ESTUDIO Y DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS – IDS SNORT PARA LA UNIVERSIDAD DEL SINU – SECCIONAL CARTAGENA - SEDE SANTILLANA

JESÚS ANTONIO CABARCAS GÓMEZ
RAFAEL IGNACIO ACEVEDO PARDO
JAIME RAFAEL BARRIOS CANTILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERIA EN SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2017

ESTUDIO Y DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS – IDS SNORT PARA LA UNIVERSIDAD DEL SINU – SECCIONAL CARTAGENA - SEDE SANTILLANA

JESÚS ANTONIO CABARCAS GÓMEZ
RAFAEL IGNACIO ACEVEDO PARDO
JAIME RAFAEL BARRIOS CANTILLO

Trabajo de grado para optar el título de especialista en seguridad informática

Docente
Mariano Romero
Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERIA EN SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2017

EXCLUSIÓN DE RESPONSABILIDAD

Las ideas expresadas en este documento son de exclusiva responsabilidad de sus autores y no comprometen la ideología de la Universidad Nacional Abierta y a Distancia UNAD.

Nota de aceptación

_____
_____
_____
_____
_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

_____

Bogotá, 28 de febrero de 2018

CONTENIDO

pág

LISTA DE TABLAS

pág.

LISTA DE CUADROS

pág.

LISTADO DE ILUSTRACIONES

pág.

INTRODUCCIÓN

En la actualidad la información se ha convertido en el activo más importante y una pieza fundamental en las actividades de una empresa u organización, tanto las Empresas, el Estado y las personas que dependen de esta se benefician de la misma.

Las Tecnologías de información y la comunicación (TIC), es una herramienta de apoyo que permite a las personas, empresas y el estado realizar actividades del día a día de una manera más rápida y optima, pero esta trae implícita una serie de oportunidades, cambios y amenazas que impactaran dentro de la organización.

Por otra parte, la protección y custodia de los datos personales contenidos en las bases de datos encargadas del tratamiento (persona natural o jurídica, pública o privada), se deben sujetar a lo establecido en la Ley estatutaria 1581 de 2012.

Por todo lo anteriormente, las consecuencias de la perdida de información dentro de una entidad que proteja datos personales y maneje información sensible trae consigo demandas por parte de las personas, indisponibilidad de los servicios prestados, pérdida de credibilidad, pérdida de imagen institucional etc. por ende con el proyecto de estudio y diseño de un sistema de detección de intrusos se pretende reducir el riesgo de ocurrencia de un siniestro y disminuir el impacto si el siniestro se presentara. A continuación se realiza una pequeña descripción de que es un IDS:

Diego Gonzales Gómez[1] Define los IDS como el fruto de la aplicación del Procesamiento Electrónico Datos (EDP) a las auditorias de seguridad, donde se utilizan mecanismos como la identificación de patrones y métodos estadísticos. Esta es una parte que no puede faltar en las modernas tecnologías de seguridad de redes.

Según María Giménez[2] un IDS es un elemento que escucha y analiza toda la información que transita por la red de datos e identifica los posibles ataques que se puedan presentar. Cuando aparece un ataque, donde se vea comprometida la seguridad, este reacciona informando al administrador y cerrando las puertas o vectores de ataques al posible intruso reconfigurando elementos de red como firewall y routers.

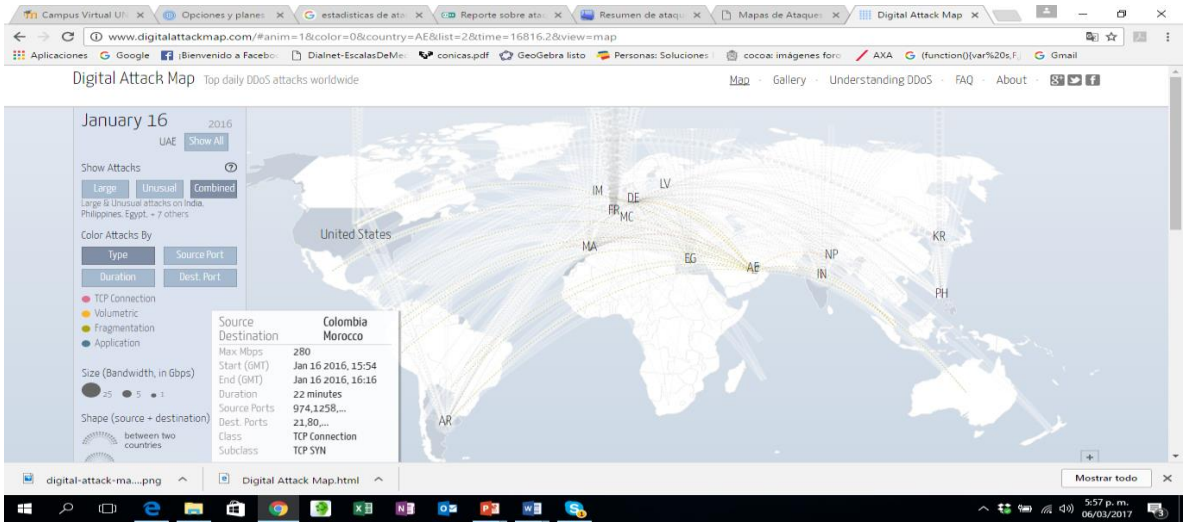
[1] GONZÁLEZ GÓMEZ, Diego [en línea]. Sistema de Detección de Instrucciones. 2010. [Citado 5, mayo, 2017]. Disponible en: <http://derecho-internet.org/docs/ids.pdf>. p.86.
[2] GIMÉNEZ GARCÍA, María Isabel [en línea]. Utilización de Sistemas de Detección de Intrusos como Elemento de Seguridad Perimetral. Almería, 262 h: Universidad de Almería, 2008. [Citado 10, abril, 2017]. Disponible en: <http://www.adminso.es/recursos/Proyectos/PFC/PFC_marisa.pdf>. p.3.

1. EL PROBLEMA DE INVESTIGACIÓN

1.1. DESCRIPCIÓN

La Universidad del SINU – Sede Santillana localizada en Cartagena, depende altamente de sus recursos computacionales para el desarrollo de su función, por lo tanto establece las siguientes medidas de seguridad, como, diseño y aplicación de políticas de seguridad perimetral, lineamientos basados en las buenas prácticas de ISO 27001, aplicación de políticas en el firewall para minimizar los riesgos de ataques que según las estadísticas que se muestran en la siguiente grafica de www.digitalattackmap.com se detecta que los principales ataques que sufre nuestro país vienen de otros continentes, así mismo una serie de capacitaciones sobre seguridad de informática al cliente interno, como a terceros relacionados.

Ilustración 1. Origen de ataques hacia Colombia.



Fuente: www.digitalattackmap.com.

Existen varios riesgos que puede sufrir la Universidad tales como ataques de denegación de servicios a los servidores principales donde está la información crítica de sus procesos misionales.

Abuso de privilegios por parte de los administradores de los servidores que tienen acceso a la información.

Divulgación estadística no autorizada de la información almacenada en los servidores como historial de notas y resultados de los estudiantes.

1.2. FORMULACIÓN DEL PROBLEMA.

¿Cómo el estudio y diseño de un Sistema de detección de intrusos – IDS SNORT ayudará a disminuir los tiempos de respuesta frente a los ataques de seguridad que puedan presentarse en la UNISINU Cartagena?

1.3. SUBPREGUNTAS

¿Qué metodología se aplica para la identificación y valoración de activos que se incluyen en el estudio?

¿Qué método o forma de trabajar tiene SNORT para que le sea más útil a la UNIVERSIDAD DEL SINU aplicando todas sus ventajas?

¿Qué clase de infraestructura tecnológica debe ser la más apropiada para que el sistema SNORT pueda desempeñarse con un óptimo grado de rendimiento?

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Diseñar el Sistema de Detección de Intrusos – IDS SNORT para mejorar el nivel de madurez en seguridad de los activos informáticos de la UNISINU que permita mitigar los riesgos a los que está expuesta su información.

2.2. OBJETIVOS ESPECÍFICOS

- Identificar y clasificar los activos críticos informáticos que se van a proteger dentro de la sede Santillana de la UNISINU.
- Evaluar el nivel de seguridad de los activos informáticos críticos de la organización.
- Describir las formas en que trabaja SNORT (Modo Sniffer, Packet Logger, modo NIDS o modo Inline) como sistema de detección de intrusos en una organización.
- Diseñar la infraestructura necesaria para el buen funcionamiento del Sistema de Detección de Intrusos – IDS SNORT en la UNISINU.

2.3. JUSTIFICACIÓN

Para la Universidad del SINÚ es muy importante el diseño de este proyecto porque permite en gran medida mitigar y contrarrestar los ataques informáticos que se presentan tanto al interior como al exterior de la entidad.

Las personas que se beneficiarán con la implementación de este proyecto serán los estudiantes y personal administrativo de la universidad.

Uno de los principales beneficios de este proyecto es que los estudiantes y personal administrativo de la universidad estarán protegidos contra cualquier intento de ataque ya sea de DDOS, SQL inyección, XSS, suplantación de identidad, entre otros tanto dentro como fuera de la organización.

Uno de los principales motivadores que influyeron a la hora de llevar a cabo el diseño de este proyecto, es establecer que la Universidad pueda contar con una herramienta que les permita tomar decisiones en tiempo real ante posible vulneración de su información, de igual forma el proyecto permitirá disminuir las probabilidades de ataques a los recursos informáticos. Otro factor importante a la hora de diseñar y adoptar un Sistema de detección de intrusos es que el costo en su implementación es menor al costo que se genera cuando ocurre un siniestro causado por un ingreso no autorizado a los recursos de la red.

Este diseño del Sistema de detección de intrusos – IDS SNORT hace que la UNIVERSIDAD DEL SINU:

Cuente con un sistema IDS capaz de registrar en tiempo real cada uno de los ataques que se presenten tanto al interior como al exterior de la entidad.

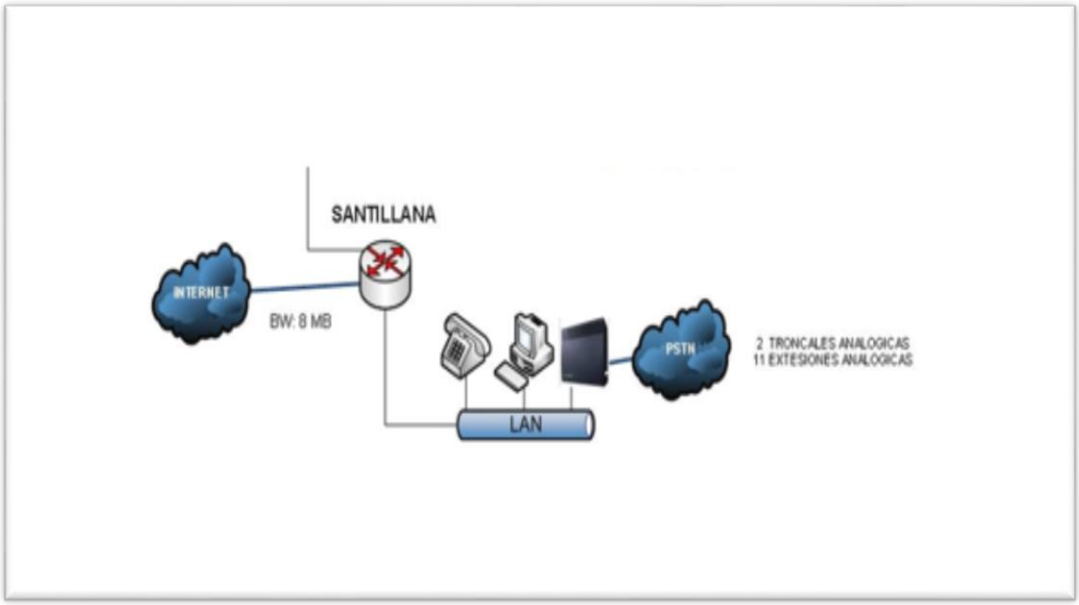
Controle y garantice la seguridad de la información dentro de la entidad.

Analice la información generada por el IDS SNORT para saber que tendencias o eventos persistentes se presentan en la red para posteriormente realizar ajustes en materia de seguridad en la infraestructura y tomar decisiones operacionales y administrativas.

2.4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

En este proyecto se va a realizar un diseño de un IDS llamado SNORT en la red de la sede Santillana de la universidad del SINU en Cartagena para ser aplicado únicamente por el área de Tecnología. A continuación, se adjunta la topología de la sede.

Ilustración 2. Topología sede UNISINU.



Fuente: Universidad del SINU.

3. MARCO DE REFERENCIA

Para llevar a cabo este trabajo se tiene en cuenta un referente conceptual que es muy importante para lograr el éxito del mismo. Un elemento importante, es el IDS: que permite vigilar cada uno de los paquetes que se están enviando y recibiendo a través de toda la red.

3.1. ANTECEDENTES DEL PROBLEMA

Se pude considerar la información como el activo más importante dentro de la universidad, por ende este genera unos efectos tanto en los procesos administrativos como educativos, permitiéndole a la institución tener una ventaja competitiva con respecto a otras universidades del sector.

A ciencia cierta no se sabe si tanto dentro como fuera de la universidad se están llevando a cabo actos de ciberataques con el fin de violentar las medidas de seguridad de la información implementadas por la institución para salvaguardar la información que reposa dentro de sus servidores.

Así las cosas, la universidad actualmente no cuenta con un sistema que permita en tiempo real establecer si se está llevando a cabo un intento de ataque a los sistemas de información que yacen dentro de esta, permitiéndole tomar acciones correctivas y mitigar el impacto del mismo.

A continuación se describen los antecedentes más relevantes de la investigación:

Emilio Mira[3] desarrollo un proyecto titulado con el nombre “Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia” en Octubre de 2001 cuya idea principal de este proyecto era instalar un IDS en una de las troncales de la universidad de valencia con el fin de mitigar los riesgos de seguridad que se venían dando al interior de esta. Como resultado de esta implementación se pudo establecer en tiempo real cuando se está realizando un ataque a la red, permitiéndole saber de dónde proviene el ataque.

Otro proyecto que se tomó como referencia fue el elaborado por Anthony González[4] en abril de 2011“Implementación de un Sistema de Detención de Intruso (IDS) en, en la Red WIFI del Laboratorio G de la Universidad Simón Bolívar sede litoral”. Fue una experiencia bastante interesante y exitosa ya que la Universidad presentaba unas deficiencias grandes en la red Inalambrica y con el resultado de este proyecto se resolvieron en gran medida concluyendo en el mejoramiento de la calidad del servicio y el monitoreo de equipos conectados a la red.

Gilber Garzon[5] en el año 2015 llevo a cabo el proyecto “Propuesta para la implementación de un sistema de detección de intrusos (IDS) en la dirección general

[3] MIRA ALFARO, Emilio José [en línea]. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Valencia, 142 p: Proyecto Final (Ingeniería Informática) Universidad de Valencia. [Citado 10, abril, 2017]. Disponible en: http://rediris.es/cert/doc/pdf/ids-uv.pdf.

[4] GONZÁLEZ DA SILVA, Anthony Rafael [en línea]. Implementar un Sistema de Detención de Intruso (IDS) en la Red Wifi del Laboratorio G de la Universidad Simón Bolívar sede litoral. Informe final de pasantías. Universidad Simón Bolívar, Coordinación de tecnología eléctrica y electrónica. 20010. 161 p. [Citado 15, mayo, 2017]. Disponible en: <https://e-archivo.uc3m.es/bitstream/handle/10016/5929/PFC_Beatriz_Martinez_Santos.pdf?sequencDe=1>.

[5] GARZON PADILLA, Gilberto [en línea]. Propuesta para la implementación de un sistema de detección de intrusos (IDS) en la dirección general sede central del instituto nacional penitenciario y carcelario INPEC“PIDSINPEC, 75 p: Proyecto de Grado (Especialista en seguridad informática) Universidad Nacional Abierta y a Distancia. [Citado 20, noviembre, 2017]. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3494/3/86057594.pdf.

sede central del instituto nacional penitenciario y carcelario INPEC“PIDSINPEC”, ya que esta carecía de un sistema capaz de contrarrestar los ataques informáticos tanto dentro como al interior de la institución. Como resultados de la investigación se obtuvieron un análisis del estado actual de la seguridad en el INPEC, así como también unas recomendaciones de donde se puede ubicar el sistema de detección de intrusos al interior de la entidad.

Luis García[6] desarrollo el proyecto titulado con el nombre “sistema inteligente de detección de intrusiones”, en la universidad complutense de Madrid en el año 2011. El propósito que tuvo esta investigación fue diseñar un sistema de detección de intrusos capaz de detectar un ataque mediante el análisis del payload del tráfico de red. Una de las ventajas que ofrece este sistema es que es capaz de detectar un código malicioso al momento que este viaja sobre la red de datos, mientras que los otros sistemas solo lo hacen al momento de recibir el binario.

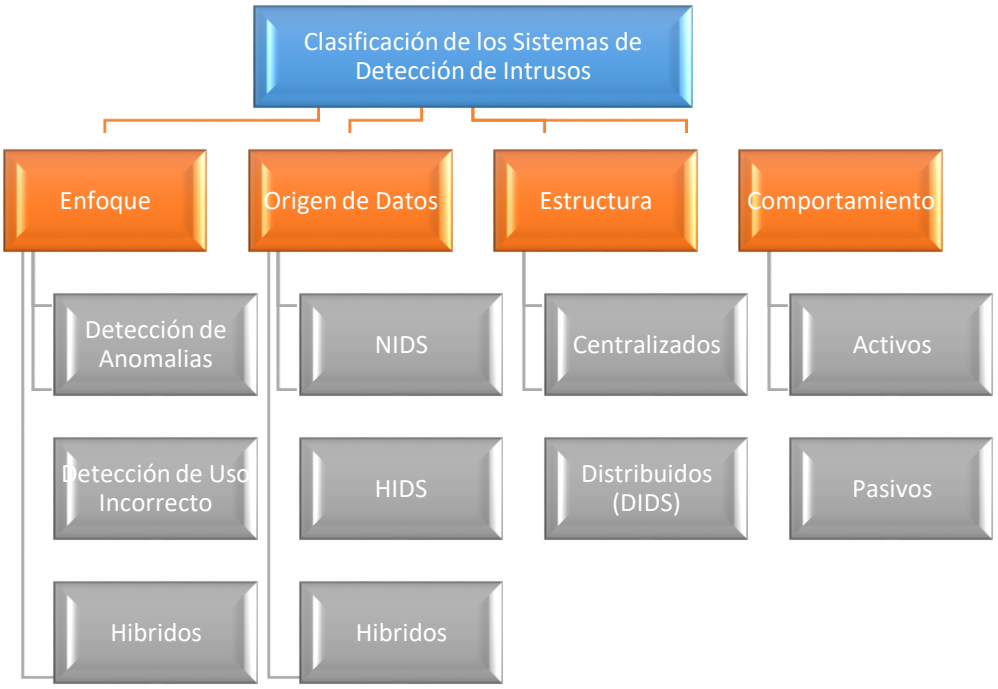
3.2. MARCO TEÓRICO CONCEPTUAL

3.2.1. Arquitectura genérica de un IDS. Según María Giménez[7] dice que actualmente existes varios tipos de IDS, y estos se clasifican dependiendo de sus características. Cada cual se diferencia el uno del otro dependiendo del monitoreo y análisis que realizan, cada cual posee sus ventajas y desventajas.

[6] MARTÍNEZ PUENTES, Javier [en línea]. Sistemas inteligentes de detección de intrusos, 119 p: Proyecto de Grado (Master en investigación informática) universidad complutense de Madrid. [Citado 20, noviembre, 2017]. Disponible en: http://eprints.ucm.es/13504/1/MA_2011-15.pdf

[7] GIMÉNEZ. Op. cit., p. 7.

Ilustración 3. Arquitectura de un IDS.



Fuente: El autor.

A continuación, se describirán cada uno de los diferentes tipos de sistemas de detección de intrusos.

3.2.2. Tipos de IDS en función del enfoque. Dentro de este existe dos grupos de IDS: los que se basan en normas, los cuales detectan el uso indebido del sistema y los adaptables que detectan las anomalías dentro del sistema.

3.2.2.1. Detección de anomalías. Consiste en el comportamiento que los usuarios tienen dentro de la red, permitiéndole establecer patrones de tal forma que si existe una desviación en el comportamiento se considera como una intrusión al sistema en cuestión.

Una de las principales características es que no se tienen que estar actualizando las firmas con periodicidad.

3.2.2.2. Detección del uso indebido. Se encarga de monitorear todas las actividades que se llevan a cabo dentro del sistema y los compara con una base de datos firmas guardas con anterioridad. Cuando se encuentra una coincidencia con alguna de las firmas almacenadas se dispara una alerta

Una de las principales características de este tipo de análisis es la precisión con la que se detectan los ataques

3.2.3. Tipos de IDS en función del origen de los datos. Con respecto a lo anterior, existen tres tipos de IDS: los basados en host, basados en red y los híbridos, a continuación, se realizará una breve explicación de cada uno de ellos.

3.2.3.1. HIDS: Host-based Intrusion Detection Systems. Este IDS tiene la tarea de identificar cada una de las amenazas e intrusiones a nivel de host local, es decir, estos solo se encargan de salvaguardar el host donde se encuentran instalados u hospedados.

Según María Giménez[8] este tipo de IDS se encargan monitorizar un gran volumen de eventos y actividades dentro del sistema con una gran fidelidad, pudiendo establecer que usuarios y procesos se encuentran envueltos en determinada acción dentro del sistema.

3.2.3.2. NIDS: Network Intrusion Detection Systems. Según María Giménez[9] dice que este tipo de IDS se encarga de monitorear y responder ante eventos generados, pero la diferencia con el HIDS es que protegen la red local donde se encuentran alojados. Su ventaja principal es que son pasivos y no interfieren con el correcto uso de la red. Su funcionamiento a través de un dispositivo configurado de forma promiscua, le permite capturar todos los paquetes que circulan por la red para su análisis.

3.2.4. Tipos de IDS en función de su estructura. Se clasifican en centralizados y distribuidos.

3.2.4.1. Distribuidos (DIDS). Según María Giménez[10] este tipo de IDS como su nombre lo indica consiste en instalar de manera distribuida varios sistemas,

[8] Ibíd., p. 14-15.
[9] Ibíd., p. 15-17.
[10] Ibíd., p. 17-18.

repartidos en diferentes equipos y puntos de red, los cuales se comunican con un nodo central que se encarga de recibir toda la información pertinente y donde se correlacionan los datos con el fin de tener una visión mucho más amplia del sistema y detectar con precisión los ataques y amenazas.

3.2.4.2. Centralizados. Según María Giménez[11] en este tipo de IDS se utilizan sensores que se encargan de transmitir la información a un sistema central donde lleva el control de todo el proceso. Una de las ventajas con respecto al distribuido es el ahorro en la adquisición de equipos.

3.2.5. Tipos de IDS en Función de su Comportamiento. Según María Giménez[12] los IDS pasivos (Escuchan el trafico pero solamente previenen ataques) e y los IDS activos (responden a los ataques con respuesta defensivas).

[11] Ibíd., p. 18-19.
[12] Ibíd., p. 19-20.

3.2.5.1. Pasivos (IDS). Como dice María Giménez[13] Este tipo de sistemas solo se encargan de generar alertas o notificaciones a las personas encaradas de la seguridad de la red, pero no toman acciones correctivas o defensivas para solucionar el evento.

3.2.5.2. Activos (IPS). Como dice María Giménez[14] Este tipo de sistemas reaccionan a eventos que se estén presentando en la red y toma las medidas correctivas necesarias para solucionar el ataque que se está presentando.

3.2.6. Introducción a Snort. Beatriz Martínez[15] define a Snort como un Sniffer de paquetes y un IDS de red. Mattew Tanase[16] considera a Snort como un software que se encarga de registrar todo el tráfico que circula tanto dentro como fuera de un ordenador conectado a la Internet.

Por otra parte Northcutt S, Kohlenberg T, Esler J, Beale J, Baker A[17] define a Snort como un IDS de red que registra y analiza todo el tráfico en tiempo real.

Beatriz Martinez[18] describe a Snort este es un software de licencia Open Source que tiene grandes características para el manejo de la seguridad. Este software

---

[13] Ibíd., p. 19.
[14] Ibíd., p. 19-20.
[15] MARTÍNEZ SANTOS, Beatriz [en línea]. Stella, una honeypot virtual de alta interacción para Windows XP. Proyecto Final (Ingeniería de telecomunicación). Madrid. Universidad Carlos III de Madrid. 2009 [Citado 15, mayo, 2017]. P 45. Disponible en: <https://e-archivo.uc3m.es/bitstream/handle/10016/5929/PFC_Beatriz_Martinez_Santos.pdf?sequencDe=1>.
[16] TANASE, Mattew. Sniffers: What They Are and How to Protect Yourself [en línea]. [Citado 20 de junio de 2017]< https://www.symantec.com/connect/articles/sniffers-what-they-are-and-how-protect-yourself >.
[17] NORTHCUTT, Stephen; KOHLENBERG, Toby; ESLER, Joel; BEALE, Jay y BAKER, Andrew R. [en línea]. Snort Intrusion Detection and Prevention Toolkit. Burlington, MA : Syngress. 2007. [Citado 5, mayo, 2017]. P 34. Disponible en: <http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=nlebk&AN=214744&lang=es&site=eds-live&ebv=EB&ppid=pp_Cover>.
[18] MARTINEZ. Op. cit., p. 45

permite analizar y monitorear distintos host dentro de una red, generando una serie de alertas de los posibles ataques llevados a cabo en contra del sistema. Este software se puede integrar con MYSQL para gestionar mejor los registros generados de los ataques.

3.2.7. Características técnicas. Las principales características técnicas que posee Snort se describirán a continuación:

FlexResp si existe una conexión que esté generando tráfico malicioso, la destruye a través de un DROP mediante el envío de un paquete con el flag RST.

Otra característica es su subsistema flexible de firmas de ataques.

Se encargan de buscar una serie de patrones que se establecieron con anterioridad que impliquen algún evento anormal dentro de la red u Host.

Aportan a la organización unas capacidades de seguridad, en lo que tiene que ver con la prevención y alertas anticipadas de cualquier evento anormal.

No se concibieron para detener ataques, pero si permiten generar una serie de respuestas a estos[19].

3.2.8. Arquitectura de Snort. La arquitectura de Snort, presenta unos componentes básicos para su funcionamiento que se describen a continuación:

[19] MENDOZA, Jaime [en línea]. Conociendo SNORT. 2010. [Citado 10, abril, 2017]. p 12. Disponible en: <https://www.owasp.org/images/d/df/OWASP_PRESENTACION_SNORT_JIMR.pdf>.

Módulo de captura del tráfico: Permite la captura de los paquetes que viajan por la red utilizando la librería libcap.

Decodificador: Se encarga de tomar los paquetes que están viajando por la red y tipificarlos en los diferentes protocolos.

Preprocesadores: Es el tipo de tráfico al cual se quiere realizar análisis del tráfico por ejemplo http, telnet, IP etc.

Motor de Detección: Se encarga del análisis de los paquetes con base en unas reglas ya preestablecidas para la detección de los ataques.

Archivo de Reglas: Son el conjunto de reglas definidas para la detección de las amenazas[20].

[20] GÓMEZ LÓPEZ, Julio. Optimización de sistemas de detección de intrusos en red utilizando técnicas computacionales avanzadas. Universidad de Almería. 2009. p 22

Ilustración 4. Esquema de Snort

Fuente: http://www.adminso.es/images/d/d0/Pfc_Carlos_cap3.pdf.

3.2.9. Modos de alerta de Snort. Este software Snort trae consigo 4 tipos de alertas las cuales describen a continuación:

Syslog. Envía las alarmas al syslog

Formato Syslog:

output alert_syslog: LOG_AUTH LOG_ALERT

output alert_syslog: host= hostname:port, LOG_AUTH LOG_ALERT
Alert_Fast: Esta alerta devuelve información sobre: tiempo, mensaje de alerta, clasificación, prioridad de la alerta, IP puerto de origen y destino.

Formato alert_Fast:

alert_fast: <output filename>

output alert_fast: alert.fast

Alert_Full: Este tipo de alerta completa devuelve información sobre: tiempo, mensaje de la alerta, clasificación, prioridad de la alerta, IP y

puerto de origen/destino e información completa de las cabeceras de los paquetes registrados.

Formato alert_Full: alert_full: <output filename>

output alert_full: alert.full.

Alert_smb: Permite a Snort realizar llamadas al cliente de SMB, y enviar mensajes de alerta a hosts Windows (WinPopUp). Para activar este modo de alerta, se debe compilar Snort con el conmutador de habilitar alertas SMB.

(enable –smbalerts). Evidentemente este modo es para sistemas Linux/UNIX.

Para usar esta característica enviando un WinPopUp a un sistema Windows, añadiremos a la línea de comandos de Snort: -M WORKSTATIONS.

Formato alert_smb:

alert_smb: <alert workstation filename>

output alert_smb: workstation.list

Alert_unixsock: Manda las alertas a través de un socket, para que las escuche otra aplicación.

Formato alert_unixsock:

alert_unixsock.

output alert_unixsock.[21]

3.2.10. Pasos configuración Snort. Para poder trabajar con Snort se deben realizar una serie de pasos para poder ponerlo en marcha, esta configuración se realiza sobre un sistema operativo Linux:

[21] GIMÉNEZ. Op. cit., p. 56-58.

Se crea el directorio de trabajo de snort:

mkdir /etc/snort

Se crea el directorio donde se van a guardar las firmas:

mkdir /etc/snort/rules

Se crea el directorio donde va a guardar el registro de actividad:

mkdir /var/log/snort

Agregar el usuario

adduser snort

Cambiar el propietario del archivo

chown snort /var/log/snort

Se crea el fichero de configuración local:

touch /etc/sysconfig/snort

Se copia el ejecutable a su directorio de trabajo:

cp /usr/local/bin/snort /usr/sbin

A continuación, se deben copiar los ficheros necesarios para poder trabajar con Snort:

Ficheros de configuración.

Se copia el fichero snort.conf en /etc/snort/ de la siguiente forma:

cp /root/snort-2.8.0.1/etc/snort.conf /etc/snort/

Se copia el fichero unicode.map en /etc/snort ejecutando:

cp /root/snort-2.8.0.1/etc/unicode.map /etc/snort/

Se copia el script de inicio del servidor:

cp /root/snort-2.8.0.1/rpm/snortd /etc/init.d/

chmod 755 /etc/init.d/snortd

Firmas:

Se deben de descargar las firmas de Snort desde www.snort.org y descomprimir las firmas en la carpeta /etc/snort/rules.

Posteriormente se copian los archivos con la extensión .config en el directorio /etc/snort. Estos archivos son classification.config y references.config:

cp /etc/snort/rules/*.config /etc/snort

Preprocesadores:

Se crea la carpeta donde se van a guardar los preprocesadores ejecutando:

mkdir /etc/snort/preproc_rules

Finalmente se copian los preprocesadores del directorio de las fuentes a la carpeta que hemos creado:

cp /root/snort-2.8.0.1/preproc_rules/* /etc/snort/preproc_rules/

El fichero de configuración (/etc/snort/snort.conf) les permite configurar el sistema para realizar las siguientes acciones:

Se debe especificar cuáles son las redes o red sobre la cual actuara Snort.

Configurar librerías dinámicas. Estas librerías son archivos independientes que son llamados desde el ejecutable.

Configurar los preprocesadores. Son extensiones que permiten definir la forma como se analizan y detectan los paquetes.

Configurar los plugins de salida. Establecer la forma de presentar la información ya sea por pantalla, Base de datos, log etc [22].

[22] Ibíd., p. 70-72.

3.2.11. Creación de reglas de detección. Julio Gómez[23] define las reglas o firmas como patrones que se buscan dentro de los paquetes de datos. Las reglas o patrones Snort son utilizadas por el motor de detección para comparar los paquetes recibidos y generar las alertas en caso de existir coincidencia entre el contenido del paquete y las firmas. El archivo utilizado para añadir o eliminar clases enteras de reglas se encuentra ubicado en /etc/snort/snort.conf. Este archivo permite desactivar toda una categoría comentando la línea de la misma.

Ahora describiremos como se crean las reglas en Snort:

3.2.11.1. Estructura de una regla. Las reglas en Snort son unas instrucciones dentro del fichero de reglas, que se deben escriben en una sola línea, en caso contrario se debe usar el carácter de escape (\).

El siguiente es un ejemplo de la creación de una regla:

alert tcp any 110 -> (content:"filename=\"infeccion.TXT.vbs\"";\ nocase; msg "Virus-Infección";)

Estas reglas se dividen en dos partes como se muestran a continuación:

La cabecera: está conformada por la acción de la regla, el protocolo IP, máscaras de red, puertos de origen y destino del paquete o dirección de la operación.

La sección opciones: trae dentro los mensajes información útil para tomar la decisión.

[23] GÓMEZ. Op. cit., p. 25-40.

3.2.11.2. Cabecera de una regla. La cabecera es la encargada de identificar el origen y destino de la comunicación, y esta información ejecuta una acción determinada. a continuación, se describe como se encuentra estructurada una regla:

<acción> <protocolo> <red origen> <puerto origen> <dirección> <red destino> <puerto destino> .

3.2.11.3. Opciones de una regla. Contiene toda la información que necesita Snort para tomar una decisión. Se definen 4 tipos de reglas, las cuales se describirán a continuación:

Metadata: Es el encargado de suministrar a los administradores del sistema información adicional relacionada con la regla.

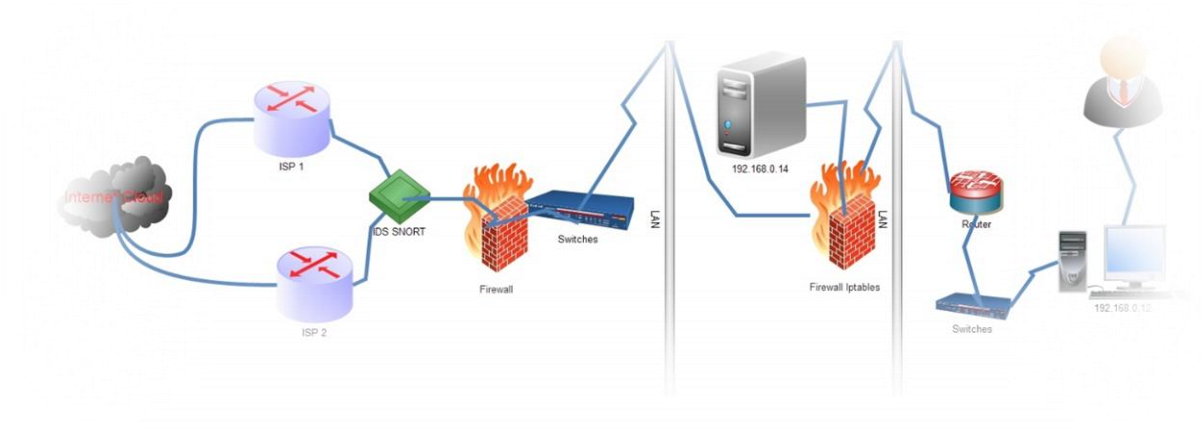
Payload: Se encarga de realizar una búsqueda de patrones o firmas dentro de la carga útil de paquetes.

Non-Payload: Se encarga de realizar una búsqueda de patrones dentro de los demás campos del paquete cuando estos no son carga útil.

Post-detection: Es el encargado de habilitar las reglas específicas, las cuales se ejecutan luego de que se ejecuta una regla[24].

[24] Ibíd., p. 25-40.

Ilustración 5. Arquitecturas de red para despliegue de Snort.



Fuente: El autor.

3.2.12. Activo. Es un componente o funcionalidad de un sistema de información que puede ser atacado de forma equivocada o con pleno consentimiento, con un impacto negativo dentro de la organización.

3.2.13. Amenaza. Causa potencial de un evento o incidente no deseado, el cual puede causar un daño al sistema o una organización[25].

3.2.14. Ids. Es un sistema que posee unos sensores que permiten detectar un acceso no autorizado a una red o a un host.

3.2.15. Snort. Es un sistema IDS que permite detectar intrusos a través de unas reglas que utilizan firmas que permiten identificar los ataques o tráfico no convencionales.

[25] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information technology — Security techniques — Information security management systems — Overview and vocabulary. ISO. 2001. ISO/IEC 2016. 28 p.

3.2.16. Mysql. Es un motor de base de datos relacional que permite almacenar estructuras de datos como son las bases de datos.

3.2.17. Fichero. Es una porción de espacio utilizado en el disco duro en binario con un nombre físico y lógico y una ubicación física.

3.2.18. Tcp. Protocolo de comunicación estándar que se utiliza en redes de computadores y de telecomunicaciones.

3.2.19. Logs. Son archivos que contienen una bitácora o registro de transacciones que se realizan sobre un determinado sistema.

3.2.20. Puertos de red. Son las puertas lógicas del sistema operativo utilizado por una aplicación para proveer los servicios, por ejemplo para FTP se utiliza el puerto 21.

3.2.21. Linux. Sistema operativo que permite realizar tareas, administrar los recursos de un equipo y provee servicios a través de un conjunto de comandos.

3.2.22. Ip. Es una dirección lógica que identifica un host en una red y a través de la IP tiene conectividad o comunicación con los otros host de la red.

3.2.23. Sniffer. Es un sistema que husmea el tráfico que va hacia una red o un host, lo identifica y luego lo almacena en LOGS o bases de datos.

3.3. MARCO DE CONTEXTO

UNIVERSIDAD DEL SINU: [26] Para el año 1974, el Dr. Elías Bechara Zainúm funda la primera sede en la ciudad de Montería con el nombre Corporación Universitaria del Sinú con el único propósito de contribuir al cambio de la región y los alrededores. A lo largo de sus existencia la universidad se ha hecho merecedora de varios reconocimientos como se destacan los siguientes “Francisco de la Torre y Miranda” del Municipio de Montería y la condecoración “Simón Bolívar” conferida por el Ministerio de Educación Nacional.

La misión y la visión de la UNIVERSIDAD DEL SINU consiste en:

“Es deber de la Universidad del Sinú, procurar la formación integral de las personas a través de la conservación, transmisión y desarrollo de la ciencia y de la cultura en busca de la verdad y generación de conocimiento, para lograr la armonía e identidad del ser humano con el mismo, con la sociedad y su ambiente creando una sociedad global más libre, culta y justa.”[27]

La visión de la universidad es:

“Seremos una Universidad con una estructura docente, administrativa y planta física pertinente para la generación del conocimiento, consolidando la comunidad académica y las acciones de proyección social que permitan cultivar valores institucionales dentro de un sistema de aseguramiento de calidad”.

[26] UNIVERSIDAD DEL SINU. Reseña Histórica [en línea]. [citado en 5 de octubre de 2017]. http://www.unisinucartagena.edu.co/index.php/resena-historica.

[27] UNIVERSIDAD DEL SINU. Misión y Visión [en línea]. [citado en 5 de octubre de 2017]. http://www.unisinucartagena.edu.co/index.php/mision-y-vision.

Los objetivos estratégicos de la sede son:

La Universidad del Sinú ha establecido seis Ejes Estratégicos que se han determinado en el Plan de Desarrollo 2012 – 2017.

En este sentido los ejes que integran la etapa de formulación estratégica, para este nuevo período de consolidación académica y administrativa, desarrollos investigativos con impacto social e inserción en las políticas de internacionalización establecidas para la universidad, son:

- Eje 1. Fortalecimiento de la Calidad Académica.
- Eje 2. Investigación, Nuevas tecnologías y Transferencias de conocimientos.
- Eje 3. Proyección Social y Extensión.
- Eje 4. Fortalecimiento y Consolidación de Bienestar Universitario.
- Eje 5. Internacionalización.
- Eje 6. Modernización Administrativa y Fortalecimiento Financiero.

3.4. MARCO LEGAL

A continuación, se relacionan las normas y leyes aplicables al proyecto.

3.4.1. Ley 1273 de 2009[28].

[28] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 (5, enero, 2009). 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.. Diario Oficial. Bogotá. 2009. 4 p.

3.4.2. Ley Estatutaria 1266 del 31 de diciembre de 2008, art 3°, lit. e, f, g y h y Sentencia C-1011/08. Datos personales e impersonales. “e) Dato personal. Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados;

f) Dato público. Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas;

g) Dato semiprivado. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley.

h) Dato privado. Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular;”[29]

[29] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1266 (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información

3.4.3. Convenio sobre la ciberdelincuencia Budapest. Tratado europeo # 185 con el objetivo de aplicar con carácter prioritario una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional[30].

3.4.4. Ley 527 de 1999[31].

3.4.5. Ley 734 de 2002[32].

3.4.6. Ley 842 de 2003[33].

3.4.7. Ley 1581 de 2012[34].

3.4.8. Ley 1712 de 2014[35].

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. Diario Oficial. Bogotá. 2008. 17 p.

[30] CONVENIO SOBRE LA CIBERDELINCUENCIA [en línea]. Budapest. (23, noviembre, 2001). [Citado 8, marzo, 2017]. 26 p. Disponible en: <http://www.oas.org/juridico/english/cyb_pry_convenio.pdf>.

[31] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527 (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial. Bogotá. 1999. no. 43673.

[32] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 734 (5, febrero, 2002). Por la cual se expide el Código Disciplinario Único. Diario Oficial. Bogotá. 2002. no. 44699

[33] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 842 (9, octubre, 2003). Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones. Diario Oficial. Bogotá. 2002. no. 45340.

[34] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá. 2012. no. 48587.

[35] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1712 (6, marzo, 2014). Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Diario Oficial. Bogotá. 2014. no. 49084 .13 p

4. METODOLOGÍA

Para llevar a cabo la metodología este proyecto nos basaremos en la metodología de Roberto Hernández Sampieri[36].

4.1. TIPO DE INVESTIGACIÓN

La investigación será aplicada ya que esta es una actividad que tiene por finalidad la búsqueda y consolidación del saber, y la aplicación de los conocimientos para el enriquecimiento del acervo cultural y científico, así como la producción de tecnología al servicio del desarrollo integral del país.

4.2. DISEÑO DE INVESTIGACIÓN

Para este proyecto la investigación fue de tipo experimental, ya que se manipularon algunas variables y escenarios para ver cómo se comportaba el IDS ante distintos eventos.

4.3. POBLACIÓN

La población está constituida por 12 trabajadores del área de sistemas

4.4. MUESTRA

La muestra estuvo conformada por 10 personas del área de sistemas donde se aplicó un muestreo probabilístico.

[36] HERNÁNDEZ SAMPIERI, Roberto [en línea]. Metodología de la Investigación. Mexico D.F. Mc Graw Hill. 2014.

Ilustración 6.Fórmula para cálculo de la muestra poblaciones finitas.

Si la población es finita, es decir conocemos el total de la población y deseásemos saber cuántos del total tendremos que estudiar la fórmula sería:

$$n = \frac{N * Z_{\alpha}^{2} p * q}{d^{2} * (N-1) + Z_{\alpha}^{2} * p * q}$$

Donde:
- N = Total de la población
- Zα= 1.96 al cuadrado (si la seguridad es del 95%)
- p = proporción esperada (en este caso 5% = 0.05)
- q = 1 – p (en este caso 1-0.05 = 0.95)
- d = precisión (en su investigación use un 5%).

Fuente: https://investigacionpediahr.files.wordpress.com/2011/01/formula-para-cc3a1lculo-de-la-muestra-poblaciones-finitas-var-categorica.pdf.

Cuadro 1. Calculo de la muestra.

Calculo Muestra Finita Murray y Larry Variables		Porcentajes	Valor
		90	1,645
n	10	95	1,96
N	12	97	2,24
Za	1,96	99	2,576
p	5		
q	0,95	95	1,96
d	5		

Fuente: El autor.

4.5. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

4.5.1. Técnica de recolección de datos. La técnica utilizada en este proyecto fue la encuesta y entrevista que permite la recolección de la información necesaria de la muestra estudiada. La encuesta fue diseñada con el objetivo de identificar la percepción de los funcionarios del área de Sistemas de la Universidad acerca de la situación actual de la seguridad informática en la institución y sus antecedentes. Se realizó a 15 funcionarios el día 5 de Septiembre de 2017.

4.5.2. Instrumentos de recolección de datos. Para el proyecto la técnica de análisis de datos que se va a utilizar es la llamada Análisis de correlaciones basada en la técnica de tabulación.

Esta técnica consiste en determinar si existe una relación entre dos variables cuantitativas diferentes y cuan fuerte es esa relación entre las variables. Se suele usar cuando se piensa que las variables tienen una evolución similar.

4.6. TECNICA DE PROCESAMIENTO DE DATOS

Teniendo en cuenta el punto anterior la técnica elegida es la TABULACION con lo cual sabremos la tendencia de las variables definidas en el cuestionario aplicado a la muestra. Esta técnica permite asignar numeración a las preguntas y una numeración a las distintas opciones que pretenden tener las respuestas a las preguntas definidas. Luego se procede a realizar graficas de análisis de los resultados.

FORMATO DE ENTREVISTA
UNIVERSIDAD DEL SINU - SEDE SANTILLANA

Nombre:	Fecha:
Edad:	Estado Civil:
Cargo que desempeña:	Estudiante de:
División / Facultad:	
Tipo de Vinculación:	

A continuación, responda las siguientes preguntas relacionadas con la seguridad de la información que Ud maneja o es relacionada con los sistemas de información de la universidad a los cuales usted accede.

Esta información es de carácter reservado.

PREGUNTA 1.

Ud ha sufrido o ha sido víctima de robo de información en esta sede de la universidad?

SI

NO

PREGUNTA 2.

Existen controles al acceder a los sistemas de información de la Universidad que permiten controlar el acceso, la copia o fuga de la información?

SI

NO

PREGUNTA 3.

Existe alguna herramienta de seguridad perimetral de protección de la información en la sede Santillana de UNISINU?

1. SI

2. NO

PREGUNTA 4.

Existen logs que permitan registrar el tráfico entrante y saliente de la red interna y perimetral de la sede Santillana de la UNISINU?

1. SI

2. NO

PREGUNTA 5.

La sede Santillana de la UNISINU ha sufrido incidentes de seguridad relacionados con indisponibilidad de servicio?

1. SI

2. NO

5. RESULTADOS

5.1. IDENTIFICACION Y CLASIFICACION DE ACTIVOS CRITICOS DE LA ORGANIZACIÓN.

Luego de realizar Identificación de los activos informáticos de la sede Santillana de UNIVERSIDAD DEL SINU se obtuvo la siguiente relación.

Tabla 1. Identificación de activos.

Nombre de activo	**Tipo de activo Magerit**	**Descripción o rol**	**Responsable**	**Disposición final**
Servidor DELL Optiplex 75	HARDWARE	Servidor Proxy	Jefe de sistemas	Centro de computo
Servidor DELL Optiplex GX 520	HARDWARE	Servidor de Red	Jefe de sistemas	Centro de computo
Servidor Power Edge 1900 (Linux)	HARDWARE	Servidor de Correo	Jefe de sistemas	Centro de computo
Servidor IBM X25 series	HARDWARE	Servidor de Base de datos	Jefe de sistemas	Centro de computo
Servidor DELL Optiplex 170L	HARDWARE	Servidor Web	Jefe de sistemas	Centro de computo
Servidor JANUS Dig Gen Core Duo	HARDWARE	Servidor Huellas	Jefe de sistemas	Centro de computo
Windows 2008 Server	SOFTWARE		Jefe de sistemas	Centro de computo
Quiron Cliente	SOFTWARE	Servidor de manejo académico	Jefe de sistemas	Centro de computo
Quiron.Net	SOFTWARE	Aplicación web para estudiantes, Docentes y funcionarios	Jefe de sistemas	Centro de computo
Quiron Campus	SOFTWARE	Aplicación virtual para estudiantes, docentes y funcionarios.	Jefe de sistemas	Centro de computo
Comodín	SOFTWARE	Software contable	Jefe de sistemas	Centro de computo
Tesorero	SOFTWARE	Software de caja	Jefe de sistemas	Centro de computo
Prisma	SOFTWARE	Software de Cartera e inventario	Jefe de sistemas	Centro de computo
Nomina	SOFTWARE	Software de Nomina	Jefe de sistemas	Centro de computo
ISIS	SOFTWARE	Software de control Bibliográfico	Jefe de sistemas	Centro de computo

Fuente: El Autor.

En la tabla anterior se encontraron unos activos informáticos con los siguientes roles:

- Servidor Proxy
- Servidor de red
- Servidor de Correo
- Servidor de base de datos
- Servidor de Huellas

También se encontraron varios softwares de servicios misionales, de apoyo y sistemas operativos como son: Windows 2008 Server, Quirón Cliente, Quiron.Net, Quirón Campus, Comodín, Tesorero, Prisma, Nomina, ISIS.

Todos los activos anteriormente mencionados están ubicados en el centro de cómputo de la sede Santillana y el custodio es el jefe de sistemas y su equipo de trabajo.

La valoración de los activos se realiza con base en los principios de confidencialidad, integridad y disponibilidad cuya calificación será la siguiente:

Confidencialidad: Este valor tendrá un rango de valores entre 1 y 5 de acuerdo a la importancia del activo, y lo representaremos con la letra C.

Integridad: Este valor tendrá un rango de valores entre 1 y 5 de acuerdo a la importancia del activo, y lo representaremos con la letra I.

Disponibilidad: Este valor tendrá un rango de valores entre 1 y 5 de acuerdo a la importancia del activo, y lo representaremos con la letra D.

Valor activo: Es la sumatoria de Confidencialidad + Integridad + Disponibilidad

Se realizó la valoración y clasificación de activos utilizando la metodología MAGERIT como se muestra a continuación:

Tabla 2. Valoración de activos.

Nombre de activo	Tipo de activo MAGERIT	Descripción o rol	Responsable	Disposición Final	C	I	D	Valor Activo
Servidor DELL Optiplex 75	HW	Servidor Proxy	Jefe de sistemas	Centro de computo	1	2	4	7
Servidor DELL Optiplex GX 520	HW	Servidor de Red	Jefe de sistemas	Centro de computo	3	3	4	10
Servidor Power Edge 1900 (Linux)	HW	Servidor de Correo	Jefe de sistemas	Centro de computo	3	2	4	9
Servidor IBM X25 series	HW	Servidor de Base de datos	Jefe de sistemas	Centro de computo	4	4	5	13
Servidor DELL Optiplex 170L	HW	Servidor Web	Jefe de sistemas	Centro de computo	3	2	3	8
Servidor JANUS Dig Gen Core Duo	HW	Servidor Huellas	Jefe de sistemas	Centro de computo	3	2	3	8
Windows 2008 Server	SW		Jefe de sistemas	Centro de computo	4	3	2	9
Quiron Cliente	SW	Servidor de manejo académico	Jefe de sistemas	Centro de computo	4	4	5	13
Quiron.Net	SW	Aplicación web para estudiantes, Docentes y funcionarios	Jefe de sistemas	Centro de computo	3	4	3	10
Quiron Campus	SW	Aplicación virtual para estudiantes, docentes y funcionarios.	Jefe de sistemas	Centro de computo	3	3	3	9
Comodín	SW	Software contable	Jefe de sistemas	Centro de computo	3	4	4	11
Tesorero	SW	Software de caja	Jefe de sistemas	Centro de computo	1	4	4	9
Prisma	SW	Software de Cartera e inventario	Jefe de sistemas	Centro de computo	2	4	3	9
Nomina	SW	Software de Nomina	Jefe de sistemas	Centro de computo	3	4	3	10
ISIS	SW	Software de control Bibliográfico	Jefe de sistemas	Centro de computo	2	3	3	8

Fuente: El Autor.

Como resultado de la valoración de activos se obtuvieron 3 activos informáticos más críticos dentro de la entidad como son: el servidor de base de datos, el software

Quirón Cliente y el software de Comodín, los cuales se van a proteger por el gran impacto que estos tienen dentro de la organización. A continuación, relacionamos los activos y el valor obtenido.

Tabla 3. Resultado valoración de activos.

NOMBRE DE ACTIVO	TIPO ACTIVO	DESCRIPCION O ROL	VALOR ACTIVO
Servidor IBM X25 series	HARDWARE	Servidor de Base de datos	13
Quirón cliente	SOFTWARE	Software de manejo académico	13
Comodín	SOFTWARE	Software Contable	11

Fuente: El Autor.

5.2. EVALUACION DEL NIVEL DE SEGURIDAD DE LOS ACTIVOS INFORMATICOS CRITICOS DE LA ORGANIZACIÓN.

Se realizó una evaluación de seguridad a los siguientes activos informáticos más críticos.

Tabla 4. Evaluación del nivel de seguridad de los activos.

NOMBRE DE ACTIVO	DESCRIPCION O ROL	FIREWALL	IPS / IDS	WAF	ANTIVIRUS	NIVEL DE SEGURIDAD
Servidor IBM X25 series	Servidor de Base de datos	NO	NO	N/A	SI	BAJO
Quirón cliente	Software de manejo académico	NO	NO	NO	SI	BAJO
Comodín	Software Contable	NO	NO	NO	SI	BAJO

Fuente: El Autor.

En la evaluación realizada se evidencia que los activos críticos no poseen sistemas de protección de seguridad como son Firewall, IPS, IDS y WAF (Web Application Firewall) por lo cual se determina que su nivel de seguridad es bajo y se considera indispensable la implementación de un sistema de detección de intrusos IDS.

5.3. DESCRIPCION DE LAS FORMAS EN QUE TRABAJA SNORT (MODO SNIFFER, PACKET LOGGER, MODO NIDS O MODO INLINE) COMO SISTEMA DE DETECCIÓN DE INTRUSOS EN UNA ORGANIZACIÓN.

5.3.1. Modo Sniffer. Captura el tráfico del host o red y lo visualiza en pantalla a través de su plugin. Luego que finaliza, visualiza una estadística del tráfico. Para empezar el modo sniffer y mostrar todo el tráfico en pantalla digitamos el comando snort -v o snort – dev en una terminal. Este modo crea un brigde o puente transparente entre dos segmentos de red. Esto significa que Snort tiene dos interfaces de red: cada una en un segmento de red diferente. Configurará estas interfaces sin una dirección IP y en modo promiscuo. Cuando ejecuta Snort, escuchará el tráfico en cada interfaz. Cuando llega un paquete a una interfaz, Snort lo inspecciona de acuerdo con sus reglas, luego lo suelta o lo envía a la otra interfaz sin ninguna modificación. Debido a esto, los dos segmentos de red que manejan puentes deben ser parte de la misma subred lógica.

De esta forma el SNORT detecta un ataque o comportamiento sospechoso, envía a IPTABLES la petición para que interrumpa el tráfico de esa sesión. Para este modo se debe configurar la tarjeta de red en modo promiscuo en cada bridge que sea utilizado.

5.3.2. Modo Packet Logger. Al igual que el MODO SNIFFER captura el tráfico del host o la red, pero adicional guarda los datos en unos logs para luego analizarlos. Para ejecutarlo en este modo se escribe el comando -l y el nombre del directorio donde se guardará.

5.3.3. Modo Nids. Este modo de operación es más completo y configurable. Permite analizar todo el tráfico de la red en busca de intrusiones a partir de reglas y firmas que el usuario configura. Este método, además de registrar los logs, almacena los eventos en una base de datos y los visualiza a través de un plugin de salida. También cuando Snort detecte tráfico sospechoso, se bloqueará ese tráfico y la dirección IP origen. El resultado mostrará intentos de acceso no permitidos, escaneos de puertos, ataques DOS, ejecución de exploits. Para configurarlo en este modo se debe modificar el fichero de configuración SNORT.CONF escribiendo el parámetro -c así:

```
/usr/sbin/snort -d  -l /var/log/snort -c  /etc/snort/snort.conf
```

Definitivamente la mejor opción es la tercera MODO NIDS ya que cumple con los objetivos más importantes de la herramienta que es la detección de Intrusos, su registro, su bloqueo, su almacenamiento con datos de fecha y hora para servir de evidencia forense. A continuación, mostraremos como sería una salida del comando.

Ilustración 7. Salida de comando SNORT.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+=+=+=+=+

05/21-11:06:18.943887 192.168.4.5:3890 -> 192.168.4.15:8080
TCP TTL:128 TOS:0x0 ID:33216 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xE3A50016 Ack: 0x8B3C1E4D Win: 0xFAF0 TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+=+=+=+=+

05/21-11:06:18.962018 192.168.4.5:3890 -> 192.168.4.15:8080
TCP TTL:128 TOS:0x0 ID:33217 IpLen:20 DgmLen:681 DF
***AP*** Seq: 0xE3A50016 Ack: 0x8B3C1E4D Win: 0xFAF0 TcpLen: 20
47 45 54 20 68 74 74 70 3A 2F 2F 77 77 77 2E 6F GET http://www.x
6D 65 6C 65 74 65 2E 63 6F 6D 2E 62 72 2F 73 75 xxxx.com.br/xx
70 65 72 6F 6D 65 6C 65 74 65 2F 64 6F 77 6E 6C xxxxxxx/downl
6F 61 64 73 2F 64 65 66 61 75 6C 74 2E 61 73 70 oads/default.asp
20 48 54 54 50 2F 31 2E 30 0D 0A 55 73 65 72 2D HTTP/1.0..User-
41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 34 Agent: Mozilla/4
2E 30 20 28 63 6F 6D 70 61 74 69 62 6C 65 3B 20 .0 (compatible;
4D 53 49 45 20 36 2E 30 3B 20 57 69 6E 64 6F 77 MSIE 6.0; Window
73 20 4E 54 20 35 2E 30 29 20 4F 70 65 72 61 20 s NT 5.0) Opera
37 2E 31 31 20 20 5B 65 6E 5D 0D 0A 48 6F 73 74 7.11 [en]..Host
3A 20 77 77 77 2E 6F 6D 65 6C 65 74 65 2E 63 6F : www.xxxxx.co
6D 2E 62 72 0D 0A 41 63 63 65 70 74 3A 20 74 65 m.br..Accept: te
78 74 2F 68 74 6D 6C 2C 20 69 6D 61 67 65 2F 70 xt/html, image/p
6E 67 2C 20 69 6D 61 67 65 2F 6A 70 65 67 2C 20 ng, image/jpeg,
69 6D 61 67 65 2F 67 69 66 2C 20 69 6D 61 67 65 image/gif, image
2F 78 2D 78 62 69 74 6D 61 70 2C 20 2A 2F 2A 3B /x-xbitmap, */*;
71 3D 30 2E 31 0D 0A 41 63 63 65 70 74 2D 4C 61 q=0.1..Accept-La
```

Fuente: http://www.maestrosdelweb.com/snort/.

5.4. DISEÑO DE LA INFRAESTRUCTURA NECESARIA PARA EL BUEN FUNCIONAMIENTO DEL SISTEMA DE DETECCIÓN DE INTRUSOS – IDS SNORT EN LA UNISINU.

Para el diseño del sistema IDS SNORT se hace necesario contar con la infraestructura tecnológica necesaria para su buen funcionamiento. A continuación, se describen los componentes que harán parte de la infraestructura necesaria para la implementación.

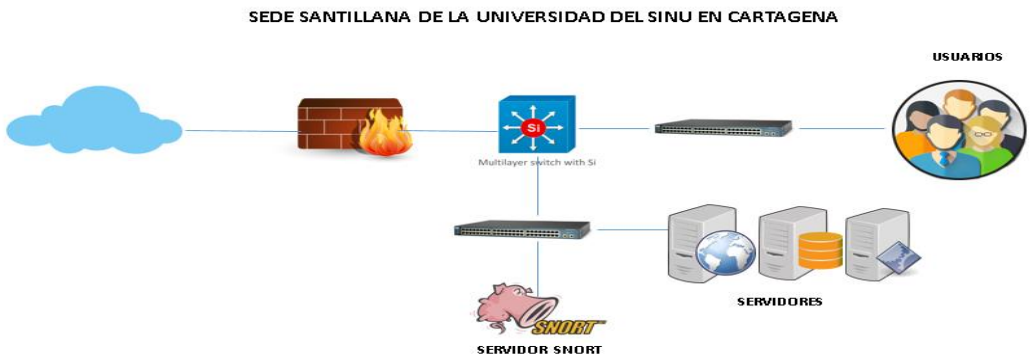
5.4.1. Software. El sistema operativo para este diseño es Ubuntu Server 16.04.3 LTS a 64 bits. Este software no requiere de licencia o suscripción alguna. Se requiere el programa SNORT IDS que en su arquitectura de software consta de 4

componentes o capas como son el motor de SNORT, el motor de base de datos MYSQL, el paquete que administra la actualización de reglas y firmas llamado PULLED PORK, el plugin que está compuesto por el PHP y el presentador Apache, con el fin de capturar el tráfico de los activos a ser monitoreados se hace necesario diseñar la infraestructura tecnológica que va soportar las operaciones que realizan los componente mencionados anteriormente. Para este software se debe adquirir una licencia de suscripción con todas las reglas y actualizaciones.

5.4.2. Hardware. Esta solución de propósito específico se recomienda que sea instalada en una maquina física con al menos 4 tarjetas de red de alta velocidad de al menos 1mbps, discos duros de estado sólido con capacidad mínima de 1 Tera en RAID 1, procesadores de generación 9 o mayor y memoria RAM mínimo de 16GB. Todo este hardware será exclusivo para la solución en diseño.

Red: esta solución se instalará en la misma subred de los servidores para que capture el tráfico, lo analice y genere oportunamente los eventos, alarmas y estadísticas.

Ilustración 8. Diagrama de red sede Santillana UNISINU.



Fuente: El autor.

5.4.3. Descripción diagrama de red. A continuación, se describe el diagrama de red con sus elementos.

Firewall Perimetral. Este firewall tiene habilitado las características de UTM como son proxy, filtro web, control de aplicaciones, Inspección SSL, políticas o reglas para controlar y restringir el tráfico, este firewall tendrá habilitada una política para darle salida a internet al servidor SNORT que le permitirá actualizar las reglas. Por otro lado, a través de este firewall los usuarios y otros dispositivos tendrán salida hacia Internet de manera controlada.

Switch de Core. Este dispositivo de red administrará las VLAN de todas las subredes existentes en la sede Santillana, tendrá los Gateway de las subredes permitiendo de esta forma la comunicación del tráfico entre varios segmentos.

Switch de Borde de usuarios. Este Switch permitirá el acceso de los usuarios a internet a través del Core y el Firewall y también el acceso a los servidores de base de datos, Quirón Cliente y el Comodín.

Switch de Servidores. Este dispositivo tendrá configurado la red de servidores y en los cuales se van a conectar el servidor de base de datos, el servidor Quirón Cliente y el servidor de Comodín.

Servidores. Estos son los activos informáticos más críticos de la sede Santillana como son: el servidor de base de datos, el software Quirón Cliente y el software de Comodín. Adicional está conectado el servidor SNORT que realizara el monitoreo con su sistema IDS sobre los más activos críticos.

A continuación, se relacionan algunas firmas de las que dispone el SNORT:

- Reglas para detección de ataques de denegación de servicios distribuidos DDOS. A continuación, se muestra un ejemplo de cómo se configura:

  alert tcp $HTTP_SERVERS any -> $EXTERNAL_NET any (msg:"ET WEB_SERVER Mambo.PerlBot Spreader IRC DDOS Attacking Message"; flow:established,to_server; content:"PRIVMSG|20|"; content:"Attacking"; within:50; fast_pattern; classtype:trojan-activity; sid:2017831; rev:2;)

- Reglas para detección de ataques XSS Cross-site scripting. A continuación se muestra un ejemplo de cómo se configura:

  alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible HTTP 401 XSS Attempt (External Source)"; flow:from_server,established; content:"401"; http_stat_code; content:"Unauthorized"; nocase; file_data; content:"<script"; nocase;

within:280; reference:url,doc.emergingthreats.net/2010514; classtype:web-application-attack; sid:2010514; rev:8;)

- Reglas para detectar NMAP, escaneo de puertos y análisis de vulnerabilidades. A continuación se muestra un ejemplo como se configura:

  alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN NMAP SIP Version Detect OPTIONS Scan"; flow:established,to_server; content:"OPTIONS sip|3A|nm SIP/"; depth:19; classtype:attempted-recon; sid:2018317; rev:1;)

- Reglas para detectar pruebas de envió de paquetes ICMP.

  alert icmp any any -> $HOME_NET any (msg:"ICMP test detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)

- Reglas para detectar ataques de SQL Inyección. A continuación se muestra un ejemplo de cómo se configura:

  alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET WEB_SPECIFIC_APPS Mambo N-Myndir UPDATE SET SQL Injection Attempt"; flow:established,to_server; content:"GET"; http_method; content:"/index.php?"; nocase; http_uri; content:"option=com_n-myndir"; nocase; http_uri; content:"flokkur="; nocase; http_uri; content:"UPDATE"; nocase; http_uri; content:"SET"; nocase; http_uri; pcre:"/UPDATE.+SET/Ui"; reference:url,packetstormsecurity.org/files/view/104706/mambonmyndir-sql.txt; classtype:web-application-attack; sid:2013708; rev:2;

Dentro de las configuraciones que debe tener el sistema IDS está la habilitación de notificaciones en tiempo real, al momento de la detección del ataque o comportamiento anómalo, el administrador de la red recibirá un correo donde se le está informando el incidente de seguridad, por otro lado, también tendrá una interfaz web o pluging de salida que le permitirá monitorear en modo grafico los eventos, alertos y estadísticas que la herramienta almacena en una base de datos.

6. DISCUSIÓN DE RESULTADOS

Esta investigación tuvo como objetivo estudiar y diseñar un sistema de detección de intrusos capas de salvaguardar los activos informáticos críticos al interior de la universidad del Sinú. Lo que se pretendió fue estudiar cual era la mejor forma para configurar el IDS SNORT, así como también cual era la infraestructura necesaria para el buen funcionamiento del software. Por otro lado se pretendió realizar una calificación y evaluación de los activos, con el fin de encontrar cuales eran los más importantes dentro de la entidad. También, se identificaron aquellas fallas de seguridad dentro de la universidad.

De los resultados obtenidos en la investigación, podemos inferir que actualmente los ataques informáticos, son mucho más sofisticados su tipología muy variada y en muchos casos las actividades maliciosas pasan desapercibidos por los sistemas de detección de intrusos. Los ciberdelincuentes utilizan técnicas de hacking cada vez más avanzadas para burlar cualquier tipo de salvaguarda del que se disponga dentro de la entidad u organización.

Como lo afirman en su investigación José Mira, Anthony González y Gilberto Garzón; el IDS SNORT permite generar alertas en tiempo real, evitando que un atacante ingrese a nuestros sistemas y se vean comprometidos. Cabe destacar que todos los autores buscan el mismo fin proteger los activos .críticos dentro de la organización

Por otro lado Javier Martínez afirma que su proyecto se diferencia de los otros porque este es capaz de detectar un código malicioso al momento que este viaja

sobre la red de datos, si bien es cierto que para el momento de la investigación era algo innovador en ese momento es una característica que trae el IDS SNORT dentro sus funcionalidades en la actualidad.

Por otro lado, los resultados obtenidos en esta investigación se pueden tomar como base para diseñar un sistema de detección de intrusos dentro de una entidad, con el fin de mitigar y contrarrestar los riesgos informáticos a los que se encuentran expuestos día a día.

Es necesario que se continúe investigando sobre cómo evolucionan los diferentes ataques informáticos y las vulnerabilidades a las cuales nos encontramos expuestos, así como también los diferentes salvaguardas existentes para contrarrestar y mitigar el impacto de que ocurra algún siniestro.

7. CONCLUSIONES

El proyecto se llevó a cabo con la finalidad de realizar el diseño del sistema de detección de intrusos IDS –SNORT para la sede Santillana de la UNISINU en donde se lograron obtener unos resultados que permitieron determinar que es factible y necesaria su implementación.

Luego de identificar y valorar los activos informáticos más críticos de la sede Santillana de UNIVERSIDAD DEL SINU se evidenció que por su nivel de criticidad es indispensable proteger los servidores y elementos de red.

En la evaluación del nivel de seguridad que mostró la alta vulnerabilidad que tienen los activos críticos, lo anterior indica que se debe reforzar la seguridad de los activos más críticos.

De acuerdo a los modos de operación del IDS-SNORT analizados, se debe usar el modo NIDS por tener más visibilidad y ser más integral.

En la infraestructura diseñada se debe realizar las configuraciones y arquitecturas recomendadas para obtener un resultado óptimo en la implementación.

7. RECOMENDACIONES

Luego de realizar el diseño del sistema de detección de intrusos IDS, se tienen las siguientes recomendaciones para la UNISINU sede Santillana:

- Que la Dirección de la universidad tome como iniciativa implementación del IDS SNORT para mejorar el nivel de seguridad de la red y servicios críticos de la sede Santillana.

- Se recomienda antes de la implementación realizar pruebas o demo para un buen dimensionamiento de la solución.

- Adquirir el servicio de suscripción para tener todo el potencial de las reglas y firmas de SNORT. Esta suscripción se renueva anualmente.

- Alinear el sistema IDS con el sistema de seguridad de la información y la gestión de incidentes de seguridad.

- Alinear el sistema IDS con un objetivo estratégico de la Universidad.

8. BIBLIOGRAFÍA

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1266 (31, diciembre, 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. Diario Oficial. Bogotá. 2008. 17 p.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 (5, enero, 2009). Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá. 2009. 4 p.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá. 2012. no. 48587.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1712 (6, marzo, 2014). Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Diario Oficial. Bogotá. 2014. no. 49084 .13 p.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527 (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial. Bogotá. 1999. no. 43673.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 734 (5, febrero, 2002). Por la cual se expide el Código Disciplinario Único. Diario Oficial. Bogotá. 2002. no. 44699.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 842 (9, octubre, 2003). Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones. Diario Oficial. Bogotá. 2003. no. 45340.

CONVENIO SOBRE LA CIBERDELINCUENCIA [en línea]. Budapest. (23, noviembre, 2001). 26 p. [Citado 8, marzo, 2017]. Disponible en: <http://www.oas.org/juridico/english/cyb_pry_convenio.pdf>.

GARZON PADILLA, Gilberto [en línea]. Propuesta para la implementación de un sistema de detección de intrusos (IDS) en la dirección general sede central del instituto nacional penitenciario y carcelario INPEC“PIDSINPEC, 75 p: Proyecto de Grado (Especialista en seguridad informática) Universidad Nacional Abierta y a Distancia. [Citado 20, noviembre, 2017]. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3494/3/86057594.pdf.

GIMÉNEZ GARCÍA, María Isabel [en línea]. Utilización de Sistemas de Detección de Intrusos como Elemento de Seguridad Perimetral. Almería: Universidad de Almería, 2008. 262 p. [Citado 10, abril, 2017]. Disponible en: <http://www.adminso.es/recursos/Proyectos/PFC/PFC_marisa.pdf>.

GÓMEZ LÓPEZ, Julio. Optimización de sistemas de detección de intrusos en red utilizando técnicas computacionales avanzadas. Universidad de Almería. 2009. 127 p.

GONZÁLEZ DA SILVA, Anthony Rafael [en línea]. Implementar un Sistema de Detención de Intruso (IDS) en la Red Wifi del Laboratorio G de la Universidad Simón Bolívar sede litoral. Informe final de pasantías. Universidad Simón Bolívar, Coordinación de tecnología eléctrica y electrónica. 20010. 161 p. [Citado 15, mayo, 2017]. Disponible en: <https://e-archivo.uc3m.es/bitstream/handle/10016/5929/PFC_Beatriz_Martinez_Santos.pdf?sequencDe=1>.

GONZÁLEZ GÓMEZ, Diego [en línea]. Sistema de Detección de Intrucciones. 2010. 292 p. [Citado 5, mayo, 2017]. Disponible en: <http://derecho-internet.org/docs/ids.pdf>.

HERNÁNDEZ SAMPIERI, Roberto [en línea]. Metodología de la Investigación. Mexico D.F. Mc Graw Hill. 2014.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information technology — Security techniques — Information security management systems — Overview and vocabulary. ISO. 2001. ISO/IEC 2016. 28 p.

MARTÍNEZ PUENTES, Javier [en línea]. Sistemas inteligentes de detección de intrusos, 119 p: Proyecto de Grado (Master en investigación informática) universidad complutense de Madrid. [Citado 20, noviembre, 2017]. Disponible en: http://eprints.ucm.es/13504/1/MA_2011-15.pdf

MARTÍNEZ SANTOS, Beatriz [en línea]. Stella, una honeypot virtual de alta interacción para Windows XP. Proyecto Final (Ingeniería de telecomunicación). Madrid. Universidad Carlos III de Madrid. 2009. 161 p. [Citado 15, mayo, 2017].

Disponible en: <https://e-archivo.uc3m.es/bitstream/handle/10016/5929/PFC_Beatriz_Martinez_Santos.pdf?sequencDe=1>.

MENDOZA, Jaime [en línea]. Conociendo SNORT. 2010. 32 p. [Citado 10, abril, 2017]. Disponible en: <https://www.owasp.org/images/d/df/OWASP_PRESENTACION_SNORT_JIMR.pdf>.

MIRA ALFARO, Emilio José [en línea]. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Proyecto Final (Ingeniería Informática). Valencia. Universidad de Valencia. 142 p. [Citado 10, abril, 2017]. Disponible en: <http://rediris.es/cert/doc/pdf/ids-uv.pdf>.

NORTHCUTT, Stephen; KOHLENBERG, Toby; ESLER, Joel; BEALE, Jay y BAKER, Andrew R. [en línea]. Snort Intrusion Detection and Prevention Toolkit. Burlington, MA : Syngress. 2007. 734 p. [Citado 5, mayo, 2017]. Disponible en: <http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=nlebk&AN=214744&lang=es&site=eds-live&ebv=EB&ppid=pp_Cover>.

TANASE, Mattew. Sniffers: What They Are and How to Protect Yourself [en línea]. [Citado 20 de junio de 2017]. Disponible en: <https://www.symantec.com/connect/articles/sniffers-what-they-are-and-how-protect-yourself>.

UNIVERSIDAD DEL SINU. Misión y Visión [en línea]. [Citado en 5 de octubre de 2017]. Disponible en: <http://www.unisinucartagena.edu.co/index.php/mision-y-vision>.

UNIVERSIDAD DEL SINU. Reseña Histórica [en línea]. [Citado 5 de octubre de 2017]. Disponible en: <http://www.unisinucartagena.edu.co/index.php/resena-historica>.