Sogamoso, Noviembre de 2023

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

Asunto: Presentación de informe N°9 contrato 20230294

Respetado Ingeniero:

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

Actividad:

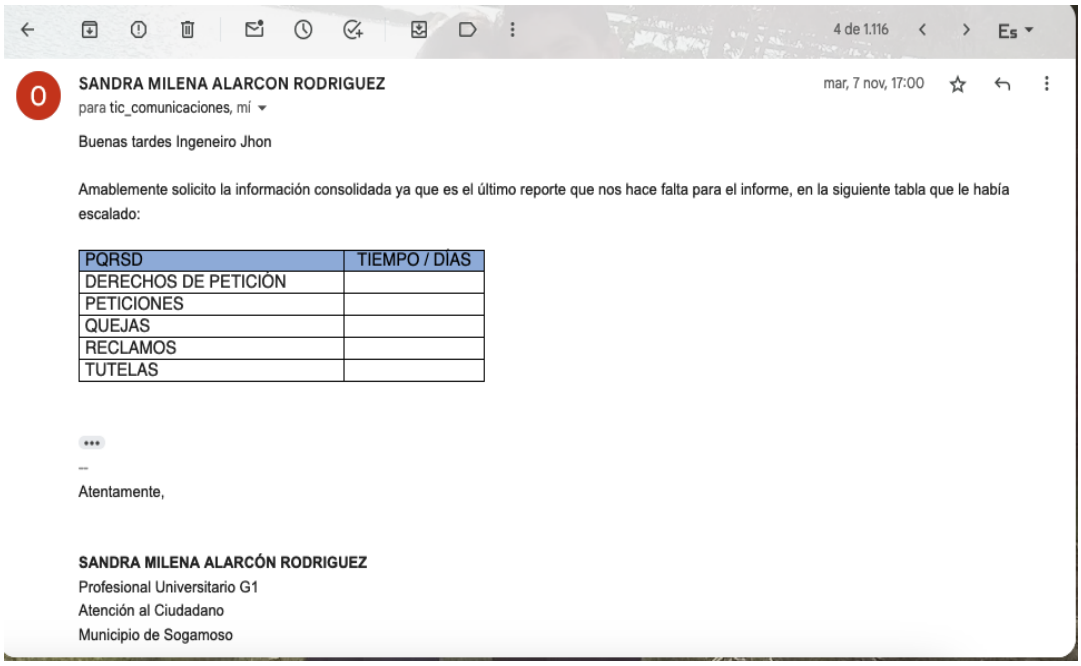
1. **Apoyar el soporte técnico de la plataforma tecnológica y redes informáticas del Municipio de Sogamoso en sus diferentes dependencias.**

   Se apoya la administración de la plataforma Orfeo. En el periodo en mención se realizaron las siguientes tareas.

   Se activa el usuario KARENLOPEZ, por reintegro de vacaciones y se requiere para asignación de oficios. Ingresando por el módulo administrativo del sistema y se hace la modificación respectiva.



   Se apoya en la elaboración de los reportes necesarios para el informe trimestral de PQRD realizado por la líder de la oficina de atención al usuario. El cual se sustenta ante la oficina de control interno de gestión y publicado en la página web de la alcaldía. Se realizan consultas directas la base de datos según los requisitos exigidos por anticorrupción y se exporta a archivos Excel para que sean analizados.



4 de 1.116

SANDRA MILENA ALARCON RODRIGUEZ mar, 7 nov, 17:00

para tic_comunicaciones, mí

Buenas tardes Ingeneiro Jhon

Amablemente solicito la información consolidada ya que es el último reporte que nos hace falta para el informe, en la siguiente tabla que le había escalado:

PQRSD	TIEMPO / DÍAS
DERECHOS DE PETICIÓN	
PETICIONES	
QUEJAS	
RECLAMOS	
TUTELAS	

--

Atentamente,

SANDRA MILENA ALARCÓN RODRIGUEZ
Profesional Universitario G1
Atención al Ciudadano
Municipio de Sogamoso



eJOHN SANCHEZ <jsanchez.alcsogamoso@gmail.com> mar, 7 nov, 19:21

para SANDRA, tic_comunicaciones

Buenas noches

Se adjunta tabla con datos de referencia.

PQRDS	TIEMPO / DIAS
DERECHOS DE PETICIÓN	13
PETICIONES	12
QUEJAS	11
RECLAMOS	50
TUTELAS	3

1 archivo adjunto • Analizado por Gmail

nuevo reporte.xlsx



4 de 1.116 Es

eJOHN SANCHEZ <jsanchez.alcsogamoso@gmail.com>
para Orfeo

mar, 7 nov, 10:40

Buen dia

envio reporte que genera bd orfeo para acciones constitucionanales

--
ate

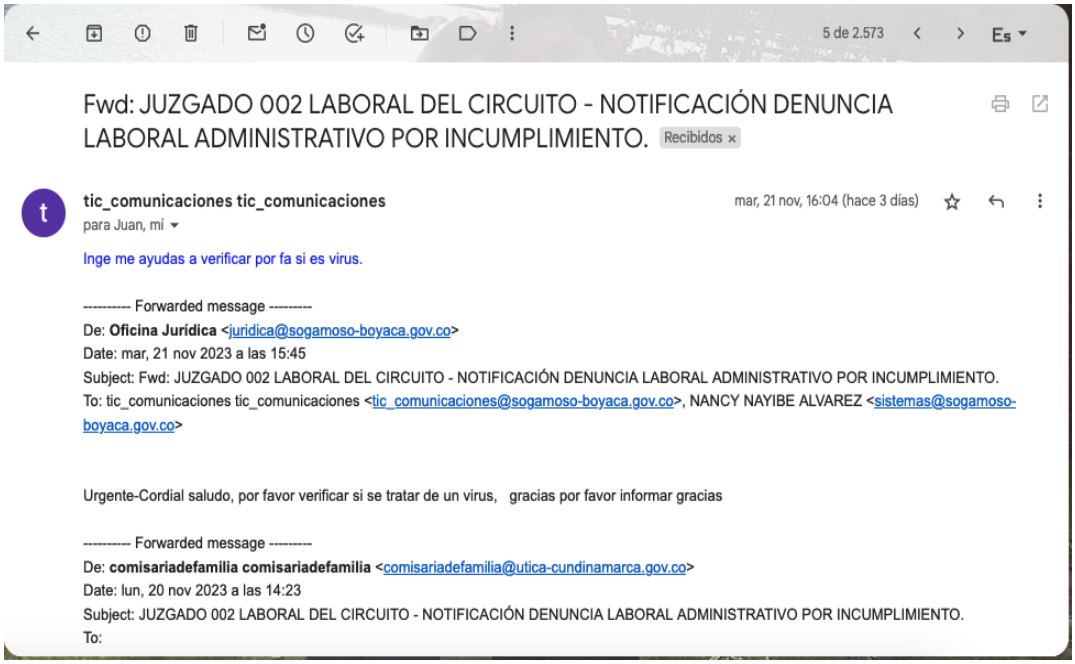
JOHN JAIRO SANCHEZ SOSA

MUNICIPIO DE SOGAMOSO
OFICNA DE TICS Y COMUNICACIONES
Plaza 6 de septiembre Edificio Administrativo.
PBX: Tel.7702040 extensión 125
www.sogamoso-boyaca.gov.co
"SOGAMOSO, Tarea de Todos"

"El presente en virtud de la Ley 527 del 18 de agosto de 1999 y la Ley 962 del 8 de julio de 2005, las cuales establecen que la información tramitada por este medio tiene plena validez y es objeto de plena prueba."

AVISO LEGAL: éste correo electrónico contiene información confidencial del Municipio de Sogamoso. usted no es el destinatario, le informamos que no podrá usar, retener, imprimir, copiar, distribuir o hacer público contenido, de hacerlo podria tener consecuencias legales como las contenidas en la Ley 1273 del 5 de enero de 2009 y todas la que le apliquen. Si ha recibido éste correo por error, por favor notifique al remitente y bórrelo. Si usted es el destinatario, le solicitamos mantener reserva sobre el contenido, los datos o información de contacto del remitente y en general sobre la información de éste documento y/o archivos adjuntos, a no ser que exista una autorización explícita.

Se solicita desde las dependencias Jurídica y Despacho del señor alcalde el análisis de dos correos electrónicos sospechosos de virus.



5 de 2.573 Es

Fwd: JUZGADO 002 LABORAL DEL CIRCUITO - NOTIFICACIÓN DENUNCIA LABORAL ADMINISTRATIVO POR INCUMPLIMIENTO. Recibidos ×

tic_comunicaciones tic_comunicaciones
para Juan, mí

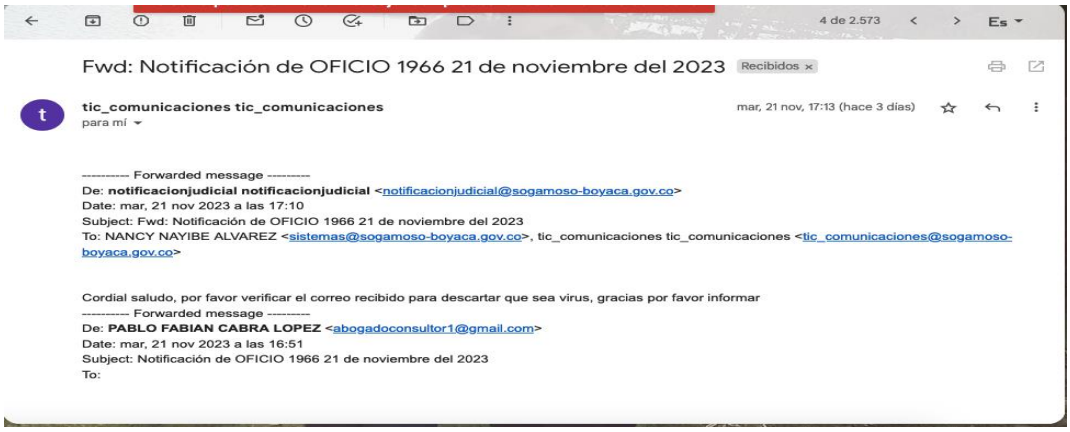
mar, 21 nov, 16:04 (hace 3 días)

Inge me ayudas a verificar por fa si es virus.

--------- Forwarded message ---------
De: **Oficina Jurídica** <juridica@sogamoso-boyaca.gov.co>
Date: mar, 21 nov 2023 a las 15:45
Subject: Fwd: JUZGADO 002 LABORAL DEL CIRCUITO - NOTIFICACIÓN DENUNCIA LABORAL ADMINISTRATIVO POR INCUMPLIMIENTO.
To: tic_comunicaciones tic_comunicaciones <tic_comunicaciones@sogamoso-boyaca.gov.co>, NANCY NAYIBE ALVAREZ <sistemas@sogamoso-boyaca.gov.co>

Urgente-Cordial saludo, por favor verificar si se tratar de un virus, gracias por favor informar gracias

--------- Forwarded message ---------
De: **comisariadefamilia comisariadefamilia** <comisariadefamilia@utica-cundinamarca.gov.co>
Date: lun, 20 nov 2023 a las 14:23
Subject: JUZGADO 002 LABORAL DEL CIRCUITO - NOTIFICACIÓN DENUNCIA LABORAL ADMINISTRATIVO POR INCUMPLIMIENTO.
To:



4 de 2.573 Es

Fwd: Notificación de OFICIO 1966 21 de noviembre del 2023 Recibidos ×

tic_comunicaciones tic_comunicaciones mar, 21 nov, 17:13 (hace 3 días)
para mí

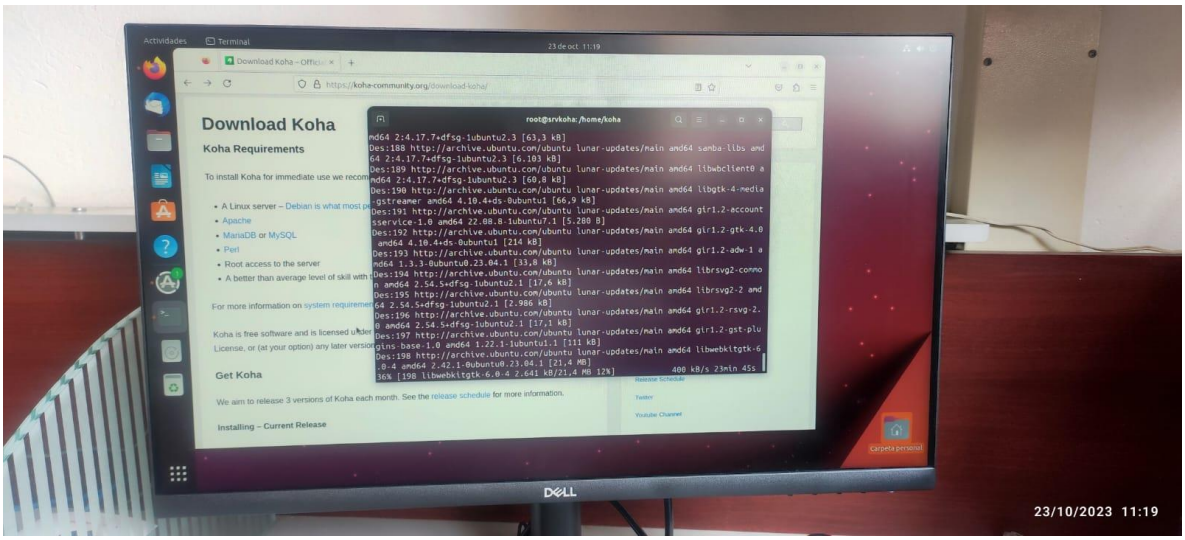
---------- Forwarded message ---------
De: **notificacionjudicial notificacionjudicial** <notificacionjudicial@sogamoso-boyaca.gov.co>
Date: mar, 21 nov 2023 a las 17:10
Subject: Fwd: Notificación de OFICIO 1966 21 de noviembre del 2023
To: NANCY NAYIBE ALVAREZ <sistemas@sogamoso-boyaca.gov.co>, tic_comunicaciones tic_comunicaciones <tic_comunicaciones@sogamoso-boyaca.gov.co>

Cordial saludo, por favor verificar el correo recibido para descartar que sea virus, gracias por favor informar
---------- Forwarded message ---------
De: **PABLO FABIAN CABRA LOPEZ** <abogadoconsultor1@gmail.com>
Date: mar, 21 nov 2023 a las 16:51
Subject: Notificación de OFICIO 1966 21 de noviembre del 2023
To:

Se analizaron aspectos importantes de los metadatos del correo como el origen y contenido de texto para validar disconcordancias que son evidentes como el dominio de correo.

Se hace acompañamiento tecnico a la biblioteca municipal, donde se instala servidor dell con procposito de KOHA (software de gestion de bibliotecas) los cuales se implementa ubuntu server 23-04 lts con tinterfaz grafica GNOME con fines de aministracion. Según el instructivo enviado se instala el software koha con base de datos mysql-server y se deja ahasta este punto en configuracion ya que según los acuerdos con bibliotecas nacionales ellos se encargan de implemetar el resto de los componentes.




Actividades
Terminal
23 de oct 11:19
Download Koha – Offic
https://koha-community.org/download-koha/
Download Koha
Koha Requirements
root@srvkoha: /home/koha
Get Koha
Installing – Current Release
Carpeta personal
DELL
23/10/2023 11:19

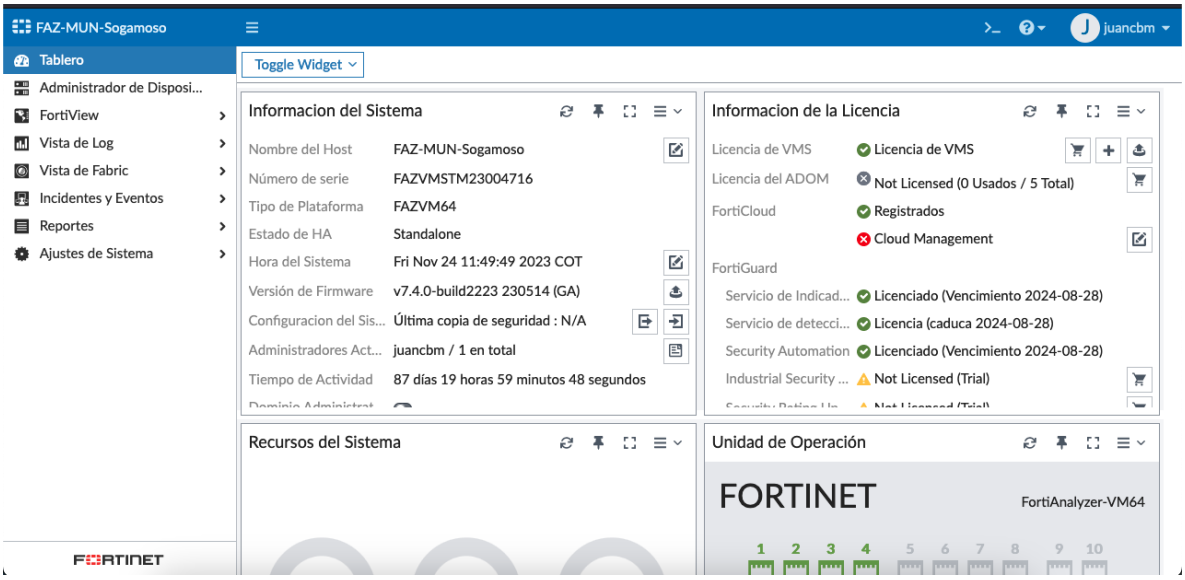

Download Koha
Koha Requirements
DELL
23/10/2023 11:19

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.**

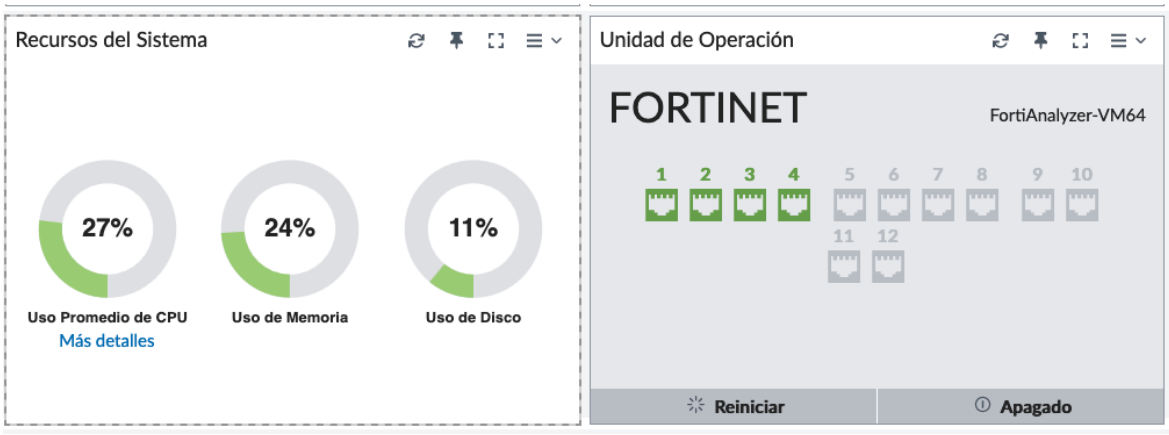
Para este periodo se recibe capacitación por parte de Fortinet en uso y apropiación de la herramienta fortianalyzer, el cual recopila y analiza los logs que se generan en los cuatros Fortinet que tiene la administración municipal (torre 6, pintor, edificio rojas y sec educación), este análisis es clasificado en módulos de seguridad que reportan que casos de atraque o intento de ingreso no autorizado ya sea por hacker u virus.

Estos reportes deben ser analizados constantemente ya que parten desde los mismos logs y de forma manual, para aquellos que no se han podido resolver, se ingresa al Fortinet para realizar acciones respectivas como creación de políticas o limitaciones de acceso.

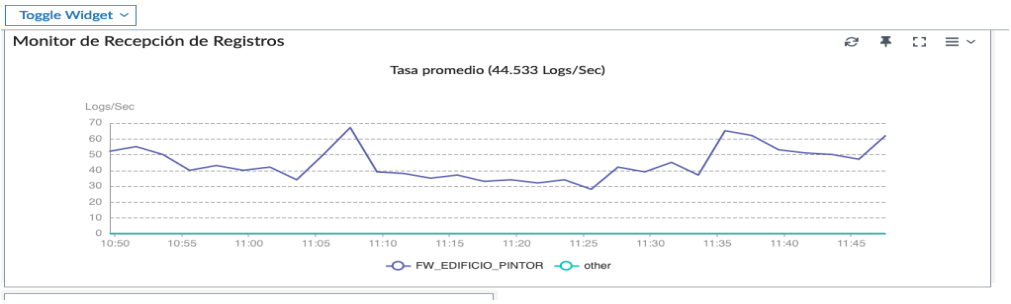
Para este período se Empieza con la revisión constante del estado funcional del forti analyzer se evidencia de que se están recibiendo los logs que son el insumo para el análisis de los riesgos eventos e incidentes. Se evidencia que operacionalmente esta bien en las licencias y recepcion de los logs.



La tasa de uso en disco se encuentra optima y los puerto de conexión al analyzer están activos y contra tiempos.



Los logs más altos que ha recepcionado fortianlyzer provienen del edificio el pintor.

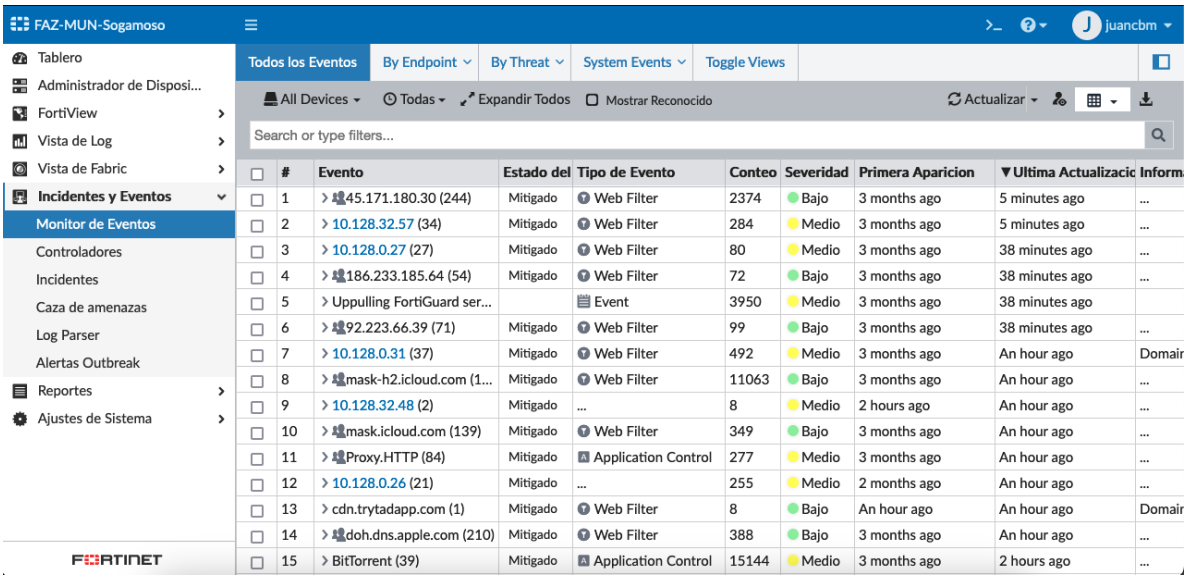


Pero al revisar los servicios activos se encuentran que dos no lo están esto afecta la recepción de los logs y la gestión que hace el fortianalyzer. Las causas son desconocidas, pero se solicitara apoyo a Fortinet par resolución del tema

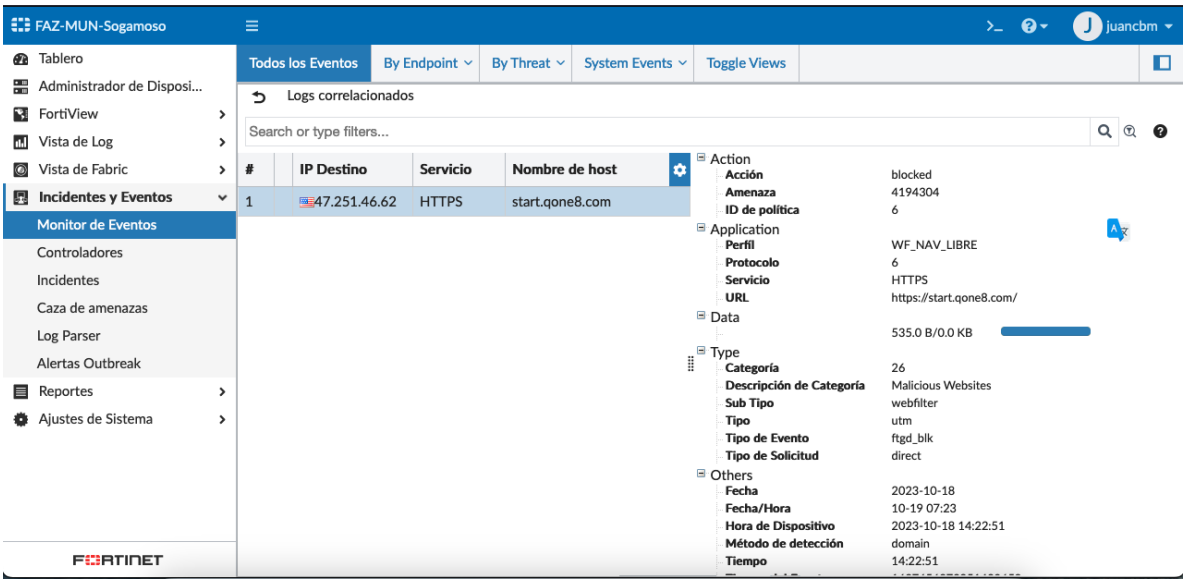
Nombre del Dispositivo	Dirección IP	Plataforma	Estado de HA	Descripci
FW_EDIFICIO_PINTOR	10.128.192.1	FortiGate-80F		
FW_EDIFICIO_ROJAS	10.144.0.1	FortiGate-40F		
FW_EDUCACION	10.64.192.1	FortiGate-80F		
FW_TORRE6	10.0.128.1	FortiGate-400E		Fw_Torre6_M

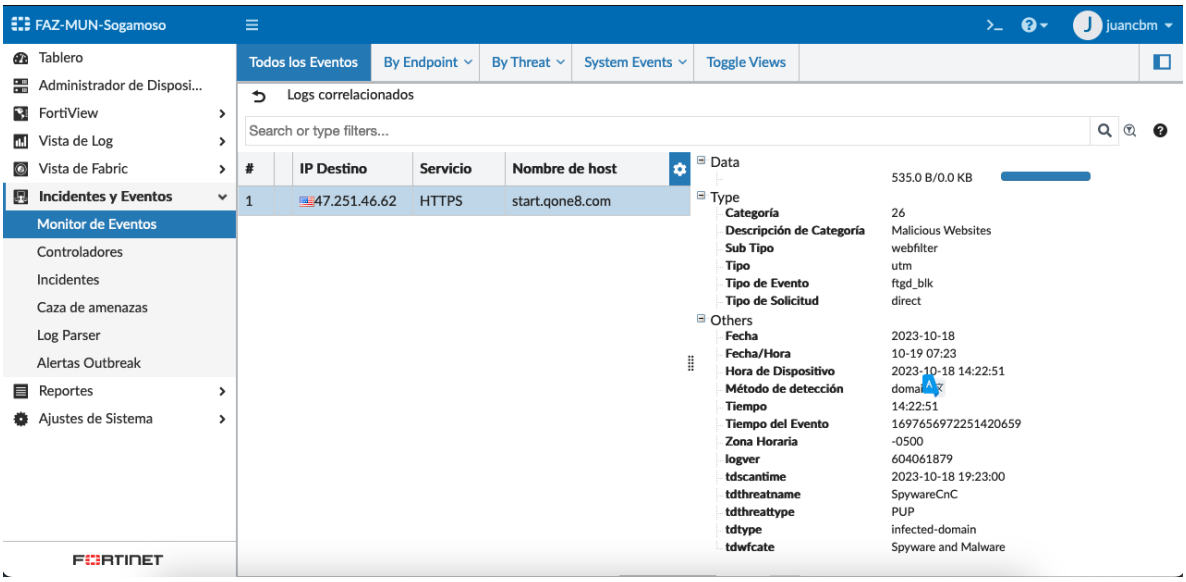
Nombre del Dispositivo	Conectividad	Modo de registro
FW_EDIFICIO_PINTOR	8 Conexion Activa	Tiempo real
FW_EDIFICIO_ROJAS	8 Conexion Activa	Tiempo real
FW_EDUCACION	4 Conexion Inactiva	Tiempo real
FW_TORRE6	1 Conexion Inactiva	Tiempo real

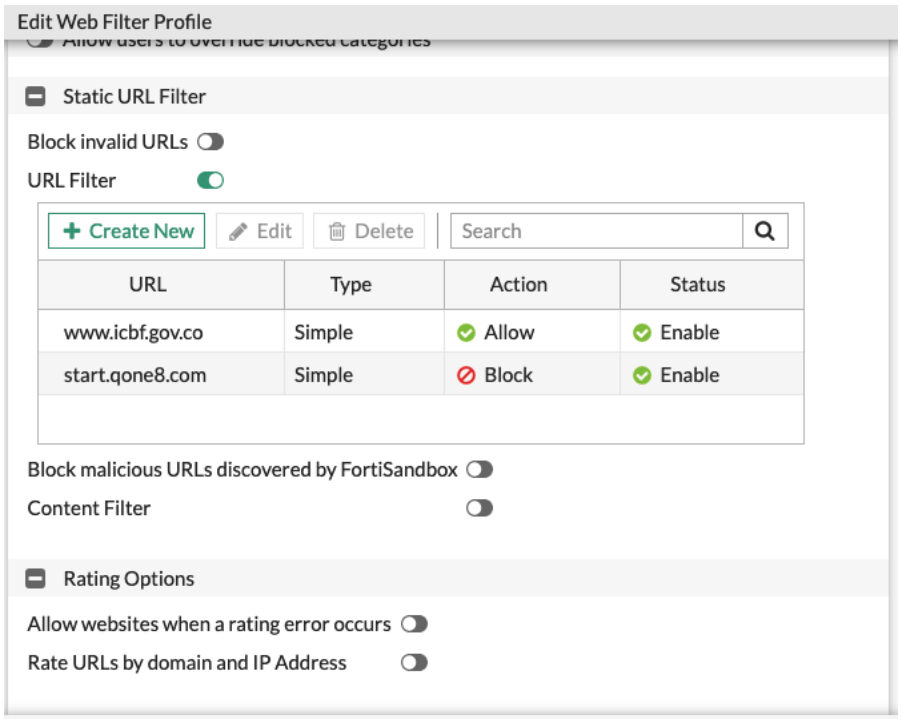
En cuanto a las incidencias se analizan los logs reportados de los otros dos y se encuentran solo dos casos de prioridad alta del edificio el pintor. El primer caso corresponde al acceso a una página que está catalogado por Fortinet de alto riesgo de spam.



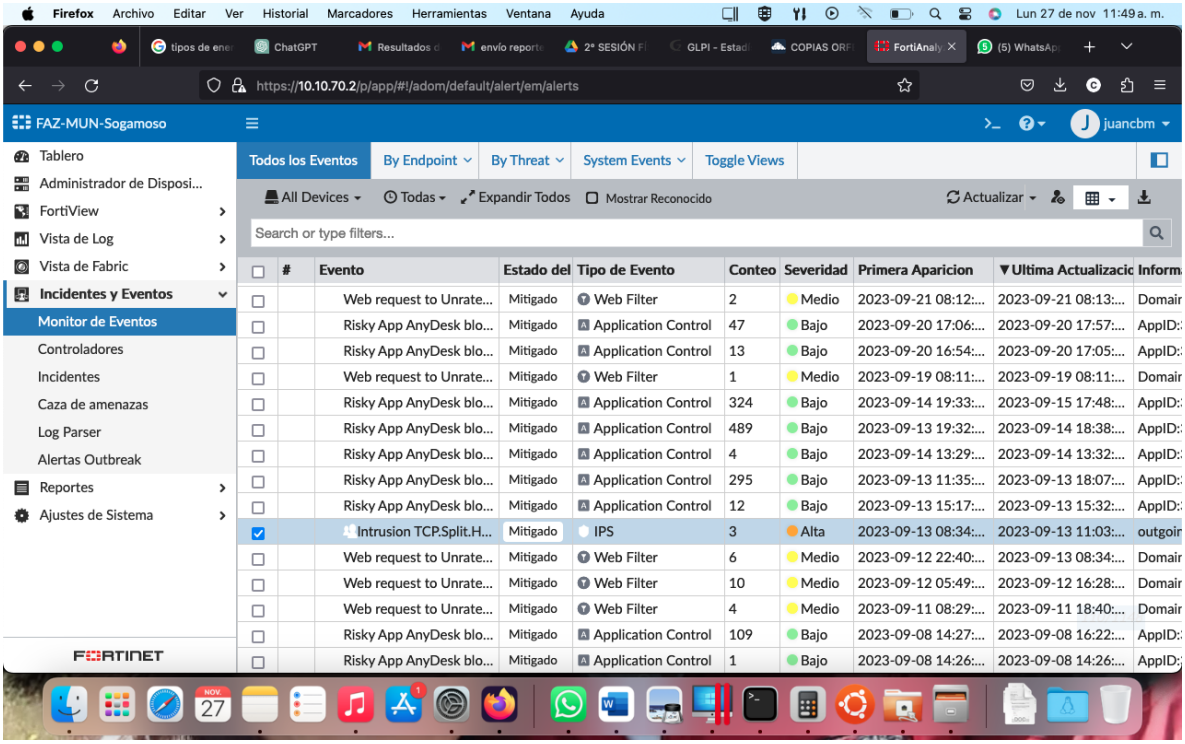
Donde la consola de fortianalyzer refleja que fue contenido pero que requiere acciones de bloqueo en Fortinet edf pintor. Se accede a las políticas de navegación y se agrega a la regla de filtrado la url restringiendo el acceso a esa u otra derivación.

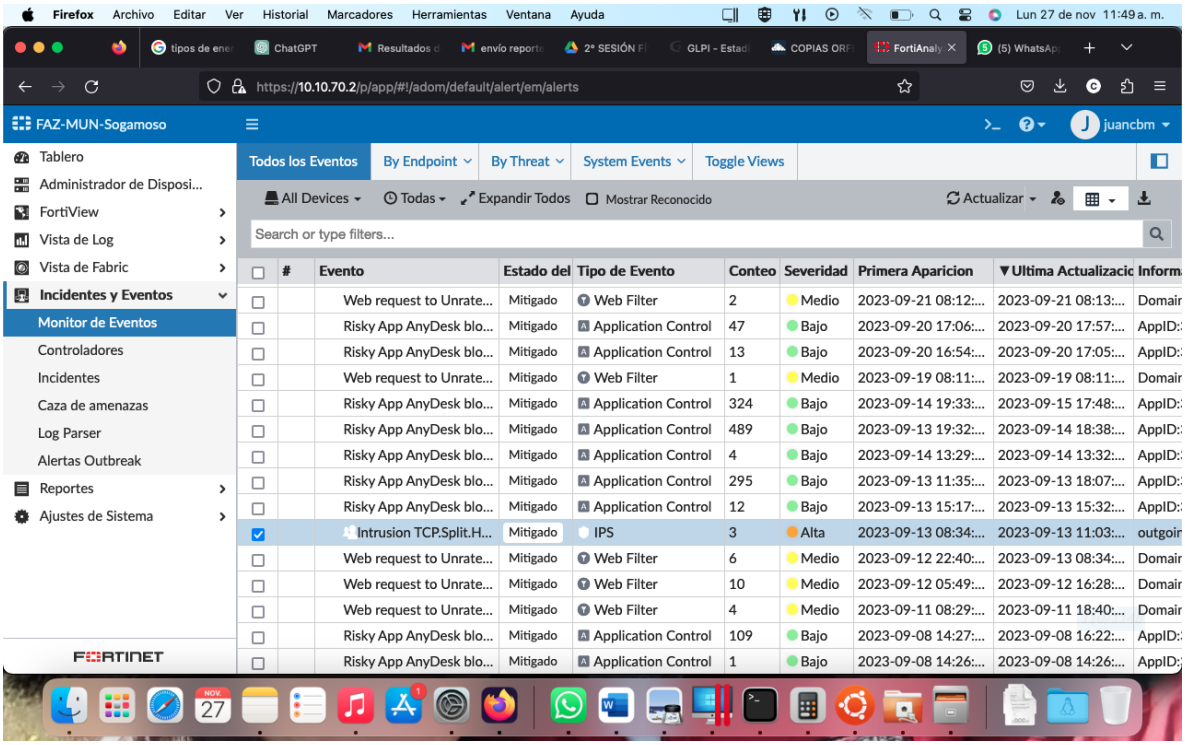






El segundo caso importante el de nivel alto registrado en edf torre 6. Un incidente de tipo intrusión el cual fue mitigado por el mismo Fortinet y se detalla como un intento de inyección código malicioso.



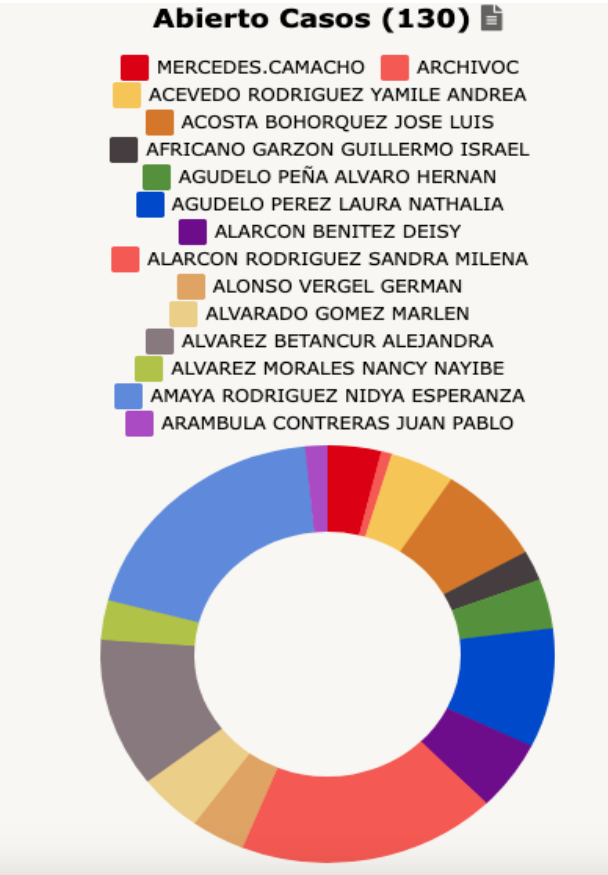


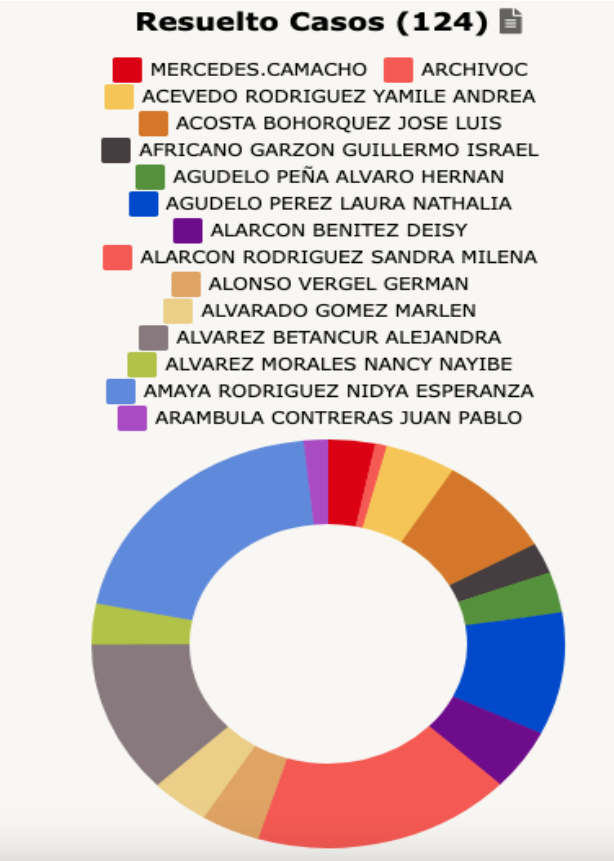
Las recomendaciones para este periodo es el constante revisión y seguimiento de los incidentes reportados ya que hay nuevos casos de intrusión por url que Fortinet lo bloquea, pero hay que realizar un ingreso manual al filtrado de contenido inmerso en la política de navegación del Fortinet.

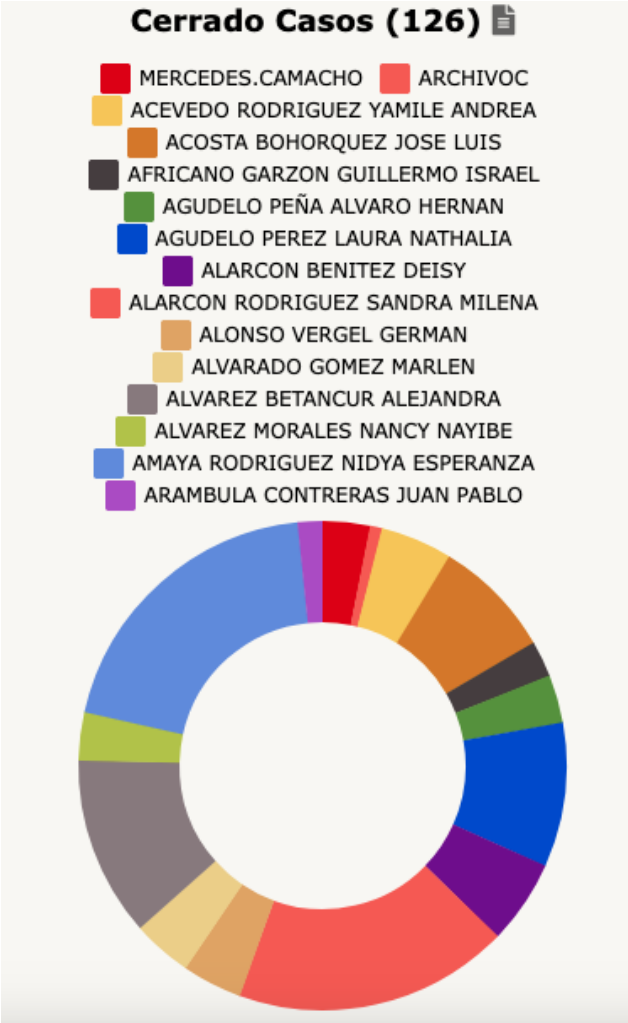
Por otro lado se sugiere un seguimiento al edf el pintor en cuanto accesos permitidos a páginas web, ya que hay muchos casos de nivel medio o bajo de ingreso ya sea directamente a página que redireccionan a criptomonedas y esta paginas las reporta como maliciosas.

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.**

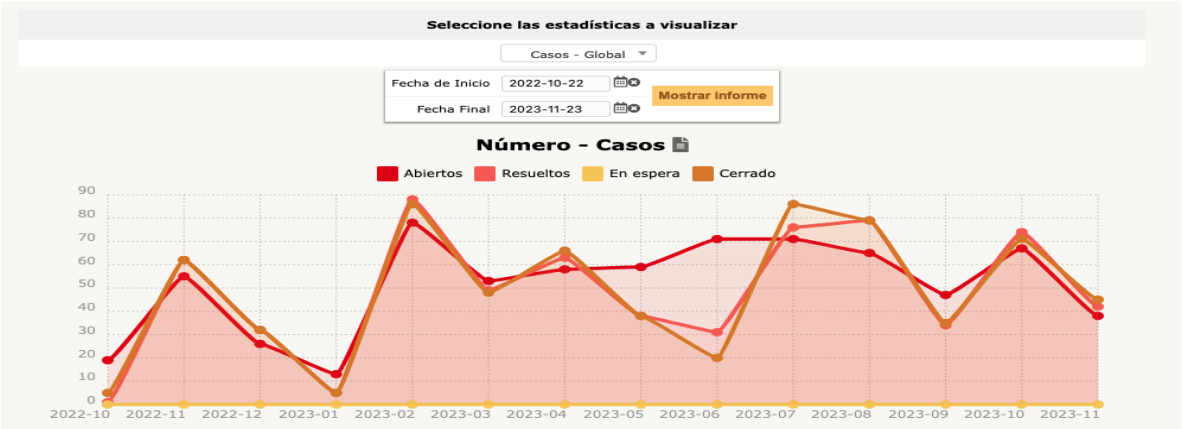
Las condiciones técnicas del aplicativo y el servidor son óptimas. Se hizo revisión previa a los casos que han sido incluidos en este nuevo periodo y se evidencia la creación de 130 casos en la administración y de esos 124 de manera oportuna se han tramitado y cerrado 126. Se puede generar la inquietud del caso de mas. Al ver la relacion de este se refleja que viene arrastrado del periodo anterior en un caso y en este se dio solucion.se conlcuye los casos generardos demuestra una efcitividad en el servicio del 95.38% para el periodo comprendido de este informe.




Resuelto Casos (124)
MERCEDES.CAMACHO
ARCHIVOC
ACEVEDO RODRIGUEZ YAMILE ANDREA
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 MORALES NANCY NAYIBE
AMAYA RODRIGUEZ NIDYA ESPERANZA
ARAMBULA CONTRERAS JUAN PABLO



Esta grafica representa 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.

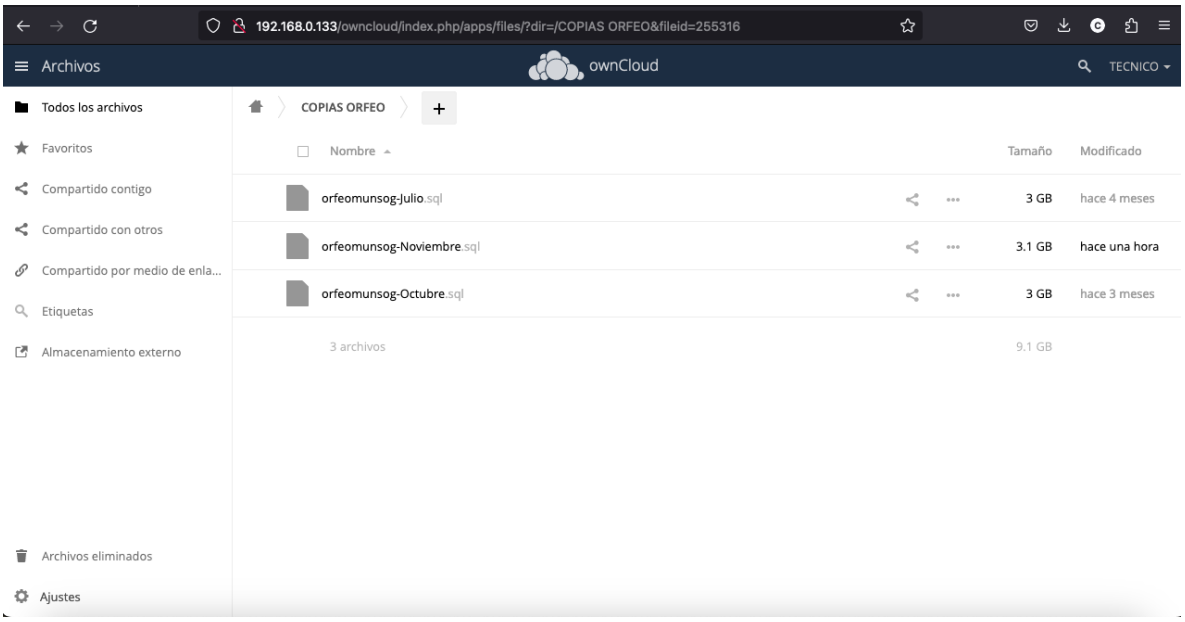


4. Realizar actualizaciones en capacitaciones en la oficina de atención al usuario relacionadas con el centro de relevo y/o demás herramientas tecnológicas dispuestas para discapacidad.

Se hace revisión en sitio del equipo donde se encuentra instalado la herramienta ZOOMTEXT y JAWS, para validar su funcionamiento y estado de actualizaciones para generar citación a capacitación dudas e inquietudes respecto a la herramienta. Se evidencia que la solución esta actualizada debidamente y el sistema operativo residente está en buen funcionamiento.

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

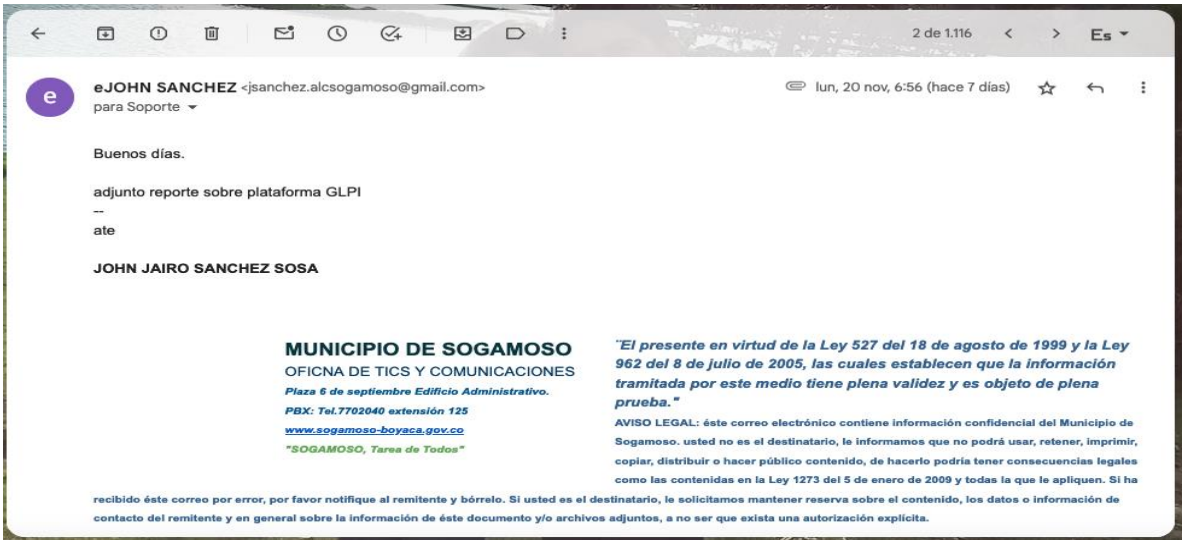
Se generan copias de seguridad correspondientes al mes de OCTUBR - NOVIEMBRE de la base de datos del sistema de gestión documental orfeo dejándolas almacenadas en la plataforma owncloud.

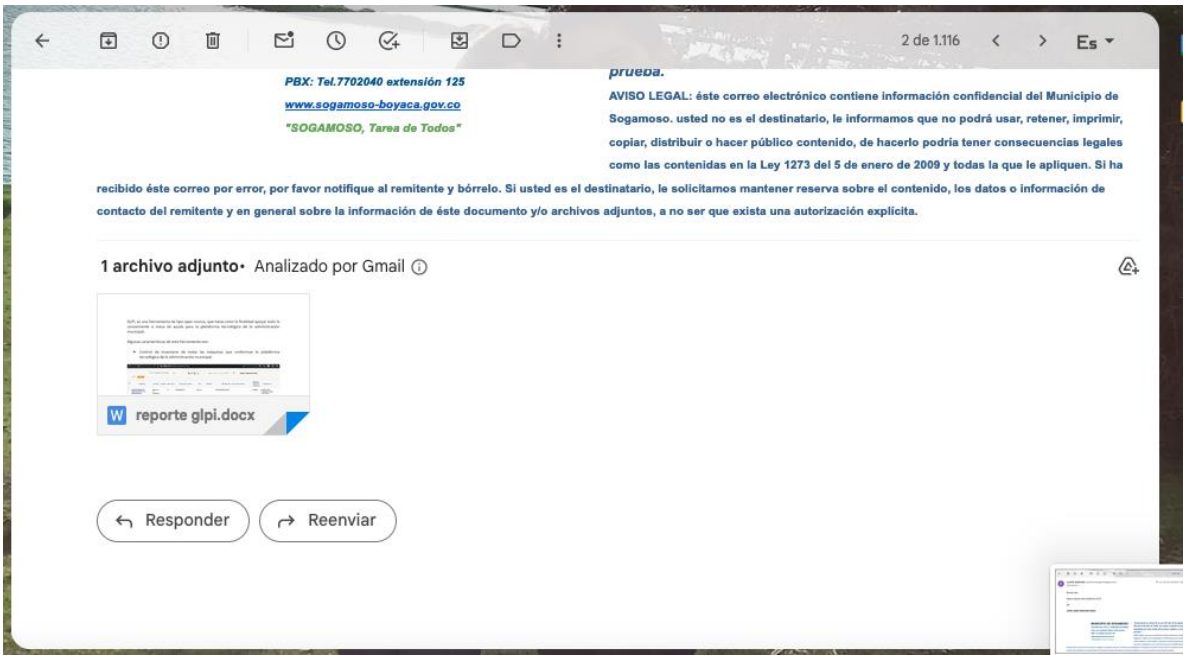


Sobre el espacio de disco del servidor Orfeo, en dialogo con la ingeniera Nancy Álvarez ya se escaló la solicitud de compra al contratista. Se está en espera de la entrega de disco duro.

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

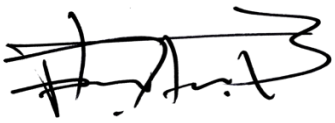
Se ha apoyado a la oficina en requerimiento de información de GLPI par proceso de empalme donde refiere la cantidad de casos reportados desde la puesta en producción con los tickets resuelto por el equipo técnico de la oficina. Se envía reporte a supervisor.



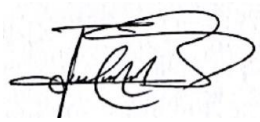


Lo anterior para efectos de pago.

Atentamente,



JOHN JAIRO SANCHEZ SOSA
Contratista



VoBo Supervisor