



INFORME MENSUAL MES DE ABRIL

CONTRATO NUMERO 2022-0792

INFORMACIÓN DEL DOCUMENTO

Fecha Creación	Versión del Documento	Responsable del Documento
01/04/2023	1.0	Carlos Alberto Alvira

Fecha Creación	Versión del Documento	Elaborado por
01/04/2023	1.0	Angie Paola Parra

1 Tabla de contenido

1 INTRODUCCION	5
2 OBJETIVO	5
3 INFORME– ADMINISTRADOR DE SOLUCIONES	6
3.1 INTRODUCCIÓN:	6
3.2 ACTIVIDADES DESARROLLADAS:	6
3.3 ANEXOS	7
3.4 CONCLUSIONES	8
4 INFORME ESPECIALIDAD DBA ORACLE	10
4.1 INTRODUCCIÓN	10
4.2 ACTIVIDADES DESARROLLADAS:	10
4.3 CONCLUSIONES:	20
5 INFORME ADMINISTRADOR DE RED	21
5.1 INTRODUCCIÓN:	21
5.2 ANEXOS	22
5.3 CONCLUSIONES	25
6 INFORME WEBMASTER	26
6.1 INTRODUCCIÓN	26
6.2 ACTIVIDADES DESARROLLADAS:	26
6.3 CONCLUSIONES:	28
7 INFORME ADMINISTRADORES DE SEGURIDAD	29
7.1 INTRODUCCIÓN	29
7.2 ESTADO GENERAL DE LAS PLATAFORMAS	29
7.3 TRÁFICO DESDE WAF WWW.ICETEX.GOV.CO	33
7.4 TRÁFICO DESDE WAF PORTAL.ICETEX.GOV.CO	34
7.5 TRÁFICO DESDE WAF COMUNIDAD.ICETEX.GOV.CO	34
7.6 TRÁFICO DESDE WAF COLOMBIACIENTIFICA.GOV.CO	35
7.7 TRÁFICO DESDE WAF IDENTIDAD.ICETEX.GOV.CO	35
7.8 ADMINISTRACIÓN PLATAFORMAS INCLUIDAS LAS PROPIEDADES DEL ICETEX Y LAS IAAS	36
7.9 DISPONIBILIDAD DE LAS PLATAFORMAS DE SEGURIDAD	37
7.9.1 FIREWALL_ZONA FRANCA	37
7.9.2 FIREWALL_AGUAS (FORTINET)	38
7.9.3 FIREWALL_MEDELLÍN	38
7.9.4 FORTIWEB	38
7.9.5 FORTISIEM	39
7.9.6 FORTISANDBOX	39
7.9.7 FORTIAUTHENTICATOR	39
7.9.8 FORTICLIENT EMS	40
7.10 GESTIÓN DE CASOS	40
7.11 ESTADO DE SALUD DE LOS EQUIPOS DE SEGURIDAD	41
7.12 FIREWALL AGUAS	41
7.13 FIREWALL FORTINET ZF	42
7.14 PERFILES DE SEGURIDAD	42
7.14.1 WEBFILTER.	42
7.14.2 . CATEGORÍAS MÁS VISITADAS	43

7.14.3	6.3. CONTROL DE APLICACIONES	45
7.14.4	FORTICLIENT EMS	45
7.14.5	FORTISIEM	46
7.15	ESTADO DE LICENCIAMIENTO DE PLATAFORMAS	46
7.15.1	FORTIGATE ZONA FRANCA	46
7.15.2	FORTISIEM	47
7.15.3	FORTISANDBOX	47
7.15.4	FORTIWEB	48
7.15.5	FORTIGATE AGUAS	48
7.15.6	FORTIGATE MEDELLÍN BALSOS	49
7.16	EVENTOS RELEVANTES	49
7.17	ACTIVIDADES	50
7.17.1	ACTIVIDADES REALIZADAS	50
7.17.2	ACTIVIDADES PENDIENTES	50
7.18	RECOMENDACIONES	50
7.19	CONCLUSIONES	50
8	CONCLUSION	51

1 INTRODUCCION

Para ofrecer una visión clara y detallada de las principales actividades y avances en la operación y optimización de nuestros portales y servicios web institucionales, presentamos el informe correspondiente al mes de abril. Este documento ha sido elaborado por los especialistas de infotic y se centra en destacar los servicios especializados en outsourcing requeridos por el contrato 2022-0792-2022 con el Icetex para la conectividad, red de comunicaciones, centro de datos y servicios conexos con valor agregado.

En el informe también se detallan las actividades llevadas a cabo en el desarrollo de los casos, tareas e incidentes que se escalaron a través de la mesa de servicio, así como las soluciones ejecutadas para satisfacer las solicitudes que se recibieron por otros medios de comunicación o herramientas colaborativas. Asimismo, se destaca la importancia de identificar la causa raíz de cada requerimiento escalado y aplicar una solución definitiva para minimizar el impacto en los usuarios y restaurar el acceso a las aplicaciones críticas lo más pronto posible. Cabe señalar que todos los procesos seguidos para solucionar las fallas o errores se han documentado cuidadosamente y se presentan los resultados obtenidos.

2 OBJETIVO

El presente informe tiene como objetivo destacar la calidad del servicio prestado por el equipo de especialistas en el mes de abril. Durante este periodo, se ha llevado a cabo la atención de todas las solicitudes, incidentes y tareas de cambios que se han registrado a través de todos los medios colaborativos que ofrece el Icetex.

Se ha trabajado de manera comprometida para atender todas las solicitudes que se han recibido, con el fin de garantizar la satisfacción de los usuarios y las necesidades del Icetex. Para ello, se han seguido rigurosos procesos de gestión y atención, que han permitido una atención eficiente y efectiva de todas las solicitudes y requerimientos que se han presentado.

3 INFORME– ADMINISTRADOR DE SOLUCIONES

3.1 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.

3.2 Actividades desarrolladas:

#	Fecha	Actividad	Evidencias
1	03/04/2023	Caso No. 64966, se deshabilitó Web Service del antiguo Reporteador.	Caso 64966.pdf
2	30/03/2023	Caso No. 64910, se solucionó falla al acceder a la opción Utilitarios – Emergencias Frecuentes – Solicitar Giro Complementario – Descargar Archivo Muestra.	Caso 64910.pdf
3	05/04/2023	Tarea No. 485031, se revisaron los permisos a directorios compartidos desde el servidor svr_aplic 192.1.1.4 y se habilitó el complemento SMB1 en el equipo del usuario.	Tarea 485031.pdf
4	04/04/2023	Caso No. 64983, se solucionó la falla en el servicio de acceso por FTP.	Caso 64983.pdf
5	19/04/2023	Tarea No. 486404, cargue de nuevos archivos .dll para la actualización del Web Service BusIcfes.	Tarea 486404.pdf
6	19/04/2023	Tarea No. 486400, cargue de nuevos archivos .dll para la actualización del Web Service ActualizacionMasivaDynamics.	Tarea 486400.pdf
7	20/04/2023	Caso No. 65422, se solucionó falla presentada en el ambiente de pruebas de la aplicación de cuentas abandonadas Web Service CabApi.	Tarea 65422.pdf
8	20/04/2023	Tarea No. 486434, cargue de nuevos archivos .dll para la actualización del Web Service PortalTransaccionalWebSite.	Tarea 486434.pdf
9	20/04/2023	Tarea No. 48266, cargue de nuevos archivos .dll para la actualización del Web Service PortalTransaccionalWebService.	Tarea 48266.pdf
10	20/04/2023	Tarea No. 486475, cargue de nuevos archivos .dll para la actualización del Web Service WsApiSolicitudes.	Tarea 486475.pdf
11	13/04/2023	Caso No 65212, reinicio de servidor MIRA producción https://www.icetex.gov.co/portalacces/ debido a bloqueo en sistema Operativo.	Reporte Falla Servidor Mira - Producción.pdf

12	13/04/2023	Caso No 65214, reinicio de servidor MIRA producción debido a bloqueo en sistema Operativo. https://www.icetex.gov.co/portalacces/	Reporte Falla Servidor Mira - Producción.pdf
13	13/04/2023	Caso No 65224, reinicio de servidor MIRA producción debido a bloqueo en sistema Operativo. https://www.icetex.gov.co/portalacces/	Reporte Falla Servidor Mira - Producción.pdf
14	13/04/2023	Caso No 65231, reinicio de servidor MIRA producción debido a bloqueo en sistema Operativo. https://www.icetex.gov.co/portalacces/	Reporte Falla Servidor Mira - Producción.pdf
15	14/04/2023	Tarea No. 486151, Se realiza la copia de la imagen (899999230.png), en el servidor de producción 192.168.51.165 donde se encuentra alojada la aplicación https://aplicaciones.icetex.gov.co/VotoElectronico/IcetexVotoElectronico en la ruta F:\aplicaciones\VotoElectronico\IcetexVotoElectronico\assets\Imagenes	Tarea 486151.pdf
16	17/04/2023	Tarea 486190, se valida la conexión desde mi PC con el usuario dcano en FileZilla al servidor 192.168.51.165 y conecta con la VPN activa, con esto se comprueba que el usuario dcano a nivel de permisos de servidor funciona, se escala con operador de seguridad.	Tarea 486190.pdf
17	20/04/2023	Tarea 485167, se realizó el despliegue de los ajustes del servicio webhook para SM en la App Pool WsPasarela de manera satisfactoria.	Tarea 485167.pdf
18	19/04/2023	Tarea 485903, se valida con la responsable de la aplicación de inprocess Sally Carcamo y la usuaria irojasm presenta bloqueos por parte de directorio activo, se le informa a Sandra Torres de las validaciones hechas.	Tarea 485903.pdf
19	19/04/2023	Tarea 486402, se confirma cambio realizado sobre apisolicitudes (ver imagen).	Tarea 486402.pdf
20	24/04/2023	Tarea 496670, se le dio acceso al usuario jfparra al servidor 192.168.51.165 para acceder a las carpetas compartidas de Vicepresidencia de crédito, se le indico que debe validar la conexión una vez le instalen el FileZilla.	Tarea 486670.pdf
21	19/04/2023	Tarea 486740 se valida en el servidor 192.1.1.4 y se toman las imágenes donde se evidencia los usuarios que tienen acceso y permisos que tengan de lectura y/o escritura de la carpeta compartida de nómina. Se adjunta archivo.	Tarea 486740.pdf

3.3 Anexos

Anexo 1: Informe de Obsolescencia Windows Servidor 200

A parte de las evidencias detalladas en el capítulo anterior, incorporamos el siguiente enlace: [Informe de Obsolescencia Windows Servidor 2003.pdf](#), el cual detalla las implicaciones que se deben tener presentes en relación con la utilización del sistema operativo Windows Server 2003.

El informe señala que el sistema operativo Windows Server 2003 ya no recibe soporte de seguridad desde julio de 2015, lo que significa que cualquier vulnerabilidad en el sistema operativo no se corregirá, lo que aumenta el riesgo de ataques cibernéticos y la exposición a amenazas de seguridad. Además, el informe destaca que la falta de soporte también implica la imposibilidad para recibir actualizaciones de software,

lo que significa que este sistema operativo está limitado para mantenerse actualizado con los últimos parches de seguridad.

Anexo 2: Actividades desarrolladas que no se escalaron por Mesa de Servicio Aranda

Durante el mes de abril de 2023, el equipo de Administradores de Soluciones ha 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. Error en portal <https://web.icetex.gov.co/portal> reportado por Sandra Nocua Diseñadora Web.
2. Backup de diversos Web Service que contienen aplicaciones críticas.
3. Caso 700 solucionado por el antiguo administrador de soluciones de Internexa, sin embargo, a pesar de estar solucionado el caso, Jeisson Delgado reportó a través de correo electrónico que la aplicación estaba presentando el error 500.30 al momento de accederla vía web, por ello se revisó la solicitud y se procedió a dar solución definitiva para su correcta funcionalidad.
4. Solución a falla reportada por Pablo Vargas referente al servicio de Reportes que se encuentra alojado en el servidor svr_aplic.
5. Redireccionamiento de url <https://www.icetex.gov.co/portalaces/Tradicional/Estado/consultaPOL.asp> hacia <https://aplicaciones.icetex.gov.co/WebsitePSE/login>
6. Depuración de logs en servidores debido al poco espacio que quedaba en una de las particiones.
7. Monitoreo de Servicios a cargo del equipo de Administradores de Soluciones.
8. Sesión de trabajo realizada con el Ing. Jose Antonio Bolaño en donde se le dio solución para que lograra enviar correos masivos a través del WebServiceVotoElectronico.
9. Por solicitud del Ing. Jhon Pava Administrador de Seguridad, se le envió por medio de correo electrónico el certificado Wildcard *.icetex.gov.co que se encuentra configurado en el servidor web IIS de los servidores.
10. Se soluciona falla en el ingreso a la aplicación <http://10.1.18.124:6580/RegistroUsuariosPJ/#/login> reportada por el Ing. Raúl Gutiérrez y Andrés Carrillo.
11. Se comparte información del Web Service WsBuslcfes a los Ingenieros Jeisson Delgado y Andrés Vargas para consumir los servicios de la aplicación <https://appwebservices.icetex.gov.co/WsBuslcfes/api/ConsultaIndividual>.

Aunque estas actividades no se han escalado a través de la Mesa de Servicio Aranda, el equipo de Administradores de soluciones ha 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.

3.4 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 abril 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.

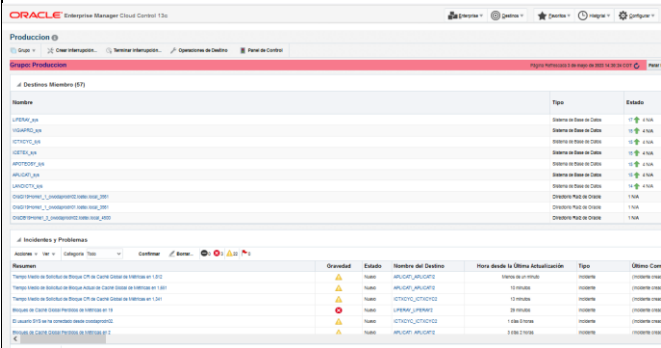
4 INFORME ESPECIALIDAD DBA ORACLE

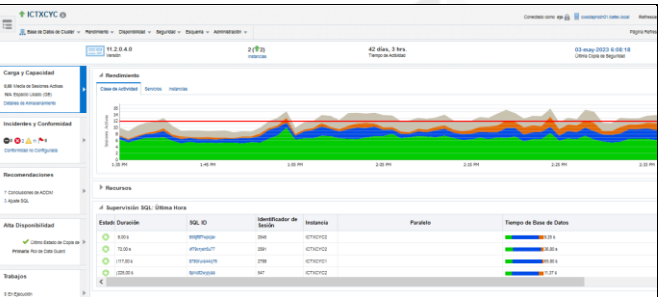
4.1 Introducción

Parametrización y configuración de plataforma de monitoreo para lograr estabilización de la misma, estandarización de plataforma mediante aplicación de tareas de mantenimiento estándar en la industria con el fin de mejorar el desempeño de las Bases de datos de la operación actual

4.2 Actividades desarrolladas:

#	Fecha	Actividad	Evidencias
1	Marzo 2023	Configuración y parametrización de la consola de monitoreo sobre los ambientes de producción.	- Se realiza configuración de plantillas de monitoreo. TEMPLATE_CLUSTER_INSTANCE TEMPLATE_DB_ICLUSTER TEMPLATE_DB_INSTANCE - Se realiza configuración de Métricas Extendidas en la consola. - Se crea grupo dinámico de producción y se agregan las Bases de datos del RAC productivo. - Se crea juego de reglas para el manejo de alertas e incidentes en el grupo de producción. - Esto nos permite y genera una visibilidad general sobre todos los componentes de las diferentes bases de datos usando las métricas estándar del producto y algunas adicionales que se creen convenientes recolectar para llevar los ambientes a cumplir con los estándares internacionales. - Permite reaccionar de manera proactiva a las diferentes alertas de espacio, red, contención, de las bases de datos y los servidores en las cuales estas se encuentran, permitiendo la visibilidad del estado y performance de los ya antes mencionados entre muchos otros componentes que se deberían estar monitoreando de los ambientes actualmente. - Se instala el monitoreo de desempeño en tiempo real para cada una de las Bases de datos del ambiente de producción, esto permite visibilidad en tiempo real de las consultas en ejecución y el consumo de recurso real sobre cada una de las

			Bases de datos para un mejor análisis de desempeños de la misma. 8. Anexo sobre UDM o user define metrics definidas para validar que hayan estándares implementados sobre las Bases de datos: 9. https://icetex-my.sharepoint.com/:x:/r/personal/nm_urcia_icetex_gov_co/Documents/Inventario%20Metricas%20Cloud%20ICTX.xlsx?d=w30674c56204d414fb4b3e63278963266&csf=1&web=1&e=sY3KPZ 10. Se crea línea base de monitoreo para objetos inválidos, constraints deshabilitados, Jobs brokeny Scheduler Jobs fallidos entre otros componentes, estos objetos de línea base se crean bajo el esquema dbnsmp el cual usa Oracle como estándar para el monitoreo por medio de la consola OEM. 11. Esto nos permite realizar un monitoreo real partiendo del estado actual de los objetos y componentes que tiene consistentes cada una de las BD's en estos momentos, esto en conjunto con el monitoreo en tiempo real permite una visión general del estado real de las diferentes bases de datos Consola de Monitoreo de Plataforma de producción con Alertamiento en tiempo real:  Hub de rendimiento de las diferentes BD's en ambiente productivo:
--	--	--	---

			
	Abril 2023	Implementación de tareas de mantenimiento (defragmentación de índices y toma de estadísticas de las Bases de datos de producción)	12. Las estadísticas que se estaban tomando en las bases de datos eran sobre objetos específicos que no se actualizaban desde Junio del 2022 y no incluían el diccionario de datos o los fixed objects, se incluyen los objetos de todos los esquemas al igual que las estadísticas del diccionario y los fixed objects. 13. Las nuevas tareas se dejaron en el crontab del nodo 1 del RAC y en el nodo 2 están las antiguas estadísticas que se tomaban de las Bases de datos comentareadas con el fin de que no se ejecuten. 14. La toma correcta de estadísticas permite que el motor identifique la mejor forma de solucionar una consulta y de esta manera genera un plan de ejecución para que el desempeño del query mejore cada vez que la consulta ingrese a la BD, de igual forma la defragmentación de índices no solo recupera espacio en disco de las hojas en blanco de los árboles de los índices sino que también mejora el rendimiento de las consultas que hacen uso de estos. Crontab nodo1: <pre> [oracle:cxvoadprodnd01 @ /u01/app/oracle/diag/rdbms/apoteosy/APOTEOSY1]\$ crontab -l #Ejecucion de estadísticas 11g 00 20 * * 6 sh /u01/app/oracle/mantenimiento/scripts/run_stats_11.sh ICTXCYC1 >/dev/null 2>&1 00 20 * * 6 sh /u01/app/oracle/mantenimiento/scripts/run_stats_11.sh ICETEX1 >/dev/null 2>&1 00 20 * * 6 sh /u01/app/oracle/mantenimiento/scripts/run_stats_11.sh APLICAT11 >/dev/null 2>&1 00 20 * * 6 sh /u01/app/oracle/mantenimiento/scripts/run_stats_11.sh APOTEOSY1 >/dev/null 2>&1 00 20 * * 6 sh /u01/app/oracle/mantenimiento/scripts/run_stats_11.sh VIGIAPRD1 >/dev/null 2>&1 #Ejecucion de estadísticas 19 normal 00 20 * * 6 sh /u01/app/oracle/mantenimiento/scripts/run_stats_19.sh LANDICTX1 >/dev/null 2>&1 #Ejecucion de estadísticas 19 contenedor y pluggable 00 20 * * 6 sh /u01/app/oracle/mantenimiento/scripts/run_stats_19_cont.sh LIFERAY1 LIFERAYPDB >/dev/null 2>&1 #Rebuild Indexes 11g 15 22 * * 5 sh /u01/app/oracle/mantenimiento/scripts/run_rebuild_11.sh ICTXCYC1 >/dev/null 2>&1 15 22 * * 5 sh /u01/app/oracle/mantenimiento/scripts/run_rebuild_11.sh ICETEX1 >/dev/null 2>&1 15 22 * * 5 sh /u01/app/oracle/mantenimiento/scripts/run_rebuild_11.sh APLICAT11 >/dev/null 2>&1 15 22 * * 5 sh /u01/app/oracle/mantenimiento/scripts/run_rebuild_11.sh APOTEOSY1 >/dev/null 2>&1 15 22 * * 5 sh /u01/app/oracle/mantenimiento/scripts/run_rebuild_11.sh VIGIAPRD1 >/dev/null 2>&1 #Rebuild 19 15 22 * * 5 sh /u01/app/oracle/mantenimiento/scripts/run_rebuild_19.sh LANDICTX1 >/dev/null 2>&19 #Rebuild 19 contenedor y pluggable 17 22 * * 5 sh /u01/app/oracle/mantenimiento/scripts/run_rebuild_19.sh LIFERAY1 LIFERAYPDB >/dev/null 2>&19 [oracle:cxvoadprodnd01 @ /u01/app/oracle/diag/rdbms/apoteosy/APOTEOSY1]\$ </pre> Crontab nodo2:



			<pre>[oracle:cxvoadprod02 @ /u01/app/oracle/diag/rdbms/apoteosy/APOTEOSY2]\$ crontab -l ##----- BACKUP ----- 02 18,21,22,23,01,03 * * * /odadaf/scripts/backup/DATABASE_BACKUP.sh > /dev/null 00 03,09,13,14,15 01 * * /odadaf/scripts/backup/EXPDP_MENSUAL.sh >> /dev/null 00 * * * /odadaf/scripts/backup/ARCHIVELOG_BACKUP.sh > /dev/null ##----- STATS ----- #40 01 * * * /odadaf/scripts/statistics/estadisticasAPOTEOSY.sh #40 01 * * * /odadaf/scripts/statistics/estadisticasAPLICATI.sh #40 01 * * * /odadaf/scripts/statistics/estadisticasICETEX.sh #40 01 * * * /odadaf/scripts/statistics/estadisticasLIFERAY.sh #40 01 * * * /odadaf/scripts/statistics/estadisticasVIGIAPRD.sh #00 02 * * * /odadaf/scripts/statistics/estadisticasICTXCYC.sh [oracle:cxvoadprod02 @ /u01/app/oracle/diag/rdbms/apoteosy/APOTEOSY2]\$ █</pre>
3	Abril 2023	Se arregla el /etc/oratab de ambos nodos del RAC para que se ejecute de manera correcta la funcionalidad .oraenv	Oratab nodo1: <pre>[oracle:cxvoadprod01 @ /u01/app/oracle/diag/rdbms/apoteosy/APOTEOSY1]\$ cat /etc/oratab #Backup file is /grid/app/grid/crsdata/cxvoadprod01/output/oratab.bak.cxvoadprod01.oracle line # # This file is used by ORACLE utilities. It is created by root.sh # and updated by either Database Configuration Assistant while creating # a database or ASM Configuration Assistant while creating ASM instance. # A colon, ':', is used as the field terminator. A new line terminates # the entry. Lines beginning with a pound sign, '#', are comments. # # Entries are of the form: # # \$ORACLE_SID:\$ORACLE_HOME:<N Y>: # # The first and second fields are the system identifier and home # directory of the database respectively. The third field indicates # to the dbstart utility that the database should, "Y", or should not, # "N", be brought up at system boot time. # # Multiple entries with the same \$ORACLE_SID are not allowed. # # VIGIAPRD1:/u01/app/oracle/product/11.2.0.4/dbhome_1:N APLICATI1:/u01/app/oracle/product/11.2.0.4/dbhome_1:N APOTEOSY1:/u01/app/oracle/product/11.2.0.4/dbhome_1:N APOTNEW1:/u01/app/oracle/product/11.2.0.4/dbhome_1:N ICTXCYC1:/u01/app/oracle/product/11.2.0.4/dbhome_1:N ICETEX1:/u01/app/oracle/product/11.2.0.4/dbhome_1:N LIFERAY1:/u01/app/oracle/product/19.3.0/dbhome_1:N LIFERAYDB1:/u01/app/oracle/product/19.3.0/dbhome_1:N LANDICTX1:/u01/app/oracle/product/19.3.0/dbhome_1:N +ASM1:/grid/app/product/19.3.0:N Oratab nodo2:</pre> <pre>[oracle:cxvoadprod02 @ /home/oracle]\$ cat /etc/oratab #Backup file is /grid/app/grid/crsdata/cxvoadprod02/output/oratab.bak.cxvoadprod02.oracle line added # # This file is used by ORACLE utilities. It is created by root.sh # and updated by either Database Configuration Assistant while creating # a database or ASM Configuration Assistant while creating ASM instance. # A colon, ':', is used as the field terminator. A new line terminates # the entry. Lines beginning with a pound sign, '#', are comments. # # Entries are of the form: # # \$ORACLE_SID:\$ORACLE_HOME:<N Y>: # # The first and second fields are the system identifier and home # directory of the database respectively. The third field indicates # to the dbstart utility that the database should, "Y", or should not, # "N", be brought up at system boot time. # # Multiple entries with the same \$ORACLE_SID are not allowed. # # ICTXCYC2:/u01/app/oracle/product/11.2.0.4/dbhome_1:N # line added by Agent APOTEOSY2:/u01/app/oracle/product/11.2.0.4/dbhome_1:N # line added by Agent APOTNEW2:/u01/app/oracle/product/11.2.0.4/dbhome_1:N # line added by Agent ICETEX2:/u01/app/oracle/product/11.2.0.4/dbhome_1:N # line added by Agent APLICATI2:/u01/app/oracle/product/11.2.0.4/dbhome_1:N # line added by Agent VIGIAPRD2:/u01/app/oracle/product/11.2.0.4/dbhome_1:N # line added by Agent LIFERAY2:/u01/app/oracle/product/19.3.0/dbhome_1:N LANDICTX2:/u01/app/oracle/product/19.3.0/dbhome_1:N LIFERAYDB2:/u01/app/oracle/product/19.3.0/dbhome_1:N +ASM2:/grid/app/product/19.3.0:N [oracle:cxvoadprod02 @ /home/oracle]\$ █</pre>
4	Abril 2023	Se realiza ejecución de paso de réplica a BD LANDICTX desde PROD, 3 horas de export, 1 hora y media paso de archivos y 4 horas y media de importación (noche del 05/04/2023)	• se crean scripts para importación en server ICTXDBORACLINUX • /Backup/LANDICTX/mensual/import_tables.sh • /Backup/LANDICTX/mensual/import_emptytables.sh Se generan scripts y se documenta procedimiento para refresh de la BD:

			<pre> cd /odadafs/backup/LANDICTX/load/ rm -rf nohup.out .oranev ICTXCYC1 nohup ./export_tables.sh & nohup ./export_emptytables.sh & scp /odadafs/backup/ICTXCYC/mensual/expdp ICTXCYC2_ TABLAS*.dmp 192.168.51.97:/Backup/LANDICTX/mensual ssh 192.168.51.97 cd /Backup/LANDICTX/mensual . oraenv LANDICTX nohup ./import_tables.sh & nohup ./import_emptytables.sh & -- se depuran los dmp al finalizar el proceso en el destino rm -rf /odadafs/backup/ICTXCYC/mensual/expdp ICTXCYC2_ TABLAS*.dmp rm -rf /odadafs/backup/ICTXCYC/mensual/expdp ICTXCYC2_ TABLAS*.dmp 2. En estos momentos ya se realizó un refresh del ambiente de forma exitosa usando los pasos documentados en este informe. </pre>
5	Abril 2023	Instalación de grid infraestructura 19.3 en servidor 10.1.4.95, las bases de datos estaban en FS aun cuando el ambiente productivo esta en RAC, se iguala a la versión de Producción,.	bajada BD DEV_95 para ver discos 500G en formato asm con el fin de instalar grid infrastructure en el server creacion de usuario grid en DEV_95 con grupos, etc adiccion de usuario grupos, etc descargado de producto de GRID modificacion parametros de kernel <pre> [root@desa sysctl.d]# pwd /etc/sysctl.d [root@desa sysctl.d]# ls -lart total 16 lrwxrwxrwx. 1 root root 14 Aug 11 2017 99-sysctl.conf -> ../sysctl.conf -rw-r--r--. 1 root root 310 Apr 19 19:45 97-oracle- database-sysctl.conf drwxr-xr-x. 2 root root 66 Apr 19 19:45 . drwxr-xr-x. 82 root root 8192 Apr 19 20:20 .. [root@desa sysctl.d]# cat 99-sysctl.conf # sysctl settings are defined through files in </pre>

		<pre> # /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/. # # Vendors settings live in /usr/lib/sysctl.d/. # To override a whole file, create a new file with the # same in # /etc/sysctl.d/ and put new settings there. To override # only specific settings, add a file with a lexically later # name in /etc/sysctl.d/ and put new settings there. # # For more information, see sysctl.conf(5) and sysctl.d(5). net.ipv4.ip_forward = 0 net.ipv4.conf.default.rp_filter = 1 net.ipv4.conf.default.accept_source_route = 0 kernel.sysrq = 0 kernel.core_uses_pid = 1 net.ipv4.ip_local_port_range = 9000 65535 net.core.rmem_default = 262144 net.core.rmem_max = 4194304 net.core.wmem_default = 262144 net.core.wmem_max = 1048576 kernel.sem = 250 32000 100 128 kernel.shmmax = 15676209152 kernel.shmall = 3827199 [root@desa dev]# cat /etc/sysctl.d/97-oracle-database- sysctl.conf fs.aio-max-nr = 1048576 fs.file-max = 6815744 kernel.shmall = 3827199 kernel.shmmax = 15676209152 kernel.shmmni = 4096 kernel.sem = 250 32000 100 128 net.ipv4.ip_local_port_range = 9000 65500 net.core.rmem_default = 262144 net.core.rmem_max = 4194304 net.core.wmem_default = 262144 net.core.wmem_max = 1048576 instalacion librerias de S.OEM creacion bash_profile para usuario grid formateo de discos a formato ASM como root fdisk /dev/sdg n, p, 1, ENTER, ENTER, w fdisk /dev/sdh n, p, 1, ENTER, ENTER, w fdisk /dev/sdi n, p, 1, ENTER, ENTER, w </pre>
--	--	--

		<pre>fdisk /dev/sdj n, p, 1, ENTER, ENTER, w fdisk -l grep "/dev/sd" oracleasm createdisk DATADISK1 /dev/sdg1 oracleasm createdisk DATADISK2 /dev/sdh1 oracleasm createdisk DATADISK3 /dev/sdi1 oracleasm createdisk DATADISK4 /dev/sdj1 oracleasm listdisks unzip /u01/medios/LINUX.X64_193000_grid_home.zip -d \$ORACLE_HOME cd \$ORACLE_HOME ./gridSetup.sh</pre> Se añaden servicios de BD al OCR <pre>srvctl add database -d APOT srvctl add database -d APOTNEW srvctl add database -d sicci</pre> Se modifican parametros de meoria de las BD's para que usen AMM (este proceso se realiza por BD): <pre>alter system set memory_max_target=2G scope=spfile; alter system set memory_target=2G scope=spfile; alter system set sga_max_size=0 scope=spfile; alter system set sga_target=0 scope=spfile; alter system set pga_aggregate_target=0 scope=spfile;</pre> se reinician las BD's y se reinicia el server para probar el <pre>oracle restart</pre> <pre>fdisk /dev/sdk n, p, 1, ENTER, ENTER, w fdisk /dev/sdl n, p, 1, ENTER, ENTER, w oracleasm createdisk DATADISK5 /dev/sdk1 oracleasm createdisk DATADISK6 /dev/sdl1</pre> Se realiza instalación de GI mediante el GI con un diskgroup de datos que incluye los discos anteriormente presentados y creados a nivel de S.O. Se remite Validación de la Infraestructura bajo el usuario grid con los servicios del CRS adicionados por cada Base datos, así no toca subir las BD's de forma manual cada vez que el server suba sino que el mismo Oracle restart realiza la subida automática de servicios,
--	--	---



			<pre>[grid@desa ~]\$ crsctl status res -t ----- Name Target State Server State details ----- Local Resources ----- ora.DATA.dg ONLINE ONLINE desa STABLE ora.LISTENER.lsnr ONLINE ONLINE desa STABLE ora.asm ONLINE ONLINE desa Started,STABLE ora.ons OFFLINE OFFLINE desa STABLE Cluster Resources ----- ora.apot.db 1 ONLINE ONLINE desa Open,HOME=/u01/app/oracle/product/11.2.0/dbhome_1,STABLE ora.apotnew.db 1 ONLINE ONLINE desa Open,HOME=/u01/app/oracle/product/11.2.0/dbhome_1,STABLE ora.cssd 1 ONLINE ONLINE desa STABLE ora.diskmon 1 OFFLINE OFFLINE STABLE ora.evmd 1 ONLINE ONLINE desa STABLE ora.sicci.db 1 ONLINE ONLINE desa Open,HOME=/u01/app/oracle/product/11.2.0/dbhome_1,STABLE ----- [grid@desa ~]\$</pre>
6	Abril 2023	Se genera proceso para refresh de la BD APOT del server 10.1.4.95 por medio de rman duplicate from active database sin necesidad de usar staging área, generando un ahorro de 400G de espacio en el server destino y de mas de 4 horas en el proceso total de restauración.	<pre>-----REFRESH APOT----- nohup rman TARGET sys/six@APOTEOSY AUXILIARY sys/six@REMOTE_APOTEOSY @refreshApot.rman > refreshApot.log & -----Borrado de la antigua apot desde rman en el dev_95----- .oraenv APOT rman target / shutdown abort startup force mount SQL 'alter system enable restricted session'; crosscheck archivelog all; delete noprompt archivelog all; delete backup; delete obsolete; drop database; yes exit -----Contenido del script refreshApot.rman----- ----- run { allocate channel p1 type disk;</pre>

			allocate auxiliary channel s1 type disk; DUPLICATE TARGET DATABASE TO APOT FROM ACTIVE DATABASE NOFILENAMECHECK; } -----Script con 6 canales----- run { allocate channel p1 type disk; allocate channel p2 type disk; allocate channel p3 type disk; allocate channel p4 type disk; allocate channel p5 type disk; allocate channel p6 type disk; allocate auxiliary channel s1 type disk; allocate auxiliary channel s2 type disk; allocate auxiliary channel s3 type disk; allocate auxiliary channel s4 type disk; allocate auxiliary channel s5 type disk; allocate auxiliary channel s6 type disk; DUPLICATE TARGET DATABASE TO APOT FROM ACTIVE DATABASE NOFILENAMECHECK; } 3. En estos momentos ya se realizó un refresh del ambiente de forma exitosa usando los pasos documentados en este informe.
7	Abril 2023	Se genera, prueba y documenta Proceso de Refresh BD SICCI / aún en proceso	se crean scripts de export se crean parfiles se dejan scripts de automatización en la siguiente ruta /odadafs/backup/SICCI/load se pasa tabla TBL_LZ de SICCI a prod bajo esquema DBSNMP en prod creamos el directorio create or replace directory DIR_EXP_TABS_SICCI as '/odadafs/backup/SICCI/load'; grant read, write on directory DIR_EXP_TABS_SICCI to sys; se generan parfiles -----exp.parfile DIRECTORY=EXPDP_MENSUAL SCHEMAS=ICETEX_NUEVO,CONCILIACIONES,CAB,LLOZ ANO,HJARABA,GIROSYA,CONCILIACIONESPROD,CONTR ALORIA,PCARRILLO,SFC_QUEJASYRECLAMOS,SYSTEM, ACTUALIZACION,DLANCERA,POWERBI,AUDITORIA,RES TORE_CUENTAS,CONDOPRU,ECASTILLO,CONEXION,CB

		P_COREBPERSOAL,HOMOLOGA,OSALAZAR,FATRIBMT IC,CONDO INCLUDE=TABLE:"IN(select table_name from dbsnmp.tbl_lz where accion#=1)" -----exp_emptytables.parfile DIRECTORY=EXPDP_MENSUAL SCHEMAS=ICETEX_NUEVO,CONCILIACIONES,CAB,LLOZ ANO,HJARABA,GIROSYA,CONCILIACIONESPROD,CONTR ALORIA,PCARRILLO,SFC_QUEJASYRECLAMOS,SYSTEM, ACTUALIZACION,DLANCERA,POWERBI,AUDITORIA,RES TORE_CUENTAS,CONDOPRU,ECASTILLO,CONEXION,CB P_COREBPERSOAL,HOMOLOGA,OSALAZAR,FATRIBMT IC,CONDO CONTENT=METADATA_ONLY INCLUDE=TABLE:"IN(SELECT TABLE_NAME FROM DBSNMP.TBL_LZ WHERE ACCION#=2)" -----exp_metadata.parfile DIRECTORY=EXPDP_MENSUAL SCHEMAS=ICETEX_NUEVO,CONCILIACIONES,CAB,LLOZ ANO,HJARABA,GIROSYA,CONCILIACIONESPROD,CONTR ALORIA,PCARRILLO,SFC_QUEJASYRECLAMOS,SYSTEM, ACTUALIZACION,DLANCERA,POWERBI,AUDITORIA,RES TORE_CUENTAS,CONDOPRU,ECASTILLO,CONEXION,CB P_COREBPERSOAL,HOMOLOGA,OSALAZAR,FATRIBMT IC,CONDO CONTENT=METADATA_ONLY EXCLUDE=TABLE se generan shell para ejecucion de exports requeridos -----export_tables.sh expdp \"/ AS SYSDBA\" parfile=exp.parfile dumpfile=expdp_ICTXCYC_TABLAS_SICCI95.dmp logfile=expdp_ICTXCYC_TABLAS_SICCI95.dmp.log -----export_metadata.sh expdp \"/ AS SYSDBA\" parfile=exp_metadata.parfile dumpfile=expdp_ICTXCYC_META_SICCI95.dmp logfile=expdp_ICTXCYC_META_SICCI95.dmp.log -----export_emptytables.sh expdp \"/ AS SYSDBA\" parfile=exp_emptytables.parfile dumpfile=expdp_ICTXCYC_EMPTYTAB_SICCI95.dmp logfile=expdp_ICTXCYC_EMPTYTAB_SICCI95.dmp.log se realiza paso de los dmp al sitio destino dejándolos en ejecución en background: scp expdp_ICTXCYC_TABLAS_SICCI95.dmp 10.1.4.95:/u02/sicci/exp ctrl + z bg
--	--	--

			scp expdp ICTXCYC_META_SICCI95.dmp 10.1.4.95:/u02/sicci/exp ctrl + z bg scp expdp ICTXCYC_EMPTYTAB_SICCI95.dmp 10.1.4.95:/u02/sicci/exp ctrl + z bg Se generan parfiles de import en el destino Se generan shell de import en el destino se dejan scripts en la siguiente ruta se prueba import y se corrigen errores:
8	Abril 2023	Se realiza proceso para Refresh de la data de la BD VIGIAPRD en la versión 19c mediante procedimiento de export import.	1. En estos momentos ya se realizó un refresh del ambiente de forma exitosa usando los pasos documentados en este informe. 2. El día jueves 4 de Mayo del 2023 en horas de la tarde se realizará el paso a producción del ambiente refrescado en la versión actualizada 19c usando este procedimiento.

4.3 Conclusiones:

5 INFORME ADMINISTRADOR DE RED

5.1 Introducción:

Se presenta informe mensual con los casos atendidos y solucionados., se ha logrado resolver cada uno de los problemas que se nos han presentado de manera oportuna y eficiente.

#	Fecha	Actividad	Evidencias
	03/04/2023	Se debe de ejecutar el RFC 728 cambio de servidor DHCP Core a servidores dedicados DHCP de la identidad debido a intermitencias en el servicio de wifi	RFC 728
	06/04/2023	Se crea caso en Aranda número IM-231945-4-65398 expresando que la sede ARAUCA se encuentra sin servicio de internet, para dar solución al inconveniente se escala el caso con el proveedor de servicio expresando que hay daño en la UM del servicio, se hace desplazamiento de personal para hacer las reparaciones necesarias en la UM normalizando el servicio	IM-231945-4-65398
	08/04/2023	Se crea caso en Aranda número IM-231543-4-65277 expresando que la sede CARTAGENA se encuentra sin servicio de internet, se encuentre un puerto alarmado en el router de la sede se procede a hacer un reunió del puerto y verificar el servicio con personal en la sede	IM-231543-4-65277
	10/04/2023	Se crea caso en Aranda número IM-231260-4-65209 expresando que la sede Arauca se encuentra sin servicio de internet, Se hace el escalamiento con el proveedor de servicio indicando que hay falla en la UM, se hacen verificaciones en los equipos y se procede a hacer reinicio de puertos solucionando el inconveniente	IM-231260-4-65209
	12/04/2023	Se crea caso en Aranda número IM-231119-4-65166 expresando que la sede Popayán se encuentra sin servicio de internet, Se hace el escalamiento con el proveedor de servicio indicando que hay falla en la UM, se hacen verificaciones en los equipos y se procede a hacer reinicio de puertos solucionando el inconveniente	IM-231119-4-65166
		Se crea caso en Aranda número IM-232543-4-65637 expresando que la sede Cúcuta se encuentra sin servicio de internet. Se procede a realizar la verificación de los equipos en sede encontrando un loop en el servicio de internet, Se hace el escalamiento con el proveedor de servicio de nivel 3 descartando enrutamiento, se solicita por parte de Ictetex desplazamiento de personal técnico a sitio para conectarse directamente a los equipos de red	IM-232543-4-65637



		Funcionará crea caso en Aranda IM-232485-4-65604 expresando que no tiene llamada a celular, larga distancia y nacional, se procede a realizar el chequeo de la línea 5512 en el call manager, encontrando que dicha extensión no formaba parte de las extensiones de funcionarios, para solucionar el inconveniente se hace el cambio de grupo y se le explica a la funcionaria como realizar llamadas	IM-232485-4-65604

5.2 Anexos

Se debe de ejecutar el RFC 728 cambio de servidor DHCP Core a servidores dedicados DHCP de la identidad debido a intermitencias en el servicio de wifi

Monitor

System Name: WLC-AGUAS
Up Time: 37 days, 18 hours, 29 minutes
System Time: Wed Apr 27 04:48:09 2016
Redundancy Mode: Disabled
Internal Temperature: +32 C
802.11a Network State: Enabled
802.11b/g Network State: Enabled
Local Mobility Group: ICETEX
CPU(s) Usage: 0%
Individual CPU Usage: 0%/1%, 0%/1%, 0%/1%, 0%/1%, 0%/1%, 0%/1%, 0%/0%, 0%/1%, 0%/0%, 0%/0%
Memory Usage: 41%
Fan Status: OK
Power Supply 1: Present, OK
Power Supply 2: Absent

Access Point Summary

	Total	Up	Down
802.11a/n/ac Radios	13	13	0
802.11b/g/n Radios	13	13	0
Dual-Band Radios	0	0	0
All APs	13	13	0

Client Summary

Current Clients	78
Excluded Clients	0
Disabled Clients	0

Session Timeout

Top WLANs

Profile Name	# of Clients
ICETEX WLAN CELULARES VIP	49
ICTX-VIP	21
ICTX-FUNCIONARIOS	8

Most Recent Traps

Rogue AP : 48:92:5a:52:41:b3 removed from Base Radio MAC : 00:26:99:23:a7:20 Interface no:0(802.11b/g)
Rogue AP : 98:6b:3d:06:05:20 removed from Base Radio MAC : 74:86:0b:59:74:80 Interface no:0(802.11n(2.4 GHz)
Rogue AP : 80:42:0c:fd:90:c4 removed from Base Radio MAC : 00:26:99:23:a5:e0 Interface no:0(802.11b/g)
Rogue AP : c0:94:ad:47:59:7c removed from Base Radio MAC : 74:86:0b:59:85:e0 Interface no:1(802.11ac)
Rogue AP : c0:94:ad:47:59:7a removed from Base Radio MAC : 00:26:99:23:a6:b0 Interface no:0(802.11n(2.4 GHz))

Top Applications

Application Name	Packet Count	Byte Count
skydrive	5123	459362
facebook	9263	1225044
stun-nat	2142	755262
youtube	6123	754919



Controller

General

Icons

Inventory

Interfaces

Interface Groups

Multicast

▶ Network Routes

▶ Redundancy

▶ Internal DHCP Server

▶ Mobility Management

Ports

▶ NTP

▶ CDP

▶ PMIPv6

▶ Tunneling

▶ IPv6

▶ mDNS

▶ Advanced

Interface Address

VLAN Identifier

20

IP Address

172.16.225.2

Netmask

255.255.252.0

Gateway

172.16.225.1

IPv6 Address

::

Prefix Length

128

IPv6 Gateway

::

Link Local IPv6 Address

fe80::224:97ff:febf:2caf/64

DHCP Information

Primary DHCP Server

172.16.225.1

Secondary DHCP Server

DHCP Proxy Mode

Global

Enable DHCP Option 82

☐

Access Control List

ACL Name

none

URL ACL

none

mDNS

mDNS Profile

none

External Module

3G VLAN

☐

Vlan1 10.1.4.1 NVRAM up up	YES	Vlan32 192.168.32.2 YES NVRAM up up	Vlan122 10.1.11.1 administratively down down	YES NVRAM
Vlan2 unassigned unset administratively down down	YES	Vlan33 10.1.0.81 NVRAM up up	Vlan123 unassigned administratively down down	YES unset
Vlan3 unassigned unset administratively down down	YES	Vlan100 10.1.35.1 YES manual up up	Vlan124 10.1.15.1 administratively down down	YES NVRAM
Vlan4 unassigned unset administratively down down	YES	Vlan101 unassigned YES unset administratively down down	Vlan125 unassigned administratively down down	YES unset
Vlan5 10.1.3.200 manual administratively down down	YES	Vlan102 unassigned YES unset administratively down down	Vlan126 10.1.100.5 up up	YES NVRAM
Vlan6 unassigned unset administratively down down	YES	Vlan103 unassigned YES unset administratively down down	Vlan127 unassigned administratively down down	YES unset



Vlan7 unassigned YES unset administratively down down	Vlan104 unassigned YES unset administratively down down	Vlan128 10.1.22.1 up up YES NVRAM
Vlan8 10.1.18.110 YES manual administratively down down	Vlan105 unassigned YES unset administratively down down	Vlan129 unassigned YES unset administratively down down
Vlan9 10.1.100.38 YES NVRAM up up	Vlan106 172.16.106.1 YES NVRAM up up	Vlan130 unassigned YES unset administratively down down
Vlan10 10.1.2.1 YES NVRAM administratively down down	Vlan107 unassigned YES unset administratively down down	Vlan131 unassigned YES unset administratively down down
Vlan11 10.1.20.1 YES NVRAM down down	Vlan108 unassigned YES unset administratively down down	Vlan132 10.1.14.1 YES NVRAM administratively down down
Vlan12 10.1.29.1 YES NVRAM up up	Vlan109 unassigned YES unset administratively down down	Vlan133 unassigned YES unset administratively down down
Vlan20 172.16.225.1 YES manual up up	Vlan110 unassigned YES unset administratively down down	Vlan134 unassigned YES unset administratively down down
Vlan21 172.16.220.1 YES NVRAM up	Vlan111 unassigned YES unset administratively down down	Vlan135 unassigned YES unset administratively down down
Vlan22 unassigned YES unset administratively down down	Vlan112 unassigned YES unset administratively down down	Vlan136 10.1.5.1 YES NVRAM administratively down down
Vlan23 unassigned YES unset administratively down down	Vlan113 unassigned YES unset administratively down down	Vlan137 unassigned YES unset up up
Vlan24 unassigned YES unset administratively down down	Vlan114 unassigned YES unset administratively down down	Vlan138 10.1.19.1 YES NVRAM administratively down down

Vlan25 unassigned YES unset administratively down down	Vlan115 unassigned YES unset administratively down down	Vlan139 10.1.30.1 YES NVRAM up up
Vlan26 unassigned YES unset administratively down down	Vlan116 172.16.116.1 YES NVRAM up up	Vlan200 172.22.1.1 YES NVRAM up up
Vlan27 unassigned YES unset administratively down down	Vlan117 unassigned YES unset administratively down down	Vlan201 172.23.0.1 YES NVRAM up up
Vlan28 unassigned YES unset administratively down down	Vlan118 10.1.9.1 YES NVRAM administratively down down	Vlan202 172.28.10.1 YES NVRAM up up
Vlan29 unassigned YES unset administratively down down	Vlan119 10.1.16.1 YES NVRAM administratively down down	Vlan203 192.168.150.1 YES NVRAM up up
Vlan30 10.1.12.15 YES NVRAM up up	Vlan120 unassigned YES unset administratively down down	Vlan204 172.16.221.1 YES NVRAM up up
Vlan31 172.31.0.1 YES manual up up	Vlan121 unassigned YES unset administratively down down	Vlan205 172.16.222.1 YES NVRAM up up

5.3 Conclusiones

todos lo casos fueron atendieron de forma oportuna y fueron cerrados en los tiempos establecidos

6 INFORME WEBMASTER

6.1 Introducción

Informe correspondiente al mes de abril del rol de Webmaster. En este informe, se detallan las principales actividades y avances de la operación y la optimización del funcionamiento de los portales institucionales.

Se han llevado a cabo diversas acciones que tienen como objetivo mejorar la calidad de los servicios en línea ofrecidos y optimizar el funcionamiento de los portales institucionales. Entre los logros destacados se encuentran la gestión de la plataforma Liferay, la renovación de licencias, la creación de nuevos usuarios y la actualización del código de Google Analytics.

Además, se están identificando áreas de oportunidad en materia de plan de mejoras y gestión de recursos, las cuales se abordarán en próximos informes.

6.2 Actividades desarrolladas:

#	Fecha	Actividad	Avance	Evidencia
1	3/04/2023	Eliminación del botón flotante del chat en la sección de Atención y Servicios a la Ciudadanía del portal institucional.	100%	Evidencia
2	3/04/2023	Gestión publicación de formulario para radicación de pqr's en el portal institucional.	100%	Evidencia
3	4/04/2023	Estabilización del ambiente de pruebas de portal institucional Liferay (Ingreso - ICETEX), presenta Error.	20%	Evidencia
4	5/04/2023	Gestión renovación de las cuentas de los sitios web www.icetex.com y www.icetex.com.co en uso por terceros, para el correcto funcionamiento de los servicios y herramientas en línea de la institución.	80%	Evidencia
5	6/04/2023	Creación de un usuario en producción general en el Portal Transaccional para el Grupo de Administración de Cartera con permisos de consulta y realización de validaciones en los procesos internos de la cartera.	100%	Evidencia
6	10/04/2023	Generación de un inventario detallado de la infraestructura que soporta el portal institucional en los entornos de producción y pruebas. Incluyendo la lista de hardware, software y otros recursos utilizados para mantener el portal en funcionamiento.	60%	Evidencia

7	10/04/2023	Generación de un plan de actualización de contenidos para el ambiente de pruebas del portal institucional. Este plan debe describir los cambios específicos que se deben realizar en el contenido del portal, así como las fechas límite para la implementación de cada cambio.	60%	Evidencia
8	11/04/2023	Gestión y corrección del error que impide a los usuarios ingresar sus credenciales de inicio de sesión en el portal transaccional.	100%	Evidencia
9	12/04/2023	Presentación de un plan de trabajo detallado que incluya las mejoras propuestas para los portales institucionales. Este plan debe contener una descripción detallada de cada mejora, un cronograma de implementación y una estimación de los recursos necesarios para completar cada tarea.	10%	Evidencia
10	12/04/2023	Proporcionar información detallada sobre las actividades de mitigación necesarias para remediar las vulnerabilidades y fechas límite para la implementación de cada actividad de mitigación en portales institucionales.	30%	Evidencia
11	13/04/2023	Gestión actualización del código de Google Analytics en el Portal ICETEX, cambiando de Universal Analytics a Google Analytics 4. Debido a que las propiedades de Universal Analytics dejarán de procesar nuevos hits a partir del 1 de julio de 2023.	100%	Evidencia
12	17/04/2023	Generación de estadísticas de uso del portal de la Comunidad ICETEX, incluyendo el número de usuarios registrados, usuarios activos y visitas mensuales durante los últimos seis meses.	100%	Evidencia
13	18/04/2023	Validación vigencia y requisitos renovación de las licencias de Google Maps.	20%	Evidencia
14	18/04/2023	Revisión intermitencia en la visualización de eventos en el calendario institucional, donde en algunos casos se muestran todas las actividades y en otros no.	100%	Evidencia
15	18/04/2023	Creación de botones solicitados a páginas de la Oficina de Planeación para mejorar la accesibilidad y usabilidad de los usuarios.	20%	Evidencia

16	19/04/2023	Reinicio de password de usuario admin de publicaciones en el portal.	100%	Evidencia
17	20/04/2023	Redireccionamiento de las siguientes URL de los proveedores de servicio, del antiguo (Millenium) al nuevo (Comware)	30%	Evidencia
18	24/04/2023	Revisión y actualización del estado de cumplimiento de los criterios establecidos en los anexos 1 y 3 de la resolución 1519 de 2020 del MinTIC.	20%	Evidencia
19	24/04/2023	Inactivación de la URL que está generando pagos equivocados de estudios de antecedentes para creditos propios.	10%	N/A
20	25/04/2023	Solución "Error, su petición no se ha podido realizar correctamente" en el portal institucional, ambiente productivo Liferay.	10%	N/A
21	26/04/2023	Creación y actualización minutograma de migración del portal en ambientes producción y pruebas	80%	Evidencia

6.3 Conclusiones:

- Se ha avanzado significativamente en la gestión de la plataforma institucional durante el mes, cumpliendo con la mayoría de las actividades planificadas.
- Se ha logrado la eliminación del botón flotante del chat en la sección de Atención y Servicios a la Ciudadanía del portal institucional y la gestión de la publicación de un formulario para la radicación de PQRS en el mismo.
- Sin embargo, todavía hay actividades que están en proceso de implementación, como la estabilización del ambiente de pruebas de Liferay, la gestión de la renovación de las cuentas de los sitios web www.icetex.com y www.icetex.com.co y la generación de un inventario detallado de la infraestructura que soporta el portal institucional en los entornos de producción y pruebas.

7 INFORME ADMINISTRADORES DE SEGURIDAD

7.1 Introducción

El Informe de Gestión Mensual contiene información relevante para evidenciar el nivel de cumplimiento del contrato firmado entre Infotíc e Ictec. El informe presenta los resultados y el análisis de la gestión de los servicios de seguridad para el mes de abril 1 al 30 de 2023.

7.2 Estado general de las plataformas

Seguridad Perimetral DC Principal (FortiGate_ZF)

System Information

Hostname	DCZF_FG_MST_ICETEX
Serial Number	FGT2KETB19900416
Firmware	v6.4.11 build2030 (GA)
Mode	NAT
System Time	2023/05/04 17:50:38
Uptime	141:18:38:03
WAN IP	190.90.13.48

Seguridad Perimetral DC Alterno (FortiGate_Balsos)

System Information

Hostname	DCB_FG_MST_ICETEX
Serial Number	FG5H0E5819904063
Firmware	v6.4.10 build2000 (GA)
Mode	NAT
System Time	2023/05/04 18:00:49
Uptime	99:08:36:05
WAN IP	Unknown

Consola de Logs y Reportes (FortiAnalyzer)



System Information

Host Name	DCZF_FL_SA_ICETEX
Serial Number	FL-1KET319000188
HA Status	Standalone
System Time	Thu May 04 17:52:57 2023 COT
Firmware Version	v6.4.6-build2363 210531 (GA)
System Configuration	Last Backup : Tue Mar 7 15:49:00 2023
Current Administrators	ejimenez /1 in total
Up Time	691 days 17 hours 10 minutes 56 seconds
Administrative Domain	☒
Operation Mode	Analyzer Collector

Plataforma de Administración Centralizada de Firewalls DC PPAL y ALTERNO (FortiManager)

System Information

Host Name	DCZF_FM_MST_ICETEX
Serial Number	FMG2HFTB19900148
HA Status	HA Protection
Cluster Members	Master FMG2HFTB19900148 Slave FMG2HFTB19900144
System Time	Thu May 04 17:54:13 2023 COT
Firmware Version	v6.2.3-build1235 191218 (GA)
System Configuration	Last Backup : Tue Mar 7 14:53:13 2023
Current Administrators	ejimenez /1 in total
Up Time	10 days 5 hours 29 minutes 19 seconds
Administrative Domain	☒
FortiAnalyzer Features	☐ OFF

WAF (FortiWeb_ZF)

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 May 4 17:55:29 2023
Firmware Version	FortiWeb-2000E 6.41,build1464(GA),210903
System Uptime	[254 day(s) 21 hour(s) 31 min(s)]

Filtrado Web (FortiGate_ZF)

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

IPS (Intrusiones por tipos)



Intrusions By Types

#	Intrusion Type	Counts
1	Other	18,262
2	Anomaly	2,519
3	Permission/Privilege/Access Control	2,338
4	OS Command Injection	1,009
5	Code Injection	925
6	Path Traversal	430
7	Malware	239
8	SQL Injection	212
9	XSS	100
10	DoS	33
11	Information Disclosure	16
12	Improper Authentication	15

Control de Aplicaciones (Categorías de Aplicaciones por consumo)

Collaboration	48.70%
Network.Service	17.21%
Update	7.89%
General.Interest	6.99%
Email	6.39%
Web.Client	5.90%
Storage.Backup	2.66%
Cloud.IT	1.89%
Video/Audio	1.25%
Social.Media	0.84%
Others	0.30%

Inspección SSL (FortiGate_ZF)

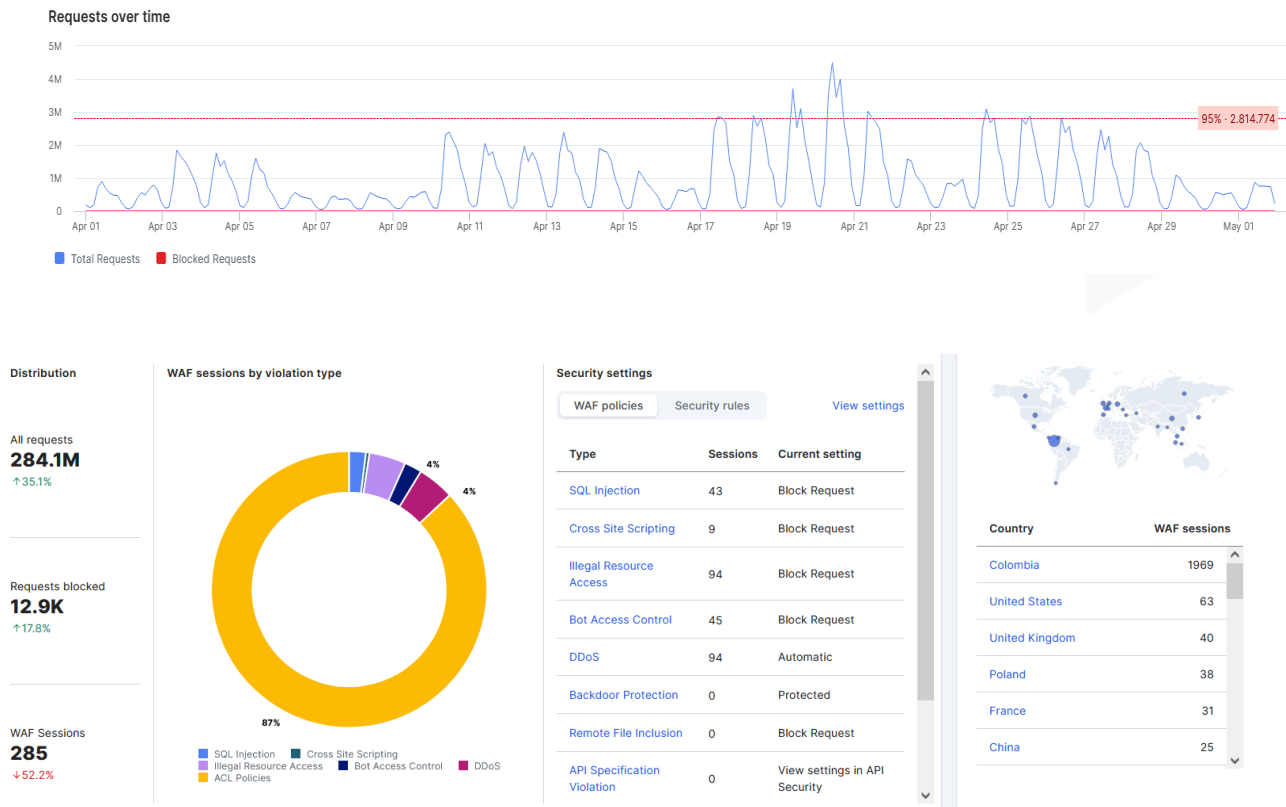
Name	Comments	Ref.
SSL Prueba certificate-inspection	Read-only SSL handshake inspection profile.	19
SSL custom-deep-inspection	Customizable deep inspection profile.	0
SSL no-inspection	Read-only profile that does no inspection.	1837
SSL certificate-inspection	Read-only SSL handshake inspection profile.	966
SSL deep-inspection	Read-only deep inspection profile.	0

Antivirus y Antimalware Perimetral (FortiGate_ZF)

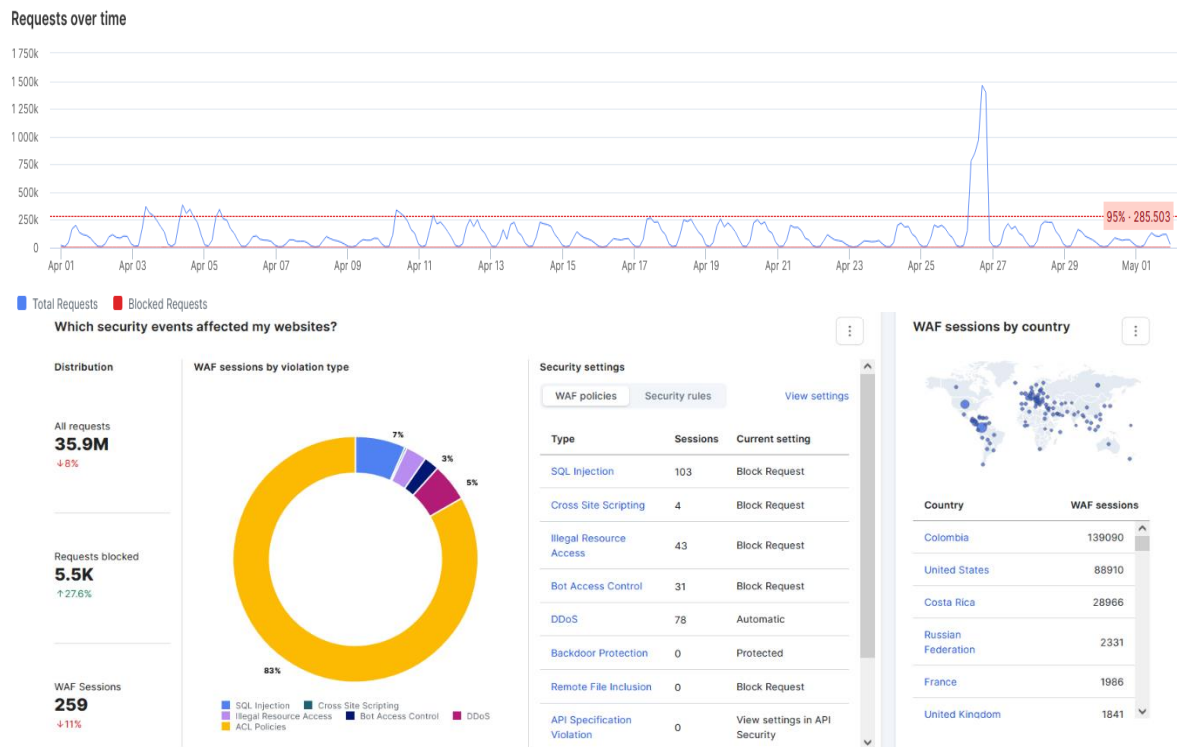
Name	Comments	Ref.
AV default	ALL con FSB	139
AV-HTTP	HTTP con FSB	96
AV-FSB	HTTP,SMTP FULL FSB	80
AV-HTTP&CIFS	HTTP,CIFS con FSB	15
AV-FTP	FTP FULL FSB	8
AV-SMTP	SMTP FULL FSB	5
AV-HTTP_Mobile	HTTP, mobile con FSB	1
AV Prueba	ALL con FSB	0
AV prueba2		0
AV wifi-default	ALL monitoreo sin FSB	0

WAF Portales (Waf Imperva) No hay alcance

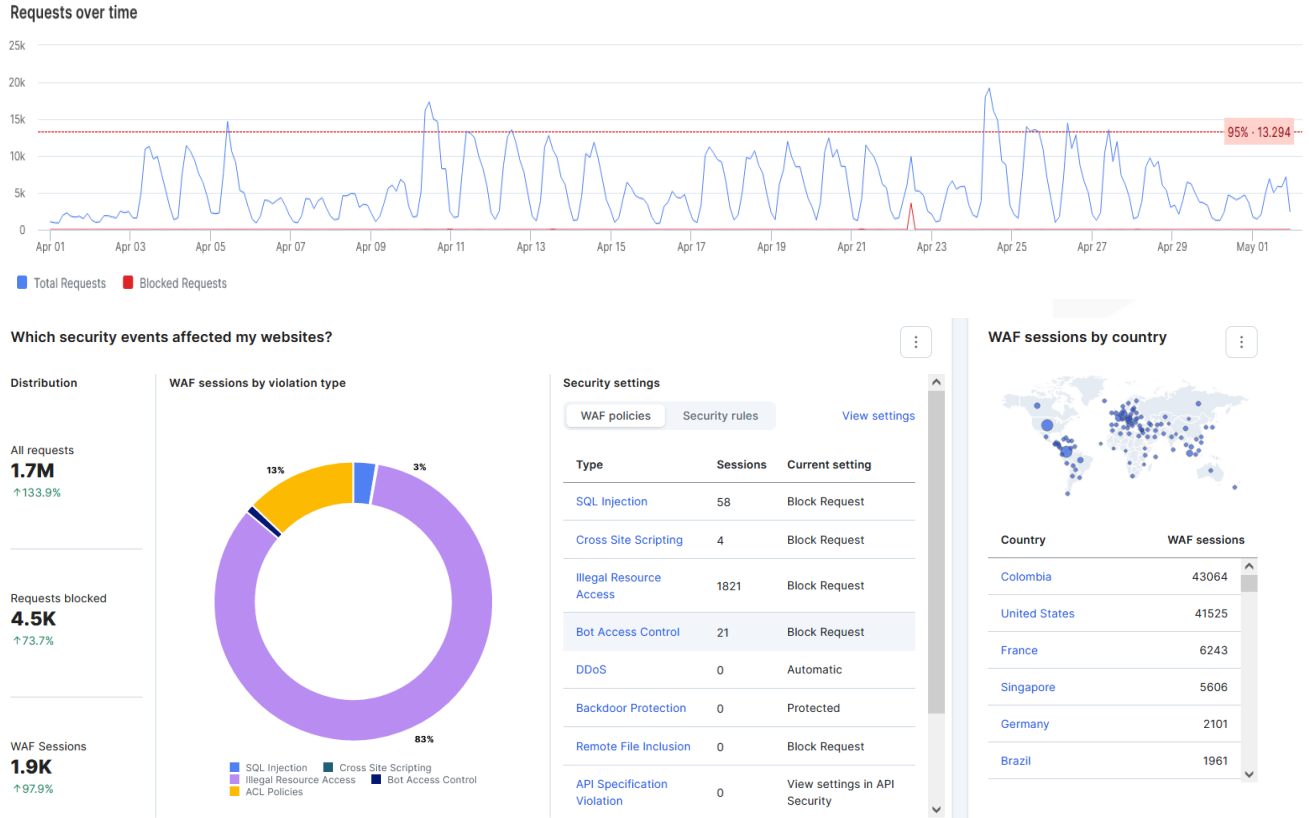
Tráfico desde WAF web.icetex.gov.co



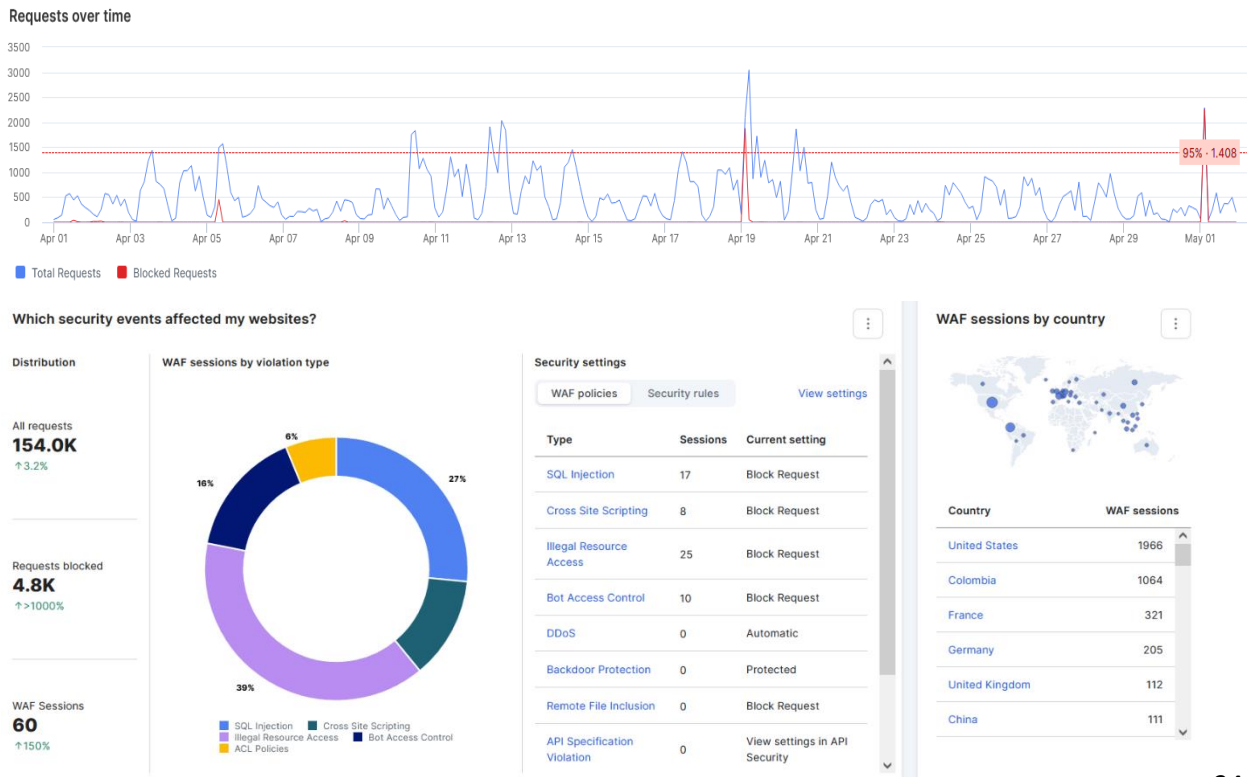
7.3 Tráfico desde WAF www.icetex.gov.co



7.4 Tráfico desde WAF portal.icetex.gov.co

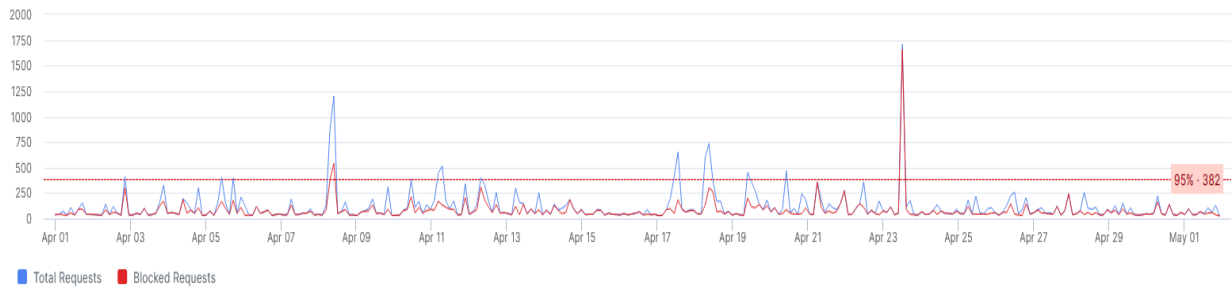


7.5 Tráfico desde WAF comunidad.icetex.gov.co



7.6 Tráfico desde WAF Colombiacientifica.gov.co

Requests over time



Which security events affected my websites?

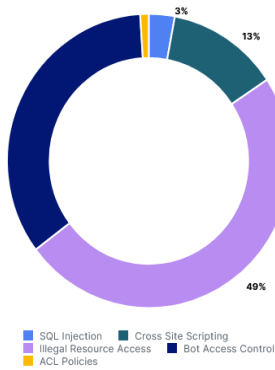
Distribution

All requests
36.0K
↑ <1%

Requests blocked
23.8K
↓ 11.2%

WAF Sessions
101
↓ 54.5%

WAF sessions by violation type



Security settings

WAF policies Security rules [View settings](#)

Type	Sessions	Current setting
SQL Injection	3	Block Request
Cross Site Scripting	13	Block Request
Illegal Resource Access	50	Block Request
Bot Access Control	35	Block Request
DDoS	0	Automatic
Backdoor Protection	0	Protected
Remote File Inclusion	0	Block Request
API Specification Violation	0	View settings in API Security

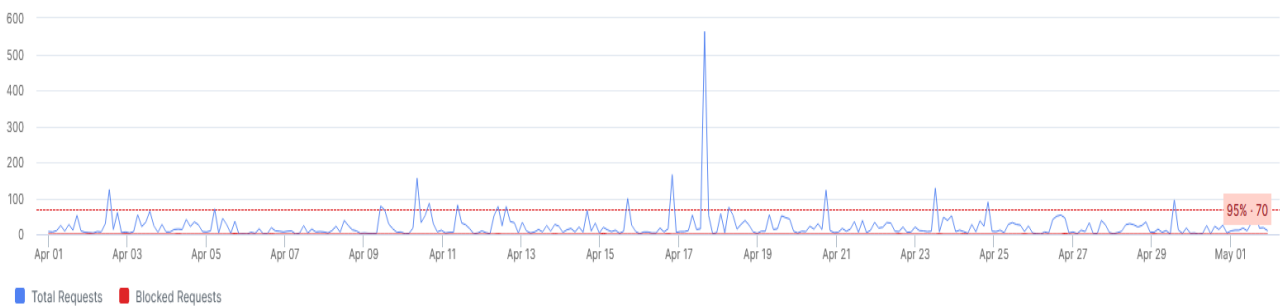
WAF sessions by country



Country	WAF sessions
United States	4675
United Kingdom	1996
Netherlands	1269
Japan	1127
Germany	498
Sweden	488

7.7 Tráfico desde WAF identidad.icetex.gov.co

Requests over time



Which security events affected my websites?

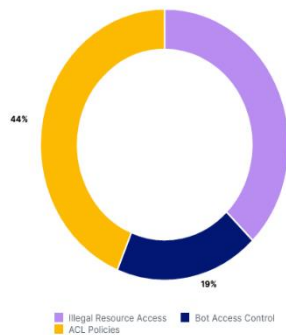
Distribution

All requests
6.6K
↓10.1%

Requests blocked
18
↓41.9%

WAF Sessions
9
↓35.7%

WAF sessions by violation type



Security settings

WAF policies Security rules View settings

Type	Sessions	Current setting
SQL Injection	0	Block Request
Cross Site Scripting	0	Block Request
Illegal Resource Access	6	Block Request
Bot Access Control	3	Block Request
DDoS	0	Automatic
Backdoor Protection	0	Protected
Remote File Inclusion	0	Block Request
API Specification Violation	0	View settings in API Security

WAF sessions by country



Country	WAF sessions
United States	1654
Colombia	121
United Kingdom	46
China	31
Ireland	20
Netherlands	17

7.8 Administración Plataformas incluidas las propiedades del ICETEX y las IaaS

- FortiClient EMS
- FortiAuthenticator
- FortiSiem
- FortiWeb
- FortiSandbox

Seguridad Endpoint EMS (Antivirus FortiClient)

System Information	
Hostname	ICTXSRVFORTEMS.icetex.local
Version	7.0.8 build 0484
Database	Backup Restore
System Time	2023-05-05 08:24:02 AM
Uptime	13:18:08:59
Mode	Standalone

Seguridad Perimetral DC Alterno (FortiGate_Aguas)

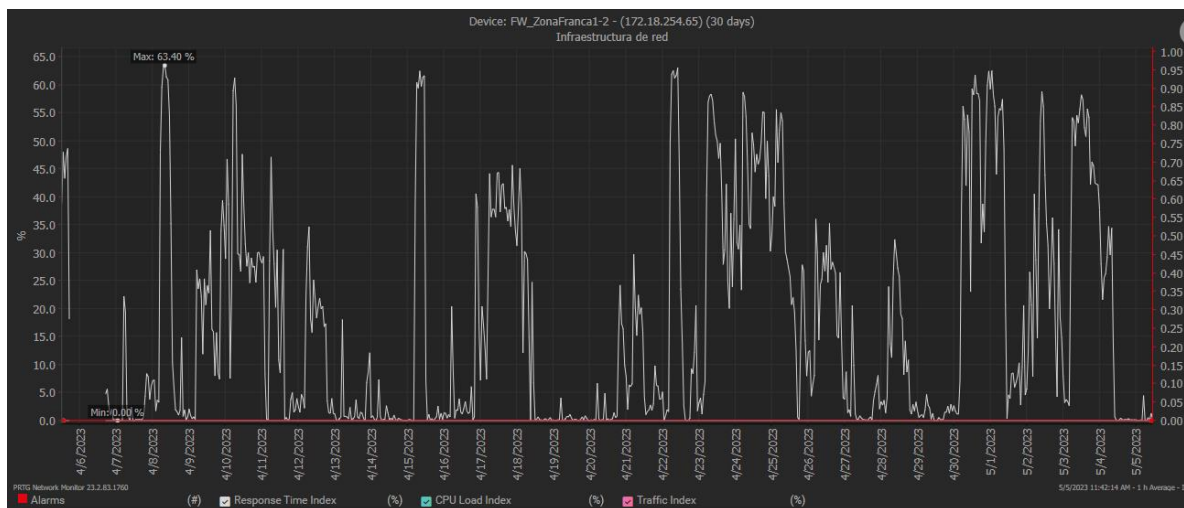


System Information

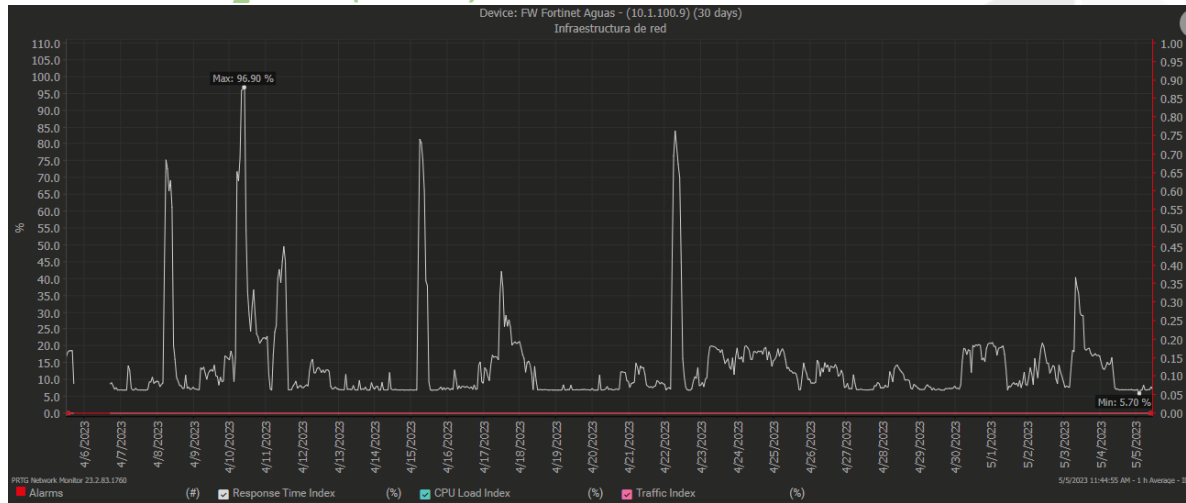
Hostname DCAGUAS_FG_MST_ICETEX
Serial Number FG6H1ETB20900947
Firmware v6.4.10 build2000 (GA)
Mode NAT
System Time 2023/05/05 08:26:32
Uptime 240:11:05:38
WAN IP  190.90.13.48

7.9 Disponibilidad de las plataformas de seguridad

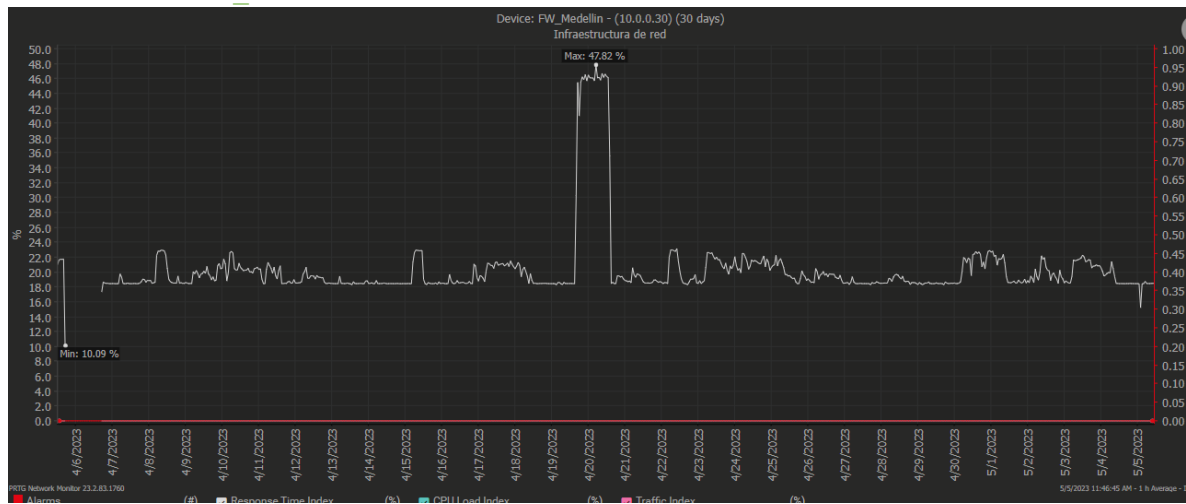
7.9.1 Firewall_Zonafranca



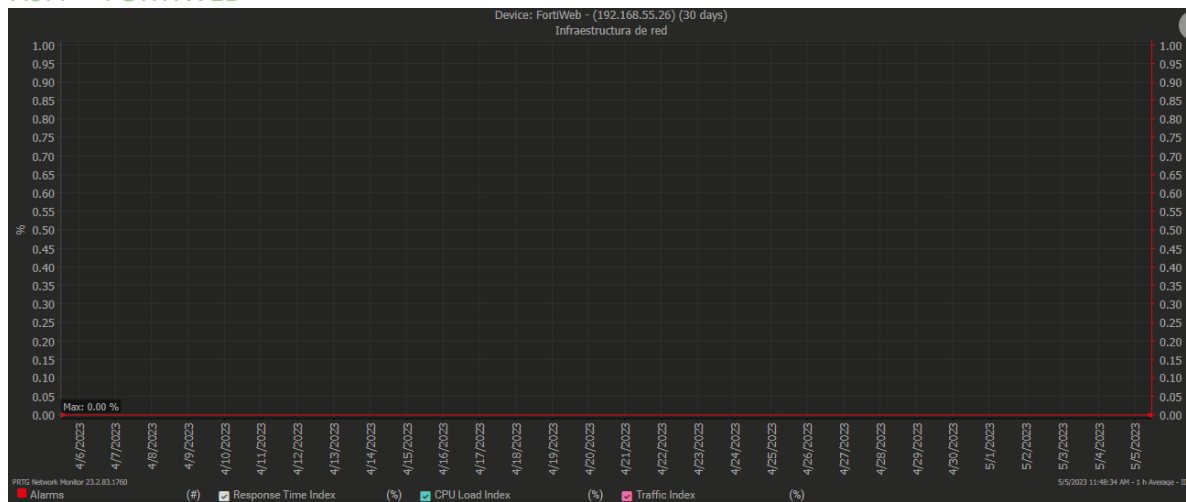
7.9.2 FIREWALL_AGUAS (FORTINET)



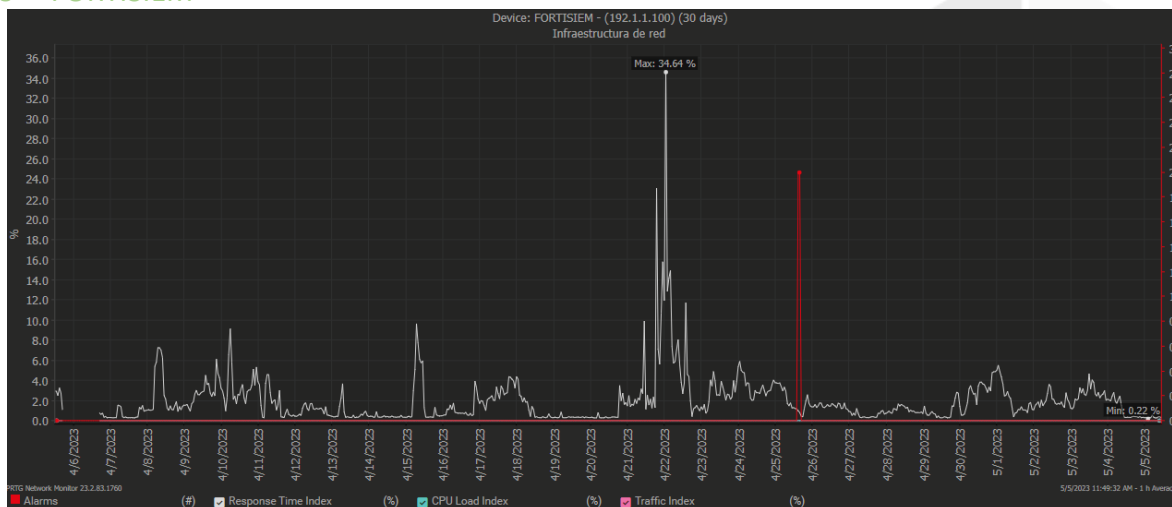
7.9.3 FIREWALL_MEDELLÍN



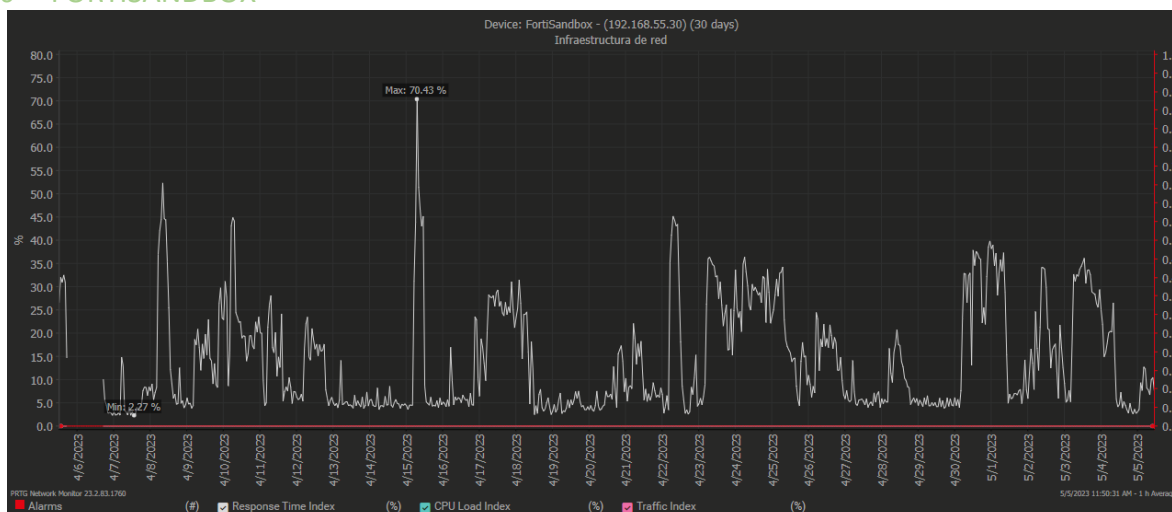
7.9.4 FORTIWEB



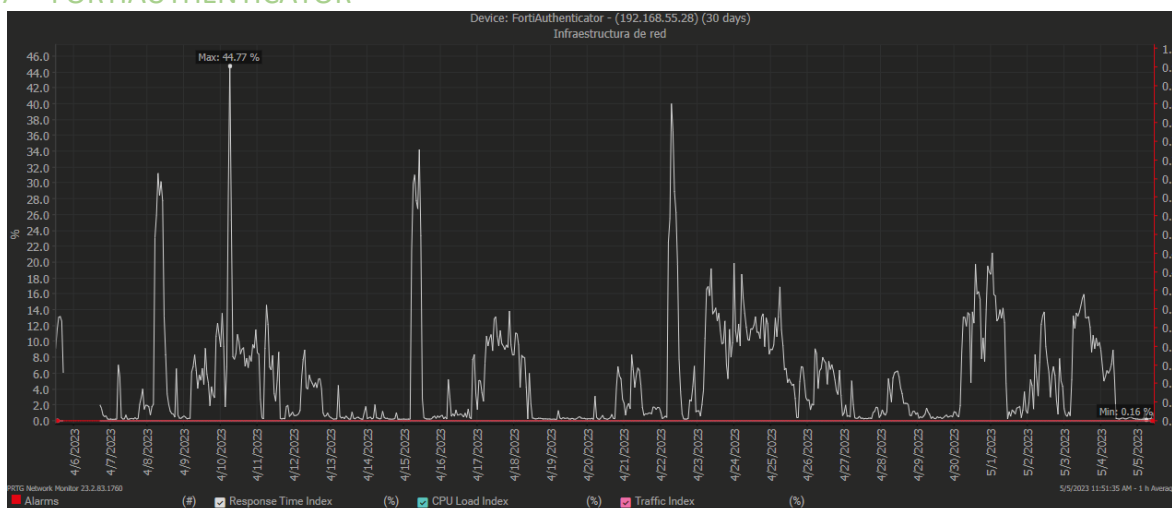
7.9.5 FORTISIEM



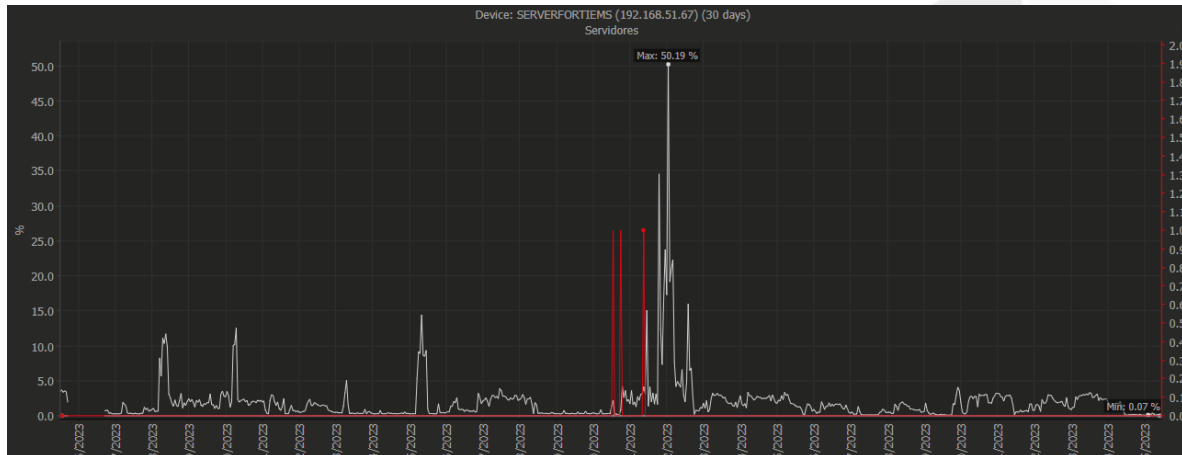
7.9.6 FORTISANDBOX



7.9.7 FORTIAUTHENTICATOR

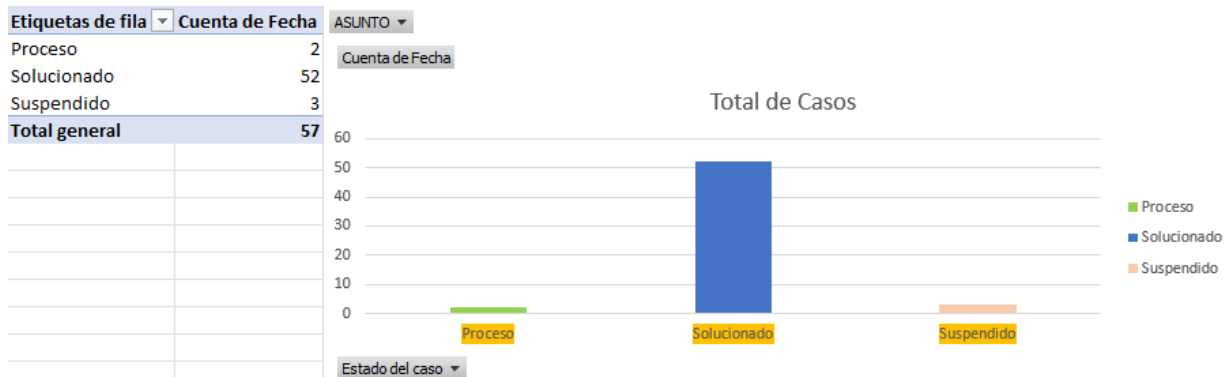


7.9.8 FORTICLIENT EMS



7.10 Gestión de casos

Durante el mes de abril se recibieron 57 casos en los cuales se incluyen Tareas, Requerimientos, Incidentes y Control de Cambio. Continuó para el periodo analizado un caso en proceso y uno en suspendido.



El caso más solicitado es el acceso de usuarios al grupo de Directorio Activo Temporal_VPN



Tareas Gestión de Accesos

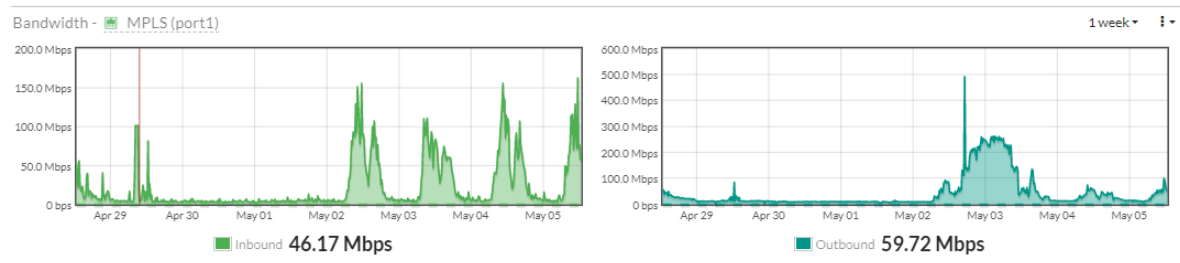
7.11 Estado de salud de los equipos de seguridad

7.12 FIREWALL AGUAS

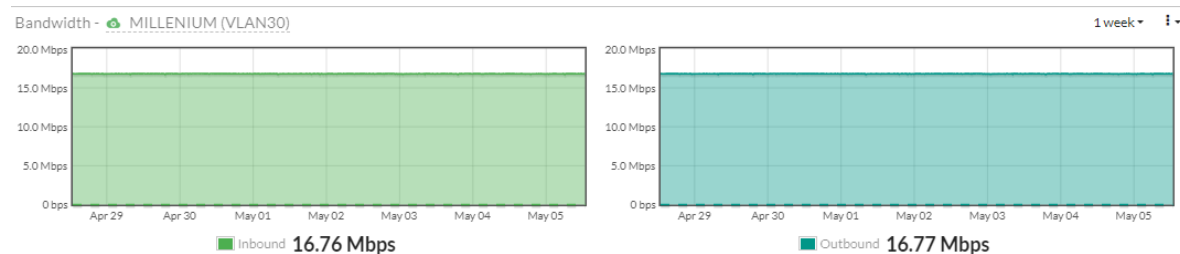
Se observa consumo de CPU promedio del 1% y máximo 8%. “No tengo acceso a las gráficas”

Se observa consumo de memoria promedio del 40% . “No tengo acceso a las gráficas”

Se observa el tráfico WAN hacia la MPLS de la sede de Aguas, promedio 52,9 Mbps (Port1)



Se observa el tráfico del canal de Millenium, promedio 16.7 Mbps (VLAN30)

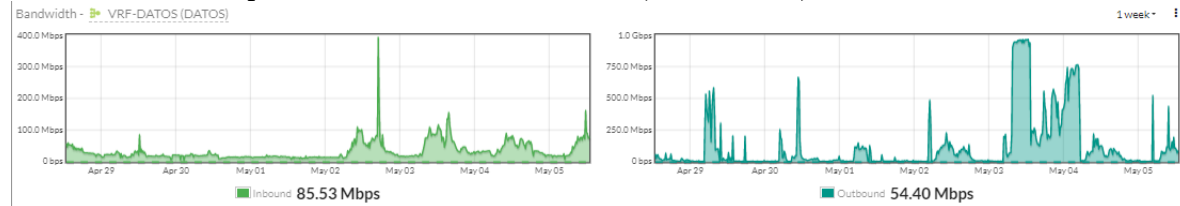


7.13 FIREWALL FORTINET ZF

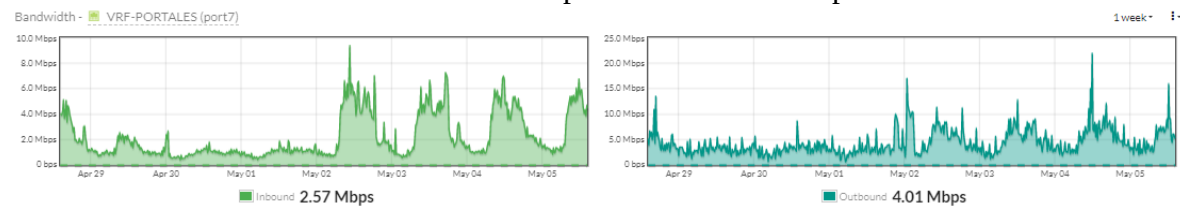
Se observa consumo de CPU promedio del 2% y un máximo de 30% “No tengo acceso a las gráficas”.

El nivel de Memoria en uso es promedio del 33% “No tengo acceso a las gráficas”.

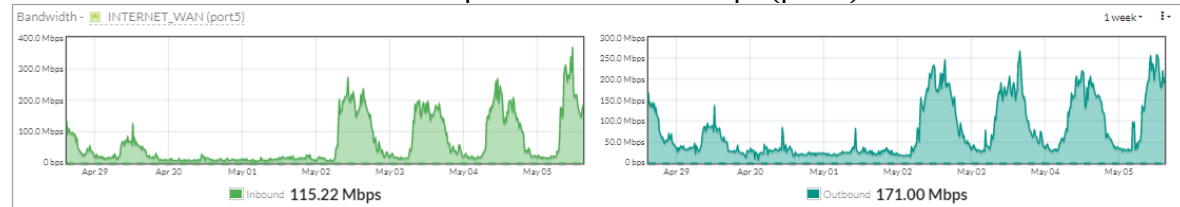
Se observa el tráfico WAN hacia la MPLS promedio 237 Mbps (VRF-DATOS), los máximos que se observan corresponden al servidor ARANDA (10.1.18.11).



Se observa el tráfico WAN hacia la MPLS portales 3.29 MB en promedio



Se observa el tráfico hacia Internet promedio 143.11 Mbps (port5)



7.14 PERFILES DE SEGURIDAD

7.14.1 Webfilter.

Perfiles de navegación web aplicados para la navegación.



7.14.2 . Categorías más Visitadas

En la imagen se observa el top de las categorías con mayor consumo, la categoría Collaboration es la que más consumo presenta con **14.36TB**

#	Application Category	Number of Applications	Number of Users	Bandwidth	Session
1	Collaboration	60	5,215	14.36 TB	36,599,759
2	Network.Service	43	4,953	5.07 TB	41,373,734
3	Update	20	4,924	2.33 TB	8,284,465
4	General.Interest	67	4,365	2.06 TB	10,881,447
5	Email	12	3,738	1.88 TB	5,535,474
6	Web.Client	9	5,121	1.74 TB	11,693,956
7	Storage.Backup	21	3,655	803.81 GB	1,230,993
8	Cloud.IT	14	3,294	569.90 GB	2,195,166
9	Video/Audio	32	2,808	376.43 GB	911,527
10	Social.Media	21	3,038	254.50 GB	2,046,599
11	Business	32	2,854	42.47 GB	422,016
12	Remote.Access	5	1,192	38.25 GB	205,424
13	Desconocido	142	4,213	6.74 GB	3,576,258
14	Game	16	1,357	1.34 GB	25,737
15	Proxy	13	279	751.14 MB	21,634
16	Mobile	2	111	22.27 MB	1,279
17	P2P	2	22	2.37 MB	910
18	VoIP	3	220	809.21 KB	1,672

En la imagen se muestra las aplicaciones con mayor consumo, por ancho de banda y sesiones, se observa que el servicio más usado es **TCP/902** utilizado por el **vCenter**.



#	Application	Bandwidth	Sent	Received	Sessions
1	TCP/902		162.41 TB		4,980
2	TCP-High_Ports		40.85 TB		23,028,263
3	Microsoft.Portal		9.36 TB		16,414,406
4	SMB		4.79 TB		7,000,603
5	SSL		3.53 TB		16,123,743
6	tcp/554		3.05 TB		7,682
7	ORACLE		2.67 TB		9,040,125
8	HTTP		2.59 TB		8,272,340
9	Microsoft.Windows.Update		2.18 TB		6,954,463
10	Microsoft.SharePoint		1.88 TB		1,082,846
11	Microsoft.Outlook.Office.365		1.82 TB		4,277,937
12	HTTPS.BROWSER		1.61 TB		9,461,079
13	SSH		1.30 TB		345,066
14	HTTPS		1.08 TB		27,284,476
15	Google.Services		1.02 TB		8,171,899
16	Microsoft.Office.Online		1,013.43 GB		4,796,776
17	CIFS		845.13 GB		1,129,569
18	Microsoft.Office.365.Portal		763.89 GB		4,511,904
19	STUN		753.32 GB		462,195
20	OneDrive		666.56 GB		401,959
21	MS-SQL_Server		614.59 GB		22,691,716
22	Microsoft.Azure		513.47 GB		257,914
23	Google.Accounts		482.55 GB		226,501
24	SMB.v3		449.21 GB		27,098
25	Microsoft.Teams		375.84 GB		2,425,178
26	Skype_Video		369.06 GB		4,201
27	DTLS		318.91 GB		8,674
28	TCP/2560		279.14 GB		125
29	YouTube		261.84 GB		531,512
30	SNMP/161		250.01 GB		37,620,253

7.14.3 6.3. Control de Aplicaciones

Top 20 de las aplicaciones más usadas

#	Risk	Application Name	Category	Technology	User	Bandwidth	Session
1	5	DNS.TXT.Records.Tunneling	Proxy	Client-Server	4	1.99 MB	5,174
2	5	Proxy.HTTP	Proxy	Network-Protocol	241	11.18 MB	2,119
3	5	Cloudflare.1.1.1.VPN	Proxy	Client-Server	37	212.02 KB	1,870
4	5	Touch.VPN	Proxy	Client-Server	7	83.74 KB	500
5	5	SOCKS5	Proxy	Network-Protocol	6	734.06 MB	448
6	5	Tor	Proxy	Client-Server	5	244.42 KB	170
7	5	Psiphon	Proxy	Client-Server	5	911.25 KB	166
8	5	SurfEasy.VPN	Proxy	Client-Server	4	550 B	57
9	5	WindScribe	Proxy	Client-Server	3	5.30 KB	42
10	5	Hotspot.Shield	Proxy	Client-Server	5	64.17 KB	37
11	5	Hola.Unblocker	Proxy	Client-Server	1	23.37 KB	16
12	5	Proxy.Websites	Proxy	Browser-Based	1	11.02 KB	6
13	5	Ultrasturf_9.6+	Proxy	Client-Server	1	0 B	4
14	5	Turbo.VPN	Proxy	Client-Server	1	48 B	1
15	4	AnyDesk	Remote.Access	Client-Server	830	28.08 GB	190,133
16	4	TeamViewer	Remote.Access	Client-Server	361	9.91 GB	8,848
17	4	Chrome.Remote.Desktop	Remote.Access	Client-Server	82	47.87 MB	6,576
18	4	Telnet	Remote.Access	Client-Server	118	379.33 KB	2,096
19	4	BitTorrent	P2P	Peer-to-Peer	12	1.49 MB	821
20	4	TeamViewer_CallRecorder	Remote.Access	Client-Server	51	181.43 MB	166

7.14.4 FORTICLIENT EMS

Informe de los equipos en los que se encuentra sincronizado FortiClient 355 dispositivos.

License Information

 Serial Number	FCTEMS0000104344
 FortiCloud Account	Add
 Fabric Agent	 Expiring 2023-05-31 Config License
	355 used of 1000
 Sandbox Cloud	 Unlicensed
 Chromebook	 Unlicensed

7.14.5 FORTISIEM

Se está trabajando en la configuración del FortiSiem, configuración de dispositivos y reglas. Para el FortiSiem se cuenta con una licencia de 200 dispositivos, actualmente se encuentran configurados 111 dispositivos, según reporte de cada administrador.

Device Usage Agent Usage

Licensed: 200

Used: 111

Unused: 89

7.15 ESTADO DE LICENCIAMIENTO DE PLATAFORMAS

Características de licenciamiento y los contratos asignados.

7.15.1 FORTIGATE ZONA FRANCA

License Information ⓘ		
Entitlement	Status	
FortiCare Support	Registered	ⓘ Actions +
FortiCloud Account	jweng@intermexa.com	
Hardware Version	Advanced hardware (Expiration Date: 2023/06/01)	
Enhanced Support	Premium (Expiration Date: 2023/06/01)	
Firmware & General Updates	Expires Soon (Expiration Date: 2023/06/01)	ⓘ Renew +
Application Control Signatures	Version 23.00546	ⓘ Actions +
Device & OS Identification	Version 1.00150	
Internet Service Database Definitions	Version 7.03194	
Intrusion Prevention	Expires Soon (Expiration Date: 2023/06/01)	ⓘ Renew +
IPS Definitions	Version 23.00547	ⓘ Actions +
IPS Engine	Version 6.00148	
Malicious URLs	Version 4.00697	
Botnet IPs	Version 7.03194	View List
Botnet Domains	Version 3.00269	View List
AntiVirus	Expires Soon (Expiration Date: 2023/06/01)	ⓘ Renew +
AV Definitions	Version 91.02987	Upgrade Database
AV Engine	Version 6.00172	
Mobile Malware	Version 91.02987	
Web Filtering	Expires Soon (Expiration Date: 2023/06/01)	ⓘ Renew +
Blocked Certificates	Version 1.00427	
Outbreak Prevention	Expires Soon (Expiration Date: 2023/06/01)	ⓘ Renew +
Industrial DB	Not Licensed	ⓘ Purchase +
Industrial Attack Definitions	Version 6.00741	
FortiIPAM	Not Licensed	ⓘ Purchase +
IoT Detection Service	Not Licensed	ⓘ Purchase +
FortiGate Cloud	Not Activated	ⓘ Activate

7.15.2 FORTISIEM

Serial Number: FSMP000000001340
 Hardware ID: 4212F192-8EF3-61A8-F30D-4EAF9DE2E3F6
 License Hardware ID: 4212F192-8EF3-61A8-F30D-4EAF9DE2E3F6
 License Type: Enterprise
 FIPS Mode: Disabled

Attribute	Value	Expiry
Devices	200	Perpetual
Endpoint Devices	N/A	N/A
Additional EPS	N/A	N/A
Total EPS	2000	Perpetual
Agents	100	Perpetual
UEBA	75	Perpetual
IOC Service	N/A	N/A
Maintenance and Support	Valid	Jun 01,2023
High Availability Service	N/A	N/A

7.15.3 FORTISANDBOX

Windows VM	✓ [Upload License]
Microsoft Office	✓ [Upload License]
VM Internet Access	✓
FDN Download Server	✓
Community Cloud Server	✓
Web Filtering Server	✓
Antivirus DB Contract	✓ 2023-06-10
Web Filtering Contract	✓ 2023-06-10
MTA Contract	✗ No Contract
MacOS VM Contract	✗ No Contract
Industry Security Signature Contract	✗ No Contract



7.15.4 FORTIWEB

License Information	
Contract	Status
Support Contract	✓ Registered
Security Service	✓ Valid Contract (Expires 2023-06-10)
	⊙ Signature Build Number: 0.00347
Antivirus	✓ Valid Contract (Expires 2023-06-10)
	⊙ Regular Virus Database Version: 91.02970
	⊙ Extended Virus Database Version: 91.02901
	⊙ Virus Engine Version: 6.00137
IP Reputation	✓ Valid Contract (Expires 2023-06-10)
	⊙ Signature Build Number: 4.00807
Credential Stuffing Defense	ⓘ Expired (1969-12-31)
	⊙ Credential Stuffing Defense Database Version: 0.00000
FortiSandbox Cloud	ⓘ Expired (1969-12-31)
	⊙ FortiSandbox Cloud Version: 0.0
GEO DB	✓ Valid Contract (Expires 2023-06-10)
	⊙ GEO Database Version: 0173

7.15.5 FORTIGATE AGUAS

License Information ⓘ		
Entitlement	Status	
FortiCare Support	✓ Registered	ⓘ Actions -
FortiCloud Account	✓ jvieng@intermexa.com	
Hardware Version	⚠ Advanced hardware (Expiration Date: 2023/06/01)	
Enhanced Support	⚠ Premium (Expiration Date: 2023/06/01)	
Firmware & General Updates	⚠ Expires Soon (Expiration Date: 2023/06/01)	ⓘ Renew -
Application Control Signatures	⊙ Version 23.00546	ⓘ Actions -
Device & OS Identification	⊙ Version 1.00150	
Internet Service Database Definitions	⊙ Version 7.03194	
Intrusion Prevention	⚠ Expires Soon (Expiration Date: 2023/06/01)	ⓘ Renew -
IPS Definitions	⊙ Version 23.00547	ⓘ Actions -
IPS Engine	⊙ Version 6.00139	
Malicious URLs	⊙ Version 4.00697	
Botnet IPs	⊙ Version 7.03194	ⓘ View List
Botnet Domains	⊙ Version 3.00269	ⓘ View List
AntiVirus	⚠ Expires Soon (Expiration Date: 2023/06/01)	ⓘ Renew -
AV Definitions	⊙ Version 91.02984	ⓘ Upgrade Database
AV Engine	⊙ Version 6.00172	
Mobile Malware	⊙ Version 91.02984	
Web Filtering	⚠ Expires Soon (Expiration Date: 2023/06/01)	ⓘ Renew -
Outbreak Prevention	⚠ Expires Soon (Expiration Date: 2023/06/01)	ⓘ Renew -
Industrial DB	⚠ Not Licensed	ⓘ Purchase -
Industrial Attack Definitions	⊙ Version 6.00741	
FortiIPAM	⚠ Not Licensed	ⓘ Purchase -
IoT Detection Service	⚠ Not Licensed	ⓘ Purchase -
FortiGate Cloud	⚠ Not Activated	ⓘ Activate



7.15.6 FORTIGATE MEDELLÍN BALSOS

License Information		
Entitlement	Status	
FortiCare Support	Registered	Actions
FortiCloud Account	jweng@internexa.com	
Firmware & General Updates	Expired (Expiration Date: 2023/04/01)	Renew
Application Control Signatures	Version 22.00482	Actions
Device & OS Identification	Version 1.00146	
Internet Service Database Definitions	Version 7.02992	
Intrusion Prevention	Expired (Expiration Date: 2023/04/01)	Renew
IPS Definitions	Version 22.00482	Actions
IPS Engine	Version 6.00139	
Malicious URLs	Version 4.00601	
Botnet IPs	Version 7.02992	View List
Botnet Domains	Version 3.00167	View List
AntiVirus	Expired (Expiration Date: 2023/04/01)	Renew
AV Definitions	Version 90.09965	
AV Engine	Version 6.00172	
Mobile Malware	Version 90.09964	
Web Filtering	Expired (Expiration Date: 2023/04/01)	Renew
Blocked Certificates	Version 1.00410	
Outbreak Prevention	Expired (Expiration Date: 2023/04/01)	Renew
Industrial DB	Pending	
Industrial Attack Definitions	Version 6.00741	
FortiIPAM	Pending	
IoT Detection Service	Pending	

7.16 Eventos relevantes

- Dada la integración de las plataformas de seguridad desplegadas en la entidad le permite al Ictetex prevenir ataques de Ciberseguridad que comprometan la continuidad del negocio.
- Durante el mes de abril no se presentaron eventos relevantes, que afectaran la disponibilidad de los servicios de la entidad a nivel de la solución de Seguridad.
- Con los módulos de IPS y Antimalware se logró bloquear más de 18,262 eventos de diferentes tipos de ataques, que pudieran comprometer la infraestructura de Ictetex

Intrusions By Types

#	Intrusion Type	Counts
1	Other	18,262
2	Anomaly	2,519
3	Permission/Privilege/Access Control	2,338
4	OS Command Injection	1,009
5	Code Injection	925
6	Path Traversal	430
7	Malware	239
8	SQL Injection	212
9	XSS	100
10	DoS	33
11	Information Disclosure	16
12	Improper Authentication	15

7.17 ACTIVIDADES

7.17.1 Actividades Realizadas

- Atención de tareas, casos e incidentes en la plataforma y escalados mediante correo.
- Atención de solicitud de permisos, creaciones de VPNs SSL, configuraciones y creación de políticas y enrutamientos ingresados por la plataforma Aranda.

7.17.2 Actividades pendientes

- Nos encontramos en proceso de migración y cambio de equipos, una vez finalizada esta actividad se validará estado final de las plataformas.

7.18 RECOMENDACIONES

- Se detecta que no existe segmentación definida en las redes de ICETEX que permitan establecer claramente que debe acceder o alcanzar que.
- 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.

7.19 CONCLUSIONES

- La segmentación de la red permite tener una mejor administración y control en caso de un incidente informático.

8 CONCLUSION

En resumen, podemos concluir que durante el mes de abril de 2023, los especialistas han resuelto todos los casos registrados en la herramienta de Mesa de Servicio Aranda de manera exitosa. Estos casos se relacionaron principalmente con problemas de acceso a servicios a través de conexiones FTP y directorios compartidos, así como la escalación de errores en algunas aplicaciones críticas. Además, se destaca que se ha avanzado significativamente en la gestión de la plataforma institucional durante el mes, cumpliendo con la mayoría de las actividades planificadas. En general, los resultados del mes son muy positivos, llevando a cabo mejoras importantes en la gestión de la plataforma institucional

Por otra parte, se ha logrado cumplir con los objetivos establecidos para el proyecto. Durante este período, se han realizado avances significativos en varias áreas clave, incluyendo:

Provisión de conectividad y red de comunicaciones: Se han implementado medidas para mejorar la conectividad y se ha avanzado en la optimización de la red de comunicaciones. Estas acciones han permitido mejorar la velocidad y la estabilidad de la red, brindando un entorno más confiable para el intercambio de información.

Servicios de seguridad informática: Se han implementado medidas de seguridad informática robustas, incluyendo firewalls, sistemas de detección de intrusiones y políticas de acceso y autenticación. Estas acciones han fortalecido la protección de los sistemas y datos del proyecto contra amenazas cibernéticas.

Integración de servicios de nube: Se ha avanzado en la estructuración para la integración de servicios de nube, permitiendo aprovechar los beneficios de la computación en la nube, como la escalabilidad, la flexibilidad y la disponibilidad de recursos.

Servicios conexos que garantizan calidad, confiabilidad, continuidad y seguridad web: Se han implementado servicios conexos que aseguran la calidad, confiabilidad, continuidad y seguridad de los servicios web del proyecto. Estas medidas han contribuido a brindar una experiencia de usuario mejorada y a garantizar la disponibilidad de los servicios ofrecidos.

Se llevaron a cabo una serie de acciones para mejorar la configuración y el rendimiento de las bases de datos en los entornos de producción. Esto incluyó la configuración de una consola de monitoreo, el mantenimiento de las bases de datos mediante la defragmentación de índices y la toma de estadísticas.

También se solucionaron problemas en la ejecución de una funcionalidad importante, se realizó una replicación de una base de datos importante y se actualizó la infraestructura del servidor para estar alineados con el entorno productivo.

Además, se implementó un proceso más eficiente para la restauración de una base de datos, lo cual nos permitió ahorrar espacio y reducir el tiempo necesario para completar el proceso. Estamos en proceso de mejorar y documentar el proceso de actualización de otra base de datos importante.

Por otra parte, es importante destacar que se han implementado exitosamente estos servicios especializados, asegurando el funcionamiento eficiente y seguro de los sistemas y la infraestructura tecnológica del ICETEX.

No obstante, es necesario señalar que aún existen aspectos pendientes de completar para lograr el cumplimiento total del alcance definido. Estos pendientes incluyen [mencionar las tareas o áreas específicas que faltan]. El equipo Infotíc está trabajando diligentemente en abordar estos puntos y se espera que, en las etapas posteriores, se avance significativamente en el cumplimiento del alcance definido.