IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN LA CLÍNICA OFTALMOLÓGICA SAN DIEGO

DORIAN ALONSO GÓMEZ BARRIENTOS
OSCAR GIOVANNY HENAO CARDENAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN- PEREIRA
2017

IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN LA CLÍNICA OFTALMOLÓGICA SAN DIEGO

DORIAN ALONSO GÓMEZ BARRIENTOS
OSCAR GIOVANNY HENAO CARDENAS

Trabajo de grado para optar al título de especialista en Seguridad Informática

DIRECTOR
JUAN JOSE CRUZ GARZÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN- PEREIRA
2017

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

11 de Febrero de 2018.

DEDICATORIA

La presente tesis la dedicamos a Dios por permitir el cumplimiento de los objetivos. A nuestros padres, porque ellos siempre están a nuestro lado brindándonos su apoyo en cada uno de los retos que se nos presentan en la vida.

AGRADECIMIENTOS

Al Doctor Humberto Contreras Díaz, por brindarnos todo su apoyo y poner a su disposición cada uno de los recursos de la Clínica de Oftalmología Sandiego, a cada uno de los docentes de la Universidad Nacional Abierta y a Distancia por proveernos las herramientas e impartir el conocimiento para poder culminar este gran proyecto.

TABLA DE CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE GRÁFICAS

Pág.

RESUMEN

El presente proyecto pretende la implementación de un sistema de detección de intrusos en la clínica oftalmológica San Diego, con el objetivo de minimizar las vulnerabilidades informáticas que se puedan presentar. Mediante el uso de un software libre se procura una solución intencionada a proteger la red corporativa de la mencionada clínica, de modo que se puedan reducir a sus mínimas expresiones las posibilidades de apropiación por parte de los intrusos de la información y datos que se preservan en los servidores, puesto que tal información es confidencial y sus datos se podrían utilizar para beneficio personal o para la comisión de actos delictivos.

PALABRAS CLAVE: Prevención y detección de intrusos, IDS, software libre, confidencialidad de la información.

INTRODUCCIÓN

Las redes de computadores facilitan el acceso a la información agilizando procesos y estableciendo relaciones entre las interdependencias para agilizar y capturar una única vez la información y de esta manera evitar duplicidad en los datos.

La información se puede catalogar como el principal activo intangible de las compañías actuales, por lo que es perentorio pensar en el tema de la seguridad de la información, pues con el auge de la tecnología de manera paralela se han incrementado los ciber crímenes lo que han puesto en juego la confidencialidad de la información.

Es por esto, que es necesario y urgente tomar todas las medidas preventivas posibles para evitar un escenario que facilite el acceso a la información de manera no autorizada y de esta manera minimizar los riesgos de la seguridad de la información, los sistemas de detección de intrusos entre otras cosas permiten monitorear y analizar en tiempo real los posibles ataques de intrusión a la red corporativa.

La Clínica de Oftalmología Sandiego a pesar de tener sistemas pagos y libres de protección para evitar que la información de sus pacientes, clientes y asociados sea capturada de manera ilícita necesita fortalecer sus medidas de protección, pues no está exenta de ataques informáticos. Por tal razón se pretende implementar un sistema de protección con el fin prevenir y controlar el acceso no autorizado a los servidores de la Clínica de oftalmología Sandiego con la instalación de software libre especializado para prevención de intrusos.

Este proyecto se realiza pensando en que los elementos que se encuentran en la red de la empresa son susceptibles de diversos tipos de ataques, ya sea para la apropiación de datos, para la denegación de los servicios que se prestan, para la realización de estafas, etc. Por ello, los sistemas encargados de proteger de dichos ataques, cada vez están tomando más importancia y son más relevantes en el diseño de las organizaciones. Con un sistema como el que se pretende implantar, una correcta gestión de los elementos e incidencias, y una buena política de seguridad, la empresa estará libre de la mayor parte de las amenazas del exterior.

El principal problema dentro de la red informática de la Clínica de Oftalmología Sandiego es que no está debidamente protegida contra ataques informáticos, los cuales pueden causar vulnerabilidad y pérdida de información indispensable para la

institución, también la manipulación de información importante por otros usuarios que tengan acceso a ella, siendo necesario implementar una gran cantidad de requisitos de seguridad para la protección de sus recursos. Por lo cual las fortalezas resultantes de la planeación, elaboración e implementación del proyecto que se presenta son las siguientes:

- Realizar Monitoreo y análisis de eventos y del comportamiento de los usuarios.
- Realizar Pruebas del estado de seguridad de la configuración de sistemas
- Seguimiento de cambios a la configuración base de seguridad de los sistemas.
- Reconocimiento de patrones de eventos que corresponden con ataques conocidos.
- Reconocimiento de patrones de actividad que estadísticamente difieren del comportamiento normal
- Alerta al personal apropiado por medios apropiados cuando un ataque ha sido detectado
- Proveer políticas de seguridad de la información

Al medir el impacto que nuestro proyecto tendrá se basará en la ventaja de utilizar productos de detección de intrusos que proporcionan a los administradores un monitoreo activo, ya que pocas personas revisan los archivos de registro y si lo hacen se hace de manera extemporánea y poco rigurosa lo que implica un riesgo de seguridad.

1. TITULO

IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN LA CLÍNICA OFTALMOLÓGICA SAN DIEGO

2. DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

En diferentes espacios se han desarrollado estudios, investigaciones y proyectos de grado sobre seguridad informática en nuestro caso nos interesan los que tratan en específico sobre implementación de sistemas de detección de intrusos (IDS). Existen análisis de seguridad a diferentes empresas y también universidades, un ejemplo está en el proyecto PROPUESTA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE DETECCION DE INTRUSOS (IDS) EN EL CELE (el Centro de Enseñanza de Lenguas Extranjeras de la Universidad Nacional Autónoma de México) (Hinojosa), al realizar una revisión de la información encontrada, se puede decir que en el CELE hay varios áreas o departamentos que tienen como característica el manejo de datos sensibles, especialmente las áreas que manejan los cobros de matrícula.

Dando un ejemplo de cual información es susceptible por pérdida o robo de datos, podemos decir que son los datos financieros de los alumnos y del propio CELE.

Al reconocer la principal vulnerabilidad que posee el CELE tenemos que decir que son los equipos de cómputo del personal académico, profesores y administrativos, dado que se encuentran en el mismo dominio de broadcast.

A continuación, se listan algunos posibles ataques:

•Man in the Middle

•Rootkits

•Backdoors

•Computadora Zombie (o alguna actividad botnet, como DoS)

•Usurpación o Robo de identidad

•Ingeniería Social

•Keystroke logging

•Spamming

Se tiene un segundo antecedente el cual es “SISTEMA DE PREVENCIÓN DE INTRUSOS PARA MEJORAR LA SEGURIDAD DE LOS SERVIDORES DE LA UNIVERSIDAD NACIONAL DE TRUJILLO” proyecto relacionado con un sistema de prevención de intrusos con el objetivo de ampliar las contramedidas de seguridad de los servidores de esa universidad. Esta investigación tiene un paso a paso para realizar la implementación de un IDS con software de licenciamiento libre de manera que genere reportes en tiempo real sobre las posibles intrusiones en el sistema.

2.2 FORMULACIÓN DEL PROBLEMA

Pregunta orientadora:

¿Es posible prevenir y controlar el acceso no autorizado a los servidores de la Clínica de oftalmología Sandiego con la instalación de software libre especializado para prevención de intrusos?

2.3 DESCRIPCION DEL PROBLEMA

Las empresas en la actualidad independientemente del sector productivo donde se encuentren requieren que su información cumpla con los pilares básicos de la seguridad de la información: confidencialidad, integralidad, disponibilidad y autenticación. Pues los datos están expuestos a múltiples riesgos lo que puede ocasionar daños que afecten el que hacer misional de la empresa, la imagen corporativa e incluso en casos extremos afectar la continuidad de negocio.

Al ser la información un activo intangible valioso, a nivel interno o externo siempre se está en riesgo de accesos no autorizados con el fin de vulnerar y o manipular la información con el propósito de tener utilidad indebida de la información obtenida. Con el auge y los avances de las tecnologías de información y las telecomunicaciones, las medidas de protección y prevención embebidas en los periféricos de red como switches, routers, UTM's no son suficientes para cubrir y proteger los ataques que día a día van evolucionando por ello se hace necesario implementar nuevas herramientas complementarias a las ya existes, posibilitando con estos tener control, monitoreo y bloqueos en el escenario de posibles ataques realizados por los delincuentes informáticos.

La Clínica de Oftalmología Sandiego posee información sensible y protegida por la ley como son las Historias Clínicas Digitales las cuales se encuentran alojadas en servidores de la clínica. A pesar de que se cuentan con protecciones para evitar el acceso no autorizado se hace necesario redoblar y garantizar estrictos protocolos y herramientas de sistemas de control y monitoreo activo para detectar los ataques informáticos y las vulnerabilidades de seguridad

2.4 JUSTIFICACIÓN

La Clínica de Oftalmología Sandiego es una institución prestadora de servicios especializada en la rama de oftalmología y todas sus subespecialidades convirtiéndose en la clínica de especialistas más grande de Suramérica, invirtiendo en tecnología biomédica de punta y garantizando que sus procesos cumplan con los más altos estándares.

Mediante la implementación de un sistema de prevención de intrusos Clínica de oftalmología Sandiego minimizará los riesgos de que personas no autorizadas accedan a datos catalogados como confidenciales.

Adicionalmente la Clínica de oftalmología Sandiego está vigilada por la Superintendencia Nacional de Salud de Colombia y la Superintendencia de Industria y comercio, los cuales regulan y controlan la privacidad de los datos para información sensible y custodia de las historias clínicas digitales.

La confidencialidad y custodia de historias clínicas digitales en Colombia está normada por la resolución 1995 de 1998 emitida por el Ministerio de Salud (hoy Ministerio de Salud y de la protección Social), dicha resolución establece que las historias clínicas digitales deben ser integrales, secuenciales, racionales científicamente y deben contar con disponibilidad en los términos que la ley orienta.

Por otro lado, la ley estatutaria 1581 de octubre de 2012 emitida por el Congreso de Colombia regula mediante unos principios rectores el tratamiento de datos personales.

En razón a lo anterior la Clínica de Oftalmología Sandiego debe proteger y garantizar que la información alojada en sus servidores con datos personales clínicos y sensibles tenga las medidas extremas de protección para evitar uso inadecuado de la información reposada en las historias clínicas y demás información sensible y que pueda causar afectación a terceros o problemas legales a la empresa.

Con este proyecto se pretende diseñar e implementar un sistema de detección de intrusos, con el propósito de que la seguridad de la información soportada en un buen sistema de seguridad, apoye y apalanque los objetivos estratégicos de la entidad. Los objetivos planteados en este proyecto, están orientados a poder

diseñar un adecuado Sistema de Gestión de Seguridad de la Información para la entidad, con el propósito de poder generar los siguientes beneficios:

- **Garantizar su Misión y Alcanzar su visión:** Al diseñar un Sistema de Gestión de Seguridad, este nos proveerá las herramientas adecuadas que nos permita garantizar la protección y aseguramiento de la información, lo que es vital para una segura gestión administrativa, operativa, financiera, y técnica de la empresa, que permita garantizar su Misión y el alcance de su Visión.

- **Disminuir costos:** Un sistema de gestión enfocado en la seguridad puede ayudar a la organización a mitigar los riesgos e incurrir en gastos innecesarios.

- **Cumplimiento normativo:** Un Sistema de Gestión de Seguridad permite determinar el estado real de la seguridad de la información de la entidad, conocer las posibles amenazas que la puedan afectar y establecer las acciones efectivas para mitigarlas, lo cual, indique una adecuada gestión de riesgos que garantizan la debida protección de la información y la privacidad de los datos personales de los clientes, lo cual, ayuda al cumplimiento de la normatividad vigente relacionada con seguridad de la información.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Implementar mediante el uso de herramientas libres un sistema de prevención y detección de intrusos para evitar el acceso no autorizado a la red corporativa de la Clínica de Oftalmología Sandiego.

3.2 OBJETIVOS ESPECÍFICOS

1. Analizar la infraestructura actual de la red de la Clínica de Oftalmología Sandiego e identificar los riesgos a los que está expuesta la red corporativa.

2. Levantar la información de la topología de red de la Clínica Sandiego.

3. Investigar herramientas de licenciamiento libre que apliquen para la infraestructura actual de la Clínica Sandiego y que permitan la detección y prevención de intrusos.

4. Implementar y configurar software libre para evitar el acceso no autorizado de intrusos a la red corporativa.

5. Documentar el proceso del sistema de prevención para la clínica Sandiego

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 ¿Qué es Seguridad?

Es una acción que busca proteger un determinado bien y servicio partiendo bajo las premisas de confiabilidad, protección y cuidado.

- SEGURIDAD INFORMÁTICA.

Es una especialidad de la seguridad de la información, cuyo objetivo es velar por la seguridad del parque informático y los datos de manera que se cumplan con los principios básicos de la seguridad de la información: confiabilidad, oportunidad, disponibilidad y veracidad.

TIPOS DE SEGURIDAD INFORMÁTICA

Según Ecured, 2017[1] la seguridad se divide en:

Seguridad física, seguridad ambiental y seguridad lógica.

- Seguridad física

Cuando se hace referencia a la seguridad física bajo el punto de vista de la seguridad de la información se refiere a cada uno de las metodologías aplicada para prevenir y detectar cualquier tipo de riesgo del sistema de cómputo.

Para poder controlar la seguridad física se requiere el uso de barreras y procedimientos para mitigar los riesgos de substracción o manipulación de los datos desde el hardware.

[1] ECURED “Seguridad Informática”. {En línea}. {10 de abril de 2017}

- Seguridad ambiental

Adicionalmente a los riesgos y/o daños que se pueden causar por personas malintencionadas, también existen amenazas externas que ponen en riesgo la seguridad de la información y que son causas por el ambiente tales como:

- Tormentas Eléctricas
- Ciclones
- Terremotos
- Vibraciones
- Humedades
- Inundaciones
- Incendios

Con el fin de minimizar las amenazas relacionadas con la seguridad ambiental se recomienda la aplicación de las siguientes reglas básicas:

- Instalar protectores de pico de tensión para todos los equipos críticos.
- Instalación de sensores de temperatura, de humo, de inundación y de emisión de gases.
- Instalar sistemas de refrigeración y aires acondicionados para evitar la condensación de calor en el hardware.

- Seguridad lógica

Hace referencia a las contramedidas para impedir el acceso no autorizado a la información.

4.1.2 mecanismos de seguridad

Según el sitio Web CMM, Introducción a la seguridad informática como mecanismos de seguridad se define:

"Generalmente, los sistemas de información incluyen todos los datos de una compañía y también en el material y los recursos de software que permiten a una compañía almacenar y hacer circular estos datos. Los sistemas de información son fundamentales para las compañías y deben ser protegidos." [2]

En relación a los mecanismos de seguridad como mínimo deben cumplir con las siguientes premisas:

- Integridad: Es la correspondencia entre lo que está y lo que se requiere.
- Confidencialidad: Garantizar que los datos sean privados y reservados.
- Disponibilidad: Es el uso de manera oportuna para acceder a la información, de manera que esté disponible en el momento que se requiera.
- Evitar el rechazo: Esto permite garantizar al no repudio, de manera que no se pueda negar que la información es fidedigna.
- Autenticación: Mediante está restricción se garantiza que solo personal autorizado tengan acceso a los datos.

4.1.3 ¿qué es un sistema de detección de intrusos?

Un Sistema de Detección de Intrusos o IDS (Intrusion Detection System) es una herramienta de seguridad que se encarga de monitorear los diferentes eventos que ocurren en un sistema informático, en el que busca de intentos de intrusión. Se puede definir intento de intrusión como cualquier intento en donde se compromete la información afectando la confidencialidad, disponibilidad, integridad pues existen

[2] CMM "Introducción a la seguridad informática". {En línea}. {22 de febrero de 2017}

atacantes locales, atacantes con privilegios pero que desean acceder a otras funcionalidades y/o usuarios que tienen derechos pero hacen mal uso de ellos.

¿Por qué utilizar un IDS? Se debe utilizar un IDS en las empresas con el fin de proteger sus sistemas de las amenazas que aparecen al incrementar la conectividad en red y la vez por la dependencia que se tiene hacia los sistemas de información. Los IDSs están ganando espacio como una pieza fundamental en la infraestructura de seguridad de las empresas. Existen varias razones para adquirir y usar un IDS, entre las cuales tenemos:

Se utiliza con el fin de prevenir problemas al evitar que atacantes accedan a nuestro sistema. Pero igualmente puede jugar en nuestro contra, dado que al tener un sistema de seguridad con un buen nivel de sofisticación puede hacer crecer la curiosidad de los atacantes.
Al implementar un IDS es posible detectar ataques y otras violaciones de la seguridad que no son detectadas por otras medidas de protección. Los atacantes, usan técnicas que son ampliamente conocidas, permitiendo esto conseguir accesos no autorizados a diferentes sistemas, principalmente a aquellos conectados a redes públicas. La mayoría de veces ocurre cuando las vulnerabilidades conocidas no son corregidas.

En algunos sistemas heredados, no es posible que los sistemas operativos sean actualizados o parcheados. Inclusive en los sistemas en los que se pueden aplicar parches, los administradores muchas veces no tienen el tiempo y recursos para instalar las últimas actualizaciones que se necesitan. Esto es un problema normal, sobre todo en aquellos ambientes que incluyen un gran número de hosts con sistemas operativos y hardware diferente.

Un sistema de detección de intrusos es una maravillosa herramienta de protección de sistemas. Un IDS permite detectar cuando un atacante intenta penetrar un sistema explotando un fallo no que no ha sido corregido. De esta manera, se podría avisar al administrador para que se realizará un back up del sistema de forma inmediata, evitando de esta forma que se pierda información vital.

4.1.4 IDSs basados en red (NIDS)

Por lo general un sistema IDS tiene una arquitectura basada en red. Este tipo de sistema monitorea en tiempo real cada uno de los paquetes de la red y en el

momento en que identifica un paquete no reconocido como confiable o que identifica como un señuelo para acceder de manera ilícita a la red, genera los mecanismos de protección para un segmento o para la red completa.

Los sistemas de detección de intrusos que son basados en red poseen por lo general un conjunto de sensores que monitorean el tráfico analizando la información que sea enviada a través de la red, por lo general este tipo de sensores trabajan en segundo plano de manera que sea imperceptible para el atacante.

Ventajas:

- Un sistema de IDS puede monitorizar una red LAN con múltiple cantidad de hosts.

- El impacto de los NIDSs no interfiere de manera significativa en las operaciones propias y normales de la red.

- Son configurables, los sensores de detección pueden ser tan exigentes o tan laxos como se requieran.

Desventajas:

- No es posible analizar la información que es transmitida de manera cifrada.

- Los IDS no pueden solo monitorean las intrusiones, pero no pueden identificar si los ataques lanzados fueron efectivos o no.

- Para algunos NIDS se les dificulta identificar los ataques que viene con paquetes de red fragmentados.

4.1.5 IDSs basados en host (HIDS)

Este tipo de detectores de intrusos analiza y realiza una auditoría sobre la información que se recoge como lo pueden ser los archivos de sistema. De esta

manera este tipo de sistemas de detección de intrusos analiza de manera precisa y forense cada uno de los procesos, usuarios y recursos del sistema involucrados.

Ventajas

- Tienen la capacidad de realizar auditorías en tiempo real de manera local a un host, cosa que los IDS basados en red no pueden hacer.

- Es posible en algunos casos analizar el tráfico de red con información cifrada.

Desventajas:

- El costo de los HIDS es mayor en relación con el costo de NIDS, pues un sistema de host tiene que monitorear cada host a diferencia de la detección de intrusos por red que se analizan a nivel de paquetes de red.

- No es posible detectar ataques lanzados de manera global a la red, sino que se identifica host por host.

- Pueden ser deshabilitados mediante la metodología de Denegación de Servicio (DoS)

Interfieren en el performance del host pues hace uso de los recursos del host disminuyendo en algunos la velocidad y rendimiento del equipo monitoreado.

4.2 MARCO LEGAL

De acuerdo a la resolución 1995 de 1998 emitida por el ministerio de salud (hoy ministerio de la protección social) la Historia Clínica es un documento “obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del usuario, los actos médicos y los demás procedimientos del equipo de la salud.”[3]

La Historia Clínica en general está regida por las siguientes normas:

4.2.1 Ley 23 de 1981

- Articulo Nº33 Las prescripciones médicas se harán por escrito, de conformidad con las normas vigentes.
- Artículos Nº34 La historia clínica es el registro obligatorio de las condiciones de salud del paciente. Es un documento privado, sometido a reserva, que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos.
- previstos por la ley.
- Articulo Nº35: En las entidades del Sistema Nacional de Salud la Historia Clínica estará ceñida a los modelos implantados por el Ministerio de Salud.

4.2.2 Ley 80 de 1989

- Que se hace necesario expedir las normas correspondientes al diligenciamiento, administración, conservación, custodia y confidencialidad de las historias clínicas, conforme a los parámetros del Ministerio de Salud y del Archivo General de la Nación en lo concerniente a los aspectos archivísticos contemplados

[3] COLOMBIA. MINISTERIO DE SALUD. Resolución número 1995 de 1999. Por la cual se establecen normas para el manejo de la historia clínica [En línea]. Gaceta del congreso. Bogotá, 8, julio, 1999. Pag 1

4.2.3 Resolución 2905 de 1994.

- Con la cual se reglamente la epicrisis como resumen de la historia clínica.

4.2.4 Resolución 1995 de 1999

- Establece las normas para el manejo de la historia clínica. Podrán acceder a la información contenida en la Historia clínica en los términos previstos en la ley: 1. El usuario, 2. El equipo de salud, 3. Las autoridades judiciales y de salud en los casos previstos por la ley, 4. Las demás personas determinadas por la ley.

En relación a la confidencialidad de la información está reglamentado por:

4.2.5 Artículo 15 de la Constitución Política de Colombia

- Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley. Con el fin de prevenir la comisión de actos terroristas, una ley estatutaria reglamentará la forma y condiciones en que las autoridades que ella señale, con fundamento en serios motivos, puedan interceptar o registrar la correspondencia y demás formas de comunicación privada, sin previa orden judicial, con aviso inmediato a la Procuraduría General de la Nación y control judicial posterior dentro de las treinta y seis (36) horas siguientes. Al iniciar cada período de sesiones el Gobierno rendirá informe al Congreso sobre el uso que se haya hecho de esta facultad. Los funcionarios que abusen de las

medidas a que se refiere este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar. Para efectos tributarios judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

4.2.6 Ley estatutaria 1266 de 2008

- por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

4.2.7 Ley 1581 de 2012

- Por la cual se dictan disposiciones generales para la protección de datos personales

4.2.8 Decreto 2952 de 2010

- por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

4.3 ESTADO DEL ARTE

Se tienen algunos proyectos similares de la implementación de un IDS enfocado a la investigación y el análisis, por lo que se tomara de manera general algunos conceptos y puntos de vista de los mismos:

En una primera sección se presentan las ideas generales de cada estudio. La segunda sección discute más en detalle cada uno de estos estudios, identificado con la misma numeración romana que se usa en esta primera.

I. "Implementación de políticas de seguridad informática para las universidades de Risaralda"[4]: Este proyecto que data desde el 2014, tiene como objetivo demostrar las prácticas no sanas de la seguridad informática y su omisión en cuento a políticas y socialización en las instituciones universitarias. En este trabajo se propone un IDS con un alcance claro y definido ayudado por algunas herramientas de detección de intrusos.

   En este proyecto se identifica la importancia de la promoción de la seguridad informática en las organizaciones pues de acuerdo al análisis se evidenció la poca existencia de conocimiento y de procedimientos relacionados con la seguridad de la información.

II. Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda[5]*, para prevención de intrusos, que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización:* Este proyecto tiene como principal objetivo implementar un sistema de gestión de seguridad informática el cual de manera general contiene:

[4] SIERRA, Óscar "Implementación de políticas de seguridad informática para las universidades de Risaralda". {En línea}. {5 de Marzo de 2017} disponible en:(http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2370/0058S572.pdf?sequence=1)

[5] UNAD "Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda". {En línea}. {18 de Abril de 2017} disponible en: (http://repository.unad.edu.co/bitstream/10596/3777/1/20904541.pdf).

- Contextualización del estado actual.
- Matriz de análisis de Riesgos de la aseguradora Suarez Padilla & Cia Ltda
- Valoración de cada uno de los activos
- Matriz de clasificación y amenazas
- Estado actual de cumplimiento de la norma ISO/IEC 27002:2005 en la organización.

- Análisis del sistema de gestión documental de la organización.
- Creación de Políticas, definición de los controles de cada uno de los dominios de la norma ISO 27001 y establecimiento de los controles necesarios para minimizar los riesgos en relación a los sistemas de seguridad informática.

5 DISEÑO METODOLÓGICO

5.1 TIPO DE INVESTIGACIÓN

El tipo de investigación es aplicada, porque permite trabajar con metodologías y técnicas que están fundamentadas con bases teórico – científica, que nos van a servir como el punto de partida en la solución de problemas de la institución.

Para Vargas Cordero, este tipo de investigación busca “la aplicación o utilización de los conocimientos adquiridos, a la vez que se adquieren otros después de implementar y sistematizar la práctica basada en investigación”[6] y dado el caso que compete a este proyecto en el cual se ponen de manifiesto los saberes adquiridos, este tipo de investigación aplica perfectamente.
la investigación aplicada permite una retroalimentación de conocimientos y es válida tanto para las novedades en el plano técnico, artesanal, industrial e incluso el científico, tal como lo plantea el mismo autor citado anteriormente.

Método metodología:

5.2 HIPOTESIS

Hipótesis de investigación (HI):
La implementación de un sistema de detección de intrusos en la clínica oftalmológica San Diego, minimiza los riesgos informáticos y ayuda a preservar la información de un hipotético ciberataque.

Hipótesis nula (HO):

[6] VARGAS CORDERO, Zolia Rosa. LA INVESTIGACION APLICADA: UNA FORMA DE CONOCER LAS REALIDADES CON EVIDENCIA CIENTIFICA. Revista educación, 2009. pp, 155-165

la implementación de un sistema de detección de intrusos en la clínica oftalmológica San Diego, no minimiza los riesgos informáticos y ayuda a preservar la información de un hipotético ciberataque.

5.3 IDENTIFICACIÓN DE VARIABLES

Variable independiente: Sistema de Prevención de Intrusos.
Variable dependiente: Mejorar la Seguridad de los Servidores.

Medición:

Dimensiones:
Depuración eficaz de correlación de evento
Alertas en tiempo real
Exclusión de eventos inusuales o anormales

5.4 POBLACIÓN Y MUESTRA

La población y muestra que se determino es el número de servidores que existen en la oficina de sistema de cómputo, cuya cantidad es de 3, esto se justifica debido a ser una cantidad menor que 30.

5.5 TÉCNICAS Y PROCEDIMIENTOS DE RECOLECCIÓN DE DATOS

5.5.1 Recolección de datos

Fuentes primarias

La información requerida para esta investigación se obtuvo a través un cuestionario y entrevistas realizadas a los trabajadores de la oficina de sistemas e informática (cómputo).

Fuentes secundarias

También recopilamos información bibliográfica: trabajos de investigación, paper's, tesis, libros, todo material escrito relacionado directamente relacionado con la prevención de intrusos en una red LAN.

5.5.2 Técnicas e instrumentos

Las técnicas a utilizar para nuestra investigación se presentan a continuación:

La observación

Este método permite hacer la recolección de manera presencial sobre cualquier incidente o fallo que pueda presentarse basado en lecciones aprendidas.

La entrevista

Se realizará a cada trabajador de la oficina de sistemas e informática (computo), para obtener puntos de vista de cada trabajador sobre la seguridad que posee cómputo y sobre los problemas que aqueja.

La encuesta

En esta se realizará un cuestionario para los trabajadores, realizando preguntas cerradas sobre la seguridad de la oficina de cómputo.
El instrumento a utilizar será: el cuestionario.

Software

El software que se utilizará será el IDS snort, el cual se dedica a escanear el tráfico de los paquetes en una red, lo colocaremos en funcionamiento para la captura de los paquetes los cuales luego analizaremos.

5.6 MÉTODOS Y PROCEDIMIENTOS

ESQUEMA TEMATICO

Descripción de Recursos Informáticos. La red de Clínica de Oftalmología Sandiego posee una topología “Estrella” para la comunicación de todos los organismos que pertenecen a la empresa

Descripción de Recursos informáticos

La infraestructura física de la clínica consta de:

Ubicación	Descripción
Sótano 2	Parqueadero privado médicos
Sótano 1	Parqueadero empleados y visitantes
Piso -2	Parqueaderos y oficina copropiedad
Piso -1	Parqueaderos y oficina de ingenierías
Piso 1	Área de admisiones, VIP y Diagnóstico
Piso 2	Área de Quirófanos
Piso 3	Área administrativa
Piso 4	Consultorios especializados desde 401-425
Piso 5	Consultorios especializados desde 501-525
Piso 6	Consultorios especializados desde 601-625
Piso 7	Consultorios especializados desde 701-725

Tabla 1División por zona por pisos. Fuente: Los Autores

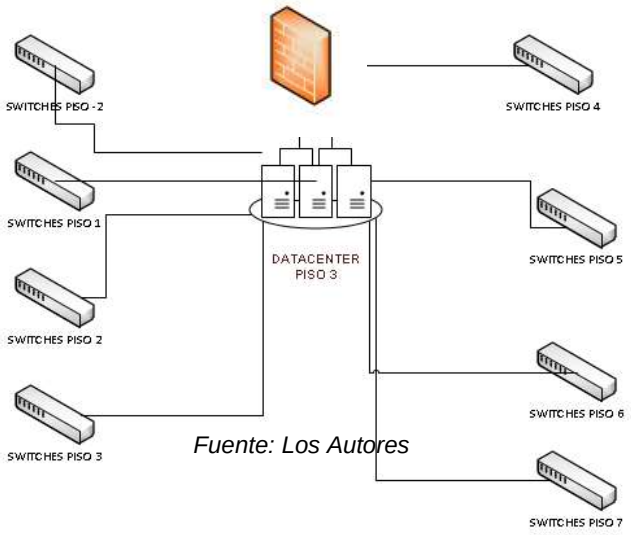
Se tienen los siguientes cuartos de sistemas en el edificio:

- Piso -2
- Piso 1
- Piso 2
- Piso 3
- Datacenter Piso 3
- Piso 4
- Piso 5

- Piso 6
- Piso 7

La interconexión entre cada cuarto se realiza mediante buitrones y mediante un backbone en fibra óptica realizando una red en estrella:

Ilustración 1 Infraestructura Clínica de Oftalmología Sandiego.

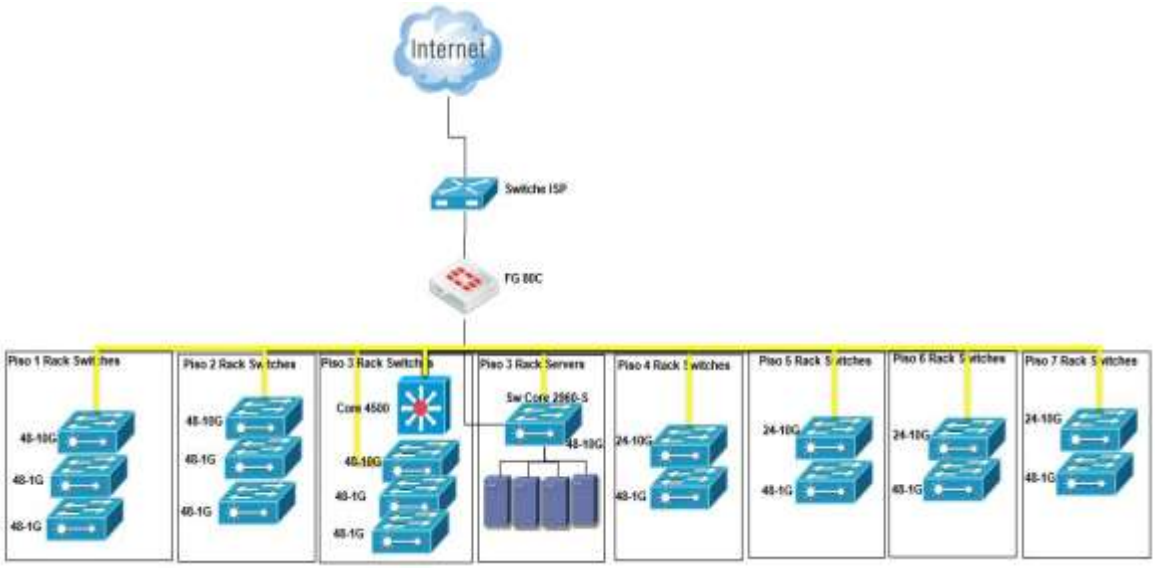


Fuente: Los Autores

Diseño de Subnetting

Se tiene la siguiente distribución de las redes:

Ilustración 2. Diseño de Subnetting. Clínica de Oftalmología Sandiego.



Fuente: Los Autores.

El diseño de subnetting está basado en VLAN la cuales se describen a continuación:

Ilustración 3 Direccionamiento VLAN Clínica de Oftalmología Sandiego

DIRECCIONAMIENTO IP CLINICA OFTALMOLOGIA SAN DIEGO									
Vlan	**Area**	**ID de red**	**Mascara subred**	**Host inicial**	**Host final**	**Broadcast**	**Gateway**	**# Host**	**ID Vlan**
1	WIFI Publico	10.1.0.0/22	255.255.252.0	10.1.0.1	10.1.3.254	10.1.3.255	10.0.1.1	1022	10
2	Clinica	10.1.4.0/23	255.255.254.0	10.1.4.1	10.1.5.254	10.1.5.255	10.1.4.1	510	11
3	Consultorios	10.1.6.0/24	255.255.255.0	10.1.6.1	10.1.6.254	10.1.6.255	10.1.6.1	254	12
4	Equipos biomedicos	10.1.7.0/24	255.255.255.0	10.1.7.1	10.1.7.254	10.1.7.255	10.1.7.1	254	13
5	CCTV	10.1.8.0/24	255.255.255.0	10.1.8.1	10.1.8.254	10.1.8.255	10.1.8.1	254	14
6	Dispositivos de red	10.1.9.0/24	255.255.255.0	10.1.9.1	10.1.9.254	10.1.9.255	10.1.9.1	254	15
7	Servidores	10.1.10.0/24	255.255.255.0	10.1.10.1	10.1.10.254	10.1.10.255	10.1.10.1	254	16
7	Impresoras	10.1.11.0/25	255,255,255,128	10.1.11.1	10.1.11.126	10.1.11.127	10.1.11.1	126	17
8	Sistemas	10.1.11.128/25	255,255,255,128	10.1.11.129	10.1.11.254	10.1.11.255	10.1.11.129	126	18
9	Voz	10.1.12.0/24	255.255.255.0	10.1.12.1	10.1.12.254	10.1.12.255	10.1.12.1	254	19
10	Crecimiento Futuro	10.1.13.0/24	255.255.255.0	10.1.13.1	10.1.13.1	10.1.13.255	10.1.13.1	254	20

Fuente: Los Autores

Plataforma de switching

Se tienen un Switch Core Cisco 4500 en el DataCenter y Switches de borde en cada uno de los sitios:

Ilustración 4. Especificación de Switching

Centro Cableado Piso 1			
Dispositivo	**Referencia**	**Serial**	**Nombre**
Switch 48P	48TD-L	FOC1803S1KG	Switch1CC1
Switch 48P	48TS-L	FCW1808A5BU	Switch2CC1
Switch 48P	48TS-L	FCW1808A5GA	Switch3CC1
Centro Cableado Piso 2			
Dispositivo			**Nombre**
Switch 48P	48TD-L	FCW1804A2TH	Switch1CC2
Switch 48P	48TS-L	FCW1808A5LD	Switch2CC2
Switch 48P	48TS-L	FCW1808A5AY	Switch3CC2
Centro Cableado Piso 3			
Dispositivo			**Nombre**
Switch 24P	WS-C4500	JAE18250BHN	Switch1CoreCC3
Switch 48P	48TD-L	FOC1803S1UG	Switch2CC3
Switch 48P	48TS-L	FCW1808A5B4	Switch3CC3
Switch 48P	48TS-L	FCW1808A59M	Switch4CC3
Switch 48P			Switch5ServerCC3
Centro Cableado Piso 4			
Dispositivo			**Nombre**
Switch 24P	24TD-L	FOC1806S0YU	Switch1CC4
Switch 48P	48TS-L	FCW1800A5MF	Switch2CC4
Centro Cableado Piso 5			
Dispositivo			**Nombre**
Switch 24P	24TD-L	FOC1806S0ZL	Switch1CC5
Switch 48P	48TS-L	FCW1808A5BY	Switch2CC5
Centro Cableado Piso 6			
Dispositivo			**Nombre**
Switch 24P	24TD-L	FOC1806S0YS	Switch1CC6
Switch 48P	48TS-L	FCW1808A5HH	Switch2CC6
Centro Cableado Piso 7			
Dispositivo			**Nombre**
Switch 24P	24TD-L	FOC1806S0XJ	Switch1CC7
Switch 48P	48TS-L	FCW1808A5BK	Switch2CC7
PISO -2			
Dispositivo	**Referencia**	**Serial**	**Nombre**
Switch 24P			Switch1CCSotano

Fuente: Los Autores

El switch core 4500 cuenta con la configuración de capa 3 en la red, definiendo sus interfaces vlans como puertas de enlace para todos los segmentos de la red.

```
interface Vlan1 description DHCP
ip address 192.168.0.231 255.255.254.0
ip helper-address 192.168.0.230
!
interface Vlan10 description WIFI_Publico
ip address 10.1.0.1 255.255.252.0
```

```
ip helper-address 192.168.0.230
!
interface Vlan11


description Clínica
ip address 10.1.4.1 255.255.254.0
ip helper-address 192.168.0.230
!
interface Vlan12 description Consultorios
ip address 10.1.6.1 255.255.255.0
ip helper-address 192.168.0.230
!
interface Vlan13
description Equipos_biomedicos ip address 10.1.7.1 255.255.255.0
ip helper-address 192.168.0.230
!
interface Vlan14 description CCTV
ip address 10.1.8.1 255.255.255.0
ip helper-address 192.168.0.230
!
interface Vlan15
description Dispositivos_de_red
ip address 10.1.9.1 255.255.255.0
ip helper-address 192.168.0.230
!
interface Vlan16 description Servidores
ip address 10.1.10.1 255.255.255.0
ip helper-address 192.168.0.230
!
interface Vlan17 description Impresoras
ip address 10.1.11.1 255.255.255.128
ip helper-address 192.168.0.230
!
interface Vlan18 description Sistemas
ip address 10.1.11.129 255.255.255.128
ip helper-address 192.168.0.230
!
interface Vlan19
description Crecimiento_futuro
ip address 10.1.12.1 255.255.255.0
ip helper-address 192.168.0.230
!


interface Vlan20
description Crecimiento_futuro
ip address 10.1.13.1 255.255.255.0
ip helper-address 192.168.0.230
```

En el despliegue de políticas de ACls se definió como parámetro de seguridad que la conexión de todos los switches se establezca por medio de SSH y solo desde los siguientes segmentos de red. Esto con el objetivo de garantizar la seguridad de los dispositivos.
10.1.9.0 0.0.
10.1.11.128
192.168.0.0
.

5.6.2 plataforma Wireless

La plataforma de APs está basada en una controladora Wireless Lan instalada en el rack principal del piso 3, a partir de este dispositivo se habilito el direccionamiento DHCP para la sincronización de los APs desplegados en la clínica.

Distribución de los APS en el Edificio

Tabla 2. Distribución de AP's en Clínica de Oftalmología Sandiego

Configuración Aps de la Clínica Oftalmología San Diego				
	Nombre del AP	**Referencia del**	**Serial**	**MAC del**
PISO 1	OPTICA	AIR-CAP2602I-	FTX1816J	B83861A1
	VIP DX	AIR-CAP2602I-	FTX1816J	B8386127
	MODULO 7	AIR-CAP2602I-	FTX1816J	B83861A1
	FACTURACION	AIR-CAP2602I-	FTX1816U	B83861B18
	DX	AIR-CAP2602I-	FTX1816U	B83861832
	UCE	AIR-CAP2602I-	FTX1816J	B83861832
PISO 2	Empleados	AIR-CAP2602I-	FTX1816U	B83861832
	Frente	AIR-CAP2602I-	FTX1816U	B83861B18
	Cafetín	AIR-CAP2602I-	FTX1816J	18E72821C
	Recepción VIP	AIR-CAP2602I-	FTX1816J	B8386127
	VIP 2 Piso	AIR-CAP2602I-	FTX1816U	B83861B18
	Mitad pasillo 2	AIR-CAP2602I-	FTX1816J	B83861B18
PISO 3	Gerencia	AIR-CAP2602I-	FTX1816U	B83861B18
	sin instalar	AIR-CAP2602I-	FTX1816U	B83861832
	Pasillo Archivo	AIR-CAP2602I-	FTX1816U	B83861A1
	Ascensores	AIR-CAP2602I-	FTX1816U	BB8361B1
	Call Center	AIR-CAP2602I-	FTX1816U	B83861A1
	Sistemas	AIR-CAP2602I-	FXT1816U	B83861B18
	Farmacia	AIR-CAP2602I-	FXT1820U	1005CAE82
	pasillo	AIR-CAP2602I-	FXT1816J	B8386A13
	Lobby	AIR-CAP2602I-	FTX1816J	B83861F31
	Lobby	AIR-CAP2602I-	FXT1820U	105CAE822
	Lobby	AIR-CAP2602I-	FXT1820U	1005CAE82
	Lobby	AIR-CAP2602I-	FXT1820U	1005CAE5E

Identificación de Procesos.

En esta fase o etapa nos permite determinar la finalidad q tiene la Oficina de Sistemas e Informática. Y de esta manera determinar la importancia que tiene la información que se maneja.

Tabla 2. Riesgos Asociados a los procesos

Procesos	Descripción	Riesgos	
		SI	NO
Administración de Datos de Médicos y Administrativos	Mantener actualizado los datos de los médicos y personal administrativo	X	
Administración del Sistema de control Biométrico	Control de entrada y salida de personal	X	
Administración del servidor web	Control del sitio Web de la clínica	X	
Administración del Sistema de Gestión	Llevar control del sistema de Atención al usuario	x	

Fuente: Los Autores

Identificación de Activos de información.

Tabla 3. Identificación de Activos de información

Procesos	Descripción	Activos de información
Administración de Datos de Alumnos, Profesores y Administrativos	Mantener actualizado los datos de los médicos y auxiliares y la parte administrativa	* Datos personales de la parte médica * Datos personales de la parte administrativa

Administración del Sistema de control Biométrico	Control de ingreso del personal	* Horas de entrada y salida del personal
Administración del servidor web	Control del sitio Web de la Clínica	* Página principal de la Clínica
Administración del Sistema de Gestión	Control del aplicativo de gestión de clientes	* Información de pagos * Información de citas

Fuente: Los Autores

Identificación de recursos de información.

Los recursos de información principales son:

- Procesos y Servicios

  - ❖ Administración de Datos de personal médico y administrativo.
  - ❖ Administración del Sistema de control Biométrico.
  - ❖ Administración del servidor web.
  - ❖ Administración del Sistema de Gestión de pagos y citas.

  - Aplicaciones Informáticas

La Clínica oftalmología sandiego trabaja con sus usuarios con aplicaciones informáticas, las cuales apoya a la gestión en los siguientes ámbitos:

Software de Sistemas
- ❖ Debian.
- ❖ Ubuntu.
- ❖ Windows

Gestores de Base de Datos
- ❖ MySQL.

- PostgreSQL.
- SQL Server

Servidor Web

- Apache.
- Apache TomCat
- IIS

Análisis de seguridad

Identificación de Amenazas: realizar un inventario clasificado de amenazas. Este inventario incluye unos valores de referencia de a frecuencia y el impacto de cada amenaza sobre cada uno de los tipos de recurso de información.

La Prevención de Intrusos abarcara lo concerniente a la seguridad lógica, y deja de lado lo referente a la seguridad física y ambiental.

- Errores y fallos no intencionados.

La Clínica Oftalmológica SanDiego, posee un alto porcentaje de usuarios que tienen conocimientos medios en el campo de la informática, y aún no ha implantado una política para fomentar a los usuarios sus conocimientos en este campo y así lograr reducir problemas como:

- Eliminación de archivos del sistema
- Desconfiguración de las impresoras.
- Contagio de Virus en discos duros y memorias.
- Descarga de Virus de internet.

- Vulnerabilidad del Software (plugins)

    - ❖ La falta de actualizaciones constantes de los servicios utilizados y actualización de sistema operativos.

    - ❖ La falta de un frameworks confiable de programación, que demuestre ser eficaz contra ataques.

    - ❖ La falta de un protocolo de encriptación para garantizar que el viaje de paquetes sea seguro y confiable

- Errores y fallos intencionados.

Uno de los principales problemas que afecta a la red es la mala configuración de red en cada piso de la clínica, que afecta el servicio de internet, ya que colocan switches y puntos WiFi para tener más puntos de acceso a internet lo que causa un gran congestionamiento de tráfico en la red.

Así mismo los atacantes pueden realizar un escaneo a la red completa y determinar puertos abiertos y vulnerabilidades de la red.

Algo que se evidencia mucho es que el personal deja las contraseñas por defecto o sin contraseñas, este es un problema muy a menudo ya que las personas no colocan contraseñas fuertes, larga, utilizando letras, signos y números por miedo a olvidarse.

5.6.3 Gestión de riesgo

Plan de gestión.

El plan de gestión requiere que se clasifiquen las amenazas y detectando puntos de control para cada una de ellas. Haciendo uso de las siguientes herramientas:

Identificación de políticas institucionales: las políticas son las medidas establecidas por la Clínica para mitigar sus riesgos. Las políticas pueden reducir la probabilidad de éxito de una amenaza, reduciendo, por tanto, su frecuencia y/o reducir el impacto en caso de producirse.

Al tener identificadas las amenazas a las que están expuestas en la red de la Clínica Oftalmológica SanDiego, realizaremos una clasificación de los riesgos

Procesos	**Descripción**	**Vulnerabilidad**
Administración de gestión de Datos de Alumnos, Profesores y Administrativos	Mantener actualizado los datos de los médicos y auxiliares y la parte administrativa	La información enviados desde el login viajan en texto plano y fácilmente legible. Ataques de tipo SQL-Inyection.
Administración del Sistema de control Biométrico	Control de ingreso del personal	Alteración del reporte de entradas y salidas, tanto como su eliminación. El equipo biométrico es vulnerable.
Administración del servidor web	Control del sitio Web de la Clínica	Caída del Servidor Web
Administración del Sistema de Gestión	Control del aplicativo de gestión de clientes	La información enviados desde el login viajan en texto plano y fácilmente legible. Ataques de tipo SQL-Inyection. Eliminación de registros

5.6.4 implementación de un sistema de prevención de intrusos.

Propuesta de IDS a implementar

Al observar los resultados obtenidos en un pen test realizado a la red, se propone la implementación de la herramienta Snort como medida de prevención contra intrusos, dado que éste es un sistema de detección de intrusiones basado en red (NIDS). Este sistema genera unas alertas para cuando se presentan estas vulnerabilidades, haciendo un registro del análisis obtenido y almacenándolo en su base de datos. Snort tiene disponibilidad bajo licencia GPL, es gratuito y funciona bajo diferentes plataformas Windows y GNU/Linux. En la actualidad es uno de los más usados y tiene una gran cantidad de filtros o patrones ya predefinidos, y actualizaciones permanentes.

- ❖ Elementos del sistema Snort

Los elementos que componen el esquema básico de su arquitectura son:

- Módulo de captura del tráfico. Este módulo es que se encarga de capturar todos los paquetes de la red, y para esto utiliza la librería libpcap.

- Decodificador. Es el encargado de formar las estructuras de datos con los paquetes que han sido capturados y a su vez identificar los protocolos de enlace, de red, etc.

- Preprocesadores. Tienen como función permitir extender las funcionalidades disponiendo los datos para la detección.

- Motor de Detección. Es el encargado de analizar los paquetes en base a las reglas especificadas para detectar los ataques.

- Archivo de Reglas. Es el que Define el conjunto de reglas que rigen el análisis de los paquetes detectados.

- Plugins de detección. Son partes del software que son compilados junto con Snort y su función es modificar el motor de detección.

- Plugins de salida. Son los permiten definir qué, cómo y dónde se guardarán las diferentes alertas y los paquetes de red que las generaron. Estos pueden ser archivos de texto, servidor syslog, bases de datos, etc.

- Módulo de captura de datos. Es el encargado de realizar la captura del tráfico que circula por la red, el cual aprovecha al máximo los recursos de procesamiento y por ende minimizando la pérdida de paquetes a tasas de inyección elevadas.

Snort requiere de bibliotecas externas para poder realizar la captura y análisis de los paquetes, de manera que cada uno de los procesos trabaje de manera independiente y le retorne a snort la función para la cual le fue encomendada.

Libpcap tiene la responsabilidad de capturar paquetes directamente de la tarjeta de interfaz de red. Esto permite que la facilidad de captura para paquetes raw suministrados por el sistema operativo esté con disposición a otras aplicaciones.

❖Preprocesadores

TCP/IP es un protocolo que es basado en capas y por ende cada capa tiene una función específica y para trabajar normalmente necesita una información.

Los paquetes de red llegan a su lugar de destino de manera aleatoria, el host receptor se encarga de organizar los paquetes de acuerdo a la secuencia lógica.

Snort tiene la función de leer todo el tráfico que pasa por la red y lo descifra, Por otro lado, tiene que llevar un control de todos los paquetes que se envían por la red, permitiendo darle forma a la información.

Los preprocesadores son componentes de Snort que no tienen una dependencia de las reglas, dado que el conocimiento sobre la intrusión depende del módulo Preprocesador. Estos se llaman cada que llegue un paquete, a los cuales se les puede aplicar reglas que estén precargadas en Snort. Se puede decir que su funcionalidad es entonces coger la información que viaja por la red de una manera desordena y darle una organización para que pueda ser interpretada. Por ende, cuando se tienen los datos ordenados que viajan por la red, se aplican las reglas con el fin de buscar un determinado ataque. La arquitectura de preprocesadores que posee Snort, reside en que tiene pequeños programas en C, los cuales toman decisiones sobre qué hacer con los paquetes. Una característica de estos programas es que se compilan junto a Snort en forma de librería.

La configuración que viene predeterminada para estos subsistemas es muy general, pero se podrán ajustar con el fin de obtener mejor rendimiento y resultados óptimos.

- **Reglas**. Las reglas o firmas son patrones que son buscados dentro de los paquetes de datos. El motor de detección utiliza estas reglas para comparar los paquetes recibidos y en caso de existir coincidencia entre el contenido de los paquetes y las firmas generar alertas. Si se necesitan añadir o eliminar clases enteras de reglas, se utiliza el archivo snort.conf.

❖ Categorías de reglas Snort

Hay 4 categorías de reglas que permiten evaluar un paquete (reglas de protocolo, reglas de contenido genéricas, reglas de paquetes mal formados y reglas IP). Y a su vez estas categorías están divididas en dos grupos, un grupo, las que tienen contenido y otro grupo, las que no tienen contenido.

- Reglas de Protocolo. Son reglas que son dependientes del protocolo que se está analizando, un ejemplo sería, en el protocolo Http, se encuentra la palabra reservada uricontent.

- Reglas de Contenido Genéricas. Estas permiten especificar patrones para buscar en el campo de datos del paquete, estos patrones pueden ser en modo ASCII o binarios, siendo muy importante para buscar exploits, los cuales por lo general suelen encontrarse en cadenas de tipo “/bin/sh”.

- Reglas de Paquetes Malformados. Especifica características sobre las cabeceras de los paquetes, que indican que se está produciendo algún tipo de anomalía, este tipo de reglas no miran el contenido solo comprueban que las cabeceras no contengan incoherencias u otro tipo de incoherencia.

- Reglas IP. La aplicación se realiza directamente sobre la capa IP, y son comprobadas para cada datagrama IP, esta clase de reglas analiza con contenido y sin él.

❖ **Personalización de reglas**

Una manera recomendada de limitar el tráfico de las alertas, es con la desactivación de reglas que no se van a aplicar en el sistema, para esto se debe ingresar en la configuración deSnort. El directorio /etc/snort/rules/ contiene varios archivos con la extensión .rules. Hay dos opciones, una es que se puede deshabilitar una clase entera de reglas comentándola en el archivo de configuración o también se puede deshabilitar reglas individuales si es requerida la protección del resto de reglas de la clase. Si se necesita comentar una regla específica, se busca en los archivos.rules adecuados y se ingresa un comentario delante de la línea de dicha regla.

Por lo regular es mejor deshabilitar una sola regla que toda la clase, a no ser que ésta no sea necesaria para una determinada configuración. El corazón de la funcionalidad de Snort es el motor de detección. Para que Snort detecte las últimas vulnerabilidades, es necesario actualizar las reglas.

Snort por defecto posee unas reglas estándar, que proporcionar una protección estable contra ataques conocidos, sin embargo, se puede diseñar algunas reglas personalizadas para que la red alcance el mejor beneficio del IDS.

Modificando nuestras propias reglas, se minimizará el riesgo de falsos positivos. Las reglas particulares tienden a poseer menos índices de falsos positivos mientras que las reglas que abarcan muchos casos generales suelen poseer índices altos.

Se pueden escribir reglas para:

- ✓ Registrar el acceso hacia o desde determinados servidores.
- ✓ Buscar determinados tipos de nombres de archivos en nuestra empresa
- ✓ Vigilar algunos tipos de tráfico que no pertenezcan a nuestra red.

El motor de detección.

Para poder realizar la detección de las actividades de intrusión en cada paquete el motor se basa en las reglas y compara cada una de las cadenas contra un patrón de referencia.

Los factores que intervienen en el tiempo de respuesta y en la carga del motor de detección son:

- ✓ Las características de la máquina.
- ✓ Las reglas definidas.
- ✓ Velocidad interna del bus usado en la máquina Snort.
- ✓ Carga en la red.

El motor de detección puede aplicar las reglas en distintas partes del paquete. Estas partes son las siguientes:

La cabecera IP. Puede aplicar las reglas a las cabeceras IP del paquete.

La cabecera de la capa de Transporte. Incluye las cabeceras TCP, UDP eICMP.

La cabecera del nivel de la capa de Aplicación. Incluye cabeceras DNS, FTP, SNMP y SMPT.

Payload del paquete. Se puede crear una regla que el motor de detección use para encontrar una cadena que esté presente dentro del paquete.

Propuesta de requerimientos e implementación

Para el correcto funcionamiento de Snort se aconseja el sistema operativo basado en Linux sin Interfax gráfica aunque la configuración sencilla de Snort corre en prácticamente en cualquier versión de Windows y de LInux, La recomendación es utilizar como mínimo dos particiones, una con el sistema operativo y la otra para almacenar los resultados de la captura; su tamaño debe depender de la cantidad de datos que se desee recopilar, y del tamaño de la red a analizar.

Propuesta para la protección del equipo

- Limitar acceso físico. Se deberá colocar el Snort en un área que sea segura, fácil de acceder, pero sólo por el personal autorizado, por lo que se instalará en el Datacenter el cual es un área restringida que cuenta con cámaras y control de acceso.

- Se deberá configurar el sistema para que inicie sólo desde disco duro.

- Control de acceso. Se deberá limitar el número de usuarios que acceden al sistema, para lo cual se tendrá una política de contraseñas adecuada.

- No instalar componentes adicionales, solo los necesarios

- Terminar todos los servicios que no se desean utilizar.
- Deshabilitar protocolos de red no utilizados.

- Establecer comunicaciones remotas si son necesarias con protocolos y aplicaciones seguras como IPSec SSH.

- Aplicar actualizaciones de seguridad, Services Pack y parches

5.6.5 implementación de ids snort en clínica de oftalmología sandiego

La colocación de Snort en la red de la Clínica San Diego se deberá tener tener en cuenta cual será tráfico que se quiere vigilar: paquetes entrantes, salientes, dentro del firewall, fuera del firewall. Se deberá colocar el IDS Snort de forma que se garantice la correlación en la red e interoperabilidad. Cuando hablamos interoperabilidad es que el sistema IDS Snort pueda compartir u obtener información de otros sistemas como firewalls, switches, router, permitiendo reconfigurar las características de la red, según los eventos que se generan.

Se puede colocar el IDS Snort así:

- Delante del firewall. De esta forma el IDS Snort puede comprobar todos los ataques producidos, sin embargo, puede que muchos de ellos no se hagan efectivos. A su vez se genera gran cantidad de información en los logs, que puede resultar equivocada.

- Detrás del firewall. Snort colocado detrás del firewall por lo regular es una opción ideal, dado que permite analizar, todo el tráfico que entra en la red.

De esta manera se garantizar que el IDS monitoree solo los paquetes que el firewall permitió pasar, teniendo en cuenta que Clínica de Oftalmología Sandiego cuenta con un UTM Fortinet modelo FG-80C y que tiene activo el IDS, por lo que protege de manera perimetral las conexiones externas.

- Combinación de los dos casos. Se pueden combinar Snort delante y detrás del firewall, esto permitirá que el control que se ejerza sea mayor. El mayor inconveniente es que se necesitan dos máquinas para la implementación.

- Firewall/NIDS Una opción es usar una única máquina que realice las funciones de firewall y de NIDS a la misma vez.

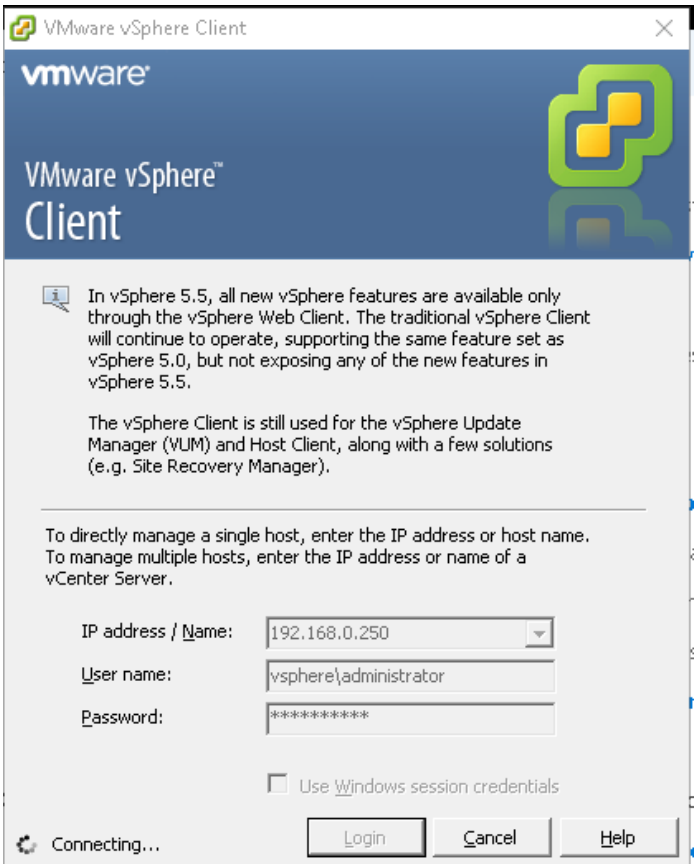
- Combinaciones avanzadas. Estos se utilizan en casos que se requiera una seguridad más alta. Un ejemplo sería el caso en que se necesite que cada NIDS monitorice un segmento de red o hosts individuales.

• Los IDS y las políticas de Seguridad. El IDS Snort deberá ser utilizado como un elemento complementario en las políticas de seguridad de la Clínica.

Proceso de Instalación

Para la instalación del sistema Snort se hace en la infraestructura virtualizada de la Clínica de Oftalmología Sandiego Vmware mediante la interfaz vsphere la cual interconecta a toda la plataforma centralizada Vcenter.

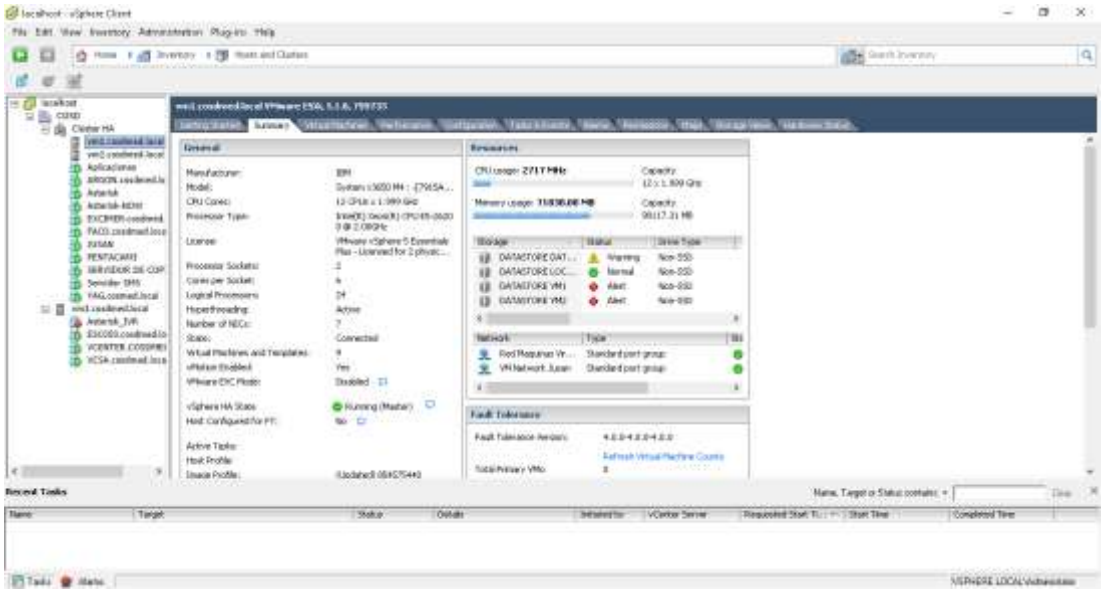
Ilustración 5 Acceder a la plataforma Vcenter Clinica Sandiego



Fuente: Los Autores

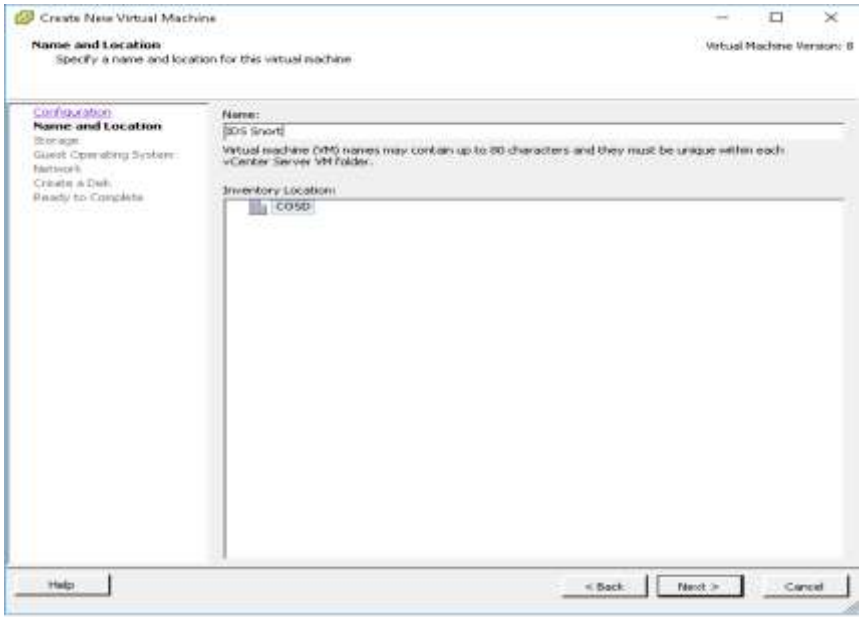
Para realizar el despliegue se hace uso del Host VM1 el cual hace parte del clúster HA (Alta disponibilidad).

Ilustración 6 Selección del Host para SNORT



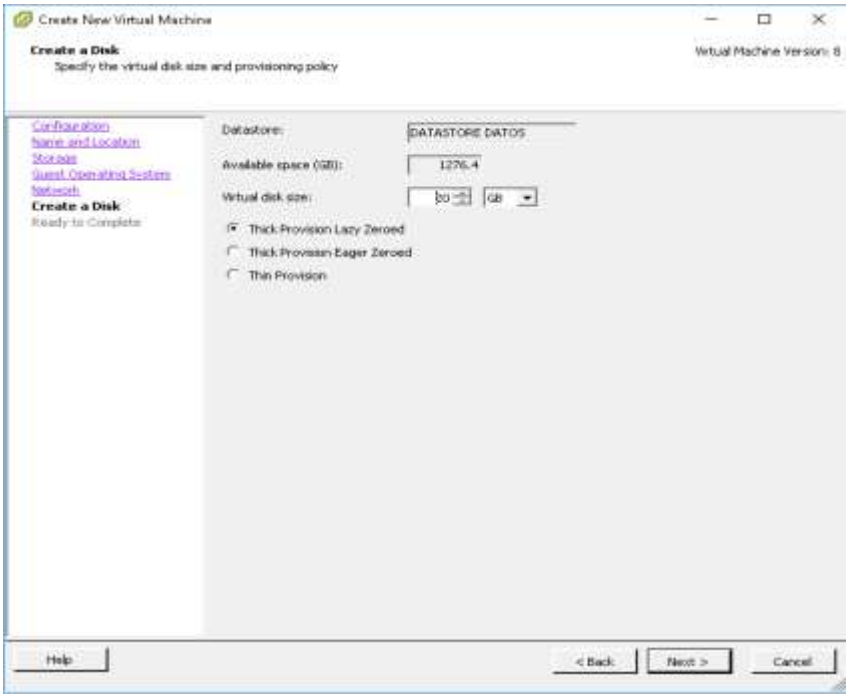
Fuente: Los Autores

Ilustración 7 Ubicacion e Identificación del SNORT



Fuente: Los Autores

Ilustración 8 Creación de Recursos



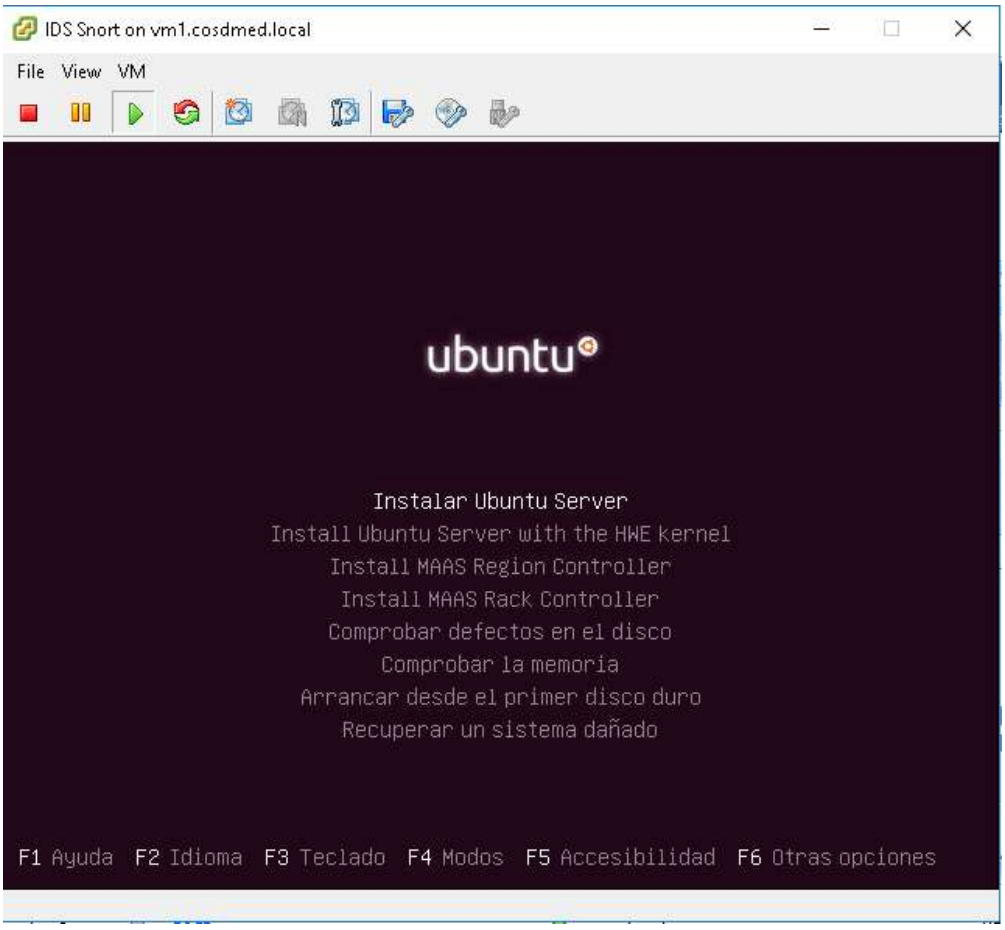
Fuente: Los Autores

Instalación del Sistema Operativo Ubuntu

Para la instalación del IDS Snort se seleccionó el sistema operativo Ubuntu Server versión 16 sin entorno gráfico, esto con el fin de aprovechar el rendimiento de la máquina y de evitar que sea vulnerada o manipulada.

El proceso de instalación se hace con los servicios estrictamente necesarios para que pueda correr correr SNORT y para administrar el sistema operativo.

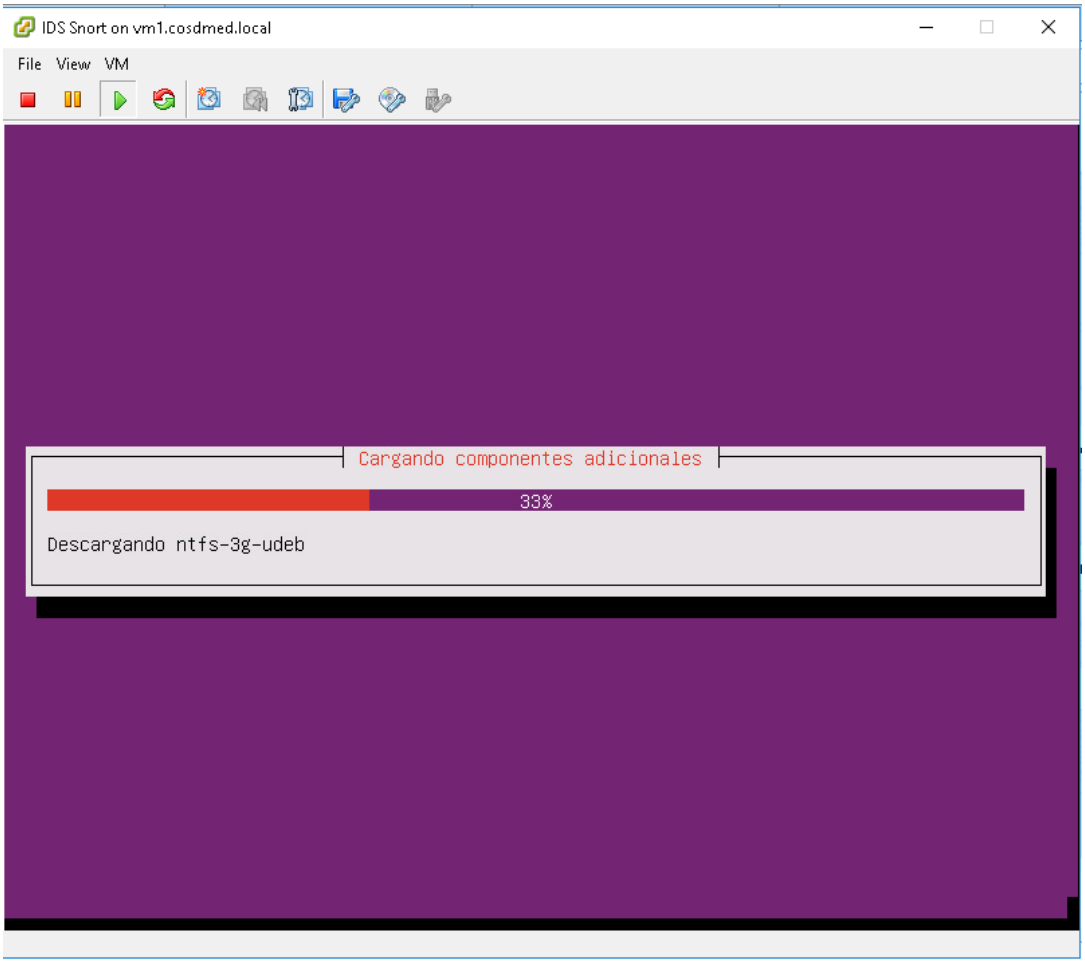
Ilustración 9 Proceso de instalación del sistema operativo



Fuente: Los Autores

Instalación de Snort

Ilustración 10Instalación de Snort en Clinica Sandiego

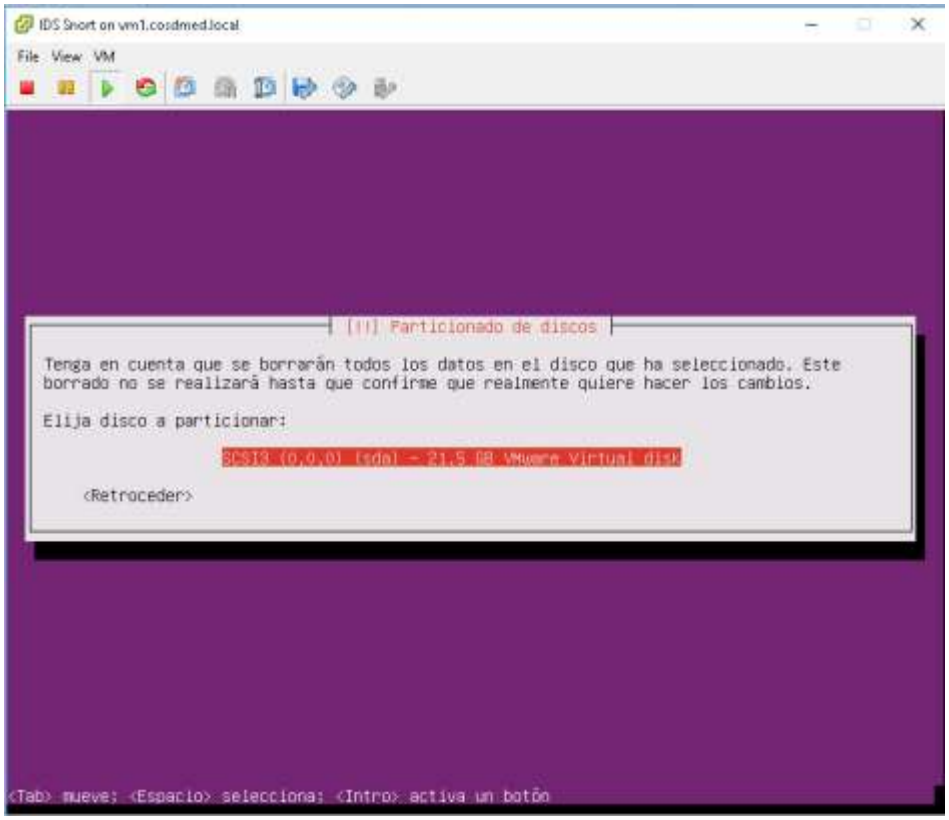


Fuente: Los Autores

5.6.6 Configuración del nombre del Host

De acuerdo a la política de seguridad informática de la Clínica de Oftalmología Sandiego se asigna el nombre al servidor virtualizado de acuerdo a su función principal o aplicativo que para este caso es Snort y se asigna una dirección Ip fija de acuerdo al pull de direcciones IP destinadas para servidores: 192.168.0.0/23

Ilustración 11 Asignación del nombre de la máquina

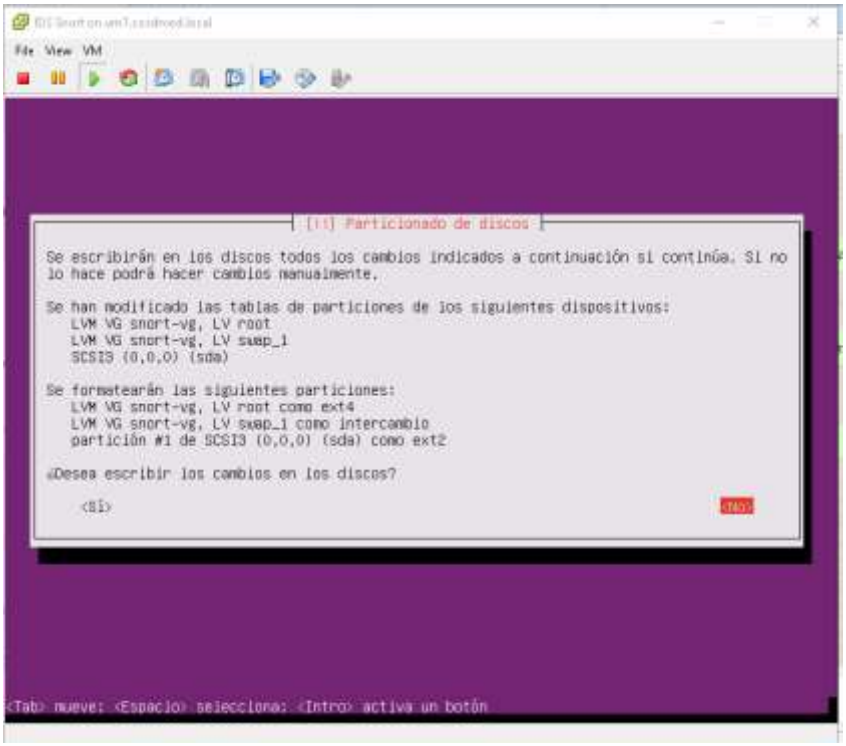


Fuente: Los Autores

Para la instalación se asignó un solo volumen, con la siguiente distribución y tipos de formato:

LV como root en Ext4
LV como swap_1 en intercambio
SDA como partición EXT2

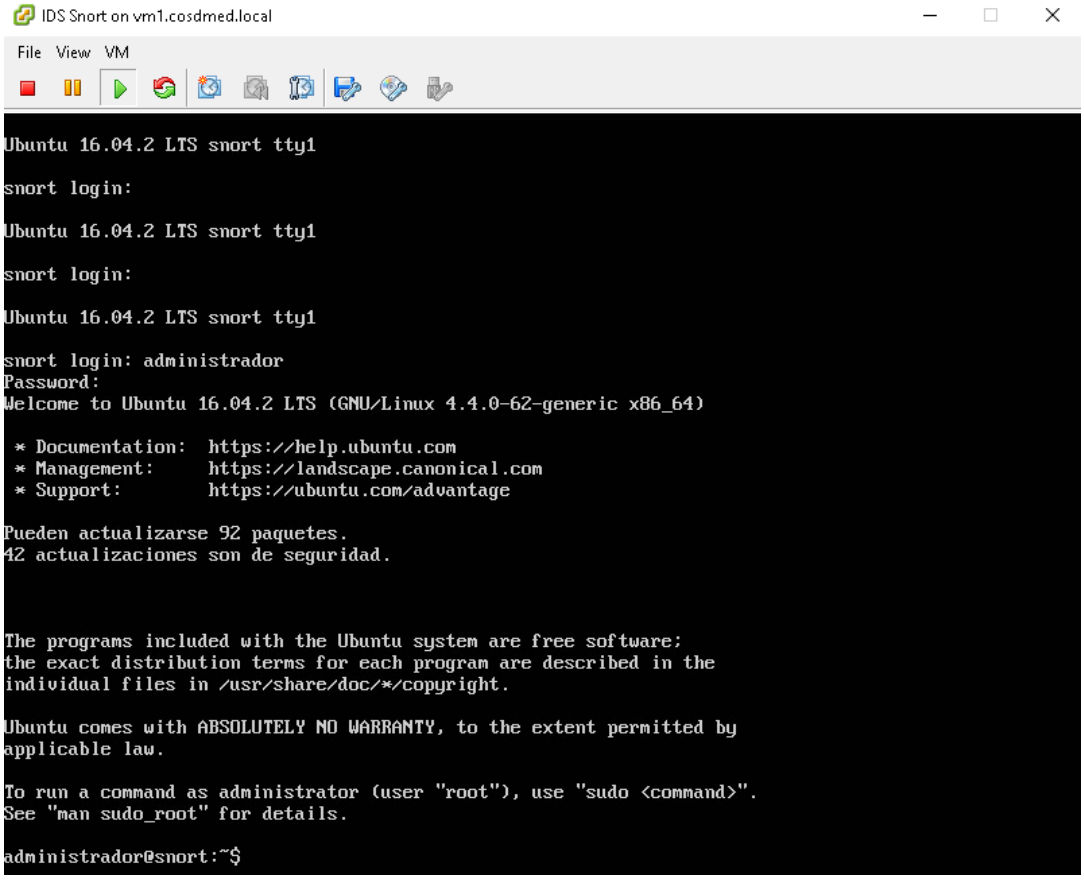
Ilustración 12 Particionado de discos



Fuente: Los Autores

Una vez se instala el sistema operativo se procede a la carga de la interfaz de texto del sistema operativo Ubuntu 16

Ilustración 13 Inicio de interfaz

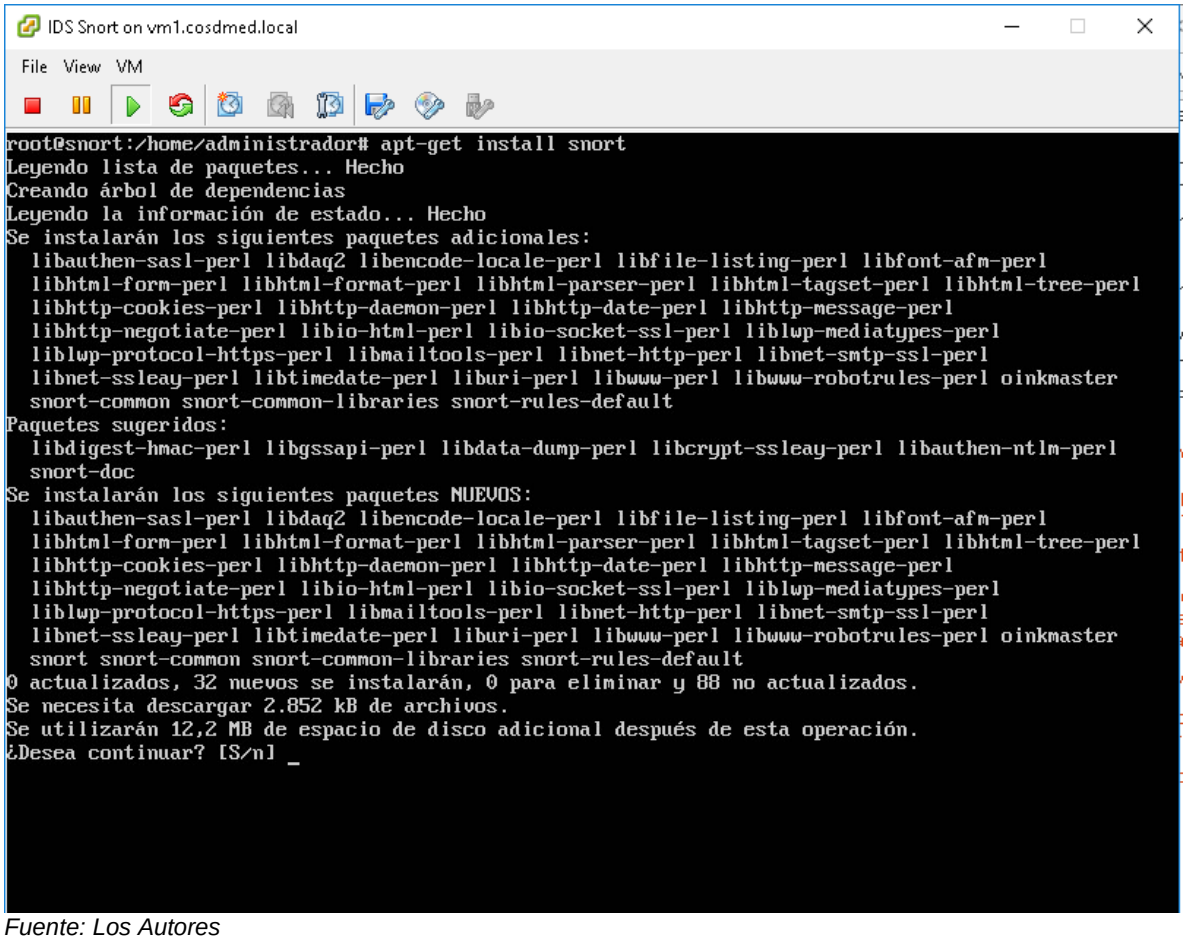


Fuente: Los Autores

5.6.7 Instalación de Snort

Para la instalación de Snort se utiliza el comando apt-get install snort para instalar el IDS Snort con todas sus dependencias:

Ilustración 14 Instalación de Snort

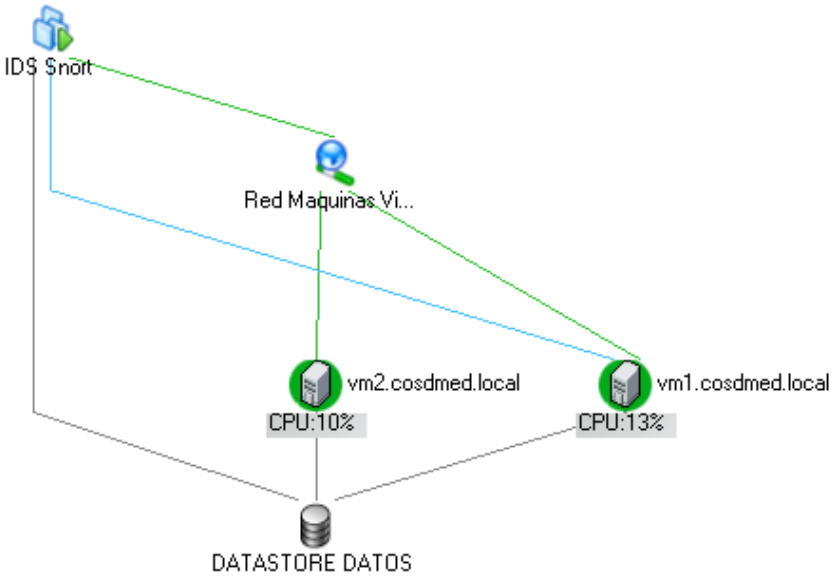


Fuente: Los Autores

5.6.8 Configuración de la interfaz de Red

En el momento de la creación de los recursos en el sistema de virtualización Vmware® se asignó solo una interfaz de red la cual está conectada a la red de máquinas virtuales 192.168.0.0/23 (Servidores) tal como se evidencia en la ilustración 16:

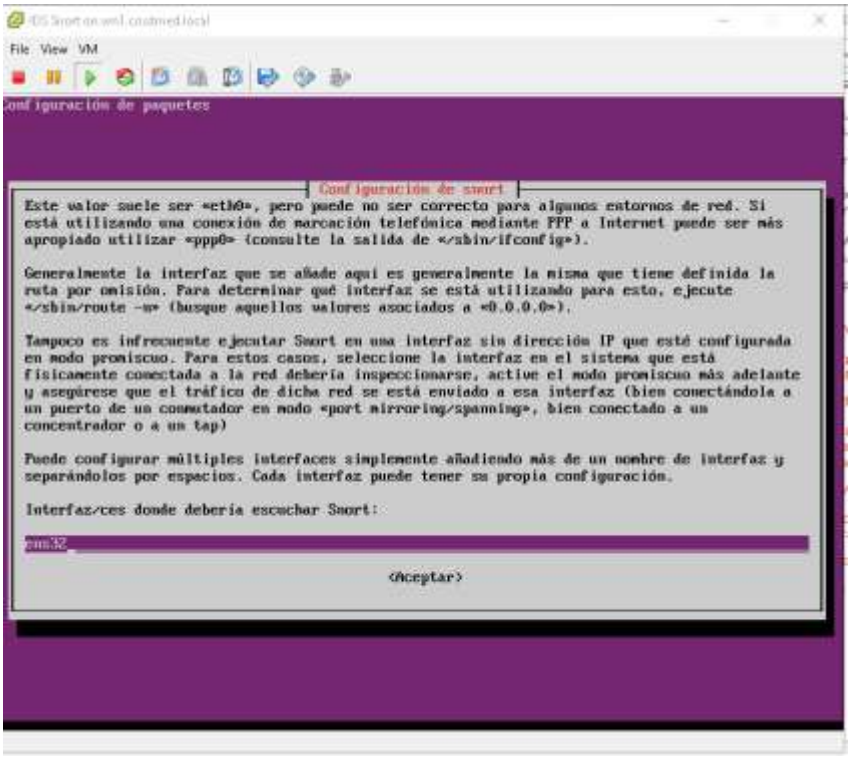
Ilustración 15 Estructura IDS Snort en Vmware



Fuente: Los Autores

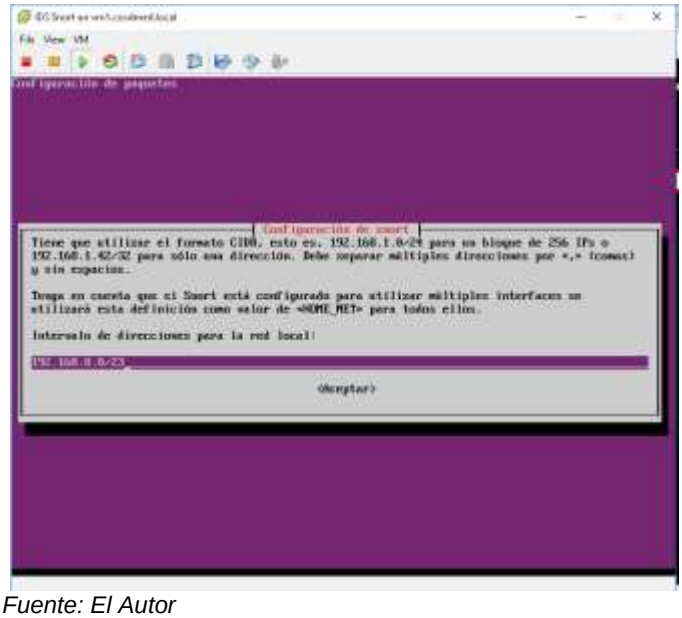
La interfaz que posee este equipo y que se puede visualizar en la ruta /sbin es la interfaz **ens32**

lustración 16Configuración de la interfaz de red para SNORT



Fuente: Los Autores

Ilustración 17 Seleccion de segmento de red en CDR

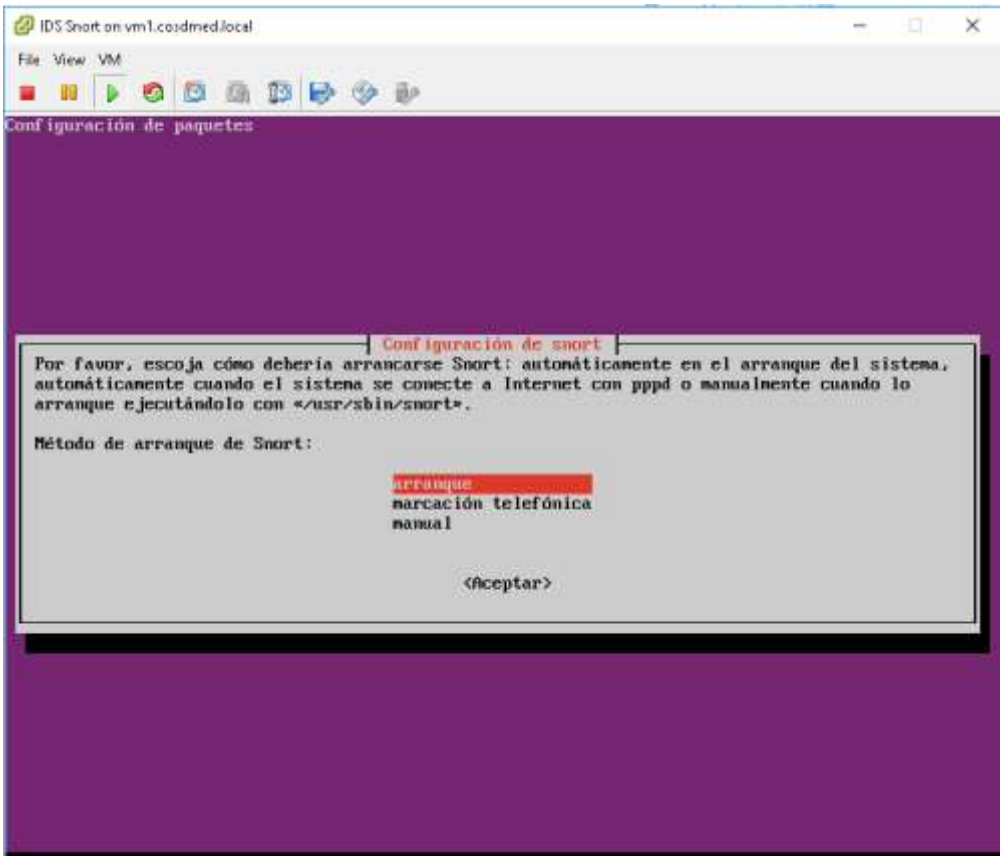


Fuente: El Autor

5.6.9 Selección de modo de arranque:

Se Selecciona modo de arranque automático para que la configuración se cargue en la ruta /etc/init.d y cuando el equipo se apague o reinicie de manera programada o abrupta

Ilustración 18 Modo de arranque Snort

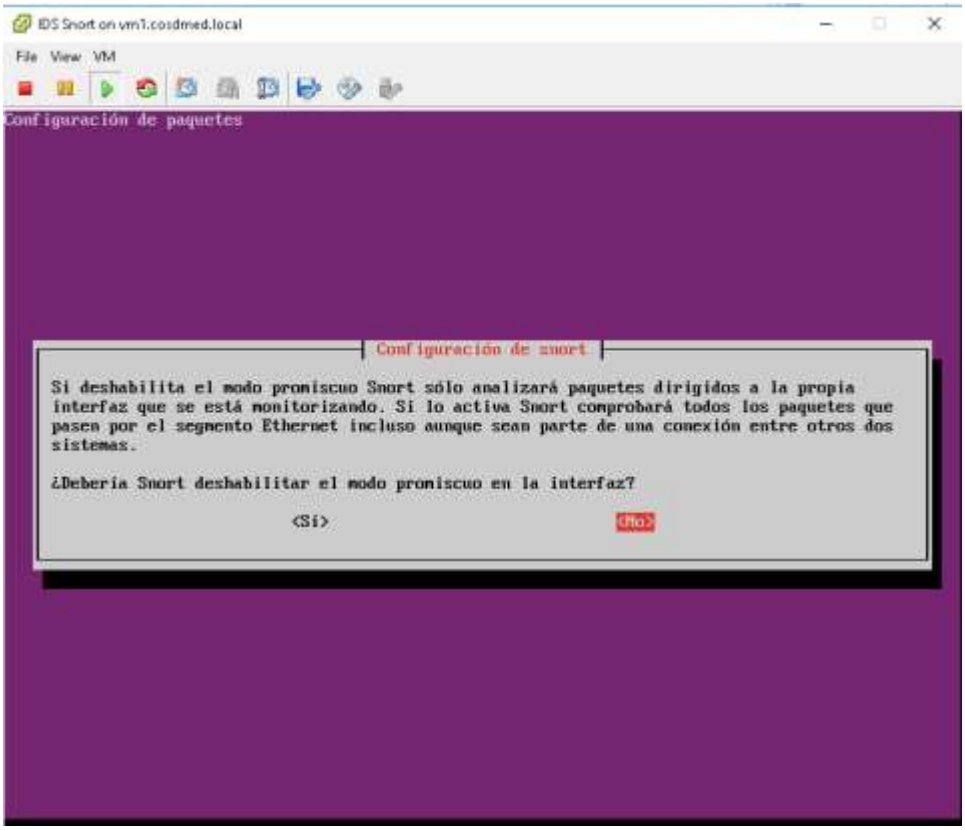


Fuente: El Autor

5.6.10 Configuración de Modo Promiscuo

Con el fin de que el IDS pueda analizar los paquetes que se transmiten por toda la red se configura el modo promiscuo:

Ilustración 19 Configuración de Modo Promiscuo

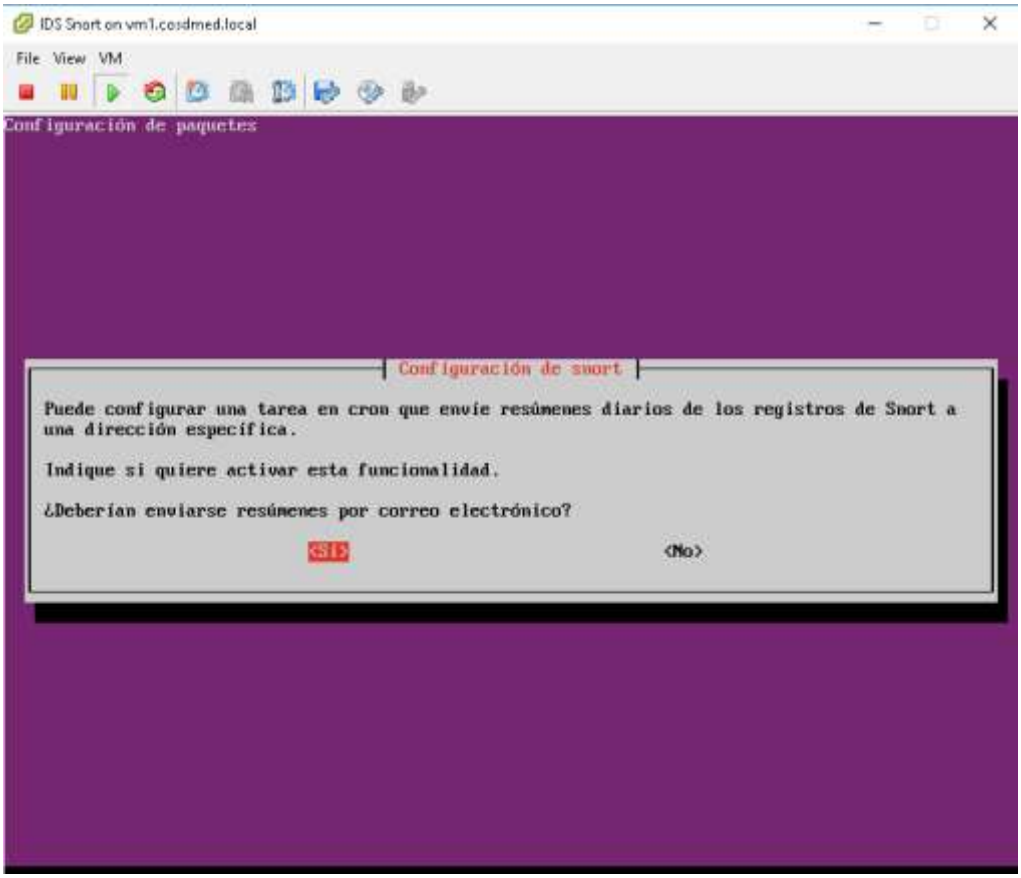


Fuente: Los Autores

5.6.11 Generación de reportes:

El monitoreo de intrusos proactivo ayuda a tomar decisiones en tiempo real y poder evitar intrusiones futuras que afecten la integridad de los datos por lo que se realiza la configuración de la cuenta del correo del jefe de sistemas para que las notificaciones lleguen en tiempo real.

Ilustración 20 Configuración de correo para generación de reportes

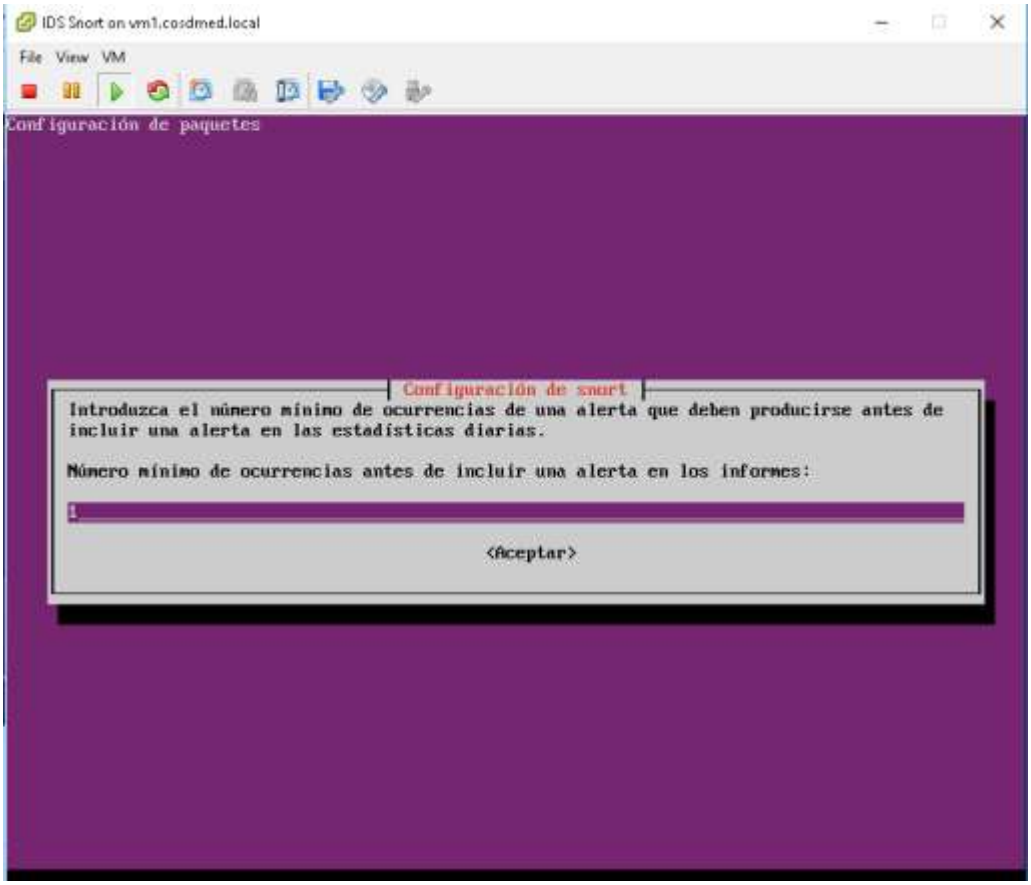


Fuente: El Autor

5.6.12 Selección del Umbral de alerta

Inicialmente se configura el umbral de alarma a 1 evento, si se generan un gran porcentaje de falsos positivos se debe reasignar el umbral por uno más alto

Ilustración 21 Selección de Umbral para generación de alertas



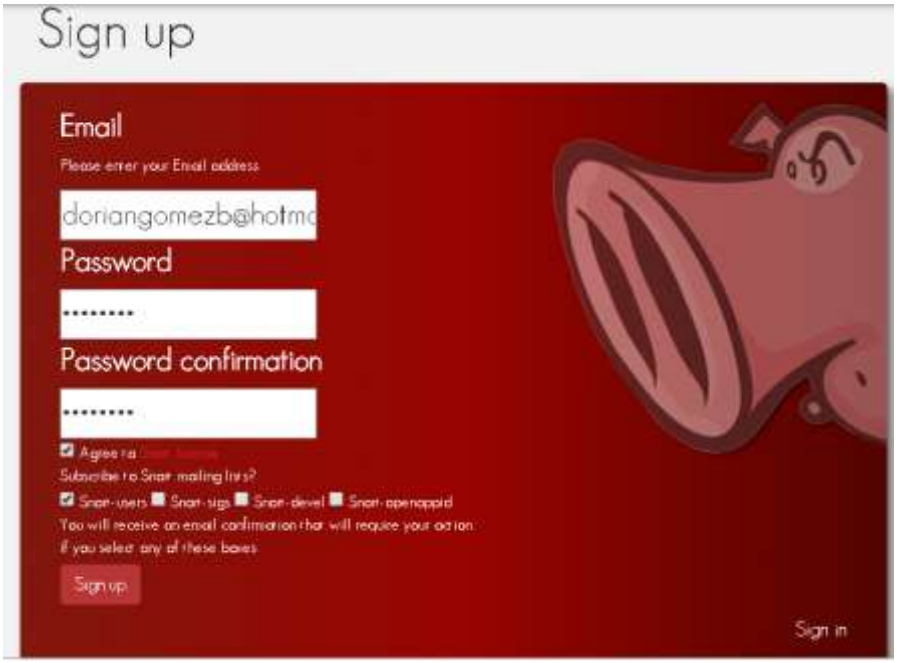
Fuente: Los Autores

5.6.13 Creación de reglas

Las reglas de detección y monitoreo garantizar que se puedan evitar e informar las intrusiones, Clinica de oftalmología Sandiego requiere tener unas reglas actualizadas y seguras, basado en lo anterior se descargaron las reglas actualizadas del sitio oficial https://www.snort.org/.

Para descargar las reglas se debe crear una cuenta de usuario y una contraseña

Ilustración 22 Registro en la página oficial de SNORT

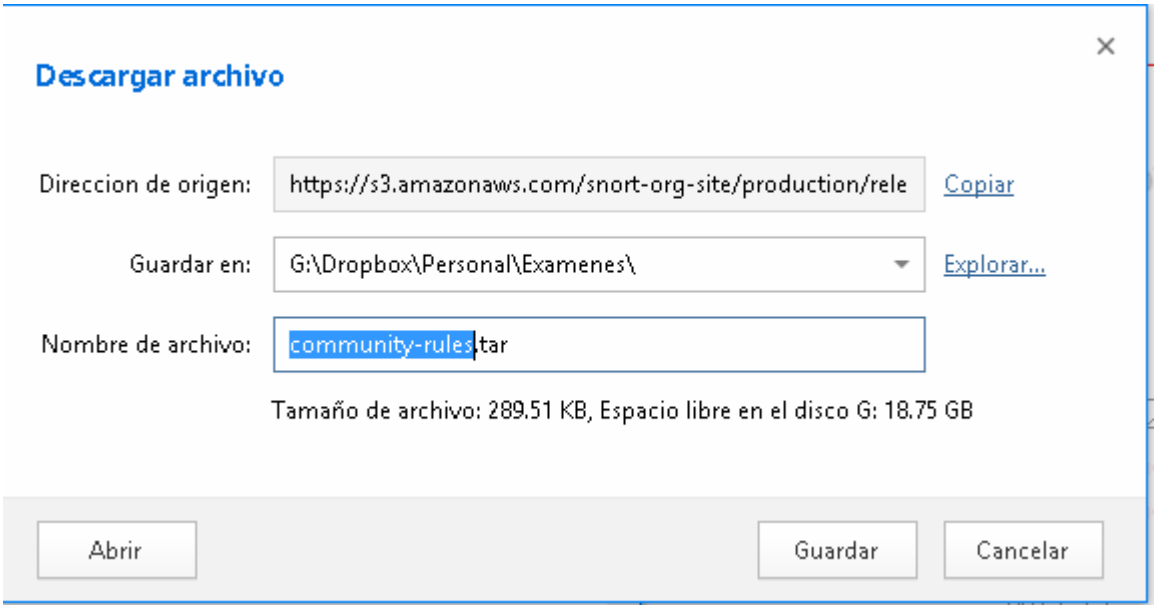


Fuente: Los Autores

Ilustración 23 Reglas version 2.9 desde SNORT

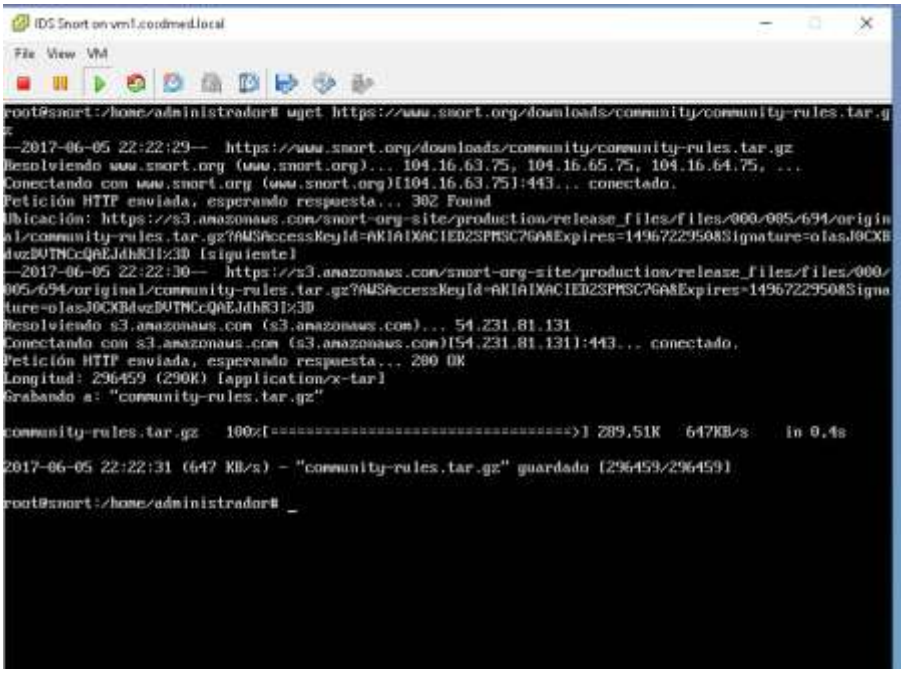
Fuente: Los Autores

Ilustración 24 Descarga de reglas SNORT



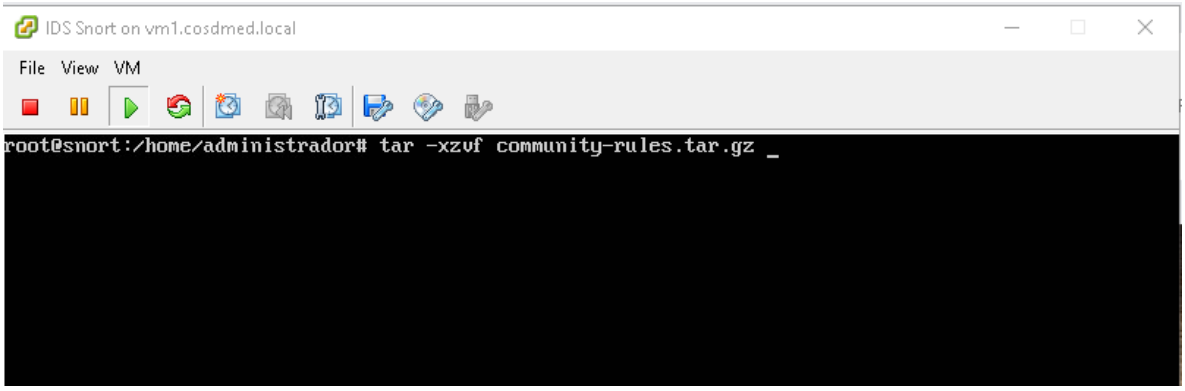
Fuente: Los Autores

Ilustración 25 Descargando las reglas en Ubuntu



Fuente: Los Autores

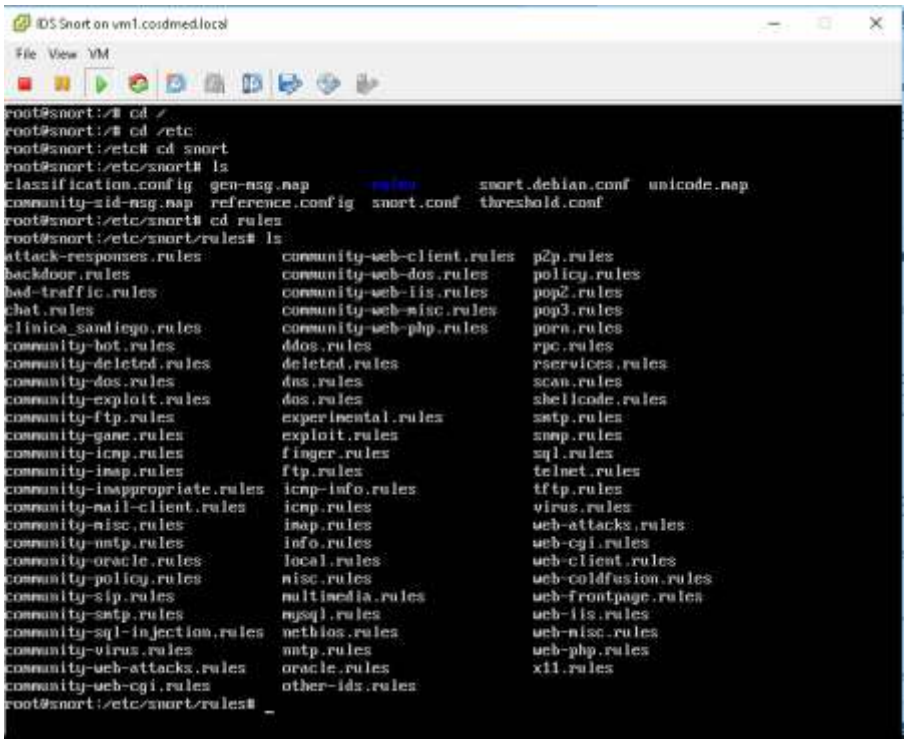
Ilustración 26 Descompresión de las reglas de SNORT



Fuente: Los Autores

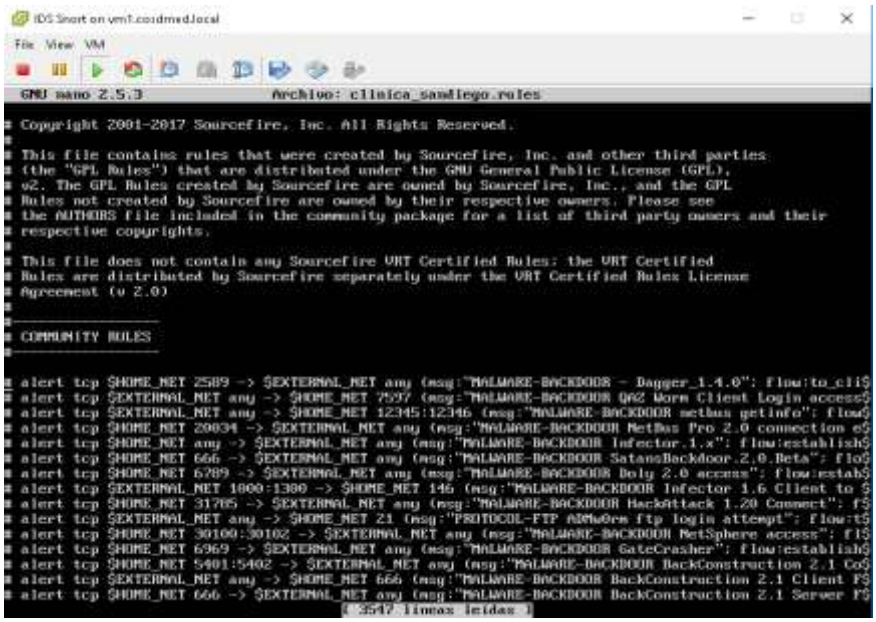
Se descomprimen las reglas en la ruta /etc/snort/rules/clinica_sandiego.rules

Ilustración 27 Enrutamiento de reglas Clinica_Sandiego



Fuente: Los Autores

Ilustración 28 Visualizando las reglas clinica_sandiego.rules



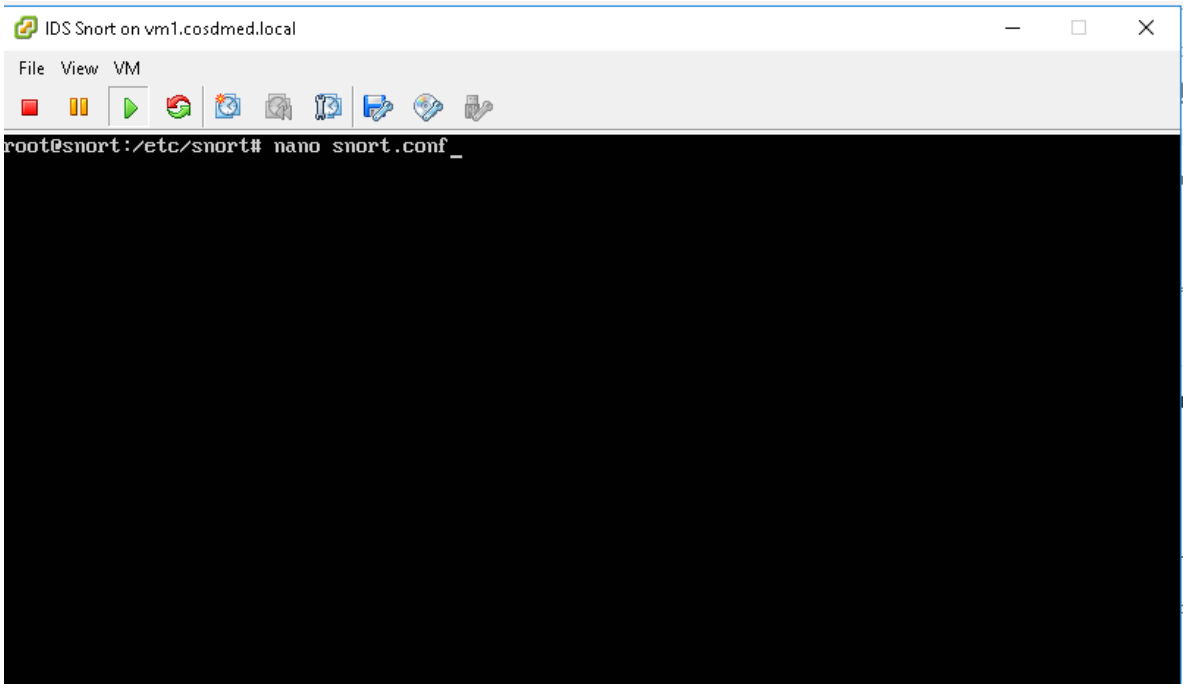
Fuente: Los Autores

5.6.14 Configuración del archivo snort.conf

El archivo snort.conf el cual se encuentra almacenado en /etc/snort/snort.conf es el encargado de administrar todas las configuraciones de este IDS entre estas:

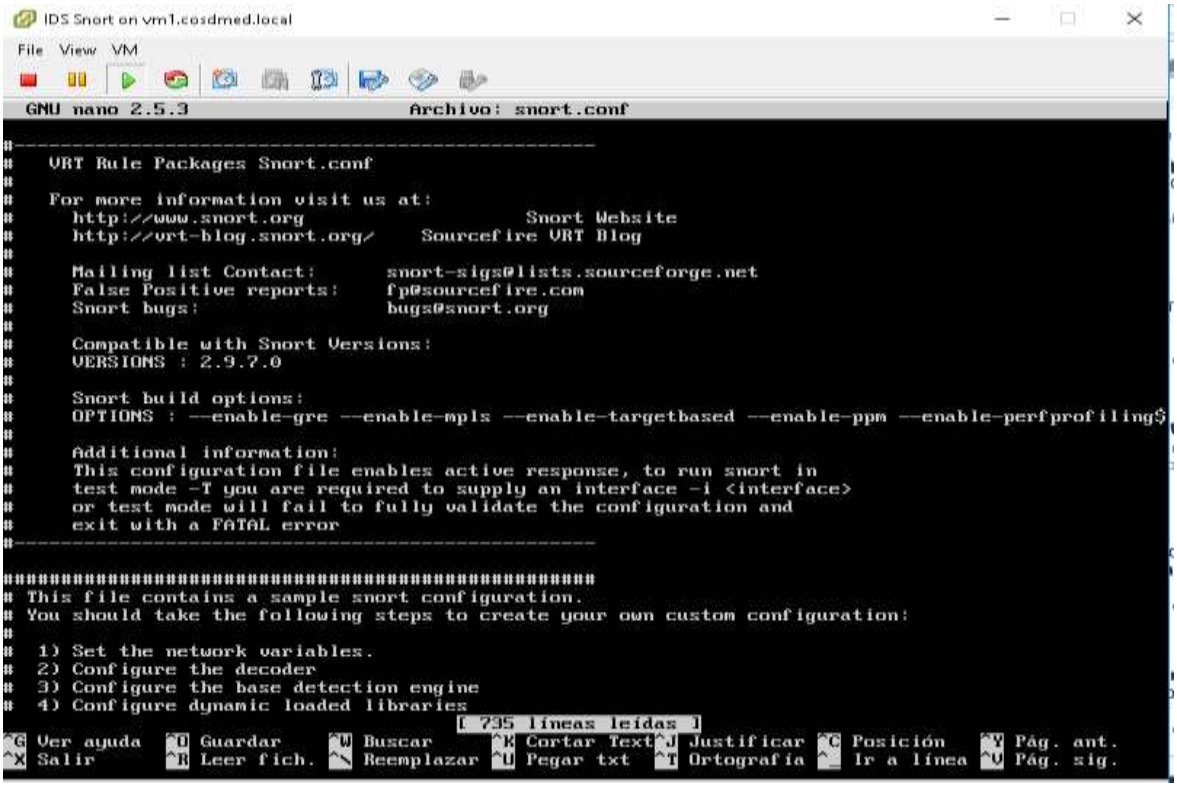
- Definición de las redes que se monitorearán
- Configuración de las librerías dinámicas.
- Configuraciones generales
- Configuraciones de las reglas de monitoreo

Ilustración 29 Edición del archivo snort.conf



Fuente: Los Autores

Ilustración 30 Archivo Snort.conf



Fuente: Los Autores

5.6.15 Inclusión de las reglas en snort.conf

Para que las reglas puedan estar activas en el monitoreo en tiempo real se requiere hacer referencias en el archivo snort.conf de la siguiente manera:

Include $RULE_PATH/clinica_sandiego.rules

En el archivo snort.conf se crea la variable :
Var $RULE_PATH= /etc/snort/rules

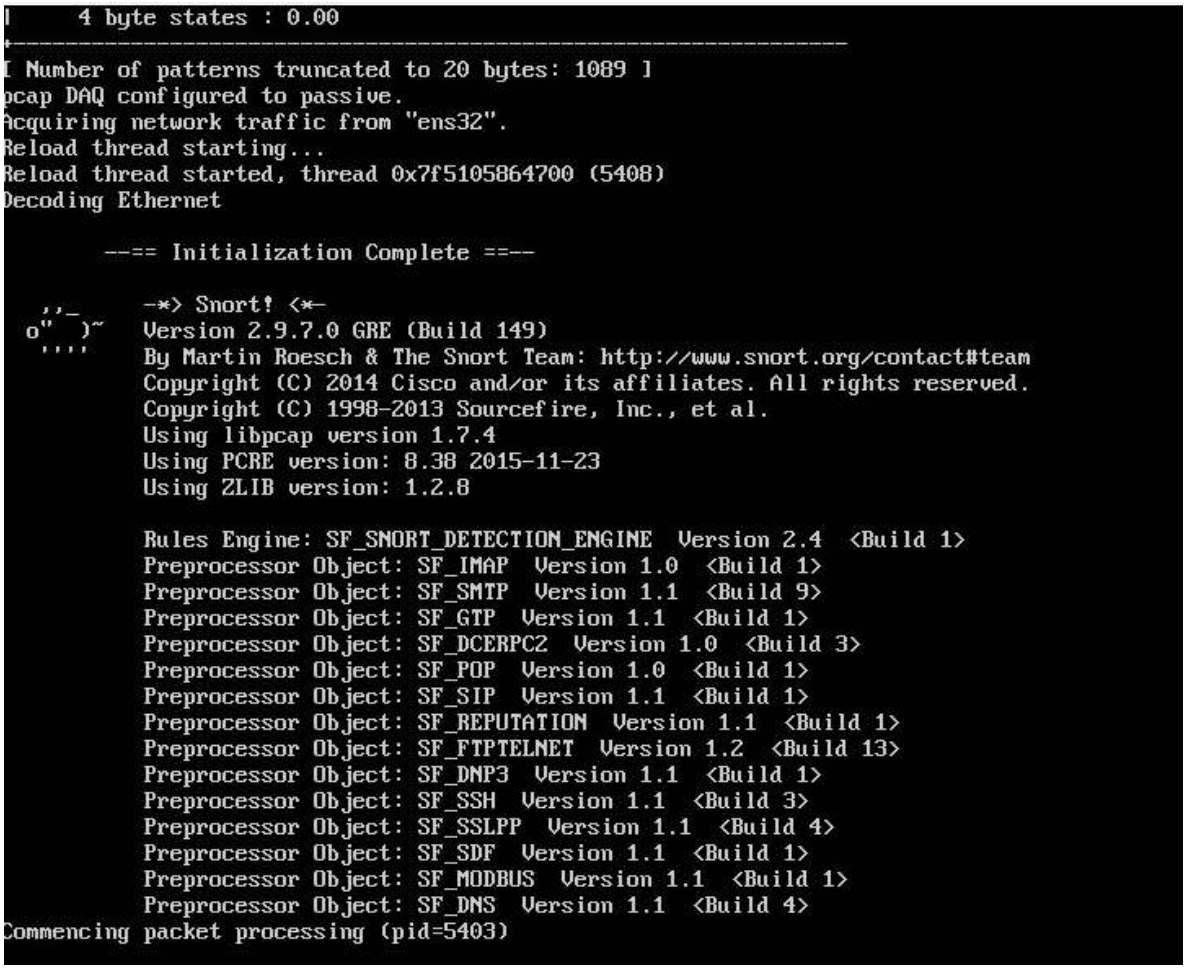
5.6.16 Validación de la configuración

Se valida la configuración con el comando snort con el siguiente comando:

snort -c /etc/snort/snort.conf

Al aparecer en ascii el logo de Snort (un cerdo) se confirma que el script de configuración y las reglas están de manera correcta.

Ilustración 31 Validación de configuración de Snort



Fuente: Los Autores

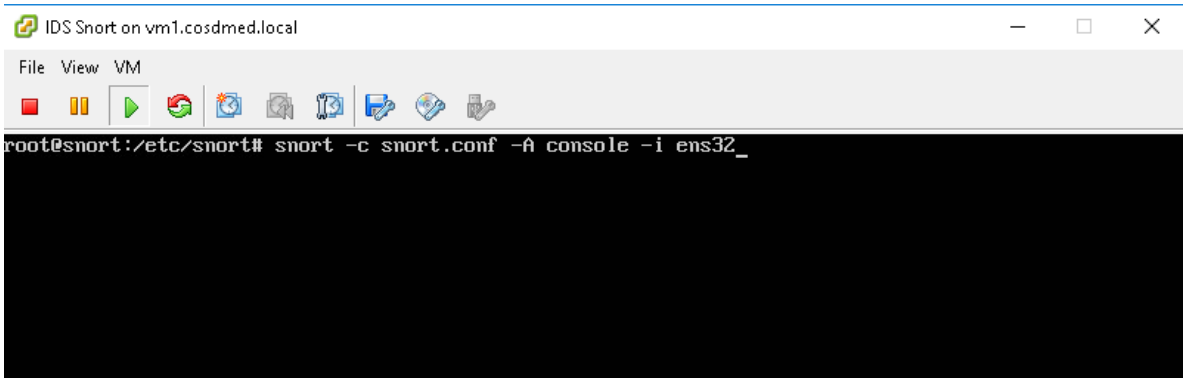
5.6.17 Ejecución del SNORT

Desde la consola se digita snort -c snort.conf –A console –i ens32

Parámetros:

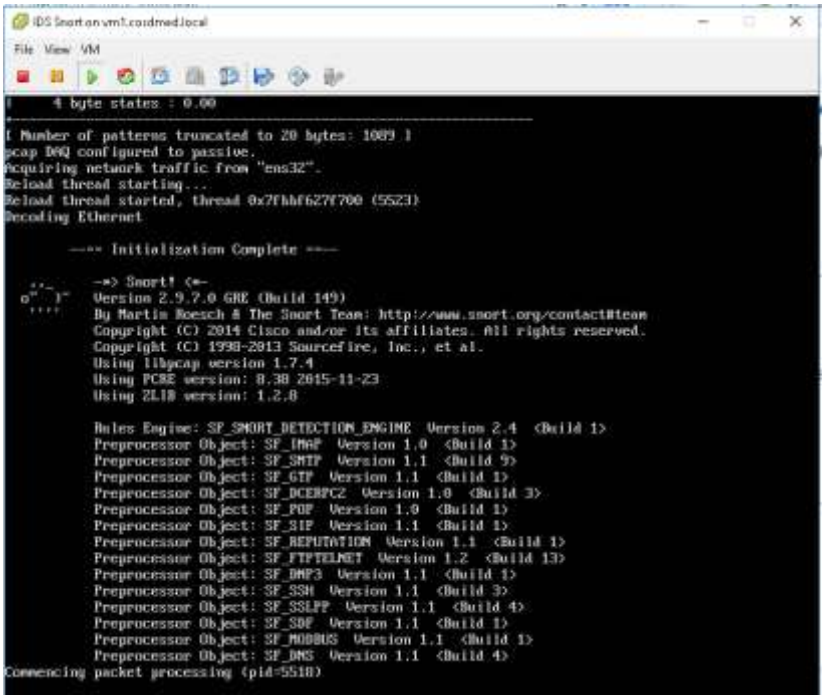
c: archivos de configuración
A: Modo de monitoreo para este caso por consola (Console)
i: Interfaz para este caso ens32

Ilustración 32 Ejecución de SNORT



Fuente: Los Autores

Ilustración 33 Monitoreo activo de Snort



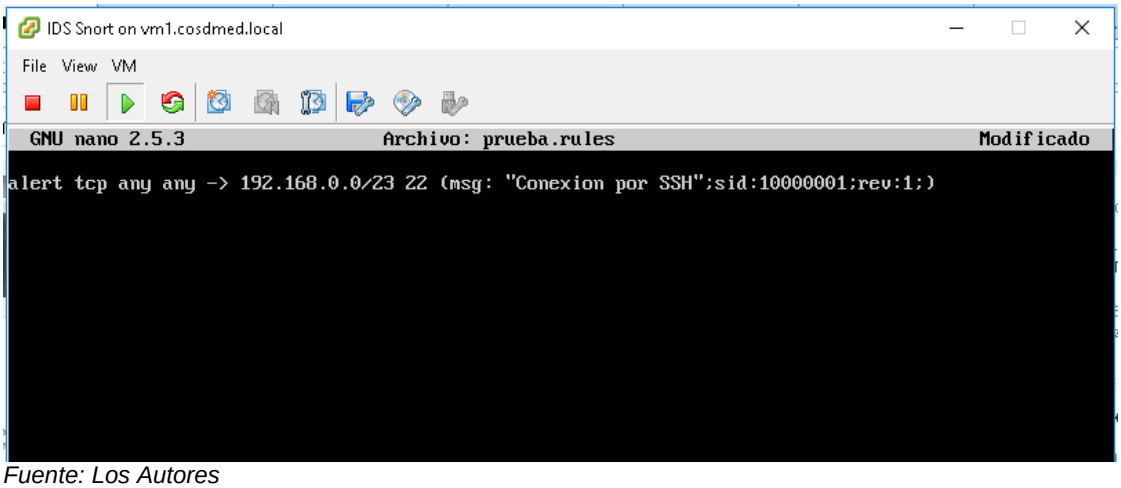
Fuente: Los Autores

Validación del funcionamiento

Para garantizar que el SNORT esté funcionando de manera correcta se crea una nueva regla que monitoreo si existe una conexión SSH de la siguiente manera:

alert tcp any any -> 192.168.0.0/23 (msg: “Conexión por SSH”;sid:10000001;rev:1;)

lustración 34 Creación de regla de prueba

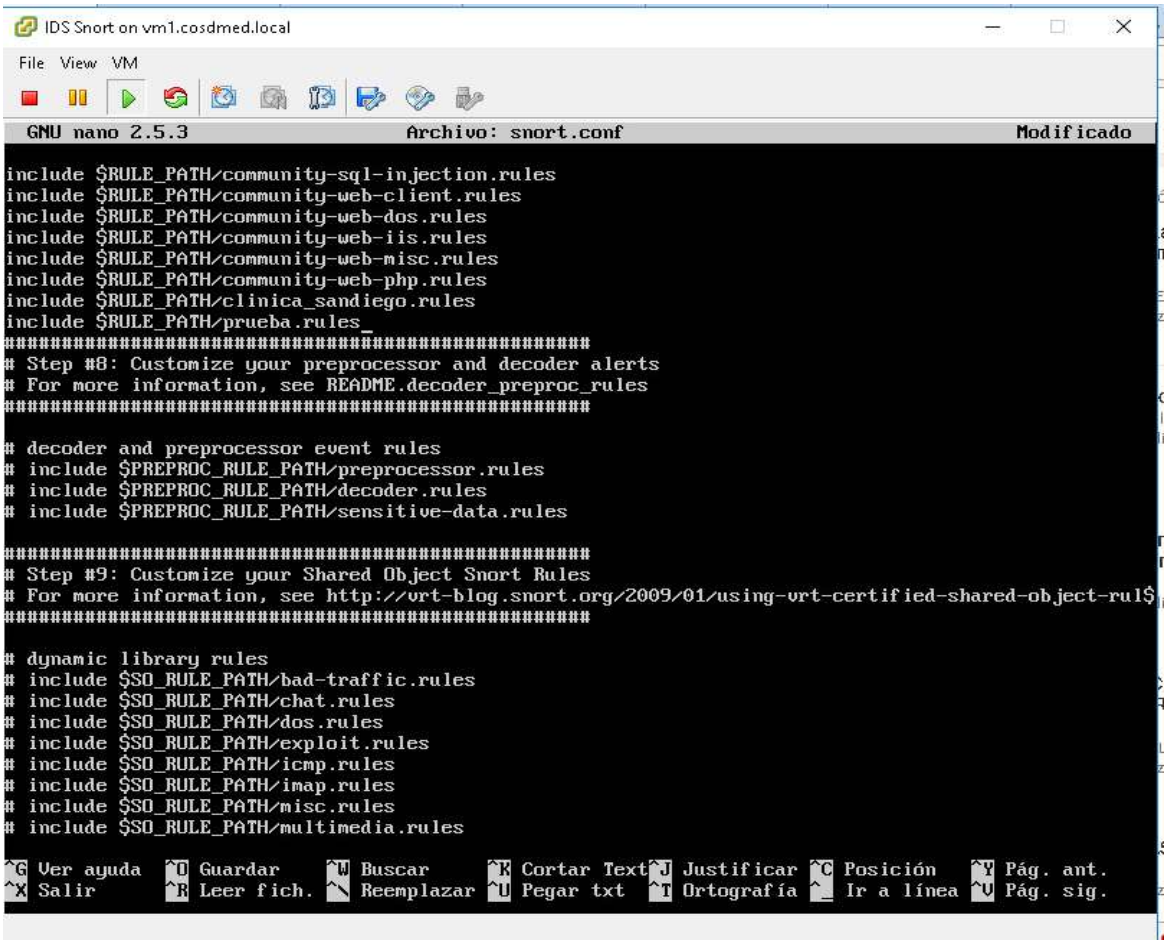


Fuente: Los Autores

Se almacena esta regla en la ruta predeterminada /etc/snort/rules con el nombre de prueba.rules. Así mismo se carga esta nueva regla (include) en el archivo de configuración /etc/snort/snort.conf:

Include $RULE_PATH/prueba.rules

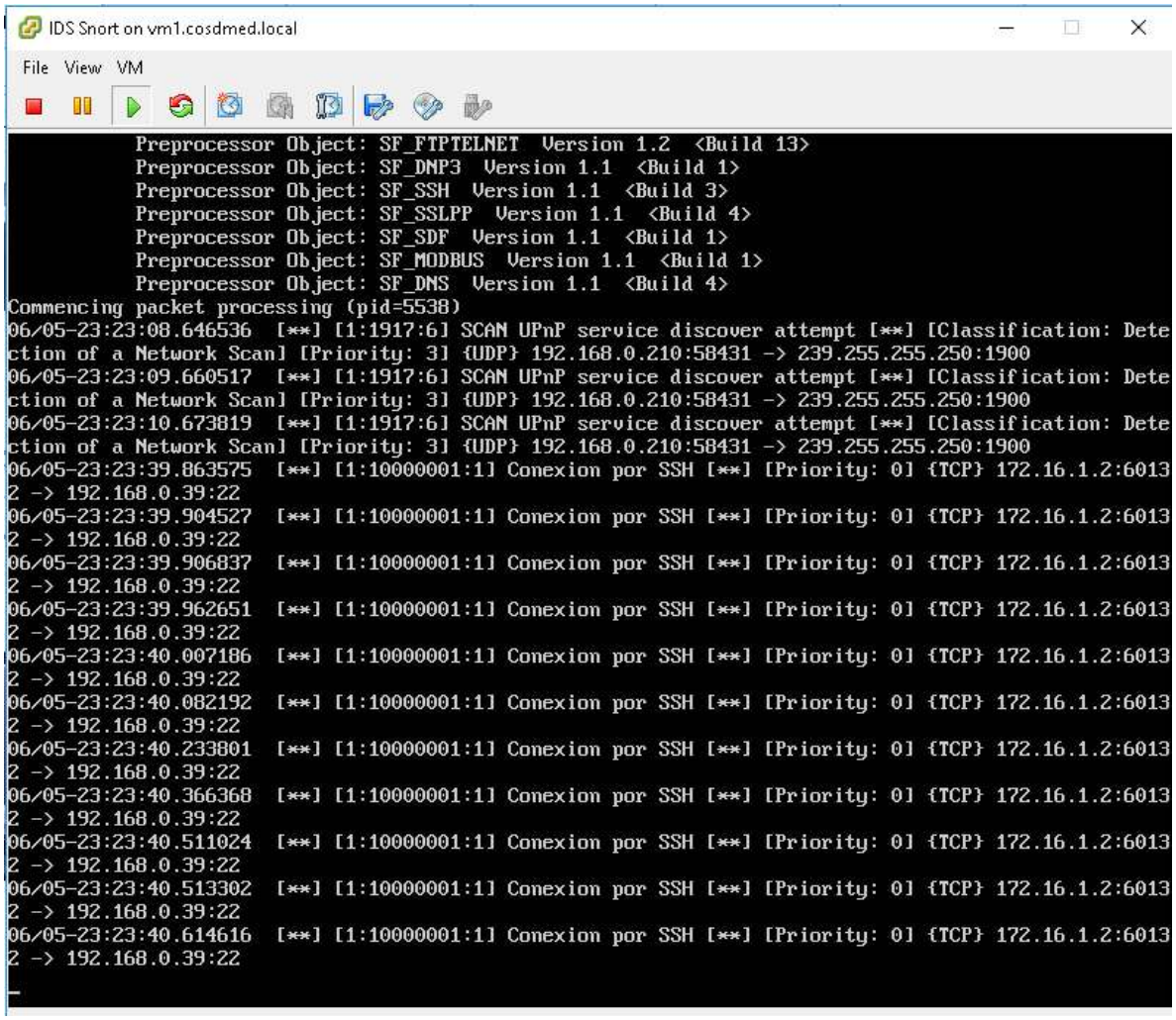
Ilustración 35 Adición de la regla de prueba en snort.conf



Fuente: Los Autores

Se inicia el servicio de snort y se realiza la prueba de conexión remota mediante SSH y el IDS genera la alerta de la intrusión configurada

Ilustración 36 Generación de Alerta



Fuente: Los Autores

PERSONAS QUE PARTICIPAN EN EL PROYECTO

PROPONENTES PRIMARIOS

DORIAN ALONSO GÓMEZ BARRIENTOS, Ingeniero de Sistemas, egresado de la Universidad del Tolima en el 2012. Actualmente trabaja como jefe de TIC de la Clínica de Oftalmología Sandiego.

OSCAR GIOVANNY HENAO CARDENAS, Ingeniero de Sistemas, egresado de la Universidad Abierta y a Distancia UNAD. Actualmente trabaja en la Alcaldía de Pereira, en el área de TIC.

PROPONENTES SECUNDARIOS

JUAN JOSE CRUZ GARZON, Ingeniero de sistemas, Especialista en Seguridad Informática. Candidato a Maestría en Seguridad Informática, Docente Ocasional Universidad Nacional Abierta y a Distancia UNAD.

HUMBERTO CONTRERAS DIAZ GRANADOS, Administrador de empresas, Gerente General de la Clínica de Oftalmología Sandiego de Medellín.

RECURSOS DISPONIBLES

RECURSO HUMANO

TABLA No Costos de personal

Nombres y Apellidos	Titulo		Función	Horas por Semana	Valor Hora	Dedicación [Semanas]	TOTAL
	Formación básica	Posgrado					
Dorian Alonso Gómez Barrientos	Ingeniero de Sistemas	-	Investigador Principal	5	$ 30.000	10	$ 1.500.000
Oscar Giovanny Henao Cárdenas	Ingeniero de Sistemas	-	Investigador Principal	5	$ 30.000	10	$ 1.500.000
SUBTOTAL							$ 3.000.000

Fuente: Los Autores

El esfuerzo de tiempo y costos del proyecto para un buen fin del mismo, como son gastos de alojamiento, viáticos, manutención entre otros, vienen incluidos en la tabla de costos de personal los cuales se ven reflejados en el valor de horas y estarán a cargo del investigador.

EQUIPOS

TABLA No Costos de utilización de equipos

Concepto	Cantidad	Total
Computador Portátil	1	$ 900.000
Impresora	1	$ 150.000
SUBTOTAL		$ 1.050.000

Fuente: Los Autores

Los costos de utilización de equipos para el desarrollo del proyecto corren por cuenta del investigador.

MATERIALES E INSUMOS

TABLA No Costos de materiales e insumos

Concepto	Total
Papelería y Fotocopias	$ 120.000
Digitación e impresión	$ 200.000
SUBTOTAL	$ 320.000

Fuente: Los Autores

Por ser para un trabajo de grado, los costos los colocará el investigador

RESULTADOS E IMPACTOS ESPERADOS

La implementación de un sistema de detección de intrusos es una herramienta fundamental para aquellas compañías que manejan información confidencial y que además tienen un flujo grande de datos a través de la red. La clínica Oftalmológica San Diego posee esas dos características y es por esto que con el presente proyecto se pretende formular una estrategia para dar más seguridad a toda la información condensada en los servidores de la clínica, puesto que la vulneración a las redes informáticas se ha vuelto una constante en las últimas décadas y quien posea las herramientas de vanguardia para enfrentar estos ataques, será quien salga avante en la guerra informativa que se libra cada día.

Sin duda mejorar la seguridad de la información es uno de los resultados más esperados y el impacto que esta nueva herramienta de detección de intrusos pueda tener en la compañía, solo será verificado una vez el sistema implementado empiece su funcionamiento.

CRONOGRAMA DE ACTIVIDADES

Año / Actividades		2017	2017							
		MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV
1	Elaboración y presentación de propuesta									
2	Aprobación de propuesta									
3	Presentación del anteproyecto									
4	Desarrollo del proyecto									
5	Aplicación de instrumentos									
6	Sistematización información									
7	Análisis e interpretación de la información									
8	Presentación del trabajo final									

CONCLUSIONES

Una vez implementado el sistema y analizados los resultados de su funcionamiento, se pueden formular las siguientes conclusiones:

La implementación de un sistema de control de intrusos con software libre minimiza el riesgo de intrusión y la captación de datos sensibles como lo son los datos consignados en la Historia Clínica de la Institución.

Un sistema de prevención de intrusos si es correctamente configurado permite analizar el comportamiento de los accesos no autorizados y tomar las contramedidas necesarias.

El software libre para detección de intrusos permite dar mayor flexibilidad al sistema perimetral sin incurrir en altos costos.

BIBLIOGRAFÍA

WEB-GRAFIA

ALTUS “E- prints complutense”. {En línea}. {24 de julio de 2017} disponible en: (http://www.altus.cr/blog/rretana/ips-funcionamiento-y-aplicacion-actual.html).

BARRANTES, Milagritos “Metodología para implementar proyectos de redes”. {En línea}. {25 de Marzo de 2017} disponible en: (http://metodologiaspararedes.blogspot.com/).

WIKIPEDIA “Seguridad perimetral”. {En línea}. {26 de Marzo de 2017} disponible en: (http://es.wikipedia.org/wiki/seguridad_perimetral).

WIKIPEDIA “Sistema de Prevención de Intrusos”. {En línea}. {15 de Marzo de 2017} disponible en: (http://es.wikipedia.org/wiki/sistema_de_prevenci%c3%b3n_de_intrusos).

UNAD “Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda”. {En línea}. {18 de Abril de 2017} disponible en: (http://repository.unad.edu.co/bitstream/10596/3777/1/20904541.pdf).

“Formando Investigadores”. {En línea}. {21 de Abril de 2017} disponible en: (http://formandoinvestigadores-gft.blogspot.com.co/2011/01/estado-del-arte.html).

CMM “Introducción a la seguridad informática”. {En línea}. {22 de Febrero de 2017} disponible en:(http://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica).

DIAZ, José “Sistema de prevención de intrusos para mejorar la seguridad de los servidores de la Universidad Nacional de Trujillo”. {En línea}. {10 de Abril de 2017} disponible en: (http://docplayer.es/3781958-Sistema-de-prevencion-de-intrusos-para-mejorar-la-seguridad-de-los-servidores-de-la-universidad-nacional-de-trujillo.html).

ECURED “Seguridad Informática”. {En línea}. {10 de Abril de 2017} disponible en:(https://www.ecured.cu/Seguridad_Inform%C3%A1tica).

FORMULA EN LOS NEGOCIOS “Seguridad Informática: Qué, Por qué y Para qué?”. {En línea}. {18 de Marzo de 2017} disponible en:(http://www.formulaenlosnegocios.com.mx/seguridad-informatica-%C2%BFque-por-que-y-para-que/).

HINOJOSA, Fernando. “Implementación de un sistema de detección de intrusos en el CELE. {En línea}. {18 de Marzo de 2017} disponible en:(https://www.academia.edu/24490616/Implementaci%C3%B3n_de_un_sistema_de_detecci%C3%B3n_de_intrusos_en_el_CELE).

SIERRA, Óscar “Implementación de políticas de seguridad informática para las universidades de Risaralda”. {En línea}. {5 de Marzo de 2017} disponible en:(http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2370/0058S572.pdf?sequence=1)

ANEXOS

RESUMEN ANALITICO ESPECIALIZADO
RAE

Tipo de Documento	Trabajo de Grado
Título	Implementación de un sistema de detección de intrusos en la clínica oftalmológica SanDiego
Autores	Gómez, Dorian;Henao, Giovanny
Palabras Claves	Detección de intrusos, seguridad informática, Clinica de oftalmología Sandiego, Historia Clínica Digital, Confidencialidad, Accesibilidad, Oportunidad, Integridad
Descripción	Trabajo de grado de Especialización, que analiza y diseña un sistema de detección de intrusos con software libre
Fuentes	11 Fuentes
Contenido	RAE, Introducción, Lista de tablas, lista de ilustraciones, Título, Formulación del Problema, Objetivos, Marco Referencial, Materiales y Métodos, Personas que participan en el proyecto, Recursos Necesarios para el desarrollo, Cronograma.
Metodología	El enfoque seguido para desarrollar esta tesis, es un enfoque Cuantitativo, pues el problema de investigación es concreto y limitado, usa la recolección de datos para probar la hipótesis. Se utiliza un tipo de investigación aplicada, porque permite trabajar con metodologías y técnicas que están fundamentadas con bases teórico – científica, que nos van a servir como el punto de partida en la solución de problemas de la institución
Conclusiones	La implementación de un sistema de control de intrusos con software libre minimiza el riesgo de intrusión y la captación de datos sensibles como lo son los datos consignados en la Historia Clínica de la Institución.

	Un sistema de prevención de intrusos si es correctamente configurado permite analizar el comportamiento de los accesos no autorizados y tomar las contramedidas necesarias. El software libre para detección de intrusos permite dar mayor flexibilidad al sistema perimetral sin incurrir en altos costos.