Sogamoso, Junio de 2023

Ingeniero
JUAN CARLOS BERNAL MESA
Profesional Universitario
Oficina de la Tics y Comunicaciones
Alcaldía de Sogamoso

Asunto: Presentación de informe N° 3 contrato 20230294

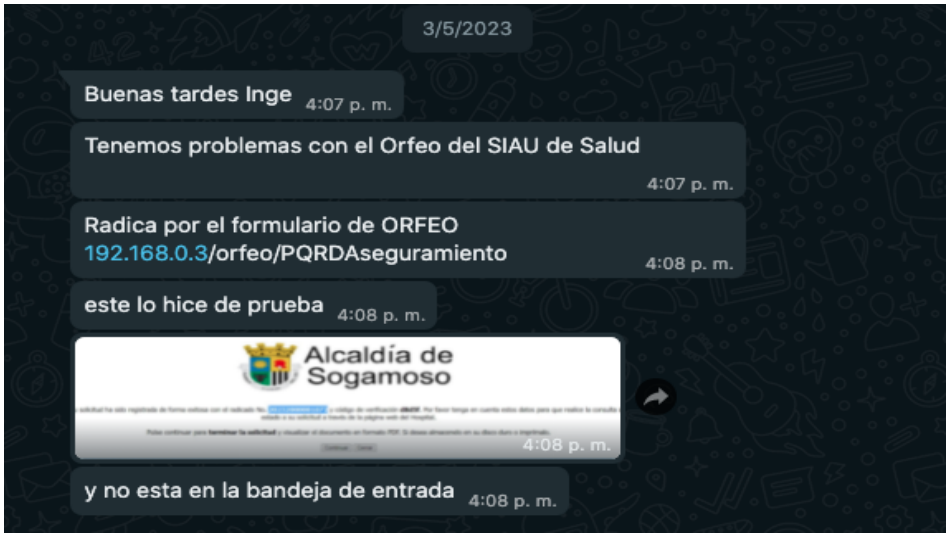
Respetado Ingeniero:

Cordialmente me permito presentar informe del periodo comprendido entre 23 de Abril al 22 de Mayo; teniendo en cuenta contrato de prestación de servicios de apoyo a la gestión número 20230294 así:

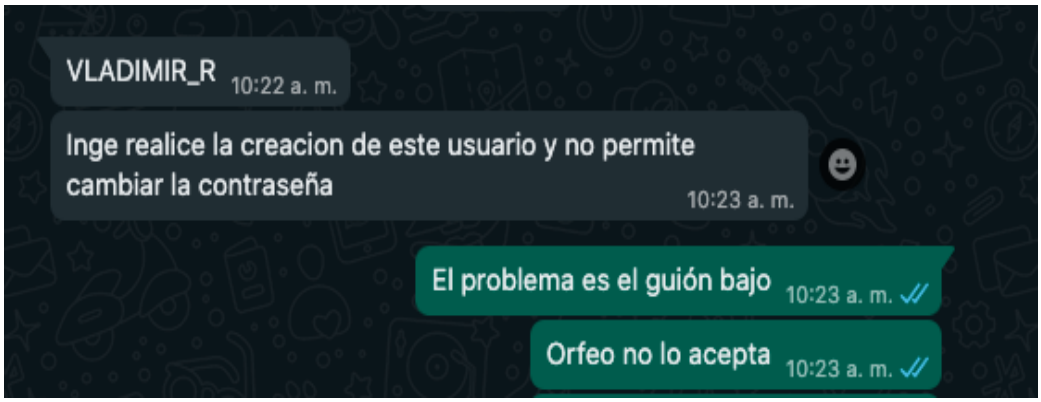
Actividad:

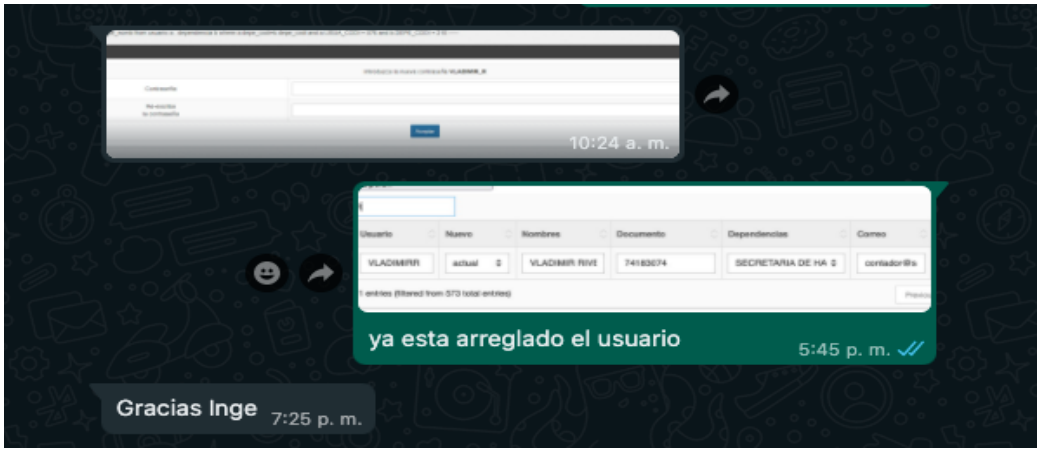
1. Apoyar el soporte técnico de la plataforma tecnológica y redes informáticas del Municipio de Sogamoso en sus diferentes dependencias.

   Por WhatsApp se manifiesta error en el formulario PQRD de Orfeo para aseguramiento ya que al radicar la petición no parece en bandeja. Se reviso el formulario y se evidencio un error en variable de identificación de usuario el cual se corrige y se hacen pruebas pertinentes.

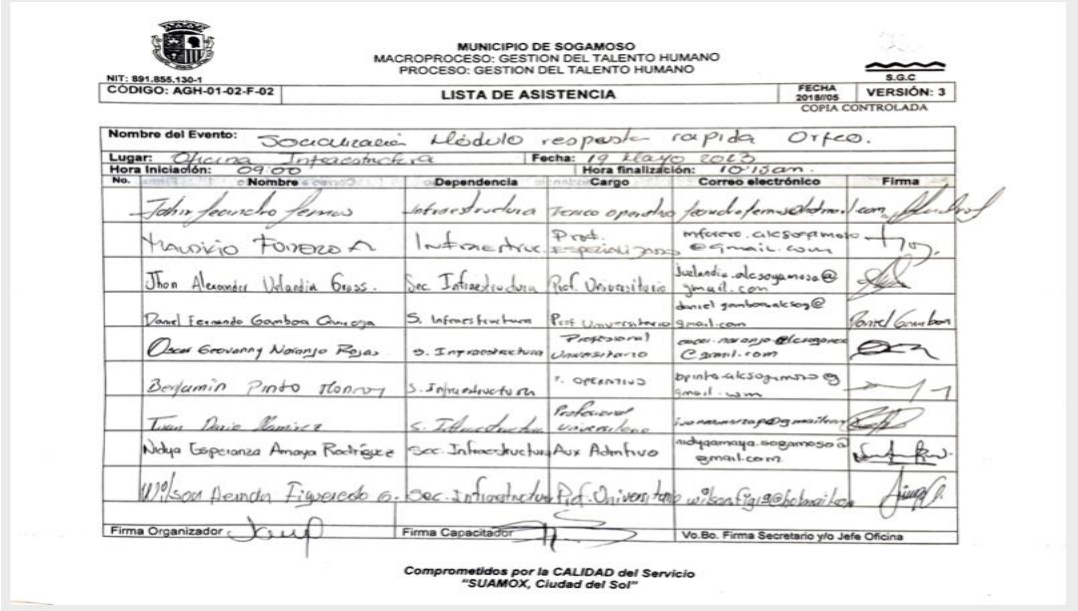


   Se solicita verificación de usuario VLADIMIR_R en Orfeo ya que no deja ingresar. Se manifiesta que el carácter “guion abajo” no es válido dentro de Orfeo.





Se brinda capacitación a funcionarios de Secretaria de Infraestructura sobre módulo de respuesta rápida para el cierre de ciclo primario de gestión documental Orfeo.



MUNICIPIO DE SOGAMOSO
MACROPROCESO: GESTION DEL TALENTO HUMANO
PROCESO: GESTION DEL TALENTO HUMANO

NIT: 891.855.130-1 | CODIGO: AGH-01-02-F-02 | LISTA DE ASISTENCIA | FECHA 2018/05 | S.G.C | VERSIÓN: 3
COPIA CONTROLADA

Nombre del Evento: Socialización Módulo respuesta rapida Orfeo.
Lugar: Oficina Infraestructura Fecha: 18 Mayo 2018
Hora Iniciación: 09:00 Hora finalización: 10:15am.

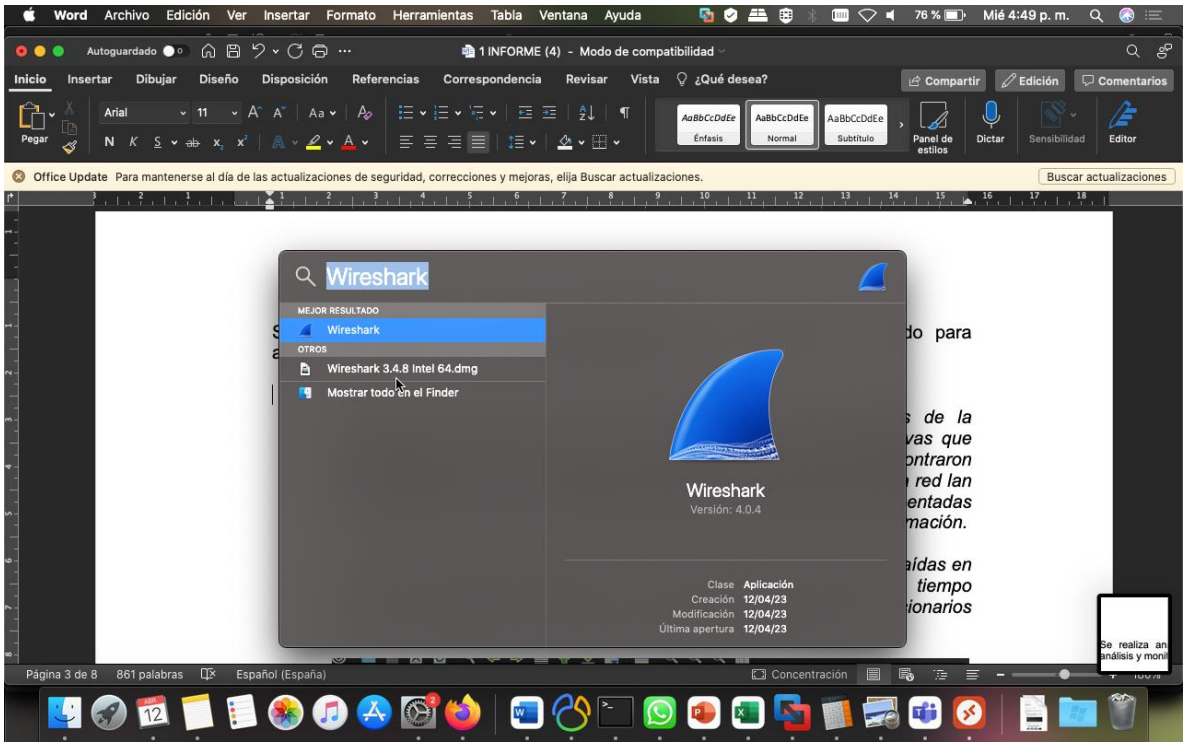
No.	Nombre	Dependencia	Cargo	Correo electrónico	Firma
	Johnn Jaimucho Torres	Infraestructura	Tecnico operativo	fenando.fernandez@...	
	Mauricio Fonseca A	Infraestruc.	Prof. Especializado	mfonseca.alcsogamoso@gmail.com	
	Jhon Alexander Valencia Grass.	Sec. Infraestructura	Prof. Universitario	Juelandia.alcsogamoso@gmail.com	
	Daniel Fernando Gamboa Quiroga	S. Infraestructura	Prof. Universitario	daniel.gamboa.alcsog@gmail.com	
	Oscar Geovanny Naranjo Rojas	S. Infraestructura	Profesional Universitario	oscar.naranjo@alcsogamoso.gmail.com	
	Benjamin Pinto Monroy	S. Infraestructura	T. OPERATIVO	bpinto.alcsogamoso@gmail.com	
	Juan Davis Ramirez	S. Infraestructura	Profesional Universitario	juanramirez@gmail.com	
	Nidya Esperanza Amaya Rodriguez	Sec. Infraestructura	Aux Admtivo	nidyaamaya.sogamoso@gmail.com	
	Wilson Alexander Figueredo G.	Sec. Infraestructura	Prof. Universitario	wilsonfig19@hotmail.com	

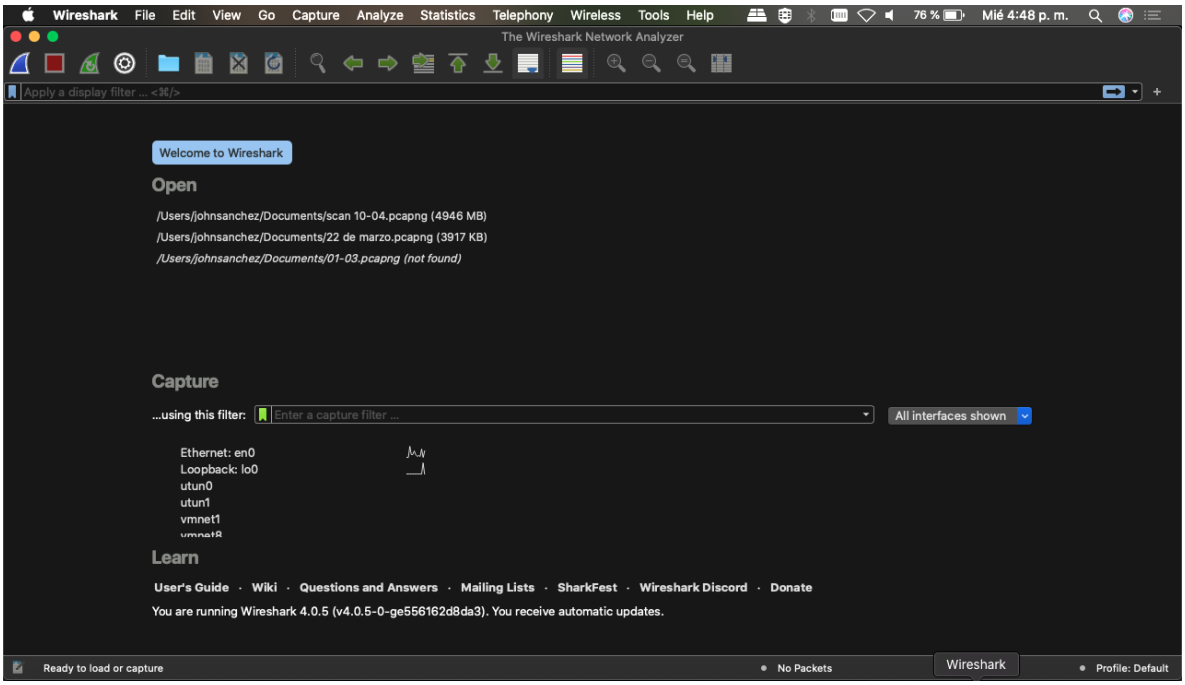
Firma Organizador | Firma Capacitador | Vo.Bo. Firma Secretario y/o Jefe Oficina

Comprometidos por la CALIDAD del Servicio
"SUAMOX, Ciudad del Sol"

2. Realizar el análisis de tráfico y paquetes de información de entrada y salida de la red de datos de la administración municipal, reportando a la entidad de manera oportuna, anomalías o incidentes de ciberseguridad según el procedimiento de seguridad y privacidad de la información del municipio de Sogamoso.

Se realiza análisis con software WIRESHARK tipo OpenSource, utilizado para análisis y monitoreo de red para hacking preventivo.





Funcionamiento de WireShark

El software escanea la red de datos en la cual se encuentra conectada, para el caso particular del municipio de Sogamoso incluye los siguientes edificios:

Edificio Torre 6
Edificio El Pintor
Edificio Rojas
Secretaria de Educación

Las demás instalaciones no se incluyen en el mapeo puesto que no están interconectados por el FORTINET.

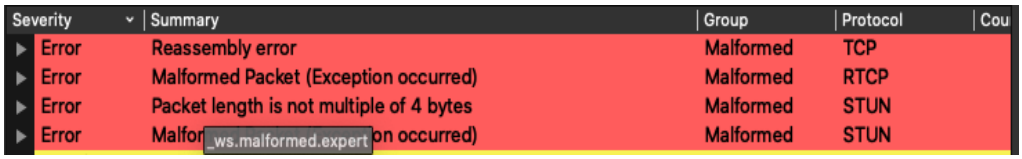
Luego de mapear la red inicia un análisis de peticiones entrada salida según protocolo y por origen de petición comparándola con un base de datos de vulnerabilidades, donde se clasifica y cualifica según el nivel si hay o no un riesgo latente de ataque o problema de red.

En este periodo correspondiente entre abril mayo se evidencio un intento de ingreso por fuerza bruta por el Fortinet buscado vulnerabilidades en los puertos por medio de boot, saturando el canal de internet de entrada.

Se revisa por wire shark en búsqueda del origen descartando que fuera interno.

Pero no se evidencia un origen interno formando paquetes para extracción.

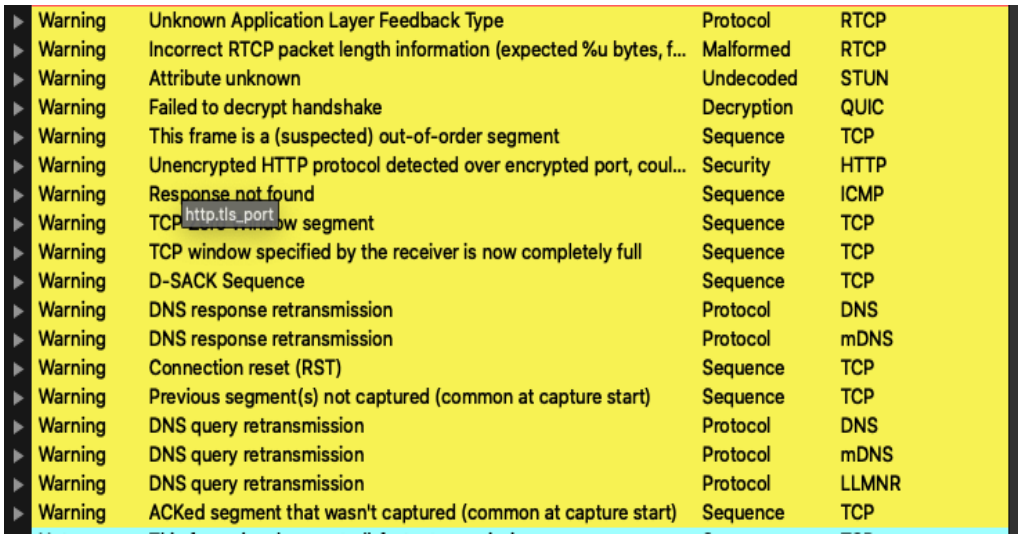
- *Se realizaron análisis de tráfico periódicos de la red de datos de la administración municipal y no sé en evidencia anomalías significativas que hagan referencia a un ciberataque se puede concluir que se dice encontraron registros de paquetes de datos perdidos desde la red internet hacia la red lan de la entidad a su vez se evidencia la eficacia de las políticas implementadas en fortinet dando así como un objetivo primario la seguridad de la información.*



Severity	Summary	Group	Protocol	Cou
Error	Reassembly error	Malformed	TCP	
Error	Malformed Packet (Exception occurred)	Malformed	RTCP	
Error	Packet length is not multiple of 4 bytes	Malformed	STUN	
Error	Malfor_ws.malformed.expert on occurred)	Malformed	STUN	

En esta pantalla se encontraron 4 errors, lo cual significa que se armarton 4 paquetes de datos los cuales no se cotejan con la bd de validación no se envidencia que tipo de información se empaqueto pero no refleja un riesgo para la red. Los protocolos de control en tiempo real o RCTP es un protocolo de comunicación que proporciona de control y esta asociado con el flujo de datos para una aplicación multimedia. Este protocolo trabaja en conjunto con el rtp en el transporte y empaquetado de datos multimedia pero no trnasporta ningún datos por si mismo.

Los protocolos STUN es un protocolo de red del tipo cliente servidor que permite a clientes NAT en contrar su dirección publica.



Warning	Unknown Application Layer Feedback Type	Protocol	RTCP
Warning	Incorrect RTCP packet length information (expected %u bytes, f...	Malformed	RTCP
Warning	Attribute unknown	Undecoded	STUN
Warning	Failed to decrypt handshake	Decryption	QUIC
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP
Warning	Unencrypted HTTP protocol detected over encrypted port, coul...	Security	HTTP
Warning	Response not found	Sequence	ICMP
Warning	TCP http.tls_port w segment	Sequence	TCP
Warning	TCP window specified by the receiver is now completely full	Sequence	TCP
Warning	D-SACK Sequence	Sequence	TCP
Warning	DNS response retransmission	Protocol	DNS
Warning	DNS response retransmission	Protocol	mDNS
Warning	Connection reset (RST)	Sequence	TCP
Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP
Warning	DNS query retransmission	Protocol	DNS
Warning	DNS query retransmission	Protocol	mDNS
Warning	DNS query retransmission	Protocol	LLMNR
Warning	ACKed segment that wasn't captured (common at capture start)	Sequence	TCP

Los warning reflejados en la imagen superior son a causa de software realizando petiones de conexión a servidores ya sea para almacenamiento de información o solicitud de actualizaciones los cuales están restringidos por políticas del Fortinet. No representan un riesgo real a la seguridad de la red interna

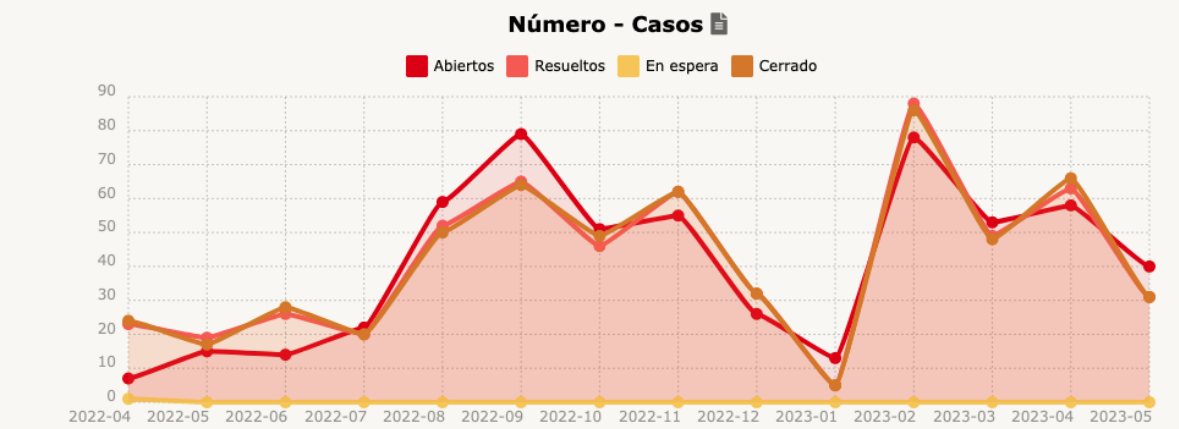
Note	This frame is a (suspected) fast retransmission	Sequence	TCP
Note	Time To Live	Sequence	IPv4
Note	Coalesced Padding Data	Protocol	QUIC
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP
Note	Seconds elapsed appears to be encoded as little-endian	Protocol	DHCP/BOOTP
Note	This QUIC frame has a reused stream offset (retransmission?)	Sequence	QUIC
Note	A new tcp session is started with the same ports as an earlier s...	Sequence	TCP
Note	ACK to a TCP keep-alive segment	Sequence	TCP
Note	TCP keep-alive segment	Sequence	TCP
Note	This frame is a (suspected) retransmission	Sequence	TCP
Note	This session reuses previously negotiated keys (Session resum...	Sequence	TLS
Note	Padding identification may be inaccurate and impact trailer diss...	Protocol	Ethertype
Note	This frame undergoes the connection closing	Sequence	TCP
Note	This frame initiates the connection closing	Sequence	TCP
Note	Duplicate ACK	Sequence	TCP
Note	Time To Live	Sequence	IPv4

Estos son eventos de bajo nivel que han ocurrido dentro de la red.

Chat	Formatted text	Sequence	HTTP
Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP
Chat	Connection establish request (SYN)	Sequence	TCP
Chat	TCP window update	Sequence	TCP
Chat	Connection finish (FIN)	Sequence	TCP
Chat	Formatted text	Sequence	SSDP

3. Realizar soporte técnico y gestión a la mesa de ayuda garantizando su disponibilidad e integridad de los datos para la gestión de casos del parque informático de la administración municipal.

Las condiciones técnicas del aplicativo y el servidor son optimas. Se hizo revisión previa a los casos que han sido incluidos en este nuevo periodo y se evidencia la creación de 106 casos en la administración y de esos 107 de manera oportuna se han tramitado y cerrado 107. Se puede generar la inquietud del caso de mas. Al ver la relacion de este se refleja que viene arrastrado del periodo anterios y en este se dio solucion.se conlcuye los casos generardos demuestra una efcitividad en el servicio del 100.94% para el periodo comprendido de este informe.



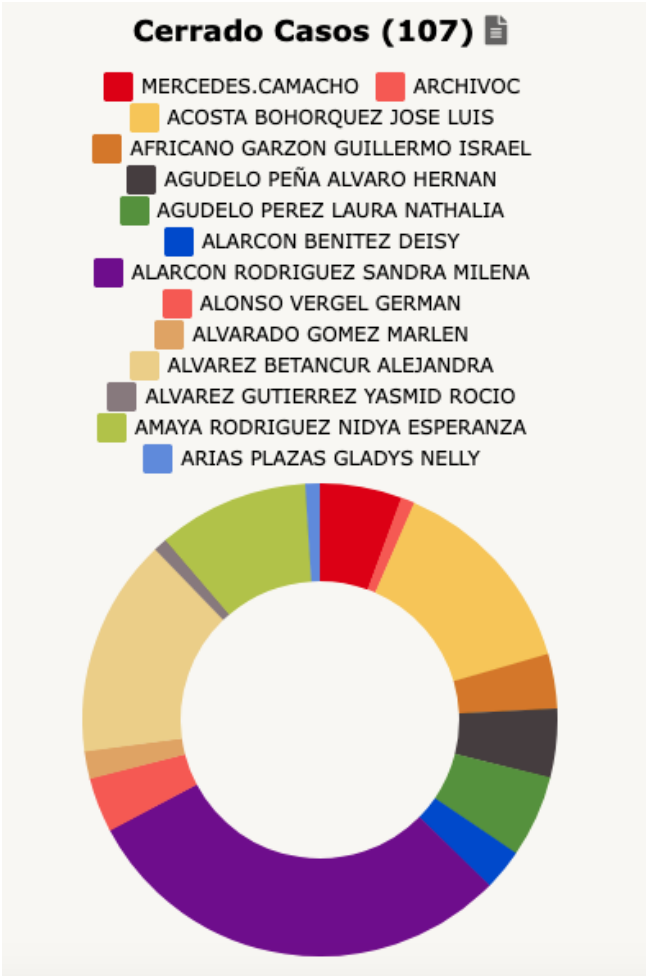
Esta grafica represente el numero de casos creados en sistema realizando una comprativa de estado de solicitudes.



Aquí se refleja en tiempo, el promedio en atencion de un caso registrado.




Resuelto Casos (107)
MERCEDES.CAMACHO
ARCHIVOC
ACOSTA BOHORQUEZ JOSE LUIS
AFRICANO GARZON GUILLERMO ISRAEL
AGUDELO PEÑA ALVARO HERNAN
AGUDELO PEREZ LAURA NATHALIA
ALARCON BENITEZ DEISY
ALARCON RODRIGUEZ SANDRA MILENA
ALONSO VERGEL GERMAN
ALVARADO GOMEZ MARLEN
ALVAREZ BETANCUR ALEJANDRA
ALVAREZ GUTIERREZ YASMID ROCIO
AMAYA RODRIGUEZ NIDYA ESPERANZA
ARIAS PLAZAS GLADYS NELLY
ALARCON BENITEZ DEISY
3

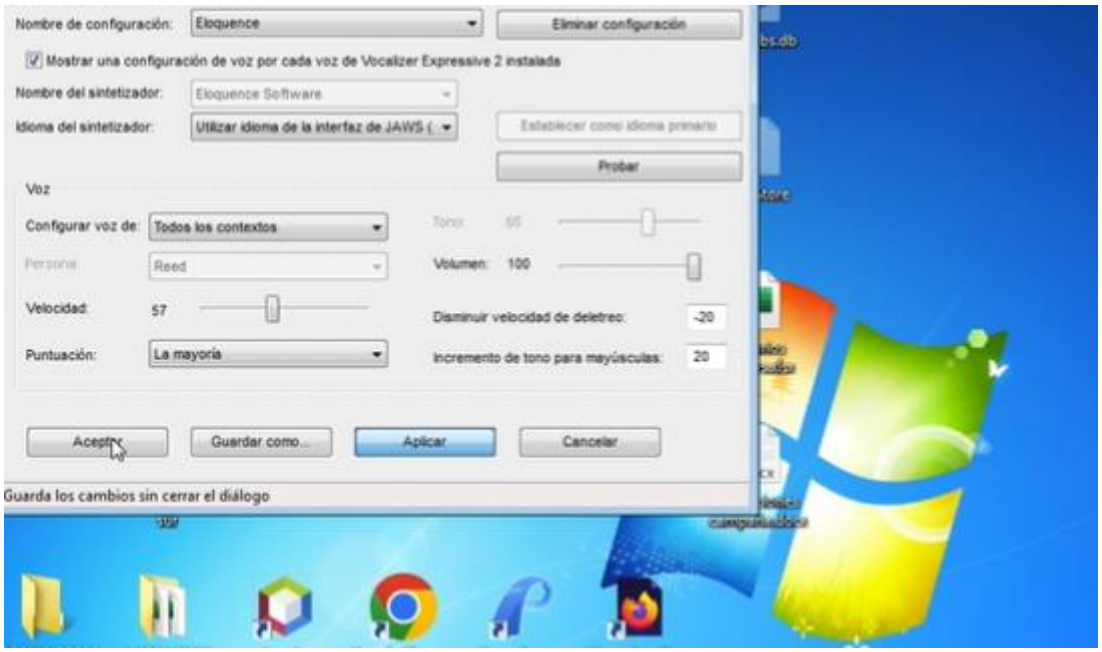

Cerrado Casos (107)
MERCEDES.CAMACHO
ARCHIVOC
ACOSTA BOHORQUEZ JOSE LUIS
AFRICANO GARZON GUILLERMO ISRAEL
AGUDELO PEÑA ALVARO HERNAN
AGUDELO PEREZ LAURA NATHALIA
ALARCON BENITEZ DEISY
ALARCON RODRIGUEZ SANDRA MILENA
ALONSO VERGEL GERMAN
ALVARADO GOMEZ MARLEN
ALVAREZ BETANCUR ALEJANDRA
ALVAREZ GUTIERREZ YASMID ROCIO
AMAYA RODRIGUEZ NIDYA ESPERANZA
ARIAS PLAZAS GLADYS NELLY

4. Realizar actualizaciones en capacitaciones en la oficina de atención al usuario relacionadas con el centro de relevo y/o demás herramientas tecnológicas dispuestas para discapacidad.

   Se genera video de uso de la herramienta JAWS para se compartido en la oficina de atención al usuario. Para posterior hacer capacitación en sitio.

   http://192.168.0.133/owncloud/index.php/f/259375

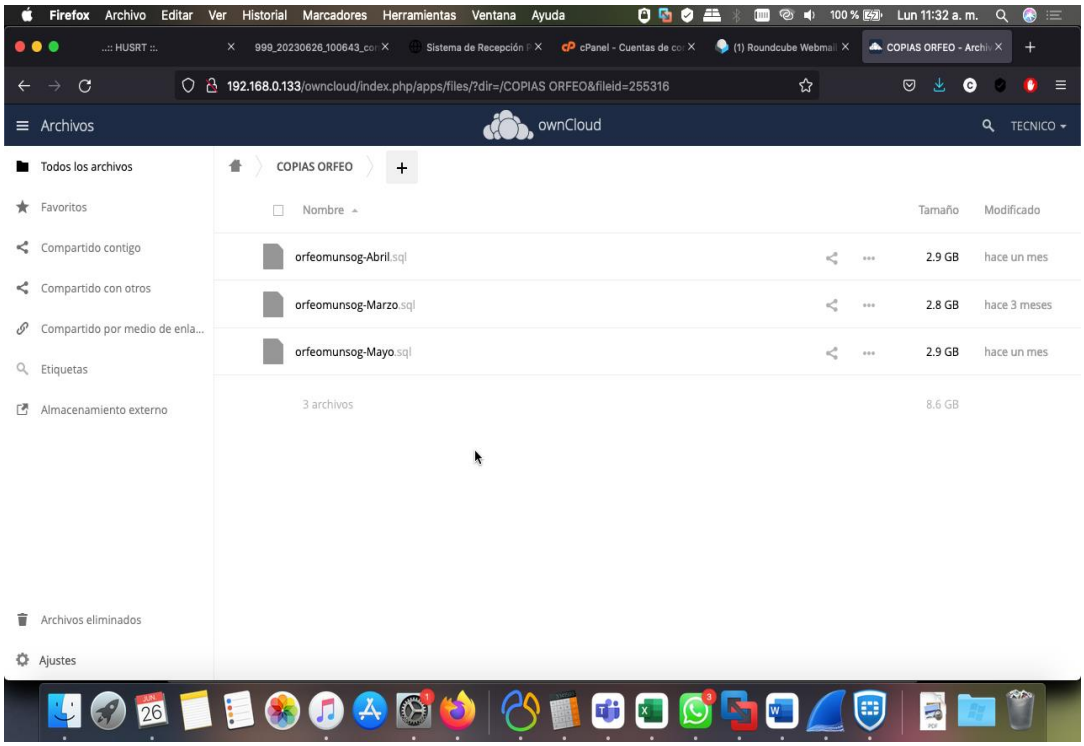






5. Generar copias de seguridad del software de gestión documental Orfeo que permitan su adecuado restablecimiento.

Se generan copias de seguridad correspondientes al mes de febrero y marzo de la base de datos del sistema de gestión documental orfeo dejándolas almacenadas en la plataforma owncloud.



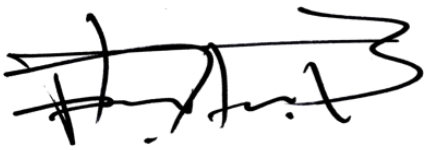
Por lo demás el sistema Orfeo a estado operando de forma intermitente, a causa del déficit de espacio en disco del servidor. Como medida de urgencia se ha liberado espacio en cache. Se sugiere la compra de un disco duro para servidor con el fin de liberar disco des sistema principal, migrando la bodega de imágenes (ya que es la carpeta que más espacio ocupa) al nuevo disco.

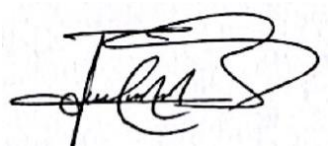
6. Las demás asignadas por el supervisor de acuerdo con el objeto de contrato.

Se asiste a reunión con la oficina asesora jurídica con el fin de elaborar acto administrativo cuyo objetivo sea la validación de las firmas mecánicas que se generan en la administración municipal u usar esto como herramienta legal para la implementación de firma digital dentro del software ORFEO.

Lo anterior para efectos de pago.

Atentamente,





Vo Bo Supervisor

_____

JOHN JAIRO SANCHEZ SOSA
Contratista