

**INFORME DE ACTIVIDADES
DEL CONTRATO**

**CONTRATO NUMERO 2022-
0792**

Septiembre 01 al 30 de 2024

CONTENIDO

Contenido

1	OBJETIVOS	7
2	RESUMEN EJECUTIVO	7
3	SERVICIOS DE CONECTIVIDAD	10
3.1	Internet Para La Gente.....	13
3.2	Canales SDWAN.....	14
3.3	Canal de Replicación (Triara – Megacenter).....	15
3.4	Señal Ética (Internet Para La Gente)	15
3.5	Continuidad a La Integración Con El Protocolo IPV6.....	16
3.5	Gestión de Vulnerabilidades en Networking	17
3.6	Conclusiones Del Servicio De Conectividad.....	17
4	SERVICIOS CENTROS DE COMPUTO.	18
4.1	Datacenter Principal	18
4.1.1	Disponibilidad de Servicios – Datacenter Principal.....	20
4.1.2	Disponibilidad TRIARA para los servicios de página web.....	22
4.1.3	Análisis componente Liferay Producción.....	23
4.1.4	Ambiente De Pruebas Liferay -ICETEX	24
4.1.5	Backup Servidores Triara	27
4.2	Datacenter Alterno	29
4.2.1	Hosting Virtual (IaaS)	29
4.2.2	Dataguard BBDD Megacenter.....	32
4.2.3	Replicación Servicios OnPremise de ICETEX a Megacenter	33
4.2.4	Disponibilidad de Servicios de Housing – Datacenter Alterno	34
4.2.5	Servicios de DRP.....	34
5	SEGURIDAD	35
5.1	Servicios de Endpoint	35
5.2	Estadísticas Portales	36
5.3	Estado General de las Plataformas.....	37
5.4	Estado de Salud de los Equipos de Seguridad	40
5.5	Servicio de centro de Operaciones de Seguridad (SOC)	40
5.5.1	Monitoreo de Marca-Estrategia OSINT-SOC.....	41
5.6	Eventos Relevantes.....	43
5.7	Recomendaciones.....	44
5.7.1	Recomendaciones Generales	44
5.7.2	Recomendaciones Específicas.....	45
5.8	Conclusiones.....	46
6	GESTION DE SERVICIO.....	47
6.1	Actividades De Operación	48
6.2	Profesionales Especializados.	48
6.2.1	Especialista en Base de Datos DBA	48

6.2.2	Especialista Web Master	49
6.2.3	Administrador de Soluciones	49
6.2.4	Especialista en Networking	49
6.2.5	Especialista Integrador De Nube.....	49
6.2.6	Especialista En Seguridad.....	50
7	SERVICIO DE COLABORACIÓN	50
7.1	<i>Disponibilidad Del Servicio – Sedes Bogotá (Aguas - Ángel).....</i>	51
7.2	<i>Gestión De Incidencias Y Requerimientos – Sedes Regionales</i>	51
7.3	<i>Gestión De Incidencias Y Requerimientos – Bogotá (Aguas - Ángel).....</i>	52
7.4	<i>Proyección Plan De Mantenimiento Módulos De Videoconferencia Vigencia 2025</i>	55
8	Cálculo De Conciliación De Los Servicios Del Mes De Septiembre	57
9	RECOMENDACIONES	58
10	CONCLUSIONES GENERALES.....	61
11	PLAN DE TRABAJO PROXIMO MES.....	62

INDICE DE TABLAS

Tabla 1 Disponibilidad de canales	12
Tabla 2 Canales instalados	12
Tabla 3 Canales pendientes por instalar o en proceso de instalación	12
Tabla 4 Canales pruebas de saturación ejecutadas hasta septiembre	13
Tabla 5 Canales pendientes por ampliar corte septiembre	13
Tabla 6 Disponibilidad canales “Internet para la gente”	14
Tabla 7 Disponibilidad canales “SDWAN”	14
Tabla 8 Estado de la instalación de la señal ética de Wifi	16
Tabla 9 Ejemplo de Direccionamiento IPv6.....	17
Tabla 10 Evidencia del Resumen del Monitoreo CPU ELK.....	19
Tabla 11 Evidencia del Resumen del Monitoreo CPU-Memoria servidores Openshift ELK.....	19
Tabla 12 Evidencia del Resumen del Monitoreo ELK-Uso de disco (/).....	20
Tabla 13 Disponibilidad Servidores en Housing – Datacenter Principal	21
Tabla 14 Disponibilidad de Servicios de Housing – Datacenter Principal	22
Tabla 15 Actualización-Análisis componente Liferay septiembre.....	24
Tabla 16 Verificación del componente Liferay Ambiente de Pruebas	25
Tabla 17 Distribución trimestral de accesos por usuarios	26
Tabla 18 Distribución trimestral de Backup ejecutados	28
Tabla 19 Distribución trimestral de Backup por servicios.....	29
Tabla 20 Servicios replicados – Datacenter MEGACENTER.....	31
Tabla 21 Recursos-Datacenter Alterno Anexo #3. EC-Alterno_IAS.....	31
Tabla 22 Distribución trimestral de replicación	32
Tabla 23 Disponibilidad de Servicios de Housing – Datacenter Alterno	34
Tabla 24 Recomendaciones plataformas de seguridad	45
Tabla 25 Recomendaciones de seguridad para ICETEX.....	46
Tabla 26 Distribución módulos de videoconferencia por sede.....	50
Tabla 27 Distribución trimestral de requerimientos y/o incidentes	56
Tabla 28 Ejecución Presupuestal.....	57

INDICE DE ILUSTRACIONES

Ilustración 1 Arquitectura canales SDWAN ICETEX.....	15
Ilustración 2 UPTIME: Portal WEB web.icetex.gov.co.....	22
Ilustración 3 Métrica de Visitantes Portal WEB web.ICETEX.gov.co.....	23
Ilustración 4 Nodo 1 vista general.....	26
Ilustración 5 Nodo 2 vista general.....	26
Ilustración 6 Evidencia Reporte Backup diarios Servidores	28
Ilustración 7 Reportes de replicación SRM a Sitio Alterno, septiembre 30 2024	30
Ilustración 8 Reportes de replicación SRM a Sitio Alterno, septiembre 30 2024	30
Ilustración 9 Evidencia Dataguard replicado a Megacenter BD.....	33
Ilustración 10 Evidencia replicado servicios OnPremise ICETEX a Megacenter.....	34
Ilustración 11 Evidencia Gráfica Estadísticas de Portales	36
Ilustración 12 Estado Plataforma- Seguridad-Perimetral-DC_Principal (FortiGate-Triara)	37
Ilustración 13 Estado Plataforma- Seguridad-Perimetral-DC-Alterno-(FortiGate-Aguas)	37
Ilustración 14 Estado Plataforma- Seguridad-Perimetral- DC-Alterno-(FortiGate-Megacenter)	38
Ilustración 15 Estado Plataforma WAF-(FortiWeb_Triara_APPS_Nuevas)	38
Ilustración 16 Estado General de las Plataformas WAF-(FortiWeb-Triara-APPS_Viejas.....	39
Ilustración 17 Estado General de las Plataformas seguridad-Local-(FortiSandBox)	39
Ilustración 18 Evidencia Estado de Salud de los Equipos de Seguridad.....	40
Ilustración 19 Evidencia Imagen Reporte Monitoreo	41
Ilustración 20 Evidencia Imagen Reporte Monitoreo OSINT	42
Ilustración 21 Disponibilidad de servicio videoconferencia sedes regionales – septiembre 2024... 51	51
Ilustración 22 Disponibilidad de servicio videoconferencia sedes Bogotá –septiembre 2024	51
Ilustración 23 Incidencias/Requerimientos sedes Regionales – septiembre 2024.....	52
Ilustración 24 Evidencia módulo funcional sede Chapinero – Septiembre 2024.....	52
Ilustración 25 Incidencias/Requerimientos sedes Bogotá – Septiembre 2024.....	53
Ilustración 26 Evidencia módulo funcional sede Aguas 65”, piso 2 – septiembre 2024.....	53
Ilustración 27 Prueba de funcionamiento OPS módulo 65” sede Aguas, piso 4 – Sep 2024	54
Ilustración 28 Módulo sede Aguas piso 8 (Presidencia) – Septiembre 2024	54
Ilustración 29 Verificación sede Aguas, piso 6 (módulo móvil) septiembre 2024	55
Ilustración 30 Verificación módulo sede Ángel - septiembre 2024	55

INTRODUCCIÓN

El presente informe detalla las actividades ejecutadas por INFOTIC durante el periodo comprendido entre el 1 y el 30 de septiembre de 2024, en el marco del contrato 2022-0792. Este contrato, iniciado oficialmente el 19 de enero de 2023, tiene como objetivo principal proporcionar servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para ICETEX.

Para la ejecución de estas actividades, INFOTIC cuenta con un equipo compuesto por 10 especialistas técnicos y 3 profesionales administrativos, quienes garantizan la atención y soporte de los servicios especializados definidos en el alcance del proyecto. Estos servicios incluyen:

- Conectividad Y Red De Comunicaciones
- Servicios de Colaboración
- Centro De Datos
- Seguridad Informática
- Servicios De Nube
- Servicios Conexos

A la fecha, el proyecto reporta un avance del 44.4 % tras 16 meses de ejecución, cumpliendo con las actividades planificadas. En este informe, se describen en detalle las acciones realizadas durante el mes de septiembre, destacando el uso de herramientas tecnológicas y el esfuerzo del equipo profesional de INFOTIC para atender los requerimientos establecidos en el contrato y satisfacer las necesidades del ICETEX.

El informe correspondiente al mes de septiembre de 2024 presenta un detalle de los servicios realizados durante este periodo por el equipo de profesionales de INFOTIC. Asimismo, se describen las herramientas tecnológicas asignadas y utilizadas para el cumplimiento de las funciones establecidas, garantizando la atención de los requerimientos del ICETEX, conforme a lo estipulado en los términos del contrato vigente.

Adicionalmente los anexos se encuentran en el repositorio de ICETEX para su revisión, evaluación y comentarios:

- Administrador de Networking
- Administrador de Bases de datos
- Administradores de Soluciones
- Administrador Web Master
- Administradores Seguridad
- Integrador Nube
- Informe de monitoreo de Marca y Osint
- Informe de monitoreo SOC
- Informe de disponibilidad
- Pruebas de saturación
- Reporte backup septiembre 2024
- Consolidado mensual backup septiembre

- Backups Diario
- Reporte de IPS Septiembre
- Informe de vulnerabilidades septiembre
- Informe de consumo Canales Septiembre
- Informe septiembre 2024 servicio de videoconferencia
- Informe de evidencias Dataguard Megacenter septiembre 2024
- Informe de replicación
- Prueba TEST
- ANS canales septiembre 2024
- Reporte de Monitoreo ICETEX septiembre 2024 - ELK
- Conciliación septiembre consolidado
- Canales Allot Centralizado Septiembre

1 OBJETIVO

Presentar las actividades ejecutadas por INFOTIC durante el periodo del 01 al 30 de septiembre de 2024, con el fin de determinar el estado, la evolución y la disponibilidad de cada una de las gestiones realizadas en los diferentes servicios prestados al ICETEX en virtud de la ejecución del contrato, para lo cual se han considerado la recolección de mediciones las cuales corresponden a la disponibilidad de los canales en el numeral 3. Servicios de Conectividad y disponibilidad de los servidores en el numeral 4.1.1. Disponibilidad de Servicios – Datacenter Principal, el análisis y la producción de informes y reportes periódicos sobre cada una de las gestiones y demás informes especiales sobre los servicios prestados.

2 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 en la mayoría de los canales los anchos de banda requeridos por ICETEX.

Se ha gestionado de manera continua los casos reportados que afectan directamente los canales o la herramienta de monitoreo.

En cuanto a los canales pendientes, estamos proceso de instalación del canal de Backup de Quibdó el cual se ha extendido su tiempo de instalación, por temas administrativos con el centro comercial donde se encuentra la oficina.

Este mes se instalaron los canales de Leticia MPLS e Internet para la gente, sin embargo, no se han recibido formalmente porque se están ejecución de las pruebas de saturación.

Toda la información sobre conectividad se mantiene a ICETEX informado mediante los seguimientos semanales con el ingeniero de Networking.

Sobre los canales SDWAN por configurar en San Andres y Leticia, se encuentran en proceso de instalación para completar las 4 sedes solicitadas contractualmente.

El servicio L2L de replicación entre los Datacenter de TRIARA (Bogotá) y MEGACENTER (Medellín) se encuentra activo y no monitoreado.

En cuanto a la gestión de vulnerabilidades, todas las detectadas en el último escaneo de los equipos de networking fueron gestionadas y solucionadas en colaboración entre los especialistas de networking y seguridad de ICETEX. Cada vulnerabilidad solucionada fue documentada y compartida mediante reportes individuales, con el propósito de garantizar la continuidad de las acciones de remediación. Desde el equipo de Networking de INFOTIC se esperan los resultados de un nuevo escaneo de vulnerabilidades para atenderlas según su nivel de criticidad y las indicaciones de ICETEX, considerando cualquier observación adicional. INFOTIC continuará con la remediación de las vulnerabilidades identificadas en los escaneos realizados, asegurando la gestión continua y efectiva de la seguridad de los activos de información.

Con relación en la implementación de IPv6, se ha avanzado en las configuraciones de las interfaces MPLS de los firewalls en Aguas, Triara y Megacenter para habilitar la comunicación entre sedes utilizando IPv6, quedando a fin de mes sede Aguas y Datacenter Triara configuradas y quedando en proceso la integración con Megacenter.

El equipo de Networking de INFOTIC se encuentra realizando la configuración del protocolo IPV6 de acuerdo con los alcances del contrato para dar continuidad a la integración con el protocolo IPV6 en todos los canales de datos que forman parte de la operación; con respecto a la configuración a nivel WAN de las sedes en el que se lleva un avance del 45.4%

Se informa que a corte del mes de septiembre el equipo técnico se encuentra documentando las evidencias de las configuraciones. Se ha avanzado de acuerdo con lo solicitado por ICETEX y conforme a sus lineamientos del plan de transición.

Servicios de Colaboración: Durante este mes se continuó con el correcto funcionamiento y disponibilidad de los equipos de videoconferencia 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 los de infraestructura tales como UPS y sistemas eléctricos, tanto en el Datacenter principal como en el Datacenter alterno.

Servicio de Seguridad: Durante septiembre de 2024 se tuvieron las actividades relacionadas con la administración y gestión de la seguridad perimetral.

Dentro de los eventos del mes se detectaron alertas de posibles ataques que no fueron detectados por el FortiWeb, después de validaciones sobre el origen del tráfico se proceden a bloquear las direcciones IP de origen en el firewall perimetral que se sitúa antes del WAF para prevenir ataques sobre los sitios web de la entidad.

También dentro de las actividades se detectaron eventos de DDoS el cual fue descartado ya que no se tiene información relevante que indicara que se tratara de algún ataque de este tipo ya que el puerto utilizado fue el TCP 443 (HTTPS) el cual es un puerto que se usa para los sitios web de la entidad y el origen no fue catalogado como malicioso.

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.

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.

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 escaneos e intentos de explotación de vulnerabilidades en las cuales se evidencio que fueron eventos de paso de información por el protocolo SMB de un equipo en la red a un servidor a cargo del coordinador de infraestructura

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.

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

Se cuenta con la cantidad de especialistas solicitados contractualmente, los cual se organizan de forma presencial y remota con el fin de cubrir las solicitudes de servicio requeridas por el ICETEX

Los parafiscales siempre se presentan con la facturación de acuerdo con los procedimientos del área financiera de ICETEX, la cual no ha tenido ninguna observación hasta la fecha

- **Bolsa para servicios por demanda:** En el mes de septiembre de 2024, no se usó la bolsa de servicios.

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 septiembre 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 septiembre de 2024.

3 SERVICIOS DE CONECTIVIDAD

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

Los informes de disponibilidad de los canales ya anchos de banda 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 Septiembre 2024 - ALLOT INFOTIC.pdf](#)

Durante el mes de septiembre 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:

[Informe Mensual Disponibilidad Septiembre 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	99,99%
	Principal / IPVPN (Angel)	INR0272	100,00%
	Backup / IPVPN (Angel)	INR0273	99,93%
IBAGUE	Principal / IPVPN	INR0073	99,64%
	Backup / IPVPN	INR0076	100,00%
LETICIA	Principal / Satelital	Pendiente	0.00%
NEIVA	Principal / IPVPN	INR0039	100.00%
	Backup / IPVPN	INR0041	99,97%
TUNJA	Principal / IPVPN	INR0104	99,98%
	Backup / IPVPN	INR0106	99,97%
VILLAVICENCIO	Principal / IPVPN	INR0085	99,98%
	Backup / IPVPN	INR0084	99,97%
ARMENIA	Principal / IPVPN	INR0074	99,98%
	Backup / IPVPN	INR0072	98,49%
MANIZALES	Principal / IPVPN	INR0088	98,47%
	Backup / IPVPN	INR0087	95,45%
MEDELLIN	Principal / IPVPN	INR0133	99,97%
	Backup / IPVPN	INR0132	99,42%
APARTADO	Principal / IPVPN	INR0144	99,43%
PEREIRA	Principal / IPVPN	INR0079	100,00%

Sede	Categoría	INR	% Mes
	Backup / IPVPN	INR0077	98,77%
QUIBDO	Principal / IPVPN	INR0014	99,91%
	Backup / IPVPN	Pendiente	0.00%
BARRANQUILLA	Principal / IPVPN	INR0103	99,98%
	Backup / IPVPN	INR0100	99,92%
CARTAGENA	Principal / IPVPN	INR0109	98,59%
	Backup / IPVPN	INR0107	99,84%
MONTERIA	Principal / IPVPN	INR0080	99,54%
	Backup / IPVPN	INR0081	99,29%
RIOHACHA	Principal / IPVPN	INR0164	99,64%
	Backup / IPVPN	INR0162	99,93%
SANTA MARTA	Principal / IPVPN	INR0154	99,69%
	Backup / IPVPN	INR0152	99,84%
SINCELEJO	Principal / IPVPN	INR0095	96,07%
	Backup / IPVPN	INR0097	95,96%
SAN ANDRES	Principal / IPVPN	INR0000367/ INR0000369	99,79%
BARRANCABERMEJA	Principal / IPVPN	No hay oficina	0.00%
SAN GIL	Principal / IPVPN	No hay oficina	0.00%
BUCARAMANGA	Principal / IPVPN	INR0062	99,87%
	Backup / IPVPN	INR0061	99,97%
CUCUTA	Principal / IPVPN	INR0044	99,98%
	Backup / IPVPN	INR0047	99,97%
VALLEDUPAR	Principal / IPVPN	INR0091	99,93%
	Backup / IPVPN	INR0090	99,55%
YOPAL	Principal / IPVPN	INR0121	99,96%
	Backup / IPVPN	INR0123	93,50%
ARAUCA	Principal / IPVPN	INR0110	99,98%
CALI	Principal / IPVPN	INR0151	99,43%
	Backup / IPVPN	INR0153	95,20%
BUENAVENTURA	Principal / IPVPN	INR0051	99,98%
MOCOYA	Principal / IPVPN	INR0135	99,55%
	Backup / Satelital	INR0136	99,87%
PASTO	Principal / IPVPN	INR0130	99,97%
	Backup / IPVPN	INR0131	99,71%
POPAYAN	Principal / IPVPN	INR0035	99,71%
	Backup / IPVPN	INR0032	99,93%
TUMACO	Principal / IPVPN	INR0147	93,86%
WAN general (concentrador total red)	MPLS PP	INR0266	99,97%
WAN general (concentrador total red)	MPLS Backup	INR0171	99,96%
Conectividad dedicada a funciones de réplica para eventos de DRP.	DWDM	INR0224	0,00%
Canal entre Sitio principal e ICETEX - Dirección General - Aguas	Principal / IPVPN	No instalado	0%
	Backup / IPVPN	No instalado	0%
Salida Internet contingencia -	Ubicado en sede AGUAS interconectado a	INR0034	100.00%

Sede	Categoría	INR	% Mes
Dirección General - Aguas	través de red MPLS		
Canal entre Sitio contingencia ICETEX - 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	99,76%
Banco de la Republica hasta Edificio Dirección General ICETEX	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0000289	99,98%
DECEVAL hasta Edificio de ICETEX Dirección General.	Ubicado en Datacenter Principal, interconectado a través de red MPLS	INR0000317	99,97%
DECEVAL hasta Edificio de ICETEX Dirección General.	Ubicado en Datacenter Principal, interconectado a través de red MPLS (Backup)	INR0000318	99,97%
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	99,97%
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 y el estado de sus canales, en proceso de entrega en el mes de septiembre:

Sede	INR canal	BW (MB)	Fecha de Instalación	ESTADO
Leticia canal principal	INR0000373	8M	27/09/2024	Pendiente pruebas de Saturación y acta de entrega.
Leticia Internet para la gente	INR0000378	10M	30/09/2024	Pendiente Acta de entrega.

Tabla 2 instalados

A continuación, se relacionan los canales que están pendientes de Instalación o en proceso de instalación:

Servicio	Observaciones
San Andres SD WAN	Pendiente instalación porque la troncal de San Andres no tenía suficientes canales y estaba en proceso de ampliación.
Leticia SD WAN	En fase de instalación
Quibdó canal de datos de Backup	En fase de instalación, ha habido retrasos que no son atribuibles al operador sino a la administración del centro comercial donde se encuentra la oficina y a ICETEX se le ha mantenido informada.

Tabla 3 Canales pendientes por instalar o en proceso de instalación

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 operación en dichas ciudades.

Se están realizando las pruebas de saturación bidireccionales y se pueden consultar los (9) canales que van hasta ahora en el siguiente link: [Pruebas Saturación Canales](#)

CIUDAD	Enlace - Tipo medio	Código Servicio	Ancho de Banda - MB	Fecha de Ejecución de la Prueba
NEIVA	Principal / IPVPN	INR0039	20	28/08/2024
NEIVA	Backup/ IPVPN	INR0041	10	28/08/2024
IBAGUE	Principal / IPVPN	INR0073	20	28/08/2024
PEREIRA	Principal / IPVPN	INR0079	20	20/09/2024
MANIZALES	Principal / IPVPN	INR0088	20	30/08/2024
TUNJA	Principal / IPVPN	INR0104	20	30/08/2024
MEDELLIN	Principal / IPVPN	INR0133	100	24/09/2024
APARTADO	Principal / IPVPN	INR0144	20	26/09/2024
SAN ANDRES	Principal / IPVPN	INR0000367	8	29/07/2024

Tabla 4 pruebas de saturación ejecutadas hasta septiembre

En conclusión, se prestó el servicio en las sedes del ICETEX brindando conectividad y sin interrumpir la operación del Instituto. Durante el mes de septiembre no se realizaron ampliaciones, en la tabla a continuación se presenta los servicios de conectividad que se encuentran pendientes de ampliación:

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 5 pendientes por ampliar corte septiembre

Desde el 13 de septiembre hubo una tormenta eléctrica en San Andrés y daño el SW de la sede por lo tanto la entidad tuvo que trabajar con el Internet para la gente mientras se envió otro equipo, se adjunta como soporte de alerta al ICETEX : [RE Daño de equipo SW sede San Andres .msg](#), donde se indica que se cuenta con un switch de 24 puertos (POE) que fue recuperado de una bodega del ICFES este dispositivo se encuentra operativo, y se procederá a configurarlo para enviarlo a reemplazar al Switch de San Andrés.

La tabla de casos de indisponibilidad se encuentra en el [Informe Septiembre 2024 - Administrador Networking.pdf](#) en la página 4 caso atendidos en el mes y su detalle.

3.1 Internet Para La Gente

Durante el mes de septiembre el servicio de Internet para la gente se prestó sin interrupciones en trece de las catorce sedes contempladas para Internet para la gente, según el Anexo#2.1 Canales

Telecomunicaciones, 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	99,67%
MEDELLIN	INTERNET PARA LA GENTE	INR0122	99,67%
APARTADO	INTERNET PARA LA GENTE	INR0140	100,00%
ARAUCA	INTERNET PARA LA GENTE	INR0115	99,87%
LETICIA*	INTERNET PARA LA GENTE		
QUIBDO	INTERNET PARA LA GENTE	INR0021	100,00%
RIOHACHA	INTERNET PARA LA GENTE	INR0159	99,85%
SAN ANDRES	INTERNET PARA LA GENTE	INR0000368	100,00%
YOPAL	INTERNET PARA LA GENTE	INR0127	100,00%
MOCOA	INTERNET PARA LA GENTE	INR0141	99,50%

Tabla 6 Disponibilidad canales "Internet para la gente"

*El Internet para la gente de Leticia se encuentra instalado el último día del mes.

3.2 Canales SDWAN

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

Sede	Categoría	Código se Servicio	% Mes
SD WAN AGUAS	SD WAN	INR0033 / 000334	100.00%
SD WAN MOCOA	SD WAN	INR0139 / 000333	99.80%

Tabla 7 canales "SDWAN"

Los canales 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.

A continuación de muestra la Arquitectura solicitada por ICETEX para los canales SDWAN y la cual se termina de implementar con los canales de Leticia y San Andres.

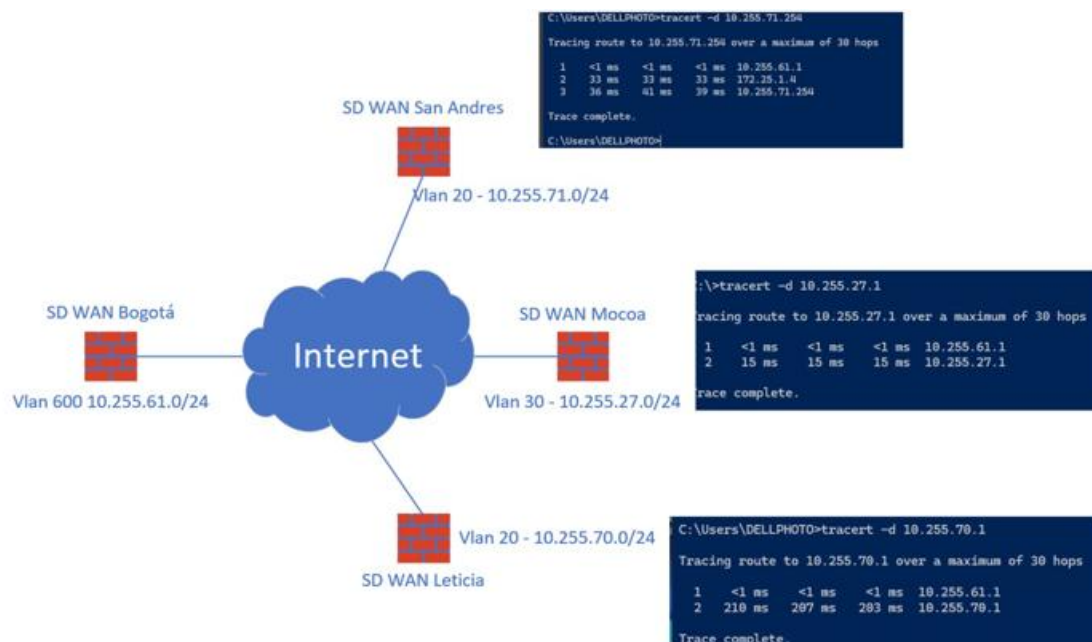


Ilustración 1 Arquitectura canales SDWAN ICETEX

3.3 Canal de Replicación (Triara – Megacenter)

Dentro del contrato 2022-079, se estableció un canal dedicado DWDM para la comunicación entre los Datacenter Principal (Triara), y el Datacenter alterno (Megacenter), como acción mejorar el servicio y con el ánimo de que ICETEX cuente con lo mejor y lo último que están manejando los operadores de tecnología a nivel de velocidad de transmisión y la seguridad que debe contener la información que se replica INFOTIC y su aliado estratégico, se instaló un LAN 2 LAN e indicó en su momento las ventajas de este canal, hasta el momento el canal es funcional sin afectaciones, está pendiente la formalización contractual de la entrega del mismo cuya evidencia de su correcta funcionalidad es el proceso de sincronización el cual se puede validar en el [Informe mensual replicación septiembre 2024.pdf](#)

Se programará el próximo mes con ICETEX la sesión técnica donde se formalizará el servicio, teniendo en cuenta que está instalado desde la vigencia anterior.

3.4 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, la cual se encuentra en proceso de elaboración porque tuvo un problema de avería en el transporte y debió iniciar su proceso de elaboración nuevamente según explica el operador de Telecomunicaciones aliado (CLARO COMUNICACIONES) se proyecta la fecha tentativa de entrega el mes diciembre.

A continuación, se presenta la relación de la señalética 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 8 Estado de la instalación de la señal ética de Wifi

3.5. Continuidad a La Integración Protocolo IPV6

Durante septiembre, ICETEX ha llevado a cabo un proceso de normalización de sus redes a nivel nacional, configurando direcciones IPv6 nativas. Este cambio ha sido coordinado con el proveedor CLARO e implicó la modificación de las configuraciones en los routers de dicho operador para reflejar las nuevas direcciones IPv6.

El aliado, Operador CLARO avanzó con las configuraciones y el 25 de septiembre indicó que los servicios que quedan por configurar tienen Gateway de voz, y que varios de los firewalls ya no cuentan con puertos disponibles para la configuración de un nuevo segmento, se procederá eliminando el enrutamiento del nuevo segmento que esta hacia su Gateway de voz y configurándolo por el puerto actual, pero en modo troncal con la 30.

INFOTIC está gestionando esta actividad, por lo tanto, se avanzó con las sedes que no tienen Gateway de voz.

Hasta la fecha, las sedes de Ángel, Aguas (VLAN 21), Barranquilla, Chapinero, Buenaventura, Riohacha, Popayán, Tumaco, Cúcuta, Arauca, Apartado y Mocoa ya están operando con IPv6 nativo.

El plan de direccionamiento adjunto detalla la correspondencia entre las direcciones IPv4 existentes y las direcciones IPv6 asignadas a cada sede.

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](#)

Sede	Segmento ipv4	Gateway ipv4	Segmento ipv6	Gateway ipv6
Aguas	10.255.0.0/24	10.255.0.1	2801:192:6:E0::/64	2801:192:6:E0::1
Chapinero Bogotá	10.255.1.0/24	10.255.1.1	2801:192:6:E1::/64	2801:192:6:E1::1
Ángel Bogotá	10.255.2.0/24	10.255.2.1	2801:192:6:E2::/64	2801:192:6:E2::1
Buenaventura	10.255.5.0/24	10.255.5.1	2801:192:6:E5::/64	2801:192:6:E5::1
Barranquilla	10.255.14.0/24	10.255.14.1	2801:192:6:EE::/64	2801:192:6:EE::1
Tumaco	10.255.16.0/24	10.255.16.1	2801:192:6:F0::/64	2801:192:6:F0::1
Cúcuta	10.255.17.0/24	10.255.17.1	2801:192:6:F1::/64	2801:192:6:F1::1
Arauca	10.255.23.0/24	10.255.23.1	2801:192:6:F7::/64	2801:192:6:F7::1
Apartado	10.255.26.0/24	10.255.26.1	2801:192:6:FA::/64	2801:192:6:FA::1
Mocoa	10.255.27.0/24	10.255.27.1	2801:192:6:FB::/64	2801:192:6:FB::1

Tabla 9 Ejemplo de Direccionamiento IPV6

Ante las observaciones formuladas por el ICETEX sobre las actividades adelantadas para dar continuidad a la implementación del protocolo IPV6 se da respuesta en el documento [INFOTIC ICETEX - IPV6 Observaciones ICETEX.pdf](#) y se programaran sesiones de trabajo para revisar la observación y realizar un plan de trabajo en conjunto para adelantar las actividades.

3.5 Gestión de Vulnerabilidades en Networking

A la fecha, el equipo de Networking cuenta con los resultados de los escaneos de vulnerabilidades realizados por ICETEX con la herramienta TENABLE y continúa ejecutando actividades de remediación para las vulnerabilidades de nivel medio y bajo, según lo indicado en los informes generados.

Los escaneos de vulnerabilidades realizados y las remediaciones se pueden consultar en la ruta [Networking](#) donde son almacenados por los pares de seguridad del ICETEX.

3.6 Conclusiones Del Servicio De Conectividad

- Todos los casos fueron gestionados exclusivamente a través de la herramienta Aranda, sin que se registrara atención por otros medios. En comparación con el mes anterior, se observó un incremento del 2% en los casos, atribuido a fallos en el servicio por parte del proveedor y a bloqueos de puertos en los equipos de la sede, la evidencia de los casos gestionados se encuentra en el [Informe Septiembre 2024 - Administrador Networking.pdf](#).
- Cada caso fue cerrado tras notificar a los funcionarios del servicio operativo sobre las incidencias pendientes con el proveedor, lo que representa una reducción del 10% en relación con el mes anterior.
- El progreso en la instalación de los canales es del 98%, con sólo las implementaciones de Quibdó Backup.

➤ En cuanto a la instalación de señaléticas, también se ha alcanzado un avance del 98%, quedando únicamente la señalética de Cali, que actualmente se encuentra en proceso de fabricación.

➤ Se continúa trabajando en el proyecto de IPv6 con un seguimiento semanal con el Icetex con el objetivo de completar el proyecto de IPv6, se presenta un avance del 45.4% sobre las sedes del ICETEX, el restante de sedes es necesario que ICETEX realice la entrega de la configuración que se debe implementar debido a que estas sedes cuentan con un router de voz lo que impide realizar la configuración definida inicialmente, a nivel de la WAN se está revisando porque CLARO no ha implementado el direccionamiento entregado para el tema de IPv6.

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

4 SERVICIOS CENTROS DE COMPUTO.

4.1 Datacenter Principal

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

Respecto al consumo de servicio en las máquinas y como se podrá observar en las ilustraciones 2,3 y 4, 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 realiza el monitoreo de los servidores en la herramienta ELK , el reporte desde ELK se puede consultar en el siguiente link: [Reporte Monitoreo ICETEX Septiembre 2024-ELK.pdf](#)

En la Tabla 10 se muestra el reporte de uso de CPU y de memoria de los servidores de Icetex especificando el hostname, código de servicio asignado en el operador de servicio, pico máximo, pico mínimo y promedio de uso durante el mes.

Hostname	Código de servicio	AVG CPU USAGE
cxvodacontg011	INR0278	9.07%
cxvodaprodn011	INR0276	34.54%
cxvodaprodn021	INR0277	45.83%
icetexbogbalsrv1	INR0237	13.33%
icetexbogelasticserver1	INR0239	1.01%
icetexbogelasticserver2	INR0240	0.21%
icetexbogelasticserver3	INR0241	0.99%
icetexbogliferaynfs	INR0238	11.67%
icetexbogliferaysrv1_R	INR0243	23.41%
icetexbogliferaysrv2_R	INR0242	3.89%
icetexboglxdarumasrv1	INR0244	3.69%
icetexboglxdarumasrv2	INR0245	1.50%
iceteboglxdarumatest	INR0246	1.14%

Hostname	Código de servicio	AVG CPU USAGE
icetexboglxorfeo1	INR0233	0.35%
icetexboglxorfeo2	INR0262	0.53%
icetexboglxroad3	INR0248	0.61%
icetexosbognfs1	INR0260	11.98%
icetexosbognfs2	INR0252	4.86%
icetexbogPortalTransacServer1	INR0236	0.65%
icetexbogPortalTransacServer2	INR0235	1.26%
ictxprusisgapp	INR0234	11.98%
ictxisisgesapp	INR0229	4.93%
ictxisisgesbd	INR0228	0%
ictxsrctrldoc	INR0000322	1.79%
icetexbogwsmira	INR0226	15.32%
icetexboglxroad2n	INR0247	1.03%
icetexboglxroadtest	INR0250	0.89%
icetexboglxroad1	INR0249	2.03%
bastion	INR0253	0.3

Tabla 10 Evidencia del Resumen del Monitoreo CPU ELK

En la Tabla 11 se muestra el reporte de uso de CPU y de memoria de los servidores de Openshift de ICETEX especificando el nombre de la máquina virtual, promedio de uso de CPU y de Memoria, pico máximo de uso, pico mínimo de uso durante el mes.

VM NAME	Codigo de servicio	AVG VM CPU.USED.GHZ
gate-vfpz6-master-0	INR0251	1,966.00
gate-vfpz6-worker-lfmk4	INR0254	504
gate-vfpz6-worker-64vd2	INR0255	1,216.00
gate-vfpz6-worker-5smdz	INR0256	481
gate-vfpz6-worker-vjtj6	INR0257	1,445.00
gate-vfpz6-master-2	INR0258	1,354.00
gate-vfpz6-master-1	INR0259	2,088.00
VM NAME	Código de servicio	AVG VM MEM.USED.GHZ
gate-vfpz6-master-0	INR0251	28.00
gate-vfpz6-worker-lfmk4	INR0254	1
gate-vfpz6-worker-64vd2	INR0255	7.00
gate-vfpz6-worker-5smdz	INR0256	1
gate-vfpz6-worker-vjtj6	INR0257	6.00
gate-vfpz6-master-2	INR0258	15.00
gate-vfpz6-master-1	INR0259	27.00

Tabla 11 Evidencia del Resumen del Monitoreo CPU-Memoria servidores Openshift ELK

En la ilustración 4 se muestra el reporte de uso de discos de los servidores de ICETEX especificando el hostname de la máquina virtual, código de servicio asignado en el operador de servicio, file System, pico máximo de uso del filesystem, pico mínimo de uso de cada file System y porcentaje promedio de uso del file System de cada una de las máquinas virtuales en el mes.

Hostname	Código de servicio	AVG DISK USAGE
cxvodacontg011	INR0278	1.9
cxvodaprodn021	INR0277	2

Hostname	Código de servicio	AVG DISK USAGE
icetexboglobserver1	INR0237	34.22
icetexbogelasticserver1	INR0239	37.85
icetexbogelasticserver2	INR0240	27.1
icetexbogelasticserver3	INR0241	30.85
icetexbogliferaynfs	INR0238	20.81
icetexbogliferayserver1_R	INR0243	36.23
icetexbogliferayserver2_R	INR0242	32.94
icetexboglxdarumasrv1	INR0244	45.79
icetexboglxdarumasrv2	INR0245	72.34
iceteboglxdarumatest	INR0246	79.95
icetexboglخورfeo1	INR0233	49.3
icetexboglخورfeo2	INR0262	75.3
icetexboglxxroad3	INR0248	39.7
icetexboglxxroad2n	INR0247	30.3
icetexboglxxroadtest	INR0250	43.62
icetexboglxxroad1	INR0249	6.4
bastion	INR0253	88.9

Tabla 12 Evidencia del Resumen del Monitoreo ELK-Usos de disco (/)

4.1.1 Disponibilidad de Servicios – Datacenter Principal

A continuación, se presenta la tabla del promedio de disponibilidad de los servidores que se encuentran en Datacenter Triara, se muestra el porcentaje de disponibilidad que tuvo cada uno de los servidores durante el mes, evidenciando que todos presentaron disponibilidad entre 99.99% a 100%:

#	Códigos de Servicio	Hostname	Disponibilidad
1	INR0228	ictxisisgesbd	100%
2	INR0229	ictxisisgesapp	100%
3	INR0233	icetexboglخورfeo1	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	iceteboglxdarumatest	100%
14	INR0247	preprodsec-icetexboglxxroad2n	100%

15	INR0248	icetexboglxxroad3	100%
16	INR0249	xroadsec-icetexboglxxroad1	99.99%
17	INR0250	qasec-icetexboglxxroadtest	100%
18	INR0262	icetexboglxxorfeo2	100%
19	INR0276	cxvodaprodn011	100%
20	INR0277	cxvodaprodn021	100%
21	INR0278	cxvodacontn011	100%
22	INR0240	icetexbogelasticserver2	100%
23	INR0260	icetexbogosgognfs1	100%
24	INR0252	icetexbogosgognfs2	100%
25	INR0236	ictxbogsvrpt1	100%
26	INR0235	ictxbogsvrpt2	100%
27	INR0000322	ictxcontroldoc	99.98%
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 13 Disponibilidad Servidores en Housing – Datacenter Principal

El siguiente cuadro presenta el porcentaje de disponibilidad de los dispositivos de seguridad, switches, controladoras y Enclosure de almacenamiento que se encuentran en Housing en el Datacenter principal y su disponibilidad durante el mes:

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	Dell	M1000E	99,80%	100%

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

Tabla 14 Disponibilidad de Servicios de Housing – Datacenter Principal

4.1.2 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 [99,96%]** tal como se evidencia en la gráfica a continuación.

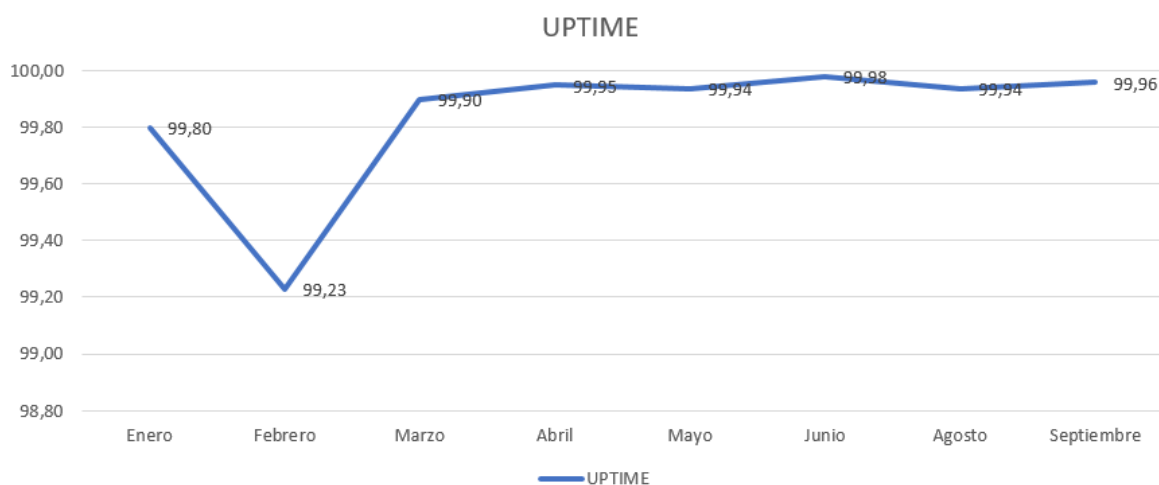


Ilustración 2 UPTIME: Portal WEB web.icetex.gov.co

Durante el mes de septiembre se evidenció un comportamiento estable del portal WEB institucional y se cumplió con el porcentaje de disponibilidad de este con un porcentaje del **99,96%** 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 387 mil usuarios, con 267 mil usuarios nuevos. El tiempo de interacción medio es de 2 minutos 06 segundos, señalando el interés de la audiencia en las diferentes páginas del portal web.icetex.gov.co

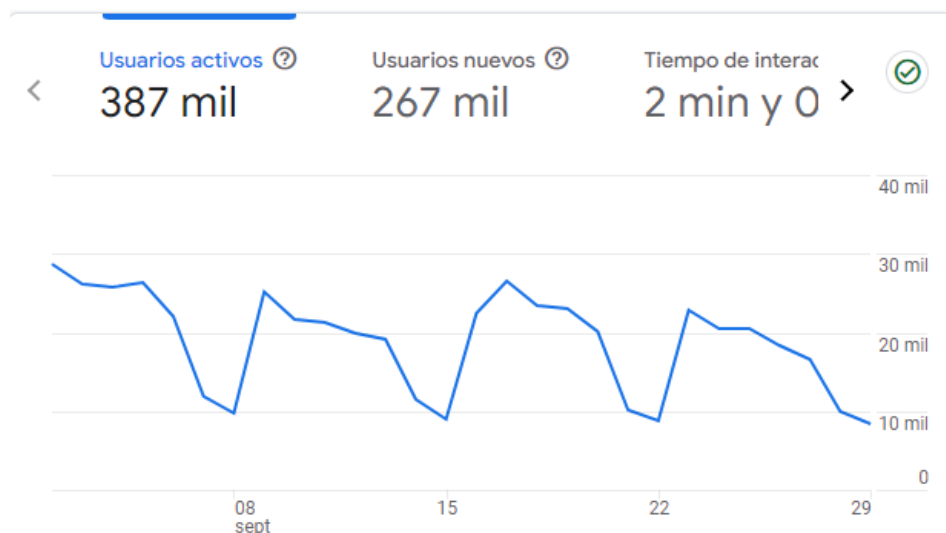


Ilustración 3 Métrica de Visitantes Portal WEB web.ICETEX.gov.co

4.1.3 Análisis componente Liferay Producción

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 hallazgos encontrados en los nodos 1 y 2 del portal Liferay 7.3.10 GA1.

A continuación, se presenta un cuadro con la actualización para el presente mes 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	En espera de la autorización de ICETEX para disponer y configurar la memoria necesaria para que los dos nodos queden iguales. Esta solicitud se realizó mediante correo electrónico del 30 de agosto del 2024.
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	La ventana de mantenimiento con N. de Caso 1116300, programada para el sábado 28 de septiembre, se suspendió por problemas con el acceso al servidor icetexbogelasticserver2 - Elasticsearch con código de servicio INR0240 y dirección IP 192.168.20.44. El servidor de Liferay reporta dos servidores de Elasticsearch, por lo tanto, este tercero se evidencia que no está configurado en el portal de Liferay como aplicación. También, la versión del sistema operativo de los 3 servidores del Elasticsearch, no se conoce solo la versión del Elasticsearch que es la 7.9.3.

		por lo tanto, lo recomendado es validar con el fabricante, la matriz de compatibilidad del sistema operativo de Elasticsearch vs la nueva versión a implementar de Linux en nodo 1 y nodo 2. Adicional la recomendación al operador es hacer una prueba piloto donde se pueda comprobar la compatibilidad de los sistemas operativos (Elasticsearch - Liferay) antes de proceder con la actualización de Linux en ambas aplicaciones. Se evidencia que el servidor icetexbogelasticsearchserver2 - Elastic search con código de servicio INR0240 y dirección IP 192.168.20.44 no está sincronizado con el servidor de Liferay 7.3.10 GA 1.
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.	Comportamiento normal.
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.	Comportamiento normal.
PARCHES DE SEGURIDAD	Nodo 1 - activation-key-dxpproduction-7.3-ICETEX-publicportal 40.xml activation-key-dxpproduction-7.3-ICETEX-publicportal - ICETEXbogliferayserver1.xml Nodo 2 - activation-key-dxpproduction-7.3-ICETEX-publicportal - ICETEXbogliferayserver2.xml	Pendiente de solicitar al cliente, la renovación de soporte Liferay para poder seguir obteniendo los parches de seguridad en la versión 7.3. También para poder cambiar a la versión 7.4 y obtener actualización de los parches de seguridad en la versión 7.4.
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 15 Actualización-Análisis componente Liferay septiembre

4.1.4 Ambiente De Pruebas Liferay -ICETEX

El ambiente de pruebas de ICETEX forma parte de los servicios ONPREMISE que no están incluidos contractualmente en la administración de INFOTIC, sin embargo, por solicitud de ICETEX se

realizaron las validaciones correspondientes, identificando que desde el 3 septiembre el ambiente de pruebas no se encuentra en funcionamiento.

Después de la validación realizada por el WEBMASTER que encontraron los siguientes hallazgos, lo cuales se entregan para gestión del equipo de infraestructura ICETEX, quienes darán solución al despliegue de en estos servidores.

Unidad	Hallazgo	Observaciones
RAM	Nodo ambiente de pruebas total de memoria RAM – 8.011 GB	Memoria RAM de 8 GB. Escaso para un ambiente de pruebas Liferay, se recomienda tener la misma cantidad de RAM en el ambiente productivo (65.79 GB Nodo 1). Se abrió caso con el proveedor donde se manifiesta que lo recomendable es tener las mismas características de los servidores productivos, sin embargo, ICETEX validará los recursos que asignará a este ambiente.
SISTEMA OPERATIVO	La última versión del Sistema Operativo Red Hat Enterprise 7.2,	Se informa a ICETEX para que los Administradores de esta infraestructura ONPREMISE (administrador de Linux - Sysadmin) realice la actualización del Sistema Operativo debido a que la actual es una versión obsoleta "Red Hat Enterprise Linux 7.2 GA server".
DISCO DURO	El espacio en disco utilizado por el CMS Liferay en el ambiente de pruebas 299 GB. El espacio disponible es de 169 GB.	Tiene un tamaño de 493 GB, con un espacio usado de 299 GB. Espacio disponible de 169 GB. El ambiente estuvo operativo hasta el lunes 2 de septiembre, el área de infraestructura no ha podido desplegar el ambiente nuevamente.
FILE SYSTEM	El espacio en utilizado por el File System el ambiente de pruebas es 66 GB.	
PARCHES DE SEGURIDAD	AMBIENTE DE PRUEBAS activation-key-dxpproduction-7.3-ICETEX-publicportal40.xml activation-key-dxpproduction-7.3-ICETEX-publicportal - ICETEXbogliferayserver1.xml	Pendiente de solicitar al cliente, la renovación de soporte Liferay para poder seguir obteniendo los parches de seguridad en la versión 7.3. También para poder cambiar a la versión 7.4 y obtener actualización de los parches de seguridad en la versión 7.4.
VOLUMEN DE LOGS	El registro histórico del ambiente de pruebas comienza desde el 25 de agosto de 2022.	El ambiente de pruebas tiene más registros históricos que los nodos 1 y 2 (liferay.2022-08-25.log).
Liferay	Se encuentra en la versión 7.3.10 GA1	
Elasticsearch	Se encuentra en la versión 7.9.3	

Tabla 16 Verificación del componente Liferay Ambiente de Pruebas

En la ilustración del nodo 1 se evidencia el comportamiento de la CPU, Memoria y almacenamiento

los cuales no superan los límites configurados:

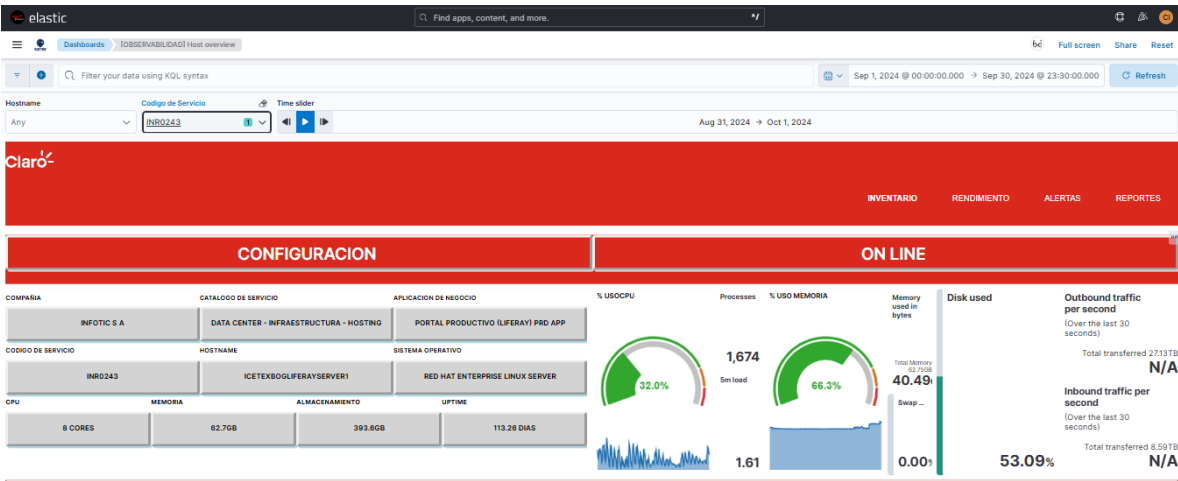


Ilustración 4 Nodo 1 vista general

En la ilustración del nodo 2 se evidencia el comportamiento de la CPU, Memoria y almacenamiento, es de aclarar que se presenta un alto consumo de memoria debido a que tiene un preformar inferior al nodo1, se solicitó a ICETEX la autorización para adquirir los componentes necesarios para tener los dos nodos idénticos, pero no se ha tenido la aprobación requerida.

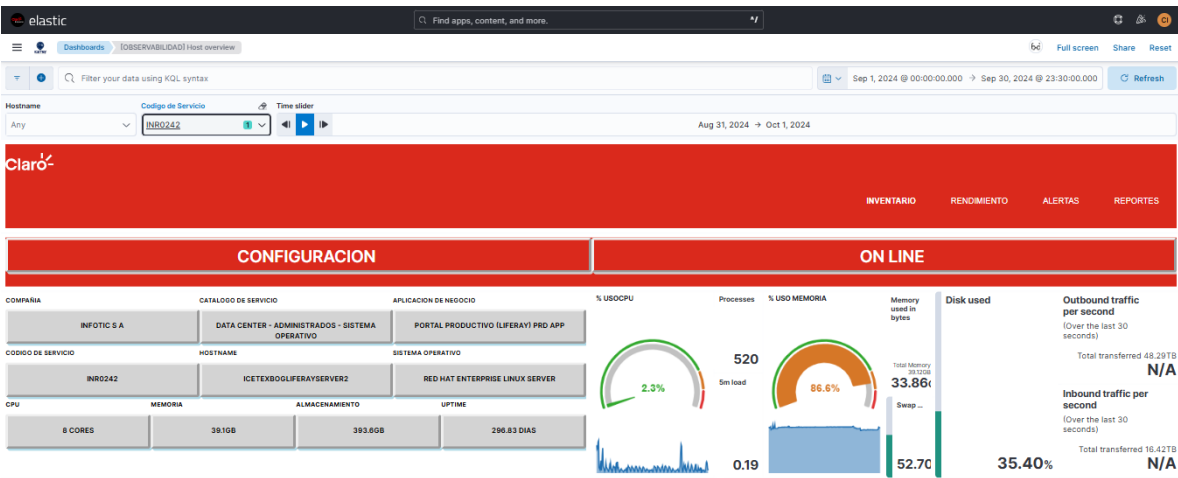


Ilustración 5 Nodo 2 vista general

El siguiente es el comportamiento a nivel de acceso al portal WEB durante el último trimestre:

	Julio	Agosto	Septiembre
Usuarios mes	568000	438000	387000
Usuarios nuevos	388000	301000	267000
Tiempo acceso (min)	154	145	126

Tabla 17 Distribución trimestral de accesos por usuarios

Durante el último trimestre se presentó un promedio de 464333 usuarios que accedieron al portal web, presentando para el mes de septiembre una disminución en el número de usuarios que

ingresaron a la página de la entidad del 31.87% que corresponde a 181000 usuarios.

A nivel de los usuarios nuevos que accedieron a la página se tiene que en promedio durante el último trimestre se tiene 318667, presentando para el mes septiembre una disminución del 31.18% que corresponde a 121000 usuarios nuevos que no ingresaron al portal de la entidad.

El tiempo que emplearon los usuarios una vez ingresaron a la página web de la durante el último trimestre correspondió a 141.67 minutos, presentando una disminución para el mes de septiembre de 18.18% que corresponde a 28 minutos.

4.1.5 Backup Servidores Triara

Durante el periodo de septiembre 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, [Consolidado mensual Backup Septiembre.pdf](#) donde se adjunta el [Reporte Backups septiembre 2024.pdf](#) que se genera automáticamente desde la herramienta que se utiliza para realizar las copias y forma manual se le ha colocado en formato de INFOTIC, es de aclarar que la ley establece que no se pueden modificar los documentos que son generados de forma automática por herramientas tecnológica para dar la seguridad y tranquilidad que el documento cumple con las condiciones de calidad, integralidad y confiabilidad de la información

Dentro de las actividades del proyecto de servicios tecnológicos para ICETEX, se tiene la toma de copias de respaldo de la información creada, actualizada 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 y las políticas de Backup.

Esta información debe ser traslada 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 proceso como se acordó contractualmente.***

A continuación, se muestra el reporte de resumen que se envía cada día como resultado de las tareas de backups del día anterior, tareas completadas, fallidas, terminadas, parcialmente satisfactorias y completadas con errores durante el proceso de toma de los backups diarios, por ejemplo, el tamaño de la aplicación de las tareas completadas el 30 de septiembre a corte 8:39 am de 1 de octubre con un tamaño de aplicación de 150.64 TB.

Backup job summary

Backup job summary report

Generated on: Oct 01, 2024 08:39 AM

Server groups : #FOTC
Servers : All
App types : All
Subclients : All
Job status : Running, Completed, Delayed, Failed, Killed, Completed with Errors, Completed with Warnings, Committed
Job Types : All
Time Frame : Last 4 weeks (Sep 3, 2024, 08:39:16 AM - Oct 1, 2024, 08:39:16 AM)
Time zone : Coreserv
Day Start Time : 12:00 AM
Snap and Backup Copy options : Snap and Backup Copy options
Advanced : None

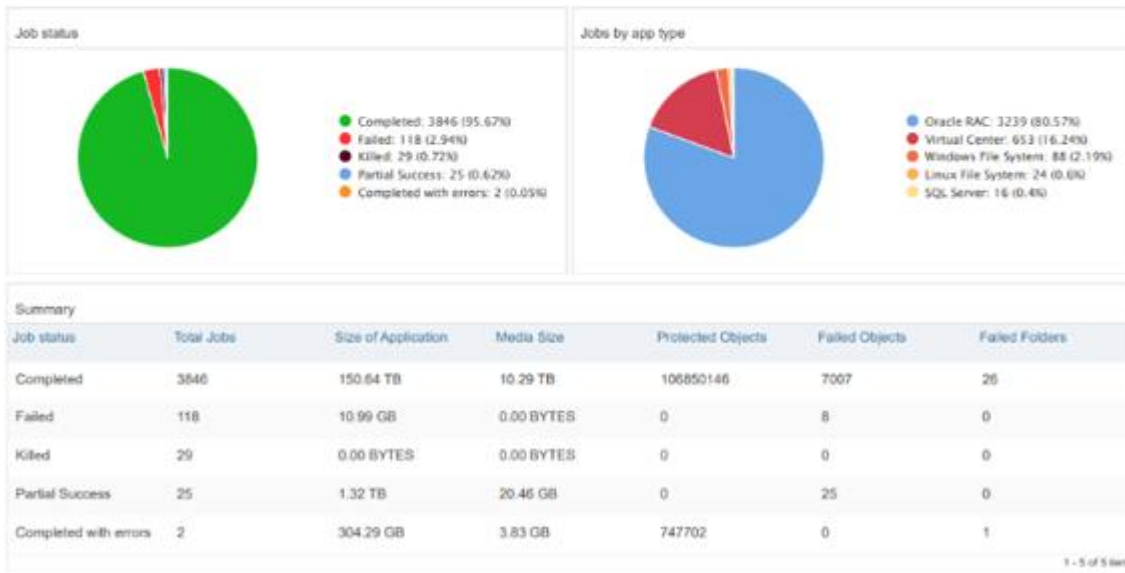


Ilustración 6 Evidencia Reporte Backup diarios Servidores

Análisis

El total del tamaño de la información respalda en cintas de Backups para el mes de septiembre corresponde a 152.27528 TB, donde 95.67% se completó en el primer lanzamiento del robot con un total de 150.64 TB de información.

El 80.57% está representado en el respaldo dado a la información del Oracle RAC, que equivale a 122.688193 TB.

Se realiza el comparativo del último trimestre con respecto a la toma de backup con el siguiente resultado:

	Julio	Agosto	Septiembre
Completado	97.93%	98.55%	95.67%
Éxito Parcial	0.82%	0.56%	0.62%
Fallido	0.65%	0.15%	2.94%
Terminado	0.58%	0.66%	0.72%
Completado con errores	0.02%		0.05%
En progreso		0.08%	

Tabla 18 Distribución trimestral de Backup ejecutados

- El promedio de los Backups completado del último trimestre en el primer lanzamiento del robot fue de 97.38%, donde el mes con mayor nivel de completado fue agosto con 98.55%; el 02.62% corresponde a los siguientes parámetros: éxito parcial, fallido, terminado, completado con errores y en progreso.
- El promedio de toma Backups Fallido durante el último trimestre corresponde a 1.25%, el mes donde más se presentó un mayor porcentaje de fallas fue septiembre con el 2.94%

	Julio	Agosto	Septiembre
Oracle RAC	77.01%	81.78%	80.57%
Virtual Center	19.59%	15.42%	16.24%
Windows File System	2.34%	1.99%	2.19%
Linux File System	0.68%	0.54%	0.60%
SQL Server	0.39%	0.28%	0.40%

Tabla 19 Distribución trimestral de Backup por servicios

- El servicio que ocupó el mayor porcentaje en la toma de backup fue el ORACLE RAC.
- El promedio del último trimestre del respaldo de Oracle RAC fue de 79.79% donde el mes con mayor tamaño de información respaldada fue agosto con el 81.78%.

NOTA: En el caso de los Backups que no fueron exitosos o que presentan algún tipo de problema son revisados de forma interna por parte de CLARO, subsanados y nuevamente tomados por el área correspondiente, para el caso de los que no se pueden solucionar se escalan con el cliente para que se revise la falla y se proceda a ejecutarlos nuevamente.

4.2 Datacenter Alterno

4.2.1 Hosting Virtual (IaaS)

En el transcurso del mes de septiembre 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 septiembre 2024.pdf](#), cuyo reporte refleja el consolidado de los informes mensuales y que se están entregando periódicamente, a continuación se puede ver el último reporte diario del mes.

Se tienen las siguientes conclusiones de la replicación para este mes:

- Se realizaron las replicaciones de los 13 equipos durante todos los días del mes de septiembre 2024.
- Se presentaron errores en las replicaciones del servidor ICTXBOGSRVPT1 correspondiente al Portal Transaccional identificado con el INR0236 y servidor icetexboglxorfeo1 correspondiente a ORFEO identificado con el INR0233 tomados en el mes de septiembre de 2024 y se corrigió al siguiente día y continuo la réplica correctamente:

Site Recovery Manager - Estado Replicas INFOTIC

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

General					
Name	Count				
OK	12				
Not Active (RPO Violation)	1				
Grupo de protección: PG_INFOTIC_7 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0226_INFOTIC_REP	OK	5 of 5	Sep 30, 2024	11.62 MB	5 minutes
Grupo de protección: PG_INFOTIC_6 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0228_INFOTIC_REP	OK	1 of 1	Sep 30, 2024	112.5 MB	1 hour
INR0229_INFOTIC_REP	OK	1 of 1	Sep 30, 2024	10 MB	1 hour
Grupo de protección: PG_INFOTIC_1 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0233_INFOTIC_REP	Not Active (RPO Violation)	6 of 6	Sep 30, 2024	8.01 MB	30 minutes

Ilustración 7 Reportes de replicación SRM a Sitio Alterno, septiembre 30 2024

INR0262_INFOTIC_REP	OK	1 of 1	Sep 30, 2024	9.13 MB	1 hour
Grupo de protección: PG_INFOTIC_5 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0236_INFOTIC_REP	OK	2 of 2	Sep 30, 2024	164.05 MB	2 hours
Grupo de protección: PG_INFOTIC_4 (4)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0237_INFOTIC_REP	OK	2 of 2	Sep 30, 2024	28.27 MB	5 minutes
INR0238_INFOTIC_REP	OK	2 of 2	Sep 30, 2024	218.57 MB	1 hour
INR0239_INFOTIC_REP	OK	2 of 2	Sep 30, 2024	30.83 MB	1 hour
INR0243_INFOTIC_REP	OK	2 of 2	Sep 30, 2024	334.28 MB	1 hour
Grupo de protección: PG_INFOTIC_3 (2)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0244_INFOTIC_REP	OK	1 of 1	Sep 30, 2024	70.3 MB	1 hour
INR0245_INFOTIC_REP	OK	1 of 1	Sep 30, 2024	16.63 MB	5 minutes
Grupo de protección: PG_INFOTIC_2 (1)					
VirtualMachine	Status	ConfiguredDisks	LastInstanceSyncPoint	LastSyncSize	RPO
INR0249_INFOTIC_REP	OK	2 of 2	Sep 30, 2024	18.1 MB	5 minutes

Ilustración 8 Reportes de replicación SRM a Sitio Alterno, septiembre 30 2024

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

#	Código de Servicio	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	icetexboglobserver1	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 20 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, sin embargo, la diferencia más significativa corresponde a dos servidores de Portal web INR0239-ICETEXbogelasticserver1 y INR0243-ICETEXbogliferayserver1 que están 32 GB de memoria por encima del definido en la línea base.

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	icetexboglobserver1-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 21 Recursos-Datacenter Alterno Anexo #3. EC-Alternio_IAS

En cuanto al excedente de memoria se definió con ICETEX realizar el ajuste de la memoria en los dos servidores de Portal y devolverlos a los valores definidos en la línea base, sin embargo, para no desmejorar el rendimiento de estos se realizará una revisión y se presentará a ICETEX cual sería el consumo real de estos servidores y así definir en cuanto se reduce la memoria y por consiguiente acordar con el ICETEX como se ajustará en términos de facturación dicho consumo adicional.

Se puede ver el soporte de este análisis en el siguiente link: [MEGACENTER-REPLICACION_2908.xlsx](#)

Análisis

Julio	Agosto	Septiembre
11286.67	11541.59	15966.78

Tabla 22 Distribución trimestral de replicación

Durante el último trimestre la replicación que se realiza entre el data center principal TRIARA y el data center alerno MEGA CENTER tuvo un promedio de transferencia de data de 12931.68 MB y se presenta un crecimiento del 27,71 % entre agosto y septiembre, que equivale a 4425.19 MB.

Durante el mes de septiembre del 2024, se presentó el error Not Active (RPO Violation) en la máquina replicada de Orfeo (INR0233_INFOTIC_REP) durante los días 18, 20, 28, 30 y la maquina replicada de portal transaccional (INR0236_INFOTIC_REP) durante los días 28, 29 los cuales fueron corregidos y se continuo normalmente la replicación en los días siguientes.

4.2.2 Dataguard BBDD Megacenter

Durante el mes de septiembre de 2024 se continuo con la replicación permanente de las BD Oracle al Datacenter alerno de acuerdo con las políticas establecidas, utilizando el Oracle Active 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 Septiembre.pdf](#)

```

10.1.18.120 - Conexión a Escritorio remoto
oracle@cxvodacontg011:~
[oracle@cxvodacontg011 ~]$ ps -fe|grep pmon
oracle 4881 1 0 Oct04 ? 00:00:43 ora_pmon_LIFERAYD
grid 6046 1 0 Jul27 ? 00:10:43 asm_pmon_+ASM
oracle 7047 1 0 Jul27 ? 00:24:18 ora_pmon_ICETEXD
oracle 7343 1 0 Jul27 ? 00:24:47 ora_pmon_APOTEOSD
oracle 7736 1 0 Jul27 ? 00:24:25 ora_pmon_APOTNEWD
oracle 8246 1 0 Jul27 ? 00:13:23 ora_pmon_VIGIADTG
oracle 8572 1 0 Jul27 ? 00:13:22 ora_pmon_LANDICTD
oracle 9297 1 0 Jul27 ? 00:24:34 ora_pmon_APLICATD
oracle 10627 9391 0 14:45 pts/2 00:00:00 grep --color=auto pmon
oracle 11890 1 0 Oct04 ? 00:01:02 ora_pmon_ICTXCYCD
[oracle@cxvodacontg011 ~]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.4.0 Production on Mon Oct 7 14:45:34 2024

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

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

SQL> sta fapplyb

Thread Last Sequence Received Last Sequence Applied TIME_RECEIVED TIME_APPLIED
-----
1 71577
2 53348
53348 30/09/2024 14:26 30/09/2024 14:26

SQL> sta uapply

Thread Last Sequence Received Last Sequence Applied Difference
-----
1 71577 71577 0
2 53348 53348 0

```

Ilustración 9 Evidencia Dataguard replicado a Megacenter BD

Se generó la consulta de los archivos recibidos y aplicados de la base de datos de ICTXCYCD a 30/09/2024 14:27 con diferencia cero (0) archivos sin aplicar, lo cual es evidencia que la replicación se encuentra sincronizada.

4.2.3 Replicación Servicios OnPremise de ICETEX a Megacenter

A continuación, se presentan la imagen de la replicación realizada de los servicios OnPremise en ICETEX hacia el Datacenter alternativo Megacenter (Medellín).

Sin embargo, se aclara que esta replicación no es administrada por INFOTIC y se incluye de manera informativa dado que el server está sólo en colocación en los Datacenter de CLARO.

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

Replication of DSDCP_AD01

Edit Settings | Pause | Source Volume | Destination Volume | Set Threshold Alert Definitions | Save Restore Point | Delete

Source SAN Array: Storage Center 35716 PRINCIPAL
Source Volume: DSDCP_AD01
Destination SAN Array: Storage Center 35804 ALTERNO
Destination Volume: Repl of DSDCP_AD01

Ilustración 10 Evidencia replicado servicios OnPremise ICETEX a Megacenter

4.2.4 Disponibilidad de Servicios de Housing – Datacenter Alterno

A continuación, se presentan los dispositivos alojados en el Datacenter alternativo en Medellín, los cuales estuvieron disponibles todo el mes de septiembre 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 23 Disponibilidad de Servicios de Housing – Datacenter Alterno

4.2.5 Servicios de DRP

Se continúa con las sesiones semanales tanto internas (INFOTIC-CLARO) como con el ICETEX con el fin de coordinar y/o realizar las pruebas preliminares y se ajusta el minutograma final para la prueba test, la cual se definió su ejecución para el viernes 04 de octubre y la cual servirá para medir tiempos, evaluar tareas paralelas y probar los escenarios para la prueba definitiva de la cual aún no se tiene

confirmada la fecha por parte de ICETEX tentativamente seria para el mes de noviembre 2024.

El procedimiento de DRP, primero se establece y a nivel de documentación se puede consultar el minutograma en el siguiente link:

[C1115614_Minutograma ICETEX DRP TEST Ope.xlsx](#)

Este documento está compuesto por las siguientes páginas:

- Explicación del minuto grama: En esta hoja se tiene una corta explicación de cómo se debe diligenciar el minutograma
- Ejecución y plan retorno: En esta hoja esta del detalle de cada una de las actividades a realizar en el DRP.
- Direccionamiento: en esta hoja están relacionada la información de los equipos de cómputo que hacen parte de la ejecución del DRP
- Diagramas: en esta hoja están dos graficas con la ingeniería de detalle que contempla la ejecución del DRP

Es de tener en cuenta que para poder ejecutar el DRP de acuerdo con el documento presentado, se ha tenido la revisión y aprobación por parte del ICETEX en reunión de Comité de cambios.

Dentro de la prueba del segundo semestre del 2024 se incluyó la verificación del RTO y RPO, una vez se ejecute el DRP se presentara en el informe el resultado de estas dos variables, es de aclarar que en el mes de julio se envió un correo donde el operador tecnológico CLARO informaba que técnicamente el menor tiempo que se puede configurar para estas mediciones es de 05 minutos, adicionalmente se revisó con el operador tecnológico CLARO cuales eran los umbrales que se tenían establecidos para estas variables y lograr el cumplimiento del contrato. Lo anterior quedara documentado dentro de los planes de trabajo, antes de proceder a reprogramar la prueba de DRP.

Para el WAF del Datacenter alternativo, se han realizado consultas jurídicas sobre la interpretación dada a las condiciones técnicas presentadas en el contrato entre las entidades ICETEX – INFOTIC, una vez se tengan las conclusiones del análisis se implementará la solución a que haya lugar.

5 SEGURIDAD

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

5.1 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 sin uso.

Para el despliegue de Web Filter de Sophos, se continua a la espera de una sesión con el área de riesgos e infraestructura para socializar el comparativo entregado el mes anterior y poder definir cómo se hará la implementación en base a las pruebas realizadas en meses anteriores. Por parte de seguridad se ha recomendado realizarlo de una manera segmentada por áreas para controlar accesos y las respectivas excepciones que se lleguen a necesitar por cada usuario o área.

Se reitera a ICETEX 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. Respecto a lo anterior, INFOTIC realizará una sesión de trabajo en la cual se van a presentar las alternativas técnicas de solución y los planes de trabajo correspondientes en conjunto con ICETEX.

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.

5.2 Estadísticas Portales

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

En la Ilustración 11 se puede ver que, en el periodo de tiempo analizado, se presenta un promedio de 800 GB de tráfico general hacia los portales protegidos por el FortiWeb Apps Nuevas donde el portal de web.ICETEX.gov.co y www.ICETEX.gov.co fueron los más consultados sobre todo en las semanas 36 a la 39 (02 de septiembre a 29 de septiembre), lo cual es un comportamiento normal para este tipo de transacciones de acuerdo con la actividad de los usuarios y las convocatorias vigentes.

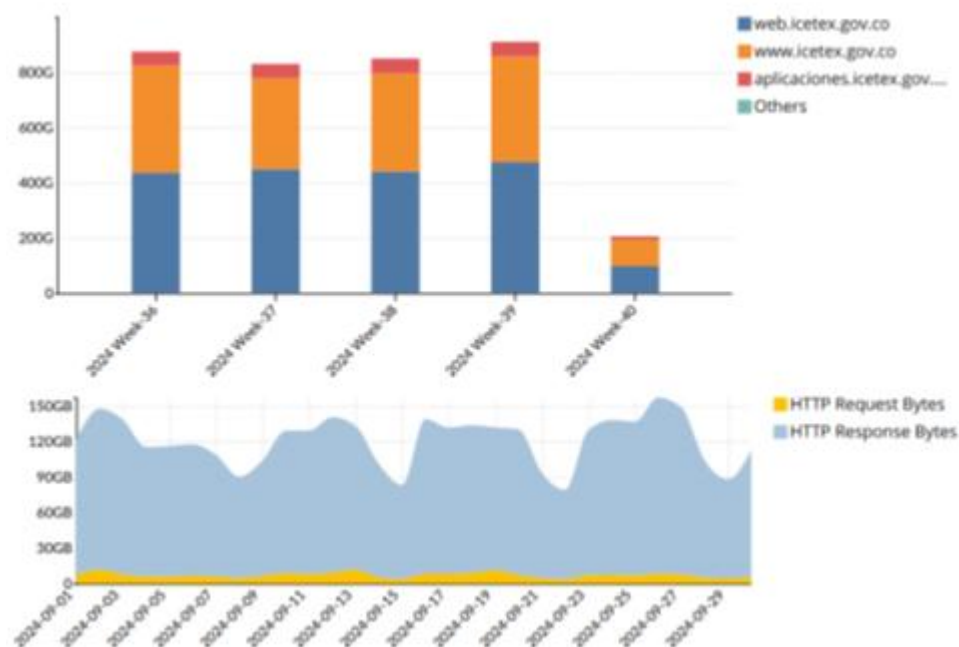


Ilustración 11 Evidencia Gráfica Estadísticas de Portales

5.3 Estado General de las Plataformas

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

En las Ilustraciones 12 a 17 se muestra la información de los firewalls gestionados por INFOTIC y propiedades tales como el Firmware instalado y datos tales como el hostname, ip WAN, etc.

System Information	
Hostname	DC_FG_SLV_ICETEX
Serial Number	FG180FTK22901182 
Firmware	v7.2.9 build1688 (Mature)
Mode	NAT
System Time	2024/10/01 09:24:33
Uptime	44:11:31:43
WAN IP	 2801:192:d::5

Ilustración 12 Estado Plataforma- Seguridad-Perimetral-DC_Principal (FortiGate-Triara)

System Information	
Hostname	DCAGUAS_FG_MST_ICETEX
Serial Number	FG6H0FTB22902021 
Firmware	v7.2.9 build1688 (Mature)
Mode	NAT
System Time	2024/10/01 09:29:35
Uptime	44:11:49:24
WAN IP	 2801:192:0:dd::8c

Ilustración 13 Estado Plataforma- 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	2024/10/01 09:30:37
Uptime	44:11:12:53
WAN IP	 190.145.153.186

Ilustración 14 Estado Plataforma- 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	Tue Oct 1 09:31:50 2024
Firmware Version	FortiWeb-2000F 7.4.4,build0649(GA),240628
System Uptime	[44 day(s) 10 hour(s) 54 min(s)]
Administrative Domain	 Disabled
Threat Analytics 	Start Trial
Advanced Bot Protection 	 Disabled

Ilustración 15 Estado Plataforma 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	Tue Oct 1 09:34:16 2024
Firmware Version	FortiWeb-2000E 7.4.4,build0649(GA),240628
System Uptime	[44 day(s) 10 hour(s) 40 min(s)]
Administrative Domain	Disabled

Threat Analytics

Start Trial

Ilustración 16 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	Tue Oct 1 09:35:58 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	207 day(s) 11 hour(s) 55 minute(s)
Windows VM	[Upload License]
Microsoft Office	[Upload License]
VM Internet Access	
FDN Download Server	
Community Cloud Server	
Web Filtering Server	
Antivirus DB Contract	2023-06-20
Web Filtering Contract	2023-06-20
MTA Contract	No Contract
MacOS VM Contract	No Contract
Industry Security Signature Contract	No Contract

Ilustración 17 Estado General de las Plataformas seguridad-Local-(FortiSandBox)

5.4 Estado de Salud de los Equipos de Seguridad

En el transcurso del mes de septiembre 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 Septiembre 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 97.67 Mbps (Port7) en la última semana.

Imagen 12 Consumo Del Canal

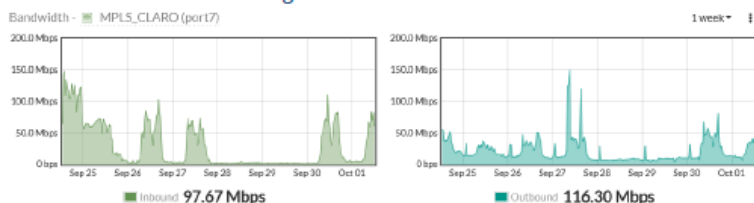


Ilustración 18 Evidencia Estado de Salud de los Equipos de Seguridad

5.5 Servicio de centro de Operaciones de Seguridad (SOC)

Durante el mes de septiembre 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 Septiembre 2024.pdf](#)

En la ilustración 19, se puede ver la forma de presentación de la información del Informe mensual del SOC en el cual se presentan gráficas y tablas de los tipos de alertas presentados durante el periodo monitoreado tanto de: Seguridad – Disponibilidad – Rendimiento, donde estos a su vez se encuentran distribuidos con niveles de severidad con tres colores:

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

3.1.1 Casos de Uso Seguridad

Se encuentran definidas 2.429 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.

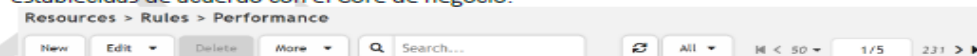


Ilustración: Cantidad de reglas de Rendimiento

Ilustración 19 Evidencia Imagen Reporte Monitoreo

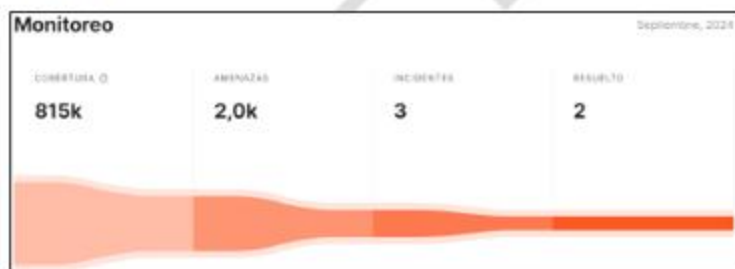
5.5.1 Monitoreo de Marca-Estrategia OSINT-SOC

Para el mes de septiembre 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 Septiembre 2024.pdf](#)

4. ANÁLISIS DE MONITOREO DE PROTECCIÓN DE MARCA Y OSINT

Durante el periodo evaluado, la plataforma de monitoreo de protección de marca y OSINT – AXUR, reporta un total de 2,0k posibles amenazas de las 815k que fueron encontradas y analizadas automáticamente por la plataforma de monitoreo. A estas 2,0k 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 20 Evidencia Imagen Reporte Monitoreo OSINT

Durante el periodo evaluado se detectaron 03 incidentes, 01 relacionado con producto falso o venta irregular, 01 relacionado con perfil falso en red social y 01 relacionados con Phishing.

5.5.1.1 Casos relacionados con Fraudes Digitales

Durante el periodo evaluado, se presentaron 40 casos, de los cuales 39 fueron descartados, teniendo en cuenta que algunos no tenían relación y otros solo mencionaban la entidad y 01 caso se reportó a la entidad y se encuentra resuelto.

5.5.1.2 Casos relacionados con Fuga de Datos

Durante el periodo evaluado, se presentaron 70 casos, de los cuales todos fueron descartados, teniendo en cuenta que algunos no tenían relación con la entidad o solo se hacía mención de esta.

5.5.1.3 Casos relacionados con el módulo Piratería Online

Durante el periodo evaluado, se presentaron 1.836 casos, de los cuales 01 caso fue reportado a la entidad y se encuentra resuelto, y 1.835 casos fueron descartados, teniendo en cuenta que eran casos relacionados con producto falso o venta irregular y solo se hacía mención al nombre de la

marca, pero al analizarlos no se tenía relación con la entidad ya que “ICETEX” corresponde al nombre de una marca de colchones, pero la plataforma lo asocia con el de la entidad, por lo tanto, estos casos fueron descartados y cerrados. Debido a la cantidad de casos descartados nos comunicamos con el equipo de soporte de la plataforma Axur, para reconfigurar los bots de búsqueda y que no se sigan detectando estos casos para reducir el número de falsos positivos.

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

Durante el periodo evaluado, se presentó 12 casos relacionados con la Deep & Dark Web, los cuales fueron descartados, teniendo en cuenta que solo se hacía mención de la marca en forma de burla o en algunos casos no tenía relación con la entidad.

5.5.1.5 **Casos Reportados a la entidad**

Durante el periodo evaluado se reportó 3 casos a la entidad, de los cuales a todos se les realizó la gestión correspondiente y hoy en día se encuentran solucionados.

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

5.6 **Eventos Relevantes**

- Con 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. Se detectaron 64 direcciones IP catalogadas como maliciosas y de las cuales se hizo un bloqueo del 100% en los dispositivos de seguridad perimetral y consola de antivirus, esto gracias a los reportes entregados por el SOC y amenazas detectadas en fuentes de información confiable.
- Se ha venido trabajando en la implementación de direccionamiento IPv6 apoyando al área de Networking en esta actividad configurando accesos a sedes sobre este protocolo. En este mes se alcanzaron las sedes de Popayán, Cúcuta, Arauca, Apartado, Mocoa, Chapinero, Riohacha y Tumaco por IPv6 pasando por el canal MPLS que interconecta estas sedes.
- Se ha venido realizando restricciones de conexiones desde direcciones IP que debido a su geolocalización puedan presentar algún riesgo y restringiendo acceso público a puertos que se muestran sobre el direccionamiento IPv4 público de la entidad como es BGP, VPN IPSec, etc
- Integración por agente del directorio activo con ip 192.168.51.101 al FortiSIEM con el objetivo de obtener información del directorio activo y observar el comportamiento para la instalación de los otros servers.
- Se ha escalado a la alta gerencia la falencia o falta de recursos de la herramienta de FortiSIEM, y la importancia ya que son los ojos ante cualquier amenaza o intruso en la seguridad informática del ICETEX.

- Se han realizado sesiones con recomendaciones de seguridad, con el objetivo de fortalecer puntos de fallo para que la entidad tome decisiones a nivel gerencial sobre sus riesgos.
- Se ha avanzado en el comité de Logs ya que se está solicitando más información y ya temas más puntuales lo cual nos indica que estamos madurando en este comité.

5.7 Recomendaciones

5.7.1 Recomendaciones Generales

- 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 negado o permitido el tráfico.
- 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.
- 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) y 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 Piratería Online – Producto falso o Venta Irregular recordar las medidas a considerar: Verificar la venta publicada si se trata de un producto o venta falso o si corresponde y es propiedad de la entidad., en caso de que se trate de ventas falsas informar si es necesario solicitar un Takedown, si estos productos o ventas están autorizados o no representa un Fraude digital, responder el correo para marcar los tickets como Cerrado: Resuelto.

5.7.2 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, líderes del componente de Seguridad Informática, designados por la supervisión.	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 sigue a la 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. Se está a la espera de una sesión para implementar LDAP seguro con certificado y que este sea compartido por ICETEX para aplicarlo en el firewall y fortalecer la capa de seguridad con respecto a la autenticación de usuarios.	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, como acceso adicional en caso de que se presente alguna falla por el canal dedicado de MPLS.	En evaluación por parte de seguridad del ICETEX.	Baja
Realizar la contención automática de equipos que se identifiquen en la red como maliciosos	En evaluación por parte de ICETEX.	Media
Realizar el aumento de recursos a la plataforma de FortiSIEM (CPU, Memoria y disco) y hacer un cambio de arquitectura con el objetivo de mejorar.	En evaluación por parte de ICETEX.	Alta
Se debe evaluar la mejor forma a nivel de seguridad la conmutación hacia Medellín generando el menor costo de tiempo.	Se está evaluando y los ejercicios de prueba test y DRP nos orientaran sobre el ejercicio.	Baja

Tabla 24 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 aplicaciones de ICETEX	En evaluación por parte de ICETEX.	Alta
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.	Crítica
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
Se debe realizar la integración de los activos críticos de la compañía a la plataforma de SIEM, no se ha podido lograr por la falta de recursos de este.	En evaluación por parte de ICETEX.	Alta

Tabla 25 Recomendaciones de seguridad para ICETEX

5.8 Conclusiones

- La implementación de políticas para BYOD (Bring Your Own Device) refuerza la seguridad al integrar dispositivos personales de manera controlada, lo que ayuda a mitigar riesgos como la pérdida de datos, accesos no autorizados y vulnerabilidades causadas por la diversidad de dispositivos.

- El uso de herramientas de monitoreo mejora la capacidad de detectar y responder rápidamente a eventos anómalos o maliciosos, facilitando una identificación temprana y reduciendo los tiempos de respuesta ante incidentes de seguridad.
- La gestión eficiente de credenciales de usuario reduce de manera notable el riesgo de incidentes graves de seguridad, al asegurar una autenticación confiable y un adecuado control de los privilegios de acceso.
- La implementación de FSSO es crucial para limitar la navegación en áreas específicas, disminuyendo el riesgo de acceso a sitios que podrían comprometer la seguridad de la infraestructura y de los usuarios de la Entidad.
- La adopción de IPv6 en la red trae consigo numerosas ventajas, como una mayor capacidad de direccionamiento, mejoras en la eficiencia del enrutamiento y soporte para nuevas tecnologías, lo que contribuye a una infraestructura más escalable y segura.
- La aplicación de controles adicionales de acceso fortalece la seguridad de la Entidad, minimizando el impacto de posibles incidentes y reforzando la protección frente a amenazas potenciales.
- Los reportes del SOC han sido determinantes en la reducción de vectores de ataque. La detección oportuna de eventos inusuales ha permitido bloquear posibles amenazas y salvaguardar la infraestructura de la Entidad.
- La optimización de las políticas de seguridad ha permitido gestionar el tráfico hacia los dispositivos de seguridad perimetral de manera más eficiente, garantizando que solo los segmentos de red y puertos necesarios para la operación estén accesibles.
- Para el WAF de la data center alternativo, se han realizado consultas jurídicas sobre la interpretación dada a las condiciones técnicas presentadas en el contrato entre las entidades ICETEX – INFOTIC, una vez se tengan las conclusiones del análisis se implementará la solución a que haya lugar.
- Para el para sistemas operativos obsoletos, se han realizado consultas jurídicas sobre la interpretación dada a las condiciones técnicas presentadas en el contrato entre las entidades ICETEX – INFOTIC, una vez se tengan las conclusiones del análisis se implementará la solución a que haya lugar.
- Para el SIEM se buscará realizar una sesión entre INFOTIC – WEXLER e ICETEX para analizar las recomendaciones presentadas por el grupo de seguridad de INFOTIC para aumentar el preforma de la máquina para mejorar el funcionamiento y desempeño de este componente.

6 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.

6.1 Actividades De Operación

Para el presente periodo evaluado, que corresponde al mes de septiembre, 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 SEPTIEMBRE.pdf](#) el cumplimiento a satisfacción de las funciones que deben gestionar cada uno de estos contratados para el desarrollo del presente contrato.

6.2 Profesionales Especializados.

El detalle de las actividades realizadas por cada uno de los ingenieros especialistas se puede consultar en el [INFORME MENSUAL SEPTIEMBRE.pdf](#)

6.2.1 Especialista en Base de Datos DBA

El proyecto cuenta con dos DBA que permiten cubrir y dar solución a los diferentes requerimientos que el ICETEX realiza en marcadas en:

- **Funciones Básicas Especialista Bases de Datos ICETEX:** Se presenta un informe anexo con la información sobre las actividades que realizan en el desarrollo de sus funciones.
- **Informes Requeridos:** Se presentan informes adicionales y de acuerdo con las necesidades del servicio durante cada periodo evaluado teniendo en cuenta la gestión del servicio y la disponibilidad de las bases de datos que el ICETEX requiere, dentro de estos se tiene las evidencias del Dataguard, Informe de replicación,
- **Tareas de administración:** Mediante herramientas tecnológicas como el “ELASTIC” se tiene configuradas alertas que permiten prevenir indisponibilidades del servicio con consumos elevados realizando acciones administrativas para evitar estos eventos.
- **Gestión operativa.** Manejo de incidentes y problemas: Los dos especialistas reciben mediante Aranda las notificaciones y de la misma forma se retroalimenta sobre las acciones realizadas y los soportes correspondientes.
- **Mejores prácticas en el mantenimiento de bases de datos, enfocada en:** dentro de las acciones de administración y el monitoreo realizadas sobre las bases de datos se aplican las mejores prácticas para el uso y manejo de las bases de datos del ICETEX.

6.2.2 Especialista Web Master

El proyecto cuenta con un WEB MASTER que permite cubrir y dar solución a los diferentes requerimientos que el ICETEX realiza en marcadas en:

- **Funciones básicas:** Se presenta un informe anexo con la información sobre las actividades que realizan en el desarrollo de sus funciones.
- **Informes:** Se presentan informes adicionales y de acuerdo con las necesidades del servicio durante cada periodo evaluado teniendo en cuenta la gestión del servicio y la disponibilidad de las bases de datos que el ICETEX requiere, dentro de esto se tiene reporte de monitoreo, Prueba TEST,

6.2.3 Administrador de Soluciones

El proyecto cuenta con dos especialistas de soluciones que permiten cubrir y dar solución a los diferentes requerimientos que el ICETEX realiza en marcadas en:

- **Funciones básicas:** Se presenta un informe anexo con la información sobre las actividades que realizan en el desarrollo de sus funciones.
- **Informes:** Se presentan informes adicionales y de acuerdo con las necesidades del servicio durante cada periodo evaluado teniendo en cuenta la gestión del servicio y la disponibilidad de las bases de datos que el ICETEX requiere, dentro de estos se tiene el informe de backup

6.2.4 Especialista en Networking

El proyecto cuenta con dos especialistas de networking que permiten cubrir y dar solución a los diferentes requerimientos que el ICETEX realiza en marcadas en:

- **Funciones básicas:** Se presenta un informe anexo con la información sobre las actividades que realizan en el desarrollo de sus funciones.
- **Informes, entregables o productos de la asesoría en networking:** Se presentan informes adicionales y de acuerdo con las necesidades del servicio durante cada periodo evaluado teniendo en cuenta la gestión del servicio y la disponibilidad de las bases de datos que el ICETEX requiere, dentro de los cuales se tiene pruebas de saturación, informe de disponibilidad, consumo de canales, ANS de canales,

6.2.5 Especialista Integrador De Nube

El proyecto cuenta con un especialista en NUBE que permite cubrir y dar solución a los diferentes requerimientos que el ICETEX realiza en marcadas en:

- **Funciones Especialista Integrador de nube:** Se presenta un informe anexo con la información sobre las actividades que realizan en el desarrollo de sus funciones.

6.2.6 Especialista En Seguridad

El proyecto cuenta con dos especialistas en plataforma de seguridad informática que permiten cubrir y dar solución a los diferentes requerimientos que el ICETEX realiza en marcadas en:

- **Funciones básicas:** Se presenta un informe anexo con la información sobre las actividades que realizan en el desarrollo de sus funciones.
- **Informes, entregables o productos de la asesoría en seguridad informática:** Se presentan informes adicionales y de acuerdo con las necesidades del servicio durante cada periodo evaluado teniendo en cuenta la gestión del servicio y la disponibilidad de las bases de datos que el ICETEX requiere, dentro los cuales se tiene, el informe de marca, el informe del SOC, informe de vulnerabilidades, reporte de IPS.

7 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:

ÍTEMS	SERVICIO	CIUDAD	DIRECCIÓN	CANTIDAD
1	Sala de video conferencia o sala virtual (Tamaño 65")	Bogotá - Aguas	Carrera 3 No. 18-32	3
2	Sala de video conferencia o sala virtual (Tamaño 65")	Bogotá - Ángel	Cl. 19 #6-68 piso 17	1
3	Sala de video conferencia o sala virtual (Tamaño 55")	Bogotá - Aguas	Carrera 3 No. 18-32	1
SEDES REGIONALES				
4	Sala de video conferencia o sala virtual (Tamaño 55")	Bogotá - Chapinero	Calle 57 No. 8-69 Local 46 - 48 y 50	1
5	Sala de video conferencia o sala virtual (Tamaño 55")	Barranquilla	Calle 70 #53-74 piso 3	1
6	Sala de video conferencia o sala virtual (Tamaño 55")	Bucaramanga	CR 29 # 45 - 45, Ofi. 703	1
7	Sala de video conferencia o sala virtual (Tamaño 55")	Cali	Calle 5 No. 66B - 67, Centro Cultural El Capitolio – Piso 3	1
8	Sala de video conferencia o sala virtual (Tamaño 55")	Medellín	Calle 52 No. 47-42 Piso 10 Ofi. 1002	1

Tabla 26 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 pasado mes de septiembre 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.

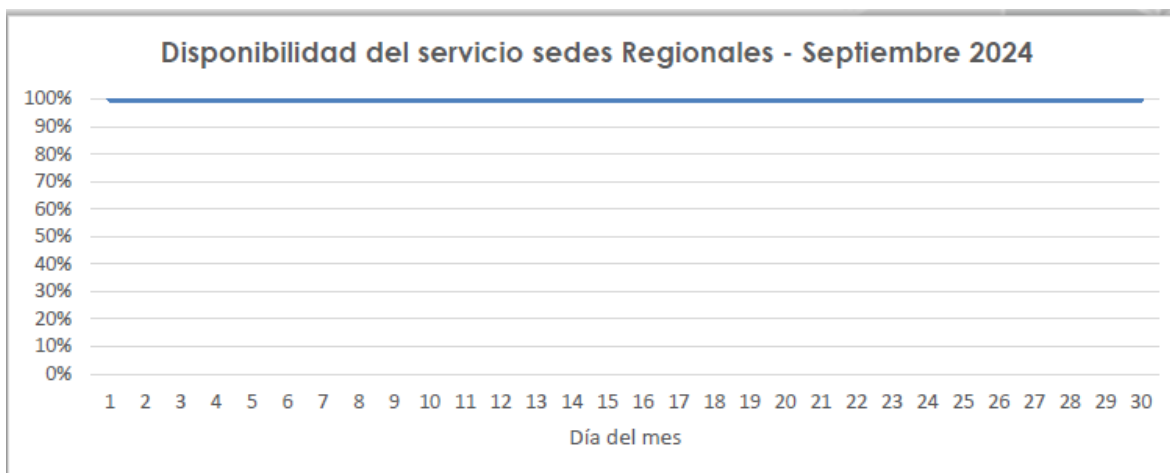


Ilustración 21 Disponibilidad de servicio videoconferencia sedes regionales – septiembre 2024

7.1 Disponibilidad Del Servicio – Sedes Bogotá (Aguas - Ángel)

En la verificación realizada en el mes de septiembre 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.

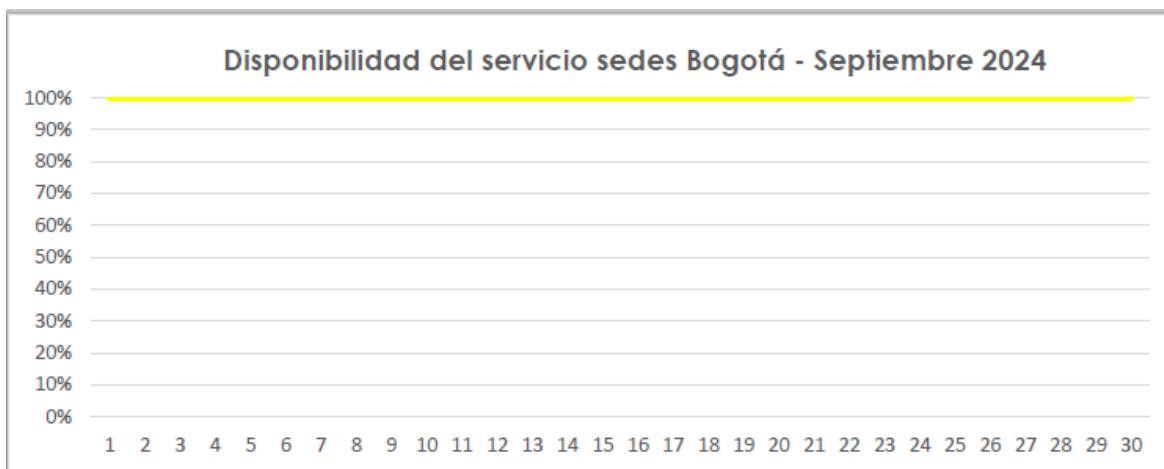


Ilustración 22 Disponibilidad de servicio videoconferencia sedes Bogotá –septiembre 2024

7.2 Gestión De Incidencias Y Requerimientos – Sedes Regionales

Para el periodo comprendido entre el 1 y el 30 de septiembre, en las sedes Regionales (Cali, Barranquilla, Bucaramanga y Medellín) no se generaron solicitudes especiales que requirieran atención y gestión de soporte técnico, se atendió un (1) requerimiento para revisión y pruebas de funcionamiento para la sede de Chapinero; No 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.

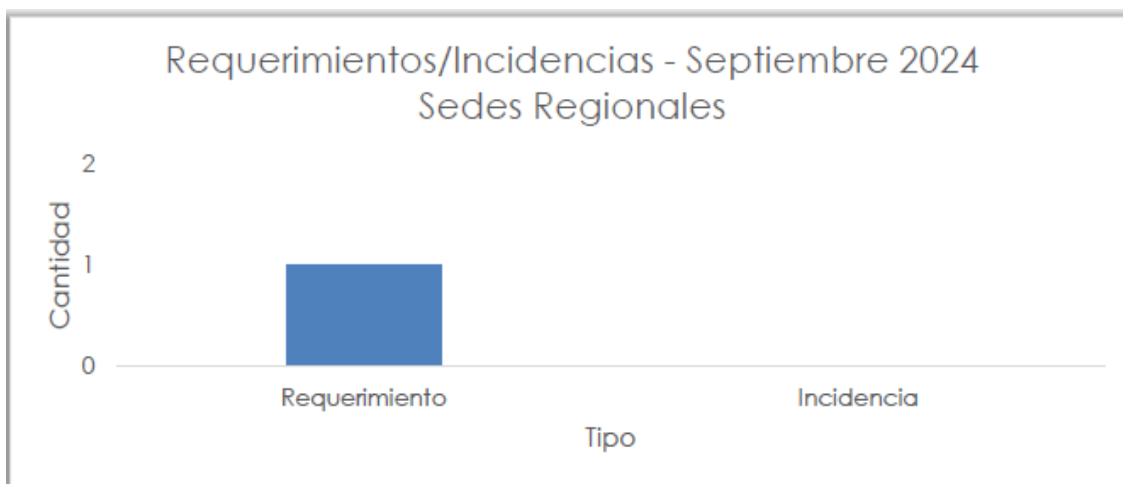


Ilustración 23 Incidencias/Requerimientos sedes Regionales – septiembre 2024

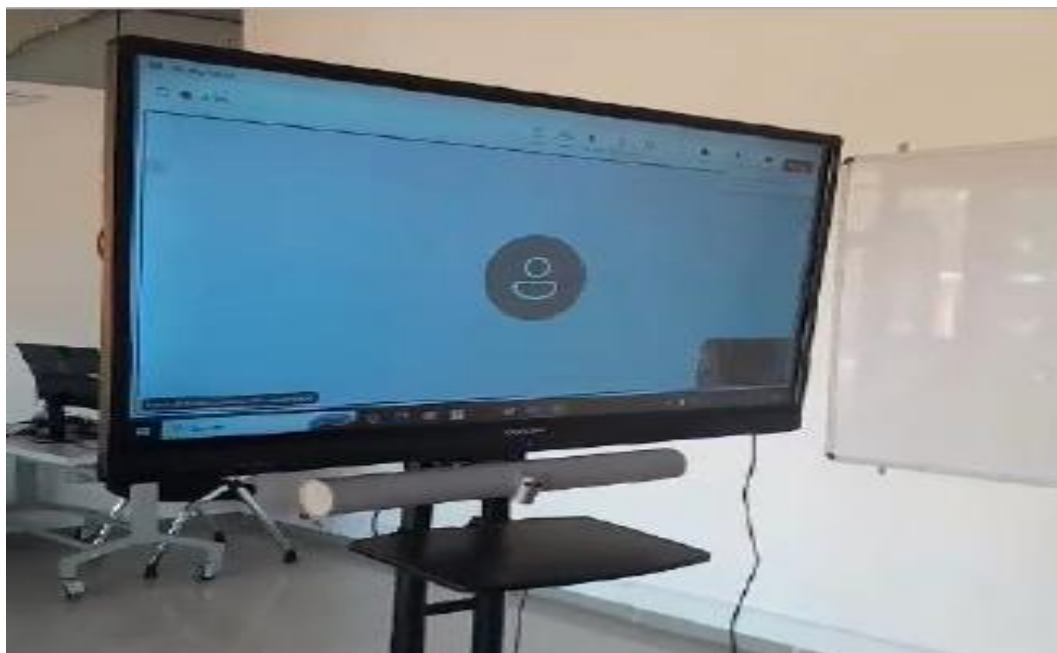


Ilustración 24 Evidencia módulo funcional sede Chapinero – Septiembre 2024

7.3 Gestión De Incidencias Y Requerimientos – Bogotá (Aguas - Angel)

Para el periodo comprendido entre el 1 y el 30 de septiembre, para las sedes de Bogotá Aguas y Ángel, se generó un (1) un requerimiento para revisión y pruebas de funcionamiento de los módulos instalados en Aguas y Ángel, solicitud que fue atendida y cerrada. No se recibieron requerimientos especiales adicionales para 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.

En la visita realizada a la sede de Aguas y Ángel, con la persona que está realizando apoyo técnico para revisión de los equipos, se realizaron pruebas de funcionamiento, revisiones del módulo y los ajustes requeridos para descartar incidencias para garantizar continuidad del servicio, sin embargo, no se encontraron 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-282611-8-20461.

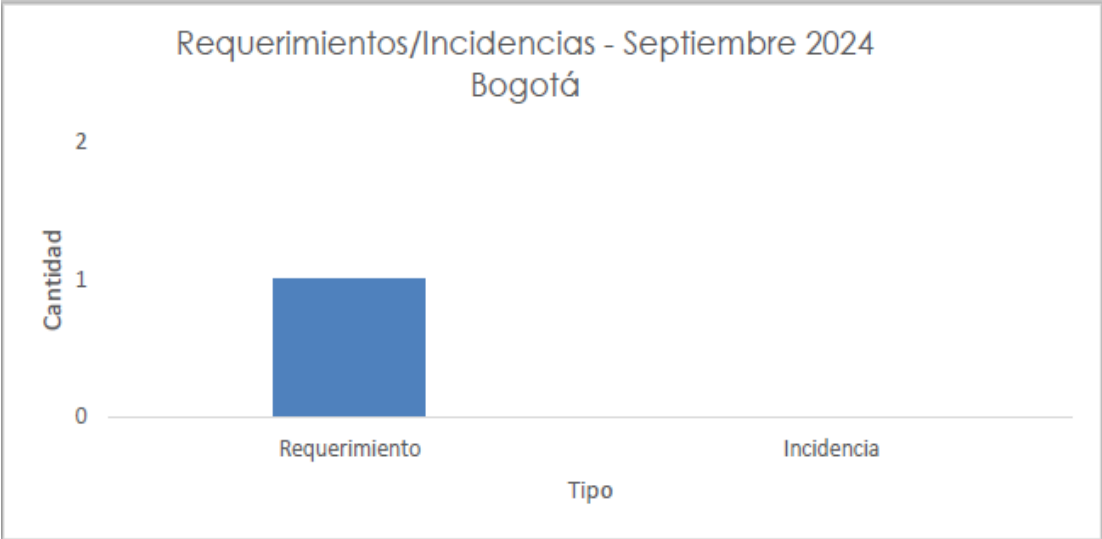


Ilustración 25 Incidencias/Requerimientos sedes Bogotá – septiembre 2024



Ilustración 26 Evidencia módulo funcional sede Aguas 65”, piso 2 – septiembre 2024

Al igual que en el piso 2, se realizan pruebas de funcionamiento en el módulo del piso 4 para validar el funcionamiento normal del servicio.

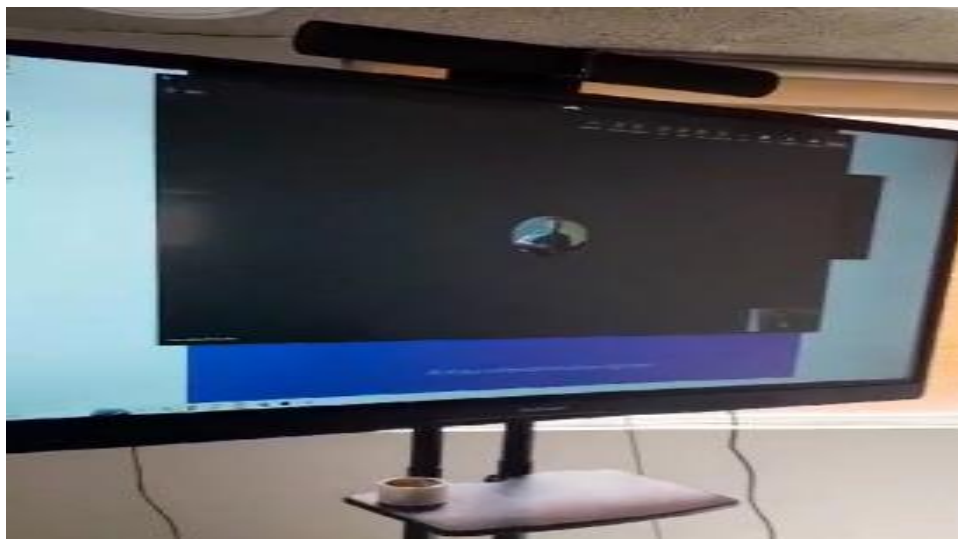


Ilustración 27 Prueba de funcionamiento OPS módulo 65" sede Aguas, piso 4 – Sep 2024

Posterior a las pruebas realizadas, se verifica funcionamiento correcto en los módulos de los pisos 2 y 4 como se evidencia en las imágenes 26 y 27, Además se verifica funcionamiento de los módulos ubicados en los demás pisos de la sede Aguas, al igual que en el módulo de la sede Ángel. Se adjuntan a presente informe algunos videos de evidencia de las pruebas realizadas.



Ilustración 28 Módulo sede Aguas piso 8 (Presidencia) – Septiembre 2024

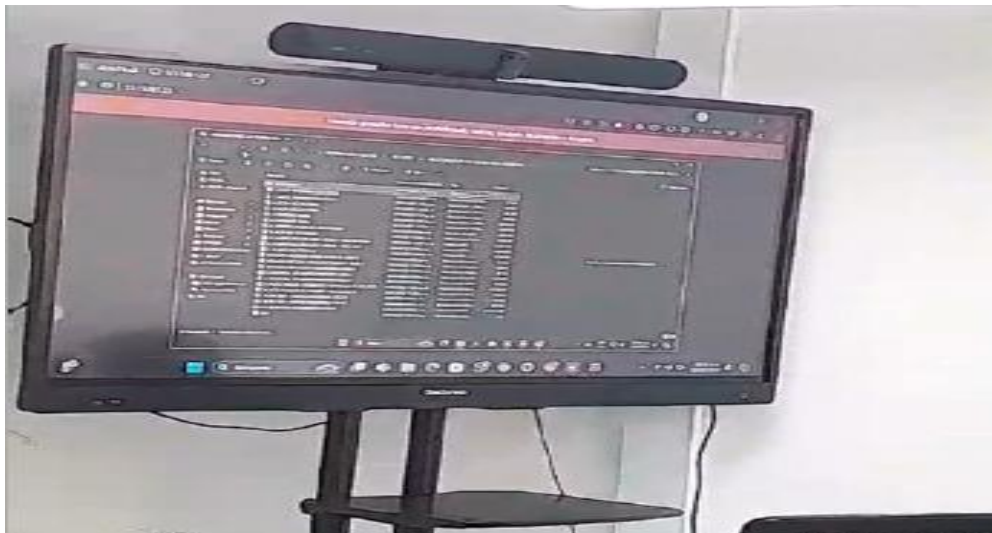


Ilustración 29 Verificación sede Aguas, piso 6 (módulo móvil) septiembre 2024

Por último, se realiza la revisión del módulo instalado en sede Ángel, que se encuentra funcional como se muestra en la siguiente imagen.

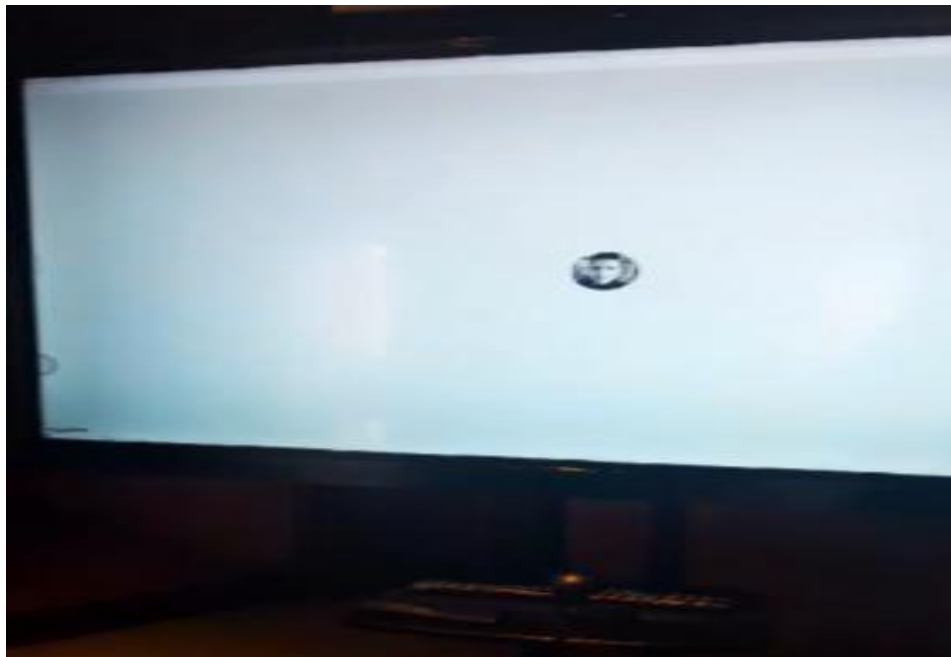


Ilustración 30 Verificación módulo sede Ángel - septiembre 2024

https://icetex.sharepoint.com/:b:/r/sites/Infraestructura/Documentos compartidos/DATACENTER INFOTIC/Ejecucion INFOTIC/17_Agosto 2024/Evidencias Agosto/Videoconferencia/Informe Agosto 2024 Servicio Video Conferencia.pdf?csf=1&web=1&e=5ugMNI

7.4 Proyección Plan De Mantenimiento Módulos De Videoconferencia Vigencia 2025

Para la vigencia del servicio 2025, teniendo en cuenta el volumen de incidencias y requerimientos que se presentan mensualmente, y el estado actual de los equipos, se tiene proyectado continuar

con revisiones mensuales de los módulos en las sedes de Bogotá Aguas y Ángel como se viene realizando durante la vigencia actual, y en general se proyecta realizar y coordinar mantenimientos preventivos semestrales sobre los módulos de videoconferencia instalados en las sedes Bogotá y en las sedes Regionales, con el fin de garantizar el buen funcionamiento de los módulos por ende la continuidad del servicio en general.

Durante el periodo de septiembre se garantizó estabilidad y continuidad del servicio de módulos de videoconferencia en las diferentes sedes de la entidad. Adicional, se atendió el requerimiento para realizar pruebas de funcionamiento de todos los módulos instalados en las sedes de Bogotá, donde se validó el funcionamiento correcto de cada módulo.

Por otro lado, en aras de garantizar continuidad del servicio en caso de que se presenten incidentes de funcionamiento con algún módulo, se cuenta con una OPS de backup (para la cual se validó funcionamiento en los módulos) con el fin evitar periodos largos de indisponibilidad de servicio, en caso de que se presenten incidentes de funcionamiento en los equipos, permitiendo remplazar la OPS que se presente alguna incidencia con la de backup en tanto se realiza la revisión pertinente.

Durante el periodo de septiembre se realizaron las siguientes actividades relacionadas al servicio de módulos de videoconferencia:

- Pruebas de funcionamiento módulos Aguas, Ángel y Chapinero
- Prueba de funcionamiento OPS backup
- Inicio de gestión administrativa y operativa para realizar revisión y mantenimientos preventivos de módulos en sedes Regionales (Barranquilla, Bucaramanga, Medellín y Cali)
- Informe mensual de operación del servicio

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

Para la vigencia del servicio 2025, teniendo en cuenta el volumen de incidencias y requerimientos que se presentan mensualmente, y el estado actual de los equipos, se tiene proyectado continuar con revisiones mensuales de los módulos en las sedes de Bogotá Aguas y Ángel como se viene realizando durante la vigencia actual, y en general se proyecta realizar y coordinar mantenimientos preventivos semestrales sobre los módulos de videoconferencia instalados en las sedes Bogotá y en las sedes Regionales, con el fin de garantizar el buen funcionamiento de los módulos por ende la continuidad del servicio en general.

Durante los últimos 03 meses se presentaron los siguientes requerimientos y/o incidentes durante la prestación del servicio de videoconferencia:

	Julio	Agosto	Septiembre
Requerimiento	0	0	2
Incidentes	0	0	0

Tabla 27 Distribución trimestral de requerimientos y/o incidentes

Se presentaron 2 requerimientos en el mes de septiembre para las sedes de Bogotá, las cuales contemplaban la revisión y pruebas sobre los equipos disponibles en cada una de las sedes, se

atendieron de forma inmediata y se confirmó que todo estaba funcionando correctamente.

8 Cálculo De Conciliación De Los Servicios Del Mes De Septiembre

A la fecha la conciliación del mes de septiembre con ICETEX se encuentra en proceso, el detalle de conciliación del mes anterior se puede ver en el siguiente link [Conciliación Septiembre 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						\$ 11.369.567.913
Pago No. 1 -	mes:	Abril	de	2023	\$ 537.090.736,00	
Pago No. 2 -	mes:	Mayo	de	2023	\$ 544.104.546,00	
Pago No. 3 -	mes:	Junio	de	2023	\$ 596.978.314,00	
Pago No. 4 -	mes:	Julio	de	2023	\$ 624.431.841,60	
Pago No. 5 -	mes:	Agosto	de	2023	\$ 650.825.466,00	
Pago No. 6 -	mes:	Septiembre	de	2023	\$ 661.959.450,00	
Pago No. 7 -	mes:	Octubre	de	2023	\$ 641.792.285,00	
Pago No. 8 -	mes:	Noviembre	de	2023	\$ 630.348.564,00	
Pago No. 9 -	mes:	Diciembre	de	2023	\$ 663.076.196,00	
Pago No. 10 -	mes:	Enero	de	2024	\$ 681.934.328,00	
Pago No. 11 -	mes:	Febrero	de	2024	\$ 732.950.101,55	
Pago No. 12 -	mes:	marzo	de	2024	\$ 733.890.372,09	
Pago No. 13 -	mes:	abril	de	2024	\$ 730,351,368.00	
Pago No. 14 -	mes:	mayo	de	2024	\$ 719,104,204.57	
Pago No. 15 -	mes:	junio	de	2024	\$ 713,673,218.00	
Pago No. 16 -	mes:	Julio	de	2024	\$ 751,372,731.00	
Pago No. 17 -	mes:	agosto	de	2024	\$ 755,684,192.00	
VALOR CAUSADO QUE NO SE HA PAGADO (valor a pagar factura) *						\$ 0
VALOR TOTAL EJECUTADO (valor pagado + valor causado no pagado)						\$ 11.369.567.913
SALDO DEL CONTRATO (valor total del contrato – valor total ejecutado)						\$ 18.516,866,974
PORCENTAJE DE EJECUCIÓN						41.03%
* 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 28 Ejecución Presupuestal

9 RECOMENDACIONES

Las siguientes son las recomendaciones para el mes de septiembre que desde cada servicio de especialistas asignados al proyecto ICETEX realizan para mejorar los diferentes ámbitos:

Backups:

- Para el correcto funcionamiento del almacenamiento de Backup, se recomienda que el ICETEX realice la entrega programada de las cintas de Backup para proceder realizar el descargue de los archivos de los equipos proveedor de tecnología, pasarlos a cinta y posterior traslado a custodia externa.
- Contemplar la opción de enviar a la nube las copias de seguridad históricos que se encuentran en la custodia externa para realizar reducción de costos y dar aprovechamiento de nube existente.

Networking

- Renovación de Equipos: Se sugiere llevar a cabo la actualización de los equipos de la entidad, ya que muchos de ellos se encuentran obsoletos y carecen de soporte por parte del fabricante, lo que podría afectar el rendimiento y la seguridad de la infraestructura.
- Reemplazo de Equipos Dañados: Durante este mes, se reportó un daño en uno de los equipos en la sede de San Andrés, el cual fue reemplazado por otro dispositivo del ICETEX. Sin embargo, se debe notificar a ICETEX que actualmente no hay disponibilidad de equipos adicionales para reemplazos futuros en caso de que surjan nuevos daños, es recomendable que ICETEX adquiera equipos para que se envíen a sedes lejanas como Iquitos y San Andrés equipos en lo posible nuevos para disminuir el riesgo de que dañen tan rápido.
- Renovación y Certificación de Cableado: Se recomienda realizar una renovación o sustitución del cableado en diversos puntos de la entidad, dado que la infraestructura de cableado es muy antigua. Se sugiere también llevar a cabo una certificación del nuevo cableado para garantizar su calidad y desempeño.
- Mantenimiento de Infraestructura: Considerando el estado actual de la infraestructura en las sedes, es crucial llevar a cabo un mantenimiento integral de los equipos y del cableado, así como proceder a la renovación de los dispositivos de red, para asegurar un funcionamiento óptimo y prevenir fallas futuras.

Aplicaciones

- Se recomienda a los usuarios finales que a pesar de que se les da atención a todas las solicitudes, estas se deben gestionar a través de la mesa de servicio de Aranda, ya que todavía existen casos que se atienden sin haber un registro de estos.
- Las aplicaciones que estén en Framework .Net Classic que sean migradas a un Framework más actual y soporte.
- Que las aplicaciones que estén implementadas en sistemas operativos obsoletos sean migradas a Servidores con sistemas operativos de versiones actuales y con soporte de Microsoft.
- Se recomienda que cada aplicación web debe tener su respectivo servidor.

Para portal Web Icetex:

- Igualar las condiciones de infraestructura entre el nodo 1 y el nodo 2 que permitirá realizar un mejor balanceo de los servicios solicitados por los diferentes usuarios que acceden a los servicios del ICETEX.
- Tener un ambiente de pruebas igual al ambiente productivo para que las pruebas que se ejecuten sean reales y reducir los tiempos utilizados en las modificaciones necesarias para pasar de pruebas a productivo.
- Realizar la actualización del sistema operativo LINUX de tienen las maquinas a la última versión liberada por el fabricante
- Realizar la actualización del liferay de tienen las maquinas a la última versión liberada por el fabricante

Integración NUBE

- Contar con accesos a Azure, como también, a la sección de análisis de costos para futuras validaciones y/o recomendaciones.
- Definir procedimientos y cronograma para la creación de futuros recursos masivos, en este caso, VMs si es el caso.
- Continuar con la remediación de hallazgos y la implementación de los tags solicitados para tener un mayor seguimiento sobre los recursos y su monitoreo.
- Levantar la información pendiente para comprender las necesidades, solicitantes, aprobadores y finalmente, justificaciones de lo existente, la entidad debe contar con una documentación e inventario de todo lo que existe en la nube como también, aplicaciones de la entidad.

- Los tags en las Nubes son indispensables para llevar a cabo seguimiento y ejecución en políticas de eliminación de recursos.

Bases de datos

- Se deben aumentar los espacios del área de recuperación de las bases de datos productivas de 1TB a 5TB para tener una retención de 10 días o más, con el TB de almacenamiento provisionado solo se puede mantener 2 días por BD.
- El antivirus de Symantec en las bases de datos sigue inactivo hasta no tener claro las parametrizaciones de restricción y los problemas ocasionados de conexión.
- Sigue pendiente retirar el permiso sudo a los usuarios infotic, gawuser y dcscsf, pues permite realizar actividades administrativas que no van con su rol.

Seguridad

- 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.
- Se debe segmentar las políticas de acuerdo con la necesidad y no otorgar acceso de toda una red o todos los servicios.
- Se debe trabajar en el perfilamiento de la navegación de acuerdo con lo entregado por ICETEX.
- Validar la autenticación de doble factor para todas las plataformas misionales del ICETEX. Continuamos a la espera de respuesta de la entidad.
- Realizar autenticación a través del LDAPS, para la gestión de las plataformas de seguridad.
- Validar la posibilidad de la integración de la consola Sophos con SIEM.
- Validar la posibilidad de la integración de una VPN para la gestión desde DT alternativo Medellín como acceso adicional en caso de que se presente alguna falla por el canal dedicado de MPLS. Continuamos a la espera de respuesta de la entidad.
- Realizar la contención automática de equipos que se identifiquen en la red como maliciosos. Continuamos a la espera de respuesta de la entidad.
- Realizar el aumento de recursos a la plataforma de FortiSIEM (CPU, Memoria y disco) y hacer un cambio de arquitectura con el objetivo de mejorar.
- Garantizar la segmentación de la red que permita claramente definir qué servicios deben ser alcanzados por cada usuario.
- Se recomienda una tecnología que permita realizar análisis de tráfico de la red (NTA-

Network Traffic Analysis).

- Se recomienda una tecnología que permita la gestión o validación de privilegios de accesos (IAM). Evitar configurar usuarios y claves dentro de las aplicaciones de ICETEX.
- Validar a nivel de punto final, los equipos que se han visto involucrados con comportamiento malicioso
- Integrar los servidores de Directorio Activo con el SIEM.
- Integrar los equipos que hacen parte del proceso de pagos con el SIEM.
- 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.
- 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.
- Se debe realizar la integración de los activos críticos de la compañía a la plataforma de SIEM, no se ha podido lograr por la falta de recursos de este.

10 CONCLUSIONES GENERALES

La replicación entre el centro de datos principal (TRIARA) y el centro de datos alternativo (MEGACENTER) durante el mes de septiembre, se realizó sobre los 13 equipos definidos con un delta de sincronización de 15966.78 MB, además los centros de datos estuvieron disponibles y en operación el 100% del tiempo y no se presentaron fallas que afectan la operación del ICETEX.

En el mes de septiembre se presentó un crecimiento del 69.07% en el parámetro de análisis “piratería online, con respecto de mes de agosto, este porcentaje equivale a 1836 casos de los cuales se resolvieron 1 y se descartaron 1835.

Los dispositivos monitoreados por el SIEM solo el 20% tienen métricas de seguridad, un 58% solo traen datos de disponibilidad y rendimiento, un 21% no trae ningún tipo de log o se encuentran inoperantes y un 1% posee errores de parcheo.

Dentro de los eventos del mes se detectaron alertas de posibles ataques que no fueron detectados por el FortiWeb, después de validaciones sobre el origen del tráfico se procedió a bloquear las direcciones IP de origen en el firewall perimetral que se sitúa antes del WAF para prevenir ataques sobre los sitios web de la entidad.

Se realizó la configuración del 45.4% de las sedes de ICETEX para la navegación de IPv6, para el restante de las sedes, se revisará en conjunto entre ICETEX e INFOTIC la opción de configuración que se debe implementar debido a que las demás sedes cuentan con un router de voz, lo que impide tener la misma configuración desarrollada hasta el momento.

Las bases de datos del ICETEX se encuentran funcionando correctamente y tienen una réplica activa entre los data center principal y alterno, lo que permite que las aplicaciones que tienen servicios con el RAC de Oracle tengan un funcionamiento acorde a lo solicitado por la entidad.

Se presento al comité de cambio un solo caso, el cual fue ejecutado y documentado.

Durante el mes de septiembre no se solicitaron restauraciones de Backup ejecutados, a la fecha los backup realizados por operador tecnológico CLARO, se encuentran en las instalaciones de la data center principal TRIARA.

11 PLAN DE TRABAJO PROXIMO MES

Se adjunta el siguiente cuadro:

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
Durante el mes de septiembre del 2024 a nivel de conectividad y redes se tiene el 98% de los canales instalados y en servicio teniendo pendiente el canal Backup de Quibdó y el de Leticia, en cuanto a la instalación de señaléticas, también se ha alcanzado un avance del 98%, quedando pendiente la se la sede de Cali, que actualmente se encuentra en proceso de fabricación.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Dentro del proceso de monitoreo de marca se presentó un crecimiento del 69.07% de los casos analizados por SOC siendo el parámetro más relevante el de la “piratería online” con un total de 1836 casos de los cuales se descartaron 1835 y se resolvió 01, de otra parte se tiene que los dispositivos monitoreados por el SIEM solo el 20% de los dispositivos tienen métricas de seguridad, un 58% solo traen datos de disponibilidad y rendimiento, un 21% no trae ningún tipo de log o se encuentran inoperantes y un 1% posee errores de parcheo. Dentro de los eventos del mes se detectaron alertas de posibles ataques que no fueron detectados por el FortiWeb, después de validaciones sobre el origen del tráfico se proceden a bloquear las	INFOTIC - ICETEX	01-oct-24	31-ene-25	

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
direcciones IP de origen en el firewall perimetral que se sitúa antes del WAF para prevenir ataques sobre los sitios web de la entidad.				
También dentro de las actividades se detectaron eventos de DDoS los cuales fueron descartados ya que no se tiene información relevante que indicara que se tratara de algún ataque de este tipo ya que el puerto utilizado fue el TCP 443 (HTTPS) el cual es un puerto que se usa para los sitios web de la entidad y el origen no fue catalogado como malicioso. Esta información se presentará de manera grafica en el componente SOC.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Se ajusta el minutograma final para la prueba test del DRP, la cual se definió su ejecución para el viernes 04 de octubre y la cual servirá para medir tiempos, evaluar tareas paralelas y probar los escenarios para la prueba definitiva de la cual aún no se tiene confirmada la fecha por parte de ICETEX tentativamente seria para el mes de noviembre 2024.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Para el WAF del Datacenter alerno, se han realizado consultas jurídicas sobre la interpretación dada a las condiciones técnicas presentadas en el contrato entre las entidades ICETEX – INFOTIC, los avances se documentarán en los informes mensuales y una vez se tengan las conclusiones del análisis se implementará la solución a que haya lugar.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Definir con Icetex el procedimiento para la instalación y configuración de los Endpoints que quedan en bodega.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
En conjunto con el ICETEX se verificará el estado de los dispositivos monitoreados y realizar depuración de equipos que no se encuentren en operación.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Depuración de las políticas en los	INFOTIC - ICETEX	01-oct-24	31-ene-25	

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
firewalls, analizar el tráfico que pasa sobre las políticas con origen, destino, puertos en ALL y en base a este análisis alineando estas políticas para permitir sólo el tráfico necesario y cerrar brechas de seguridad asociadas a esta configuración.				
Segmentación las políticas de acuerdo con la necesidad y no otorgar acceso de toda una red o todos los servicios.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
En conjunto con el ICETEX se trabajará en el perfilamiento de la navegación de acuerdo con lo entregado por ICETEX.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
En conjunto con el ICETEX se validará la autenticación de doble factor para todas las plataformas misionales del ICETEX.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
En conjunto con el ICETEX revisar la autenticación a través del LDAP, para la gestión de las plataformas de seguridad.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
En conjunto con el ICETEX validar la posibilidad de la integración de la Consola Sophos con SIEM.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Realizar una sesión conjunta ICETEX-INFOTIC para definir el plan sobre las observaciones de los hallazgos del ambiente de producción del portal Web.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Respecto a lo anterior, INFOTIC realizará una sesión de trabajo en la cual se van a presentar las alternativas técnicas de solución y los planes de trabajo correspondientes en conjunto con ICETEX.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Garantizar la segmentación de la red que permita claramente definir qué servicios deben ser alcanzados por cada usuario.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Se recomienda una tecnología que permita realizar análisis de tráfico de la red (NTA- Network Traffic Analysis).	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Se recomienda una tecnología que permita la gestión o validación de privilegios de accesos (IAM). Evitar	INFOTIC - ICETEX	01-oct-24	31-ene-25	

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
configurar usuarios y claves dentro de las aplicaciones de ICETEX.				
Validar a nivel de punto final, los equipos que se han visto involucrados con comportamiento malicioso	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Integrar los servidores de Directorio Activo con el SIEM.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Integrar los equipos que hacen parte del proceso de pagos con el SIEM.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
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.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
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.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Se debe realizar la integración de los activos críticos de la compañía a la plataforma de SIEM, no se ha podido lograr por la falta de recursos de este.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Programará la sesión formalización del servicio del canal LAN 2 LAN	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Se ha escalado a la alta gerencia la falencia o falta de recursos de la herramienta de FortiSIEM, y la importancia ya que son los ojos ante cualquier amenaza o intruso en la seguridad informática del ICETEX.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
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	INFOTIC - ICETEX	01-oct-24	31-ene-25	

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
negado o permitido el tráfico.				
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.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Verificar los dispositivos que están presentando errores para la lectura de eventos desde el FortiSIEM a través de los protocolos WMI y VM_SDK.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
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.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
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.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
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) y en el caso que no se considere un fraude para la entidad responder este correo y se procederá a cerrar el caso como Resuelto.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Con respecto a los casos de Piratería Online – Producto falso o Venta Irregular recordar las medidas a considerar: Verificar la venta publicada si se trata de un producto o venta falso	INFOTIC - ICETEX	01-oct-24	31-ene-25	

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
o si corresponde y es propiedad de la entidad., en caso de que se trate de ventas falsas informar si es necesario solicitar un Takedown, si estos productos o ventas están autorizados o no representa un Fraude digital, responder el correo para marcar los tickets como Cerrado: Resuelto.				
Coordinar sesión en conjunto ICETEX-INFOTIC para revisar conclusiones del numeral 5.8	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Para portal Web Icetex, se realizará una mesa de trabajo para analizar los hallazgos encontrados en los ambientes de producción y pruebas.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
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.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Se debe segmentar las políticas de acuerdo con la necesidad y no otorgar acceso de toda una red o todos los servicios.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Se debe trabajar en el perfilamiento de la navegación de acuerdo con lo entregado por ICETEX.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Validar la autenticación de doble factor para todas las plataformas misionales del ICETEX. Continuamos a la espera de respuesta de la entidad.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Realizar autenticación a través del LDAPS, para la gestión de las plataformas de seguridad.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Validar la posibilidad de la integración de la consola Sophos con SIEM.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Validar la posibilidad de la integración de una VPN para la gestión desde DT alternativo Medellín como acceso adicional en caso de que se presente alguna falla por el canal dedicado de MPLS. Continuamos a la espera de respuesta de la entidad.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Realizar la contención automática de equipos que se identifiquen en la red	INFOTIC - ICETEX	01-oct-24	31-ene-25	

Actividades	Responsables	Fecha Inicio	Fecha fin	Verificación
como maliciosos. Continuamos a la espera de respuesta de la entidad.				
Realizar el aumento de recursos a la plataforma de FortiSIEM (CPU, Memoria y disco) y hacer un cambio de arquitectura con el objetivo de mejorar.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Garantizar la segmentación de la red que permita claramente definir qué servicios deben ser alcanzados por cada usuario.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Se recomienda una tecnología que permita realizar análisis de tráfico de la red (NTA- Network Traffic Analysis).	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Se recomienda una tecnología que permita la gestión o validación de privilegios de accesos (IAM). Evitar configurar usuarios y claves dentro de las aplicaciones de ICETEX.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Validar a nivel de punto final, los equipos que se han visto involucrados con comportamiento malicioso	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Integrar los servidores de Directorio Activo con el SIEM.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Integrar los equipos que hacen parte del proceso de pagos con el SIEM.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
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.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
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.	INFOTIC - ICETEX	01-oct-24	31-ene-25	
Se debe realizar la integración de los activos críticos de la compañía a la plataforma de SIEM, no se ha podido lograr por la falta de recursos de este.	INFOTIC - ICETEX	01-oct-24	31-ene-25	

Tabla 29 Plan de trabajo próximo mes