PROPONER UN SISTEMA DE DIAGNÓSTICO Y MONITOREO QUE PERMITA IDENTIFICAR EVENTOS PARA RESOLVER PROBLEMAS DE INFRAESTRUCTURA DE TI, DE LA RED DE DATOS DE LA EMPRESA SOCIEDAD CLÍNICA EMCOSALUD

CESAR AUGUSTO CELIS PERDOMO
FRANCY PATRICIA TRUJILLO MURCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
NEIVA
2017

PROPONER UN SISTEMA DE DIAGNÓSTICO Y MONITOREO QUE PERMITA IDENTIFICAR EVENTOS PARA RESOLVER PROBLEMAS DE INFRAESTRUCTURA DE TI, DE LA RED DE DATOS DE LA EMPRESA SOCIEDAD CLÍNICA EMCOSALUD

CESAR AUGUSTO CELIS PERDOMO
FRANCY PATRICIA TRUJILLO MURCIA

Tesis de grado para optar por el título:
Especialista En Seguridad Informática

Director de Proyecto:
Erika Liliana Villamizar Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
NEIVA
2017

Nota de Aceptación:

_____
_____
_____
_____
_____

Jurado

Jurado

Neiva, Abril de 2017

DEDICATORIA

Este proyecto la dedico a Dios y mi madre que está en el cielo quien supo guiarme por el buen camino, darme fuerzas para seguir adelante y no desfallecer.

A mi familia, mi esposo John Jairo Ortiz Cumbe y mi hija Jessica Julieth Ortiz Trujillo quienes con su amor, sacrificio y apoyo incondicional me han apoyado en ésta etapa de mi proyecto de vida.

A mi padre y hermanas quienes han sido mi mayor motivación para nunca rendirme, llegar a esta instancia de mis estudios, ya que ellos siempre han estado presentes para apoyarme moral y psicológicamente.

Francy Patricia Trujillo

El Presente es dedicado a mi familia, mi esposa María Jenny Bustos Jiménez, a mis hijos Juan Felipe y Valeria Celis Bustos, a mis padres y hermanos que han sido mi apoyo fundamental e incondicional y la motivación para culminar con éxito este nuevo proyecto en mi vida.

Cesar Augusto Celis Perdomo

AGRADECIMIENTOS

Damos gracias a Dios por darnos la oportunidad de cursar la especialización en seguridad informática.

Un agradecimiento especial a la ingeniera Erika Liliana Villamizar Torres, por su apoyo incondicional en la elaboración de este proyecto. Al ingeniero Salomón González quien fuera el tutor asignado en la primera etapa del anteproyecto

A nuestras familias por su apoyo incondicional, su colaboración y sobre todo su paciencia, en las largas jornadas que tuvimos que ausentarnos para cumplir con las actividades programadas en el proyecto.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ACCESS POINT: Dispositivo de hardware o software que actúa como un centro de comunicación para los usuarios de dispositivos inalámbricos que desean conectarse a una LAN cableada. Son importantes para proporcionar mayor seguridad inalámbrica y para ampliar el rango físico de servicio a un usuario móvil.

ADMINISTRADORES DE DISPOSITIVOS O SERVIDORES VPN: Técnicos encargados de la instalación, mantenimiento, configuración de parámetros adecuados de seguridad e implementación de los procedimientos y políticas de seguridad y operaciones en los dispositivos o servidores de red privada virtual (VPN).

ADMINISTRADORES DE LOS FIREWALLS DE RED: Técnicos encargados de administrar, mantener y operar el hardware o software que tiene la capacidad para limitar el acceso entre las redes o sistemas conforme a lo configurado en las políticas de seguridad (firewalls).

ADMINISTRADORES DEL SISTEMA DE PREVENCIÓN DE INTRUSOS (IPS): Técnicos encargados de administrar, mantener y operar el sistema de prevención de intrusos (IPS).

BACKBONE: Sección central de la red, de gran capacidad y alta velocidad, por la cual otros segmentos de red están conectados.

DMZ: Es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permiten a la red externa.

DOMINIO: Conjunto de objetos con información y políticas de seguridad comunes. En el Microsoft Active Directory es una colección de recursos (cuentas, impresoras, computadoras) que constituyen una frontera de administración y de aplicación de políticas de seguridad.

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP): Protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, teniendo conocimiento en todo momento quién ha estado utilizando de esa IP, cuánto tiempo la ha tenido en uso y a quién se la ha asignado posteriormente.

FILE TRANSFER PROTOCOL (FTP): Protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basada en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar o enviar archivos desde el, independientemente del sistema operativo utilizado en cada equipo.

FIREWALL: Hardware o software que tiene la capacidad para limitar el acceso entre las redes o sistemas conforme a lo estipulado en las políticas de seguridad.

PERFILES O ROLES: Conjunto de privilegios agrupados bajo un nombre, que permiten realizar una administración más efectiva de los derechos de acceso.

PROXIES: Servidores que interceptan el tráfico web de los clientes y realizan las solicitudes de acceso en nombre de ellos, por motivos de: seguridad, rendimiento, anonimato.

PRUEBAS DE PENETRACIÓN: Es un método para evaluar la seguridad de la red o un sistema computacional mediante la simulación de un ataque desde una fuente maliciosa conocida como hacker o cracker.

TRÁFICO: Es la cantidad de datos enviados y recibidos por los programas de aplicación a través de una red de datos.

RESUMEN

El presente proyecto se centra en proponer un sistema de diagnóstico y monitoreo que permita identificar eventos para resolver problemas de infraestructura y seguridad de TI de la red de datos de la Empresa Sociedad Clínica Emcosalud. Para este fin se realiza un estudio detallado a la red física, así como al tráfico de datos en la misma, con diversas aplicaciones que están presentes en el mercado y son especializadas en detectar anomalías en el funcionamiento de las redes tanto de origen físico de red como de origen lógico por mal uso de los usuarios.

El proyecto solo abarca la sugerencia de implementación de la herramienta más conveniente para el monitoreo de la red, y se hacen recomendaciones de mejoras físicas y lógicas a la red de datos para que sean tomadas en cuenta por la gerencia en pro de mejorar el rendimiento, la disponibilidad y seguridad de la red de datos de la empresa.

Palabras Claves: Red de datos, Sistema de Monitoreo de red, NAGIOS, Colasoft, capsa9free, Wireshark, Trafico de Red, Centro de Cableado.

0. **INTRODUCCIÓN**

En la actualidad, la seguridad de la información es un objetivo fundamental en las empresas, la importancia que tiene para las organizaciones la convierte en el activo prioritario, por lo cual es imperativo salvaguardarla de las constantes amenazas a las que se ve expuesta, ya que es codiciada por los delincuentes informáticos que quieren obtenerla a cualquier precio y a cualquier medio. Las empresas que se preocupan por mejorar su seguridad informática están mejor posicionadas en el entorno en el que se desempeñan optimizando la confianza de sus clientes y su imagen ante proveedores y competencia.

Como la evolución tecnológica corre a pasos gigantes las redes de comunicación han evolucionado a la par, haciéndose más complejas e interconectando no solo las computadoras de una oficina o un edificio si no que gracias a la internet podemos comunicarnos con host (computadoras) en otros edificios, en otras ciudades e inclusive en otros continentes, de esta forma nace la red de redes (Internet), la cual abre las puertas a un mundo de posibilidades de negocios, de conocimientos y de amenazas tanto a las personas como a las empresas, de ahí el afán de lograr una interconexión cada vez más confiable entre los dispositivos ya sea mediante cable de datos (Redes LAN o WAN) o por conexiones inalámbricas (Redes Wifi).

Paralelo a la evolución tecnológica también evolucionaron los delitos, apareciendo en el contexto los de tipos informático que son más sofisticados y difíciles de identificar gracias a la utilización de equipos informáticos y conocimientos en áreas tecnológicas como la programación y la configuración de redes.

Las redes de datos al ser las vías de transmisión de la información en las empresas se convierten en objetivos y son atacadas tanto de forma interna como externa en pro de obtener la información que por ella se transmiten. A su vez, también están expuestas a fallos por falta de programación o planificación de la misma o por un deficiente mantenimiento. Es frecuente ver como muchas veces se caen los servicios de red por recalentamiento de los switch, por cables deteriorados o simplemente porque manos inescrupulosas o inexpertas dañan las configuraciones de los equipos de comunicación.

Los virus informáticos no atacan los equipos de comunicación, pero si atacan los host interconectados con ellas, entonces las redes de datos también son utilizadas para transmitir aplicativos maliciosos que atentan contra la información y la infraestructura tecnológica de la empresa.

La Sociedad Clínica Emcosalud no es ajena a estas problemáticas, en los últimos meses se ha visto afectada por una serie de incidentes en su entorno y dentro de ella, que han afectado considerablemente la red de datos y en consecuencia el buen funcionamiento de la empresa.

Con la elaboración del presente proyecto se busca poner en conocimiento de las directivas de la Sociedad Clínica Emcosalud y la Gerencia, una herramienta capaz de mejorar la seguridad de su red de datos mediante la constante monitorización de los eventos acontecidos periódicamente en la misma. A su vez identificar problemas de infraestructura que afecten el buen rendimiento en la transmisión de información y proponer posibles soluciones.

1. DESCRIPCIÓN DEL PROBLEMA.

La Sociedad Clínica Emcosalud es una empresa que pertenece al sector salud, y su objetivo principal es brindar un servicio eficiente a sus pacientes, gracias a esto ha logrado mantener buenos estándares de calidad que la mantienen como una de las principales en la región. En los últimos años la empresa ha evolucionado sus servicios brindando más cobertura a una población que está creciendo paulatinamente. Esto ha ocasionado que la clínica tenga que aumentar sus puntos de trabajo contratando más personal, lo cual también ha incrementado la necesidad de mejorar su infraestructura tecnológica y en especial su red de datos la cual se ha afectado considerablemente porque en sus inicios no fue concebida para una cantidad tan grande de usuarios.

Lo anterior tiene como consecuencia unas serie de fallos en la prestación de servicios, las comunicaciones se tornan lentas y engorrosas, los aplicativos se bloquean y la red presenta muchos fallos, lo cual hace que los requerimientos de fallos de comunicación sean cada día más frecuentes y la información este más expuesta a amenazas externas e internas asociadas a los fallos y vulnerabilidades en la red de datos.

2. FORMULACIÓN DEL PROBLEMA.

¿De qué manera se puede mejorar la seguridad de la red de datos de la SOCIEDAD CLINICA EMCOSALUD, además de garantizar un monitoreo periódico de la misma para identificar eventos oportunamente?

3. JUSTIFICACIÓN DEL PROYECTO

Las redes de datos son herramientas indispensables en las infraestructuras tecnológicas de cualquier empresa. Su buen funcionamiento se traduce en buen comportamiento de la empresa, en sus procesos y en sus resultados ayudándola a cumplir con los objetivos trazados.

Por el contrario, si la red de datos falla, se traducirá en trabas en los procesos haciéndolos más lentos o que sencillamente no se ejecuten, lo cual tendrá un efecto desastroso en cualquier empresa ya que además de afectar la comunicación y perder tiempo, también se es posible que se presenten perdidas económicas a la organización.

La dependencia de las organizaciones en función de la comunicación interna y externa, el crecimiento de las mismas al aumentar la cantidad de usuarios de las redes de datos, evidencia la necesidad de una constante medición de la disponibilidad y rendimiento de sus servicios informáticos que permita anticiparse a los problemas que puedan afectar su buen funcionamiento. Partiendo de la premisa que se puede administrar lo que medimos, los responsables del manejo de las tecnologías en la Sociedad Clínica Emcosalud deben contar con herramientas que les permitan conocer en todo momento los inconvenientes que se presentan en su red de datos, y así poder detectarlos oportunamente por medio de diagnóstico y monitoreo permanente a la red de datos en el área administrativa, asistenciales y ayudas diagnosticas; también poder predecir y mitigar el impacto del crecimiento o cambio dentro de la misma.

“La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización. ”[1]

Por lo anterior se pretende el mejoramiento de la red de datos de la empresa Sociedad Clínica Emcosalud, mediante el estudio de implementación de un sistema de monitoreo de su red de datos.

[1] Arcert. [En Línea]. “Manual de Seguridad en redes”. http://instituciones.sld.cu/dnspminsap/files/2013/10/Manual-de-Seguridad-de-Redes.pdf. [Citado en el 2013]

4. OBJETIVOS DEL PROYECTO

GENERAL

Recomendar a la empresa sociedad clínica EMCOSALUD un sistema de diagnóstico y monitoreo que le permita identificar eventos para resolver problemas de infraestructura de TI, de su red de datos

ESPECÍFICOS

- Realizar el levantamiento de la información pertinente que sirva de insumo para llevar a cabo la ejecución del presente proyecto.

- Realizar un análisis físico del estado actual de la red de datos de empresa Sociedad Clínica Emcosalud.

- Investigar 4 tipos de herramientas de seguridad para el monitoreo de red, identificación de eventos y vulnerabilidades.

- Realizar un análisis lógico de la red de datos de la empresa Sociedad Clínica Emcosalud probando las 4 herramientas investigadas.

- Proponer la solución de la herramienta de diagnóstico para la red de datos de la empresa Sociedad Clínica Emcosalud.

- Dar recomendaciones generales para mejorar la red de datos a nivel físico y lógico de la empresa Sociedad Clínica Emcosalud.

5. MARCO REFERENCIAL

5.1 MARCO TEÓRICO

Con la evolución de las tecnologías informáticas se logró un gran avance en las comunicaciones gracias a los nuevos recursos tecnológicos de comunicación, que en última nos han hecho la vida más fácil a todos los usuarios de computadoras personales y empresariales, brindándonos la capacidad de trasmitir una mayor cantidad de datos de forma más rápida y casi a cualquier parte del mundo

En este contexto y bajo estas iniciativas de globalización de las comunicaciones electrónicas apareció hacia la década de los 70's con ARPANet (Advanced Research Projects Agency Network o Red de la Agencia para los Proyectos de Investigación Avanzada de los Estados Unidos), que trazaba la comunicación a alta velocidad de computadoras y a la cual se fueron vinculando otras redes de datos de otras entidades gubernamentales, generando la gran red de redes que hoy en día conocemos como internet.

Con la evolución de internet la transmisión de información de todo tipo, personal, educativa, pública o empresarial se elevó a niveles gigantescos al punto que es una herramienta imprescindible para el funcionamiento de la sociedad actual y la mayoría de las empresas se interconectan a través de sus redes de datos.

Pero desafortunadamente no todo es dicho, así como los negocios, la educación entre otros campos de nuestra sociedad se ha beneficiados y han crecido paulatinamente también aparecen en este contexto los ciberdelincuentes que utilizan la tecnología para atacar las redes de datos y lograr extraer la información que por ella transita, causar malos funcionamientos y hasta el daño total de los dispositivos que conforman la red.

Como respuesta a todos los delitos informáticos que surgieron con la evolución tecnológica y la globalización de las comunicaciones aparece en el universo tecnológico el concepto de seguridad informática, que no es otra cosa que "la adopción de un conjunto de normas, herramientas y procedimientos que buscan

garantizar la disponibilidad, integridad, confidencialidad y buen uso de los sistemas de información y los datos que en ellos se manejan".[2]

Hasta hace unos años no se disponía de las herramientas de administración de recursos informáticos que hoy existen, era necesario contratar a una empresa o personal especializado para esta labor, lo cual tenía costos muy elevados para la empresa y hacia que las gerencias no invirtieran en personal especializado sino hasta cuando se presentaba algún inconveniente con un costo muy elevado en los sistemas de información.

"Las redes empresariales se van haciendo más importantes y complejas, y es necesario para cualquier departamento de TI asegurar el correcto funcionamiento de los procesos y minimizar los fallos informáticos, para evitar pérdidas económicas, de tiempo y productividad. Un sistema que monitorice constantemente la red, ofrece ventajas como el ahorro de tiempo, planificación de recursos, optimización de la red y es muy importante para brindar un buen servicio a los usuarios."[3]

Un sistema de monitoreo de red es una herramienta fundamental que hace un diagnostico periódico 24/7 sobre los componentes de la red (hots, servidores, concentradores, switch, routers, etc) en busca problemas causados por la sobrecarga y/o fallas, como también problemas de la infraestructura de red (u otros dispositivos). Comúnmente, los datos evaluados son tráfico de la red, carga de usuarios, consumo de hardware, tiempo de respuesta y disponibilidad (ouptime), aunque otras estadísticas, tales como consistencia y fiabilidad pueden ser útiles para algunos administradores

5.2 **MARCO CONCEPTUAL**

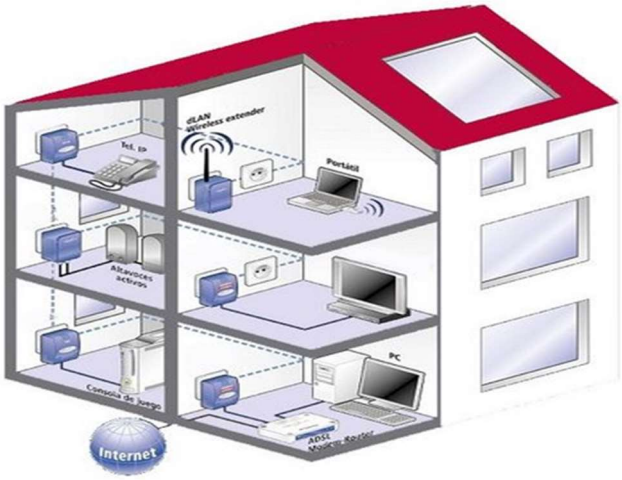
- Red de datos: También llamados red de ordenadores o computadoras se denomina a un conjunto de ordenadores conectados entre sí por dispositivos físicos con el único objetivo de transmitir datos entre ellos, de forma de impulsos eléctricos u ondas electromagnéticas.

- Tipos de redes: Existen varios tipos de redes WAN, LAN, MAN.

[2] RÍOS, Julio [En Línea]. SEGURIDAD INFORMÁTICA < http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml> [Citado en 2010].
[3] Muñoz , Juan [En línea]. ¿Por qué es importante monitorizar nuestra red? https://www.tecnozero.com/blog/por-que-es-importante-monitorizar-nuestra-red/ [s.f.]

- LAN (Red de Área Local): Se denomina LAN, a un conjunto de equipos conectados entre sí en una misma organización y un área geográfica pequeña.

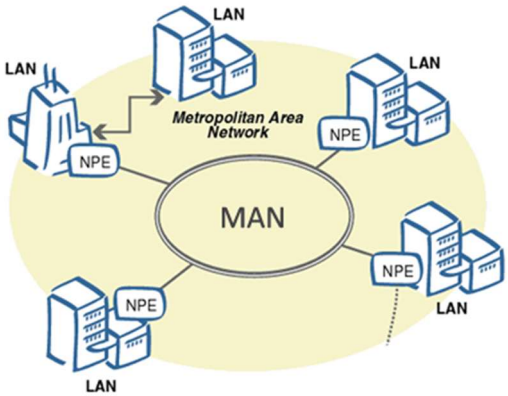
Figura 1 Red LAN



Fuente:http://construiryadministrarred14wendy.blogspot.com.co/2012/05/arquitectura-de-red-lan.html

- MAN (Red de Área Metropolitana): Como su nombre lo indica es una red más grande que la LAN, puede abarcar la parte urbana de ciudades pequeñas, contiene varias LAN interconectadas, manteniendo muy buena velocidad de transmisión de datos. Permite que dos nodos de distintas LAN, se puedan comunicar como si estuvieran en la misma red de área local.

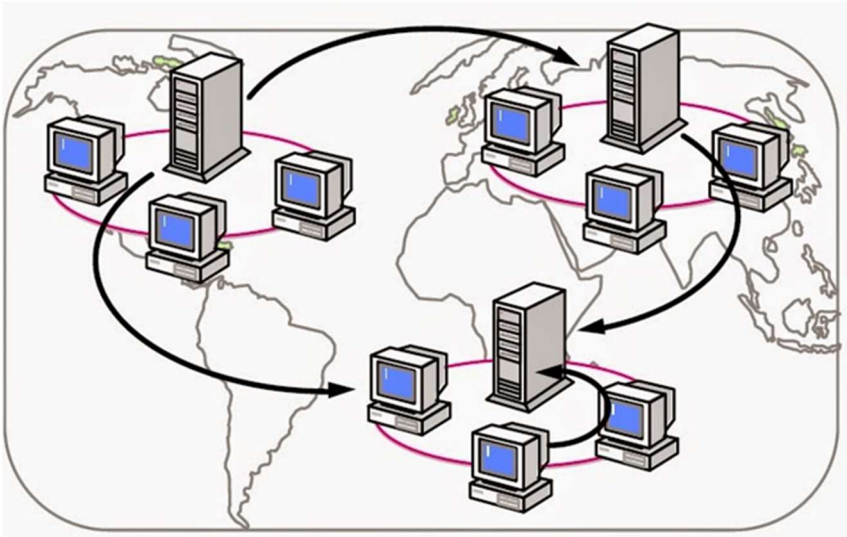
Figura 2 Red MAN



Fuente: http://informaikta.blogspot.com.co/p/redes.html

- WAN (Red de Área Extensa): Podemos decir que las redes WAM, son el conjunto de varias LAN interconectadas entre sí en grandes extensiones geográficas, su cobertura puede abarcar desde ciudades hasta continentes, su velocidad de transmisión de datos suele ser menor que las redes LAN.

Figura 3 Red WAN



Fuente:http://competenciasbasicasistemasonce.blogspot.com.co/2015/04/capitulo-ii-clasificacion-de-las-redes.html

- Monitoreo de Red: Un monitoreo de red es el uso de herramientas y aplicaciones que intermitentemente vigila, escanea y controla una red de datos o computadoras en busca de componentes defectuosos, lentos o dañados, para luego generar un reporte al administrador de la red, con el objeto de anteponerse a los fallos de la misma.

  "La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de cómputo son actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un esquema capaz de notificarnos las fallas en la red y de mostrarnos su comportamiento mediante el análisis y recolección de tráfico."[4]

[4] Vicente, Carlos Alberto [en línea]. "Monitoreo de Recursos de Red" https://juliorestrepo.files.wordpress.com/2011/04/monitoreo.pdf [Citado en 2011]

- Gestión de Redes de Datos: Se puede resumir en el conjunto de tareas de despliegue, integración, y coordinación del hardware, software y los elementos humanos para monitorizar, probar, analizar, evaluar y controlar los recursos de una red para conseguir servicios adecuados a los objetivos de una instalación y una organización.

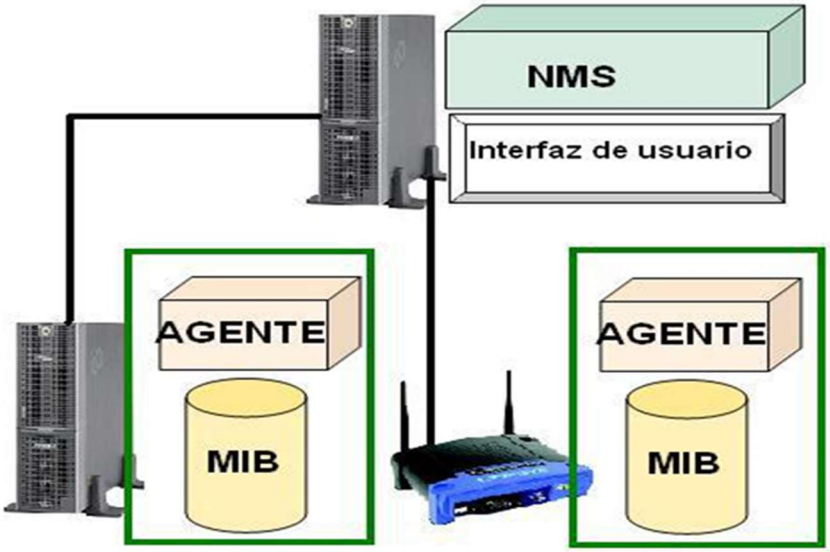
- SNMP. Por su sigla en inglés (Simple Network Management Protocol), es un protocolo de la capa de aplicación, su función en facilitar la comunicación y el intercambio de datos administración entre los dispositivos de red. Estos dispositivos generalmente son los routers, switches, servidores, estaciones de trabajo etc. Que soportan este protocolo. El protocolo permite a los administradores de red supervisar el desempeño, buscar y resolver los problemas presentados en cada uno de los dispositivos de la red de datos así como planificar un incremento o crecimiento de la red.

- NMS (Network Management Systems, NMS), por su sigla en inglés Sistema Administrador de Red, es el encargado de ejecutar aplicaciones para supervisar y controlar los dispositivos que son administrados en la red. Se encarga también de determinar el volumen de recursos de procesamiento y memoria requeridos para la administración de la red.

- Dispositivo Administrado: También llamados componentes de red puede ser cualquier dispositivo que participe en el funcionamiento de la red (routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras). Estos contienen información que puede ser puesta a disposición de los NMS.

- Agente: Es una aplicación o software de administración de red contiene información de la administración de los dispositivos administrados, la traduce y la pone a disposición del SNMP.

Figura 4 Arquitectura SNMP



Fuente: https://velezconde.wordpress.com/herramientas-para-gestion-y-monitoreo/

5.2.1 Áreas funcionales de la Gestión de red. La gestión de una red de datos se puede categorizar en cinco fases:

- Gestión de fallos (Fault): Sus funciones en mantener la red funcionando correctamente, buscando anteponerse a los fallos que pueda presentar la red en cualquiera de sus componentes.

  Ante un fallo se tiene que actuar así:

  - Diagnosticar de forma rápida donde se presentó el fallo.
  - Aislar a la red del fallo, reconfigurándola de forma que el impacto que ocasiona el fallo sea el menor posible.
  - Resolver en el menor tiempo posible de forma que la red

- Gestión de configuración (Configuration). Muchos de los componentes de las redes pueden ser configurados para realizar diferentes funciones, por ejemplo, un nodo puede actuar como router o como host, se pueden variar los temporizadores de transmisión en el nivel de transporte.

- Gestión de la contabilidad (Accounting). En todas las redes de datos es importante mantener un registro del uso que los usuarios hacen de la red.

  En las redes corporativas, se utiliza para distribuir el gasto entre departamentos, vigilar el uso excesivo que hacen de ellas ciertos usuarios y determinar cómo este uso puede perjudicar a los demás, para planificar el futuro de la red su crecimiento y distribución de los recursos de la red.

  Que debe Monitorizarse:

  - Recursos de comunicaciones LANs, WANs, líneas dedicadas.

  - Hardware

  - Software y Aplicaciones

  - Servicios de información ofrecidos en la red

- Gestión de las presentaciones (Performance): Su función es la monitorización de las presentaciones de la red para comprobar que están dentro de los límites permisibles de esta forma realizar operaciones de control para mejorarlas. Un ejemplo sería monitorizar el porcentaje de utilización, tráfico cursado y tiempos de respuesta.

- Gestión de la seguridad (Security). Se ocupa de gestionar la distribución y mantenimiento de claves para encriptación, gestionar los mecanismos de control de acceso monitorización del acceso a las máquinas de la red y a la propia información de gestión su herramienta más importante es el Log.

5.2.2 Monitorización. La información de Monitorización se puede clasificar en:

- Estática: Se trata de la información de la red que no cambia frecuentemente como la configuración de la red y los dispositivos que la conforman.

- Dinámica: Esta información está relacionada con los eventos de la red, que cambian frecuentemente.

- Estadística: Es la información derivada de la dinámica, y sirve para la medición de eventos en la red.

5.2.3 Elementos de un Sistema de Monitorización. Existen tres elementos integrantes de un sistema de monitorización:

- Aplicación de Monitorización: necesita de los datos monitorizados. puede ser de cualquier área funcional.

- Función Gestora: Realiza la función básica de obtener los datos de monitorización para la aplicación.

- Función Agente: Recolecta y almacena la información de monitorización para facilitarla al gestor.

5.2.4 Información De Monitorización. En el proceso de monitorización intervienen muchos tipos de datos que se debe considerar y analizar:

- Agente Monitorizador. Genera agregaciones y análisis estadísticos de la información, si no está junto al gestor toma el papel de agente para comunicarse con él.

- Polling. Es una forma de control en las redes de datos de nivel local, está basada en una serie de mensaje de petición/ respuesta entre gestor y agentes.

- El gestor. Solicita la información a cualquier elemento de la red solicitando información que cumpla con los criterios establecidos por el.

- Monitorización de prestaciones. Selecciona los medidores apropiados para los componentes de la red, no todos los medidores son iguales por lo tanto debe categorizarlos por fabricantes, aunque hay algunos medidores que son genéricos para todos los fabricantes.

- Tiempo de Respuesta. Un menor tiempo de respuesta requiere una mejor disponibilidad de recursos, tanto de hardware como de red por lo tanto genera un incremento en los costos. Conviene realizar mediciones separadas de los elementos que intervienen en la red para detectar cuellos de botella.

- Disponibilidad. La disponibilidad se puede medir la confiabilidad de los componentes que normalmente se calcula dividiendo el tiempo medio entre fallos y el tiempo promedio para reparar.

- Troughput. Es la tasa promedio de éxito en la entrega de un mensaje sobre un canal de comunicación. Conviene monitorizar las llamadas atendidas, las transacciones realizadas, como forma de prever posibles problemas de prestaciones.

- Utilización. Busca detectar atascos o cuellos de botella y áreas de importante congestión. Con un alto grado de utilización el tiempo de respuesta se comporta exponencialmente.

5.2.5 Monitorización de Fallos. En la monitorización de fallos podemos encontrar tres tipos de fallos:

- Fallos Inobservables: Hay fallos que no se pueden observar por que el equipo que los presenta no tiene los mecanismos para identificarlos.

- Fallos parcialmente observables: Aunque se pueden identificar u observables es difícil identificar su causa.

- Incertidumbre en la Observación: aunque tengamos el fallo correctamente identificado su causa se puede dar en muchos parámetros.

5.2.6 Generaciones de ataques a las redes de datos. Existen tres generaciones de ataques a las redes de datos:

- Primera generación. Ataques físicos. Estos ataques se centralizan en los componentes electrónicos, computadoras, cables, tarjetas, concentradores swichs, routers entre otros dispositivos de red.

- Segunda generación. Ataques sintácticos. Son ataques contra la lógica operativa de las computadoras y las redes, buscan vulnerabilidades existentes en software, algoritmos de cifrados y protocolos.

- Tercera generación. Ataques semánticos. Estos ataques son los que se aprovechan de la confianza de los usuarios en la información. Este tipo de ataques pueden ir desde la introducción de información falsa, hasta la modificación del contenido de los datos en servicios con datos confidenciales.

5.2.7 Estructura De La Gestión De Red. El objetivo genérico de un sistema de gestión de red es proporcionar una plataforma de gestión distribuida para todo tipo de entornos de red con las siguientes características.

- Monitorear el estado actual de la red y su funcionamiento y responder a los comandos del computador que controla la red.

- Proporcionar un filtrado inteligente de las alarmas, que ayude a minimizar el tiempo requerido para localizar fallos.

- Aislar errores, de una manera automática, tanto de hardware como de software.

- Generar tráfico para simular condiciones reales en la red y realizar pruebas de funcionamiento.

- Adoptar acciones correctoras que ayuden al personal encargado de la red a solucionar problemas.

- Presentar información de la configuración, dando así una perspectiva más amplia de la red.

- Recoger y analizar datos de gestión muy valiosos, que permitan hacer una planificación de la red a corto y largo plazo.

- Almacenar estadísticas sobre el funcionamiento de la red.

- Formular aquellas recomendaciones útiles para el usuario.

La gestión de red se lleva a cabo mediante una aplicación software residente en el computador designado como Gestor de la red que, mediante una interface de operador, permite la gestión, y otras residentes en cada uno de los elementos que conforman la estructura de la red, es decir nodos y medios de transmisión.
Según el modelo ISO en su documento norma ISO 7498-42.1, hay cinco funciones de gestión de red:

- Gestión de la Configuración: Registrar y mantener la configuración de la red, la actualización de parámetros para garantizar un funcionamiento correcto de la red.

- Gestión de fallos: Detección y reparación de problemas o errores de la red.

- Gestión de la Seguridad: Control del proceso de acceso de mensajes en la red. Proporcionar protección a los recursos de red, servicios y datos para evitar el peligro. También proporciona la privacidad del usuario.

- Performance Management: Incluye la medición del rendimiento de hardware, software y los medios de transmisión en la red.

- Contabilidad de gestión: Controlar los usuarios de tarificación por el uso personal de registro de uso de la red, y ofrecer un servicio necesario para los usuarios de la red.

5.2.8 Administración del rendimiento. Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado. La administración del rendimiento se divide en 2 etapas: monitoreo y análisis

5.2.9 Monitoreo. Consiste en observar y recolectar la información referente al comportamiento de la red en aspectos como los siguientes:

- Utilización de enlaces: Se refiere a las cantidades ancho de banda utilizada por cada uno de los enlaces de área local (Ethernet, Fastethernet, Gigabit Ethernet, etc.), ya sea por elemento o de la red en su conjunto.

- Caracterización de tráfico. Es el trabajo de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red, como http, ftp, que son más utilizados. Además, esto también permite establecer un patrón en cuanto al uso de la red.

- Porcentaje de transmisión y recepción de información. Encontrar los elementos de la red que más solicitudes hacen y atienden, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos y servicios.

- Utilización de procesamiento. Es importante conocer la cantidad de procesador que un servidor está consumiendo para atender una aplicación. Esta propuesta considera importante un sistema de recolección de datos en un lugar estratégico dentro de la red, el cual puede ser desde una solución comercial como Spectrum o la solución propia de la infraestructura de red, hasta una solución integrada con productos de software libre.

5.2.10 Análisis. Una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y

tomar decisiones adecuadas que ayuden a mejorar su desempeño. En el proceso de análisis se pueden detectar comportamientos relacionados a lo siguiente:

- Utilización elevada. Si se detecta que la utilización de un enlace es muy alta, se puede tomar la Decisión de incrementar su ancho de banda o de agregar otro enlace para balancear las cargas de tráfico. También, el incremento en la utilización, puede ser el resultado de la saturación por tráfico generado maliciosamente, en este caso se debe contar con un plan de respuesta a incidentes de seguridad.

- Tráfico inusual. El haber encontrado, mediante el monitoreo, el patrón de aplicaciones que circulan por la red, ayudará a poder detectar tráfico inusual o fuera del patrón, aportando elementos importantes en la resolución de problemas que afecten el rendimiento de la red.

- Elementos principales de la red. Un aspecto importante de conocer cuáles son los elementos que más reciben y transmiten, es el hecho de poder identificar los elementos a los cuales establecer un monitoreo más constante, debido a que seguramente son de importancia. Además, si se detecta un elemento que generalmente no se encuentra dentro del patrón de los equipos con más actividad, puede ayudar a la detección de posibles ataques a la seguridad de dicho equipo.

- Calidad de servicio. Otro aspecto, es la Calidad de servicio o QoS, es decir, garantizar, mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, retardo, a aplicaciones que requieren de un trato especial, como lo son la voz sobre IP (VoIP), el video sobre IP mediante H.323, etc.

- Control de tráfico. El tráfico puede ser reenviado o ruteado por otro lado, cuando se detecte saturación por un enlace, o al detectar que se encuentra fuera de servicio, esto se puede hacer de manera automática si es que se cuenta con enlaces redundantes.

5.2.11 Metodología y técnicas de monitoreo. Para desarrollar este punto se propone seguir la metodología en el cual se plantea que para prestar un mejor servicio a los usuarios se debe realizar un monitoreo oportuno de fallas, bajo el cual radica la importancia de tener acceso a informes periódicos, para lo cual se contó principalmente con los enfoques activo y pasivo; sus técnicas, así como la estrategia

de monitoreo, incluyendo la definición de métricas y la selección de las herramientas.

5.2.11.1 *Monitoreo Activo*. Es un monitoreo que se basa en el envío de paquetes de prueba en la red, permitiéndonos evaluar en diferentes puntos, determinadas aplicaciones, y midiendo sus tiempos de respuesta tanto de llegada o como de salida. . Este enfoque tiene la característica de agregar tráfico en la red y es empleado para medir el rendimiento de la misma.

Técnicas de Monitoreo activo:

Basado en ICMP

- Diagnosticar problemas en la red.
- Detectar retardo, pérdida de paquetes.
- RTT
- Disponibilidad de host y redes. Basado en TCP
- Tasa de transferencia.
- Diagnosticar problemas a nivel de aplicación Basado en UDP
- Pérdida de paquetes en un sentido (one – way)

5.2.11.2 *Monitoreo Pasivo*. Esta técnica es utilizada para obtener estadísticas sobre la utilización de ancho de banda en los dispositivos de red, para ello se requiere tener acceso a dichos dispositivos. Al mismo tiempo, este protocolo genera paquetes llamados traps que indican que un evento inusual se ha producido.

“En este tipo de ataques el intruso no altera la comunicación, si no que únicamente la escucha o la monitoriza, para obtener la información que está siendo transmitida.”[5]

Técnicas de monitoreo pasivo:

- Solicitudes remotas:
- Mediante SNMP:

5.2.11.3 *Captura de tráfico*. Se puede realizar de dos formas:

- Mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que se recibe en un puerto hacia otro donde estará conectado el equipo que realizará la captura.

- Mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra. Esta técnica es utilizada para contabilizar el tráfico que circula por la red.

5.2.11.4 *Análisis de tráfico*. Se utiliza para caracterizar el tráfico de red, es decir, para identificar el tipo de aplicaciones que son más utilizadas. Se puede implementar haciendo uso de dispositivos de prueba que envíen información mediante RMON o a través de un dispositivo intermedio con una aplicación capaz de clasificar el tráfico por aplicación, direcciones IP origen y destino, puertos origen y destino, etc.

5.2.11.5 *Herramientas De Monitorización Y Análisis Del Tráfico En redes De Datos*. Existen varios tipos de herramientas que se encargan del monitoreo y análisis de la red. En particular, los denominados sniffers son de gran utilidad. En la actualidad sniffer es una denominación aceptada para aquellas herramientas cuya función principal es monitorizar y analizar tráfico, o sea, examinar paquetes, protocolos y tramas enviadas a través de la red. La captura y visualización de las tramas de datos por sí sola puede no ser muy útil o eficiente, es por ello que los analizadores de protocolos también muestran el contenido de los datos de los

[5] Medina, José Manuel. [En Línea]. “Seguridad en Redes” https://core.ac.uk/download/pdf/16307906.pdf [Citado en 2013]

paquetes. Teniendo los paquetes de datos y la información del flujo de tráfico, los administradores pueden comprender el comportamiento de la red.

5.2.11.6 *Características comunes de los aplicativos de monitorización de red*. Existe una buena cantidad de sniffers en el mercado que ofrecen determinadas prestaciones, de las cuales se mencionan a continuación las más relevantes para la gestión de la red:

- Escucha de tráfico en redes LAN (Local Area Network) y WLAN (Wireless LAN).

- Captura de tráfico a través de las diferentes interfaces de red de la computadora.

- Capacidad de examinar, salvar, importar y exportar capturas de paquetes en diferentes formatos de captura, tales como: PCAP (Packet Capture), CAP, DUMP, DMP, LOG.

- Comprensión de protocolos de las diferentes capas de la arquitectura de comunicaciones, como por ejemplo: DHCP (Dynamic Host Configuration Protocol), GRE (Generic Routing Encapsulation), TCP (Transmission Control Protocol), entre otros.

- Aplicación de filtros para limitar el número de paquetes que se capturan o se visualizan.

- Cálculo de estadísticas y gráficas detalladas con indicadores como paquetes trasmitidos y perdidos, velocidad promedio de transmisión, gráficos de flujo de datos, entre otras.

- Detección de los nodos que se encuentran en la red, ofreciendo información como sistema operativo, fabricante de la interface, entre otras. Reconstrucción de sesiones TCP.

- Análisis y recuperación de tráfico VoIP (Voice over IP).

- Generan reportes de tráfico en tiempo real y permiten configurar alarmas que notifiquen al usuario ante eventos significativos como paquetes sospechosos, gran utilización del ancho de banda o direcciones desconocidas (LC Rey, 2012).

5.3 **MARCO LEGAL**

- La Ley Estatutaria 1581 del 17 de octubre de 2012: Establece las condiciones mínimas para realizar el tratamiento legítimo de los datos personales de los clientes, empleados y cualquier otra persona natural. El literal k) del artículo 17 de dicha ley obliga a los responsables del tratamiento de datos personales a adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la citada ley y en especial, para la atención de consultas y reclamos.

- La ley 1273 de 2009: Incurre en el delito de violación de datos personales quien "sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes".[6]

- Código Penal Art. 255: Sanciona a quien sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público. Si el culpable fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

- Ley N° 24.624. Artículo 30: Autoriza el archivo y la conservación en soporte electrónico u óptico indeleble de la documentación financiera, de personal y de control de la Administración Pública Nacional y otorga valor jurídico y probatorio a la documentación existente que se incorpore al Archivo General de la Administración, mediante la utilización de tecnología que garantice la estabilidad, perdurabilidad, inmutabilidad e inalterabilidad del soporte de guarda físico de la mencionada documentación.

[6] MINTIC. [En Línea]. "Ley 1273 de 2009" http://www.mintic.gov.co/portal/604/w3-article-3705.html [s.f]

- Instituto Nacional Americano de Estándares (ANSI): Es una organización sin fines de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos. ANSI es miembro de la Organización Internacional para la Estandarización (ISO) y de la Comisión Electrotécnica Internacional (International Electrotechnical Commission, IEC). La organización también coordina estándares del país estadounidense con estándares internacionales, de tal modo que los productos de dicho país puedan usarse en todo el mundo.

5.4 **MARCO CONTEXTUAL**

5.4.1 Razón Social: SOCIEDAD CLÍNICA EMCOSALUD

5.4.2 Tipo de Negocio: La sociedad Clínica Emcosalud es una empresa privada dedicada a la prestación de servicios de salud.

5.4.3 Sector Comercial: Pertenece al sector salud, es una empresa prestadora de servicios de salud.

5.4.4 Reseña Histórica: La Empresa Cooperativa de Servicios de Salud EMCOSALUD, nace el nueve de mayo de 1986, dentro del proceso de integración cooperativa y por la necesidad de ofrecer una alternativa solidaria en la prestación de servicios de salud a la población asociada y vinculada al sector, en el marco del antiguo SNS (Sistema Nacional de Salud), con el aporte de las cooperativas Emcofun, Utrahuilca, Fondo de Empleados del Departamento, Coomagisterio, Emcoven, Cooperhuila, Cooptelepostal, Coopelectrohuila, Cootrainem y Cootrapal. Ante el crecimiento de la población a atender, Emcosalud abre su radio de acción y cobertura, y el 27 de abril de 1999, alcanza el propósito de tener Clínica propia dotada con equipos con tecnología de punta que la constituyeron en una de las mejores del sur colombiano.

5.4.5 Misión: Somos una Institución Prestadora de Servicios de Salud, de carácter privado, que propende por el mejoramiento de la calidad de vida de las personas y de la colectividad del Sur Colombiano, mediante acciones de promoción de la salud, prevención, tratamiento y rehabilitación de la enfermedad, suministrando servicios eficientes y de calidad de acuerdo con nuestra capacidad científica y tecnológica, propiciando el crecimiento institucional y el desarrollo integral del cliente interno y externo.

5.4.6 Visión: Nos proponemos ser la empresa con la mejor infraestructura física y tecnología para la atención de usuarios que no permita ejercer un liderazgo en la Región Sur Colombiana y a nivel nacional, logrando innovación permanente, mejoramiento continuo y gestión humana, tanto en el ámbito técnico, administrativo y financiero como en la calidad del servicio, promocionando el trabajo en equipo y el desarrollo del recurso humano comprometido con la institución.

5.4.7 Servicios Ofrecidos: La sociedad Clínica Emcosalud cuenta con un amplio portafolio de servicios para sus pacientes:

- Urgencias: Atención integral y multidisciplinaria al paciente que presenta una urgencia de origen médico o quirúrgico, de manera amable, oportuna, científica y técnica con el apoyo de un equipo humano altamente especializado y entrenado. Médicos generales cubren el servicio las 24 horas del día, además presencia permanente de pediatría, ginecobstetricia y medicina interna en horario diurno y se encuentran adscritas todas las especialidades y subespecialidades médicas y quirúrgicas de disponibilidad, con una respuesta máxima de una hora al llamado.

- Hospitalización: Es una unidad de atención médica dedicada a la prestación de servicios de internación en un ambiente de hotelería, confort, calidad humana, excelencia médica y técnico - científica. La Clínica Emcosalud ofrece como disponibilidad hotelera: Habitaciones unipersonales, bipersonales y compartidas.

- Cirugía: Cirugía general y especializada, urgente y programada durante 24 horas continúas. Se dispone de una (1) sala de partos y tres (3) quirófanos dotados con la más alta tecnología.

- Laboratorio Clínico: Realización de exámenes las 24 horas de todos los niveles de complejidad para pacientes ambulatorios y hospitalarios, totalmente sistematizado y automatizado.

- Imagenología: Alta calidad humana sumada a la calidad de los equipos para garantizar excelentes resultados en el campo diagnóstico: Radiología intervencionista, radiologías convencionales, ecografía convencional, ecografía

doppler, tomografía computarizada helicoidal multicorte, mamografía, radioscopia, ecocardiografía.

- UCI Adultos: Unidad de atención médico hospitalaria para el paciente en estado crítico, con recurso humano altamente especializado, y con la mejor estructura física y tecnológica. Instalaciones amplias con cubículos confortables e independientes que permiten dar una atención individual a cada paciente.

- UCI Neonatal: Tres cubículos amplios con capacidad para 18 pacientes (5 críticos, 5 de cuidado intermedio y 8 de cuidado básico) dotados para un cuidado óptimo del neonato.

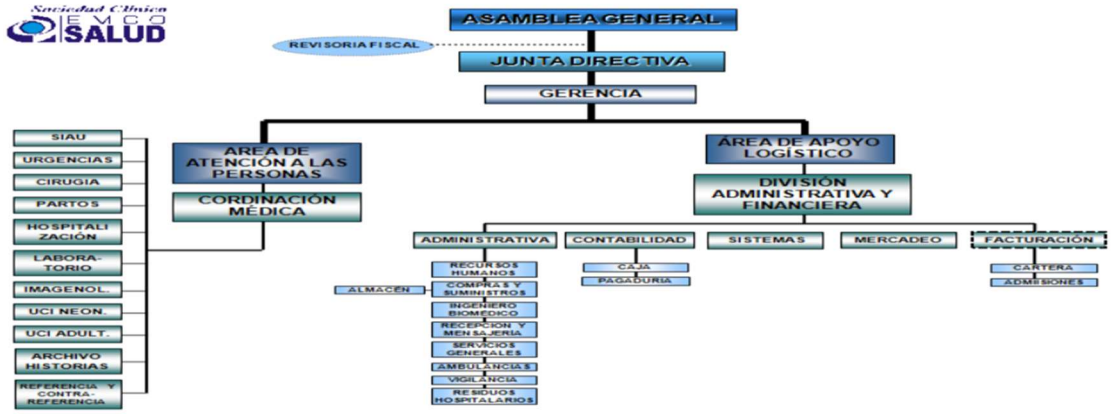
- Terapia Respiratoria: Consultorio de terapia respiratoria con los más modernos equipos para tratamientos respiratorios.

- Consulta Especializada: Contamos con los servicios de los mejores profesionales en todas las ramas de la medicina para atención oportuna a nuestros pacientes.

- Servicio de Ambulancia: Tres Básicas y una Medicalizada las 24 horas del día.

5.4.8 Organigrama Sociedad Clínica Emcosalud

Figura 5 Organigrama



Fuente: Manual C.I.E.

5.4.9 Logo Empresarial

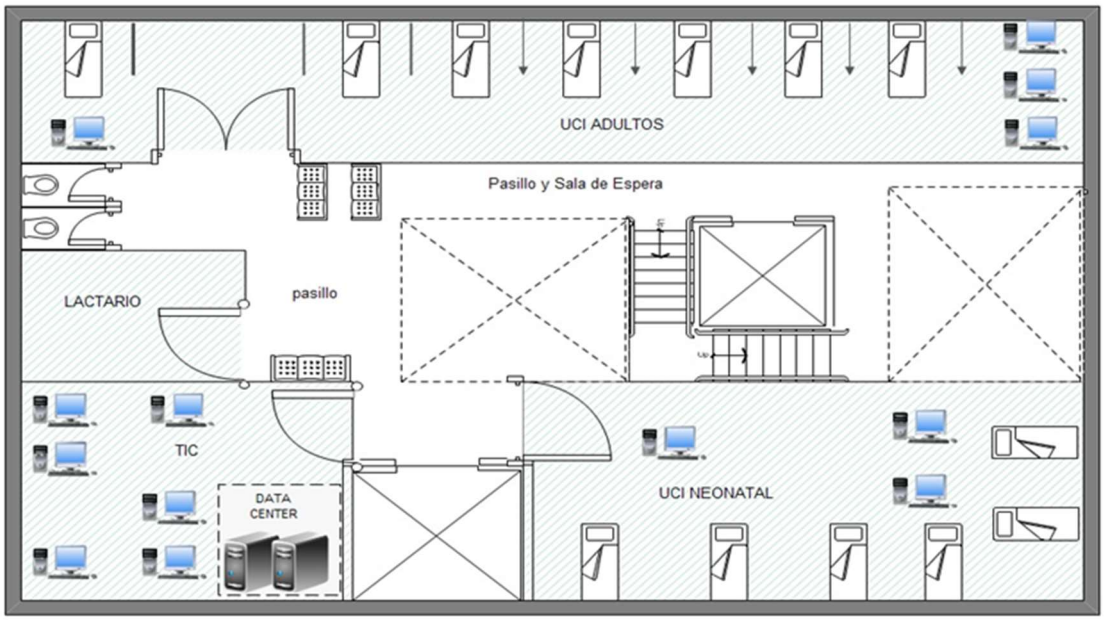
Figura 6 Logo Empresarial

Fuente: Manual C.I.E.

5.4.10 Planos Físicos Edificio, Ubicación equipos de computo

5.4.10.1 *Quinto Piso*:

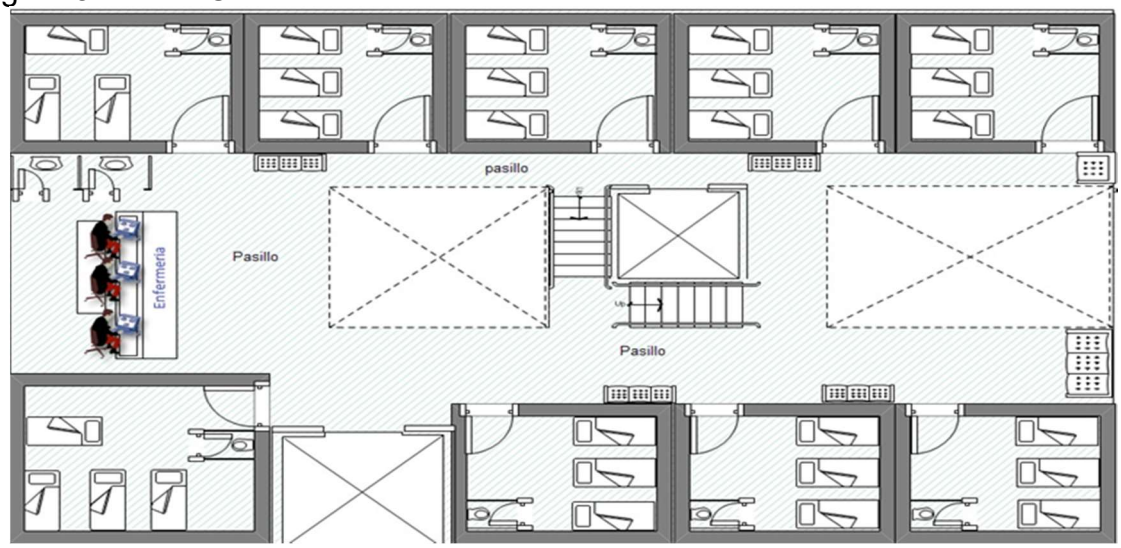
Figura 7 Planos Quinto Piso



Fuente: Los autores

5.4.10.2 *Cuarto Piso*:

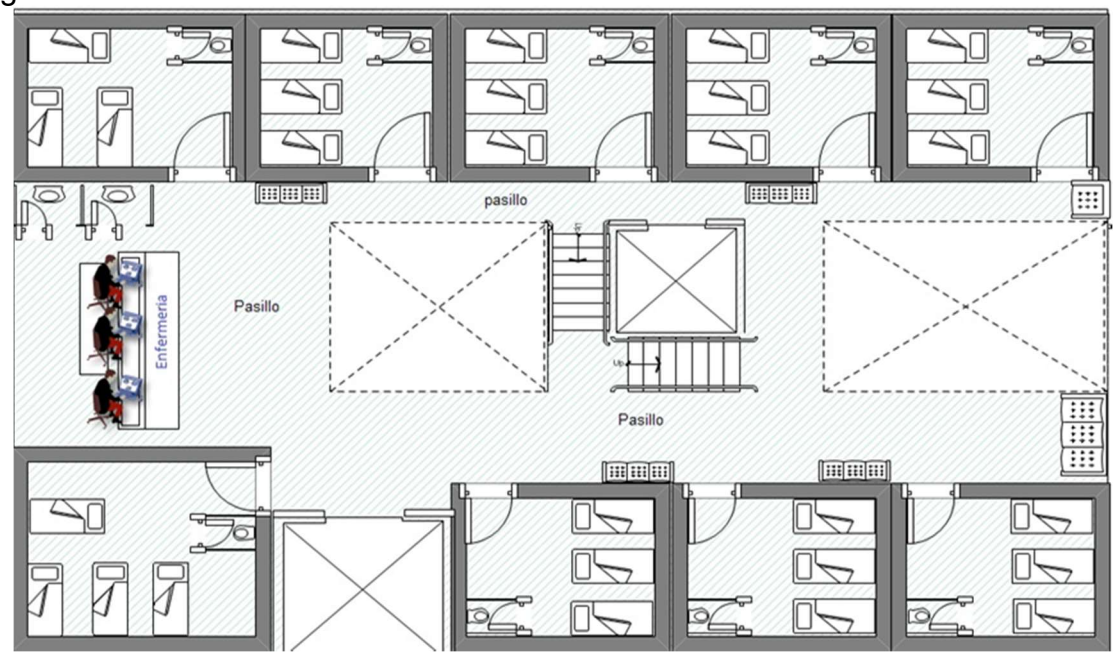
Figura 8 Planos Cuarto Piso



Fuente: Los autores

5.4.10.3 *Tercer Piso*:

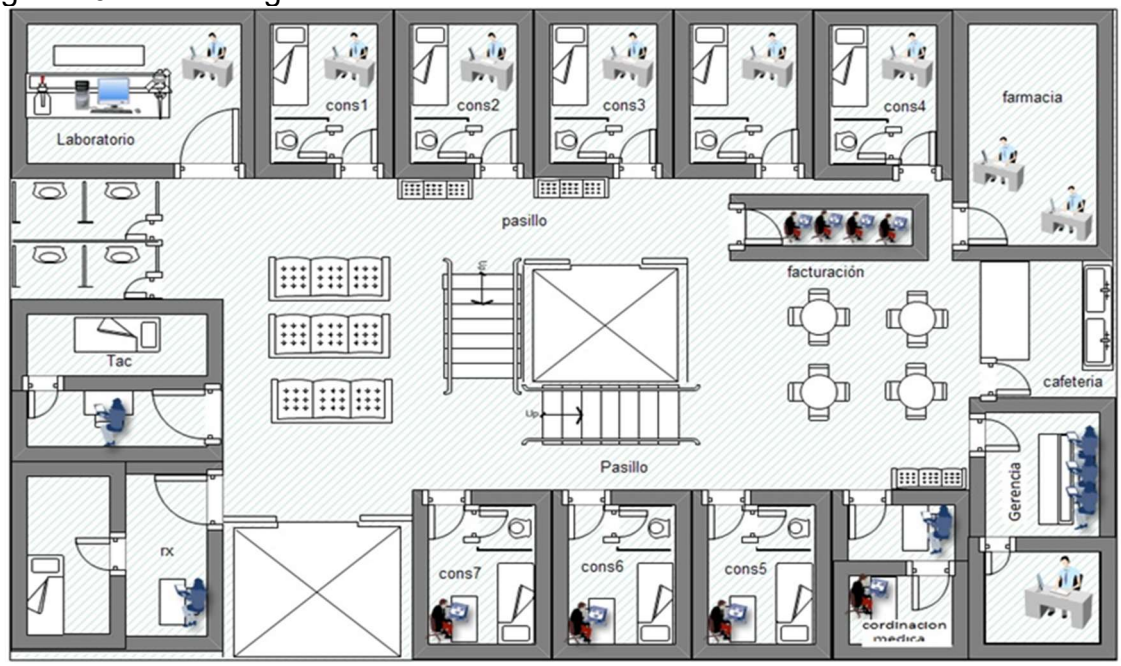
Figura 9 Planos Tercer Piso



Fuente: Los autores

5.4.10.4 *Segundo Piso*:

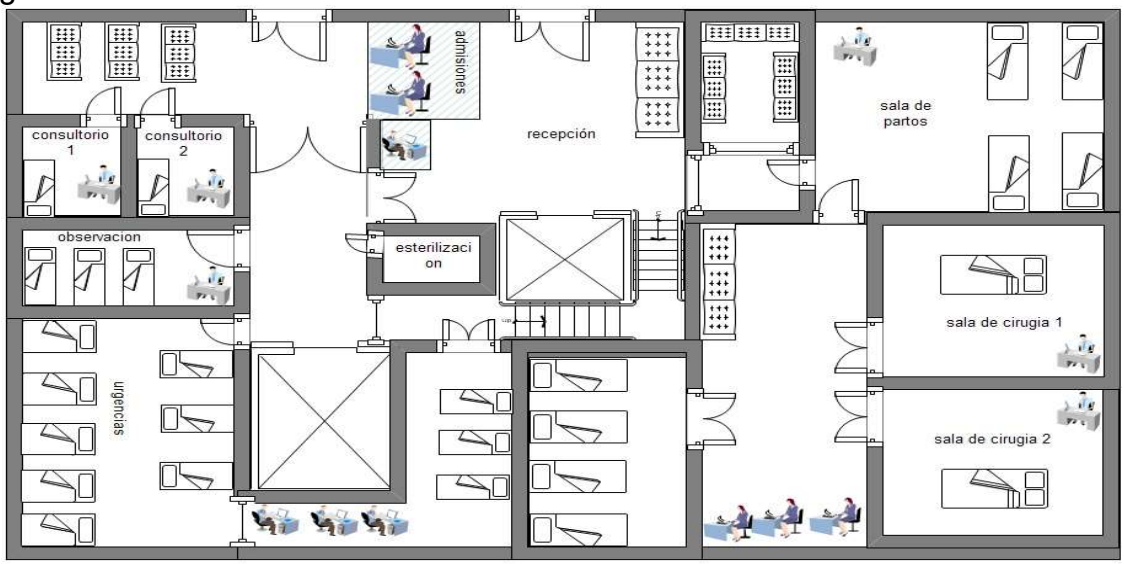
Figura 10 Planos Segundo Piso



Fuente: Los autores

5.4.10.5 *Primer Piso*:

Figura 11 Planos Primer Piso



Fuente: Los autores

6. METODOLOGÍA DE DESARROLLO

Para el desarrollo de la investigación se efectuaron los siguientes pasos.

- Análisis de las condiciones físicas y topológicas de la red de datos.
- Definición de los dispositivos y servicios de red.
- Determinación de los requerimientos y principales problemas de monitoreo de la red existente.
- Identificar herramientas para el monitoreo y control de la red.
- Selección de la mejor alternativa para realizar la gestión de diagnóstico y monitoreo de la red.
- Diseño del servidor.
- Programación y configuración del servidor en la estación principal.
- Implementación del servidor para el control de dispositivos y servicios de la red de datos.
- Evaluación de las posibles fallas que tenga el servidor y comprobación de su correcto funcionamiento.

6.1 METODOLOGÍA DE INVESTIGACIÓN

La presente es una investigación aplicada, que se desarrolla utilizando:

- Investigación bibliográfica, porque la explicación científica de las variables del tema de investigación se realizó consultando en libros de electrónica, revistas, publicaciones y artículos científicos disponibles en línea referentes a la programación de dispositivos de red y herramientas que permitan realizar la gestión de diagnóstico y monitoreo de la red de datos. Siendo el proceso más adecuado para obtener información.

- Investigación de campo, mediante el método de observación para lo cual se realizó un estudio sistemático de los hechos en el lugar en que se produce los acontecimientos. Con esta modalidad se dará contacto en forma directa con la realidad, para tener información de acuerdo con los objetivos del proyecto.

6.2 PLAN DE RECOLECCIÓN DE LA INFORMACIÓN

La recolección de información se inició previa a la visita de reconocimiento y presentación del proyecto de investigación, utilizando como recurso entrevista y fichas de observación. Es importante aclarar que la identificación de la empresa se hizo previamente en el inicio de la propuesta en consecuencia no se va a referenciar nada en la etapa de ejecución de la propuesta.

6.3 PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN

Una vez que sea obtenida la información apropiada de la investigación, esta formará parte de un proceso estadístico, el cual consiste en la tabulación de los datos, de forma ordenada y sistemáticas.

La revisión y la codificación de los resultados permitieron detectar los errores, omisiones y eliminar respuestas contradictorias de manera organizada para facilitar la tabulación

7. PRODUCTO A ENTREGAR

Al finalizar el proyecto se entregará un informe escrito con los hallazgos en seguridad identificados en el diagnóstico de la red de datos de la empresa Sociedad Clínica Emcosalud, y las recomendaciones de alternativas a tener en cuenta para solucionarlas.

También se entregará un informe contextual de la herramienta de monitoreó de redes más apropiada para implementar en la Sociedad Clínica Emcosalud, en el cual se describa los beneficios que este puede brindar a la entidad.

Es de aclarar que el alcance del proyecto no contempla implementación de ninguna herramienta de monitoreo ni de ninguna configuración para hacer mejoras en la red. Solo está contemplado el estudio de debilidades, recomendaciones de solución y determinación del software más apropiado en el tema de monitorización de la red de datos

8. DESARROLLO DEL PROYECTO

Levantamiento de la información pertinente para la ejecución del proyecto.

Se inició la elaboración del proyecto mediante entrevistas realizadas al personal encargado de tecnología en la empresa y se solicitaron datos importantes para el proyecto como inventarios de activos, documentación de procesos realizados obteniendo los siguientes resultados:

8.1 ANÁLISIS ESTADO ACTUAL DE RECURSOS TECNOLÓGICOS SOCIEDAD CLÍNICA EMCOSALUD

8.2 INVENTARIO DE EQUIPOS TECNOLÓGICOS

La sociedad Clínica Emcosalud en la actualidad cuenta con inventario de equipos tecnológicos un poco desactualizados que son administrados por el personal de la oficina de tecnología a continuación se relaciona en la siguiente tabla:

Tabla 1. Inventario de equipos

T. EQUIPO	MARCA	MODELO	SERIAL_PC
ACCESS POINT	UNIFI	UAP-LR	0418d666654E
IMPRESORA	SAMSUNG	ML-1865W	Z5RNBKABC00099H
IMPRESORA	SAMSUNG	ML-1865W	Z5RNBKABC00094X
PC DESKTOP	HP	HP COMPAQ 8000 ELITE	MXJ0050%42H
PC DESKTOP	HP COMPAQ	DX2400	MXL93207SH
PC DESKTOP	HP COMPAQ	HP COMPAQ 8000 ELITE	MXJ00906MJ
PC DESKTOP	COMPAQ	PRESARIO SR1717LA	MXK6090YP2
PC DESKTOP	CLON	CLON	NO TIENE
PC DESKTOP	HP	HP COMPAQ 8000 ELITE	MXJ0050%41S
PC DESKTOP	LENOVO	7483B24	1S7483B24MJAYT93

PC DESKTOP	LENOVO	7483B24	1S7483B24MJAYV72
PC PORTATIL	DELL	STUDIO XPS	FS3CLL1
PC PORTATIL	DELL	INSPIRON 6400	27M35D1
PC DESKTOP	HP	4300	MXL32812LJ
RADIO	COBRA	MICRO TALK	T531067025
RADIO	COBRA	MICRO TALK	T510042735
RADIO	COBRA	MICRO TALK	T510042645
RADIO	COBRA	MICRO TALK	T531065676
ROUTER	CISCO	2800	FTX1244A14R
ROUTER	TP-LINK	TL-WA5110G	POR VERIFICAR
ROUTER	CISCO	WRT120N	JUT00K705836
SERVIDOR	SUPERMICRO		C51200527D00136
SERVIDOR	IBM	NETFINITY 5100	987654321 (23A0169)
SWITCH	ENCORE	ENH924-CX	588712120000106

Fuente: Los autores

8.3 **PERSONAL DE AREA TECNOLOGÍA**

Tabla 2. Personal Tecnología

CARGO	PERFIL
Jefe de sistemas	Titulación en Ingeniería de Sistemas
Ingeniero de Soporte Software	Titulación en Ingeniería de Sistemas, tener conocimientos en programación y bases de datos.
Ingeniero de Soporte Hardware	Titulación en Ingeniería de Sistemas, conocimientos en redes, mantenimientos de hardware.
Auxiliares de Sistemas	Técnicos en Sistemas

Fuente: Los Autores

8.4 **SOFTWARE Y APLICACIONES**

Tabla 3. Software y Aplicaciones

SOFTWARE	TIPO LICENCIA
Sistema de Información Asistencial E-salud	Pagada
Sistemas Operativos Windows 2003 server	Pagada

Sistemas Operativos Windows 8.1	Pagada
Sistemas Operativos Windows 10	Pagada
Herramientas ofimática Office 2013	Pagada
Aplicativo de comunicación interna Spark	Gratis
Sistema de Información Contable SIIGO	Pagada
Sistema de reporte de morbilidad RUAF	Gubernamental
Sistema de afiliación de paciente Macrwma	Privada
Antivirus Avas free	Libre

Fuente: Los Autores

8.5 DOCUMENTACIÓN, POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, MÉTODOS Y PROCESOS

En este punto se contó con la colaboración oportuna del personal de tecnología el cual nos facilitó la documentación correspondiente a los activos de información, que son componentes de la red de datos de la Sociedad Clínica Emcosalud o que guardan alguna relación con la ella o con su seguridad.

8.5.1 Políticas de Seguridad de la Información: La Sociedad Clínica Emcosalud no cuenta con políticas de seguridad definidas, lo único que tiene documentado para tal fin son dos capítulos del reglamento interno de trabajo los cuales se describen a continuación:

CAPITULO XVII PROHIBICIONES ESPECIALES PARA LA EMPRESA Y LOS TRABAJADORES

ARTÍCULO 69. Se prohíbe a los Trabajadores.

Inciso 5. Sustraer de las dependencias de la Empresa los materiales o elementos de trabajo así como documentos que son de uso privativo de interés exclusivo de la misma.

Inciso 11. Disponer los bienes, equipos, herramientas de trabajo, Software, documentos, bibliografías, textos, así como de servicios de la Empresa o que se encuentren dentro o fuera de su custodia para otros fines y/o cuando estos no sean inherentes al ejercicio de las actividades propias y función empresarial de la Empresa.

Inciso 13. Dañar intencionalmente los inmuebles, infraestructura sanitaria, instalaciones, vehículos, maquinaria, equipos, instrumentos, documentación, materias primas, y demás bienes de propiedad de la Empresa.
Inciso 14. Ocuparse en cosas distintas de sus labores durante las horas de trabajo, sin previo permiso del superior inmediato.

Inciso 17. Retirar de los archivos o dar a conocer documentos sin autorización escrita de la Gerencia General.

Inciso 19. Rendir información, declaración o dictamen falsos que atenten contra los intereses de la Empresa o le causen trastornos en sus actividades.

PARAGRAFO: se atiene de igual manera a lo establecido en el artículo 17 de la ley 1474: El que como empleado, asesor, directivo o miembro de una junta u órgano de administración de cualquier entidad privada, con el fin de obtener provecho para sí o para un tercero, haga uso indebido de información que haya conocido por razón o con ocasión de su cargo o función y que no sea objeto de conocimiento público, so pena de las obligaciones penales que estipula el mismo artículo.

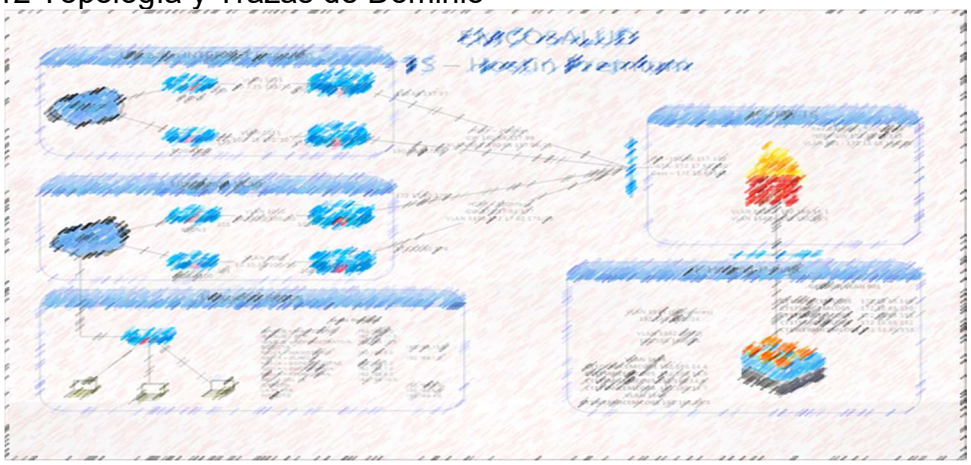
Inciso 22. Confiar a otro trabajador la ejecución del trabajo asignado, sin permiso expreso de la Empresa.

Inciso 23. No utilizar su cargo o función con fines de lucro ni recibir dádivas o compensaciones por gestiones que realice en su desempeño.

Inciso 24. Es de obligatorio cumplimiento la observancia de las herramientas tecnológicas para uso exclusivo de la actividad laboral.

8.6 TOPOLOGÍA Y TRAZAS DEL DOMINIO EMCOSALUD

Figura 12 Topología y Trazas de Dominio



Fuente: Los Autores

8.7 **PROCESOS Y MÉTODOS**:

Según entrevistas realizadas al personal de tecnología los procesos que se realizan son correctivos a eventualidades presentadas esporádicamente no hay un cronograma con procesos programados para mantenimiento, revisión y diagnóstico de la red.

No se han establecido métodos de revisión, mantenimiento, ingreso, diagnósticos, cambios, etc. En la infraestructura de la red de datos todo se hace de manera inmediata sin programación ante los fallos presentados.

El croquis de la red de la empresa en estos momentos es obsoleto ya que se han hecho muchas remodelaciones físicas al edificio, han ingresado nuevos funcionarios se han creado nuevos puestos de trabajo, pero nunca se ha actualizado el croquis.

9. ANÁLISIS DE LOS ACTIVOS FÍSICOS DE LA RED DE DATOS

9.1 ACTIVOS FÍSICOS

Para realizar el análisis detallado de la red de datos se hizo una correspondiente revisión de los equipos relacionados con la red de datos y una revisión física del estado actual de la red y sus componentes.

9.1.1 Servidores: Los servidores que se encuentran en el centro de datos son ya bastante obsoletos, ya que datan de un periodo comprendido entre 2000 y 2005 y sus recursos ya son escasos para brindar cobertura a los servicios dependientes de ellos, como servicio de almacenamiento compartido de toda la empresa bases de datos de aplicativos macrwma, servidor virtual de aplicativo Spark. Estos son

- Servidor IBM, modelo NETFINITY 5100, el cual presenta una cantidad de memoria RAM de 256 Mb, capacidad de disco duro de 120 Gb, en un arreglo de 4 disco duros, procesador Intel Pentium III, en el momento se encuentra en un 90% porcentaje de su capacidad de almacenamiento y procesamiento.

- Servidor Supermicro también está obsoleto y data de del año 2006 es utilizado para administrar los servicios de Base de datos Aplicativo Macrwma, servidor Openfile, el cual presenta una cantidad de memoria RAM de 3GB, Un arreglo de dos discos con capacidad de 80GB cada uno y uno de 150GB, procesador Intel Xeon 3Gh, en el momento se encuentra en un 70% porcentaje de su capacidad de almacenamiento y procesamiento.

9.1.2 Switch: Se cuenta con 3 Switch ENCORE con modelo ENH924-CX, dos se encuentran ubicados en el rack de comunicaciones en la oficina de sistemas y otro está ubicado en la oficina de facturación en el segundo piso y de él depende la red del segundo y primer piso.

El que esa ubicado en el primer piso se encuentra dentro de un gabinete pequeño, junto a un paspanel este gabinete es demasiado pequeño por lo tanto la ventilación dentro del mismo es mínima. Los switch ya presentan deteriores y tienen varios puertos obsoletos.

9.1.3 Radios: La empresa cuenta con 4 radios de marca Cobra modelo MICRO TALK, adquiridos en los primeros meses del año 2016, y son utilizados para establecer comunicación con las redes de las sedes cercanas a la clínica, sin embargo hay que hacer la aclaración que aunque la clínica cuenta con 5 pisos de altura esta altura no es suficiente para establecer una comunicación confiable entre la clínica y las sedes de Emcosalud.

9.1.4 Routers: En el rack de comunicaciones están ubicados dos router uno TP-LINK TL-WA5O110G encargado de enrutar las conexiones desde los equipos de la red y otro de marca CISCO modelo WRTme120N, es cuál es el cargado de recibir la señal de internet.

Estos router no son tan antiguos el cisco es suministrado por el proveedor de conectividad Telefónica y el TP-LINK es propio de la Sociedad Clínica Emcosalud.

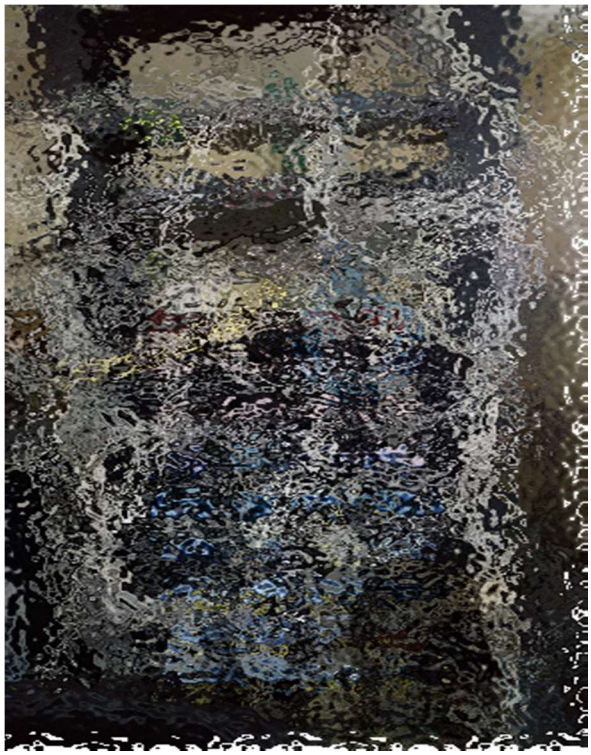
9.1.5 Access Point: En el edificio de la Sociedad Clínica Emcosalud hay distribuidos 3 access point de marca UNIFI y modelo UAP-LR, el primero se encuentra ubicado en el 4 piso y da cobertura a quipos que no están dentro de la red cableada del 4 y 3 piso. Otro está ubicado en la oficina de coordinación medica en el segundo piso este da cobertura inalámbrica a los equipos que están por fuera de la red. Fueron adquiridos en el año 2015, su funcionamiento está dentro de los niveles normales.

9.1.6 Cableado estructurado: La Sociedad Clínica Emcosalud cuenta con cableado de red UTP en todos sus pisos el 80% en categoría 5, dispositivos de conmutación marca 3COM, CISCO y TP-LINK.

Se observó que La Sociedad Clínica Emcosalud, cuenta con 80 puntos cableados, que supone una cobertura del 80% de los puestos de trabajo actuales, sin embargo, 20 se encuentran deshabilitados y no se ha identificado su ubicación en el centro de cableado.

En la inspección visual del estado de cableado en todos los pisos como en el centro de servidores y cableado se encontraron grandes problemas que, aunque en el momento no estén causando inconvenientes en el servicio es casi seguro que en un futuro muy cercano se van a presentar fallos.

Figura 13 Rack



Fuente: Los Autores

El rack de comunicaciones se encuentra bastante desorganizado, se pueden apreciar cables desconectados que no se identifica si pertenecen o no a un punto de red, adicional, en él están ubicados también los patch panel para los cables de voz que van hacia las diferentes oficinas (líneas telefónicas).

Figura 14 Patch Panel-Datos y Voz

Fuente: Los Autores

Según información suministrada por el personal de tecnología los patch panel para datos son los que tienen etiquetas rojas y los de voz son los que tienen etiquetas azules.

Figura 15 Numeración Patch Panel

Fuente: Los Autores

Sin embargo, se encuentran patch panel con los dos colores lo cual es confuso a la hora de identificar fallos.

Figura 16 Identificación Patch Panel

Fuente: Los Autores

Como se puede observar en la imagen anterior algunos cables se encuentran identificado con marquillas, pero otros no la tienen, esta situación es personalmente perjudicial a la hora de brindar un soporte en el servicio de red e internet porque el funcionario va a tener primero que hacer seguimiento al cableado para identificar el cable que falla.

Figura 17 Cables de Datos

Fuente: Los autores

Algunos cables de datos que salen del rack de comunicaciones van por canaleta metálica, mientras que otros van sueltos sin ninguna organización.

Figura 18 Canaletas

Fuente: Los Autores

Las canaletas en el tercero y cuarto piso se encuentran muy deterioradas y los cables como se pueden observar están por fuera de la misma.

Figura 19 Cables eléctricos y de datos

Fuente: Los Autores

En los escritorios también se evidencia mucho desorden y enredo entre los cables de datos y eléctricos.

Figura 20 Toma de Pared

Fuente: Los Autores

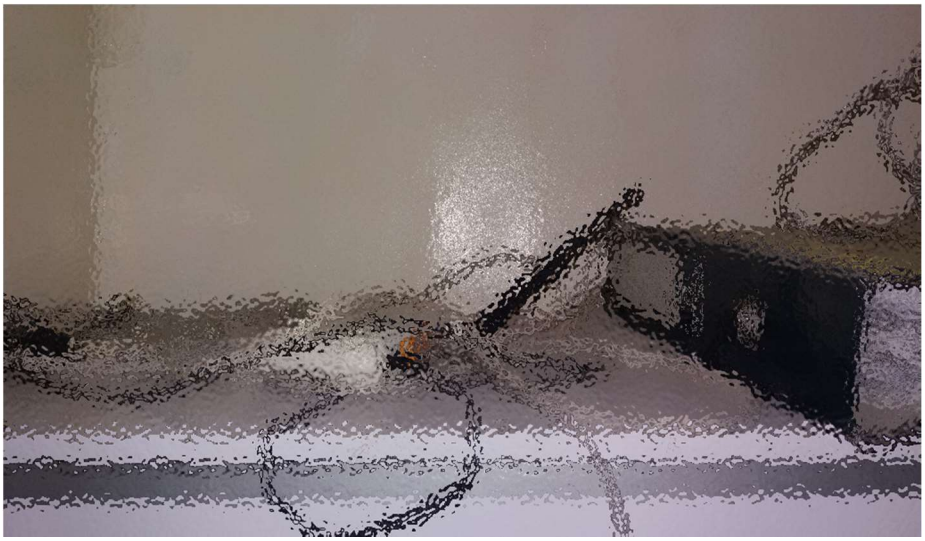
Actualmente ya no existen las tapas de los conectores de cableado Utp. Se han halado los cables de datos de la misma toma de pared hasta los equipos de cómputo.

Figura 21 Evidencia Soporte Swich

Fuente: Los Autores

Se han improvisado pequeños switch para poder dar cobertura a los nuevos puestos de trabajo que se han abierto recientemente.

Figura 22 Evidencia Router



Fuente: los autores

En este caso es un Router inalámbrico instalado en urgencias para que se conecten los médicos que traen su propio equipo portátil.

Figura 23 Cableado estructurado

Fuente Los Autores

Figura 24 Cielo Raso

Fuente: Los Autores

Se han realizado aberturas rusticas en el cielo raso para poder bajar los cables de datos, se puede apreciar que hay varios cables reventados o cortados que no se logran identificar si vienen directamente del 5 piso, o si pertenecen a la red del segundo piso.

Figura 25 Mal estado Canaletas

Fuente: Los Autores

En la anterior imagen se puede evidenciar el mal estado del cableado de datos, sus canaletas sin tapas permiten que los cables se mezclen, podemos apreciar que los cables de datos están muy cerca de los cables eléctricos.

La norma dice:

Tabla 4. Norma para Cableado Eléctrico/Datos

		Distancia A	
Tipo de instalación	Sin divisor o con divisor no metálico	Divisor de aluminio	Divisor de acero
Cable de datos UTP y cable eléctrico no apantallado	200 mm	100 mm	50 mm
Cable de datos ScTP y cable eléctrico no apantallado	50 mm	20 mm	5 mm
Cable de datos UTP y cable eléctrico apantallado	30 mm	10 mm	2 mm
Cable de datos ScTP y cable eléctrico apantallado	0 mm	0 mm	0 mm

Fuente: Los Autores

9.1.7 Medición del Canal: La Sociedad Clínica Emcosalud tiene contratado servicio de un canal MPLS de 18 MB, dedicados para, el funcionamiento de sus aplicaciones y comunicaciones.

Figura 26 Test de Velocidad

Fuente: Los Autores

En la anterior imagen se puede apreciar las mediciones del ancho de banda del canal de internet de la Sociedad Clínica Emcosalud, la cual hizo vía web.

9.2 HALLAZGOS ENCONTRADOS

A continuación, se listan los hallazgos detectados en la red de la Sociedad Clínica Emcosalud.

- En algunos pisos el cableado es de mala calidad o está ya muy deteriorado por el tiempo.

- Se encontró mal uso del cableado (quebrado, sin certificar, o mal uso de los usuarios).

- Muchos puntos de red (Faceplate) no están etiquetados o su información no corresponde con la realidad.

- Se utiliza cableado UTP cat. 5 y otros UTP cat. 6.

- En algunos puntos se encontraron Jack de categoría 6 con cableado categoría 5 o también al contrario cable UTP categoría 5 con Jack de categoría 6.

- En algunos pisos por restructuraciones de las instalaciones se hicieron remodelaciones de oficinas, debido a esto hubo una modificación en la trama del cableado, se tuvo que cambiar y habilitar puntos nuevos

- La rotulación de los puntos de internet no es segura por cambios estructurales se han modificado y la información es errónea.

- No se tiene un orden en el cableado y peinado de los racks.

- Se encontraron cables UTP cortados en de los cuales se desconocen si están ocupando puertos en el rack.

9.3 **SEGURIDAD DE LA INSTALACIONES**

El centro de cableado que es el mismo de los servidores se encuentra dentro de la oficina de sistemas en el quinto piso del edificio, la seguridad para el mismo es deficiente, la oficina presenta como única medida de seguridad una puerta en madera la cual tiene dos chapas, una de perilla normal y la otra de seguridad. No se lleva un sistema de registro al personal ajeno a la oficina, no hay cámaras de seguridad en la entrada ni en el interior de la oficina para tener un respaldo ante cualquier eventualidad en el área de sistemas y de servidores.

Figura 27 Ingreso Oficina de Sistemas y centro de servidores y cableado

Fuente: Los Autores

La empresa no cuenta con políticas de seguridad de la información, ni con un sistema confiable de prevención de desastres naturales e industriales, no hay detectores de temperatura ni de humo, la única medida de seguridad ante desastres es un extintor categoría C, especial para sistemas eléctricos y electrónicos.

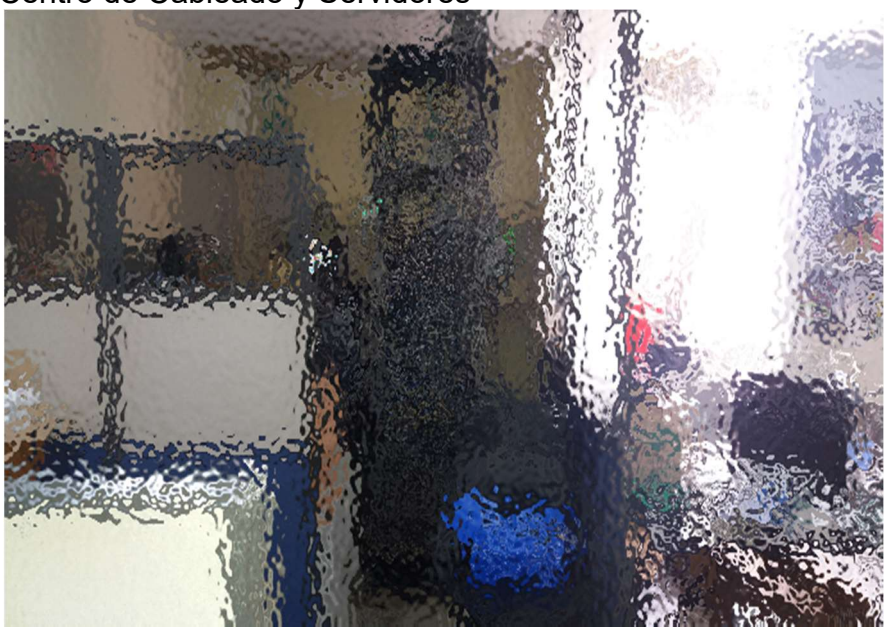
Figura 28 Extintor

Fuente: Los Autores

Como se puede observar que el área de servidores es la misma del centro de cableado, está totalmente desprotegida no cuenta con una puerta que divida el centro de cableados y servidores con el resto de la oficina, es decir que cualquier

persona puede ingresar sin inconvenientes y manipular cualquier componente tanto en los servidores como el rack del cableado estructurado.

Figura 29 Centro de Cableado y Servidores



Fuente: Los Autores

El cableado eléctrico de los servidores y de los equipos de escritorio se encuentra mezclado con los cables de datos y los cables de voz de la planta telefónica, lo cual genera ruido en el cableado tanto de datos como de voz.

9.3.1 Infraestructura física del centro de datos: Se encuentra una infraestructura física bastante descuidado y poco apropiada para albergar servidores y rack de comunicación, en ella también se ubican las UPS, y la planta telefónica. Algunos de los hallazgos encontrados:

- Se presentan muchos desechos provenientes del cielo raso el cual presenta un gran deterioro por humedad y suciedad.

Figura 30 Falta limpieza

Fuente: Los Autores

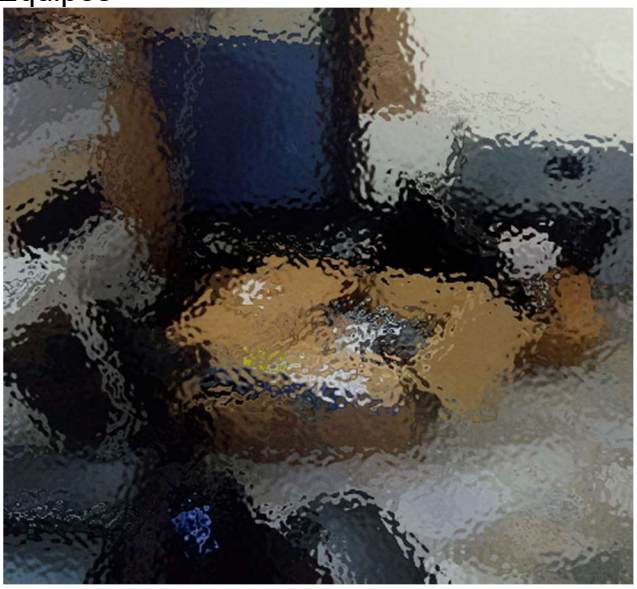
Mala distribución de los equipos, se encuentran aglomerados unos sobre otros

Figura 31 Distribución de Servidores

Fuente: Los Autores

Se encontraron partes de otros equipos que no presentan ninguna vinculación con el área en revisión.

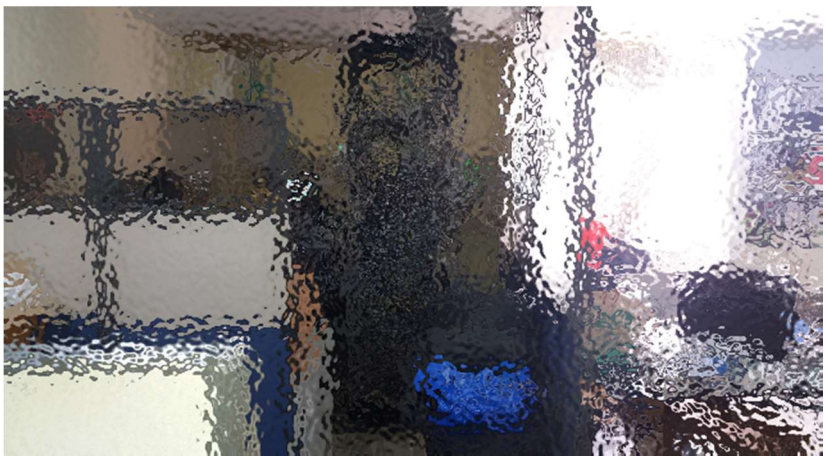
Figura 32 Restos de Equipos



Fuente: Los Autores

- Las divisiones no son las apropiadas, son obsoletas porque no brindan ninguna seguridad para los equipos o infraestructura de red ni para el personal de la oficina ya que genera mucho ruido y radiación que es perjudicial para la salud de los funcionarios.

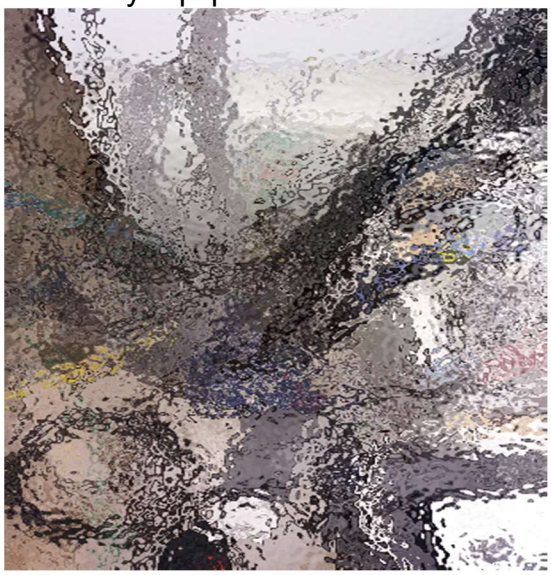
Figura 33 Divisiones



Fuente: Los Autores

- El cableado proveniente de la planta telefónica esta enredado con los eléctricos y de datos de los servidores.

Figura 34 Distribución cableado y equipos



Fuente: Los Autores

10. ANÁLISIS LÓGICO Y DE TRÁFICO DE LA RED DE DATOS

10.1 ANÁLISIS DE TRÁFICOS DE LA RED

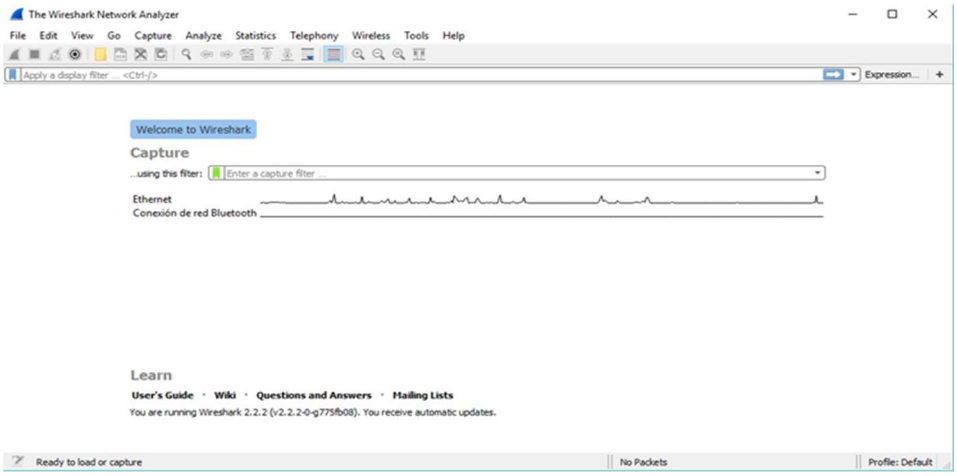
Para realizar el análisis del tráfico de la red se investigaron varias aplicaciones especializadas en monitoreo y gestión de redes escogiendo entre ellas las tres que se ajustaran a las necesidades de vigilancia y seguimiento de la red de datos de la Sociedad Clínica Emcosalud ellas son: wireshark, Colasoft Capsa9 free y NAGIOS.

10.1.1 Wireshark: El analizador Wireshark, es uno de los más populares analizadores que existen. Se trata de una herramienta gráfica utilizada por los profesionales y/o administradores de la red para identificar y analizar el tipo tráfico en un momento determinado.

Se trata de un producto gratuito cuyas características más relevantes son:

- Disponible para UNIX, LINUX, Windows y Mac OS.
- Captura los paquetes directamente desde una interfaz de red.
- Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.
- Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.
- Filtra los paquetes que cumplan con un criterio definido previamente.
- Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente.

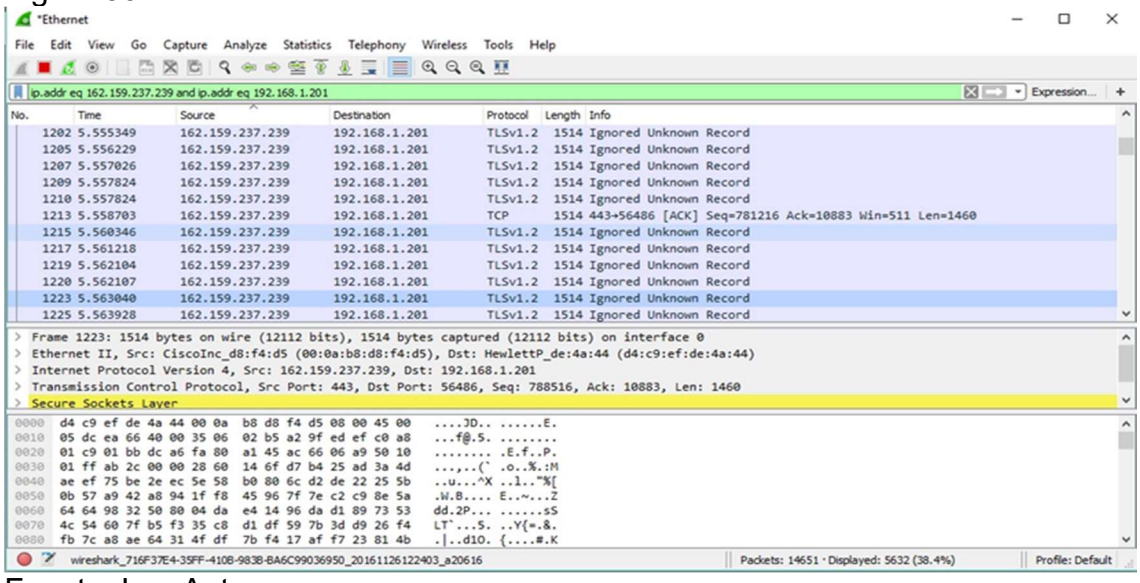
Figura 35 Análisis de red WIRESHARK



Fuente: Los Autores

Al ejecutarse inicia el escaneo de por la tarjeta de red del equipo donde se instala.

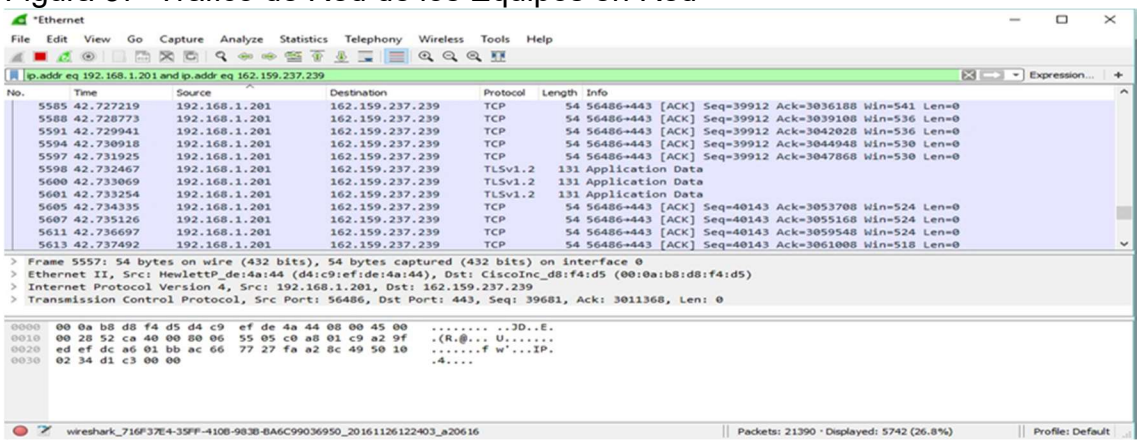
Figura 36 Scaneo de la Red



Fuente: Los Autores

En la siguiente imagen se analiza el contenido desde una ip externa hacia un equipo de la red. Se puede analizar el tráfico de los equipos conectados a la red y revisar su contenido.

Figura 37 Tráfico de Red de los Equipos en Red



Fuente: Los Autores

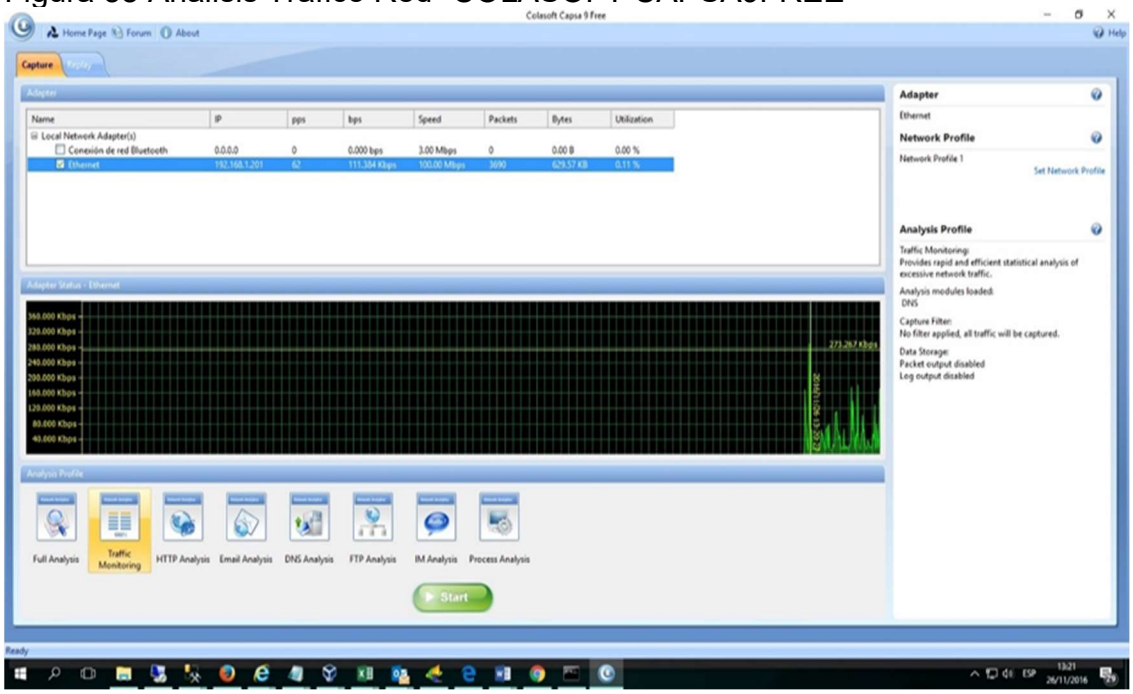
Aunque es una herramienta poderosa para el análisis de trafico de red como podemos ver en las imágenes es necesario un nivel de conocimiento avanzado para poder dominarlo y sacarle el máximo provecho, hace falta también una herramienta grafica de análisis donde podamos observar claramente la distribución de nuestra red.

10.1.2 Colasoft Capsa9 Free: Capsa Free es un analizador de red que le permite monitorear el tráfico de red, solucionar problemas de red y analizar paquetes. Las características incluyen soporte para más de 300 protocolos de red (incluyendo la capacidad de crear y personalizar protocolos), MSN y Yahoo! Messenger filtros, monitor de correo electrónico y auto-guardar, e informes personalizables y cuadros de mando. Sus principales características son:

- Análisis extendido de la seguridad de la red.
- Estadísticas versátiles de tráfico y ancho de banda.
- Decodificación de paquetes en profundidad.
- Múltiples monitoreo de comportamiento de red.
- Diagnóstico automático de la red de expertos.

- Conexiones visualizadas en matriz.
- Poderoso análisis de conversación.
- Útiles y valiosas herramientas integradas.
- Informe rápido e intuitivo.

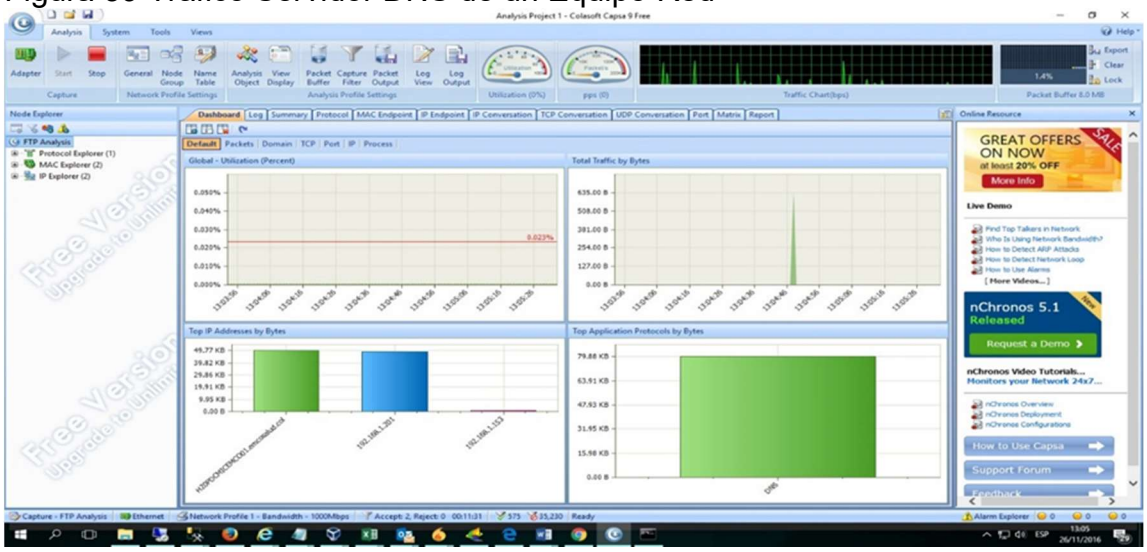
Figura 38 Análisis Trafico Red -COLASOFT CAPSA9FREE



Fuente: Los Autores

En el momento que se ejecuta inicia el análisis de la red de datos de la empresa.

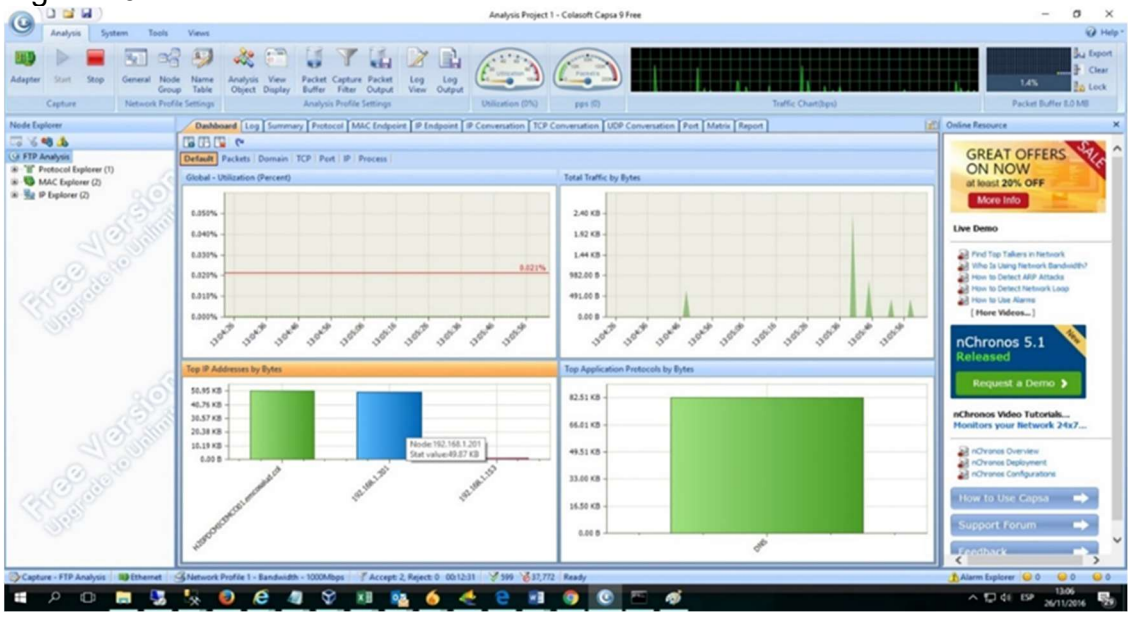
Figura 39 Trafico Servidor DNS de un Equipo Red



Fuente: Los Autores

El primer pantallazo nos muestra el tráfico al servidor DNS de un equipo de la red podemos observar que es alto el tráfico desde esa dirección IP.

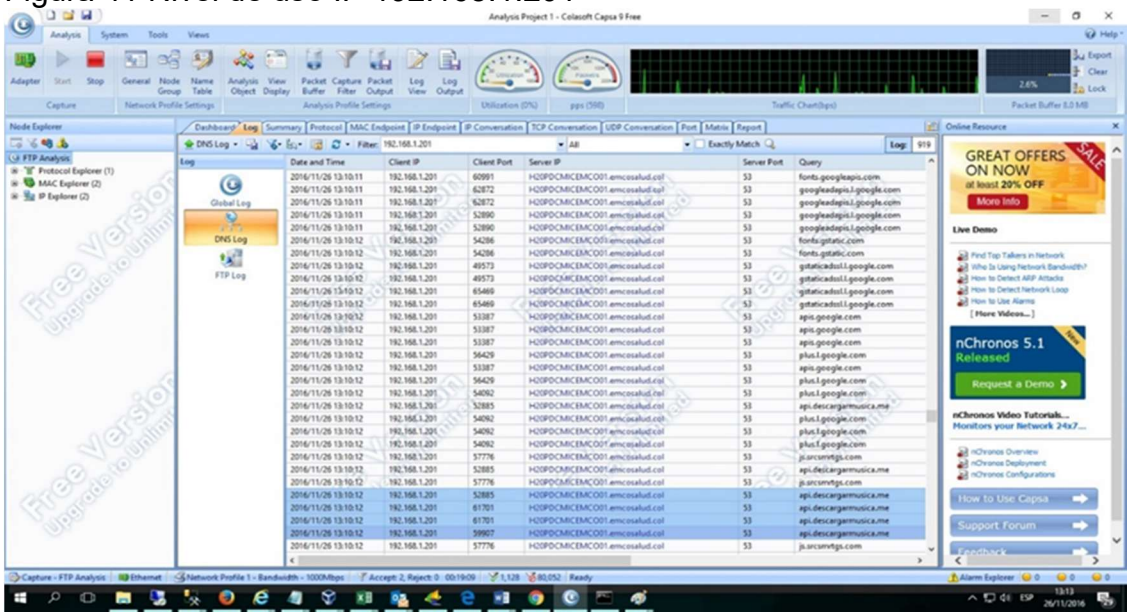
Figura 40 Nivel de uso de red



Fuente: Los Autores

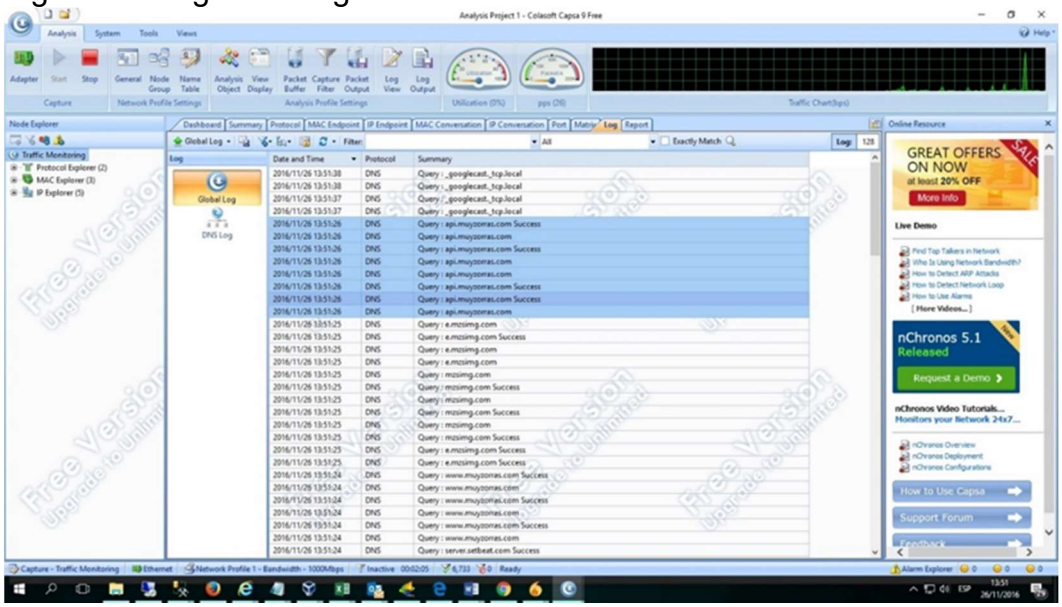
Tomamos como referencia otro equipo de la red para determinar el nivel de uso que presenta la dirección IP 192.168.1.201, el cual no es normal.

Figura 41 Nivel de uso IP 192.168.1.201



Fuente: Los Autores

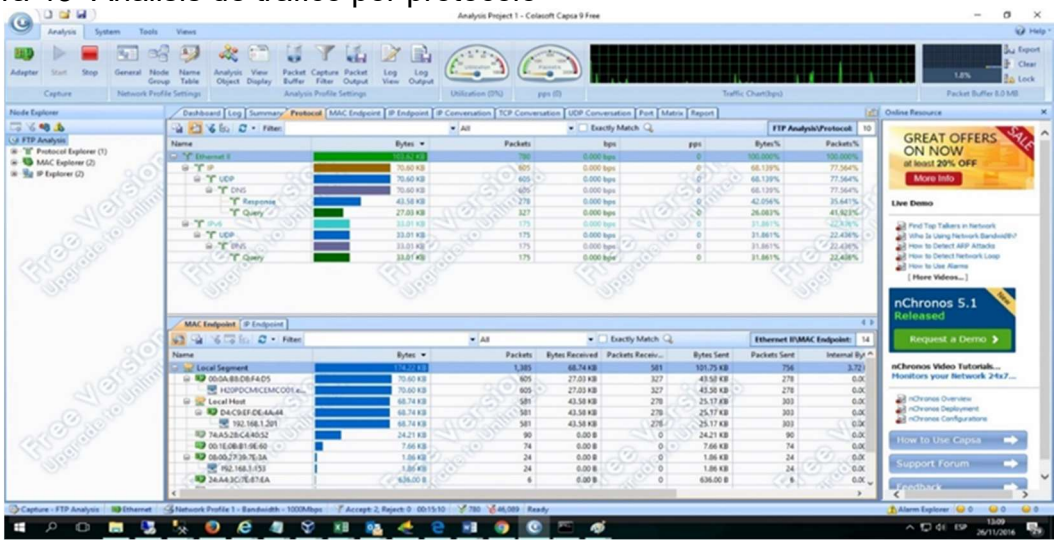
Figura 42 Log de navegación



Fuente: Los Autores

Mediante el log de navegación podemos identificar que el usuario del equipo con dirección IP 192.168.1.201 está navegando páginas que no están permitidas como podemos observar en el log donde muestra que visitó páginas de descarga de música y páginas de contenido sexual.

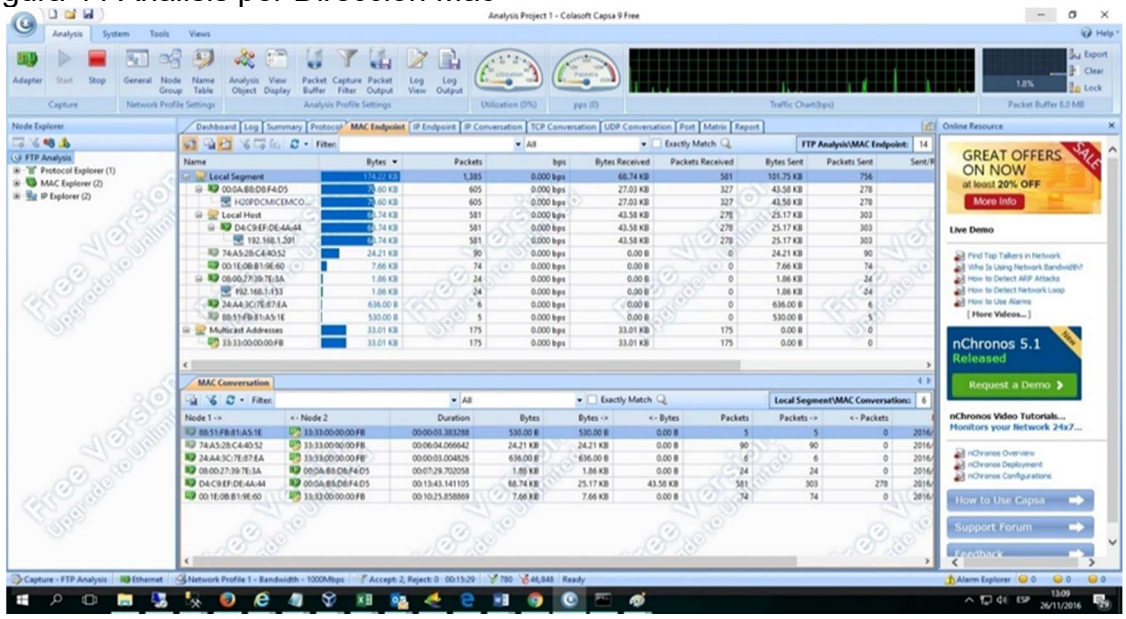
Figura 43 Análisis de tráfico por protocolo



Fuente: Los Autores

Se hace un análisis del tráfico por protocolo o por dirección Mac

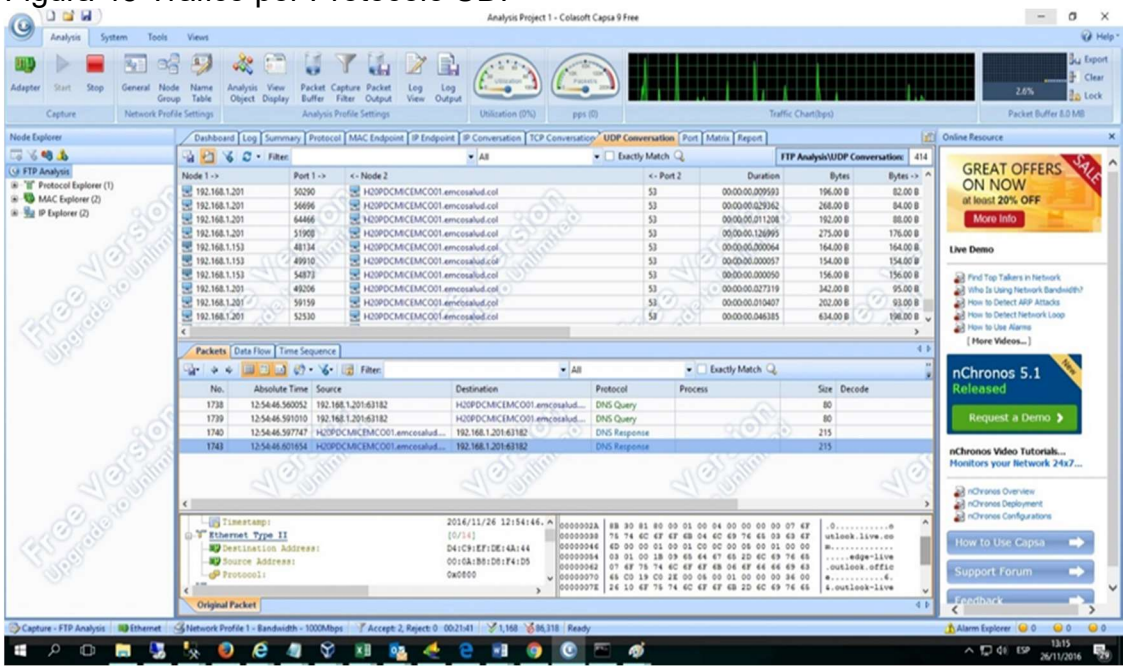
Figura 44 Análisis por Dirección Mac



Fuente: Los Autores

Muestra la saturación por la dirección Mac del equipo.

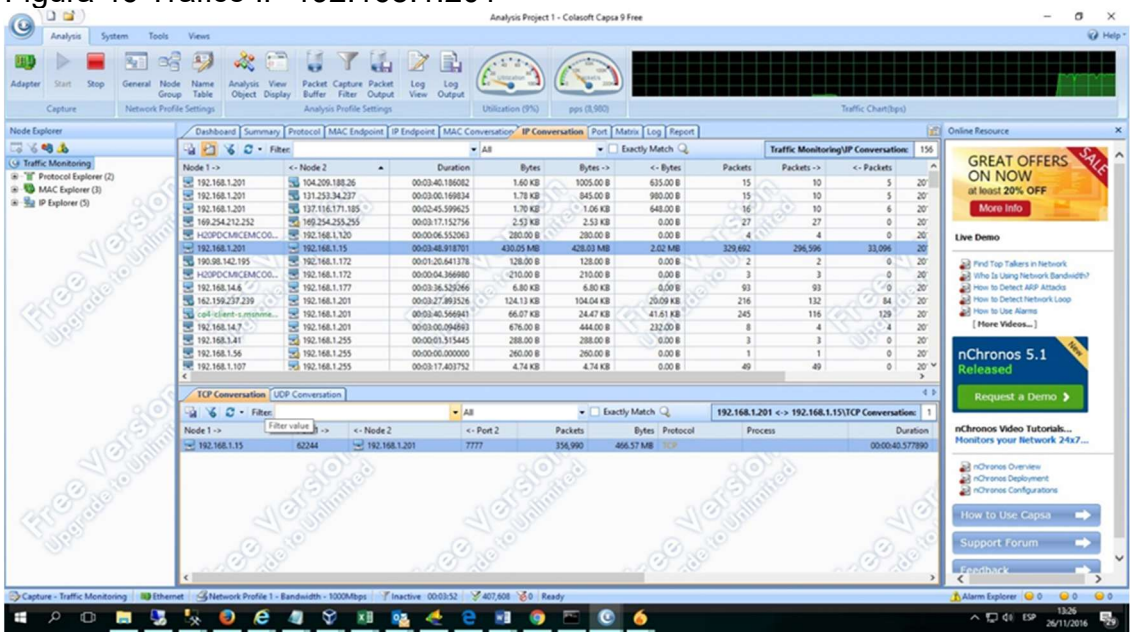
Figura 45 Tráfico por Protocolo UDP



Fuente: Los Autores

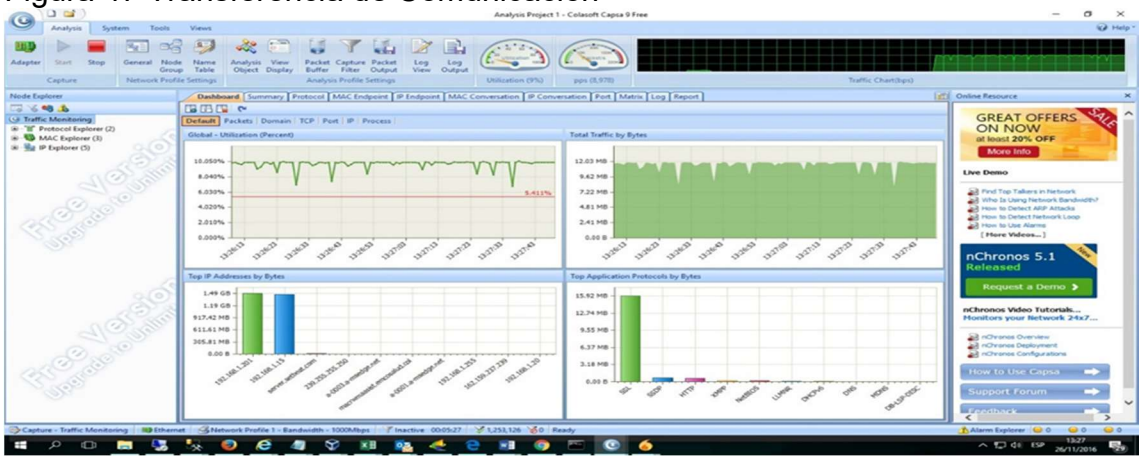
Observamos el tráfico por protocolo UDP

Figura 46 Trafico IP 192.168.1.201



Fuente: Los Autores

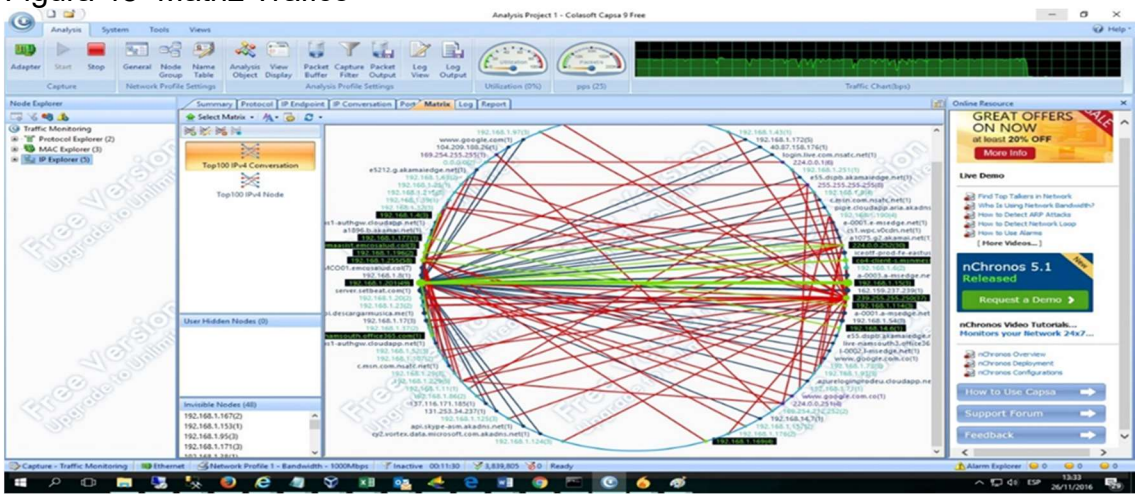
Figura 47 Transferencia de Comunicación



Fuente: Los Autores

En este apartado se detectó la transferencia exagerada entre dos nodos, en este caso también es el equipo de dirección IP 192.168.1.201 y el equipo con dirección 192.168.1.15, esta comunicación baja considerablemente el rendimiento de la red, se evidencia falta de conciencia de los usuarios en el uso de la red.

Figura 48 Matriz Tráfico



Fuente: Los Autores

Por último, podemos ver un gráfico del tráfico que ha tenido la red de datos durante las pruebas realizadas.

En conclusión: Podemos decir que se evidencia grandes fallos de seguridad en la red de datos y que se evidenciaron fácilmente con esta aplicación la cual sería muy recomendada para implantar ya que es muy completa e intuitiva para su uso, pero desafortunamente es una herramienta con licencia de evaluación por lo tanto ante la falta de presupuesto sería difícil implantarla.

10.1.3 Nagios: Probablemente la herramienta libre más conocida. Desde 1996 trabajando en USA para construir este software de monitorización. Su core es la parte más importante de la herramienta y sobre el core se pueden construir plugins para monitorizar elementos particulares.

Ventajas:

- Se encuentran muchos perfiles con experiencia Nagios.
- Si se tiene gran conocimiento de la herramienta, la configuración manual puede darle mucha potencia a la hora de monitorizar casos aislados y particulares.
- Ofrece muchos plugins para adaptar Nagios a las necesidades del usuario.
- Para la configuración básica es muy fácil.

Inconvenientes:

- El interfaz gráfico carece de una buena usabilidad.
- Costo de aprendizaje elevado.
- Cada instalación al final resulta un “puzzle” en el que más que un producto estándar tenemos una implementación propia, con cientos de parches, código propio o de terceros y complicada de evolucionar o de mantener por terceros.
- Informes sencillos.

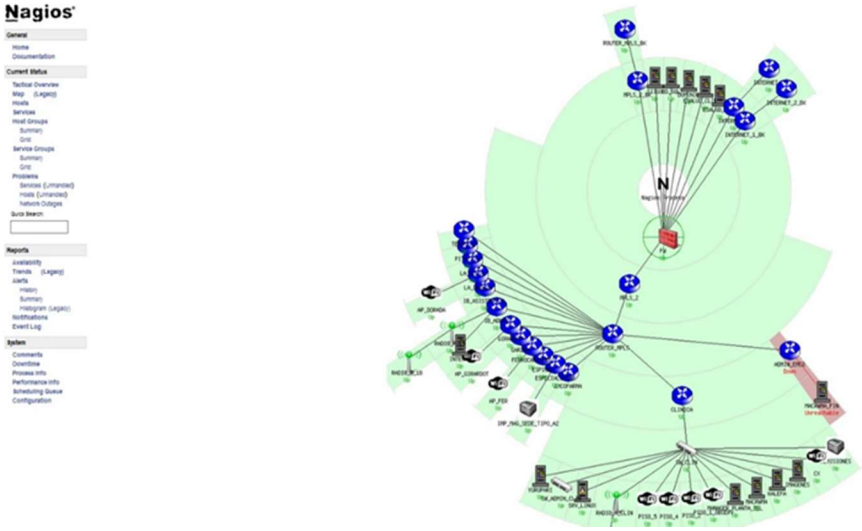
- Muy pobre en su tratamiento de SNMP, tanto de polling como de gestión de traps.

Figura 49 NAGIOS

Fuente: Los Autores

Es una herramienta gratuita que se puede implementar en servidor Linux.

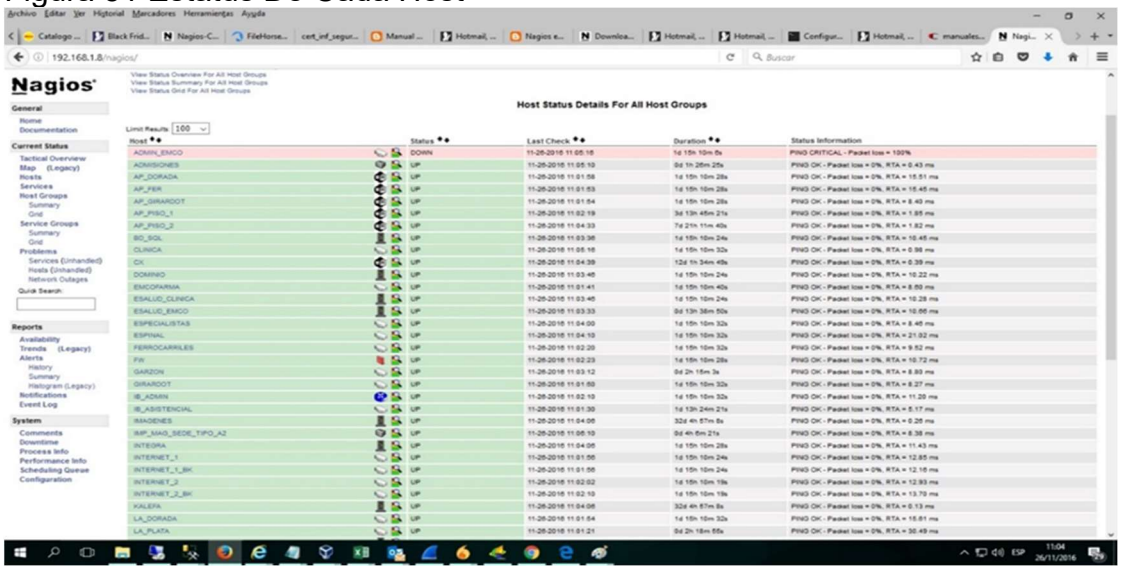
Figura 50 Distribución Red Emcosalud



Fuente: Los Autores

Podemos apreciar la distribución de la red de datos de la Empresa Cooperativa de Servicios de Salud Emcosalud y Sociedad Clínica Emcosalud.

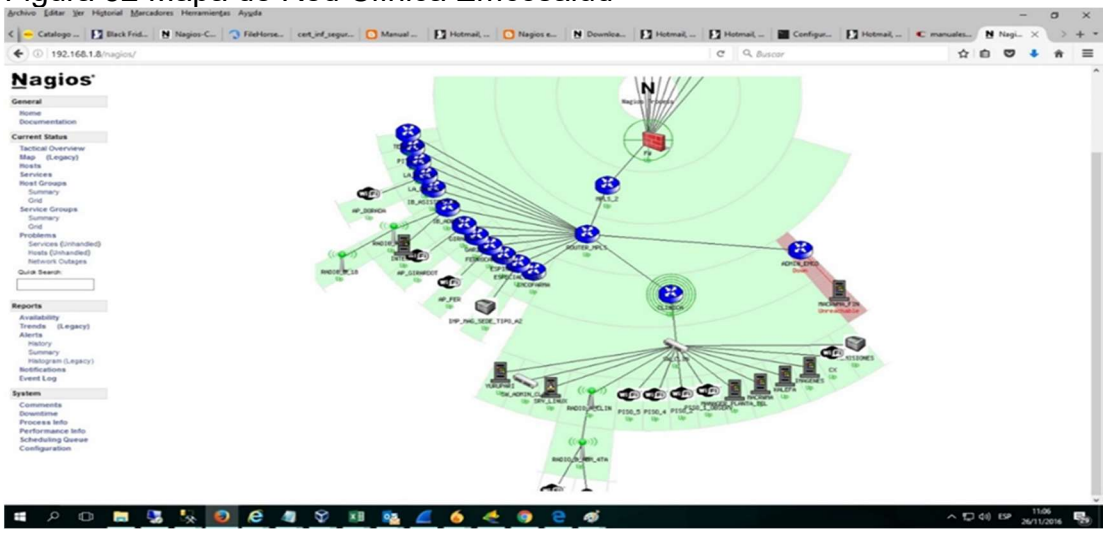
Figura 51 Estatus De Cada Host



Fuente: Los Autores

En la imagen podemos revisar el status de cada uno de los host de la red, podemos identificar que hay un host parado el aplicativo nos indica que hay que revisarlo.

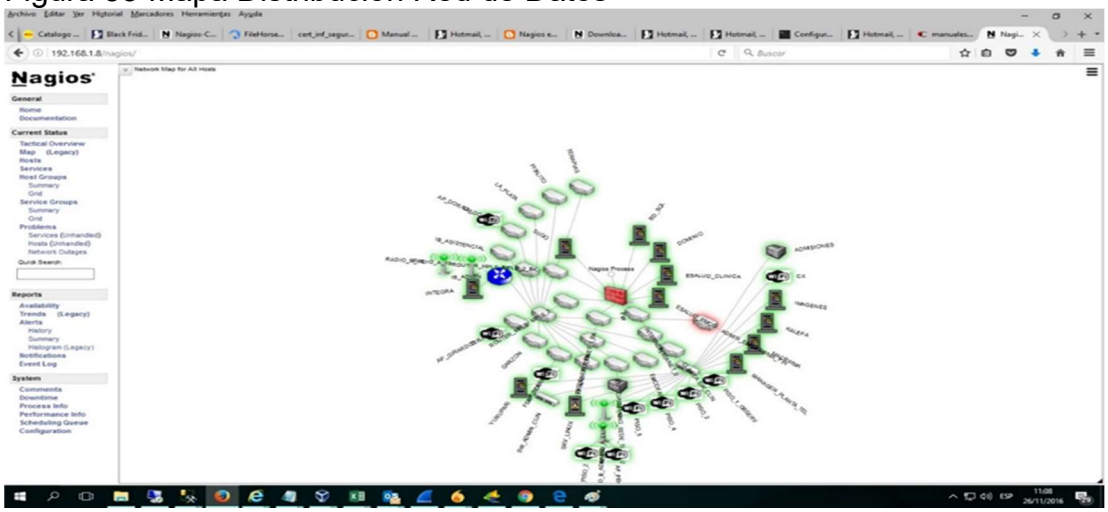
Figura 52 Mapa de Red Clínica Emcosalud



Fuente: Los Autores

Imagen más detallada, el mapa de red de la Sociedad Clínica Emcosalud con cada uno de sus componentes en estos momentos encontramos en el mapa un router caído y un servidor, pero están por fuera de la red de datos de la empresa.

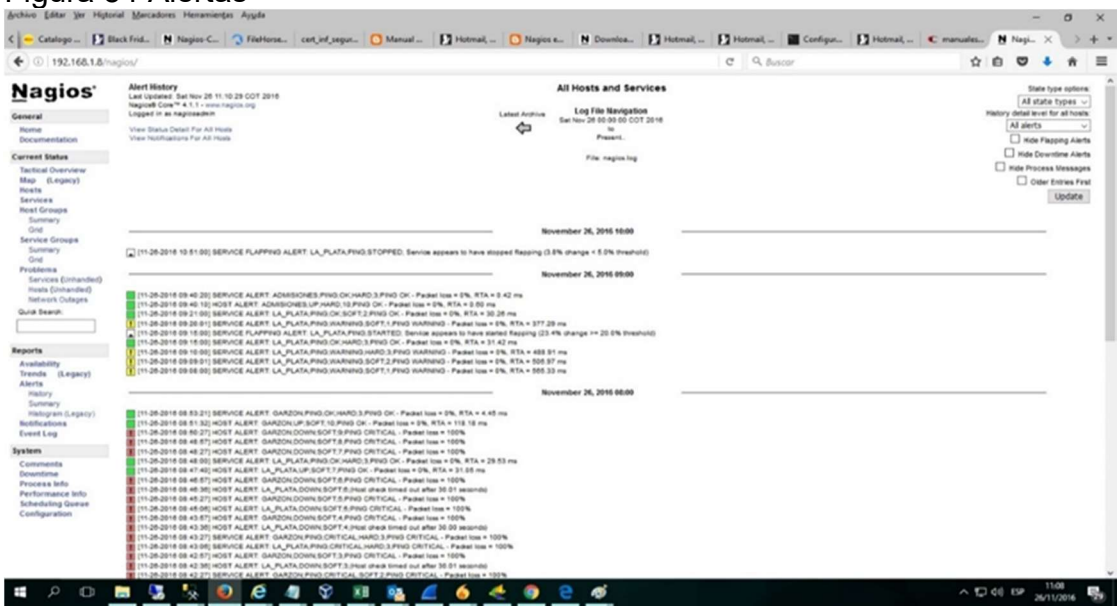
Figura 53 Mapa Distribución Red de Datos



Fuente: Los Autores

Mapa con la distribución de la red de datos del grupo empresarial Emcosalud al cual pertenece la Sociedad Clínica Emcosalud.

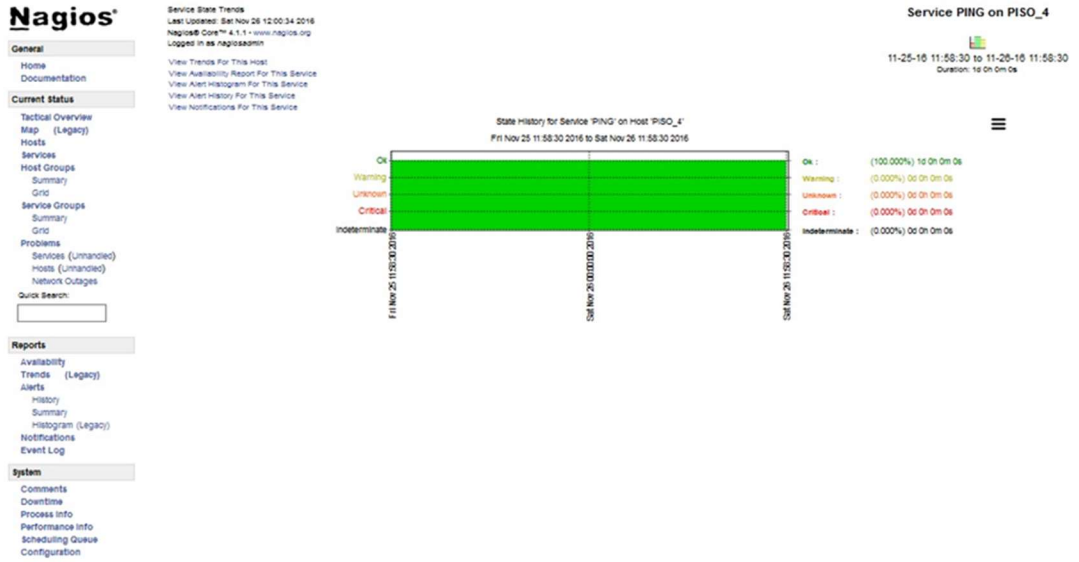
Figura 54 Alertas



Fuente: Los Autores

Podemos identificar alertas sobre fallos en los servicios brindados en la red de datos.

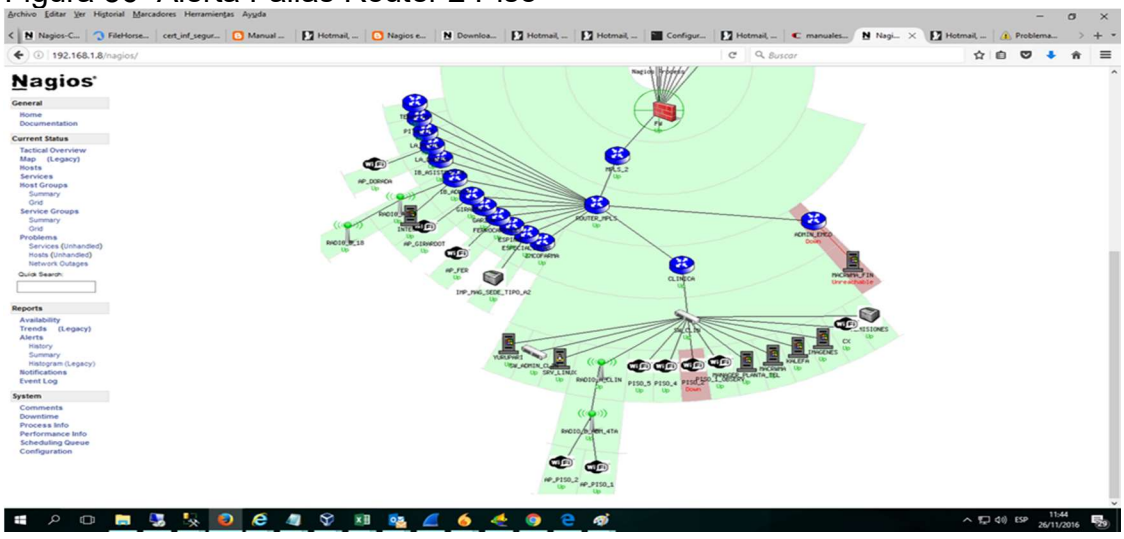
Figura 55 Reporte Estado de Host



Fuente: Los Autores

En la imagen se puede observar un reporte del estado del host del piso 4

Figura 56 Alerta Fallas Router 2 Piso



Fuente: Los Autores

Alerta sobre la caída de un Router en el segundo piso inmediatamente se presenta el fallo NAGIOS, nos alerta cambiando de color el icono correspondiente al dispositivo.

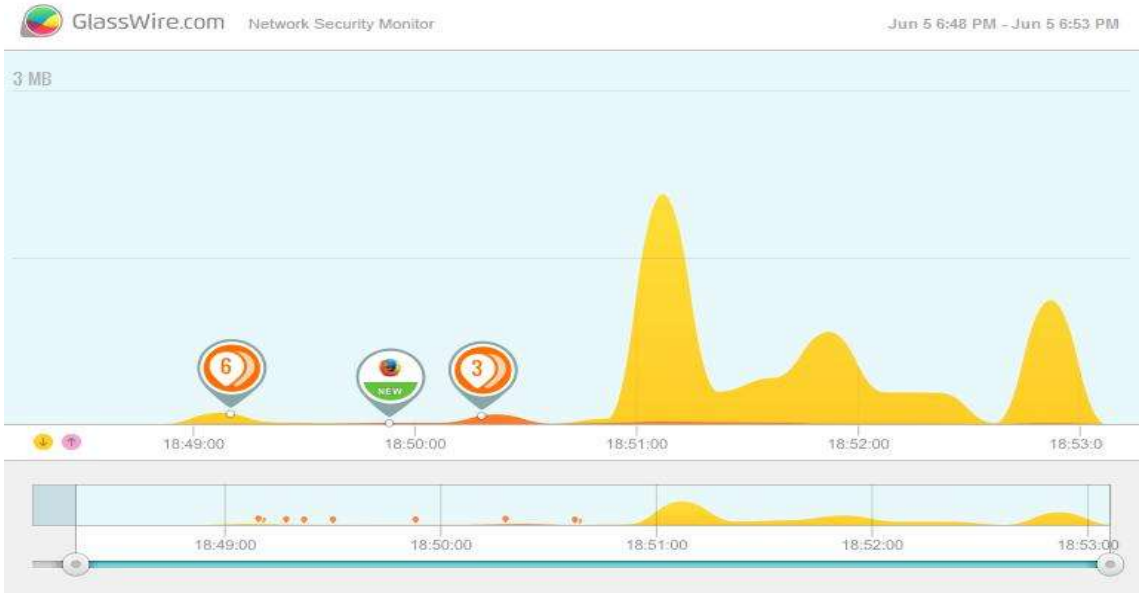
10.1.4 GlassWire: Es una herramienta gratuita enfocada principalmente en el monitoreo de red orientada a los ordenadores, en su versión pro es posible hacer un monitoreo de eventos en toda la red.

Figura 57 GlassWire

Fuente: Los Autores

Este aplicativo inicialmente permite implementar un firewall, en los equipos y a su vez facilita el análisis del tráfico de red desde el pc hacia internet, que aplicaciones se están conectando y cuanta información están trasmitiendo.

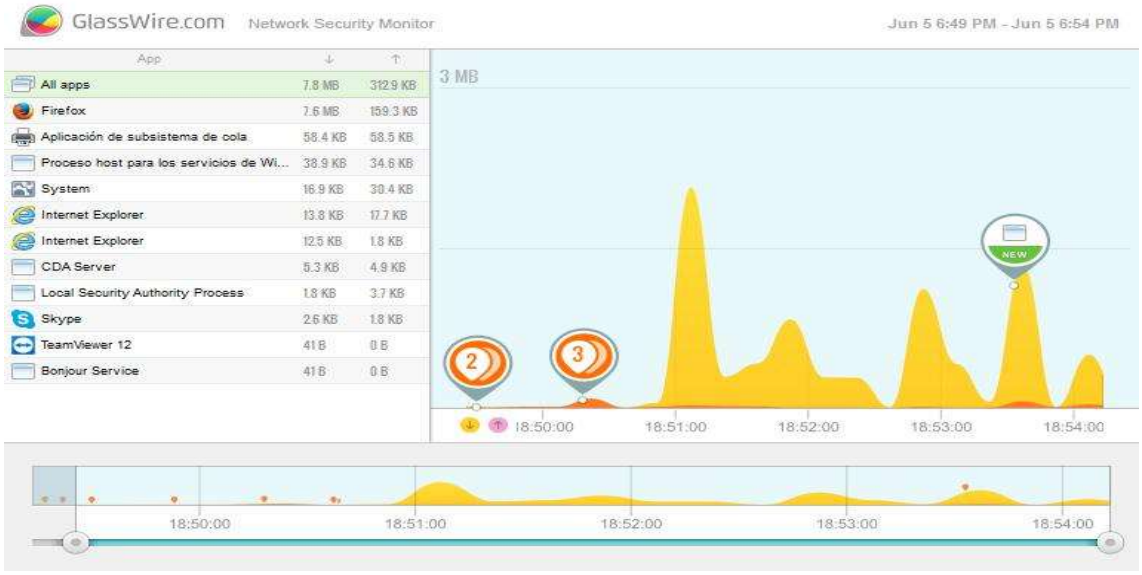
Figura 58 Gráfico de aplicaciones conectadas a internet



Fuente: Los Autores

En la anterior imagen se puede observar como el aplicativo grafica el tráfico que genera las aplicaciones con salida a internet.

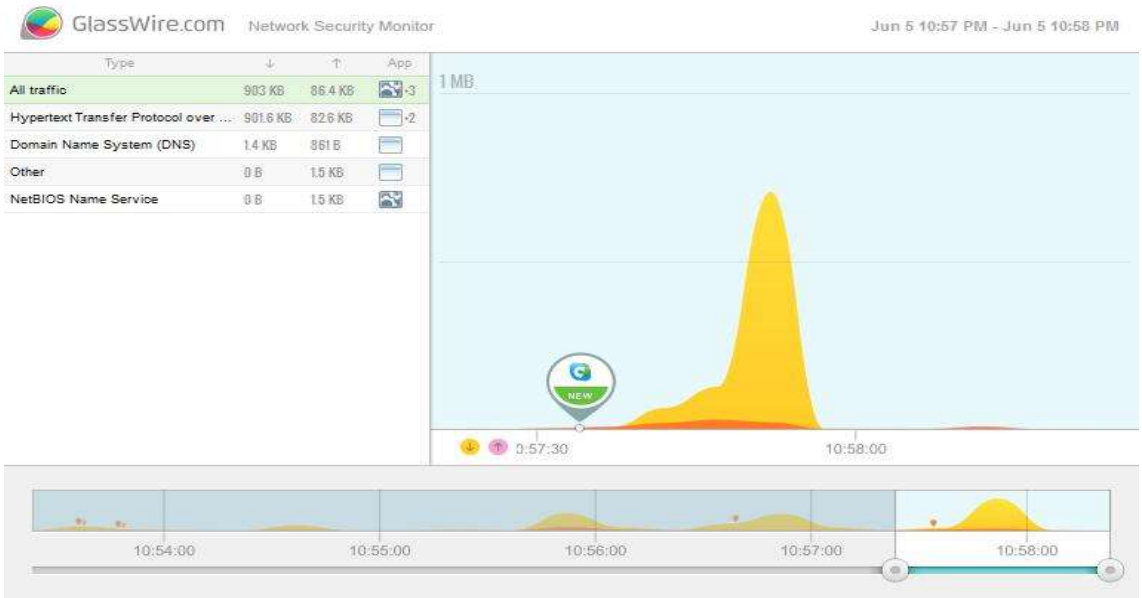
Figura 59 All Apps



Fuente: Los Autores

Podemos observar cuanto consume cada una de las aplicaciones tanto en descarga con en subida de datos (Download y upload).

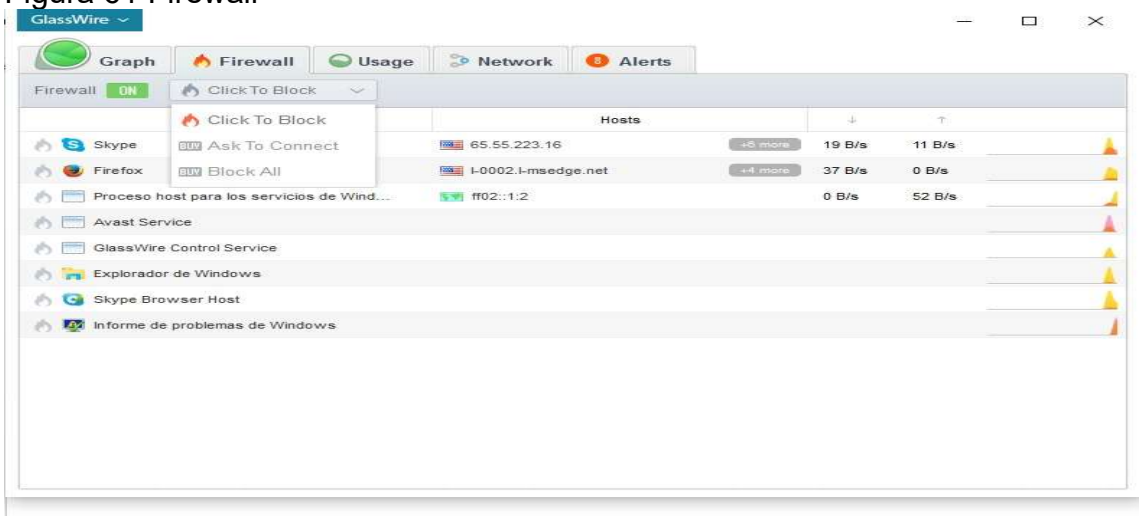
Figura 60 Traffic



Fuente: Los Autores

Se puede observar el tráfico que hay desde el pc monitoreado a internet se puede apreciar el total (all traffic) o por aplicaciones de forma independiente.

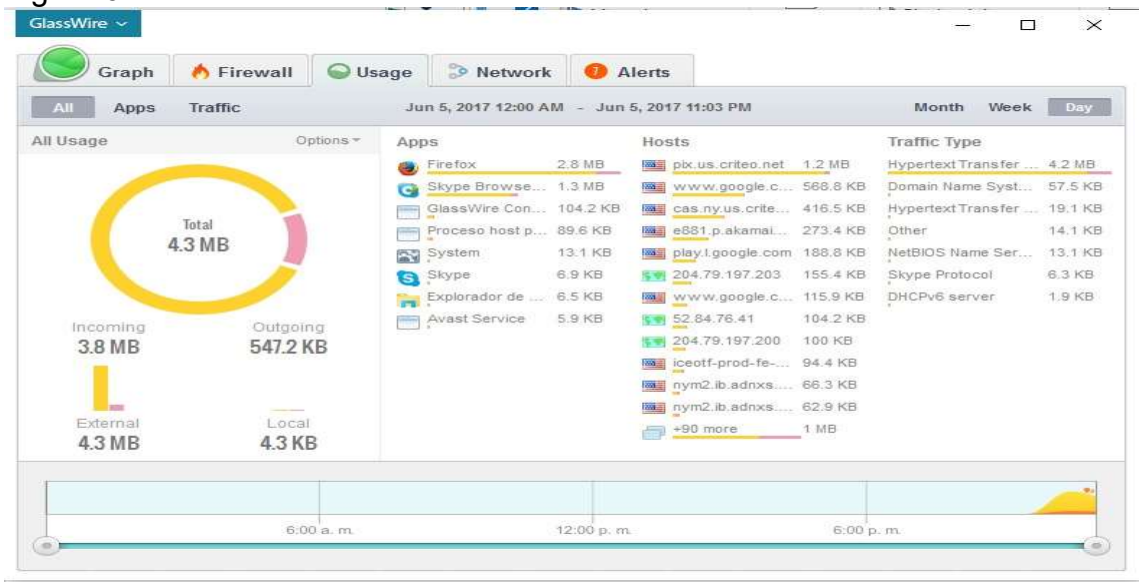
Figura 61 Firewall



Fuente: Los Autores

GlassWire tiene incorporado un básico firewall en el cual es posible bloquear el acceso a ciertas url y direcciones IP.

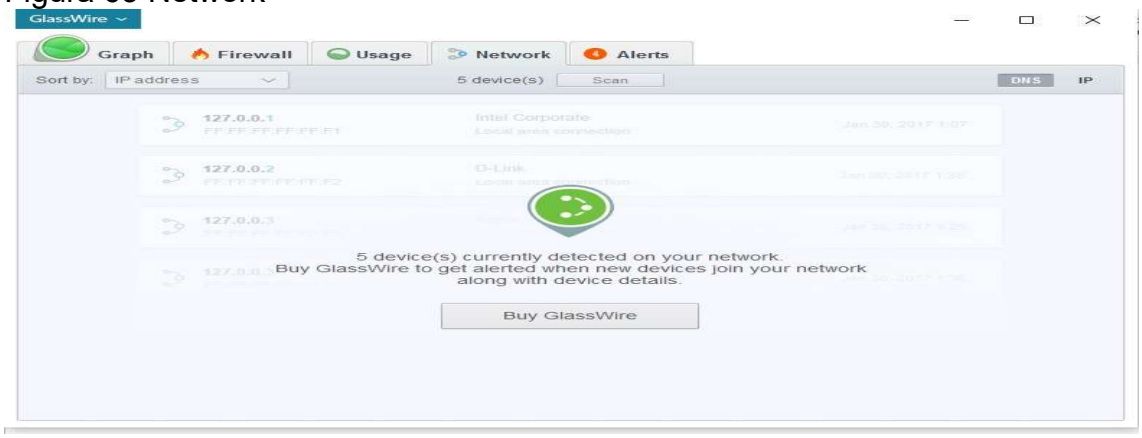
Figura 62 Remote Server Monitor



Fuente: Los Autores

GlassWire puede supervisar toda la actividad de la red del servidor y alertarlo de las amenazas potenciales. También con la pestaña de uso de GlassWire puede ver exactamente cuánto ancho de banda está utilizando en detalle para ayudar a mantenerse bajo los límites de su empresa de alojamiento. Bloquee el ancho de banda acumulando aplicaciones o violadores de privacidad bajo la pestaña Firewall de GlassWire.

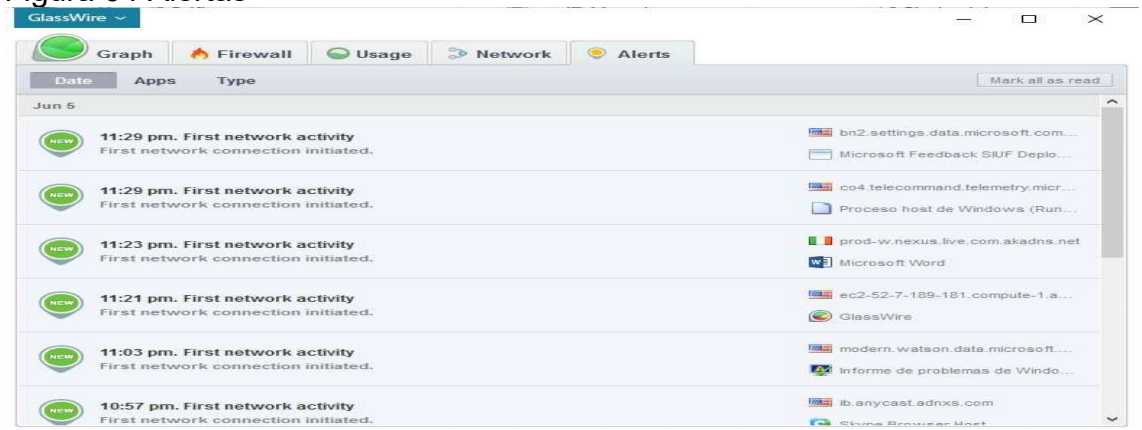
Figura 63 Network



Fuente: Los Autores

En la opción de red el aplicativo identifica cantos dispositivos hay conectados a la red, y a su vez puede generar alertas cuando más equipos se unen a la red y muestra las características de cada uno de ellos. Para poder acceder a esta opción de GlassWire, es necesario adquirir una de las tres versiones pagas (Basic, Pro y Elite).

Figura 64 Alertas



Fuente: Los Autores

Pose un sistema de avisos en el cual nos informa todas las actividades de conexión tanto internas como externas al pc.

Aunque es una aplicación bastante gráfica y fácil de comprender se puede determinar que está más enfocada a los pc individuales que al monitoreo de la red en general, como la versión probada es free no fue posible ingresar a la opción Network, para observar su comportamiento.

11. HERRAMIENTA DE MONITOREO DE RED SELECCIONADA

Tras realizar las pruebas con los cuatro aplicativos para monitorización de redes de datos, se logró identificar sus ventajas y desventajas antes las necesidades de la red de la Sociedad Clínica Emcosalud. Todos arrojaron resultados positivos y se identificaron inconvenientes en cuanto al manejo de la red por parte de los usuarios de la misma. Sin embargo el software que más funcionalidades para el monitoreo e identificación de anomalías en la red de datos es Colasoft capsa9free aunque la versión probada fue un demo gratuito por un corto periodo de tiempo, se lograron identificar muchas inconsistencias en el tráfico de la red y varias afectaciones al buen uso de los recursos de red e internet por parte de los usuarios, aunque este aplicativo es muy recomendable en lo relacionado con la detección de eventos en el uso y consumo de red, Nagios por su parte es una herramienta muy buena para identificar daños en los dispositivos en tiempo real gracias a la virtualización que hace de la red de datos en todos sus niveles, permitiendo saber de forma inmediata cuando hay problemas en cualquiera de los recursos que la conforman, permitiendo tomar medidas correctivas de forma oportuna.

Unir los dos aplicativos sería ideal para la administración de cualquier red de datos, pero Colasoft capsa9free no es gratuito y la empresa en el momento no está interesada en invertir en compra de nuevas aplicaciones, en consecuencia el software más ajustado al presupuesto y a las necesidades evidenciadas en el estudio físico realizado a la red de datos de la Sociedad Clínica Emcosalud es NAGIOS, gracias a sus características de virtualización de la red y otras que se enuncian a continuación:

- Monitorización de servicios de red (SMTP, POP3, HTTP, HTTPS, NTP, ICMP, SNMP, FTP,DNS, etc).

- Monitorización de los recursos de equipos hardware (carga del procesador, uso de los discos, procesos del sistema) en varios sistemas operativos.

- Monitorización de equipos remotos, a través de túneles SSL cifrados o SSH.

- Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, usando sus lenguajes de programación preferidos (Bash, C++, Perl, Ruby, Python, PHP, C#).

- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.

- Notificaciones a los contactos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos.

- Rotación automática del archivo de registro.

- Soporte para implementar hosts de monitores redundantes.

- Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas, archivos de registros.

12. RECOMENDACIONES

Al hacer las revisiones visuales de la red, se encontraron gran cantidad de puntos mal manejados en la configuración y mantenimiento de la red de datos, lo cual puede generar fallos al punto de poner en riesgo la disponibilidad del servicio, para cambiar esta situación es necesario:

12.1 **RECOMENDACIONES FÍSICAS**:

- Hacer un rediseño de la red que abarque los nuevos puntos y que permita dimensionar el crecimiento de la misma.

- Hacer una actualización de infraestructura tecnológica.

- Reparar los problemas del sistema eléctrico presenta muchas picos y descargas que afectan a los dispositivos de transmisión.

- Mejorar y rediseñar la estructura del cableado y la organización de la oficina de sistemas.

- Se recomienda la certificación del cableado y de los puntos del internet en toda la infraestructura de la Sociedad Clínica Emcosalud.

- Revisión de punto a punto para determinar la funcionalidad de los mismos y de esta forma identificar los cables que no están habilitados y retirar ese cableado innecesario.

- Cambiar el cableado a categoría 6 para tener un mejor rendimiento del tráfico de datos.

- Organizar el cableado en el centro de datos identificando en el pash panel cada cable con sus respectivas marquillas de identificación.

- Se debe separar los servidores del centro de cableado, para brindar más seguridad tanto a los servidores como al cableado.

- Se deben implementar medidas de seguridad al centro de cableado para evitar ingresos no autorizados al mismo.

- Es necesario contratar con una empresa especializada en cableado estructurados para rediseñar la red de la empresa.

12.2 **RECOMENDACIONES LÓGICAS**:

- Instalación de un sistema de detección de intrusos IDS gratuito se recomienda SNORT ya que es gratuito y ayuda a detectar intrusos y alerta al administrador de la red.

- Capacitación al personal en el manejo de herramientas de detección de intrusos, monitoreo de redes, manejo de cableado estructurado, mantenimiento preventivo de equipos enrutadores y concentrador.

- Tener la documentación correspondiente a la red y a los dispositivos que la conforman (croquis, garantías, manuales de instalación y funcionamiento, inventario de puntos de red, etc).

- El cableado estructurado se debe ajustar a la norma ANSI/TIA/EIA -568-A que especifica los requisitos mínimos para cableado de telecomunicaciones dentro de edificios comerciales, incluyendo salidas y conectores, así como entre edificios de conjuntos arquitectónicos.

- También se aconseja tener un canal de internet de respaldo solo cuenta con uno y no sabemos cuándo este canal se inhabilite.

- Hacer un diseño para la red inalámbrica definiendo puntos importantes para ubicación de routers inalámbricos, accespoint etc.

- Crear protocolos de solución a fallos y contingencia ante la posibilidad de fallos en la red.

- Realizar pruebas de ruido con amplificadores de espectro y sniffers inalámbricos antes, durante y después de la instalación de algún Punto de Acceso.

13. CONCLUSIONES

- Al revisar y monitorear los dispositivos de la red nos permite tener un control en tiempo real, determinando la prestación del servicio y sus condiciones actuales.

- Las simulaciones de tráfico son de gran ayuda y funcionalidad para determinar el comportamiento de nuestros dispositivos y la red.

- Se puede concluir que el análisis y monitoreo de la red es fundamental para una buena administración y control.

- Realizar el diagnóstico de la red de comunicaciones de la Sociedad Clínica Emcosalud, le permitirá al área de sistemas contar con un documento actualizado, donde se caracterice su infraestructura., con miras a mejorar la administración y hacer una gestión de red mucho más eficiente, basado en el sistema de gestión de red.

- La definición de los niveles de priorización de los dispositivos es fundamental para organizar adecuadamente la infraestructura con miras a soportar los usuarios y servicios que cada piso va a atender.

- Un buen plan de mejoramiento si se va a tener en cuenta la priorización del tráfico, antes debe contar con pruebas y mediciones que argumenten su utilidad, de lo contrario no aplicaría.

BIBLIOGRAFÍA

ARBELAES , Luis Guillermo. Diagnostico de la Red de Comunicaciones de la Universidad Católica de Pereira [En línea]. Pereira: Universidad Católica de Pereira. 2013., 118 p. Disponible en: http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/1736/CDMIST69.pdf?sequence=1

DORADO, Juan Luis. Conceptps Básicos sobre planificación de redes [En Línea]. s.l. Diario de Planificación y Diseño de Redes y Servicios 2012. Disponible en: https://diarioredesyservicios.wordpress.com/2012/01/11/conceptos-basicos-sobre-planificacion-de-redes/

ECHEVERRÍA, Carlos. La importancia del monitoreo de red en la implementación de soluciones de negocios [En línea]. México: Mundo Contact. 2014., Disponible en: http://mundocontact.com/la-importancia-del-monitoreo-de-red-en-la-implementacion-de-soluciones-de-negocios/.

MEDINA RAFAEL, José Manuel. Seguridad en redes [En Línea]. Veracruz: Universidad Veracruzana. 2013. 88 p. Disponible en: http://cdigital.uv.mx/bitstream/123456789/32368/1/medinarafaeljosemanuel.pdf

MORENO, Jonny. Arquitectura para el monitoreo de redes [En línea]. s.l. https://morenojhonny.wordpress.com. 2012. Disponible en: https://morenojhonny.wordpress.com/2012/06/15/6-1-arquitectura-para-el-monitoreo-de-redes/.

MUÑOZ, Juan. ¿Por qué es importante monitorizar nuestra red? [En línea]. Madrid: www.tecnozero.com. s.f. Disponible en: https://www.tecnozero.com/blog/por-que-es-importante-monitorizar-nuestra-red/

PAESSLER. Monitorización de red como elemento esencial en el concepto de seguridad de TI [En línea]. Alemania. Paessler AG. s.f. Disponible en: https://www.es.paessler.com/press/whitepapers/security

VEGA TIRADO, Rafael Emiro. Et al. Proyecto Monitoreo y gestión de redes [En línea]. Antioquia: Servicio Nacional de Aprendiza SENA regional Antioquia. 2008. Disponible en: https://es.scribd.com/doc/11526277/Proyecto-Monitoreo-Y-Gestion-de-la-Red-Final

GÓMEZ VIEITES, Álvaro. Tipos de ataques e intrusos en las redes informáticas [En línea]. s.l. Escuela de Negocios Caixanova. 2014. Disponible en: http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

MEJÍA HERRERA, Luis Fernando. Que es gestión y monitoreo de red [En línea]. s.l. Luis Fernando Mejía Herrera administración de redes. 2009. Disponible en: http://servidorespararedes.blogspot.com.co/2009/01/que-es-aplicaciones-web.html

WIKIPEDIA. Monitoreo de red [En línea]. s.l. Wikipedia la Enciclopedia Libre. s.f. Disponible en: https://es.wikipedia.org/wiki/Monitoreo_de_red

GOBIERNO DE LAS TIC. Tipos de Redes Informáticas [En Línea]. s.l. Gobierno TI. 2011. Disponible en: https://gobiernoti.wordpress.com/2011/10/04/tipos-de-redes-informaticas/

ANEXOS

Anexo 1. Carta de Presentación de la propuesta

CARTA DE PRESENTACIÓN DE LA PROPUESTA

Neiva, 13 de mayo 2016

Doctor
Cesar Augusto losada parra
Director Administrativo y financiero
Ciudad

Ref.: Presentación Propuesta: limplementar un sistema de diagnóstico y monitoreo de la red de datos de la Empresa Sociedad Clínica Emcosalud

Cordial saludo;

Respetuosamente, me dirijo a Usted, para presentar formalmente la propuesta del proyecto de grado denominado: Implementación de un sistema de diagnóstico y monitoreó de la red de datos, para optar al título de: Especialista en Seguridad Informática en que otorga la Universidad Nacional Abierta y A Distancia - UNAD.

Adjunto proyecto en medio magnético.

Agradezco de antemano, la colaboración prestada.

Atentamente;

CESAR AUGUSTO CELIS PERDOMO
CEL: 3152406164
Email: cesar.celis.perdomo@hotmail.com

FRANCY PATRICIA TRUJILLO MURCIA
CEL: 3132092141
Email: franpatri2011@hotmail.com

Anexo 2. Resumen Analítico En Educación – Rae

Universidad Nacional Abierta y a Distancia	**FORMATO**
	RESUMEN ANALÍTICO EN EDUCACIÓN - RAE
Fecha de Aprobación:	**Página 99 de 103**

1. Información General	
Tipo de documento	Monografía
Acceso al documento	Universidad Nacional Abierta y a Distancia
Título del documento	PROPONER UN SISTEMA DE DIAGNÓSTICO Y MONITOREO QUE PERMITA IDENTIFICAR EVENTOS PARA RESOLVER PROBLEMAS DE INFRAESTRUCTURA DE TI, DE LA RED DE DATOS DE LA EMPRESA SOCIEDAD CLÍNICA EMCOSALUD
Autor(es)	Cesar Augusto Celis Perdomo, Francy Patricia Trujillo Murcia
Director	Erika Liliana Villamizar Torres
Palabras Claves	Palabras Claves: Red de datos, Sistema de Monitoreo de red, NAGIOS, Colasoft, capsa9free, Wireshark, Trafico de Red, Centro de Cableado.

2.Descripción
El presente proyecto se centra en proponer un sistema de diagnóstico y monitoreo que permita identificar eventos para resolver problemas de infraestructura y seguridad de TI de la red de datos de la Empresa Sociedad Clínica Emcosalud. Para este fin se realiza un estudio detallado a la red física, así como al tráfico de datos en la misma, con diversas aplicaciones que están presentes en el mercado y son especializadas en detectar anomalías en el funcionamiento de las redes tanto de origen físico de red como de origen lógico por mal uso de los usuarios. El proyecto solo abarca la sugerencia de implementación de la herramienta más conveniente para el monitoreo de la red, y se hacen recomendaciones de mejoras físicas y lógicas a la red de datos, para que sean tomadas en cuenta por la gerencia en pro de mejorar el rendimiento, la disponibilidad y seguridad de la red de datos de la empresa.
3.Fuentes

ARBELAES, Luis Guillermo. Diagnóstico de la Red de Comunicaciones de la Universidad católica de Pereira [En línea]. Pereira: Universidad Católica de Pereira. 2013., 118 p. Disponible en: http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/1736/CDMIST69.pdf?sequence=1

DORADO, Juan Luis. Conceptos Básicos sobre planificación de redes [En Línea]. s.l. Diario de Planificación y Diseño de Redes y Servicios 2012. Disponible en: https://diarioredesyservicios.wordpress.com/2012/01/11/conceptos-basicos-sobre-planificacion-de-redes/

ECHEVERRÍA, Carlos. La importancia del monitoreo de red en la implementación de soluciones de negocios [En línea]. México: Mundo Contact. 2014., Disponible en: http://mundocontact.com/la-importancia-del-monitoreo-de-red-en-la-implementacion-de-soluciones-de-negocios/.

MEDINA RAFAEL, José Manuel. Seguridad en redes [En Línea]. Veracruz: Universidad Veracruzana. 2013. 88 p. Disponible en: http://cdigital.uv.mx/bitstream/123456789/32368/1/medinarafaeljosemanuel.pdf

MORENO, Jonny. Arquitectura para el monitoreo de redes [En línea]. S.l. https://morenojhonny.wordpress.com. 2012. Disponible en: https://morenojhonny.wordpress.com/2012/06/15/6-1-arquitectura-para-el-monitoreo-de-redes/.

MUÑOZ, Juan. ¿Por qué es importante monitorizar nuestra red? [En línea]. Madrid: www.tecnozero.com. s.f. Disponible en: https://www.tecnozero.com/blog/por-que-es-importante-monitorizar-nuestra-red/

PAESSLER. Monitorización de red como elemento esencial en el concepto de seguridad de TI [En línea]. Alemania. Paessler AG. s.f. Disponible en: https://www.es.paessler.com/press/whitepapers/security

VEGA TIRADO, Rafael Emiro. Et al. Proyecto Monitoreo y gestión de redes [En línea]. Antioquia: Servicio Nacional de Aprendiza SENA regional Antioquia.

2008. Disponible en: https://es.scribd.com/doc/11526277/Proyecto-Monitoreo-Y-Gestion-de-la-Red-Final

GÓMEZ VIEITES, Álvaro. Tipos de ataques e intrusos en las redes informáticas [En línea]. s.l. Escuela de Negocios Caixanova. 2014. Disponible en: http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

MEJÍA HERRERA, Luis Fernando. Que es gestión y monitoreo de red [En línea]. s.l. Luis Fernando Mejía Herrera administración de redes. 2009. Disponible en: http://servidorespararedes.blogspot.com.co/2009/01/que-es-aplicaciones-web.html

WIKIPEDIA. Monitoreo de red [En línea]. s.l. Wikipedia la Enciclopedia Libre. s.f. Disponible en: https://es.wikipedia.org/wiki/Monitoreo_de_red

GOBIERNO DE LAS TIC. Tipos de Redes Informáticas [En Línea]. S.l. Gobierno TI. 2011. Disponible en: https://gobiernoti.wordpress.com/2011/10/04/tipos-de-redes-informaticas/

4.Contenidos

El documento inicia con el resumen, la introducción y las palabras abstractas, luego encontramos la definición y formulación del problema que se presenta en la red de datos en la sede principal de Sociedad Clínica Emcosalud, con su respectiva justificación del estudio de fallos y recomendación de un sistema de monitoreo de redes que mejore y garantice el correcto funcionamiento de la infraestructura tecnológica y de comunicaciones en la empresa.

Luego está el objetivo general “Recomendar a la empresa sociedad clínica EMCOSALUD un sistema de diagnóstico y monitoreo que le permita identificar eventos para resolver problemas de infraestructura de TI, de su red de datos”, con sus respectivos objetivos específicos para lograr alcanzarlo.

Sigue el marco referencial, el cual contiene el marco teórico que habla sobre la los avances alcanzado por las redes de datos y lo imprescindibles que se han vuelto en las empresas, pero también muestra que son vulnerables a personas mal intencionadas que las convierten en su blanco de acción logrando extraer información importante trasmitidas en ellas, generar mal funcionamiento y hasta caídas totales del servicio.

Por lo anterior se hace importante implementar medidas de protección y detección de anomalías en las redes de datos.

En el siguiente apartado encontramos el marco contextual el cual contiene los conceptos y definiciones importantes para comprender la temática del proyecto, el marco legal que no es más que la normatividad relacionada con el buen uso de los recursos tecnológicos y la protección a los datos administrados y tratados con ellos.

El marco contextual es la información relacionada con la empresa Sociedad Clínica Emcosalud, los servicios que ofrece, como se encuentra distribuida, con sus respectivos planos, su organigrama y el logo institucional.

La metodología de desarrollo del proyecto se puede visualizar las acciones realizadas para lograr el cumplimiento de los objetivos del mismo, la metodología de la investigación habla del tipo de investigación realizada en el proyecto y como se logró la recolección de información importante.

El siguiente apartado corresponde al desarrollo del proyecto en el cual se evidencia el análisis de los recursos tecnológicos de la Sociedad Clínica Emcosalud, iniciando con la información correspondiente al inventario de activos de la oficina de tecnología, la documentación de procesos y políticas de seguridad de los sistemas de información en la empresa. Luego se continúa con el análisis de los activos físicos de la infraestructura tecnológica de la red de datos y los hallazgos encontrados en los mismos, así como la seguridad de las instalaciones físicas en donde se encuentran.

El siguiente punto es el análisis lógico y de tráfico de la red de datos, en este punto se utilizaron 4 herramientas disponibles en el mercado que cumplen las funciones de monitoreo de redes, ellas son: Wireshark, Colasoft Capsa9 Free, Nagios y GlassWire.

Por ultimo encontramos la herramienta de monitoreo seleccionada como la más cumple como solución a las necesidades de la empresa y las recomendaciones físicas y lógicas para optimizar la red de datos de la Sociedad Clínica Emcosalud.

5.Metodología

La metodología utilizada en el proyecto es aplicada, en una primera fase la investigación bibliográfica que consistió en la consulta de diversas fuentes bibliográficas electrónicas (libros virtuales, artículos, revistas y publicaciones electrónicos disponibles en línea en Internet). Una segunda fase con investigación de campo mediante observación directa de los componentes que conforman la red de datos y entrevistas con los funcionarios de la oficina de tecnología, los cuales conocen de forma concreta la problemática presentada. Por último se realizaron pruebas de herramientas de monitoreo, para constatar

la información suministrada por los funcionarios y de esta forma identificar posibles fallos de la red de datos.

6.Conclusiones

- Al revisar y monitorear los dispositivos de la red nos permite tener un control en tiempo real, determinando la prestación del servicio y sus condiciones actuales.

- Las simulaciones de tráfico son de gran ayuda y funcionalidad para determinar el comportamiento de nuestros dispositivos y la red.

- Se puede concluir que el análisis y monitoreo de la red es fundamental para una buena administración y control.

- Realizar el diagnóstico de la red de comunicaciones de la Sociedad Clínica Emcosalud, le permitirá al área de sistemas contar con un documento actualizado, donde se caracterice su infraestructura., con miras a mejorar la administración y hacer una gestión de red mucho más eficiente, basado en el sistema de gestión de red.

- La definición de los niveles de priorización de los dispositivos es fundamental para organizar adecuadamente la infraestructura con miras a soportar los usuarios y servicios que cada piso que se va a atender.

- Un buen plan de mejoramiento si se va a tener en cuenta la priorización del tráfico, antes debe contar con pruebas y mediciones que argumenten su utilidad, de lo contrario no aplicaría.

Elaborado por:	Cesar Augusto Celis Perdomo y Francy Patricia Trujillo Murcia		
Revisado por:			
Fecha de elaboración del Resumen:	24	07	2017