Sogamoso, Marzo de 2023

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

Asunto: Presentación de informe N°1 contrato 20230294

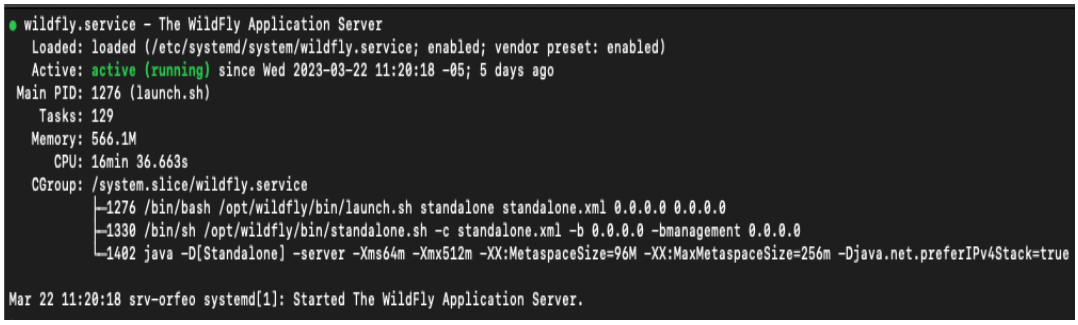
Respetado Ingeniero:

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

Actividad:

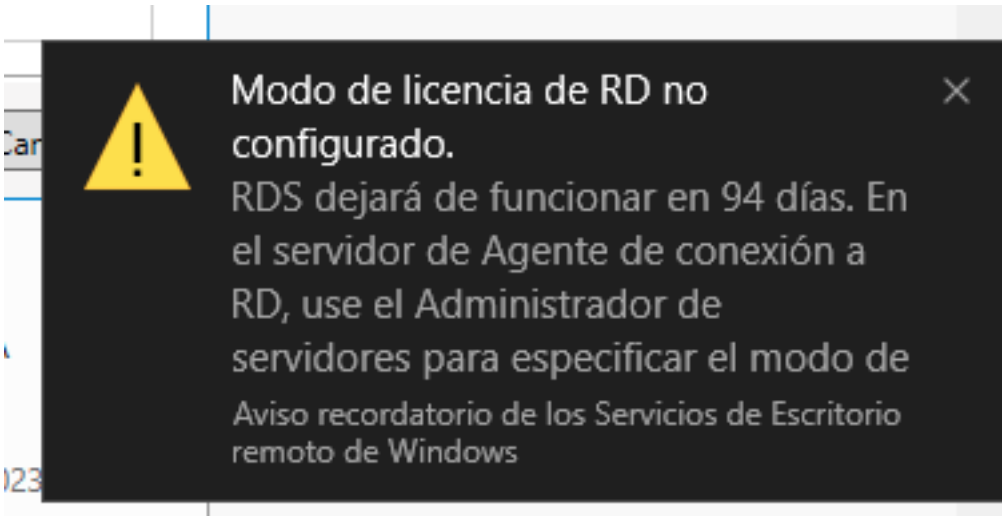
1. Apoyar el soporte técnico de la plataforma tecnológica y redes informáticas del Municipio de Sogamoso en sus diferentes dependencias.

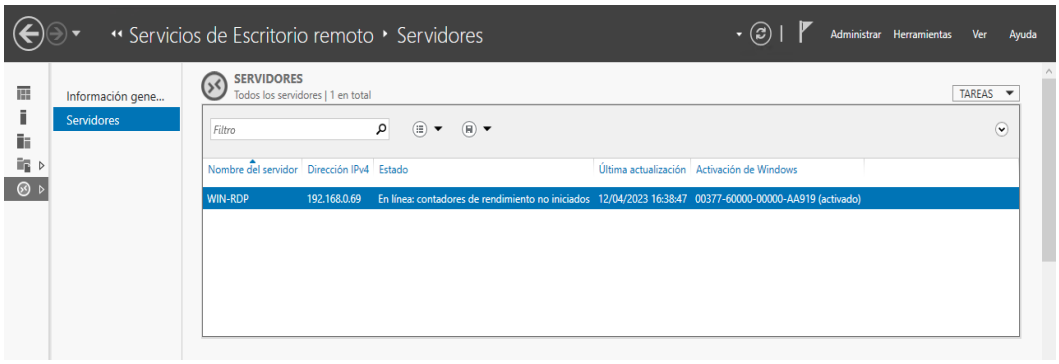
    - Se realiza revisión el servidor orfeo puesto que el servicio wildfly no está funcionando para la plataforma de la cámara de comercio dicho servicio fue activado nuevamente para el personal de sysman.

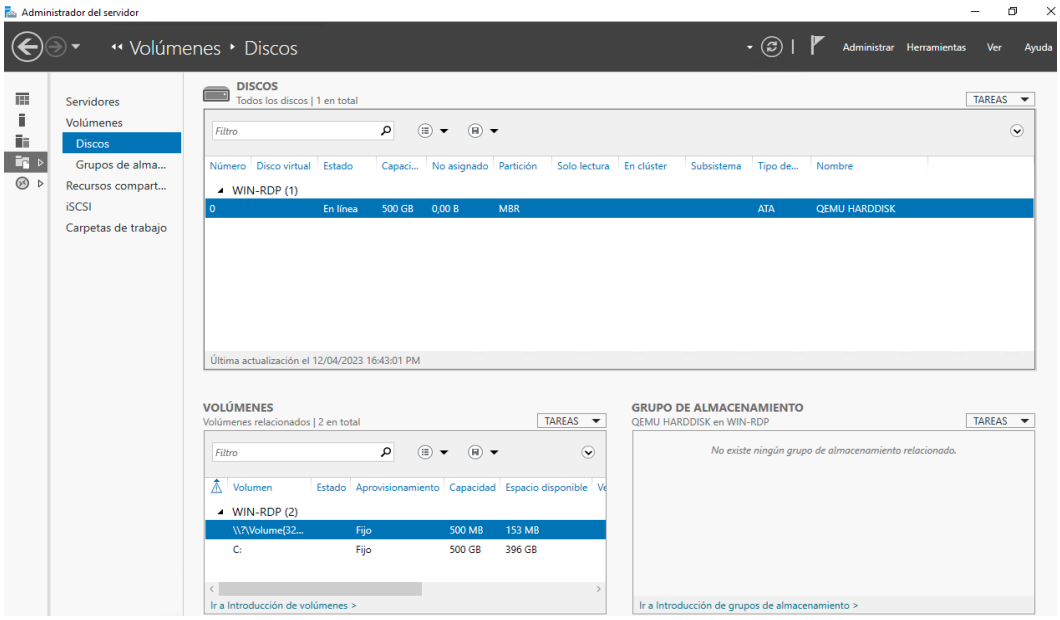


    - Se hace revisión a impresora térmica de atención al usuario por configuración en la impresión de stickers.

    - Se hace activación de licencia de prueba para el servidor RDP de la administración municipal de los cuales quedan 94 dias de version prueba.

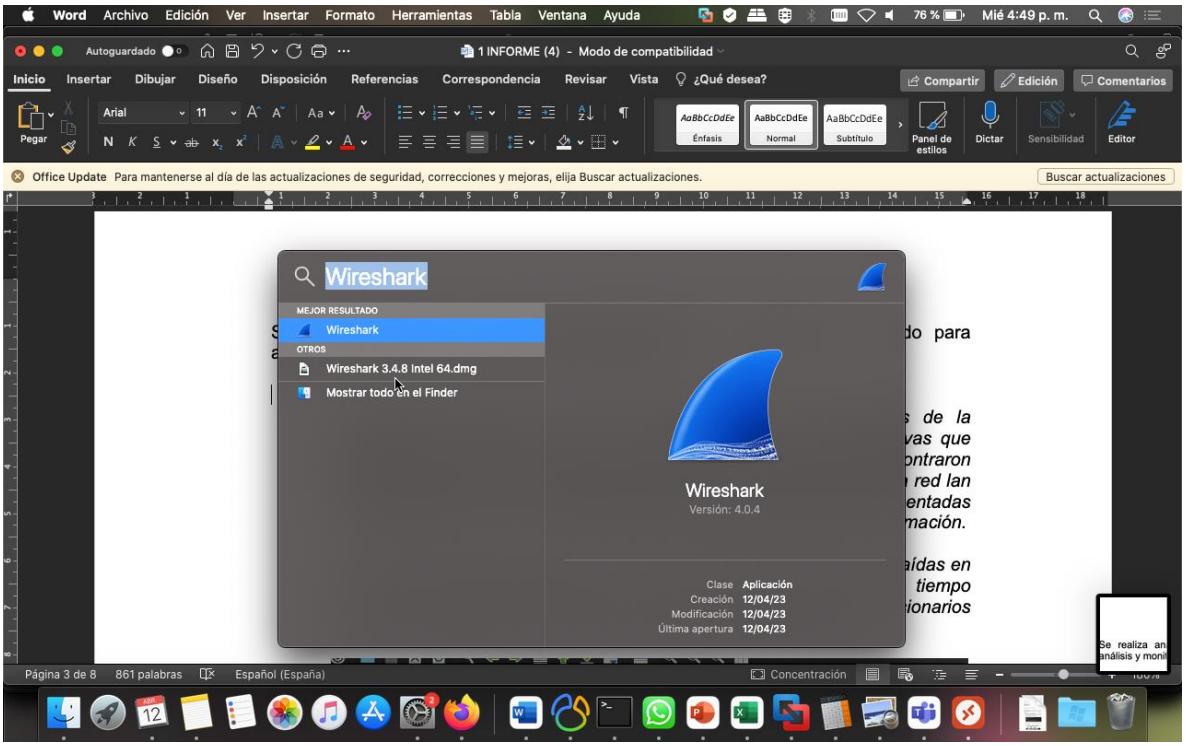


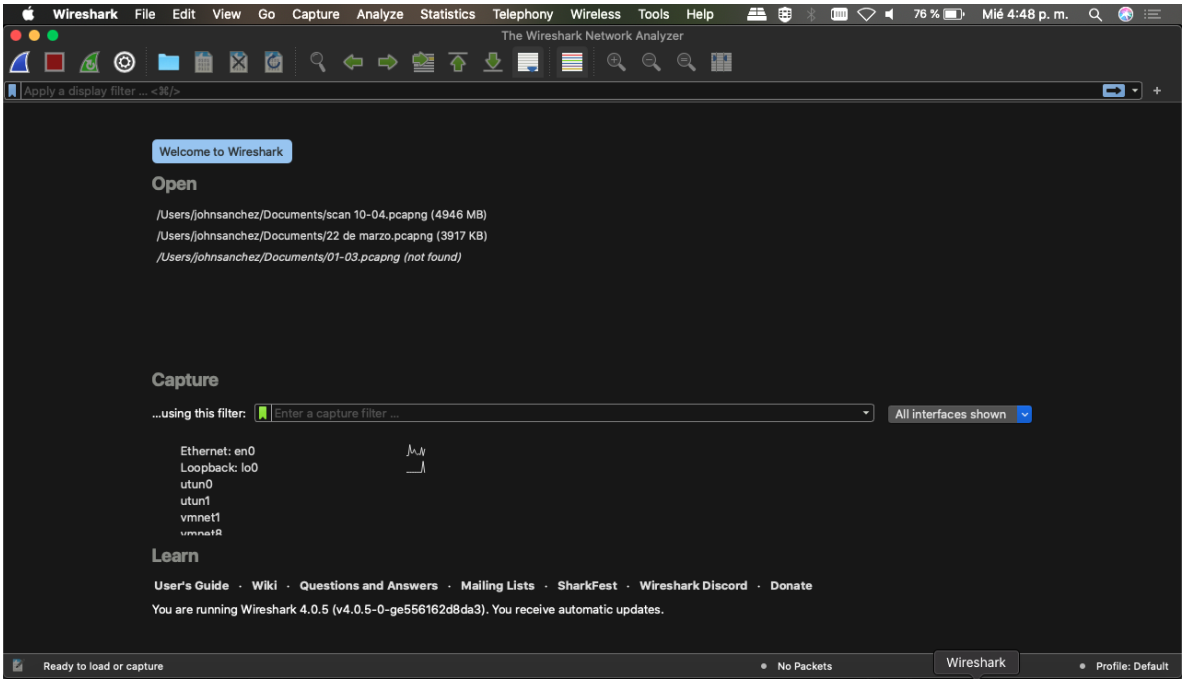




2. Realizar el análisis de tráfico y paquetes de información de entrada y salida de la red de datos de la administración municipal, reportando a la entidad de manera oportuna, anomalías o incidentes de ciberseguridad según el procedimiento de seguridad y privacidad de la información del municipio de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

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





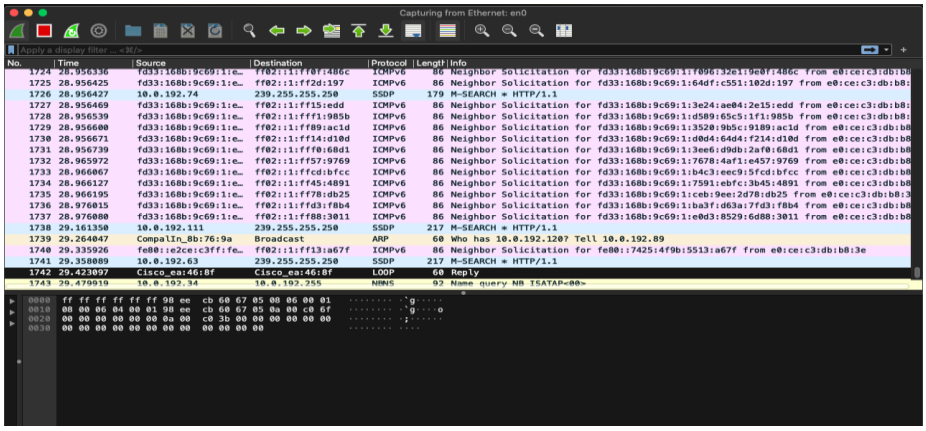
Funcionamiento de WireShark

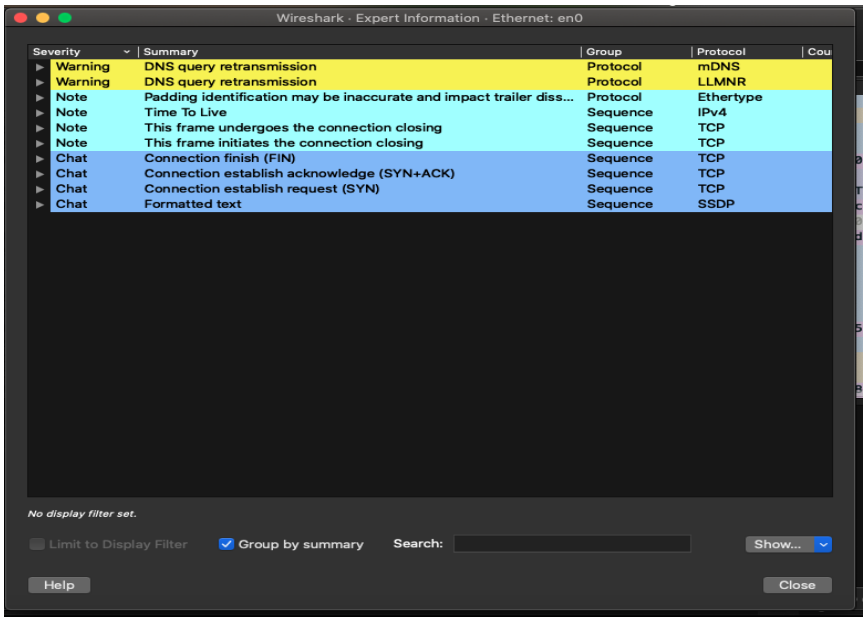
El software escanea la red de datos en la cual se encuentra conectada, para el caso particular del municipio de Sogamoso incluye los siguientes edificios:

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.

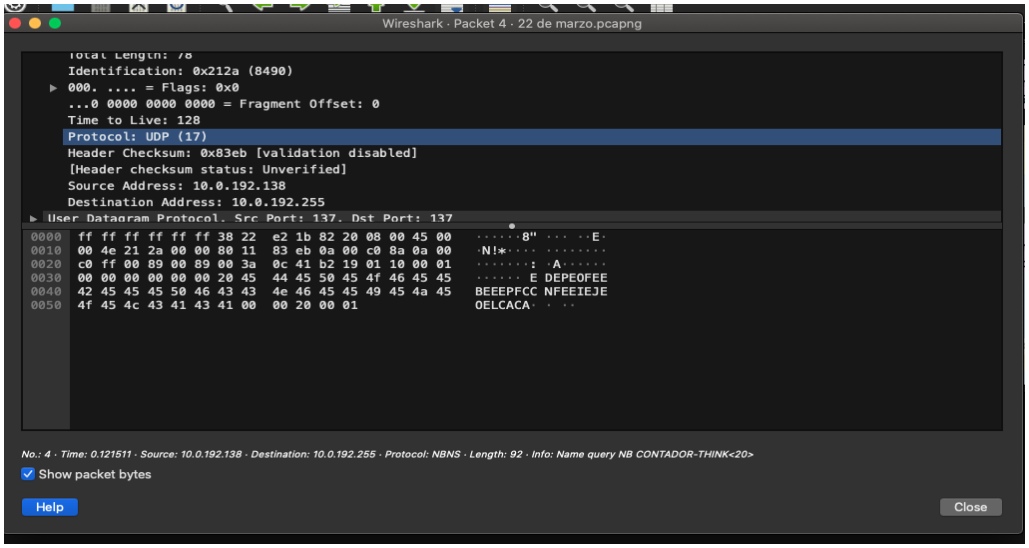
Luego de mapear la red inicia un análisis de peticiones entrada salida según protocolo y por origen de petición comparándola con un base de datos de vulnerabilidades, donde se clasifica y cualifica según el nivel si hay o no un riesgo latente de ataque o problema de red.



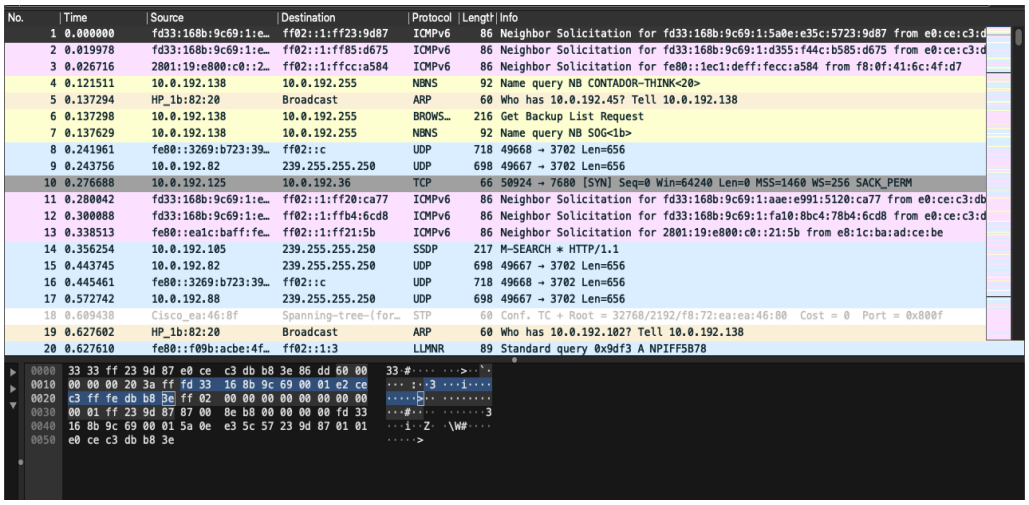


- *Se realizaron análisis de tráfico periódicos de la red de datos de la administración municipal y no sé en evidencia anomalías significativas que hagan referencia a un ciberataque se puede concluir que se dice encontraron registros de paquetes de datos perdidos desde la red internet hacia la red lan 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.*

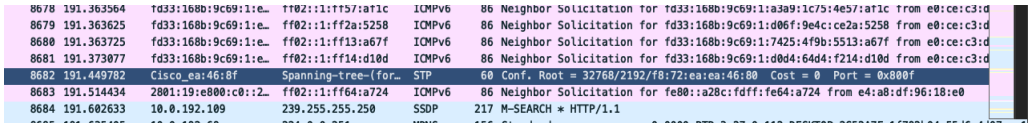
  como eventos de segundo plano se puede evidenciar problemas de caídas en el servicio de internet respecto a dns en periodos muy cortos de tiempo también las páginas a los cual es han estado ingresando a los funcionarios pero que por políticas del anillo perimetral se encuentran baneadas.



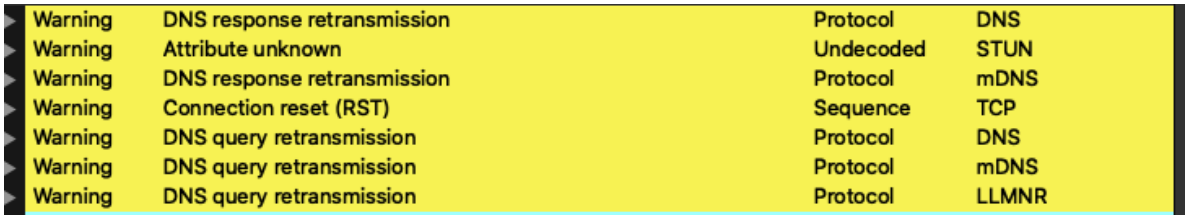
Se selección un reporte con estado de alerta por retransmision de DNS por protocolo ipv4. En esta grafica de observa que fue una peticion interna a un equipo que no dio respuesta. Esto puede suceder porque existe alguna carpeta compartida y no dejo acceder o un aplicativo que no dejo ingresar.



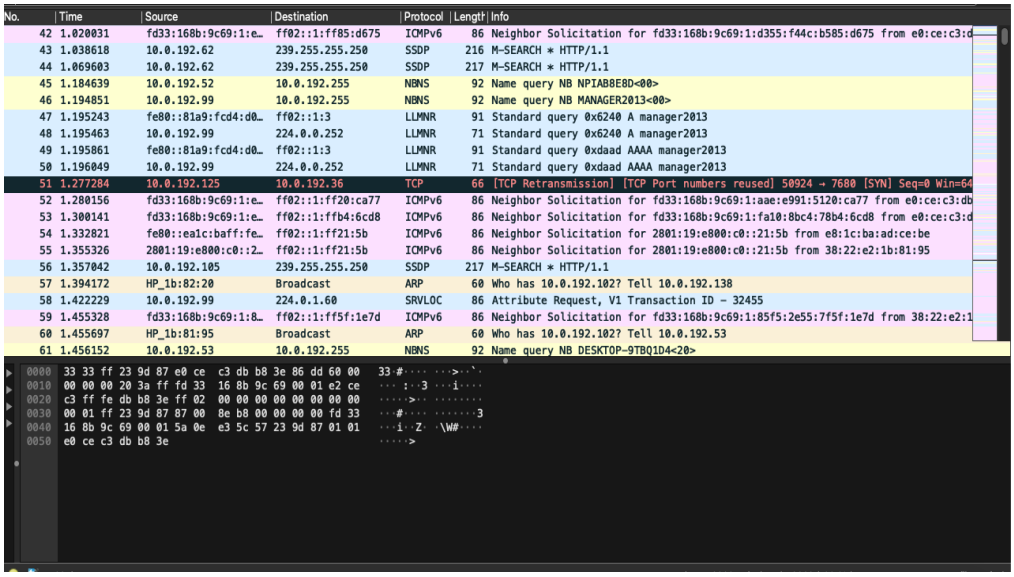
Esta grafica muestra la lectura del mapeo que se realiza en toda la red de datos.



Aquí se evidencia el trafico que esta generando una maquina por protocolo Ipv6 y no encuentra negociocion con el destino. Esta actividad no genera alerta alguna de actividad sospechosa.



Aquí se refleja los warning en el mapero de red. Son eventos que hay que prestar atencion porque son solicitudes realizadas pero no ha desembocado en respuesta satisfactoria por parte del receptor. Entre ellos la retransmision de DNS. Se tiene precaucion en ello por que existen tecnica de suplantacion de paginas web por medio de retransmicion de DNS que es el redicreccionamiento a otro servidor de dominio.

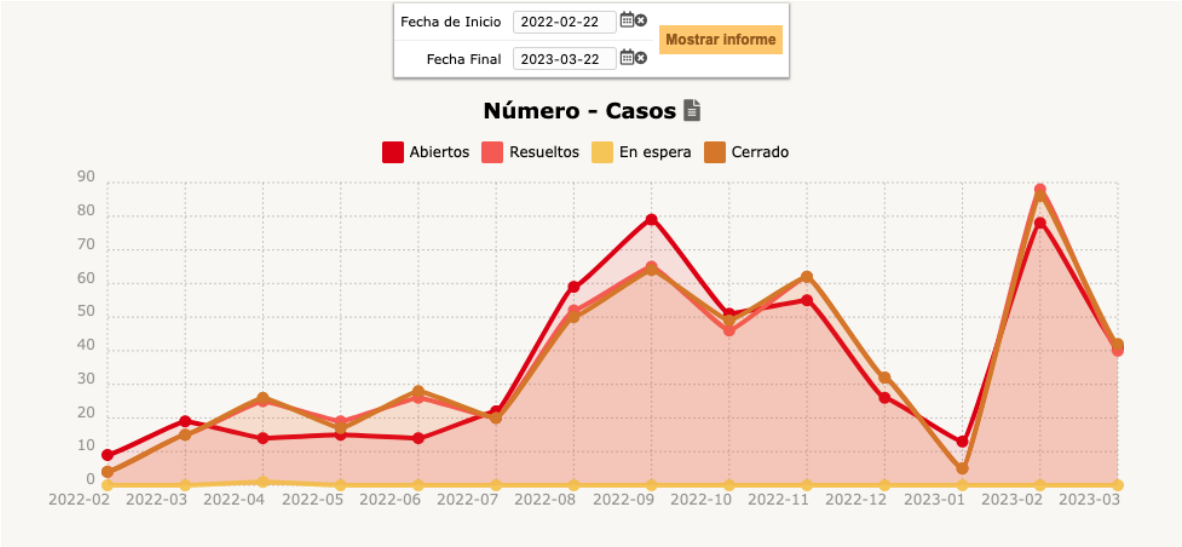


Al revisar a profundida este caso puntual no genero alerta algun de seguridad porque la peticion fue interna de la red.

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 97 casos en la administración y de esos 97 de manera oportuna se han tramitado y cerrado 94

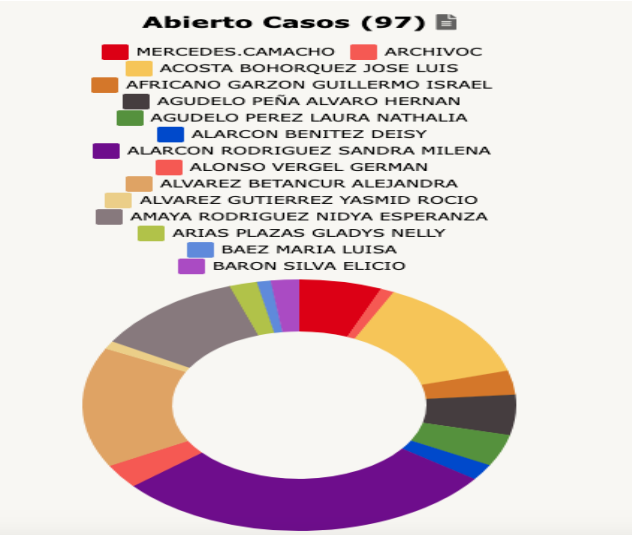
casos mostrando una efcitividad en el servicio del 97% para el periodo comprendido de este informe.

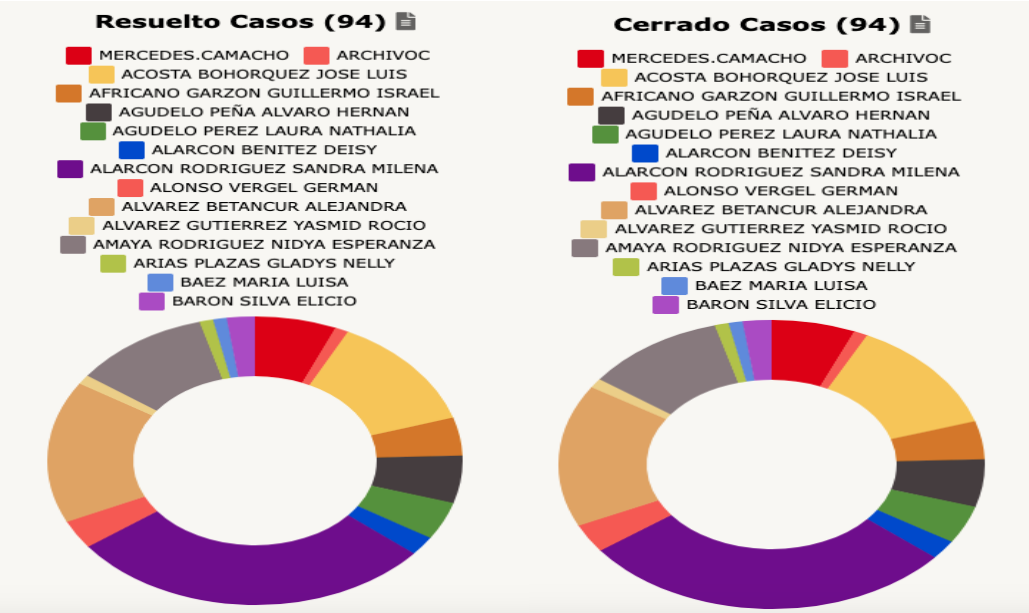


Esta grafica represente el numero de casos creados en sistema realizando una comprativa de estado de solicitudes.



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





Se sostuvo reunión con el nuevo administrador de la mesa de ayuda y se explica el funcionamiento de la plataforma en cuanto a asignación de casos cómo se reciben cómo se dan respuesta cómo se hacen los seguimientos y se hacen las recomendaciones respecto a los técnicos que atienden cada tarea.

sí inicia planificación para actualización del módulo de inventarios para ingresar lo que son servidores escáner y switch que forman parte de la plataforma tecnológica del municipio.

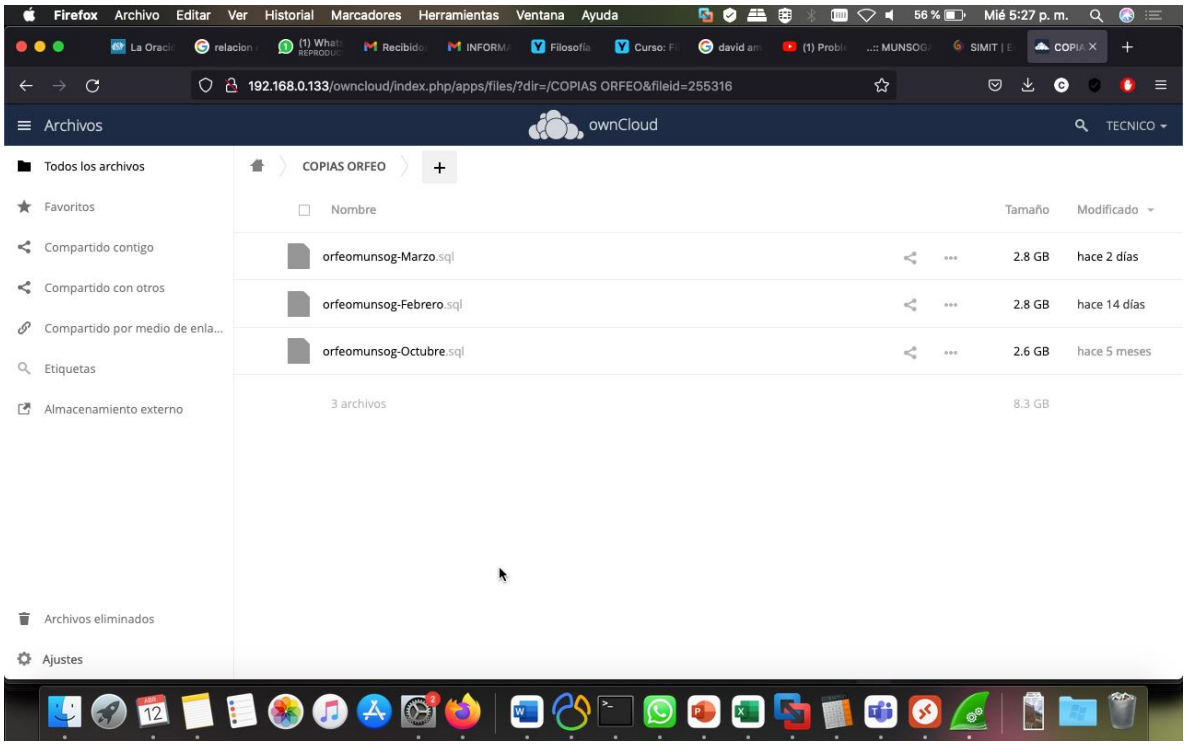
4. Realizar actualizaciones en capacitaciones en la oficina de atención al usuario relacionadas con el centro de relevo y/o demás herramientas tecnológicas dispuestas para discapacidad.

Se ha programado para el mes de abril capacitación con los funcionarios de atención al usuario el uso de la herramienta JAWS y ZOOMTEXT. Ya que se cuenta con

nuevos funcionarios que están para la atención al público. Fecha aproximada 17 de abril en la oficina Atención al Usuario.

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 jurídica para validar la simplificación de pasos de las respuestas que se generan en la dependencia y que son radicadas en la ventanilla única en El Salvador feo en miras de poder reducir carga de los funcionarios y optimizar el tiempo en otras actividades netas de la dependencia.

   se brinda asesoría y soporte para la detección de error te daño las cámaras de vigilancia de Sogabastos. Se revisa el switch y se evidencia que 4 puertos no estan respondiendo. Se sugiere cambio de swicth por posible daño fisico.

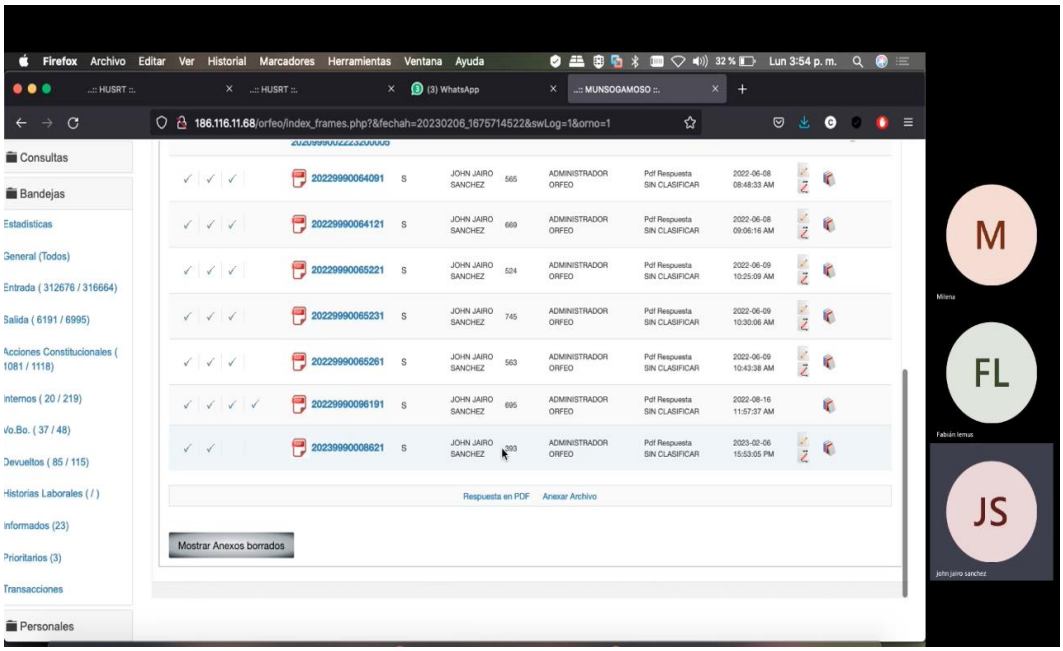


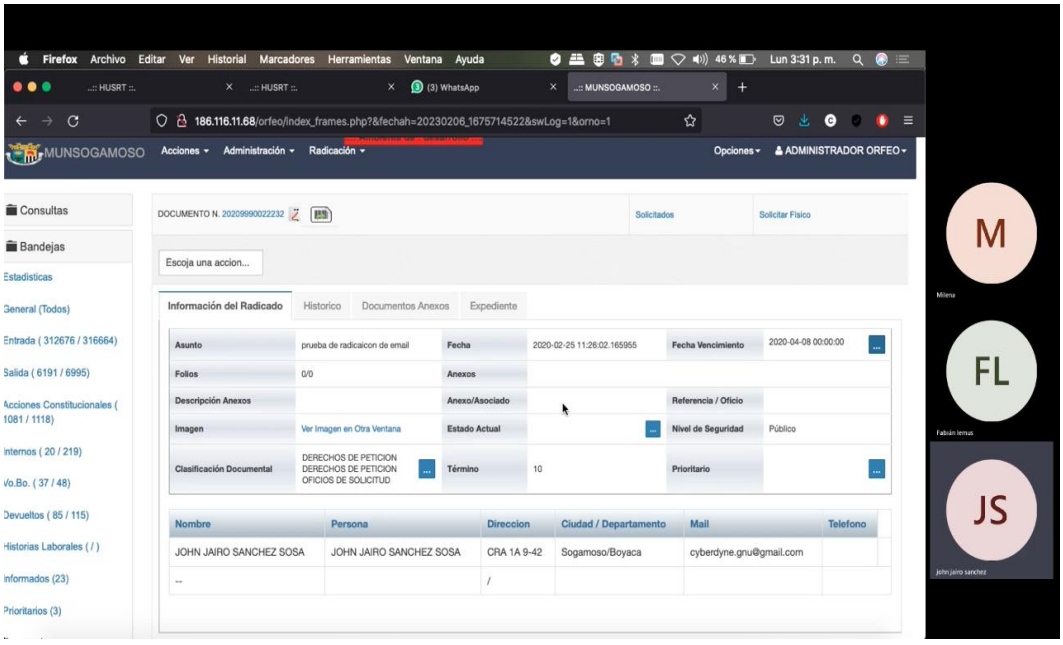


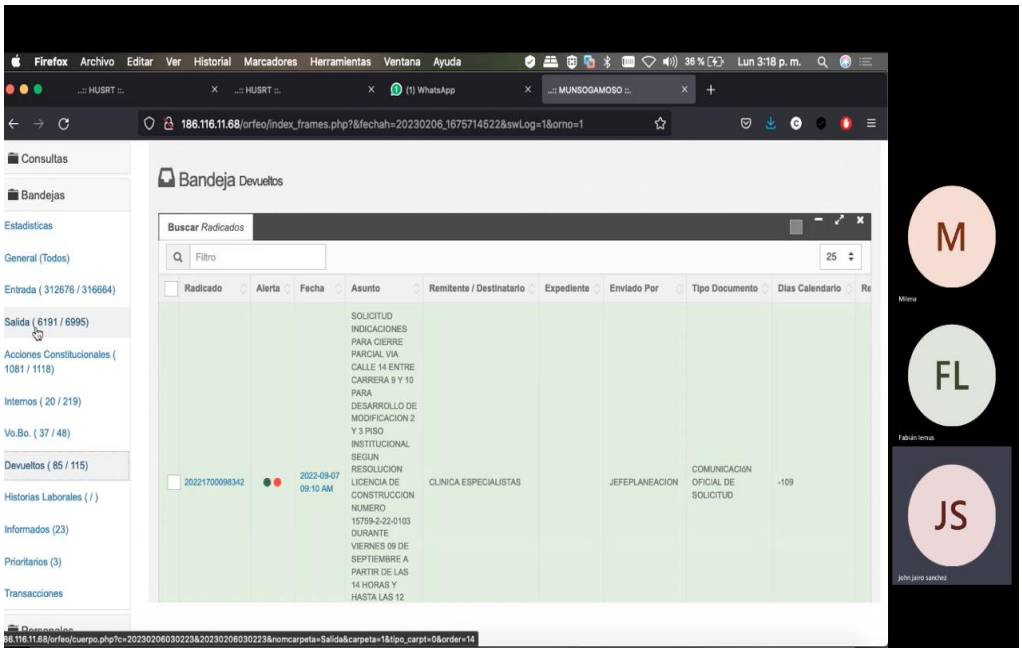


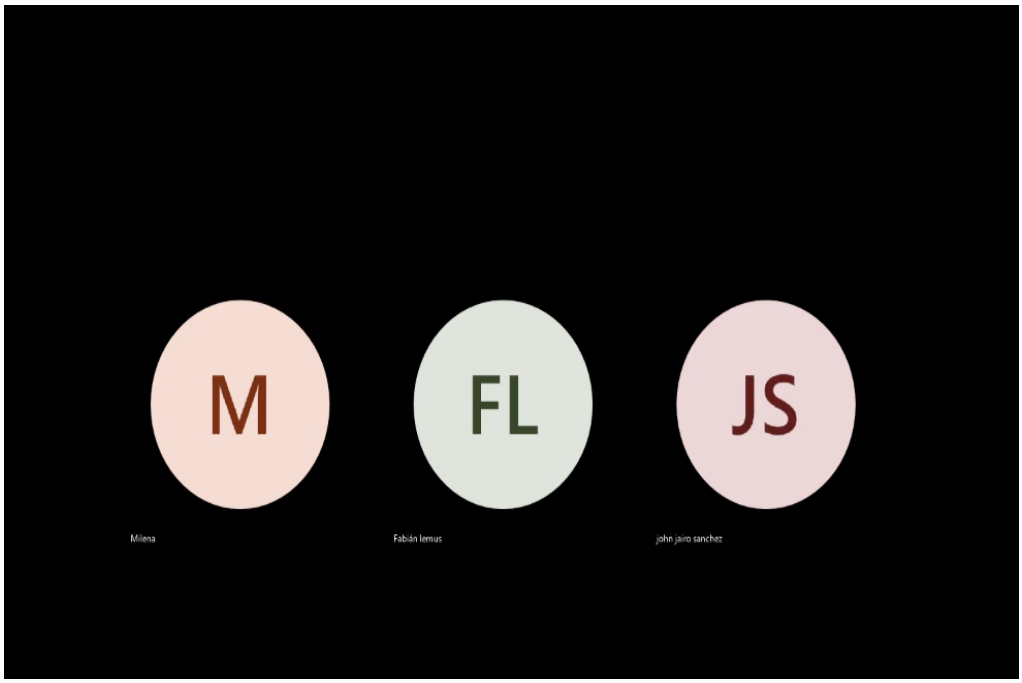
se brinda asesoría técnica para el inicio de la actualización pues sí del formulario PQRD aseguramiento con el fin de poder brindar una mejor recepción de la información en base a los índices y variables definidas en la dependencia y que son datos de evaluación ante la superintendencia de salud en cuanto a la atención de la ciudadanía.

Se brinda induccion a funcionario de atencion al usuario via microsoft teams, en cuanto al uso de la herramienta ORFEO, en miras de realizar actividades tipo administrativas, como creacion y asignacion de perfiles de usuario, activacion e inactivacion de los mismos cuando sea por retiro, respuesta rapida, clasificacion trd.






Firefox Archivo Editar Ver Historial Marcadores Herramientas Ventana Ayuda
Lun 3:18 p. m.
186.116.11.68/orfeo/index_frames.php?&fechah=20230206_1675714522&swLog=1&orno=1
Consultas
Bandejas
Estadisticas
General (Todos)
Entrada (312676 / 316664)
Salida (6191 / 6995)
Acciones Constitucionales (1081 / 1118)
Internos (20 / 219)
Vo.Bo. (37 / 48)
Devueltos (85 / 115)
Historias Laborales (/)
Informados (23)
Prioritarios (3)
Transacciones
Bandeja Devueltos
Buscar Radicados
Filtro
25
Radicado
Alerta
Fecha
Asunto
Remitente / Destinatario
Expediente
Enviado Por
Tipo Documento
Dias Calendario
20221700098342
2022-09-07 09:10 AM
SOLICITUD INDICACIONES PARA CIERRE PARCIAL VIA CALLE 14 ENTRE CARRERA 9 Y 10 PARA DESARROLLO DE MODIFICACION 2 Y 3 PISO INSTITUCIONAL SEGUN RESOLUCION LICENCIA DE CONSTRUCCION NUMERO 15759-2-22-0103 DURANTE VIERNES 09 DE SEPTIEMBRE A PARTIR DE LAS 14 HORAS Y HASTA LAS 12
CLINICA ESPECIALISTAS
JEFEPLANEACION
COMUNICACIóN OFICIAL DE SOLICITUD
-109
M
Milena
FL
Fabián lemus
JS
john jairo sanchez

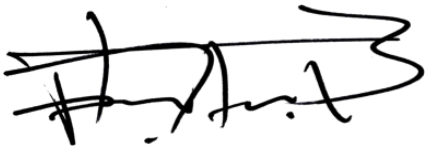

M
Milena
FL
Fabián lemus
JS
john jairo sanchez

A	B	C	D	E	F	G
1. Resumen						
Título de la reunión	Reunión con john jairo sanchez					
Participantes que asistieron	3					
Hora de inicio	2/06/23, 2:55:26 PM					
Hora de finalización	2/06/23, 4:20:24 PM					
Duración de la reunión	1 h 24 min 58s					
Tiempo medio de asistencia	1 h 12 min 37s					
2. Participantes						
Nombre	Primera entr	Última salid	Duración de	Correo electr	Id. de partici	Rol
john jairo sanchez	2/06/23, 3:0	2/06/23, 4:2	1 h 12 min 5	Johnsanchez	Johnsanchez	Organizador
Fabián lemus	2/06/23, 3:0	2/06/23, 4:2	1 h 12 min 27s			Moderador
Milena	2/06/23, 3:0	2/06/23, 4:2	1 h 12 min 26s			Moderador
3. Actividades de la reunión						
Nombre	Hora de entr	Hora de salic	Duración	Correo electr	Rol	
john jairo sanchez	2/06/23, 3:0	2/06/23, 4:2	1 h 12 min 5	Johnsanchez	Organizador	
Fabián lemus	2/06/23, 3:0	2/06/23, 4:2	1 h 12 min 27s		Moderador	
Milena	2/06/23, 3:0	2/06/23, 4:2	1 h 12 min 26s		Moderador	

Se brinda asesoria en secretaria general para la instalacion de token firma electronica del Señor Alcalde para portal de min hacienda.

Lo anterior para efectos de pago.

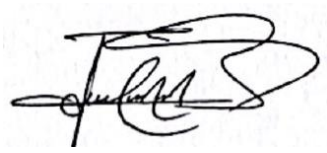
Atentamente,



_____

JOHN JAIRO SANCHEZ SOSA
Contratista

VoBo



Supervisor contrato