

INFORME DE JULIO 2023
CONTRATO 2022-0792



Tabla de contenido

INTRODUCCION	4
OBJETIVOS	4
INFORME DE ACTIVIDADES DBA	5
Resultados/Entregables:	5
Anotaciones/Novedades:	7
INFORME ADMINISTRADOR DE RED	8
Introducción:	8
#	8
Actividad	8
Evidencias	8
Anexos	9
INFORME MAYO – INTEGRADOR NUBE	10
Actividades desarrolladas:	10
1. Anexos	10
Conclusiones:	11
INFORME ADMINISTRADOR DE SOLUCIONES	1
Introducción:	1
Actividades desarrolladas:	1
1. Anexos	3
Conclusiones	4
INFORME ADMINISTRADOR WEBMASTER	5
Introducción	5
Actividades desarrolladas:	5
Conclusiones:	7
INFORME JULIO – ADMINISTRADORES DE SEGURIDAD	8
2.1. TRIARA	8
2.3. FORTIGATE MEDELLIN	10
2.3. FORTIGATE MEDELLIN	10
2.4. FORTIWEB APPS NUEVAS	11
2.5. FORTIWEB APPS VIEJAS	11
2.6. FORTISANDBOX	12
5.2. FORTIGATE AGUAS	17
9. CONCLUSIONES	33
CONCLUSIONES	34

INFORMACIÓN DEL DOCUMENTO

Fecha Creación	Versión del Documento	Responsable del Documento
01/07/2023	3.0	Carlos Alberto Alvira

Fecha Creación	Versión del Documento	Elaborado por
01/07/2023	3.0	Angie Paola Parra

INTRODUCCION

Durante el mes de julio, ICETEX llevó a cabo una serie de actividades significativas en relación con la migración de su centro de datos. El presente informe tiene como objetivo recalcar las actividades realizadas en el desarrollo de los casos, Durante el transcurso del mes de julio, ICETEX ha llevado a cabo una serie de actividades de gran relevancia en relación con la migración de su centro de datos. En este informe, se busca destacar y subrayar las diversas acciones emprendidas en el desarrollo de casos, tareas e incidentes que fueron escalados a través de la mesa de servicio Aranda. Asimismo, se resaltan las múltiples soluciones implementadas en respuesta a las solicitudes canalizadas a través de medios de comunicación alternativos, como Microsoft Teams, Outlook y Whatsapp. En adición a esto, este informe se enriquece con la inclusión de documentos complementarios que ofrecen una descripción exhaustiva de los procesos adoptados para abordar y resolver las fallas o inconvenientes identificados.

La premisa que guió nuestra resolución de los requerimientos escalados consistió en la identificación de las causas fundamentales de cada problemática, seguida de la aplicación de soluciones definitivas destinadas a minimizar el impacto experimentado por los usuarios. Para ello, se utilizó una amalgama de herramientas colaborativas y canales de comunicación, tales como Microsoft Teams, Outlook y Whatsapp, facilitando así una respuesta integral y eficaz a los desafíos presentados.

OBJETIVOS

El objetivo central de estas acciones fue reinstaurar el acceso a las aplicaciones de vital importancia, garantizando la continuidad operativa ininterrumpida de ICETEX. A través de una combinación de diligencia, análisis meticuloso y respuesta proactiva, se buscó no solo resolver los problemas de manera efectiva, sino también sentar bases sólidas para prevenir eventuales dificultades en el futuro.

INFORME DE ACTIVIDADES DBA		
Cliente:	ICETEX	
Proyecto:	ICETEX	
Período del Informe:	Del: 01/07/2023	Al: 31/07/2023
Días Laborados:	treinta y uno (31)	
Profesional:	Napoleón Murcia Gómez	
Identificación	Nit: 1.053.771.871	
Dependencia:	Dirección de Tecnología	
Rol/ Responsabilidad	DBA	
Objetivo del Período:		

En el marco de este informe, se han llevado a cabo una serie de pruebas fundamentales para evaluar la funcionalidad y eficacia de la plataforma Aranda. Estas pruebas han sido un componente esencial en nuestra búsqueda de optimizar los procesos internos y ofrecer soluciones más efectivas. Si deseas tener acceso a los detalles completos de estas pruebas, te invitamos a que accedas al siguiente enlace: [Insertar aquí el enlace correspondiente]. En dicho enlace, encontrarás un desglose exhaustivo de las pruebas realizadas, así como los resultados obtenidos, contribuyendo de manera significativa a nuestra comprensión de cómo Aranda puede potenciar nuestra operatividad.

Resultados/Entregables:

1. Generación de trazas en BD APOTEOSY para diagnóstico de proceso con lentitus..
2. Cancelación de pools de usuario coreut e icetex_nuevo
3. Configuración diskgroup ACFS para montaje de unidad /DATOS_ICETEX
4. Ejecución proceso de refresh APOTPRU.
5. Borrado de db links apuntando a producción.
6. Arreglo de db links apuntando a PROD de la BD APOTPRU recién refrescada
7. Paso a producción definitivo esquema CINA.
8. Paso a producción definitivo esquema HIST_COBOL.
9. Depuración de áreas de archives en BD's de PROD
10. Modificación de memoria asignada a cada una de las BD's para remediar
11. sobredimensionamiento de recursos del server y evitar nuevas caídas del clusterware.
12. Incremento de parámetros de cursores abiertos en BD sicci con el fin de corregir issue.

13. Creación usuario para sistema de gestión documental SGDEALOGS.
14. Se mitiga alerta de ocupación de FS /grid depurando medios de instalación de producto.
15. Pruebas de conectividad durante reporte de indisponibilidad de BD.
16. Atención de casos usando sqlloader directamente en el server de prod.
17. Depuración de áreas de archivos Dataguards (DR), cambio de memoria de las BD's dataguard con el fin de hacer match con producción, validación de la sincronización de cada uno de los dataguard.
18. Arreglo de Jobs en producción.
19. Se deshabilitan jobs de estadísticas de la BD ya que estas están configuradas desde S.O enel crontab.
20. Validación de usuarios con intentos fallidos de conexión en BD Producción con el fin de validar mas de 300 intentos fallidos de conexión del usuario MONITOREO.
21. Se realiza depuración del área de archivos de los stand by y se reactiva media recovery.
22. Se realiza análisis y se brindan privilegios al esquema CINA para que pueda quedar sin objetos inválidos.
23. Generación de métrica en OEM para monitoreo de dblinks en ambiente de pruebas sicci a cualquier ambiente en el rac de producción.
24. Creación de esquema CINA en BD de preproducción 19c.
25. Configuración de auditoría de modificación de ddl's en BD's de producción.
26. Migración esquema CINA de BD ICTXCYC (11.2.0.4) a BD VIGIAPRD 19c (Producción).
27. Cambios accesos usuario gawuser S.O 192.1.2.73.
28. Afinamiento de proceso en BD APOTEOSY usando advisors y generando índices.

Anotaciones/Novedades:

- ❑ Adicionalmente En lo que va del mes de mayo y al momento de la generación de este informe se han atendido 430 requerimientos de ejecución de scripts los cuales están siendo atendidos con la ayuda del operador dba.
- ❑ Aun se espera respuesta de proveedor claro en cuanto al esquema de backups de las BD's.
- ❑ Se automatizan tareas de depuración y mantenimiento de backups y de logs de auditoría, tracefiles, trm, xml del alert entre otros.
- ❑ Se realiza depuración de alertas de monitoreo, en este momento solo hay 14 retantes por validación y depuración.
- ❑ Se realiza instalación de cliente Oracle 19c para proyecto de gestión documental en server Windows.
- ❑ Se realiza análisis de caída de clusterware y se remite evidencia con causa raíz e informe, de este informe se desprende la modificación de los pools de memoria de las diferentes BD's del sist

	INFORME ADMINISTRADOR DE RED	
Cliente:	Icetex	
Proyecto:	Servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el Icetex. Contrato 0792-2022	
Período del Informe:	Del: 1/07/2023	Al: 30/07/2023
Profesional:	Carlos Roldan	CC: 80901301
Dependencia:	Dirección de Tecnología	
Rol/ Responsabilidad	Administrador de Red	
Objetivo del Período:	Atender todas las solicitudes, incidentes y tareas de cambios que se registren para los Administradores de Soluciones a través de todos los medios colaborativos que ofrece el Icetex.	

Introducción:

El presente informe tiene como objetivo recalcar las actividades realizadas en el desarrollo de los casos, tareas e incidentes que se escalaron a través de la mesa de servicio Aranda, así como también las diferentes soluciones que se ejecutaron de acuerdo a las solicitudes que se hacían llegar por otros medios de comunicación o herramientas colaborativas como lo son Microsoft Teams, Outlook y Whatsapp, además en este informe se anexan varios documentos que describen a detalle los procesos que se siguieron para solucionar las fallas o errores problema y se presentan los resultados obtenidos. El enfoque en el que nos basamos para resolver todos los requerimientos escalados consistió en identificar la causa raíz de cada uno de estos y aplicar una solución definitiva para minimizar el impacto en los usuarios y restaurar el acceso a las aplicaciones críticas lo más pronto posible.

#	Actividad	Evidencias
1	Inc. Falla de Conectividad a la Red	IM-242535-4-68433
2	Inc. Falla Equipos de Cómputo	IM-242486-4-68414
3	Inc. Falla Conectividad Red WIFI Corporativa	IM-242196-4-68331
4	Falla de Conectividad a la Red Buenaventura 90	IM-242070-4-68301
5	Falla de Conectividad a la Red Mocoa IM 91	IM-242069-4-68300
6	Inc. Falla Conectividad Red WIFI Corporativa	IM-242010-4-68282
7	Inc. Falla Conectividad Red WIFI Corporativa	IM-241996-4-68278

Anexos

IM-242535-4-68433

Servicio restablecido y en monitoreo se encuentra operando bien el servicio, todo fue a raíz de la caída de DECEVAL

SW4507-CORE#ping 8.8.8.8 repeat 1000

Type escape sequence to abort.

Sending 1000, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:

!!

Success rate is 100 percent (1000/1000), round-trip min/avg/max = 4/5/44 ms

IM-242486-4-68414

Se rectifica a claro la entrega de servicios formal en sede realizando e instalando el equipo en el lugar correcto solicitado por el usuario

IM-242196-4-68331

Circuito funcionando correctamente luego de escalado a ISP confirmado con usuario

IM-242070-4-68301

Equipo switch ejecutando crash y fallas se envía repuesto para cambio sin embargo se deja servicio funcional provisionalmente, adicional se envía un sw de repuesto para cambiar el existente.

IM-242069-4-68300

Se normaliza el servicio, se hacen pruebas con la funcionaria dejando operativo el servicio

<ICETEX_MOCOA>display arp

IP ADDRESS	MAC ADDRESS	EXPIRE(M)	TYPE	INTERFACE	VPN-INSTANCE
VLAN					

192.168.60.254	0025-9e9c-32fa		I	Vlanif1	
192.168.60.14	9c93-4e87-7a6f	20	D-0	Eth0/0/4	
192.168.60.1	e8ed-d658-06ef	20	D-0	Eth0/0/1	

IM-242010-4-68282

Equipo switch propiedad de Icetex con fallas y crash se envia equipo de respuesto desde sede aguas y se deja funcional provisioanlamente el servicio INCIDENT No 68301 Equipo switch ejecutando crash y fallas se envia repuesto para cambio sin embargo se deha servicio funcional provisionalmente

IM-241996-4-68278

Servicio restablecido se prueba y se deja en monitoreo servicio ok

<ICETEX_MOCOA>display arp

IP ADDRESS	MAC ADDRESS	EXPIRE(M)	TYPE	INTERFACE	VPN-INSTANCE
VLAN					

192.168.60.254	0025-9e9c-32fa		I	Vlanif1	
192.168.60.14	9c93-4e87-7a6f	20	D-0	Eth0/0/	
192.168.60.1	e8ed-d658-06ef	20	D-0	Eth0/0/1	

1INCIDENT No 68300

Servicio restablecido se prueba y se deja en monitoreo servicio ok

<ICETEX_MOCOA>display arp

IP ADDRESS	MAC ADDRESS	EXPIRE(M)	TYPE	INTERFACE	VPN-INSTANCE
------------	-------------	-----------	------	-----------	--------------

	INFORME MAYO – INTEGRADOR NUBE
Cliente:	Icetex
Proyecto:	Servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el Icetex. Contrato 0792-2022
Período del Informe:	Del: 1/07/2023 Al: 30/07/2023
Profesional:	Jose Luis Mantilla G.
Identificación	CC: 91'533.878
Dependencia:	Tecnología
Rol/Responsabilidad	Integrador de Nube
Objetivo del Período:	

Actividades desarrolladas:

#	Fecha	Actividad	Evidencias
1	Julio	Eliminación de recursos Azure, aplicación home liviano.	Eliminados los recursos creados y usados para la aplicación home liviano (Rocky Linux 9.2 con apache y redirections)
2	Julio	Asistencia a reuniones y atención a inquietudes y correos.	
3	Julio	En espera de reunión con el ing. Humberto para destinar migraciones o creación de recursos en Azure (más detalle en conclusiones).	Solicitud de reuniones para analizar necesidades y depurar recursos actuales en la nube de Azure, a su vez, no cuento con accesos para la nube GCP.

1. Anexos

No hay anexos más que el uso de una aplicación que la respuesta por correo a los ingenieros que fueron anexados cuando se solicitó la eliminación de los recursos de Azure creados para la aplicación que contenía home liviano. A su vez, quedo en espera de la reunión solicitada con el ingeniero Humberto Díaz al gerente de proyecto quien conoce la necesidad y los futuros lineamientos para definir los cambios, migraciones o implementaciones destinadas en Azure.

Queda pendiente el envío de reporte de hallazgos de lo encontrado en la infraestructura actual como plus o

Valor adicional.
Imágen de los recursos creados en Azure:

Home > rg-temporary Resource group

Search << + Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags Move Delete Export template Open in mobile

Overview Activity log Access control (IAM) Tags Resource visualizer Events

Settings Deployments Security Policies Properties Locks Cost Management Cost analysis Cost alerts (preview) Budgets Advisor recommendations

Essentials Subscription (move) : Microsoft Azure ICETEX Produccion Deployments : 1 Succeeded Subscription ID : d731d718-501c-4d29-8bc0-c3dbbb1817bc Location : East US Tags (2) : aprobacion : adiaz@icetex.gov.co solicitud : cblanco.cont@icetex.gov.co

Resources Recommendations (9)

Filter for any field... Type equals all Location equals all Add filter

Showing 1 to 6 of 6 records. Show hidden types No grouping

Name	Type	Location
temporary	Virtual network	West US 2
vm-temporary	Virtual machine	West US 2
vm-temporary-ip	Public IP address	West US 2
vm-temporary-nsg	Network security group	West US 2
vm-temporary773	Network Interface	West US 2
vm-temporary_OsDisk_1_a989ae3892214811ba7437eea278cddd	Disk	West US 2

Conclusiones:

Estoy en espera de reunión solicitada al gerente de proyecto para reunirme con el ing. Humberto Diaz y personas pertinentes para definir las futuras necesidades y validar de los 117 recursos encontrados en Azure ya que no puedo determinar cuáles pueden o deben ser eliminados, por lo tanto, es necesario debatir y socializar el informe entregado anteriormente con las personas responsables para su respectiva depuración.

También es importante analizar la infraestructura para determinar cuales se deben migrar a Azure (quizá nuevos proyectos o migración de máquinas virtuales).

No cuento con accesos a la plataforma GCP debido a que la entidad tiene multinube, es probable que se requieran migrar de una nube a la otra, por lo tanto, esta solicitud está pendiente.

INFORME ADMINISTRADOR DE SOLUCIONES		
Ciente:	lctex	
Proyecto:	Servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el lctex. Contrato 0792-2022	
Período del Informe:	Del: 1/07/2023	Al: 31/07/2023
Profesional:	Davis Alexander Mogollón Fandiño José Francisco Escobar Escorcía	CC: 11226339 CC: 72288982
Dependencia:	Dirección de Tecnología	
Rol/ Responsabilidad	Administrador de Soluciones	
Objetivo del Período:	Atender todas las solicitudes, incidentes y tareas de cambios que se registren para los Administradores de Soluciones a través de todos los medios colaborativos que ofrece el lctex.	

Introducción:

El presente informe tiene como objetivo recalcar las actividades realizadas en el desarrollo de los casos, tareas e incidentes que se escalaron a través de la mesa de servicio Aranda, así como también las diferentes soluciones que se ejecutaron de acuerdo a las solicitudes que se hacían llegar por otros medios de comunicación o herramientas colaborativas como lo son Microsoft Teams, Outlook y Whatsapp, además en este informe se anexan varios documentos que describen a detalle los procesos que se siguieron para solucionar las fallas o errores problema y se presentan los resultados obtenidos. El enfoque en el que nos basamos para resolver todos los requerimientos escalados consistió en identificar la causa raíz de cada uno de estos y aplicar una solución definitiva para minimizar el impacto en los usuarios y restaurar el acceso a las aplicaciones críticas lo más pronto posible.

Actividades desarrolladas:

#	Fecha	Actividad	Evidencias
1	05/07/2023	Tarea No. 489602, cargue de nuevos archivos .dll para la actualización del Web ServiceWebHistCobol.	Tarea 489602.pdf
2	10/07/2023	Tarea No. 489660, cargue de nuevos archivos .dll para la actualización del Web ServiceWebHistCobol.	Tarea 489660.pdf
3	06/07/2023	Tarea No. 489328, cargue de nuevos archivos .dll para la actualización del Web ServiceApiSolicitudes.	Tarea 489328.pdf

4	05/07/2023	Tarea No. 489506, acceso por escritorio remoto al servidor 10.1.4.241 con permisos de administrador al usuario pcastrillon.	Tarea 489506.pdf
5	12/07/2023	Tarea No. 489878, actualización de parámetros sobre el archivo de configuración appsettings del web services CuentasInactivasApi referente a la ruta en donde se encuentran los archivos para descargar desde la aplicación.	Tarea 489878.pdf
6	11/07/2023	Caso No. 68041, se revisó el caso, sin embargo, este presentaba fallas debido al servicio del CORE.	Caso 68041.pdf
7	13/07/2023	Caso No. 68139, se monitoreó la aplicación de PSE durante toda la mañana y estuvo totalmente funcional por lo que no se presentaron fallas.	Caso 68139.pdf
8	18/07/2023	Caso No. 68357, se realizó el reinicio del AppPool del Website Desembolsos y se validó con la usuaria el funcionamiento correcto de la aplicación.	Caso 68357.pdf
9	26/07/2023	Caso 68574, se realizaron validaciones correspondientes a nivel del servidor que contiene la aplicación PSE encontrando que está totalmente funcional, sin embargo, existió una falla en el servicio del CoreFX (Servicio SM http://10.158.7.10:9080/smServices2/services/smServices.smServicesHttpSoap11 Endpoint) 7 am del día 26/07/2023	Caso 68574.pdf
10	19/07/2023	Caso 79995, se creó en el archivo host del servidor 192.168.20.4 el registro 186.84.73.132 www.icetex.gov.co, lo para redireccionar el acceso, además en el archivo ConsultaSolicitudesRenovar.asp ubicado en la ruta 192.168.20.4\sitioicetex\portalacces\Tradicional\Renovar se cambió en la línea de urlcore = "https://www.icetex.gov.co/proxycore/api/ConsultaCredito/" &rsTrae_Datos("idsolicitud") el http por https.	Caso 79995.pdf
11	25/07/2023	Caso 80154, se realizó la configuración de la máquina 192.168.51.190 donde se le asignó el registro DNS cina.icetex.gov.co, además se le instalaron los componentes .NET, NETCore y NETCore Runtime.	Caso 80154.pdf
12	21/07/2023	Tarea 490391, se realizó el despliegue del BackEnd de la aplicación cuentas inactivas donde se copiaron nuevos archivos en la siguiente ruta F:\aplicaciones\CuentasInactivasAPI, se reinició la AppPool CIAAPI, el usuario hace pruebas y la aplicación funciona correctamente.	Tarea 490391.pdf
13	18/07/2023	Tarea 490006, se realizó el cambio de las imágenes membrete-01.png y membrete-02.png en los servidores de aplicación 192.1.1.4 y 192.168.20.4 en la ruta portalacces/GestionCartera/img, además se realizaron pruebas con el usuario y el certificado queda con las nuevas imágenes.	Tarea 490006.pdf
14	17/07/2023	Tarea 490075, se realizó el despliegue del FrontEnd de la aplicación cuentas inactivas donde se copiaron nuevos archivos en la siguiente ruta F:\aplicaciones\CuentasInactivasFront, se reinició el AppPool CIFront y la aplicación funcionó correctamente.	Tarea 490075.pdf
15	13/07/2023	Tarea 490164, se procedió a revisar el archivo appsetting.json del Backend de la aplicación Cuentas Inactivas y se encontró que la ruta que almacena las certificaciones es la siguiente: E:\WebSiteTemp\CuentasInactivas por tal motivo se realizó una sesión con los desarrolladores de la aplicación y se cambió la ruta por la siguiente: F:\Documentos CINA\	Tarea 490164.pdf

16	25/07/2023	Tarea 490352, se realizó la actualización de la cadena de conexión del ambiente de cuentas Inactivas producción en el servidor 192.168.51.165 del archivo appSettings.json en el parámetro: service_name=VIGIAPRD, se validó con el usuario y el cambio funciona correctamente.	Tarea 490352.pdf
17	27/07/2023	Se copian las carpetas del Front y Backend del servidor de cuentas inactivas preproducción(192.168.51.190) y se pegan en el servidor 192.168.51.165 donde se encuentra el ambiente de cuentas inactivas de producción y también se creó la aplicación en el IIS con nombresCuentasInactivasPreCIFront y CuentasInactivasPreCIAPI	Tarea 490627.pdf

1. Anexos

Anexo 1: Actividades desarrolladas que no se escalaron por Mesa de Servicio Aranda

Durante el mes de julio de 2023, se han llevado a cabo varias actividades que no se escalaron por medio de la Mesa de Servicio Aranda. Estas actividades incluyen lo siguiente y se pueden validar en el enlace [Actividades desarrolladas que no se escalaron a través de ARANDA.pdf](#):

1. Sesión de trabajo con el soporte de Bancolombia para revisar los servicios que están expuestos por la herramienta de GoAnyWhere del Ictetex.
2. Revisión de alerta referente al WebServiceApiSolicitudes reportada por el visor de eventos del sistema operativo en el cual está configurada la aplicación de PSE.
3. Revisión del servicio ipdeceval y servidor web apache tomcat para la aplicación pagares.bvc.com.co
4. Sesión de trabajo referente a la ejecución de parches en bases de datos Oracle, para ello se estuvo monitoreando el portal web <https://web.ictetex.gov.co/portal> para su disponibilidad.
5. Sesión de trabajo con el fin de revisar funcionalidad de descarga de factura en la aplicación Cuentas Inactivas.
6. Segunda sesión de trabajo con el soporte de Bancolombia para revisar los servicios que están expuestos por la herramienta de GoAnyWhere del Ictetex.
7. Tercera sesión de trabajo con el soporte de Bancolombia para revisar los servicios que están expuestos por la herramienta de GoAnyWhere del Ictetex.
8. Solucionó a falla reportada en el web service ServicioIntegracionRUV.
9. Renovación de licencias en los nodos 1 y 2 de Liferay que soportan el portal web <https://web.ictetex.gov.co/portal>.

Aunque estas actividades no se han escalado a través de la Mesa de Servicio Aranda se han seguido los procedimientos adecuados para garantizar que todas las solicitudes, incidentes y actualizaciones sobre los Web Service de las aplicaciones sean atendidas de manera oportuna y eficiente.

Conclusiones

En conclusión, todos los casos registrados en la herramienta de Mesa de Servicio Aranda fueron solucionados exitosamente por los Administradores de Soluciones durante el mes de julio de 2023.

Además, se observó que los casos estaban relacionados con accesos a servicios a través de conexiones FTP y directorios compartidos, también se escalaron errores presentados en las algunas aplicaciones críticas del Icetex y además se ejecutaron tareas de cambios que conllevaron a la actualización de archivos .dll sobre diversos Web Service que están configurados en los servidores web IIS.

Es importante destacar que, gracias al enfoque proactivo de los administradores de soluciones, todos los casos fueron abordados oportunamente y se logró una resolución efectiva de las solicitudes, incidentes y tareas de cambio reportadas.

Por último, se recomienda seguir con el continuo monitoreo de todas las aplicaciones y el seguimiento de los casos registrados sobre la herramienta de Mesa de Servicio Aranda, con el fin de mantener la estabilidad en la operación de los servicios publicados tanto para los usuarios internos como externos del Icetex.

	INFORME ADMINISTRADOR WEBMASTER
Proyecto:	Servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el Icetex.
Período del Informe:	Del: 1/07/2023 Al: 31/07/2023
Profesional:	Carlos Roberto Blanco Luna
Identificación	CC: 88030985
Dependencia:	DTI
Rol/ Responsabilidad	WEBMASTER
Objetivo del Período:	Informe(s) de avance de Julio del proyecto de acuerdo con el plan estratégico de Tecnología aprobado por la Dirección y de los cambios efectuados sobre la plataforma tecnológica a nivel de Servidores Web, de acuerdo con los requerimientos del Instituto.

Introducción

El presente informe tiene como objetivo presentar un resumen de las actividades realizadas durante el mes de julio de 2023, en el marco de la gestión y mantenimiento del portal web.icetex. Durante este periodo, se llevaron a cabo diversas tareas enfocadas en la optimización de la infraestructura, la implementación de nuevos servicios, la revisión de licencias y la actualización de contenidos, entre otros aspectos relevantes para asegurar el correcto funcionamiento y la eficiencia de la plataforma.

A continuación, se detallarán las actividades ejecutadas, así como las conclusiones y recomendaciones resultantes de cada una de ellas.

Actividades desarrolladas:

#	Fecha	Actividad	Avance	Evidencia
---	-------	-----------	--------	-----------

1	01/07/2023	Validación Informe de Migración: Infraestructura del Portal web.icetex La actividad consistió en realizar una exhaustiva revisión del informe de migración de la infraestructura del Portal web.icetex. Se verificaron los detalles técnicos y los procedimientos de migración utilizados para garantizar una transición exitosa hacia la nueva infraestructura. Se confirmó que se siguieron las mejores prácticas y recomendaciones, asegurando la integridad y disponibilidad del portal.	Completado	Informe de Validación
2	03/07/2023	Validación implementación Servicio DDoS ICETEX En esta actividad, se llevó a cabo la validación del servicio DDoS implementado por INFOTIC. Se validaron las pruebas realizadas de carga y simulaciones de ataques para evaluar la eficacia del servicio en la mitigación de ataques DDoS. Los resultados mostraron que el servicio es capaz de detectar y neutralizar los ataques de manera efectiva, proporcionando una mayor seguridad y disponibilidad del portal web.icetex.	En proceso	Survey Servicio AntiDDoS
3	07/07/2023	Gestión Cambio Parchado BBDD Oracle Durante esta gestión, se planificó y ejecutó el parchado de la base de datos Oracle utilizada por el portal web.icetex. Se realizaron copias de seguridad adecuadas y se siguieron los procedimientos recomendados para aplicar los parches sin afectar la disponibilidad del sistema. La implementación del parche se llevó a cabo de manera exitosa, asegurando la integridad y seguridad de los datos almacenados en la base de datos.	Completado	Registro de Gestión de Cambio

4	10/07/2023	Revisión y gestión de la Actualización de enlaces desactualizados en pdf históricos cargados en el portal Se procedió a revisar y gestionar la actualización de enlaces desactualizados presentes en documentos PDF históricos cargados en el portal. Se identificaron los enlaces inválidos y se procedió a corregirlos para garantizar que los usuarios puedan acceder a la información relevante sin inconvenientes.	Completado	Registro de Actualización de Enlaces
5	12/07/2023	Gestión e instalación de licencias definitivas liferay En esta actividad, se llevó a cabo la gestión de las licencias definitivas de Liferay utilizadas en el portal web.icetex.	Completado	Registro de Gestión de Licencias

Conclusiones:

- ☐ Durante el mes de julio, se logró avanzar satisfactoriamente en la ejecución de las actividades planificadas para el mantenimiento y optimización del portal web.icetex. La revisión y ajuste de la infraestructura, la implementación de nuevos servicios y la actualización de contenidos desactualizados contribuyeron significativamente al mejoramiento del rendimiento y la seguridad de la plataforma.
- ☐ Asimismo, la participación en auditorías, el seguimiento de brechas de seguridad y el cumplimiento de compromisos legales, como la resolución 1519 de 2020, demuestran el compromiso y responsabilidad del equipo técnico en garantizar la accesibilidad web y la calidad del portal para los usuarios.
- ☐ La gestión de licenciamiento ha sido fundamental para el adecuado funcionamiento y despliegue del portal web.icetex en la plataforma Liferay. La actualización y obtención de licencias definitivas ha garantizado el cumplimiento de las políticas de uso de software y permitido mantener un entorno de producción estable y seguro. Es importante continuar con un seguimiento periódico para asegurar que todas las licencias se encuentren vigentes y que los nodos del portal estén correctamente autorizados, lo que contribuirá a mantener la integridad y eficiencia del sistema en beneficio de los usuarios y la institución.

	INFORME JULIO – ADMINISTRADORES DE SEGURIDAD
Cliente:	Icetex
Proyecto:	Servicios especializados en outsourcing para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado para el Icetex. Contrato 0792-2022
Período del Informe:	DEL-AI: 01 Julio de 2023 al 31 Julio 2023
Profesional	Edwin JiménezJhon Pava
Profesional	CC 80749306 1057577413
Dependencia:	Soporte y AdministraciónProyectos
Rol/ Responsabilidad	Administradores de seguridad
Objetivo del Período:	Gestión de soporte y administración de lasplataformas Migración de Internexa a Claro

1. INTRODUCCIÓN

El Informe de Gestión Mensual contiene información relevante para evidenciar el nivel de cumplimiento del contrato firmado entre INFOTIC e ICETEX. El informe presenta los resultados y el análisis de la gestión de los servicios de seguridad para el mes de julio de 2023.

2. ESTADO GENERAL DE LAS PLATAFORMAS

Administración Plataformas incluidas las propiedades del ICETEX y las IaaS
FortiWebs
FortiSandbox
FortiGates

2.1. TRIARA

System Information

Hostname	DC_FG_MST_ICETEX
Serial Number	FG180FTK22901087 
Firmware	v7.2.5 build1517 (Feature)
Mode	NAT
System Time	2023/08/03 14:51:27
Uptime	20:16:01:36
WAN IP	 186.84.155.234

Seguridad Perimetral DC Principal (FortiGate_Triara)

 default	Perfil con las mínimas restricciones
 Navegacionpcs_Comware	Perfil con restricciones
 Navegacionpcs Comware con redes	Perfil con restricciones
 WF-Aereolineas	RF-186510-7-9612 24/03/2022
 WF-Avanzado	Perfil para FSSO Navegación Avanzada
 WF-Comunicaciones	Perfil para FSSO comunicaciones
 WF-General	Perfil para todos
 WF-General_Sedes	Perfil para todos
 WF-Redessociales	Perfil para FSSO Navegación Avanzada
 WF-Tesoreria	Perfil con restricciones específicas por auditoria.
 WF-Tesoreria_Sala_Segura	Permisos para equipos de Sala Segura de Tesoreria
 WF-VIP	Perfil para FSSO Navegación_VIP
 WF-wetransfer	Perfil para FSSO Navegación Avanzada
 wifi-default	Perfil de FULL acceso para pruebas

Inspección SSL (FortiGate_Triara)

Name	Comments
 Prueba certificate-inspection	Read-only SSL handshake inspection profile.
 custom-deep-inspection	Customizable deep inspection profile.
 certificate-inspection	Read-only SSL handshake inspection profile.
 deep-inspection	Read-only deep inspection profile.
 no-inspection	Read-only profile that does no inspection.

Antivirus y Antimalware Perimetral (FortiGate_Triara)

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

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



Name	
default	ALL con FSB
AV-FSB	HTTP,SMTP FULL FSB
AV-HTTP	HTTP con FSB
ICETEX	
AV-HTTP&CIFS	HTTP,CIFS con FSB
AV-FTP	FTP FULL FSB
prueba2	
AV-SMTP	SMTP FULL FSB
AV-HTTP Mobile	HTTP, mobile con FSB
Prueba	ALL con FSB
wifi-default	ALL monitoreo sin FSB

2.2. FORTIGATE AGUAS

Seguridad Perimetral DC Alterno (FortiGate Aguas)

System Information

Hostname DCAGUAS_FG_MST_ICETEX
 Serial Number FG6H0FTB22902021
 Firmware v7.2.5 build1517 (Feature)
 Mode NAT
 System Time 2023/08/03 14:53:26
 Uptime 20:16:25:11
 WAN IP 186.84.155.234

2.3. FORTIGATE MEDELLIN

Seguridad Perimetral DC Medellin (FortiGate_Medellin)

System Information

Hostname DCB_FG_MST_ICETEX
 Serial Number FG6H0FTB22902086
 Firmware v7.2.5 build1517 (Feature)
 Mode NAT
 System Time 2023/08/03 14:52:37
 Uptime 20:16:26:57
 WAN IP 186.84.73.225

2.4. FORTIWEB APPS NUEVAS

WAF (FortiWeb_Triara_APPS_Nuevas)

System Information

HA Status	Standalone
Host Name	FortiWeb
Serial Number	FV-2KFTE21000029
Operation Mode	Reverse Proxy
System Time	Thu Aug 3 15:00:08 2023
Firmware Version	FortiWeb-2000F 7.23,build0365(GA),230616
System Uptime	[45 day(s) 1 hour(s) 41 min(s)]
Administrative Domain	✖ Disabled

2.5. FORTIWEB APPS VIEJAS

WAF (FortiWeb_Triara_APPS_Viejas)

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	Thu Aug 3 15:04:08 2023
Firmware Version	FortiWeb-2000E 7.23,build0365(GA),230616
System Uptime	[45 day(s) 2 hour(s) 20 min(s)]

2.6. FORTISANDBOX

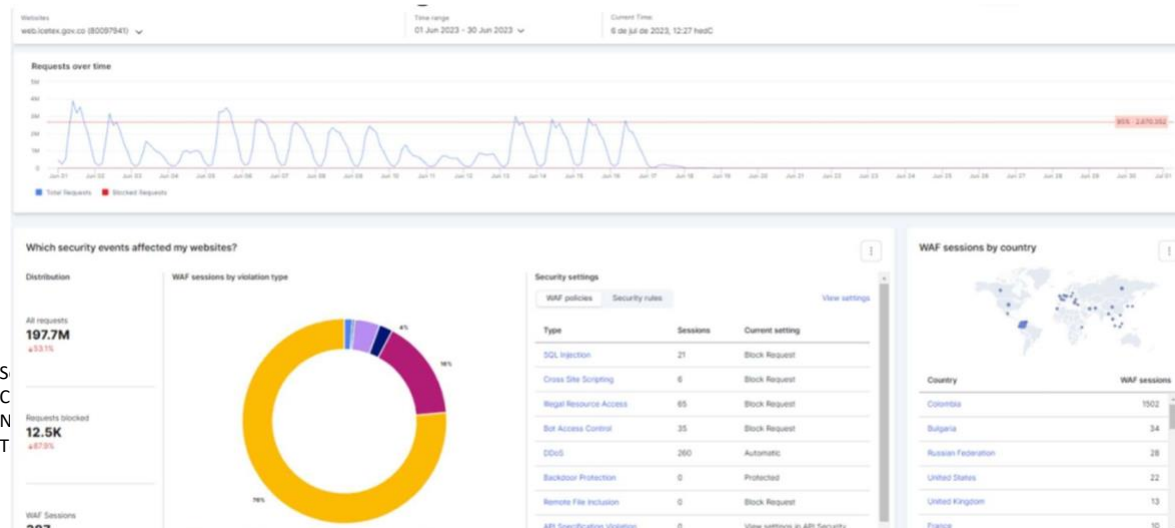
Seguridad Local (FortiSandBox)

System Information

Unit Type	Standalone
Host Name	fsa.icetex.gov.co [Change]
Serial Number	FSA1KD3A17000156
System Time	Thu Aug 3 15:05:42 2023 -05 [Change]
Firmware Version	v3.2.3,build0255 (GA) [All firmwares]
System Configuration	Last Backup: 2023-06-17 04:45 [Backup/Restore]
Current User	ejimenez
Uptime	45 day(s) 3 hour(s) 19 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

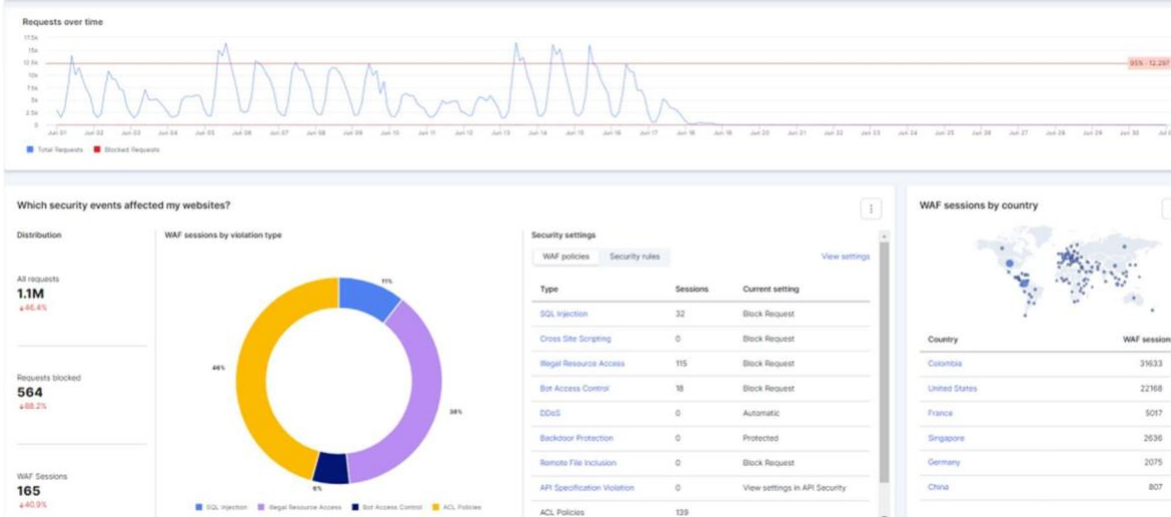
3. PORTALES PROTEGIDOS POR EL WAF (Waf Imperva)

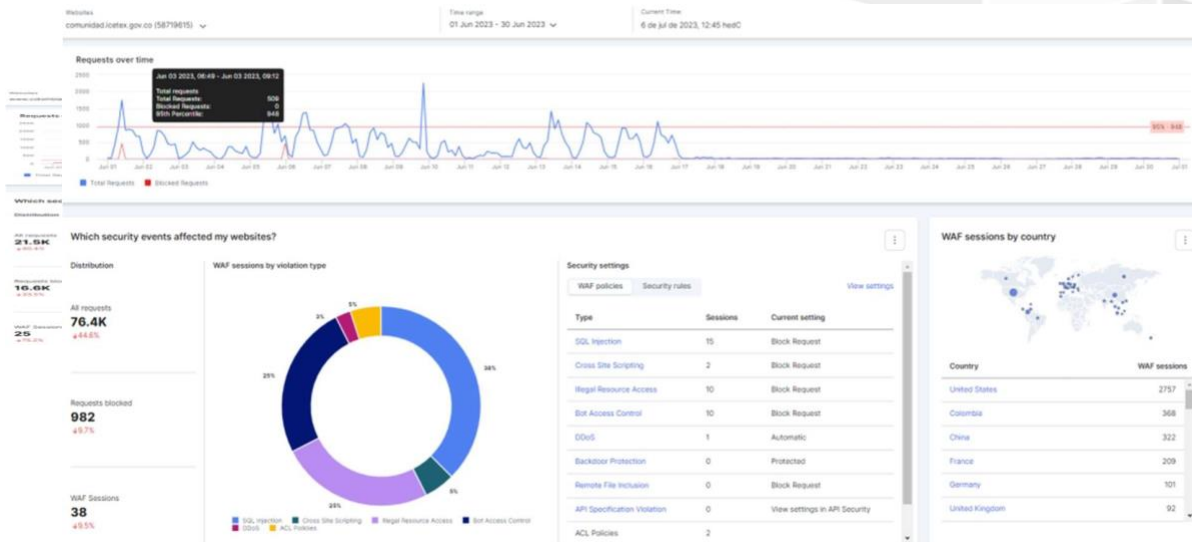
Tráfico desde WAF web.icetex.gov.co





Tráfico desde WAF www.icetex.gov.co





Tráfico desde WAF comunidad.icetex.gov.co



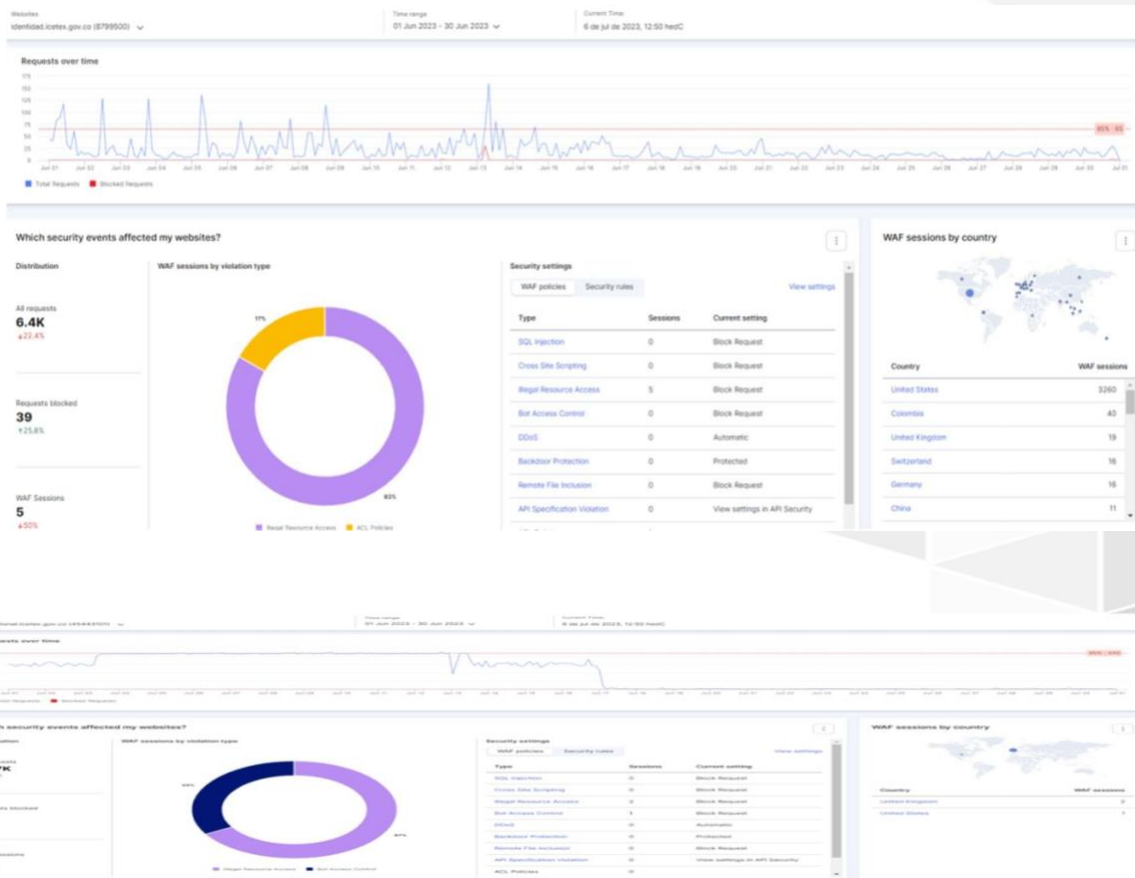
Tráfico desde WAF identidad.icetex.gov.co

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

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



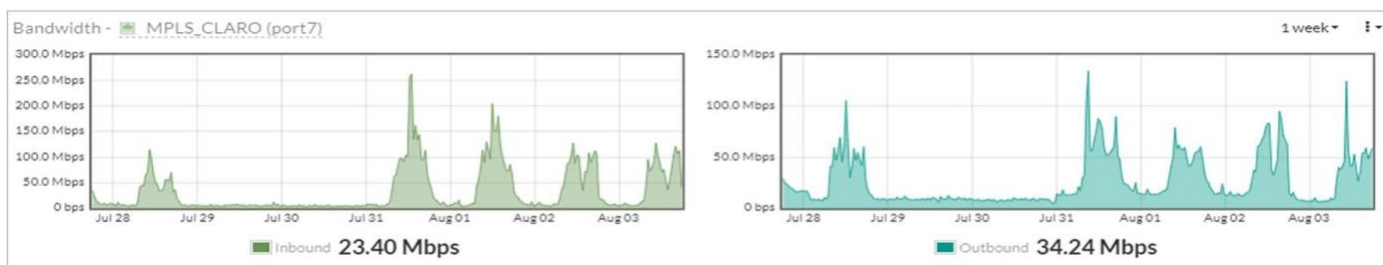
CO-SC-CER921046



4. ESTADO DE SALUD DE LOS EQUIPOS DE SEGURIDAD

4.1. FIREWALL AGUAS

Se observa el tráfico hacia la MPLS de la sede de Aguas, con un promedio 28,82 Mbps (Port7), desde el momento en que se hizo la migración.



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

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

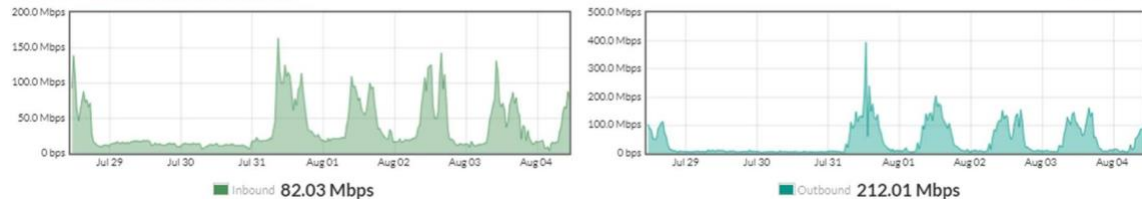


CO-SC-CER921046

4.2. FIREWALL FORTINET TRIARA

Se observa el tráfico hacia la MPLS promedio 147,02 Mbps (CLARO(MPLS_DC)), desde el momento en que se hizo la migración.

Bandwidth - INR0185 CLARO (MPLS_DC)



5. ESTADO DE LICENCIAMIENTO DE PLATAFORMAS

Características de licenciamiento y los contratos asignados.

5.1. FORTIGATE TRIARA

License Information		
Entitlement	Status	
FortiCare Support	Registered	Actions
FortiCloud Account	licencias@wexler.com.co	
Hardware Version	Advanced hardware (Expiration Date: 2026/05/19)	
Enhanced Support	Premium (Expiration Date: 2026/05/19)	
Firmware & General Updates	Licensed (Expiration Date: 2026/05/19)	Actions
Application Control Signatures	Version 25.00614	
Device & OS Identification	Version 1.00155	
Internet Service Database Definitions	Version 7.03316	
Intrusion Prevention	Licensed (Expiration Date: 2026/05/19)	Actions
IPS Definitions	Version 25.00614	
IPS Engine	Version 7.00314	
Malicious URLs	Version 4.00776	
Botnet IPs	Version 7.03316	View List
Botnet Domains	Version 3.00392	
AntiVirus	Licensed (Expiration Date: 2026/05/19)	Upgrade Database
AI Malware Detection Model	Version 2.12156	
AV Definitions	Version 91.05721	
AV Engine	Version 6.00288	
Mobile Malware	Version 91.05721	
Web Filtering	Licensed (Expiration Date: 2026/05/19)	
Blocked Certificates	Version 1.00440	
Email Filtering	Licensed (Expiration Date: 2026/05/19)	
Outbreak Prevention	Licensed (Expiration Date: 2026/05/19)	

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

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



CO-SC-CER921046

5.2. FORTIGATE AGUAS

License Information		
Entitlement	Status	
FortiCare Support	Registered	Actions
FortiCloud Account	licencias@wexler.com.co	
Hardware Version	Advanced hardware (Expiration Date: 2026/05/12)	
Enhanced Support	Premium (Expiration Date: 2026/05/12)	
Firmware & General Updates	Licensed (Expiration Date: 2026/05/12)	
Application Control Signatures	Version 25.00614	Actions
Device & OS Identification	Version 1.00155	
Internet Service Database Definitions	Version 7.03316	Actions
Intrusion Prevention	Licensed (Expiration Date: 2026/05/12)	
IPS Definitions	Version 25.00614	Actions
IPS Engine	Version 7.00314	
Malicious URLs	Version 4.00776	
Botnet IPs	Version 7.03316	View List
Botnet Domains	Version 3.00392	View List
AntiVirus	Licensed (Expiration Date: 2026/05/12)	
AI Malware Detection Model	Version 2.12157	
AV Definitions	Version 91.05721	Upgrade Database
AV Engine	Version 6.00288	
Mobile Malware	Version 91.05721	
Web Filtering	Licensed (Expiration Date: 2026/05/12)	
Blocked Certificates	Version 1.00440	
Email Filtering	Licensed (Expiration Date: 2026/05/12)	
Outbreak Prevention	Licensed (Expiration Date: 2026/05/12)	

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

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



CO-SC-CER921046

5.3. FORTIGATE MEDELLIN

License Information		
Entitlement	Status	
FortiCare Support	✓ Registered	⋮ Actions -
FortiCloud Account	✓ licencias@wexler.com.co	
Hardware Version	✓ Advanced hardware (Expiration Date: 2026/06/02)	
Enhanced Support	✓ Premium (Expiration Date: 2026/06/02)	
Firmware & General Updates	✓ Licensed (Expiration Date: 2026/06/02)	
Application Control Signatures	⊙ Version 25.00614	⋮ Actions -
Device & OS Identification	⊙ Version 1.00155	
Internet Service Database Definitions	⊙ Version 7.03316	⋮ Actions -
Intrusion Prevention	✓ Licensed (Expiration Date: 2026/06/02)	
IPS Definitions	⊙ Version 25.00614	⋮ Actions -
IPS Engine	⊙ Version 7.00314	
Malicious URLs	⊙ Version 4.00776	
Botnet IPs	⊙ Version 7.03316	View List
Botnet Domains	⊙ Version 3.00392	View List
AntiVirus	✓ Licensed (Expiration Date: 2026/06/02)	
AI Malware Detection Model	⊙ Version 2.12157	
AV Definitions	⊙ Version 91.05721	⊕ Upgrade Database
AV Engine	⊙ Version 6.00288	
Mobile Malware	⊙ Version 91.05721	
Web Filtering	✓ Licensed (Expiration Date: 2026/06/02)	
Blocked Certificates	⊙ Version 1.00440	
Outbreak Prevention	✓ Licensed (Expiration Date: 2026/06/02)	

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

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



CO-SC-CER921046

5.4. FORTIWEB NUEVAS APPS

License Information

Contract	Status	
Support Contract	✓ Registered	Launch Portal
Security Service	✓ Valid Contract (Expires 2026-06-04)	
	⦿ Signature Build Number: 0.00354	
	⦿ Signature Engine Version: 5.1.2	
Antivirus	✓ Valid Contract (Expires 2026-06-04)	
	⦿ Regular Virus Database Version: 91.05717	
	⦿ Extended Virus Database Version: 91.05640	
	⦿ Virus Engine Version: 6.00283	
IP Reputation	✓ Valid Contract (Expires 2026-06-04)	Update
	⦿ Signature Build Number: 4.00821	How To Renew
Credential Stuffing Defense	⚠ Expired (1969-12-31)	
	⦿ Credential Stuffing Defense Database Version: 0.00000	
FortiSandbox	⚠ Expired (1969-12-31)	
	⦿ FortiSandbox Database Version: 0.0	
GEO DB	✓ Valid Contract (Expires 2026-06-04)	
	⦿ GEO Database Version: 0184	
Threat Analytics	⚠ Expired (1969-12-31)	

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

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



CO-SC-CER921046

5.5. FORTIWEB VIEJAS APPS

License Information

Contract	Status	
Support Contract	Registered	Launch Portal
Security Service	Expired (2023-06-20)	
	Signature Build Number: 0.00350 Signature Engine Version: 5.1.2	
Antivirus	Expired (2023-06-20)	
	Regular Virus Database Version: 91.04324 Extended Virus Database Version: 91.04167 Virus Engine Version: 6.00283	
IP Reputation	Expired (2023-06-20)	Update
	Signature Build Number: 4.00814	How To Renew
Credential Stuffing Defense	Expired (1969-12-31)	
	Credential Stuffing Defense Database Version: 0.00000	
FortiSandbox	Expired (1969-12-31)	
	FortiSandbox Database Version: 3.169	
GEO DB	Expired (2023-06-20)	
	GEO Database Version: 0179	
Threat Analytics	Expired (1969-12-31)	

License Information

Contract	Status	
Support Contract	Registered	Launch Portal
Security Service	Expired (2023-06-20)	
	Signature Build Number: 0.00350 Signature Engine Version: 5.1.2	
Antivirus	Expired (2023-06-20)	
	Regular Virus Database Version: 91.04324 Extended Virus Database Version: 91.04167 Virus Engine Version: 6.00283	

VM Images							
Edit Clone Number		Delete VM		Undelete VM		Enabled VM Types: 4 / 4	
						Keys: 8 / 12	
						Clone Number: 8 / 8	
	Name	Version	Status	Enabled	Clone #	Load #	Extensions
- Default VMs (2/2)							
	WIN7X64VM	7	activated	✓	2	2	jse exe msi wsf upx vbs bat cmd dll ps1 jar pdf htm js url lnk zip WEBLink
	WIN7X86VM	6	activated	✓	2	2	ppspx ppt pptx doc docx rtf dotx docm dotm xltb xltm xlsx xlam potx sldx pptm ppsm potm ppam sldm onetoc thmx msg dot xlt pps pot eml iqy htm js url lnk zip
- Optional VMs (2/8)							
	WIN10X64VM	2	activated	✓	2	2	jse exe msi wsf upx vbs bat cmd dll ps1 jar pdf htm js url lnk zip WEBLink
	WIN10X86VM	2	activated	✓	2	2	jse exe msi wsf upx vbs bat cmd dll ps1 jar pdf htm js url lnk zip WEBLink
	WIN7X64SP1	1	✗	✗	0	0	N/A
	WIN7X86SP1O16	1	✗	✗	0	0	N/A
	WIN10X64VMO16	1	✗	✗	0	0	N/A
	WIN81X64VMO16	1	✗	✗	0	0	N/A
	AndroidVM	1	✗	✗	0	0	N/A
- Remote VMs (1)							
	MACOSX	0	installed	✓	1	0	mac dmg

6. EVENTOS RELEVANTES

- re permite el detectar y prevenir ataques de ciberseguridad que comprometan la continuidad del negocio.
- Durante el mes de julio no se presentaron eventos relevantes, que afectaran la disponibilidad de losservicios de la entidad a nivel de la solución de Seguridad

7. ACTIVIDADES

- ② Atención de incidentes, requerimiento, eventos y cambios en las plataformas de seguridad, solicitud depermisos, creaciones de VPNs, configuraciones y creación de políticas y enrutamientos, con entradas a través de la plataforma Aranda, por correo, chat WhatsApp, Teams y por otros medios.
- ② Elaboración y entrega de solicitudes requeridas por el ingeniero de seguridad del Icetex:Prestación de soporte técnico durante el periodo.
- ② Se realizan ajustes de configuraciones de los firewalls de Aguas y de Triara reduciendo el número de políticas y ordenándolas por flujos, también se quitaron políticas con origen y destino any en la interfaz.
- ② Se realiza la implementación del Fortimanager y se agrega el firewall de Triara con opciones deFortiAnalyzer.
- ② Se a tiende a varias sesiones de migración de OPenshift a triara, incluidas dos ventanas en las cuales serealizaron actividades de clonado de máquinas y está pendiente la ventana final para la migración.

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

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



CO-SC-CER921046

- ☐ Se realizan ajustes de conexiones sobre servicios de pruebas contra Openshift.
- ☐ Se atienden solicitudes del cliente sobre bloqueos de url y peticiones.
- ☐ Se realiza plan de mejora sobre la red de WIFI con el uso de portal cautivo, para saber quién realiza alguna acción.
- ☐ Se realizan varias sesiones con el proveedor de Claro con el fin de validar los servicios con Banco de la República y Deceval, con el fin de realizar la migración de los servicios a la red de Claro.
- ☐ Se realiza parte del documento de implementación y estará por terminar en el mes de agosto.
- ☐ Se realizan análisis de reportes generados por el SOC y se toman acciones si son requeridas.
- ☐ Se asiste a sesiones de validación de GoAnywhere para validar conexión contra Bancolombia.
- ☐ Se realizan desbloques algunos portales web desde el WAF.
- ☐ Solicitud de recursos para la herramienta Fortisium.
- ☐ Inclusión de los equipos de seguridad a la Herramienta Fortisium.
- ☐ Afinamientos al Fortisium.

7.1.1. Gestión de casos

Para el mes de julio se reportaron un total de 75 casos 3 de ellos no fueron escalados por medio de Aranday todos quedaron en un estado de solucionado.

Fecha	NUMERO DE CASO	ASUNTO	Estado del caso
5/07/2023	67653	Bloqueo por parte del WAF a identidad.icetex.gov.co/Login/validate	Solucionado
5/07/2023	67751	no acceso a Aranda y a 10.1.18.55 por RDP	Solucionado
5/07/2023	67765	Bloqueo del WAF a C&Cetex	Solucionado
5/07/2023	67722	Bloqueo del WAF a Talento Humano	Solucionado

5/07/2023	13290	No acceso a 192.168.20.30, 192.168.20.31, http://10.1.18.25 y a http://10.1.18.26	Solucionado
5/07/2023	67708	Caso gestionado bajo el caso 67668	Solucionado
5/07/2023	79193	Relacion de redes con VLANs	Solucionado
5/07/2023	79263	Bloqueo del WAF a identidad.icetex.gov.co/Login/Recuperar	Solucionado
Fecha	NUMERO DE CASO	ASUNTO	Estado del caso
7/07/2023	79215	Falla de acceso usuarios Tiqal	Solucionado
7/07/2023	79313	Falla en los servicios alcanzados por RST a ICETEX desde la VPN SSL	Solucionado
7/07/2023	67820	Bloqueo por el WAF a https://www.icetex.gov.co/portalacces/index.asp?idaplicamenu=1&visible=5&strNivel=0	Solucionado
7/07/2023	67858	Falla total de C&CTEX	Solucionado

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

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



CO-SC-CER921046

7/07/2023	13283	Falla de acceso usuarios Tiqui	Solucionado
7/07/2023	79382	Acceso a 443 y 4567 desde 192.168.158.11	Solucionado
7/07/2023	67668	Falla de acceso a 192.168.51.120 (\\ictxsrvfs) y \\192.168.51.80 (\\ictxsrvfs01)	Solucionado
Fecha	NUMERO DE CASO	ASUNTO	Estado del caso
7/07/2023	67711	Falla de acceso de 192.168.20.35 a internet (52.43.215.41) por puerto 443	Solucionado
6/07/2023	67801	Falla de comunicación entre 192.168.53.10 y 192.168.245.110 y 192.168.245.114	Solucionado
7/07/2023	67480	Acceso a http://win-imvrpavqqpn.icetex.gov.co/WSAC/principal.aspx y http://192.168.245.110:8080/smicetex/welcome.sm	Solucionado
7/07/2023	67641	Formato VPN banco BBVA	Solucionado

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

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



CO-SC-CER921046

7/07/2023	67384	Falla de acceso a web.millenium.com.co desde comware	Solucionado
Fecha	NUMERO DE CASO	ASUNTO	Estado del caso
11/07/2023	67907	Falla de acceso a 192.168.20.121/login.aspx	Solucionado
11/07/2023	13317	Caso gestionado bajo el caso 13321	Solucionado
11/07/2023	13334	Acceso por WIN SCP a 192.168.53.10	Solucionado
11/07/2023	68030	Acceso a http://192.168.245.114:8080/smicetex/login.sm	Solucionado
11/07/2023	13321	Acceso a http://digiturno5.comware.com.co para los puertos 8823, 8830, 8812 y 8810	Solucionado
11/07/2023	13321	Acceso a RSThttp://192.168.0.208/ecrm/	Solucionado

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

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



CO-SC-CER921046

12/07/2023	13287	Falla de acceso a https://mesadeservicios.icetex.gov.co/ASDKV8/Login.aspx (192.168.51.60)	Solucionado
12/07/2023	76743	No alcanza la impresora de Bucaramanga	Solucionado
12/07/2023	76743	No alcanza por RDP equipo de OutImpresion	Solucionado
Fecha	NUMERO DE CASO	ASUNTO	Estado del caso
12/07/2023	76743	No alcance a servidor de impresión aguas	Solucionado
12/07/2023	76743	No alcance a las impresoras de aguas	Solucionado
12/07/2023	76743	No alcance a la impresora de Cali	Solucionado
12/07/2023	67946	Falla Chat por Captcha RST	Solucionado
12/07/2023	67586	Falla de acceso a /Login/Validate?callback=http://acuerdos.icetex.gov.co/CallBack&app=CARTERA	Solucionado



INFOTIC
SOLUCIONES INTELIGENTES

Fecha	NUMERO DE CASO	ASUNTO	Estado del caso
12/07/2023	67704	No acceso a Twitter Comware	Solucionado
12/07/2023	68112	No acceso a 192.168.20.121 por RDP	Solucionado
12/07/2023	79640	No acceso acceso a https://graph.window s.net/, https://login.microsoft online.com/765c0330-c7d0-42cd-8f1f-980cbef05be5/oauth2 /token y https://graph.microsof t.com/beta/users/%7B 0%7D	Solucionado
12/07/2023	68122	No acceso a https://mesadeservici os.icetex.gov.co/usdkv 8/#/login/	Solucionado

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

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



CO-SC-CER921046



Fecha	NUMERO DE CASO	ASUNTO	Estado del caso
13/07/2023	68141	No acceso a https://pagares.bvc.com.co:1445/seguridad_web/faces/loginOTP.jsp intermitencia DNS	Solucionado
13/07/2023	68133	No acceso a https://pagares.bvc.com.co:1445/seguridad_web/faces/loginOTP.jsp intermitencia DNS	Solucionado
13/07/2023	67963	Sin acceso a http://ictxarandtestbd/ReportServer/Pages/ReportViewer.aspx?%2fReportes+Aranda+Icetetex%2fMenu&rs%3aCommand=Render	Solucionado
13/07/2023	79700	Acceso a 192.168.51.95	Solucionado
14/07/2023	N/A	Correo malicioso	Solucionado
14/07/2023	79762	No logra acceso a 192.168.53.10 por puerto 22 CIFIN, TransUnion	Solucionado
17/07/2023	79785	Comunicación Entre Bancolombia e ICETEX port 22	Solucionado



Fecha	NUMERO DE CASO	ASUNTO	Estado del caso
17/07/2023	68310	Comunicación Entre BCSC e ICETEX port 22	Solucionado
17/07/2023	68238	Bloqueo del WAF a C&CTEX	Solucionado
17/07/2023	68286	Falla de acceso a "Transparencia y Derecho de Acceso a la Información Pública"	<u>Solucionado</u>
18/07/2023	68305	Falla de Acceso a 192.168.20.30 y a la 192.168.20.31 por puerto 22 y 5432	Solucionado
18/07/2023	68332	Falla de Acceso a svr_aplic/portalaacces /	Solucionado
18/07/2023	68334	Falla de Acceso a svr_aplic/portalaacces /	Solucionado
18/07/2023	68336	Falla de Acceso a svr_aplic/portalaacces /	Solucionado



Fecha	NUMERO DE CASO	ASUNTO	Estado del caso
18/07/2023	13382	Falla de acceso a 192.168.245.106	Solucionado
19/07/2023	79954	Falla de conectividad por puerto 22 desde Banco Bogotá	Solucionado
19/07/2023	79644	Bloqueo del WAF a https://aplicaciones.icetex.gov.co/CargueArchivo	Solucionado
19/07/2023	13348	Se requiere acceso a http://192.168.0.208/ecrm y telefonía 192.168.0.240	Solucionado
19/07/2023	79968	Falla de conectividad por puerto 22 desde BBVA	Solucionado
19/07/2023	68289	Falla de conexión a 190.90.13.11	Solucionado
21/07/2023	68434	Falla de conexión a http://svr_aplic/portal/acces/	Solucionado
21/07/2023	68346	Falla de conexión a https://10.253.197.195/sslvpn/Login/Login	Solucionado



INFOTIC
SOLUCIONES INTELIGENTES

Fecha	NUMERO DE CASO	ASUNTO	Estado del caso
21/07/2023	68431	Falla de conexión a internet	Solucionado
21/07/2023	68390	Falla de logueo a Daruma	Solucionado
24/07/2023	80129	Falla de conectividad de 192.168.168.254 hacia 192.168.150.199	Solucionado
24/07/2023	68358	Bloqueo por parte del WAF a https://www.icetex.gov.co/portalacces/index.asp?visible=4&strNivel=1&IdAplicaMenu=1	Solucionado
24/07/2023	79706	Sr requiere acceso a 192.168.45.57 VMwareOperationAnalyzer	Solucionado
25/07/2023	68133	Intermitencia en el servicio Deceval	Solucionado
26/07/2023	80154	Publicación de la URL https://cina.icetex.gov.co/CuentasInactivasFront/login	Solucionado

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

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



CO-SC-CER921046



INFOTIC
SOLUCIONES INTELIGENTES

Fecha	NUMERO DE CASO	ASUNTO	Estado del caso
26/07/2023	80239	Falla de conexión a	Solucionado
27/07/2023	79721	Acceso con el flujo servidor 192.168.158.11 "Daruma" genera la petición hacia 10.158.7.21 "Bus" y posteriormente este va a orfeo "10.1.18.25" y este último vuelve a 192.168.158.11 "Daruma"	Solucionado
27/07/2023	80280	Se requiere acceso a 10.158.7.41 a través de la VPN de ZF	Solucionado
31/07/2023	68533	Falla de Acceso a http://192.168.158.11 /app.php/staff/ Desde VPN, redesde de sedes y Escritorio Remoto	Solucionado
31/07/2023	N/A	Acceso a internet a televisor 10.1.2.60	Solucionado
26/07/2023	N/A	Cambio de Peer VPN Registraduría	Solucionado

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

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



CO-SC-CER921046

Fecha	NUMERO DE CASO	ASUNTO	Estado del caso
28/07/2023	68359	No hay conexión desde http://192.168.20.35/app.php/staff/ hacia http://10.1.18.25/orfeo/login.php	Solucionado
21/07/2023	80039	bloqueo del waf en aplicaciones.icetex.gov.co/CargueArchivos/CargueArchivos	Solucionado

7.2. Actividades Pendientes

- ❑ Nos encontramos en proceso de ajustes de la migración, una vez finalizada esta actividad se validará estado final de las plataformas.
- ❑ Establecer redes NAT para todas las conexiones por VPN con la finalidad de proteger las IPs de los servidores reales y evitar replicaciones o solapamientos de las redes.
- ❑ Mejoramiento de este informe para una entrega de valor

8.1. Recomendaciones plataformas de seguridad

- ❑ Se debe realizar la validación de si los usuarios conectados a VPN y los que hacen uso de la VPN punto a punto, es necesario que naveguen a través del ICETEX.

8.2. Recomendaciones seguridad de ICETEX

- ❑ Se detecta que no existe segmentación definida en las redes de ICETEX que permitan establecer claramente que 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 de privilegios de accesos.
- ❑ Establecer proceso de hardening de equipos.
- ❑ Estructuración de análisis de incidentes.
- ❑ Estructurar y resguardar los procesos de críticos de la compañía a nivel de seguridad (ejm: tesorería).

9. CONCLUSIONES

- ❑ La segmentación de la red permite tener una mejor administración y control en caso de un incidente informático.
- ❑ El analizador de la red permite identificar que ocurre transversalmente en la red.
- ❑ El robustecimiento de la posición de la seguridad de la información de la entidad ICETEX, permite estar mejor posicionado frente a un incidente informático o de ciberseguridad.

CONCLUSIONES

En resumen, el mes de julio ha sido un período de logros notables en cuanto a la ejecución de las actividades programadas para el mantenimiento y la optimización de la plataforma. La revisión minuciosa y los ajustes aplicados a la infraestructura, así como la incorporación de nuevos servicios y la actualización de contenidos obsoletos, han desempeñado un papel fundamental en la elevación tanto del rendimiento como de la seguridad de la plataforma.

Un aspecto destacable reside en la proactividad demostrada por los especialistas involucrados. Gracias a su enfoque diligente, todas las situaciones presentadas fueron abordadas con prontitud, lo que condujo a una resolución eficaz de las solicitudes, incidentes y tareas de cambio que fueron notificadas. Estos resultados positivos reflejan el compromiso y la destreza del equipo en la gestión de los desafíos y en la consecución de soluciones efectivas.

En conjunto, los avances alcanzados durante este período son un testimonio del esfuerzo colectivo y la dedicación hacia la mejora continua. Estamos seguros de que estas acciones contribuirán de manera sustancial a la calidad y confiabilidad de la plataforma, beneficiando a nuestros usuarios y reforzando la posición de web.icetex como un recurso sólido y eficiente.