Sogamoso, Mayo 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 Marzo al 22 de Abril; teniendo en cuenta contrato de prestación de servicios de apoyo a la gestión número 20230294 así:

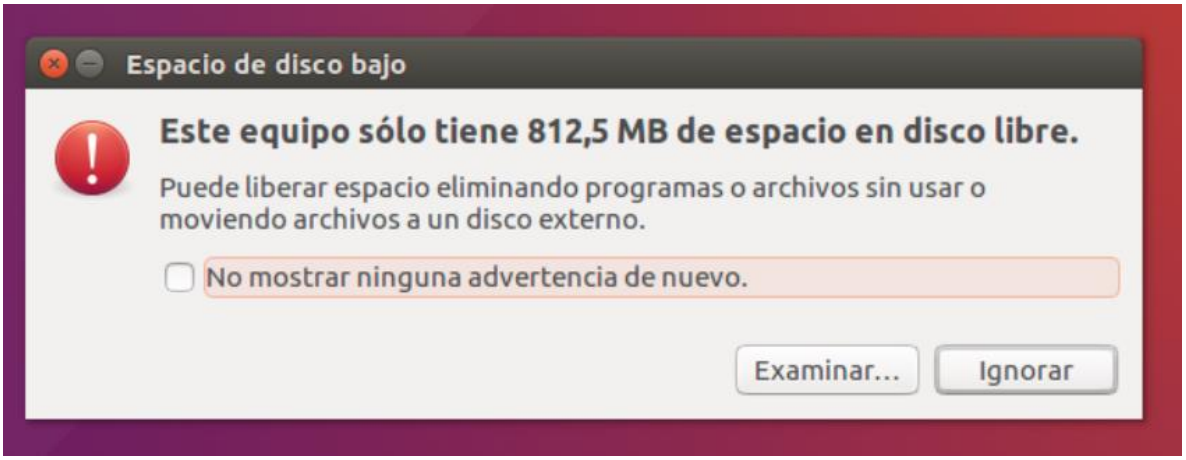
Actividad:

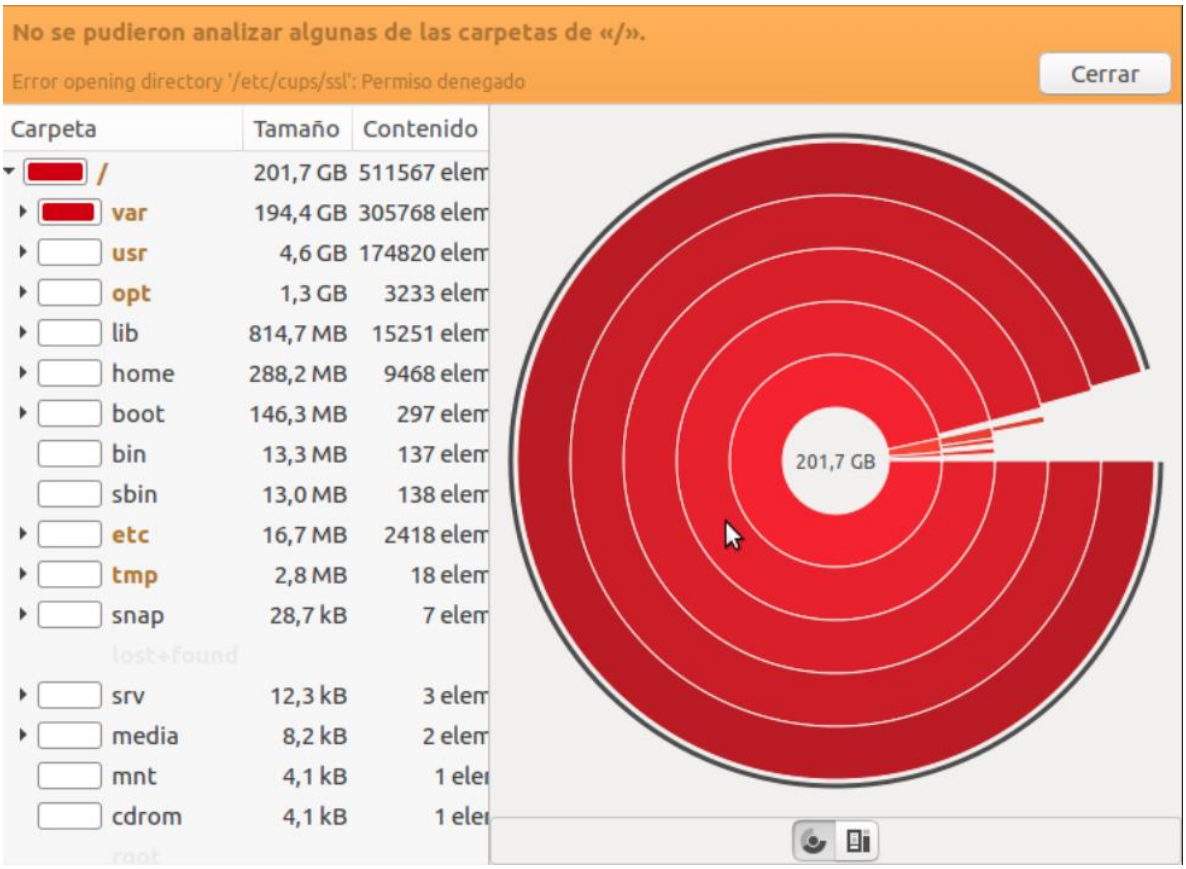
1. Apoyar el soporte técnico de la plataforma tecnológica y redes informáticas del Municipio de Sogamoso en sus diferentes dependencias.

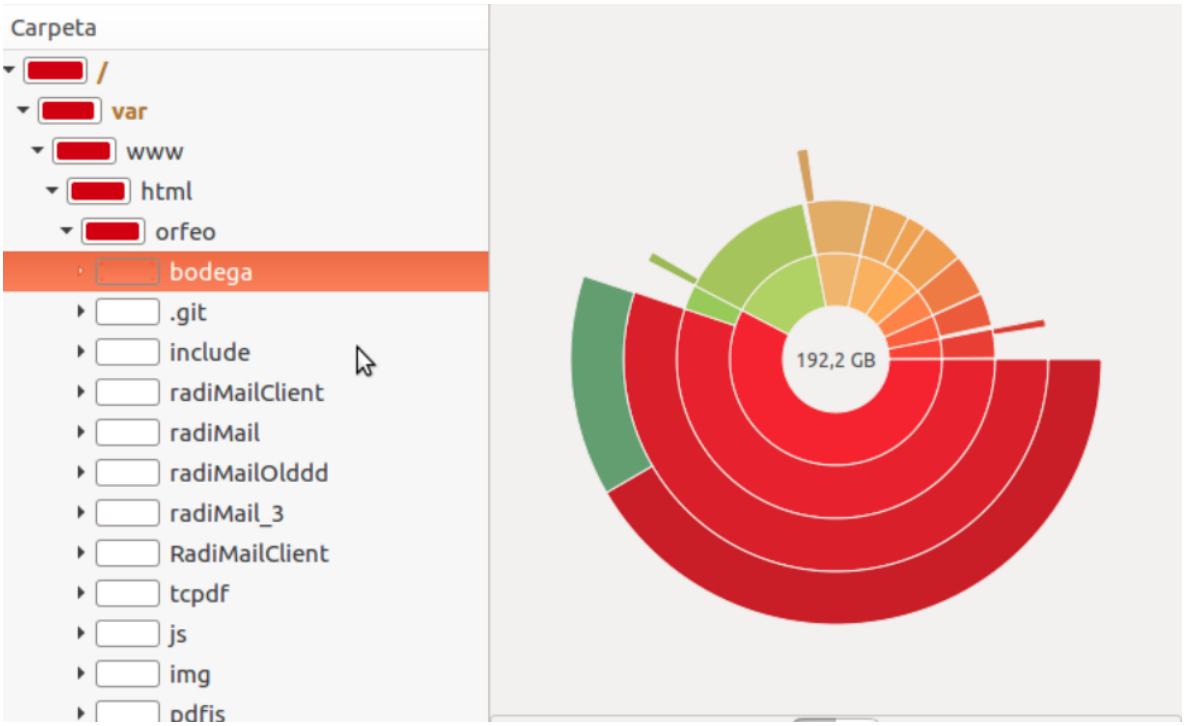
    - Se apoya al equipo tecnico de la oficina en el reseteo de la bios de un lenovo todo en uno de la oficina asesora del pespacho del alcalde.

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

    - Se libera espacio de servidor orfeo ya que no deja ingresar a diferente modulos. La razon es que el espacio en disco duro asigando a bodega de imágenes a ocupado mas del 95%




No se pudieron analizar algunas de las carpetas de «/».
Error opening directory '/etc/cups/ssl': Permiso denegado
Cerrar
Carpeta
Tamaño
Contenido
/ 201,7 GB 511567 elem
var 194,4 GB 305768 elem
usr 4,6 GB 174820 elem
opt 1,3 GB 3233 elem
lib 814,7 MB 15251 elem
home 288,2 MB 9468 elem
boot 146,3 MB 297 elem
bin 13,3 MB 137 elem
sbin 13,0 MB 138 elem
etc 16,7 MB 2418 elem
tmp 2,8 MB 18 elem
snap 28,7 kB 7 elem
lost+found
srv 12,3 kB 3 elem
media 8,2 kB 2 elem
mnt 4,1 kB 1 ele
cdrom 4,1 kB 1 ele
root
201,7 GB


Carpeta
/
var
www
html
orfeo
bodega
.git
include
radiMailClient
radiMail
radiMailOlddd
radiMail_3
RadiMailClient
tcpdf
js
img
pdfis
192,2 GB

La solucion fue eliminar archivo temporales para dar alivio de espacio, pero es una medida provisional mientras se asiga contrato de suministro para instalr un nuevo disco.

- Se brina apoyo en servidor de directorio activo para la actualizacion de fondo de pantalla con imágenes de campaña de la oficina de control interno de gestion. El cual se ejecuta comando para borrado de cache de servicios GPO y envio de orden de actualizacion a maquinas registradas en el dominio.

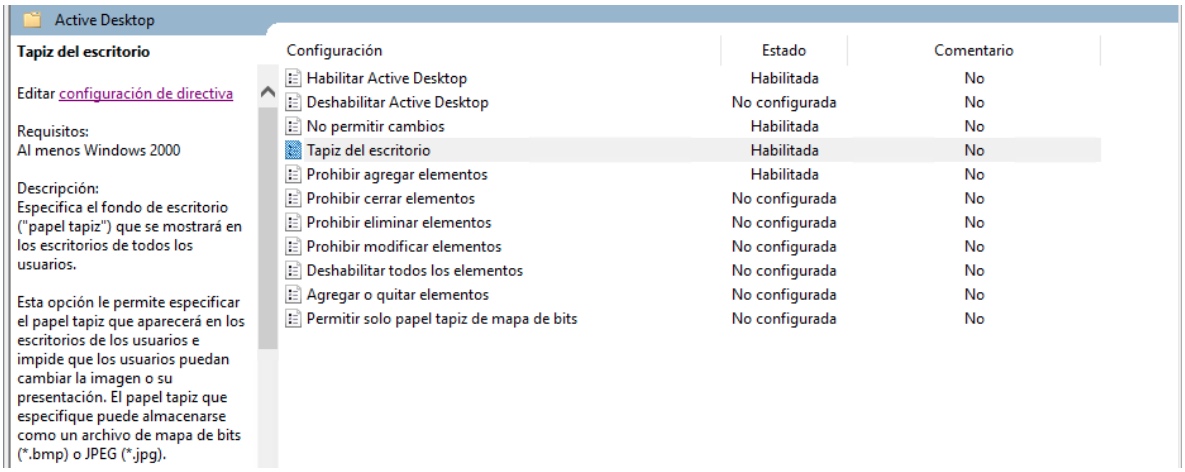



```
Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>gpupdate /force
Actualizando directiva...

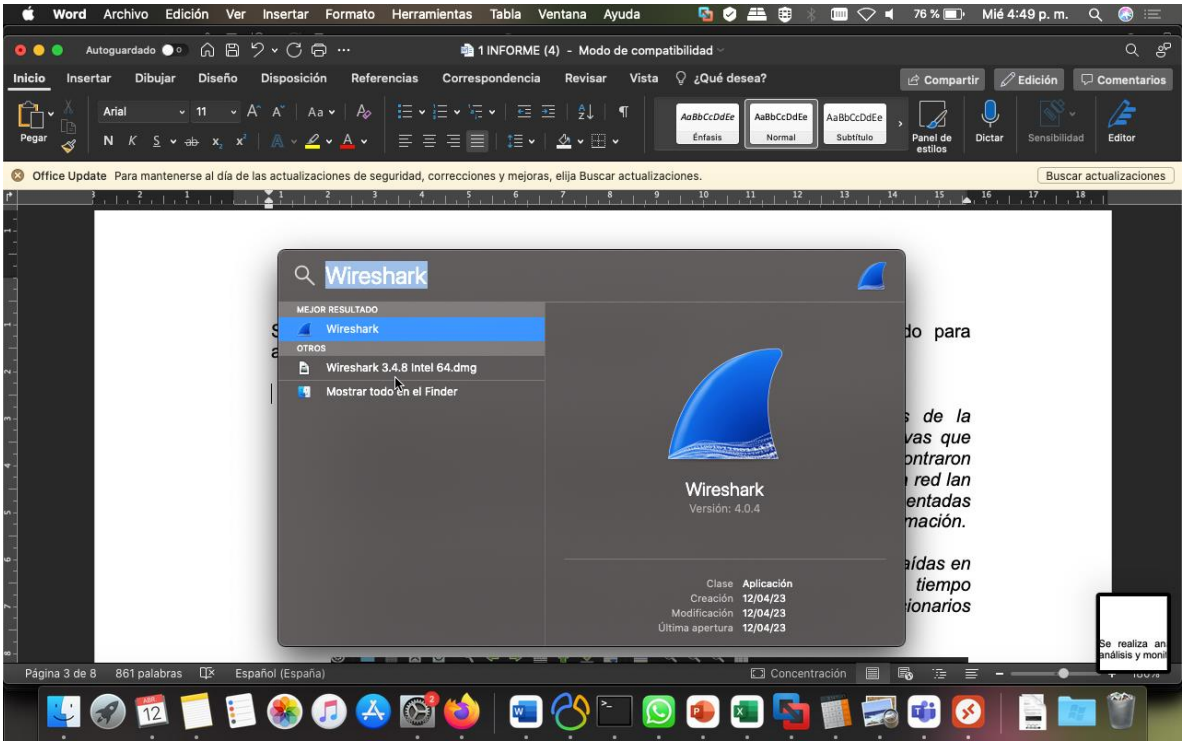
La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.

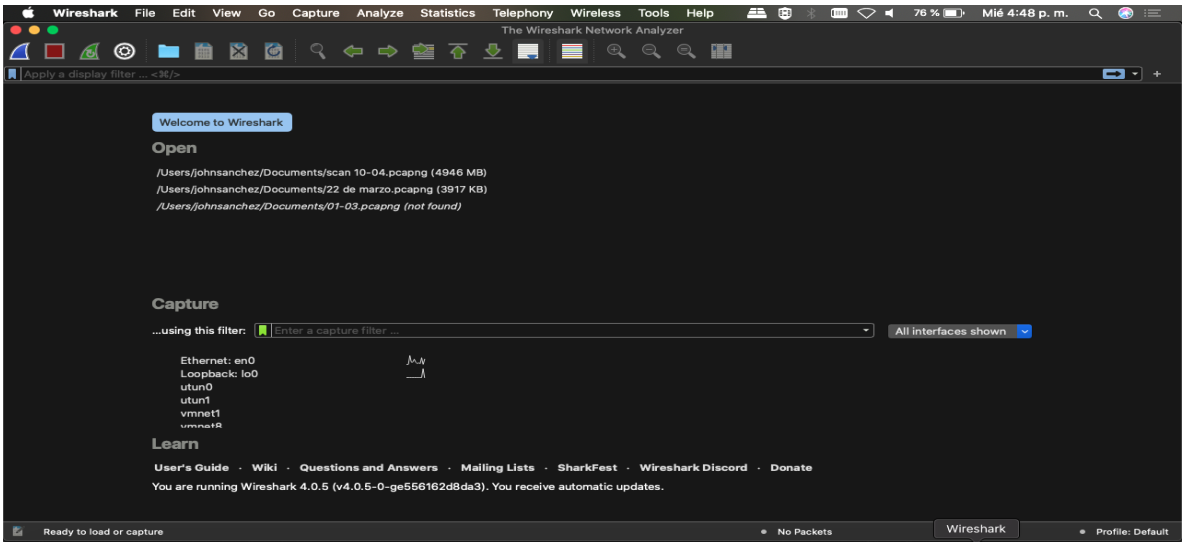

C:\Windows\system32>_
```



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.





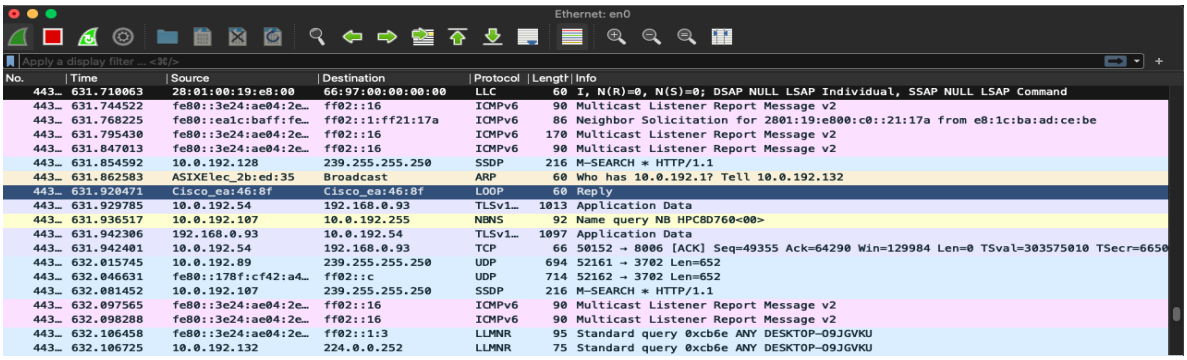
Funcionamiento de WireShark

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.

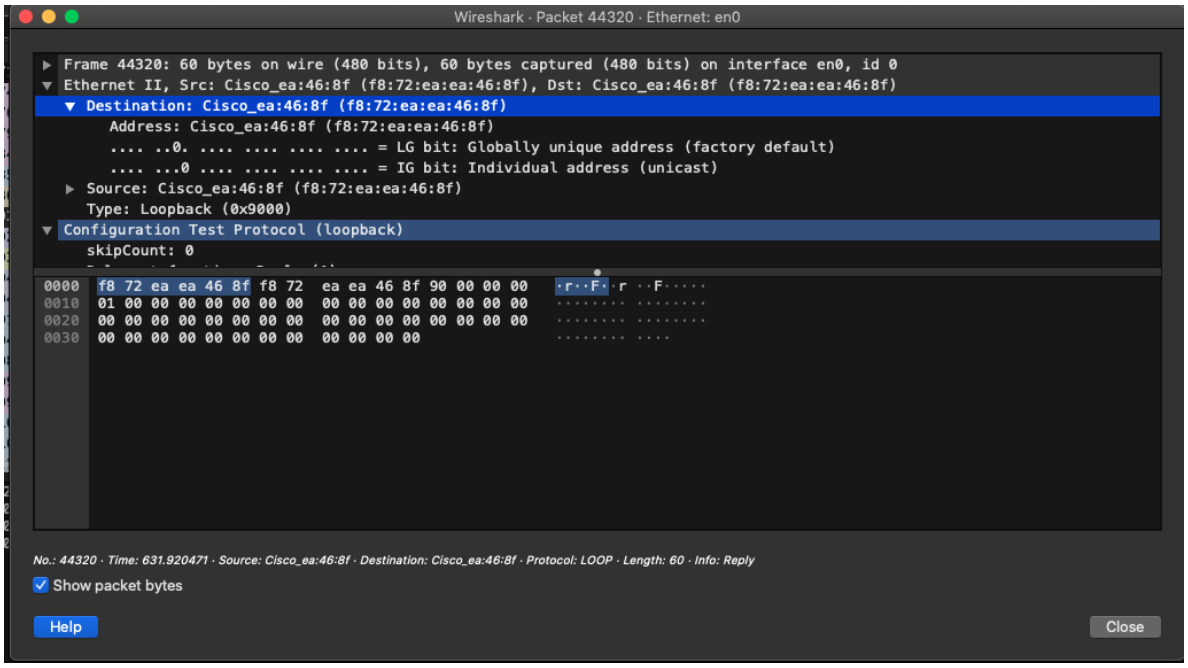
Luego de mapear la red inicia un análisis de peticiones entrada salida según protocolo y por origen de petición comparándola con un base de datos de vulnerabilidades, donde se clasifica y cualifica según el nivel si hay o no un riesgo latente de ataque o problema de red.



En esta imagen se demuestra un registro de mapeo por protocolo, se filtran según la necesidad para evaluar el paquete de datos entrada y salida, se verifica el origine y el destino de la ip para asi descartar un ataque o filtrado de información.

▶	Warning	DNS response retransmission	Protocol	mDNS
▶	Warning	D-SACK Sequence	Sequence	TCP
▶	Warning	DNS response retransmission	Protocol	DNS
▶	Warning	DNS query retransmission	Protocol	DNS
▶	Warning	Connection reset (RST)	Sequence	TCP
▶	Warning	DNS query retransmission	Protocol	mDNS
▶	Warning	DNS query retransmission	Protocol	LLMNR
▶	Note	A new tcp session is started with the same ports as an earlier s...	Sequence	TCP
▶	Note	This session reuses previously negotiated keys (Session resum...	Sequence	TLS
▶	Note	Duplicate ACK	Sequence	TCP
▶	Note	This frame is a (suspected) spurious retransmission	Sequence	TCP
▶	Note	This QUIC frame has a reused stream offset (retransmission?)	Sequence	QUIC
▶	Note	Coalesced Padding Data	Protocol	QUIC
▶	Note	This frame is a (suspected) retransmission	Sequence	TCP
▶	Note	Padding identification may be inaccurate and impact trailer diss...	Protocol	Ethertype
▶	Note	ACK to a TCP keep-alive segment	Sequence	TCP
▶	Note	TCP keep-alive segment	Sequence	TCP
▶	Note	This frame undergoes the connection closing	Sequence	TCP
▶	Note	This frame initiates the connection closing	Sequence	TCP
▶	Note	Time To Live	Sequence	IPv4
▶	Chat	Formatted text	Sequence	HTTP
▶	Chat	Connection finish (FIN)	Sequence	TCP
▶	Chat	TCP window update	Sequence	TCP
▶	Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP
▶	Chat	Connection establish request (SYN)	Sequence	TCP
▶	Chat	Formatted text	Sequence	SSDP

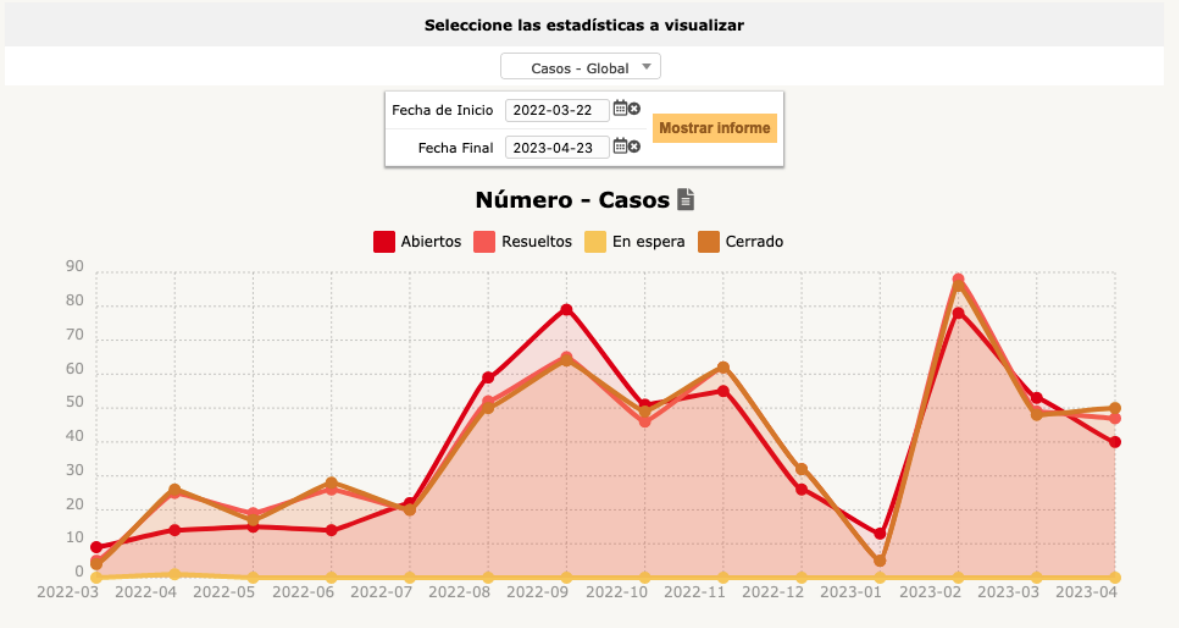
En esta imagen compila los datos analizados por niveles de criticidad, se revisan los de nivel warning que reflejarían interés pero al mirar los paquetes son paginas secundarias o apis de otras subpágina que no resuelven el DNS por ejemplo u otros paquetes refleja un reinicio de sesión pero por la misma causa de DNS no resuelto.



- Se brindo apoyo para rastreo de consumo de ancho de banda por servicio detectado por ISP en la red WAN del municipio. Se reviso la plataforma FORTINET y se escala a funcionario a cargo de análisis del sistema perimetral de seguridad.

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.

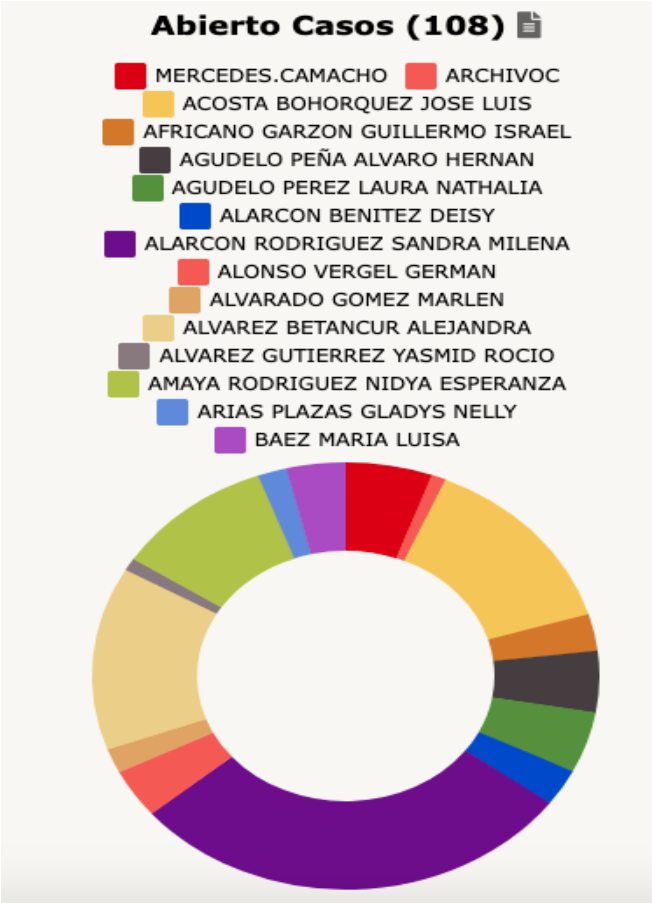
Las condiciones técnicas del aplicativo y el servidor son óptimas. Se hizo revisión previa a los casos que han sido incluidos en este nuevo periodo y se evidencia la creación de 108 casos en la administración y de esos 107 de manera oportuna se han tramitado y cerrado 107 casos mostrando una efcitividad en el servicio del 99.04% para el periodo comprendido de este informe.

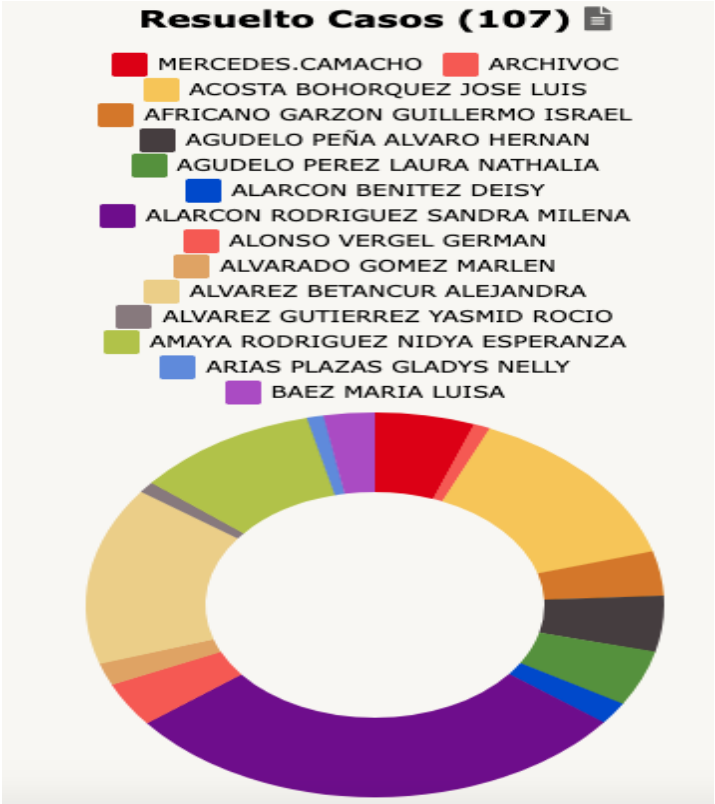


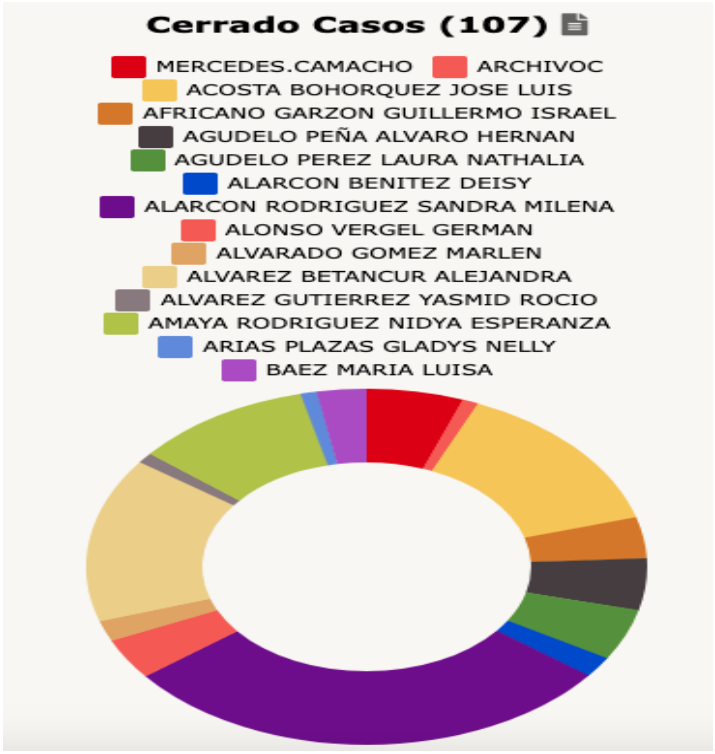
Esta grafica represente el numero de casos creados en sistema realizando una comprativa de estado de solicitudes.



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


Abierto Casos (108)
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
BAEZ MARIA LUISA


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
BAEZ MARIA LUISA

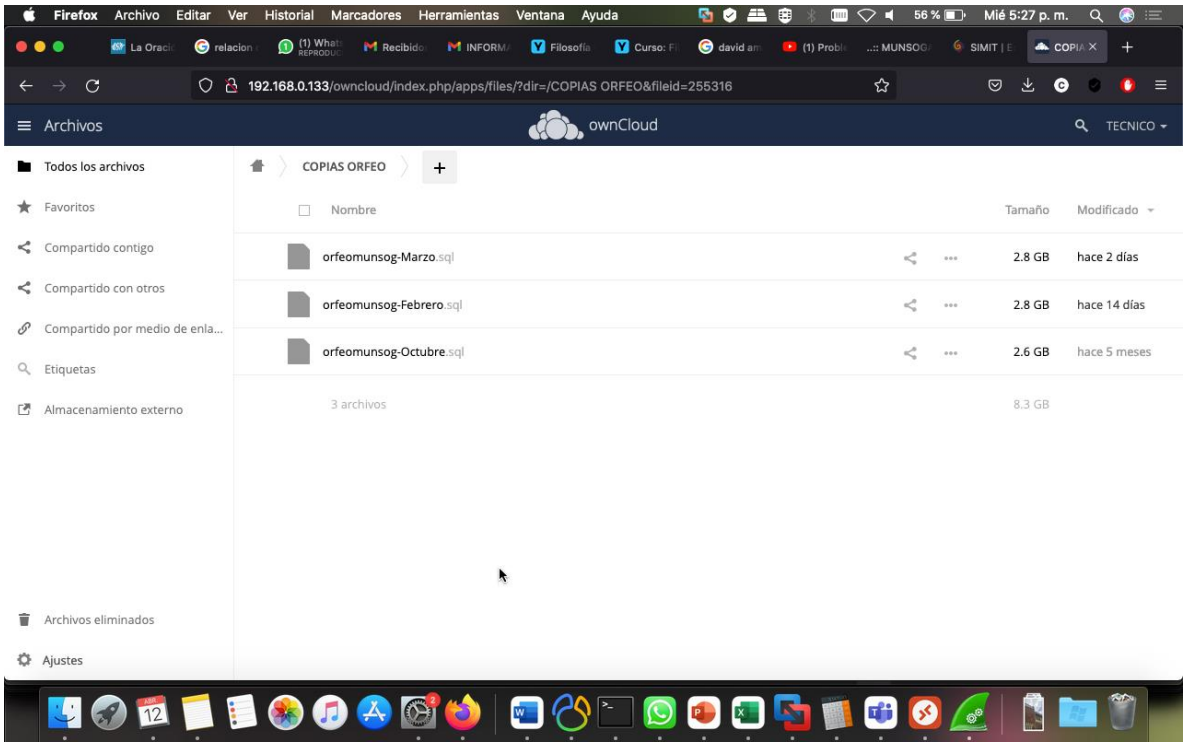

Cerrado Casos (107)
MERCEDES.CAMACHO
ARCHIVOC
ACOSTA BOHORQUEZ JOSE LUIS
AFRICANO GARZON GUILLERMO ISRAEL
AGUDELO PEÑA ALVARO HERNAN
AGUDELO PEREZ LAURA NATHALIA
ALARCON BENITEZ DEISY
ALARCON RODRIGUEZ SANDRA MILENA
ALONSO VERGEL GERMAN
ALVARADO GOMEZ MARLEN
ALVAREZ BETANCUR ALEJANDRA
ALVAREZ GUTIERREZ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

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 instructivo de uso de la herramienta JAWS para ser compartido en la oficina de atención al usuario. Para posterior hacer capacitación en sitio.

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 brinda asesoria en robotica a estudiantes y docente con proyecto de robot con el cual se presentaron en la ciudad de tunja. Se escucha el objetivo principal del priyecto y las tareas que tiene que realizar. Se le hace sugerencia al docente de enmarcar el campo de accion del robot que fuese menos que el rango de los sensores. Al igual se les suguirio ideas para mejora del proyecto.





Se revisaron 8 camaras de la plaza de mercado en donde vuelve a fallar switch que habia sido reemplazado el año anterior. El motivo actual fue la filtracion de agua a la caja de inspecicon haciendo corto electrico. Se elaboro informe tecnico de la situacion de las camaras, el cual fue enviado por correo.


11/04/2023 16:36

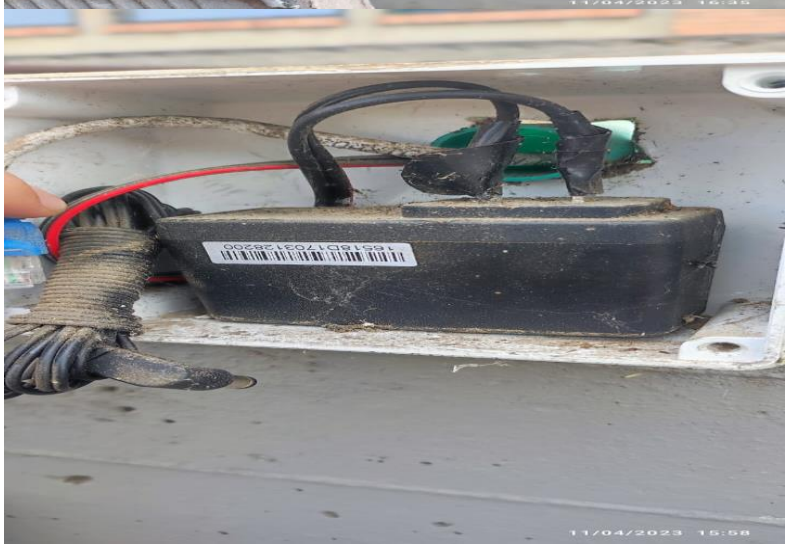

11/04/2023 16:35


11/04/2023 15:55


11/04/2023 15:55

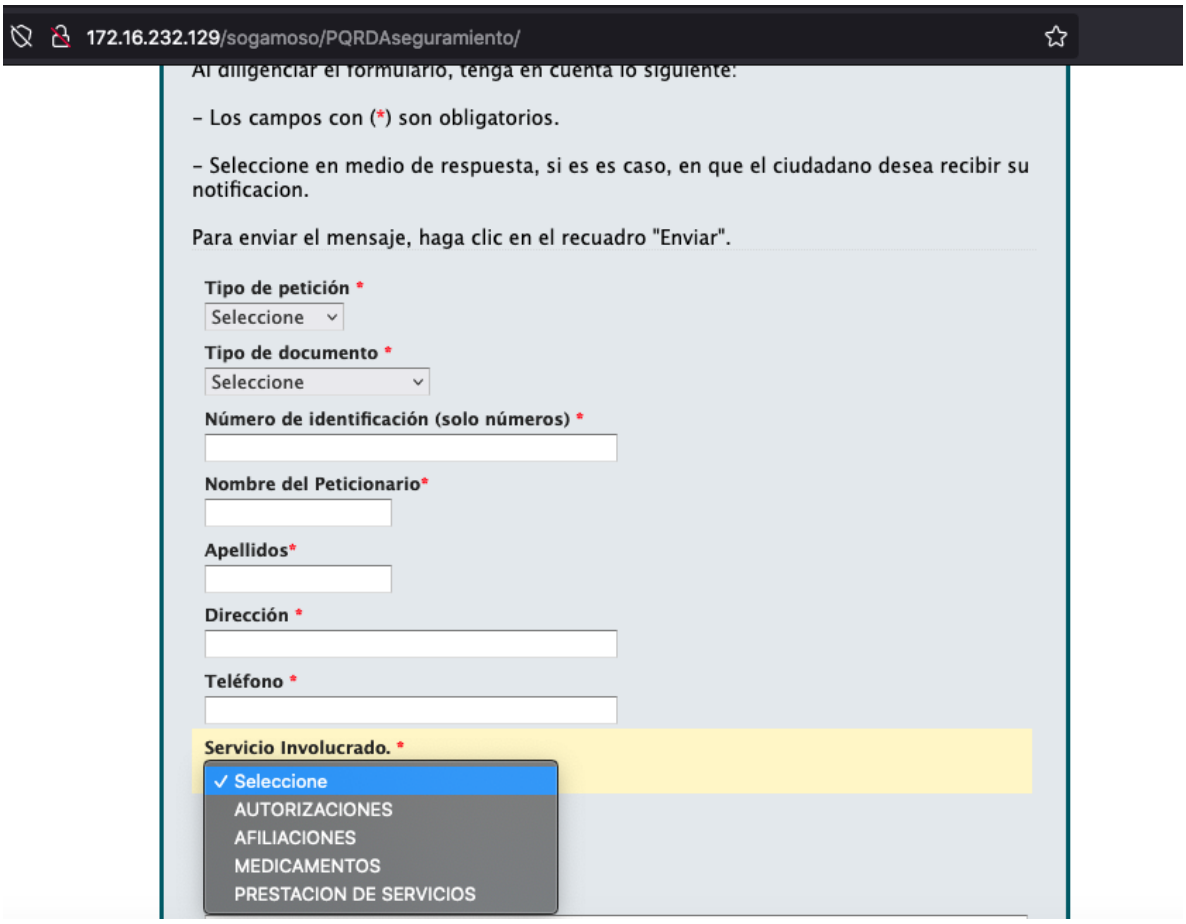


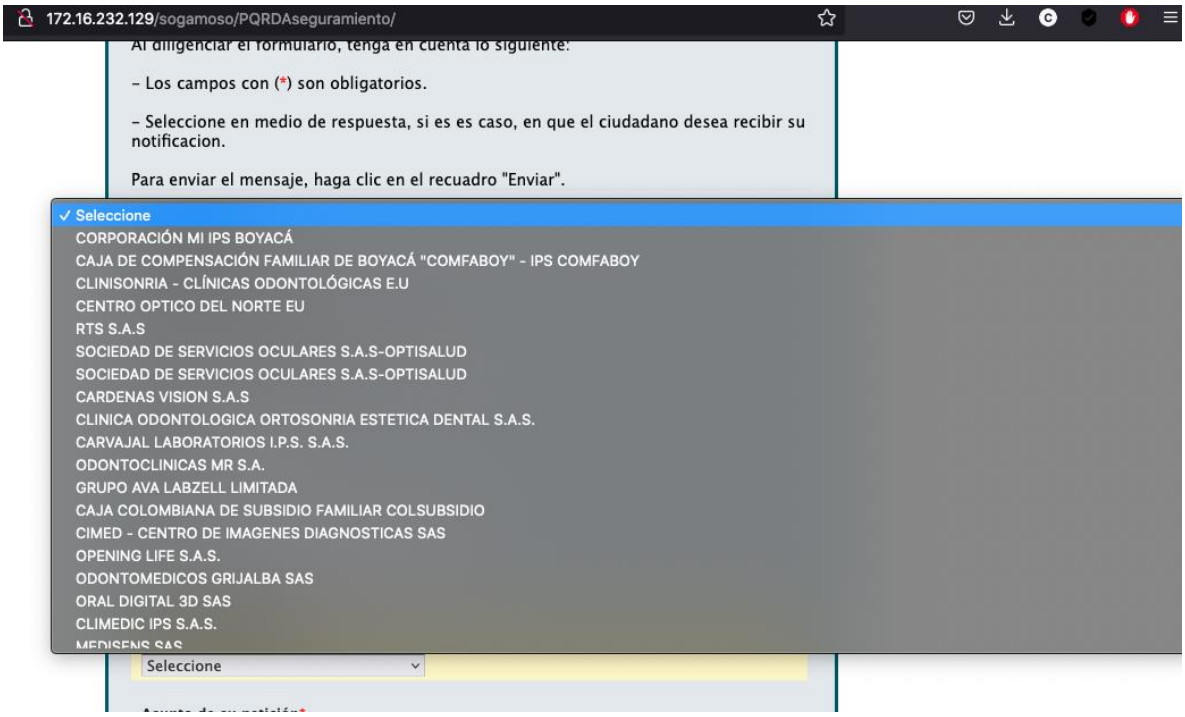




- se brinda asesoría técnica para el inicio de la actualización pues sí del formulario PQRD aseguramiento con el fin de poder brindar una mejor

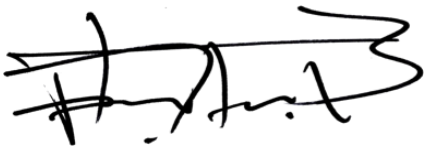
recepción de la información en base a los índices y variables definidas en la dependencia y que son datos de evaluación ante la superintendencia de salud en cuanto a la atención de la ciudadanía.





Lo anterior para efectos de pago.

Atentamente,



_____

JOHN JAIRO SANCHEZ SOSA
Contratista

VoBo



Supervisor contrato