UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

ARTÍCULO CIENTÍFICO:

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

“SISTEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE DATOS DE LA INDUSTRIA FLORALP S.A EN LA CIUDAD DE IBARRA, BASADO EN LA PLATAFORMA DE SOFTWARE LIBRE”

AUTORA: GABRIELA JANETH LÓPEZ PAREDES

DIRECTORA: ING. SANDRA CASTRO

Ibarra – 2015

SISTEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE DATOS DE LA INDUSTRIA FLORALP S.A EN LA CIUDAD DE IBARRA, BASADO EN LA PLATAFORMA DE SOFTWARE LIBRE

Gabriela J. López P.
Universidad Técnica del Norte

***Resumen*— La masiva utilización de servicios informáticos y redes como medios para trasferir, procesar y almacenar información en los últimos años ha incrementado, trasformando la información en todas sus formas y estados en un activo de altísimo valor, el cual se debe proteger y asegurar para garantizar su integridad, disponibilidad y confidencialidad.**

Los sistemas de seguridad de la información pueden ser algún dispositivo o herramienta física que permita resguardar un bien, un software o sistema que de igual manera ayude de algún modo a proteger un activo y que no precisamente es algo tangible, o una medida de seguridad que se implemente esto se lo puede realizar por medio de las políticas de seguridad que se basan en estándares para su creación.

El uso de estándares abiertos contribuye primordialmente en el aspecto económico de las grandes y pequeñas empresas al permitir el ahorro en licenciamiento y adquisición de hardware, ya que se reutilizan equipos debido a la manejabilidad y bajo consumo de recursos de las aplicaciones instaladas en ellos.

***Términos Indexados*—ISO, IEC, IDS, DMZ, QoS.**

I. INTRODUCCIÓN

Es una industria dedicada a la elaboración y comercialización de productos lácteos artesanales especializada en quesos maduros, manteniendo características de origen y calidad exigidas por el mercado, asegurando una relación personal, justa y transparente con sus clientes, proveedores, la comunidad y el medio ambiente.
FLORALP es una industria con visión de futuro, desde su inicio ha innovado y crecido a través de los años empezó elaborando leche pasteurizada y quesos frescos.

Documento recibido en Junio del 2015. Esta investigación se realizó como proyecto previo para obtener el título profesional en la carrera de Ingeniería en Electrónica y Redes de Comunicación de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte.
G.J.López, egresada de la Carrera de Ingeniería en Electrónica y Redes de Comunicación (teléfono 5939-3078-067; e-mail: gaby_janeth_7hotmail.com).

Hoy se ha convertido en el ejemplo de la industria láctea en la producción de quesos maduros artesanales como son queso holandés, cheddar, brie, camembert, gruyere, parmesano, tilsiter, raclette, ricotta, mozarella, mantequilla, crema, queso crema, yogurt, etc. Ubicando sus productos en los mejores autoservicios, hoteles, restaurantes, cafeterías, e industrialmente a nivel nacional.

Así la era del desarrollo humano, de procesos, de gestión de la calidad, de la mejora continua, del involucramiento donde la decidida intervención apoyo y ejecución de los miembros de la familia gravitaban enormemente en la consecución de las metas y objetivos; fortaleciendo los canales de comunicación internos y mejorando con preocupación permanente la calidad de vida, el conocimiento y el involucramiento de todos los colaboradores de todas las áreas.

De esta forma se lleva adelante una prospectiva de mercados internacionales naturales para los productos de la industria, siempre definida en hacer quesos maduros de excelente calidad para nichos especializados de dichos quesos y enmarcados en un sistema de gestión integral que garantice la sustentabilidad de la industria y la satisfacción de sus consumidores.

II. FUNDAMENTOS TEÓRICOS DE SEGURIDAD EN REDES

A. Seguridad informática

La seguridad informática se orienta a la protección de la infraestructura de red y todo lo relacionado a esta, de tal forma garantiza la confidencialidad, disponibilidad e integridad mediante la protección, clasificación y conocimiento de impactos o daños de las potenciales amenazas o intenciones perjudiciales de forma indirecta o directa para minimizar riesgos.

Confidencialidad
En la seguridad informática la confidencialidad se entiende por la protección de la información buscando prevenir la divulgación de información a personas o sistemas no autorizados, permitiendo únicamente el acceso a personas que cuenten con la debida autorización.

Integridad
Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema libre de modificaciones.

Disponibilidad
El sistema debe mantenerse funcionando eficientemente, estar disponible para quienes deban acceder a ella y ser capaz de recuperarse rápidamente en caso de fallo.

Autenticidad
Permite asegurar el origen de la información, la identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser.

B. Debilidades de un sistema de información

Los tres primeros puntos conforman el triángulo de debilidades del sistema. [1]

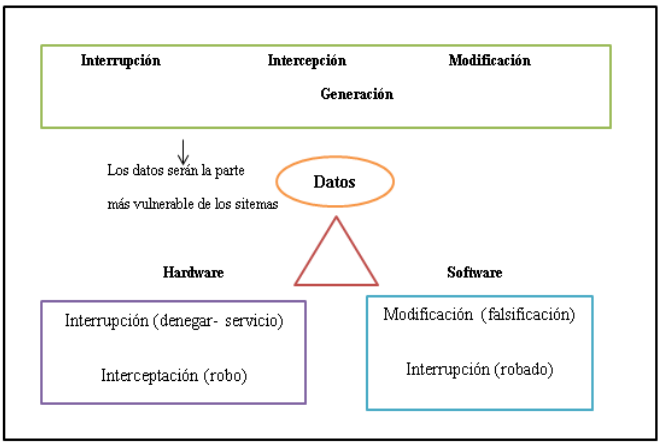

Figura 1. Triángulo de debilidades del sistema
Fuente: Jorge Ramiro Aguirre. Libro Electrónico de Seguridad Información y Criptografía

- *Hardware*

Pueden producirse errores intermitentes, conexiones sueltas, desconexión de tarjetas.

- *Software*

Puede producirse la sustracción de programas, ejecución errónea, modificación, defectos en llamadas a los sistemas.

- *Datos*

Pueden producirse la alteración de contenidos, introducción de datos falsos, manipulación fraudulenta de datos.

- *Memoria*

Pueden producirse de un virus, mal uso de la gestión de la memoria, bloqueo del sistema.

- *Usuarios*

Puede producirse la suplantación de identidad, accesos no autorizados visualización de datos confidenciales.

C. Ataques y amenazas

Ataque.- Es un método que intenta desestabilizar el funcionamiento de la red intentando obtener de forma no autorizada la información.

Amenaza.- Es cualquier cosa que pueda interferir con el funcionamiento adecuado de la red aprovechándose de las debilidades del sistema.

Formas de amenazas

Los ataques a los sistemas de seguridad son muy frecuentes por lo que se expone cuatro categorías de ataques como:

Interrupción
Es un ataque contra la disponibilidad esto se da cuando el sistema es destruido o se vuelve no disponible. La interrupción puede ser temporal o permanente dependiendo de qué tan grave es la amenaza, estos ataques son más rápidos de identificar pero lo más difíciles de solucionar por ejemplo: la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación.

Intercepción
Es un ataque no autorizado que se va contra la confiabilidad del sistema de seguridad, esto se da cuando una entidad puede ser (persona, un programa o un ordenador) desconocido accede a un recurso. La intercepción es la amenaza más difícil de detectar, por lo que no produce ningún cambio en el sistema.

Modificación
Este tipo de ataques se dedican a conseguir alterar o manipular la información de alguna forma no autorizada este es un ataque contra la integridad, principalmente los intrusos se dedican a cambiar los valores de un archivo o eliminar información que se esté utilizando aprovechándose de las vulnerabilidades de los sistemas de seguridad.

Generación
Es un ataque contra la autenticidad, una entidad no autorizada inserta objetos falsificados en el sistema. Ejemplos de este ataque son la inserción de mensajes falsos en una red o añadir registros a un archivo. Estos ataques se pueden clasificar de forma útil en términos de ataques pasivos y ataques activos (Salazar, 2011).

D. Mecanismos de seguridad

Los mecanismos de seguridad son técnicas que se utiliza para implantar un servicio, es decir, es aquel mecanismo que está diseñado para detectar, prevenir o recobrarse de un ataque de seguridad. [2]

Mecanismos de prevención
En esta etapa se toman las acciones necesarias para prevenir una posible intrusión o la violación de la seguridad, permitiendo aumentar la fiabilidad del sistema. Estas acciones

se pueden realizar tanto a nivel de software o a nivel de hardware.

Mecanismos de detección
Son aquellos que se utilizan para detectar violaciones a la seguridad o intentos de violaciones ya que si no se da cuenta del ataque el daño va a ser mayor. Como por ejemplo tenemos los programas de auditoría

Mecanismos de respuesta
Son aquellos que se aplican cuando una violación del sistema se ha detectado, ya que busca minimizar los efectos de un ataque o problema y finalmente retomar al sistema a su modo de trabajo normal. Como ejemplo tenemos las copias de seguridad o el hardware adicional.

Mecanismo de análisis forense
Permite determinar las acciones que ha realizado el atacante desde ver que agujeros de seguridad han utilizado para entrar al equipo, hasta ver las acciones que ha realizado en el sistema, de esta forma prevenir y detectar posteriores ataques al sistema.

E. Modelos de seguridad

Para la correcta implantación de la seguridad informática, se deben establecer y mantener acciones que busquen cumplir con los tres requerimientos para la información, estos son disponibilidad, confidencialidad e integridad.

Seguridad perimetral

El modelo de seguridad perimetral es un uno de los métodos posibles de defensa de un sistema que fortalecen el perímetro externo de la infraestructura de la red basándose en un conjunto de medidas estrategias que permiten y deniegan el acceso a determinados usuarios.

Seguridad por obscuridad

Un sistema por obscuridad consiste en mantener en secreto la existencia de la red, algoritmos y protocolos utilizados, de tal manera, que cualquier sistema puede ser seguro mientras nadie fuera de su grupo de implementación de seguridad se le permita conocer nada de sus mecanismos internos, un ejemplo de este modelo de seguridad es ocultando contraseñas en archivos binarios suponiendo que "nadie lo va a encontrar nunca".

Defensa de profundidad

El término defensa en profundidad (en ocasiones denominada seguridad en profundidad o seguridad multicapa) procede de un término militar utilizado para describir la aplicación de contramedidas de seguridad con el fin de formar un entorno de seguridad cohesivo sin un solo punto de error. Las capas de seguridad que forman la estrategia de defensa en profundidad incluyen el despliegue de medidas de protección desde los enrutadores externos hasta la ubicación de los recursos, pasando por todos los puntos intermedios. [3]

F. Tecnologías de seguridad

Las tecnologías de seguridad tienen como objetivo la implementación de diferentes sistemas integrales para la seguridad de la información como son los siguientes: [4]

VPN.- Una red privada virtual (VPN) es una tecnología utilizada en empresas de gran tamaño facilitando la extensión de la red pública, de tal forma que permite una conexión segura sin ningún riesgo restringiendo la información a personas ajenas a la empresa u organización. [5]

NAT.- El NAT tiene la tarea de traducir las IPs privadas de la red en una IP pública para que la red pueda enviar paquetes al exterior; y luego realizarla de forma inversa, es decir, traducir luego esa IP pública, de nuevo a la IP privada de una desktop.

Firewall.- Es un sistema o un grupo de sistemas (software o hardware) que permite o deniega diferentes servicios desde el exterior, es decir, que se conecta entre la red y el cable de la conexión a internet solo dejando pasar el tráfico autorizado desde y hacia el exterior como se muestra en la Figura 2.

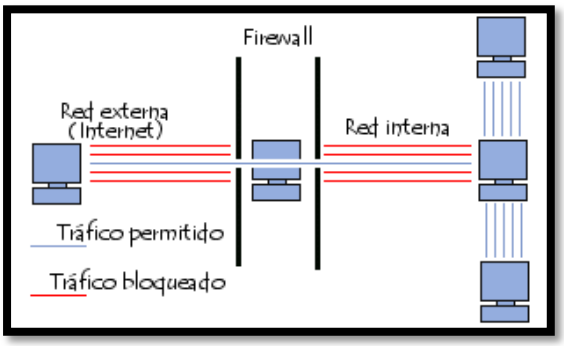

Figura 2. Implementación de un Firewall
Fuente: Seguridad en Linux Recuperado de: Mohan, K., Seagren E .,& Alder R.(2008)

Sistemas de detección de intrusos
Son la parte fundamental de la seguridad de los firewall, estos monitorizan la actividad de los sistemas en busca de violaciones de las políticas de seguridad, tales como ataques de denegación de servicios, sustracción o modificación de la información. [6]

- ✓ HIDS (Host-Bases Intrusion-Detection System)
- ✓ NIPS (Network Intrusion Prevention System)
- ✓ NIDS (Network-Based Intrusion Detection System)

En la Figura 3 se muestra el funcionamiento de un sistema de detección de intrusos

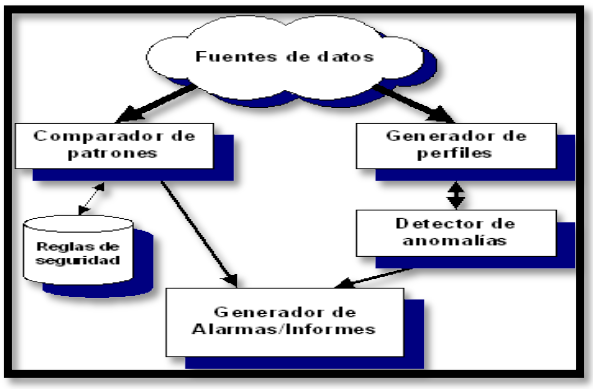

Figura 3. Esquema general de un Sistema Detector de Intrusos
Fuente: Elementos de detección de intrusos Recuperado de: http://www.dgonzalez.net/papers/ids/html/cap02.htm

G.Estándares de seguridad informática

Los estándares de seguridad son una herramienta que apoyan a la gestión de la seguridad informática, ya que los ambientes cada vez más complejos requieren de modelos que administren las tecnologías de manera integral, sin embargo, existen distintos modelos aplicables en la administración de la seguridad. [7]

Estándar internacional ISO/IEC 27001

De acuerdo (Estándar Internacional ISO/IEC 27001), menciona que:

Los estándares internacionales son una muy buena guía que proporciona un modelo para establecer implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). El diseño e implementación del SGSI de una organización está influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados el tamaño y estructura de la organización.

Adoptan algún modelo para aplicarse a los procesos de SGSI, como lo es el modelo PDCA (Planear-Hacer-Checar-Actuar). En la Figura 4 muestra el desarrollo el proceso de implementación de un SGSI:

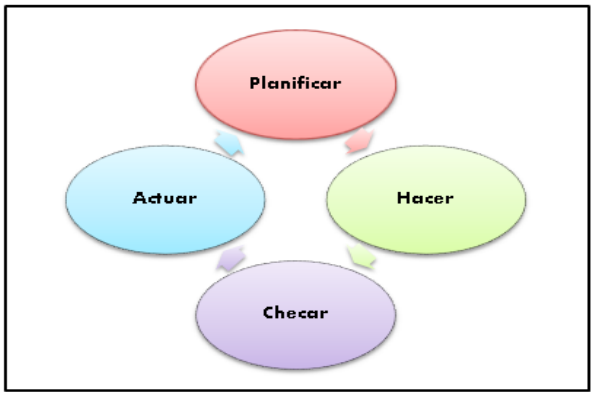

Figura 4. Modelo de desarrollo PDCA
Fuente: Modelo de Gestión (Muro, 2010) Recuperado de: http://goo.gl/poG11L

Modelo PDCA

A continuación, vamos a describir las actividades que se realizan en cada una de las cuatro fases del ciclo PDCA.

- Planificar

En esta fase se establecen políticas, objetivos, procesos y procedimientos relevantes para mejorar el riesgo y mejorar la seguridad de la información. Las políticas de seguridad que considere los requerimientos para que luego puedan ser aprobados por la dirección o la gerencia.

- Hacer

Esta fase cubre la implantación de las políticas, controles, procesos y procedimientos que reduzcan el riesgo a niveles considerados como aceptables.

- Checar

Durante esta fase se realizan diferentes tipos de revisiones para comprobar la correcta implantación del sistema, es decir, evaluar y medir el desempeño del proceso en comparación con la política, objetivos y de esta forma reportar los resultados a la gerencia para su revisión.

- Verificar

Tomar acciones correctivas y preventivas basadas a una auditoría interna para el mejoramiento del SGSI, comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar la forma de proceder, además es importante tener la seguridad de que las mejores introducidas alcanzan los objetivos previstos.

Áreas y controles

La norma se desarrolla en 11 áreas o dominios que recogen los 133 controles a seguir.

- Política de seguridad.
- Organización de la información de seguridad.
- Administración de recursos.
- Seguridad de los recursos humanos.
- Seguridad física y del entorno.
- Administración de las comunicaciones y operaciones.
- Control de accesos.
- Adquisición de sistemas de información, desarrollo y mantenimiento.
- Administración de los incidentes de seguridad.
- Administración de la continuidad de negocio.
- Marco legal y buenas prácticas.
-

III. Análisis de la Infraestructura Actual de la Red de Datos de la Floralp

A. Estudio De La Situación Actual De La Red

Como se observa en la Figura 5 se trata de una red plana que hace uso de varias direcciones IP's, además, no cuenta con un modelo jerárquico por lo que a continuación se detalla cada equipo de networking.

Se cuenta con dos routers un Cisco 1700 del proveedor de CLARO y un Cisco1800 del proveedor de CNT que son de propiedad de cada proveedor.

En la parte de distribución existe el router Cisco-Linksys WRT110 donde este hace uso de una de las cuatro IP's públicas, por lo tanto, este canal al no ser filtrado por ningún equipo de seguridad como firewall IDS/IPS (Sistema de Detección de Intrusos y Sistema de Prevención de Intrusos), representa una gran vulnerabilidad en cuanto al tráfico que puede ingresar o salir a través de este enlace.

Dos IP's públicas del proveedor de Claro se usan, una para el servicio de LIFESIZE y la otra IP para el servidor KYPUS donde este brinda el servicio de Firewall diseñado para prevenir el acceso no autorizado, además, este equipo se conecta hacia el switch Linksys SF 2000 donde también provee el servicio de conexión de los usuarios hacia la red externa.

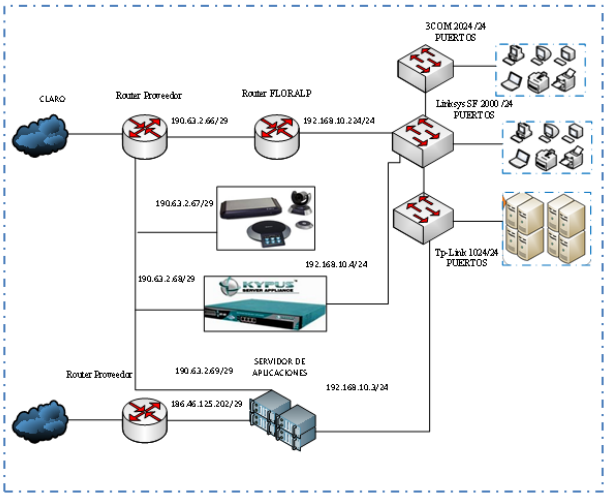

Figura 5. Diagrama de topología de red
Fuente: Graficación en Microsoft Visio 2010 realizado por Gabriela López

En lo referente al acceso se distingue dos capas: la primera conformada por el switch 3Com 2024 que se encuentra ubicada para la planta de producción que se conecta a través de Fibra Óptica hacia el switch Linksys SF 2000 para la planta administrativa y la segunda por el switch Tp-Link 1024 para la conexión de los servidores, donde estos dan el servicio a los usuarios.

B. Direccionamiento IP

La red de datos de la industria FLORALP utiliza 10 direcciones IP's públicas que se describen los rangos en la siguiente Tabla 1.

Tabla 1. Direcciones IP's Publicas

IP PÚBLICA	MÁSCARA	DESCRIPCIÓN
190.63.x.x	255.255.255.0	ROUTER FLORALP
190.63.x.x	255.255.255.0	LIFESIZE
190.63.x.x	255.255.255.0	RED EXTERNA
190.63.x.x	255.255.255.0	APPEON
190.63.x.x	255.255.255.0	SIN USO
186.46.x.x	255.255.255.0	SERVIDOR DE APLICACIONES
186.46.x.x	255.255.255.0	SIN USO
186.46.x.x	255.255.255.0	SIN USO
186.46.x.x	255.255.255.0	SIN USO
186.46.x.x	255.255.255.0	SIN USO

Fuente: Proporcionado por el Departamento de Sistemas

C. Accesos de los usuarios

Los usuarios al momento que manejan la información no son responsables ya que no cuentan con lineamientos de alguna política de seguridad para la protección de la misma. Además, la información que manejan se encuentra vulnerable ya que personas no autorizadas ajenas a la industria tienen acceso sin ningún problema, por lo que ellos no tienen ningún privilegio durante el tiempo de uso de la red de la FLORALP.

D. Elementos de red

Los principales elementos de red que son parte de la infraestructura de la misma se detallan en la siguiente Tabla 2.

Tabla 2. Descripción de los Rack's

Cantidad	Elemento de red	Ubicación
5	Servidores Físicos	Rack 2
2	Router	Rack 1
1	Switch Administrables	Rack 1
1	Switch no Administrable	Rack 2
2	Switch no Administrable	Rack 3
1	Central PBX	Rack 1
	Equipos de Proveedor	
2	CLARO	Rack 1
1	Router	
	ODF	
2	UPS	Rack 2
1	Monitores	Rack 2
	Equipos de Proveedor CNT	
1	Router	
1	ODF	Rack 2

Fuente: Proporcionado por el Departamento de Sistemas

E. Servidores

Un servidor es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente, especializada con muy altas capacidades de proceso, encargada de proveer diferentes servicios a las redes de datos, tanto inalámbricas como las basadas en cable; estos servidores tienen sistemas que les permiten resolver ciertas averías de manera automática así como sistemas de alerta para evitar fallas en operaciones de datos críticos, ya que deben estar encendidos los 365 días del año las 24 horas del día.

- Servidor de dominio
- Servidor de aplicaciones
- Servidor de respaldos
- Servidor DHCP

F. Medición de tráfico de red

Para tener un conocimiento real de cuál es la situación actual de la red se ha realizado un monitoreo de cada IP para determinar la información sobre qué tipo de puertos y protocolos son utilizados dentro de la red interna. Para el monitoreo se ha tomado en cuenta diferentes herramientas de monitoreo que se pueden utilizar, además se deberá considerar que tipo de aspectos van a ser monitoreados, de tal forma entre los más considerados para la realización del presente proyecto son:

- Ancho de banda

  En la Figura 6 se observa el consumo del ancho de banda durante un mes donde se puede apreciar cuatro picos en el horario de 09:30am a 10:30am, 11:30am a 12:30pm, 16:00pm a 16:30 y de 16:30pm a 17:30pm donde se realiza más congestión de información de la red.

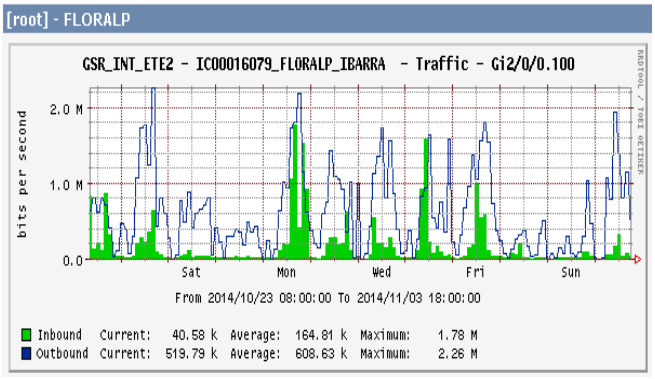

Figura 6. Consumo del Ancho de Banda durante un mes
Fuente: Resultados obtenidos del monitoreo mediante el software MRTG proporcionado por una IP pública de CLARO.

- Tipos de Puertos y Protocolos.

En la siguiente Figura 7 se realiza un cuadro estadístico que nos indica que tipos de protocolos son más utilizados por todos los usuarios y que pertenecen en el rango 192.168.10.0/24.

- Servicios utilizados

El análisis de este parámetro se lo realiza, mediante los datos obtenidos del monitoreo de puertos y protocolos donde contienen las gráficas de las estadísticas que indican el tipo de servicios más utilizados dentro de la red con lo que se determina que el protocolo HTTP, SMTP y POP3 tienen un porcentaje alto por motivo que los usuarios hacen uso de servicios que prestan cada uno como el correo electrónico, llamadas o trasferencia de archivos mediante Skype y el acceso al servidor de aplicaciones que se lo realiza mediante una página web.

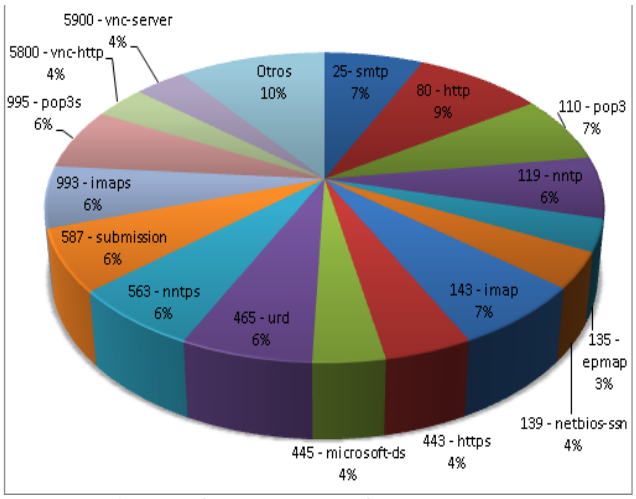

Figura 7. Grafico Estadístico de puertos más utilizados por los usuarios.
Fuente: Datos obtenidos mediante las herramientas NTOP y Wireshark

IV. Diseño Del Sistema De Seguridad Perimetral Para La Red De Datos.

A. Planteamiento de las políticas de seguridad

Antes de realizar un diseño de un sistema de seguridad perimetral es importante conocer cuáles son los recursos y servicios que brinda la red. De tal manera se debe realizar un documento donde consten todas las políticas de seguridad de red. En este documento constará de controles y objetivos utilizando el modelo PDCA para establecer las políticas, el manejo y responsabilidad de la red, el diseño de un modelo de seguridad y los planes de contingencia o planes de acción en caso de que la seguridad haya sido violada.

B. Políticas de seguridad

Las políticas de seguridad son normas que permiten conocer el comportamiento de la red con relación a la seguridad de la información, cada definición permitirá realizar procedimientos y planes que protejan a los recursos de la red tanto en pérdidas y daños que puedan suscitarse.

Una parte muy importante del desarrollo de políticas es que estas deben ser bien concisas y efectivas ya que de ellas depende mucho que la industria pueda proteger toda su información. Para que el administrador de la red pueda elaborar el documento de las políticas de seguridad debe tener conocimiento de que tipo de servicios y recursos son utilizados por la mayoría de usuarios y de esta forma le permitirá priorizar que tipo de usuarios pueden tener acceso y cuales tendrán restricciones.

C. Desarrollo de los controles y políticas del SGSI afines a la seguridad de la información

Cada una de las políticas realizadas en este documento se encuentra elaborada con el apoyo del Jefe del departamento de sistemas. Los diferentes objetivos, controles y políticas utilizadas en el presente proyecto son los siguientes:

Objetivos

Crear políticas que garanticen el buen uso, manejo, integridad, exactitud y preservación de la información de la industria, y protegerla contra la modificación, divulgación, manipulación o destrucción no autorizada o accidental.

Garantizar la privacidad de la información personal, sensitiva o vital de la industria, sus empleados y sus beneficiarios, de esta forma, proveer de sanciones en caso de que ocurra mal uso o pérdida de información reservada de la industria.

Alcance

Estas políticas aplican a todos los departamentos de la industria que tengan acceso a equipos de Computación y/o Sistemas de Información, que ingresan, crean, procesan o tienen custodia de información.

Responsabilidad

Son responsables todos los gerentes y jefes de cada departamento, personal administrativo y empleados de observar y cumplir la política de seguridad de la información dentro del área a su responsabilidad y por ende hacer cumplir al personal bajo su cargo. En la siguiente Figura 8 se puede mirar una política planteada.

FLORALP INDUSTRIA LECHERA FLORALP S.A

DOMINIO	1. Política de seguridad.
CONTROL	1.2 Política de seguridad de información.
ALCANCE	Esta política se aplica a todos los que pertenecen al departamento de sistemas donde son responsables de la elaboración y ejecución de las políticas de seguridad con el compromiso de las autoridades.
RESPONSABLE	Departamento de sistemas

- El departamento de sistemas debe identificar, supervisar regularmente la implantación de las políticas de seguridad de información.
- Proporcionar apoyo técnico y administrativo a una fuente especializada en seguridad de la información si fuese necesario.

Figura 8. Política Planteada
Fuente: Planteamiento de las políticas de seguridad de la industria FLORALP

D.Selección de software para firewall en base a la norma IEE 830.

Análisis de las posibles soluciones de OPEN SOURCE

A continuación se detalla las posibles soluciones de open source.

- CentOS
- Ubuntu
- Debian

Calificación para cada solución de software para la seguridad perimetral

Luego de realizar la valoración a cada requerimiento basándose en la norma IEE 830, se procede a la comparación respectiva de cada solución de software para la implementación del sistema de seguridad.

Tabla 3.Valoración para cada solución de software

REQUERIMIENTO	CENTOS	UBUNTU	DEBIAN
REQ01	1	1	1
REQ02	2	2	2
REQ03	1	1	0
REQ04	2	1	1
REQ05	2	1	1
REQ06	2	1	1
REQ07	1	0	1
REQ08	1	1	1
REQ09	2	1	1
REQ10	1	0	1
REQ11	1	1	1
REQ12	1	0	1
REQ13	1	0	0
REQ14	1	0	0
REQ15	1	2	1
REQ16	0	0	1
TOTAL	**20**	12	14

Fuente: Realizado por Autor

Una vez realizado la calificación de cada requerimiento se observó que el software con mayor puntaje es CentOS, la confiabilidad y la estabilidad de esta herramienta permite la implementación del sistema de seguridad perimetral.

CentOS entre sus características importantes se destaca por el alto uso como servidores y una gran compatibilidad con sistemas operativos, aplicaciones y servicios; mayor confiabilidad, comunidades, soporte técnico para la solución de problemas, eficiencia de la administración de la red, un alto grado de procesamiento de información y una amplia gama de compatibilidad de plataforma, por lo tanto, CentOS hace la mejor opción para la solución de seguridad informática.

E. Selección del software para el sistema de detección de intrusos en base a la norma IEE 830

Análisis de las posibles soluciones de OPEN SOURCE

A continuación se detalla las posibles soluciones de open source.

- Snort
- Suricata

Calificación para cada solución de software para la seguridad perimetral

Luego de realizar la valoración a cada requerimiento basándose en la norma IEE 830, se procede a la comparación respectiva de cada solución de software para la implementación del sistema de seguridad.

Tabla 4.Valoración para cada solución de software IDS

REQUERIMIENTO	SNORT	SURICATA
REQ01	1	1
REQ02	1	0
REQ03	1	1
REQ04	2	1
REQ05	1	0
REQ06	0	1
REQ07	1	0
REQ08	2	1
REQ09	1	1
REQ10	1	0
REQ11	1	0
REQ12	1	1
REQ13	2	1
TOTAL	15	8

Fuente: Realizado por Autor

Una vez realizado la calificación de cada requerimiento se observó que el software con mayor puntaje es Snort, el grado de integridad al resto del IDS suministra una efectividad al proporcionar confiabilidad y adaptabilidad con diferentes plataformas o ambientes de tal manera es un complemento perfecto para el sistema de seguridad perimetral.

Snort permite que los administradores y los encargados puedan observar y comprender lo que les dicen esta herramienta revelando problemas antes que ocurra la pérdida., de tal manera Snort hace la mejor opción para la solución de detección y búsqueda de anomalías dentro de la infraestructura de red.

V. Implementación Del Sistema De Seguridad Perimetral Para La Red De Datos

La base para la implementación del sistema de seguridad perimetral son los siguientes puntos:

- Topología de red
- Plan de direccionamiento
- Ubicación de servidores y puntos de acceso
- Análisis de los dispositivos de red con el fin de identificar los aspectos de hardware y software que pueden influir con la implementación.

Luego de haber realizado y analizado cada punto se puede dimensionar la red con las aplicaciones y protocolos que están siendo utilizados por los usuarios y servidores así como la necesidad del ancho de banda.

A. Diseño de la ubicación del servidor de seguridad perimetral

Direccionamiento IP de las tarjetas de red del servidor de seguridad

Para el nuevo diseño de la red se ha tomado en consideración un nuevo direccionamiento IP que permita la facilidad de identificar cada interfaz del servidor que se encuentra conectado a la infraestructura de red, se mantiene un solo de segmento de red debido a que el número de usuarios no es elevado, de tal manera, evitar el desperdicio de direcciones IP's.

Tabla 5. Direccionamiento del servidor Firewall

Equipo	Interfaz	IP	Máscara	DNS
SERVIDOR FIREWALL	eth0	190.63.2.66	/28	200.25.207.114
	eth1	192.168.20.1	/24	200.25.207.114
	eth2	192.168.20.254	/24	200.25.207.114

Fuente: Direccionamiento IP Realizado por Gabriela López

Diseño y análisis del ambiente del servidor de seguridad perimetral

El servidor de seguridad perimetral asume roles importantes en la industria en este caso es utilizado como firewall para establecer una metodología de seguridad dirigida tanto para el tráfico interno como externo a la red. Las necesidades de la red son:

- Asegurar el acceso y fiabilidad a la red.
- Mantener la confidencialidad e integridad de la información transmitida.
- Acceso seguro y rápido a los servidores internos.

Descripción básica del entorno de trabajo del servidor de seguridad perimetral

El servidor de seguridad perimetral va estar en medio del router del proveedor de CLARO, el switch Linksys SF 2000/24 y del Switch TP-LINK 24 ports10/100Mbps, este servidor va a tener tres interfaces de red, una llamada WAN que va a estar dando la cara al internet, la otra se denomina DMZ donde están ubicados todos los servidores de la industria y la última interfaz se llama LAN que va a manejar la red interna donde se encuentran ubicados todos los usuarios y dispositivos inalámbricos identificados dentro de la red.
Como se indica en la Figura 9.

Servidor firewall

Las reglas de las iptables que van a aplicarse para asegurar la red interna como externa son las siguientes:

- Permitir el tráfico a la interfaz interna.
- Permitir el tráfico interno.
- Hacer enmascaramiento de la red externa a la interna y viceversa.
- Permitir acceso desde LAN a WAN por los siguientes puertos.
  - ✓ Puerto HTTP www
  - ✓ Puerto FTP
  - ✓ Puerto SSH
  - ✓ Puerto POP3 y SMTP e-mail

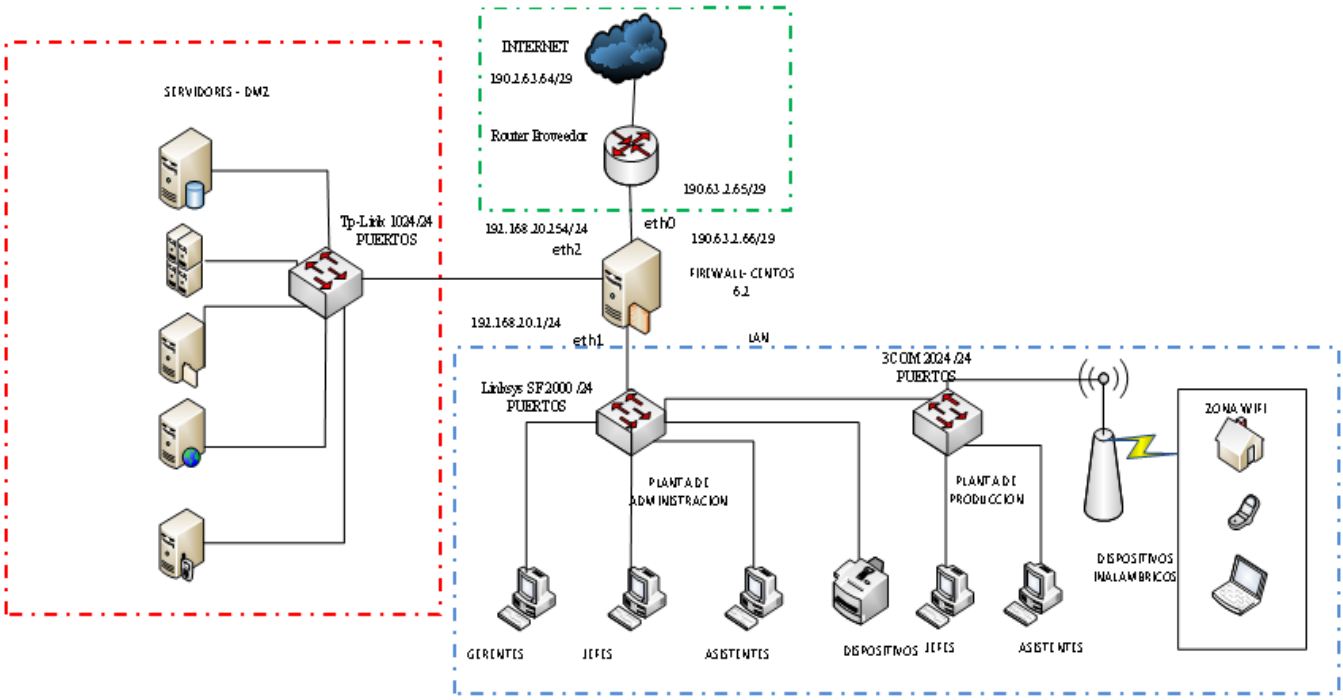

Figura 9. Diseño de la topología de red
Fuente: Graficación en Microsoft Visio 2010 realizado por Gabriela López

B. Ubicación del IDS dentro de la topología de red

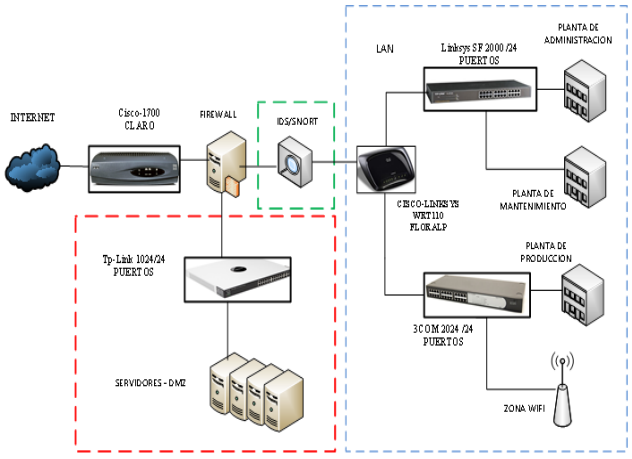

Figura 10. Ubicación del IDS
Fuente: Graficación en Microsoft Visio 2010 realizado por Gabriela López

Requisitos para la instalación de snort

Apache.- Es un servidor web HTTP de código abierto para plataformas de sistemas operativos como UNIX y Windows NT. Su propósito es suministrar un servidor seguro y eficiente que brinde servicios HTTP actuales con soporte PHP y configurable para las aplicaciones de bases de datos como MySQL (Camelo, 2010).

PHP.- Es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web, entre sus importantes características esta la compatibilidad con las bases de datos como MySQL.

MySQL.- Es un sistema de gestión de base de datos relacional, multihilo y multiusuario, que utiliza como módulo de salida de las alertas proporcionadas por el IDS. Es necesario tener almacenadas las alertas en una base de datos para mantener un buen funcionamiento del sistema. (Alfaro, 2010).

BASE.-Es una interfaz web en PHP que permite gestionar de una forma fácil y cómoda las bases de datos de seguridad generadas por IDS, cortafuegos, y herramientas de monitoreo.

VI. Pruebas y Resultados

Se realiza las respectivas pruebas de funcionalidad de cada uno de los servicios implementados en la red de datos, con el fin de observar y comprobar su correcto desempeño. Para lo cual, se propone efectuar la simulación de determinados ataques informáticos y el establecimiento de un conjunto de reglas para filtrado de tráfico específico

A. Desarrollo de las pruebas del servicio squid.

Acceder a la página web de youtube.com definida en el archivo sitios sociales

A continuación se accede al sitio web www.youtube.com definido en el archivo sitios sociales debido a que existe concurrencia, como se muestra en la siguiente Figura 64 la denegación a esta página donde su dirección IP es de un asistente.

Figura 11. Acceso a un sitio social
Fuente: Captura de pantalla del acceso a la palabra youtube

B. Test de penetración

A continuación se simulan ciertos ataques informáticos que se cometen usualmente dentro de la seguridad de la información entre ellos: ataques por DoS, avenamiento ARP y por fuerza bruta. Además se señalan los pasos y herramientas que hacen uso para la ejecución dentro de la red de datos de la industria FLORALP.

Para la realización de estas pruebas se debe considerar el software en este caso se ha escogido Kali Linux donde no es más que una distribución avanzada gratuita basada en Debian para pruebas de penetración y auditorias de seguridad.

El test de penetración se realiza mediante un conjunto de fases para la simulación de ataques en escenarios controlados permitiendo evaluar la seguridad del sistema de seguridad, de tal forma, encontrar los puntos débiles y vulnerables de la red.

En la siguiente figura 13 indica las fases de un test de penetración.

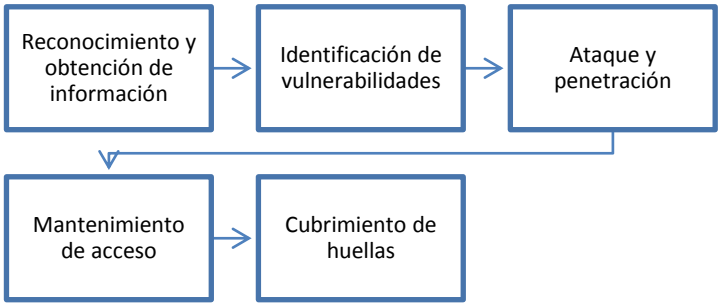

Figura 12. Anatomía de un test de penetración
Fuente: Ataques informáticos, Recuperado de http://goo.gl/VCc6Ef

Fase de exploración

Escaneo de puertos y host

Para la simulación del ataque se utiliza Nmap una herramienta de código abierto para exploración de red y auditoría de seguridad donde este utiliza paquetes IP en bruto en formas novedosas para determinar qué hosts están disponibles en la red, qué servicios están ofreciendo y qué sistemas operativos que se están ejecutando.

Este se lo hace mediante la herramienta de Kali Linux donde se puede visualizar que host se encuentran mediante el siguiente comando.

nmap –sn 192.168.20.1/24

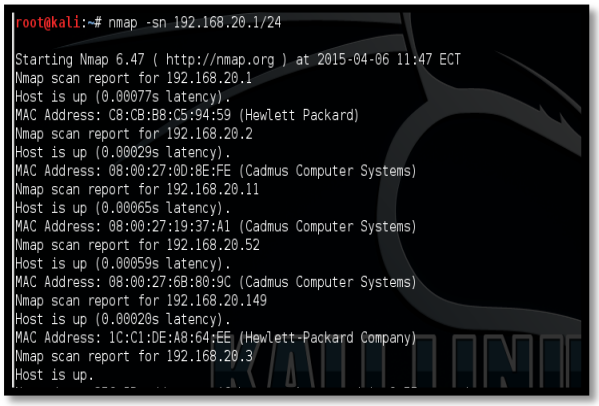

Figura 13. Escaneo de host mediante Nmap
Fuente: Exploración de host mediante Kali-Linux

En la figura 15 se muestra el despliegue de la alerta en Snort:

Figura 14. Alertas en Snort
Fuente: Captura de las alertas por Snort

Luego de haber realizado diferentes ataques antes mencionados Snort ha identificado todas las anomalías, por lo tanto, nos brinda un cuadro estadístico del escaneo de anomalías mediantes sus sensores.

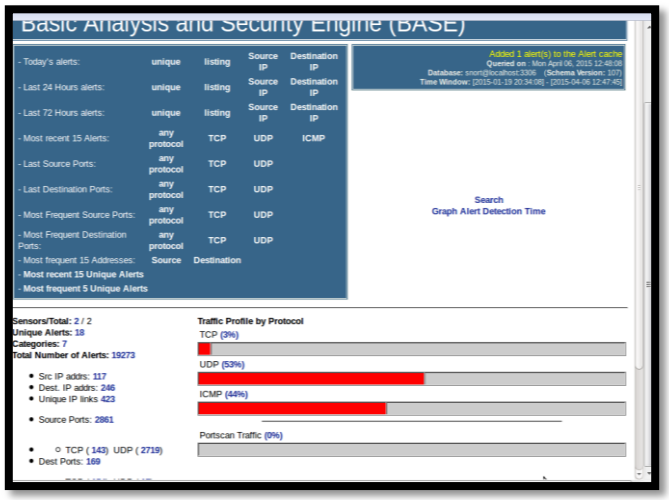

Figura 15. Alertas en Snort
Fuente: Captura de las alertas por Snort

A lo que se refiere el test de penetración permitió que a ciertas técnicas que ofrece Kali Linux simular un ambiente para la ejecución de los ataques internos, donde fueron descubiertos mediante ciertas pruebas comunes como la denegación de servicios, avenamiento ARP y ataques de fuerza bruta donde tuvieron éxito debido a que la red en ese momento no contaba con alguna seguridad.

VII. Análisis Económico

A. Presupuesto referencial

Para poder brindar una solución de bajo costo para la industria se realiza un presupuesto referencial de los equipos, instalación, configuración del sistema de seguridad perimetral. Este proyecto al tener un sistema bajo software libre, que es una plataforma segura y libre permite tener una alternativa confiable y económica.

Detalle del costo total referencial

El costo total referencial para la implementación del sistema de seguridad perimetral se ha tomado todos los equipos y herramientas considerando que fuesen nuevos y en caso de implementación en otra sucursal.

El total del proyecto es la suma de los componentes para la instalación del sistema de seguridad perimetral es de $4946.00 en caso de que no se cuente con los equipos.

Pero es importante la reutilización de la tecnología por lo que no se han tomado ciertos equipos debido a que ya existen dentro de la infraestructura de la red y el costo quedaría en un total de $2180.00 Todos los precios están sujetos a cambios, en vista que fueron cotizados con la fecha de mayo de 2015

Costo beneficio

Cálculo del costo-beneficio

Para el análisis del costo beneficio del proyecto es necesario analizar los costos incurridos en la implementación del sistema de seguridad perimetral y los beneficios que generará el proyecto con la implementación del mismo haciendo uso de tecnología existente, para lo cual utilizaremos la siguiente fórmula:

$$\frac{B}{C} = \frac{Beneficios}{Costos\ y\ Gastos}$$

Luego del análisis de los costos, gastos y beneficios que generan el proyecto aplicamos la fórmula para la determinación del beneficio costo, para lo cual se utilizan los siguientes parámetros de evaluación:

Reemplazando los valores en la fórmula tenemos:

$$\frac{B}{C} = \frac{Beneficios}{Costos\ y\ Gastos}$$

$$\frac{B}{C} = \frac{2766.00}{2180.00}$$

$$\frac{B}{C} = 1{,}2$$

Todos los resultados obtenidos indican que es factible y rentable implementar el presente proyecto.

Beneficiarios

La seguridad generalmente no es una inversión que genere un beneficio económico, se trata de prevenir pérdidas. En otras palabras, cuando se invierte en seguridad, las instituciones no esperan ganancias, el objetivo es reducir los riesgos que amenazan la información, con el propósito de minimizar la cantidad de pérdidas de información gracias a la inversión que se realiza.

Los beneficiarios de este sistema serian todos los usuarios que pertenecen a los diversos departamentos que hacen uso de los servicios que ofrece la red de datos debido a que toda la información que se encuentran manejando estaría mejor resguardada.

Otros de sus beneficios son las restricciones de acceso de los usuarios a sitios que eventualmente generen daño y la

limitación del uso del ancho de banda en favor de aquellas aplicaciones que son claves para la industria.

Gracias a la utilización de software libre brinda servicios de alto nivel sin pagar ningún precio para la adquisición del mismo permitiendo ser muy competitivo con software pagados.

CONCLUSIONES

Se debe tener bases teóricas que nos brinden información suficiente sobre cuáles son las principales características de un sistema de seguridad perimetral como base para la realización del presente proyecto, debido a que esto constituirá como fuente de investigación para próximos interesados sobre seguridad de información.

El análisis del tipo de tráfico que se encuentra circulando dentro de la infraestructura de la red nos permite conocer los servicios y protocolos que cada uno de los usuarios manejan, de tal forma, se puede determinar los requerimientos necesarios para el diseño del sistema de seguridad perimetral.

Para el diseño del sistema de seguridad perimetral se ha tomado en cuenta la norma ISO/IEC 27001 para la elaboración de las políticas de seguridad, debido a que se sigue un proceso de mejora continua la que nos permita tener un esquema ágil y flexible que se ajusta a los requerimientos de la industria.

El análisis de diferentes plataformas de Software en base al estándar IEEE 830 de especificaciones de requerimiento de software permite la selección de la mejor alternativa que se ajuste a los requerimientos del diseño del sistema de seguridad perimetral.

El uso de software libre en instituciones privadas se ha convertido en un factor fundamental en la gestión, administración y seguridad de las tecnologías de la información debido a que consume muy pocos recursos de memoria, procesador y espacio en disco del computador, permitiendo la reutilización de recursos y disminución de gastos por parte de la industria al no tener que adquirir nuevos equipos.

Mediante la implementación el servicio del proxy la caché del squid permite el filtrado de contenidos y por su capacidad de hacer caché, se logró aumentar el tiempo de respuesta en la navegación y evitar saturación del canal de internet, manteniendo un monitoreo en tiempo real y estadísticas diarias de navegación.

Snort es un software IDS de gran aceptación, potente y gratuito lo cual nos permite conocer cuando está siendo atacada mediante sensores que realizan un monitoreo constante.

La integración IDS identificó satisfactoriamente los ataques simulados con la herramienta Kali-Linux de hacker ético, la cual es ampliamente utilizada para un test de penetración en la red, comprobando su eficiencia frente a una serie de pruebas con diversas técnicas.

Se debe estar consciente de que no existe algún sistema que brinde una protección completa pero con la mejora continua y la adopción de métodos y estándares de seguridad de la información se mantiene un nivel de seguridad aceptable que reduce los riesgos de la red.

REFERENCIAS

[1] Aguirre, J. R. (2006). Libro Electrónico de Seguridad Información y Criptografía. Madrid-España.

[2] Estrella. (Abril de 2010). Mecanismos de Seguridad. Recuperado el Septiembre de 2014, de http://www.buenastareas.com/ensayos/Mecanismos-De-Seguridad/229947.html

[3] VINUEZA, T. (2012). HONEYNET VIRTUAL HÍBRIDA EN EL ENTORNO DE RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE DE LA CIUDAD DE IBARRA. Ibarra.

[4] Manuel, I. L. (30 de Mayo de 2013). SliderShared.com. Recuperado el 31 de Marzo de 2014, de http://es.slideshare.net/MelvinBrian/seguridad-en-profundidad

[5] MICHILENA, M. A. (2013). METODOLOGÍA DE SEGURIDAD INFORMÁTICA CON BASE EN LA NORMA ISO 27002 Y EN HERRAMIENTAS DE PREVENCIÓN DE INTRUSOS PARA LA RED ADMINISTRATIVA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA. Ibarra.

[6] Seguridad, F. d. (s.f). Fundamentos de Seguridad Informatica. Recuperado el Octubre de 2014, de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Estandares.php

[7] Torres, V. (13 de Marzo de 2012). Ciber Informatico. Recuperado el 6 de Abril de 2015, de http://ciberinfosystem.blogspot.com/2012/03/anatomia-de-un-ataque.html

Gabriela J. López P.

Nació en Ibarra- Ecuador el 5 de Enero de 1989. Realizó sus estudios primarios en la Escuela "María Angélica Idrobo". En el año 2006 obtuvo su título de Bachiller en ciencias especialización físico matemáticas en el colegio "Teodoro Gómez de la Torre". Actualmente, egresada de la Carrera de Ingeniería en Electrónica y Redes de Comunicación de la Universidad Técnica del Norte de la ciudad de Ibarra.