Sogamoso, Julio de 2023

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

Asunto: Presentación de informe N°4 contrato 20230294

Respetado Ingeniero:

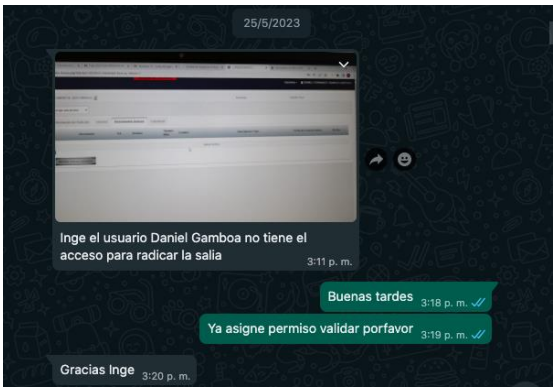
Cordialmente me permito presentar informe del periodo comprendido entre 23 de Mayo al 22 de Junio; teniendo en cuenta contrato de prestación de servicios de apoyo a la gestión número 20230294 así:

Actividad:

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

Se apoya a la oficina de atención al usuario en Orfeo en las siguientes actividades:

- Se asignar permiso a usuario DANIELGAMBOA para realizar radicaciones salida.



Por medio de asignación de perfiles del módulo usuario y perfiles de Orfeo se asigna la opción usuario normal el cumple con las necesidades de la solicitud de la dependencia.



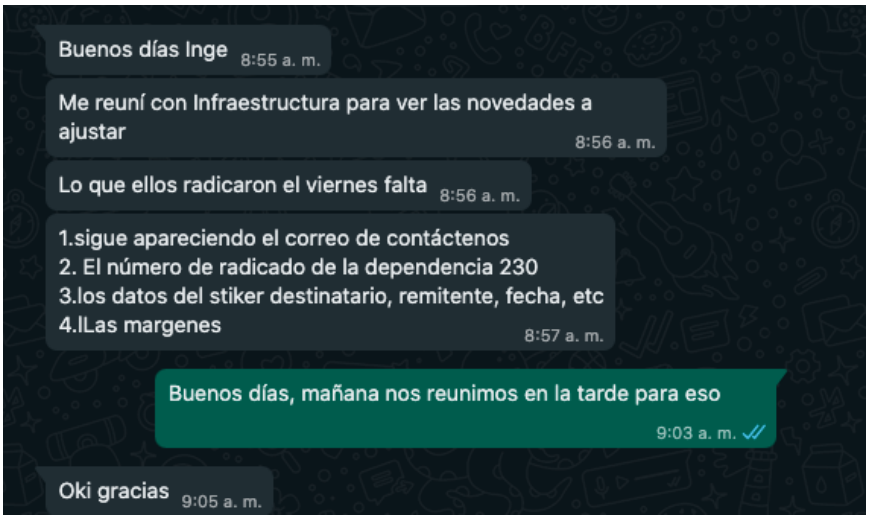
- Se solicita cambio en el nombre de la nueva jefe de Control Disciplinario.



Se ingresa por módulo de usuarios y perfiles de ORFEO a la doctora Liliana Suarez.

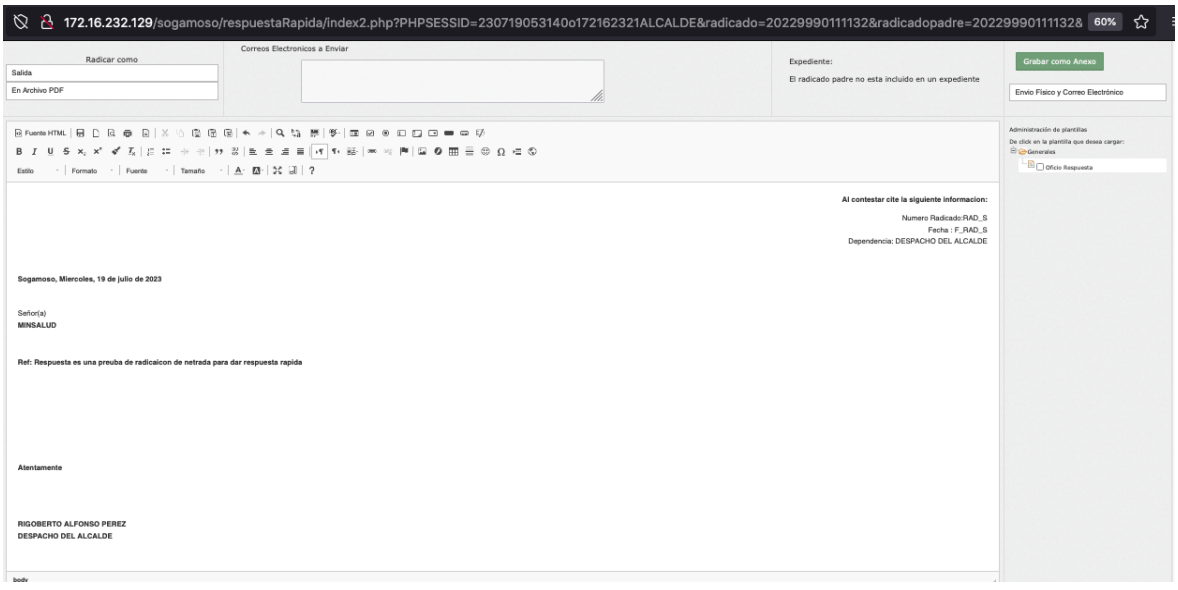


Se realiza levantamiento de ajustes a modulo respuesta rápido de parte de secretaria de infraestructura. Se hacen los cambios sugeridos.



A partir de la reunión realizada entre la oficina de atención al usuario y secretaria de Infraestructura realizada en el mes de mayo se definido la implementación en plan piloto del módulo de respuesta rápida el cual permitirá hacer cierre de los ciclos de gestión de documentos dentro del software ORFEO. Como ventajas obtendremos mejor trazabilidad en la información entrada y salida de cada petición radicada, como a su vez un mejor reporte en el informe de PQRD.

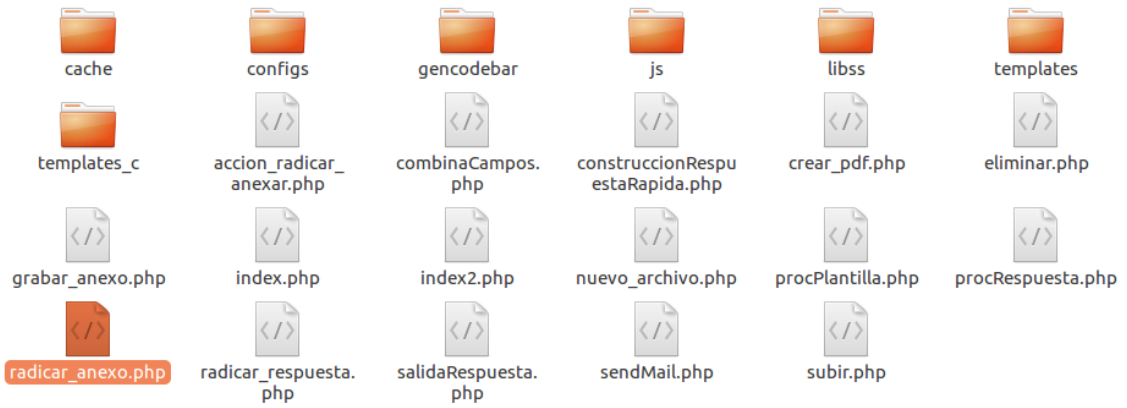
Como inicio se activó el módulo de respuesta rápida para cada funcionario de la dependencia.





Se generaron una serie de requerimientos respecto ajustes del formato de respuesta pdf el cual los funcionarios generan observación en productivo.

Se toma el modelo de documento en pdf modificando las márgenes y los espacios entre líneas para que se vea un documento más organizado. De igual forma se agrega en la sección de sticker la dependencia de origen del dato. En cuanto al número de radicación queda inmerso el código de la dependencia. Esto queda plasmado en el código fuente de Orfeo.




```
                FROM
                    DEPENDENCIA
                WHERE
                    DEPE_CODI = $tpDepeRad";

$creaNoRad    = $db->conn->Execute($isql_consec);
$tpDepeRad    = $creaNoRad->fields["secuencia"];
$rad = new Radicacion($db);
$rad->radiTipoDeri  = 0;          // ok ????
$rad->radiCuentai   = 'null';     // ok, Cuenta Interna, Oficio, Referencia
$rad->eespCodi      = $iden;      //codigo emepresa de servicios publicos bodega
$rad->mrecCodi      = 3;          // medio de correspondencia, 3 internet
//$rad->radiFechOfic  = "$ddate/$mdate/$adate"; // igual fecha radicado;
$rad->radiFechOfic  = "now()"; // igual fecha radicado;
$rad->radiNumeDeri  = $numRadicadoPadre; //ok, radicado padre
$rad->radiPais      = $pais;     //OK, codigo pais
$rad->descAnex      = '.';       //OK anexos
$rad->raAsun        = "Respuesta al radicado " . $numRadicadoPadre; // ok asunto
$rad->radiDepeActu  = $coddepe;    // ok dependencia actual responsable
$rad->radiUsuaActu  = $usua_actu; // ok usuario actual responsable
$rad->radiDepeRadi  = $coddepe;    //ok dependencia que radica
$rad->usuaCodi      = $usua_actu; // ok usuario actual responsable
$rad->dependencia   = $coddepe;    //ok dependencia que radica
$rad->trteCodi      =  0;          //ok, tipo de codigo de remitente
$rad->tdocCodi      = $tdoc;       //ok, tipo documental
$rad->tdidCodi      = 0;           //ok, ????
$rad->carpCodi      = 1;           //ok, carpeta entradas
$rad->carPer        = 0;           //ok, carpeta personal
$rad->ra_asun       = "Respuesta al radicado " . $numRadicadoPadre;
$rad->radiPath      = 'null';
$rad->usuaDoc       = $radUsuaDoc;
$codTx              = 62;

$nurad = $rad->newRadicado($tipo_radicado, $tpDepeRad);
$rad_salida = $nurad;
$fecha_rad_salida = date("d-m-Y");

//echo "$rad_salida -- $fecha_rad_salida <br />";

if($fecha_rad_salida) $respuesta = str_replace('F_RAD_S', $fecha_rad_salida, $respuesta);
```

```php
<?php
 define('ADODB_ASSOC_CASE', 1);

  require_once($ruta_raiz."/config.php");
  include_once ($ruta_raiz."/include/tx/Expediente.php");

  include_once($ruta_raiz."/class_control/anexo.php");
  //include_once($ruta_raiz."/class_control/anex_tipo.php");
  include_once($ruta_raiz."/include/tx/Tx.php");
  include_once($ruta_raiz."/include/tx/Radicacion.php");
  //include_once($ruta_raiz."/class_control/Municipio.php");
  //include_once($ruta_raiz."/include/PHPMailer_v5.1/class.phpmailer.php");
  //require_once($ruta_raiz."/tcpdf/config/lang/eng.php");
  //require_once($ruta_raiz."/conf/configPHPMailer.php");
  require_once($ruta_raiz."/tcpdf/tcpdf.php");


require_once($ruta_raiz."/include/db/ConnectionHandler.php");
  $db      = new ConnectionHandler($ruta_raiz);

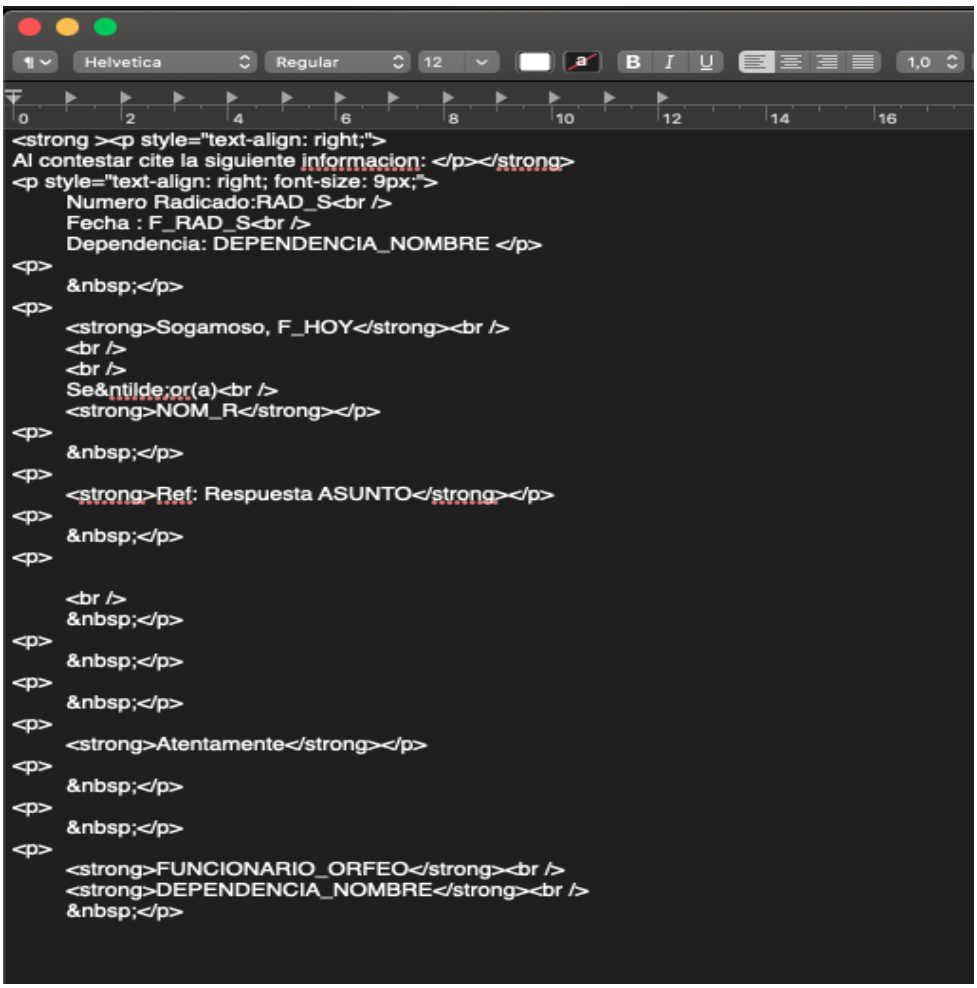
  //$db->conn->SetFetchMode(ADODB_FETCH_ASSOC);
  $hist    = new Historico($db);
  $Tx      = new Tx($db);


  //$db->conn->debug = true;

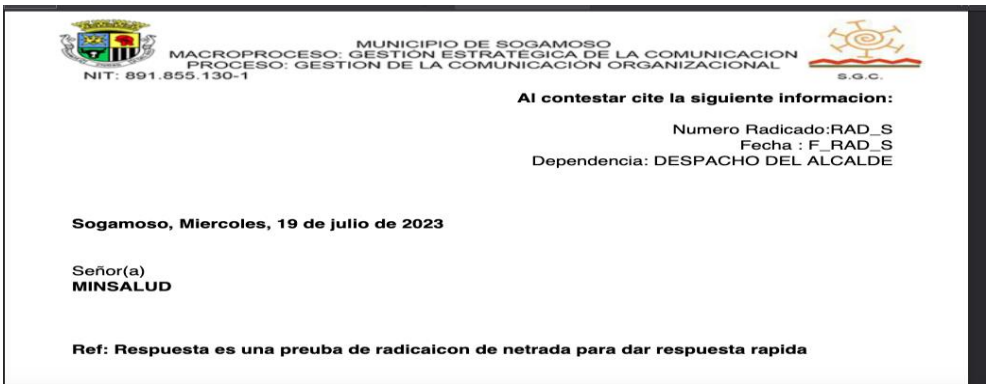
  $sqlFechaHoy      = $db->sysdate();
  $numRadicadoPadre = $_POST["radPadre"];

  $tamanoMax      = 7 * 1024 * 1024; // 7 megabytes
  $fechaGrab      = trim($date1);
  $numramdon      = rand (0,100000);
  $contador       = 0;
  $regFile        = array();
  $conCopiaA      = '';
  $enviadoA       = '';
  $cCopOcu        = '';

  $ddate          = date('d');
  $mdate          = date('m');
  $adate          = date('Y');
```



El producto final de cara al funcionario y ciudadano es este



MUNICIPIO DE SOGAMOSO
MACROPROCESO: GESTION ESTRATEGICA DE LA COMUNICACION
PROCESO: GESTION DE LA COMUNICACION ORGANIZACIONAL
NIT: 891.855.130-1
s.g.c.

Al contestar cite la siguiente informacion:

Numero Radicado:RAD_S
Fecha : F_RAD_S
Dependencia: DESPACHO DEL ALCALDE

Sogamoso, Miercoles, 19 de julio de 2023

Señor(a)
MINSALUD

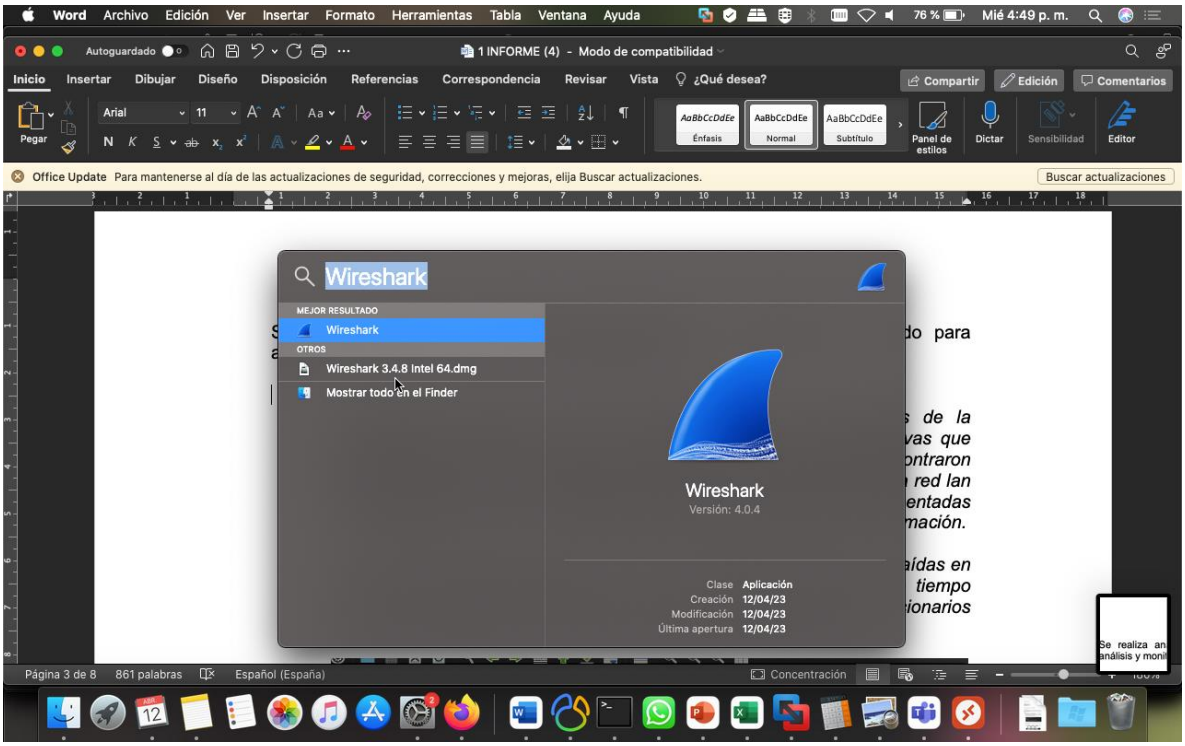
Ref: Respuesta es una preuba de radicaicon de netrada para dar respuesta rapida

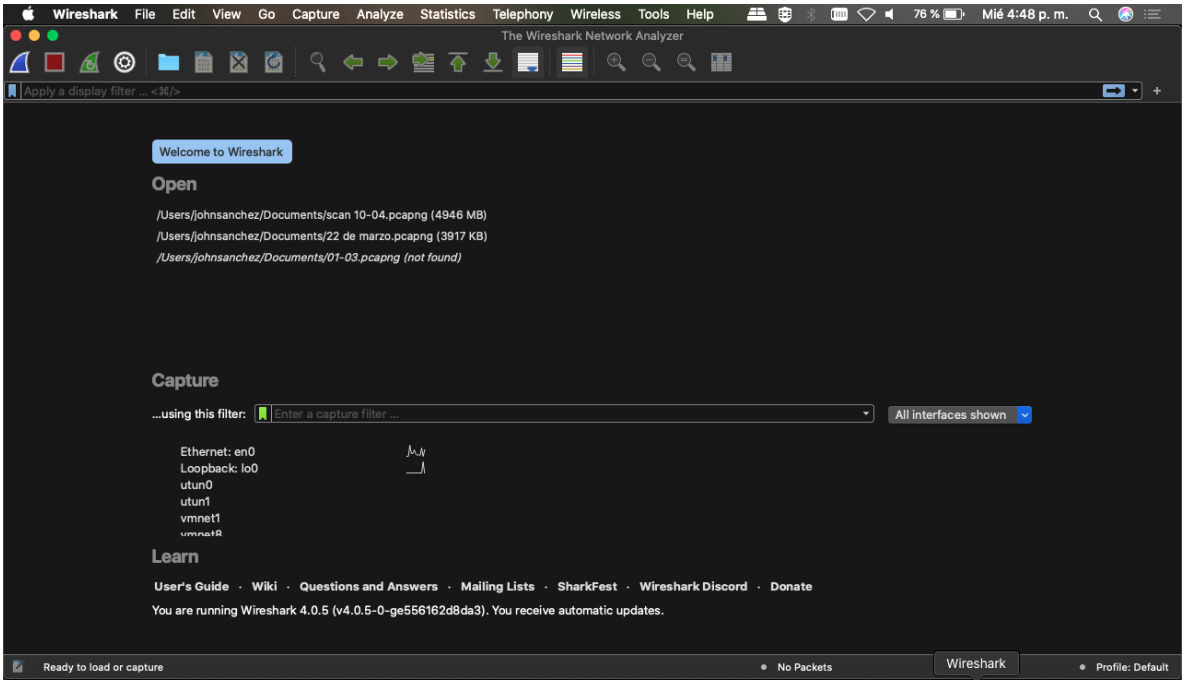
Se hace seguimiento a recomendación generada sobre el servidor Orfeo en el mes de mayo “Por lo demás el sistema Orfeo a estado operando de forma intermitente, a causa del déficit de espacio en disco del servidor. Como medida de urgencia se ha liberado espacio en cache. Se sugiere la compra de un disco 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.”. en conversaciones adelantadas con la ingeniera Nancy Alvarez estamos a espera de contrato de mantenimiento a la plataforma tecnológica de la cual se hará adquisición de disco duro necesario.

Se hace validación de caso sysmanweb respecto a error en la impresión del código de barras en la oficina de impuestos, se hizo traslado al puesto de trabajo para verificar el paso a paso del proceso. Se evidencia que se existe un fallo en la impresión laser, el caso debe ser reportado directamente a SYSMAN.

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

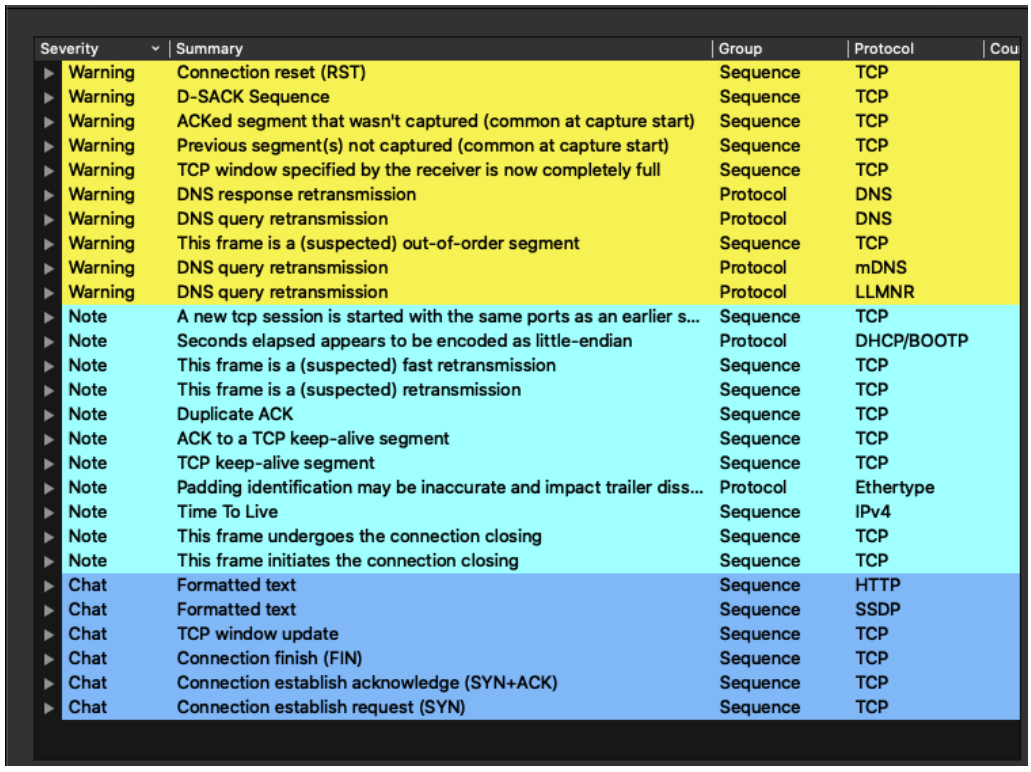
Secretaria de Educación

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 mayo y junio

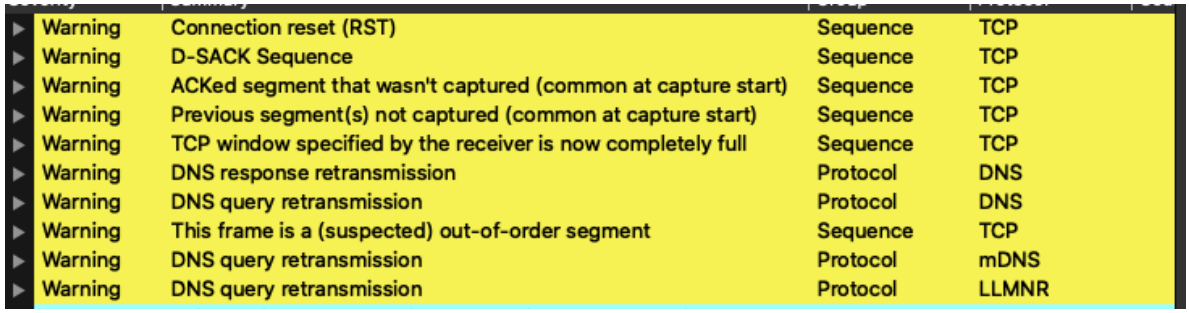
Se realizaron análisis de tráfico periódicos de la red de datos de la administración municipal y no sé en evidencia anomalías significativas que hagan referencia a un ciberataque se puede concluir que se dice encontraron registros de paquetes de datos perdidos desde la red internet hacia la red lan de 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
Warning	Connection reset (RST)	Sequence	TCP	
Warning	D-SACK Sequence	Sequence	TCP	
Warning	ACKed segment that wasn't captured (common at capture start)	Sequence	TCP	
Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	
Warning	TCP window specified by the receiver is now completely full	Sequence	TCP	
Warning	DNS response retransmission	Protocol	DNS	
Warning	DNS query retransmission	Protocol	DNS	
Warning	This frame is a (suspected) out-of-order segment	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	Seconds elapsed appears to be encoded as little-endian	Protocol	DHCP/BOOTP	
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	
Note	This frame is a (suspected) retransmission	Sequence	TCP	
Note	Duplicate ACK	Sequence	TCP	
Note	ACK to a TCP keep-alive segment	Sequence	TCP	
Note	TCP keep-alive segment	Sequence	TCP	
Note	Padding identification may be inaccurate and impact trailer diss...	Protocol	Ethertype	
Note	Time To Live	Sequence	IPv4	
Note	This frame undergoes the connection closing	Sequence	TCP	
Note	This frame initiates the connection closing	Sequence	TCP	
Chat	Formatted text	Sequence	HTTP	
Chat	Formatted text	Sequence	SSDP	
Chat	TCP window update	Sequence	TCP	
Chat	Connection finish (FIN)	Sequence	TCP	
Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP	
Chat	Connection establish request (SYN)	Sequence	TCP	

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	Connection reset (RST)	Sequence	TCP
Warning	D-SACK Sequence	Sequence	TCP
Warning	ACKed segment that wasn't captured (common at capture start)	Sequence	TCP
Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP
Warning	TCP window specified by the receiver is now completely full	Sequence	TCP
Warning	DNS response retransmission	Protocol	DNS
Warning	DNS query retransmission	Protocol	DNS
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP
Warning	DNS query retransmission	Protocol	mDNS
Warning	DNS query retransmission	Protocol	LLMNR

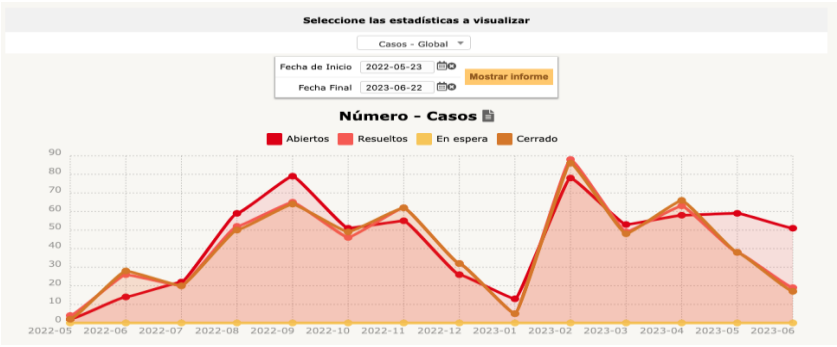
Los warning reflejados en la imagen superior son a causa de software realizando peticiones de conexión a servidores ya sea para almacenamiento de información o solicitud de actualizaciones los cuales están restringidos por políticas del Fortinet. No representan un riesgo real a la seguridad de la red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

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

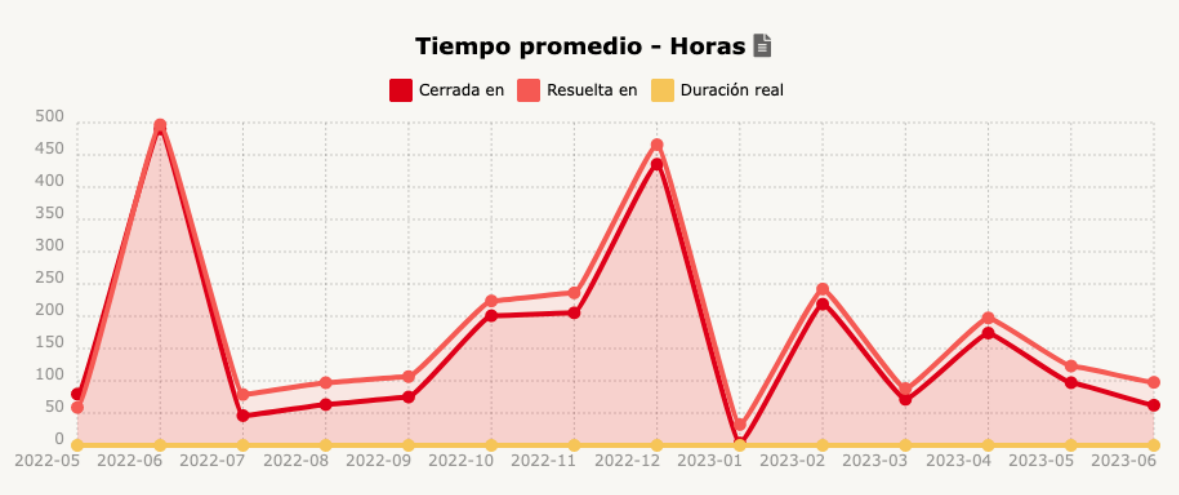
Recomendaciones: validar el estado de actualizaciones Windows ya que parte del tráfico de petición se debe a peticiones hechas por maquina hacia servidores para descarga de paquetes.

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.

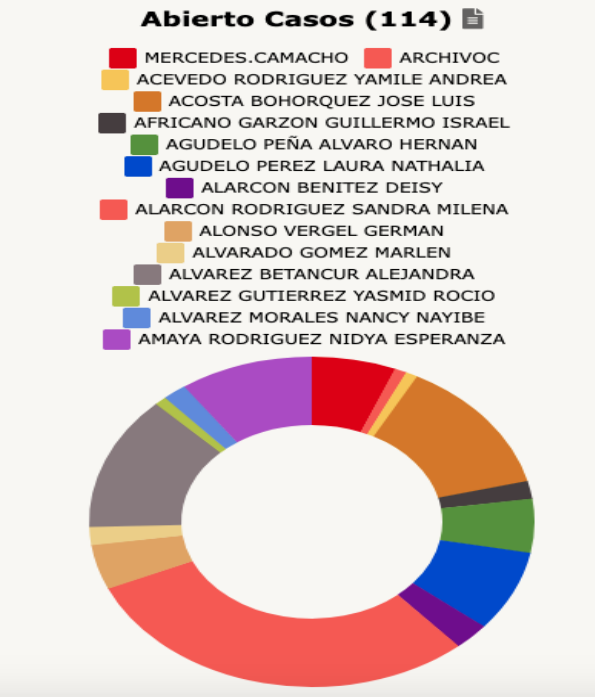
Las condiciones técnicas del aplicativo y el servidor son optimas. Se hizo revisión previa a los casos que han sido incluidos en este nuevo periodo y se evidencia la creación de 114 casos en la administración y de esos 109 de manera oportuna se han tramitado y cerrado 109. Se puede generar la inquietud 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 95.6% para el periodo comprendido de este informe.

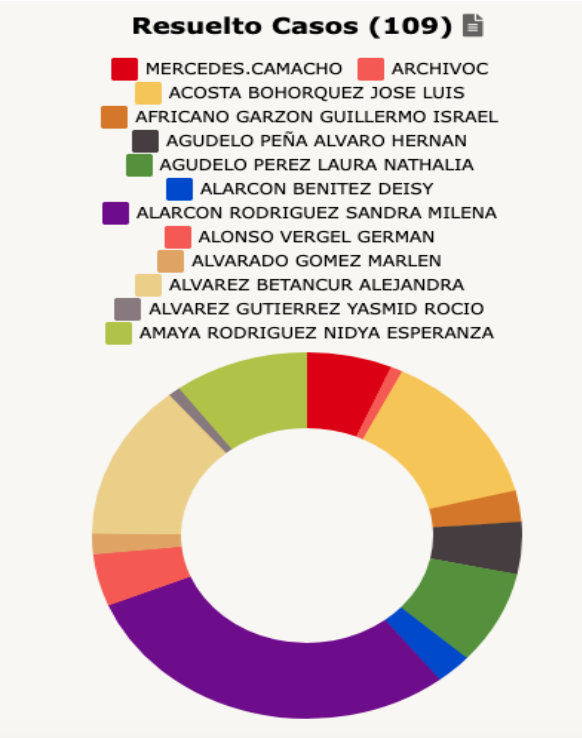


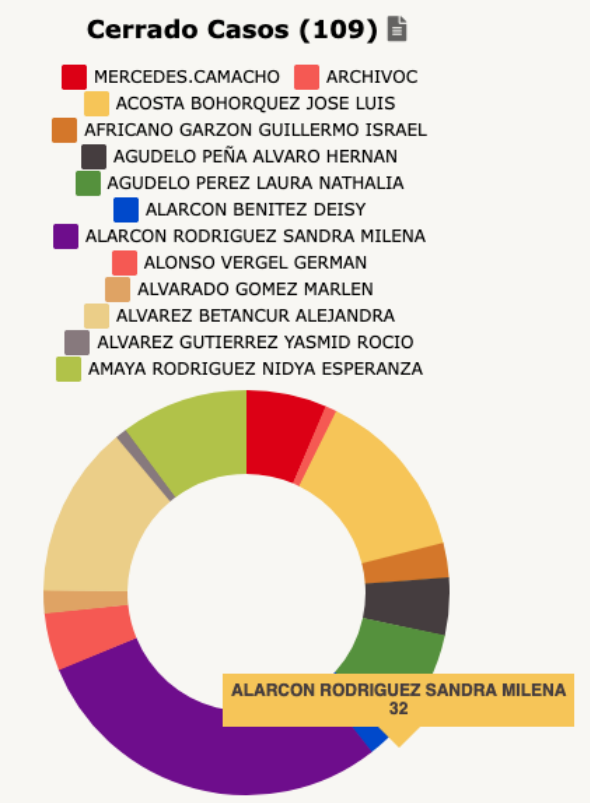
Esta grafica represente el numero de casos creados en sistema realizando una comprativa de estado de solicitudes.



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




Resuelto Casos (109)
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

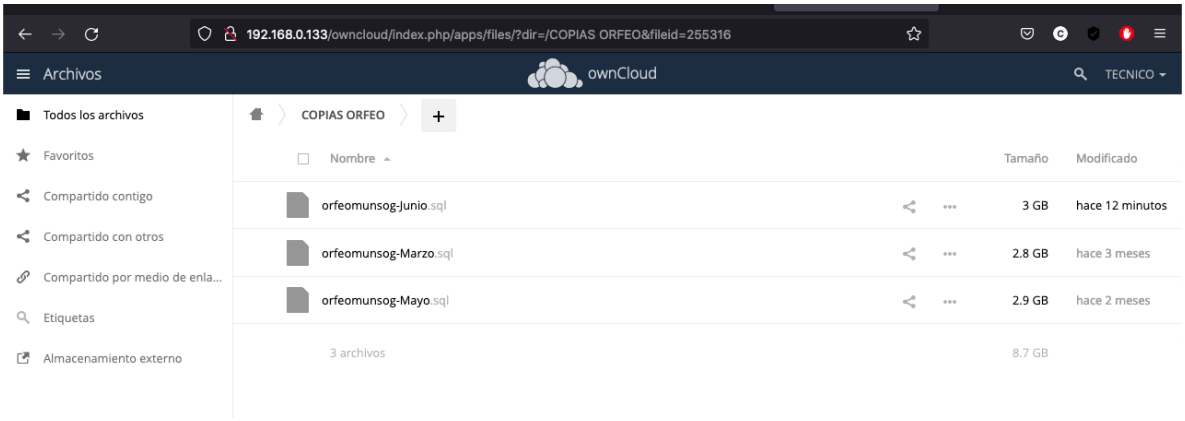

Cerrado Casos (109)
MERCEDES.CAMACHO
ARCHIVOC
ACOSTA BOHORQUEZ JOSE LUIS
AFRICANO GARZON GUILLERMO ISRAEL
AGUDELO PEÑA ALVARO HERNAN
AGUDELO PEREZ LAURA NATHALIA
ALARCON BENITEZ DEISY
ALARCON RODRIGUEZ SANDRA MILENA
ALONSO VERGEL GERMAN
ALVARADO GOMEZ MARLEN
ALVAREZ BETANCUR ALEJANDRA
ALVAREZ GUTIERREZ YASMID ROCIO
AMAYA RODRIGUEZ NIDYA ESPERANZA
ALARCON RODRIGUEZ SANDRA MILENA
32

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 realizo programación para capacitación. Pero fue aplazada para el mes de junio. A razón de visitas técnicas.

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

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

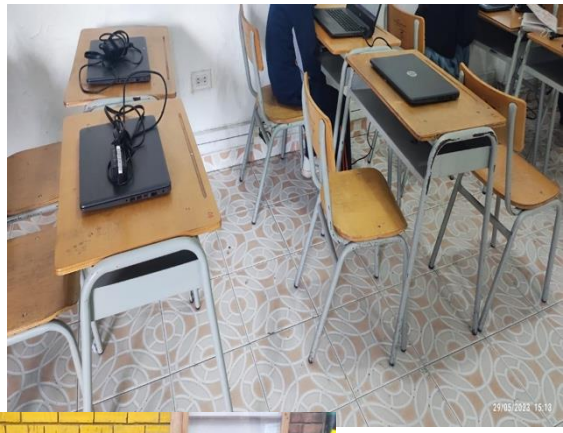


Por lo demás el sistema Orfeo a estado operando de forma intermitente, a causa del déficit de espacio en disco del servidor. Como medida de urgencia se ha liberado espacio en cache. Se sugiere la compra de un disco duro para servidor con el fin de liberar disco des sistema principal, migrando la bodega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

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

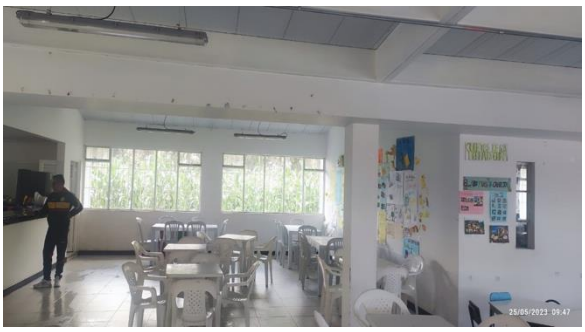
Se hace acompañamiento junto con ingeniero de la empresa OTTIS a visita técnica a instituciones educativas en cuanto a requerimientos solicitados para mejoramiento del servicio de internet. Los colegios visitados fueron I.E Gustavo Jiménez sedes: central, ramada, la manga, sucre y Juan José Rondón. I.E integrado sedes: Uriel Armando Bravo y Aristóbulo Angarita. I.E Los Libertadores. I.E. Rafael Gutiérrez sede el papayo, I.E Marco Antonio Quijano sede el Hatillo. I.E. Magdalena, I.E bellas Artes. I.E San Martin de Tours, I.E Independencia.

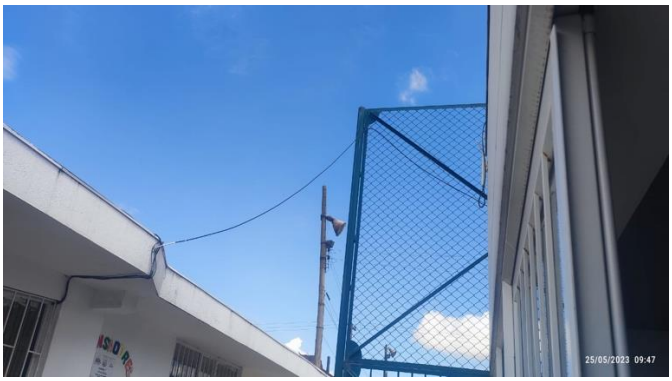












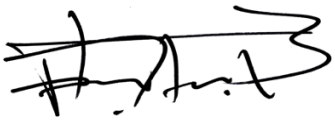


Las demás evidencias quedaron plasmadas en informe técnico remitido por correo electrónico a oficina tic comunicaciones y soporte sistemas.

De igual forma se apoyó a visita a colegios como morca, Integrado y general Santander para apoyo en formulación de proyecto de robótica en mira de la feria prevista para el 17 de agosto.

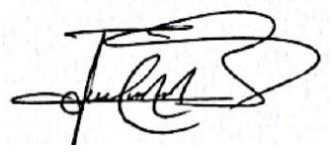
Lo anterior para efectos de pago.

Atentamente,



_____

JOHN JAIRO SANCHEZ SOSA
Contratista



VoBo Supervisor