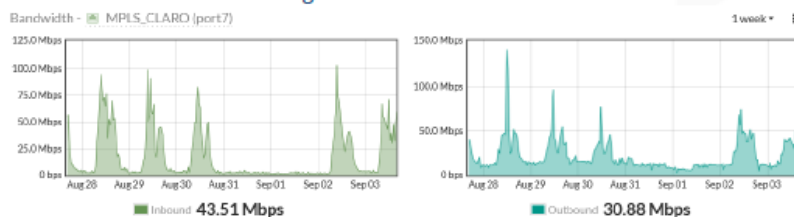


Ilustración 19 Evidencia Estado de Salud de los Equipos de Seguridad

6.5 Servicio de centro de Operaciones de Seguridad (SOC)

Durante el mes de agosto 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 Agosto 2024.pdf](#)

TLP:ROJO		INFORME MENSUAL MONITOREO SOC	Página	7 de 66
----------	--	-------------------------------	--------	---------

3.1.1 Casos de Uso Seguridad

Se encuentran definidas 2.429 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.

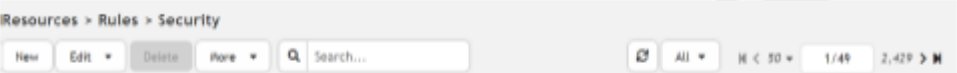


Ilustración: Cantidad de reglas de seguridad

3.1.2 Casos de Uso Disponibilidad

Para los casos de uso de disponibilidad se cuenta con 168 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.

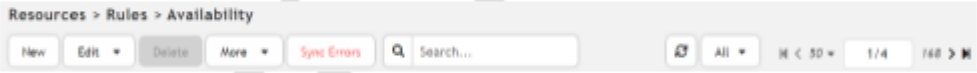


Ilustración: Cantidad de reglas de Disponibilidad

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.

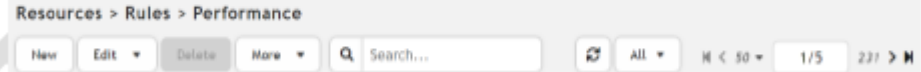


Ilustración: Cantidad de reglas de Rendimiento

3.1.4 Casos de Uso Cambio

De las reglas de Cambios, se han especificado 114 reglas, que se encarga de identificar cambios, alteraciones o variaciones en el estado de usuarios, agentes, dispositivos, entre otros miembros de la entidad.



Ilustración: Cantidad de reglas de Cambio

Ilustración 20 Evidencia Imagen Reporte Monitoreo

6.5.1 Monitoreo de Marca-Estrategia OSINT-SOC

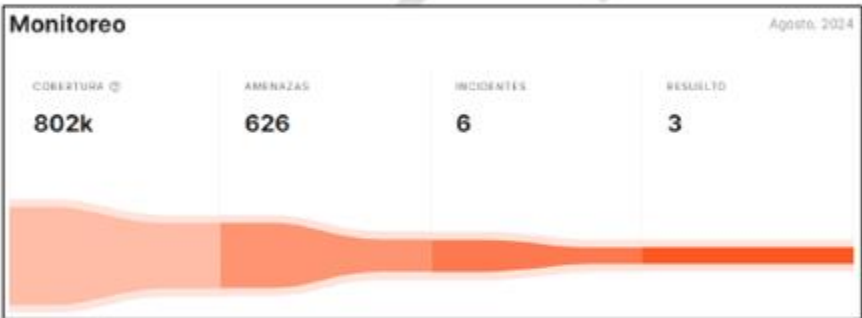
Para el mes de agosto y de acuerdo con lo programado se continuó con el monitoreo de marca, donde se implementó la estrategia OSINT(Open Source Intelligence), como técnicas y herramientas que permitan recopilar información pública, analizar los datos y correlacionarlos convirtiéndolos en conocimiento 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 [Informe Mensual MARCA-OSINT ICETEX Agosto 2024.pdf](#)

4. 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 626 posibles amenazas de las 802k que fueron encontradas y analizadas automáticamente por la plataforma de monitoreo. A estas 626 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 21 Evidencia Imagen Reporte Monitoreo OSINT

Durante el periodo evaluado se detectaron 06 incidentes, 02 relacionados con otros datos confidenciales, 02 relacionados con perfil falso en red social y 02 relacionados con Phishing.

6.5.1.1 Casos relacionados con Fraudes Digitales

Durante el periodo evaluado, se presentaron 52 casos, de los cuales 50 fueron cerrados, teniendo en cuenta que algunos no tenían relación y otros solo hacían mención a la entidad y 02 casos se reportaron a la entidad y se encuentran resueltos.

6.5.1.2 **Casos relacionados con Fuga de Datos**

Durante el periodo evaluado, se presentaron 56 casos, de los cuales 54 fueron cerrados, teniendo en cuenta que algunos no tenían relación con la entidad o solo se hacía mención de la misma y 02 casos están en tratamiento.

6.5.1.3 **Casos relacionados con el módulo Piratería Online**

Durante el periodo evaluado, se presentaron 502 casos, de los cuales todos fueron cerrados, teniendo en cuenta que eran casos relacionados con producto falso o venta irregular y solo se hacía mención del nombre de la marca, pero ésta no tenía relación con la entidad ya que "ICETEX" corresponde al nombre de una marca de colchones y la plataforma lo asocia con el de la entidad, por lo tanto, todos los casos fueron descartados y cerrados.

6.5.1.4 **Casos relacionados con el módulo Deep & Dark Web**

Durante el periodo evaluado, se presentó 15 casos relacionados con la Deep & Dark Web, los cuales fueron cerrados ya que están relacionados con los casos de la plataforma Russian Market en el que ya se realizó una investigación sobre estas detecciones.

6.5.1.5 **Casos Reportados a la entidad**

Durante el periodo evaluado se reportó 05 casos a la entidad, de los cuales 04 se le solicitaron takedown, al día de hoy se solucionaron 03 casos, 01 están en curso y 01 caso se encuentra en espera de retroalimentación por parte de la entidad y está en tratamiento.

Par ver la información más detallada de cada uno puede remitirse al siguiente link: [Informe Mensual MARCA-OSINT ICETEX Agosto 2024.pdf](#)

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% según los reportes entregados por el SOC y amenazas detectadas en fuentes de información confiable.
- Se realiza la protección de puntos finales y servidores con la herramienta de AV Sophos.
- Se ha venido trabajando en la implementación de direccionamiento IPv6 apoyando al área de Networking en esta actividad.
- Se realiza la restricción de la conexión VPN-SSL a países no autorizados y se han bloqueado intentos de acceso a puertos que se muestran sobre el direccionamiento IPv4 publico incluyendo puertos como BGP, VPN IPSec, etc. Desde direcciones IP con reputación maliciosa.

6.7 RECOMENDACIONES

6.7.1 Recomendaciones Generales

- ✓ Con respecto a la gestión que se ha venido realizando, se recomienda continuar con las validaciones y retroalimentación para cierres de casos, con el fin de mitigar las brechas de seguridad detectadas a través de la plataforma de monitoreo de protección de marca y OSINT.
- ✓ Con respecto a los casos de Fraudes Digitales – Perfil Falso en Red Social recordar las medidas a considerar:
 - Validar si el perfil en mención es considerado un fraude para la entidad, en el caso que así sea, se deberá solicitar el takedown de los sitios. (Cabe aclar que ya se completaron el total de Takedown del paquete contratado, si se solicitan más takedown éstos tendrán un costo adicional)
 - En el caso que no se considere un fraude para la entidad responder este correo y se procederá a cerrar el caso como Resuelto.
- ✓ Con respecto a los casos de Fuga de Datos – otros datos confidenciales recordar las medidas a considerar:
 - Validar si el documento en mención es de carácter privado o confidencial, en el caso que así sea, se deberá solicitar el takedown de este sitio.
 - En el caso que sean de carácter público se procederá a cerrar el caso como Resuelto.
 - Es importante recomendar a nivel general a todos los funcionarios de la entidad la importancia de la protección de datos personales y corporativos, con sus respectivas implicaciones que puede tener la exposición de estos datos en Internet.
- ✓ Verificar 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 denegado o permitido el tráfico.
- ✓ Realizar bloqueo de las direcciones IP origen o destinos identificadas como maliciosas en indicadores de compromisos- IoC.
- ✓ 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.
- ✓ 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.	Al depurar las políticas en los firewalls, se ha venido analizando el tráfico que pasa sobre las políticas con origen, destino, puertos en ALL y en base a este análisis se ha ido alineando estas políticas para permitir solo el tráfico necesario y cerrar brechas de seguridad asociadas a esta configuración.	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. A nivel de la consola de Antivirus y en base a las pruebas que se han realizado, se está a la espera de exponer los resultados y que ICETEX tome la decisión en cuanto a cómo se implementara estos perfiles de Web Filter.	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. En este momento se tiene una integración entre las plataformas para captura de logs sobre las API de Sophos y los eventos que este reporta y se visualizan correctamente en el 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 14 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.	Como parte de las pruebas de IPv6, se están realizando pruebas de DHCPv6 en la red para que el servidor entregue direccionamiento IPv6 a las redes de la Entidad y que esta segmentación cumpla los estándares del protocolo IPv6.	Media
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 configurar usuarios y claves dentro de las	En evaluación por parte de ICETEX.	Alta

aplicaciones de ICETEX		
Validar a nivel de punto final los equipos que se han visto involucrados con comportamiento malicioso.	Se evalúa por parte de ICETEX. Se hace seguimiento por parte del SOC quien reporta comportamiento malicioso. Sin embargo es necesario establecer políticas de conexión de equipos externos BYOD debido a que muchos de los casos reportados por el SOC vienen de equipos personales que no hacen parte de la Entidad.	Critica
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
Adquirir un equipo Firewall para correo para prevenir brechas de seguridad asociadas al uso del correo electrónico y que este es susceptible a muchos tipos de amenazas.	En evaluación por parte de ICETEX.	Alta
Evaluar los riesgos sobre las plataformas en la nube y considerar aplicar plataformas de seguridad para los ambientes cloud que cuenta la entidad ya que estos contienen servicios críticos para la misma.	En evaluación por parte de ICETEX.	Alta

Tabla 15 Recomendaciones de seguridad para Icetex

6.8 CONCLUSIONES

- ✓ Realizar actualización del firmware en los dispositivos de seguridad perimetral, previene vulnerabilidades nuevas que puedan afectar la seguridad e integridad de la información de la entidad, actualizando a las versiones más recientes y estables que ofrece el fabricante.
- ✓ La gestión adecuada de credenciales de usuario reduce el riesgo de eventos críticos en la seguridad de la infraestructura, garantizando autenticación segura y control adecuado de los privilegios de acceso.
- ✓ Las herramientas de monitoreo optimizan la detección y respuesta ante eventos anómalos o maliciosos, mejorando la capacidad de identificación temprana y reduciendo los tiempos de respuesta ante incidentes de seguridad.
- ✓ Los reportes del SOC han permitido reducir los vectores de ataque. La detección oportuna de eventos anómalos ha facilitado el bloqueo de posibles amenazas, protegiendo la infraestructura de la Entidad.
- ✓ La implementación de políticas para BYOD (Bring Your Own Device) mejora la seguridad al integrar dispositivos personales de manera segura en el entorno corporativo, lo que ayuda a mitigar riesgos como la pérdida de datos, accesos no autorizados y vulnerabilidades derivadas de la diversidad de dispositivos.
- ✓ Implementar FSSO es esencial para controlar la navegación por áreas y reducir los riesgos de acceso a sitios que puedan representar amenazas para la infraestructura y los usuarios de la Entidad.
- ✓ La aplicación de controles adicionales de acceso contribuye a mitigar riesgos en incidentes de seguridad, fortaleciendo la seguridad de la Entidad frente a posibles amenazas.
- ✓ La depuración de políticas permite gestionar el tráfico hacia los equipos de seguridad perimetral de forma eficiente, controlando el acceso solo a los segmentos de red y puertos necesarios para la operación.

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 agosto, 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 AGOSTO.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 puede consultar en el [INFORME MENSUAL AGOSTO.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 en Barranquilla, Bogotá, Bucaramanga, Cali y Medellín:

ÍTEM	SERVICIO	CIUDAD	DIRECCIÓN	CANTIDAD
1	Sala de video conferencia o sala virtual (Tamaño 65")	Bogotá - Aguas	Carrera 3 No. 18-32	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 16 Distribución módulos de videoconferencia por sede

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

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

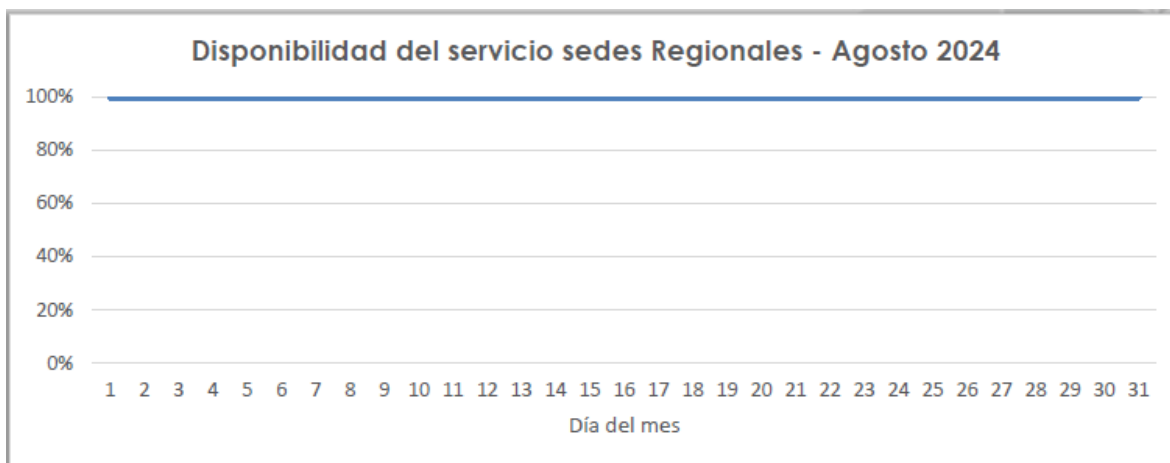


Ilustración 22 Disponibilidad de servicio videoconferencia sedes regionales – agosto 2024

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

En la verificación realizada en el mes de agosto del 2024 sobre la solución de videoconferencia distribuida en la ciudad de Bogotá, sedes Aguas y Ángel, la solución completa presentó una disponibilidad del 100% 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.

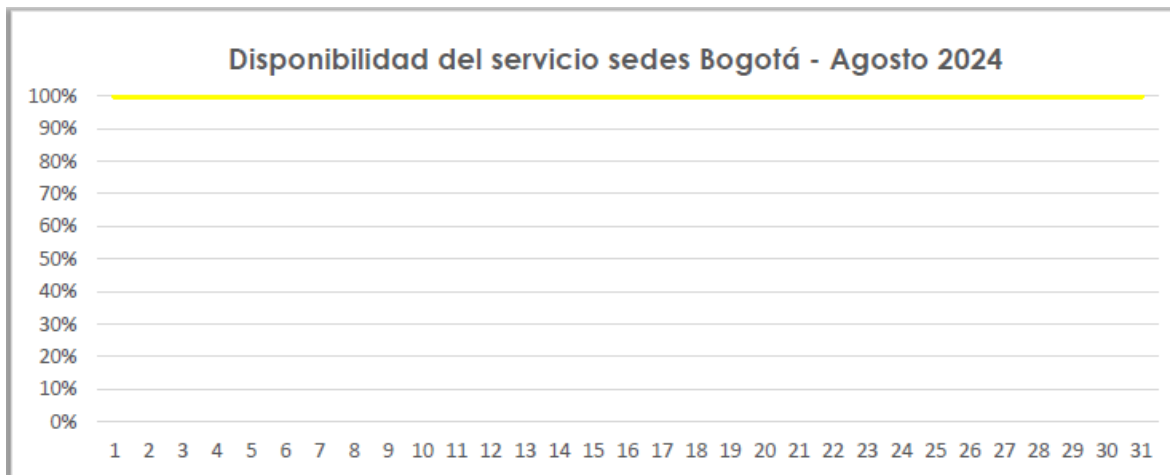


Ilustración 23 Disponibilidad de servicio videoconferencia sedes Bogotá –agosto 2024

8.2 Gestión de incidencias y requerimientos – sedes regionales

Para el periodo comprendido entre el 1 y el 31 de agosto, en las sedes Regionales no se generaron solicitudes especiales que requirieran atención y gestión de soporte técnico; Tampoco se reportaron incidencias a nivel del servicio para estas sedes durante el periodo, sin embargo, se contó con la disponibilidad para recibir cualquier solicitud de soporte (Incidencia/requerimiento) o apoyo concerniente a la solución de videoconferencia desplegada.

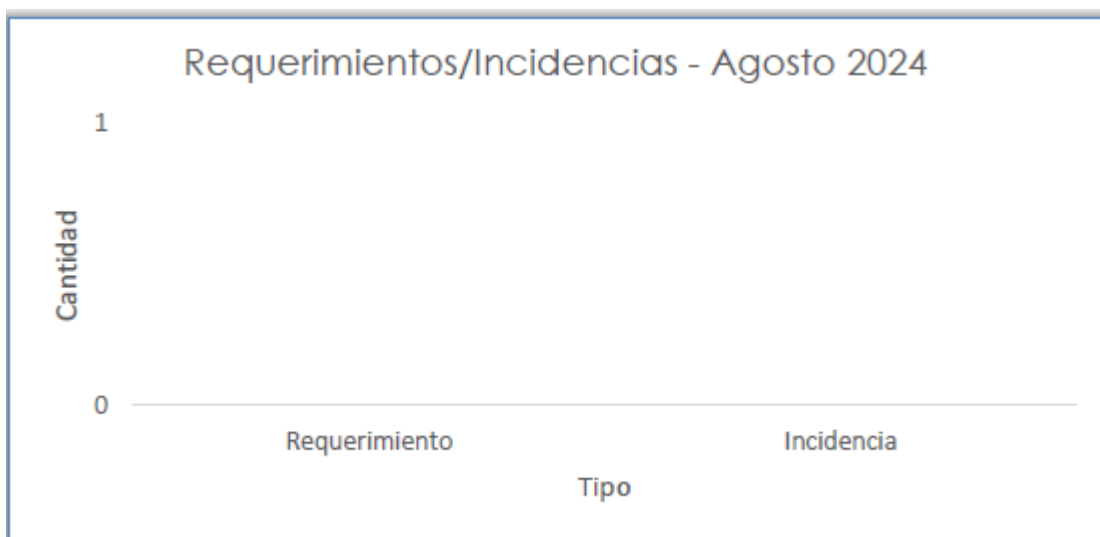


Ilustración 24 Incidencias/Requerimientos sedes Regionales – agosto 2024

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

Para el periodo comprendido entre el 1 y el 31 de agosto, para las sedes de Bogotá Aguas y Ángel, no se generaron solicitudes especiales que requirieran gestión y atención del soporte técnico; tampoco fueron reportadas incidencias a nivel del servicio para estas sedes durante el mes del presente informe, no obstante, como en los periodos anteriores, se contó con la disponibilidad para recibir cualquier requerimiento de soporte o solicitud de apoyo en lo concerniente a la solución de videoconferencia desplegada.

Se realiza la visita periódica de rutina a la sede de Aguas y Ángel, con la persona que está realizando apoyo técnico para revisión de los equipos, con el fin de validar el funcionamiento, realizar ajustes o revisiones requeridas y descartar incidencias de los módulos para garantizar continuidad del servicio, sin embargo, no se reportaron novedades y los módulos se encuentran funcionando de manera correcta y con la regularidad requerida. La solicitud de ingreso para la visita se realizó mediante el caso RF-278846-8-20156.



Ilustración 25 Evidencia primera visita módulo funcional sede Aguas 65", piso 2 – agosto 2024

En el módulo del piso 4, se realiza una prueba de funcionamiento de la OPS Backup con la que se cuenta para garantizar continuidad del servicio cuando se presenten contingencias o incidentes en el servicio de alguno de ellos módulos desplegados.



Ilustración 26 Prueba de funcionamiento OPS Backup módulo 65" sede Aguas, piso 4 – agosto 2024

Posterior a la prueba realizada, se deja funcional el módulo con la OPS original como se evidencia en la imagen No. 27, y se verifica funcionamiento del módulo móvil que se encuentra en el piso 6 (Ilustración 28).

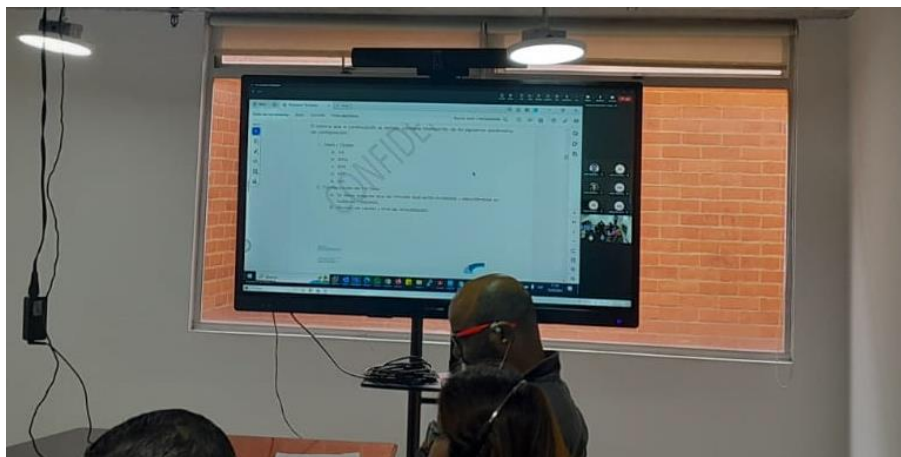


Ilustración 27 Módulo sede Aguas piso 4 – agosto 2024



Ilustración 28 Verificación sede Aguas, piso 6 (módulo móvil) agosto 2024

Por último, se realiza la revisión del módulo instalado en “Presidencia”, piso 8, que se encuentra funcional y el que se encuentra en la sede de Ángel como se muestra en las siguientes imágenes.

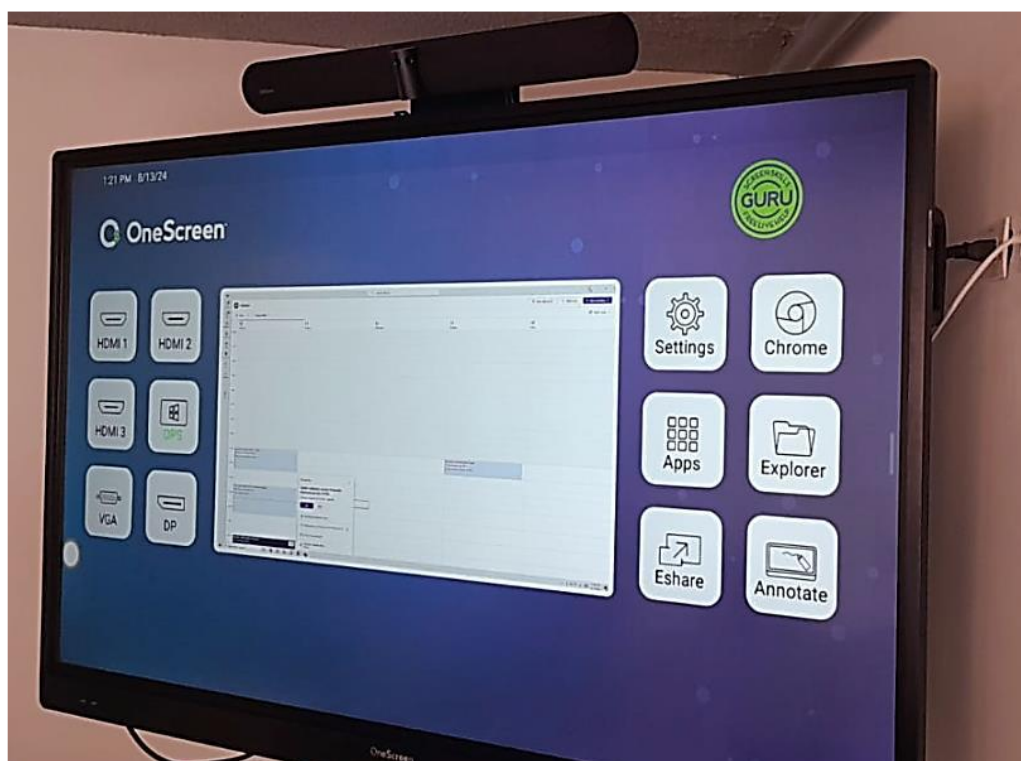


Ilustración 29 Verificación sede Aguas, piso 8 - agosto 2024

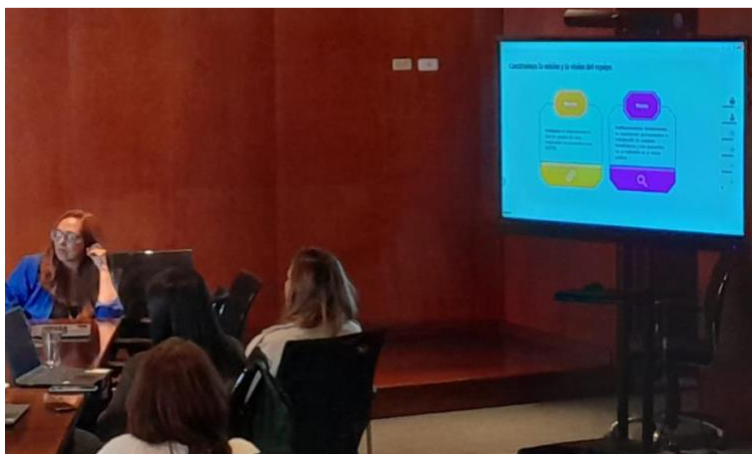


Ilustración 30 Verificación módulo sede Ángel - agosto 2024

Durante el mes de agosto 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.

- ✓ Durante el periodo comprendido entre 1 y 31 de agosto 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 cuenta con disponibilidad continua para atender todas solicitudes de soporte técnico para estas plataformas y apoyo que sea requerido.

Las evidencias se pueden encontrar en el siguiente [Informe Agosto 2024 Servicio Video Conferencia.pdf](#)

9 CALCULO DE CONCILIACIÓN DE LOS SERVICIOS DEL MES DE AGOSTO

A la fecha la conciliación del mes de Agosto con ICETEX se encuentra en proceso, el detalle de conciliación del mes anterior se puede ver en el siguiente link [Conciliación Agosto 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					\$ 10,685,370,451
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
				\$ 624.431.841,60	
Pago No. 5 -	mes:	Agosto	de	2023	\$ 650.825.466,00

<i>Pago No. 6</i> - mes: Septiembre de 2023	\$ 661.959.450,00
<i>Pago No. 7</i> - mes: Octubre de 2023	\$ 641.792.285,00
<i>Pago No. 8</i> - mes: Noviembre de 2023	\$ 630.348.564,00
<i>Pago No. 9</i> - mes: Diciembre de 2023	\$ 663.076.196,00
<i>Pago No. 10</i> - mes: Enero de 2024	\$ 681.934.328,00
<i>Pago No. 11</i> - mes: Febrero de 2024	\$ 732.950.101,55
<i>Pago No. 12</i> - mes: marzo de 2024	\$ 733.890.372,09
<i>Pago No. 13</i> - mes: Abril de 2024	\$ 730.351.368,00
<i>Pago No. 14</i> - mes: Mayo de 2024	\$ 719.104.204,57
<i>Pendiente Pago No. 15</i> - mes: Junio de 2024	\$ 746.025.308,88
<i>Pendiente Pago No. 16</i> - mes: Julio de 2024	\$ 790.507.369,22
VALOR CAUSADO QUE NO SE HA PAGADO (<i>valor a pagar factura</i>) *	\$ 790,462,899.80
VALOR TOTAL EJECUTADO (<i>valor pagado + valor causado no pagado</i>)	\$ 11,475,833,351
SALDO DEL CONTRATO (<i>valor total del contrato – valor total ejecutado</i>)	\$ 19,923,163,507
PORCENTAJE DE EJECUCIÓN	36.55%
* 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 17 Ejecución Presupuestal